Guide

Cisco public

# Cisco Network Security

October 2026

© 2026 Cisco and/or its affiliates. All rights reserved.

# Contents


Introduction 3

SKUs and ordering guidance for Cisco Secure Firewall Appliances 10

Cisco Secure Firewall Small Business Edition License Pack 30

Ordering vDP with the Cisco Secure Firewall Platform 32

SKUs and ordering guidance for Cisco Security Manager 115

SKUs and ordering guidance for Cisco Secure Firewall Management Center 117

SKUS and Ordering Guidance for Cisco Secure Firewall Management Center Virtual Appliance 118

Connect and protect bundle ordering 121

SKUs and ordering 121

Additional resources 124

Cisco Capital Financing 124


© 2026 Cisco and/or its affiliates. All rights reserved.

# Introduction

**Purpose**

This document describes ordering Cisco physical, virtual, and containerized network security solutions, including:

- Cisco Secure Firewall Threat Defense (FTD).
- Cisco Secure Firewall Adaptive Security Appliance (ASA).
- Cisco Firepower 1000 Series, 4100 Series, and 9300 Series Appliances (which can run either FTD or ASA software, and in case of 9300 could run both ASA and FTD on separate Service Modules).
- Cisco Secure Firewall 200 Series, 1200 Series, 3100 Series,4200 Series, and 6100 Series Appliances (which can run either FTD or ASA software).

In addition, this guide details the process of enabling extended logging and analytics for both FTD and ASA platforms as well as Cisco ISE Passive Identity Connector (ISE-PIC) for identity integration into FTD.

This guide will help you make sure that the right quantities and types of parts are selected to reduce the risk of order rejection.

**Audience**

This guide is intended for Cisco Sales Teams and Partners – and that includes Distributors.

**Scope**

This document covers orderability for the following products, associated licenses and options:

- Cisco Secure Firewall (both Firewall Threat Defense and ASA software).
- Hardware appliances (Cisco Firepower or Cisco Secure Firewall ).
- Virtualized and containerized appliances (FTDv and ASAv).

Firewall management solutions

- **Cisco Secure Firewall Management Center**: provides complete and unified management over firewalls, application control, intrusion prevention, URL filtering, and advanced malware protection. Quickly and easily go from managing a firewall to controlling applications to investigating and remediating malware outbreaks. Firewall Management Center is available in all form factors – physical appliance, virtual appliance, public cloud and cloud-delivered (software as a service model).
- **Cisco Security Cloud Control** helps you establish and maintain a security posture by managing security policies across Cisco security devices. Cisco Security Cloud Control also incorporates the cloud-delivered version of Secure Firewall Management Center. As a cloud service, it is an always-available, highly reliable, highly scalable, multitenant platform.

Cisco Security Cloud Control provides management of security policy, objects and configuration for Cisco Adaptive Security Appliance and Cisco Secure Firewall Threat Defense (formerly Next-Generation Firewalls, or NGFW). Also supported are the Meraki MX Firewalls and AWS Security Groups for pure policy and object management. Configuration management for these platforms is still available through their native user interface.

**Note:** For the Cisco Security Cloud Control Ordering Guide, please click here.

© 2026 Cisco and/or its affiliates. All rights reserved.

- **Cisco Security Manager software** is an on-premises centralized management platform for Cisco Adaptive Security Appliances (ASA), enabling consistent policy enforcement, troubleshooting, and summarized reports.

#### Optional Software

- Cisco Secure DDoS Protection (formerly Radware Virtual DefensePro DDoS Mitigation).
- Cisco Secure Client (formerly Cisco AnyConnect Secure Mobility Client).

#### Support

- Cisco Smart Net Total Care appliance support services.
- Cisco Software Application Support plus Upgrades (SASU).

**Note:** Any order for a service will be subject to the detailed terms and conditions presented in this guide.

#### Selecting the Appropriate Management Solution

Several management solutions are available to manage Cisco Secure Firewalls. Use these guidelines to choose the best or ask a Cisco Security expert for advice.

Choosing the right management solution is tied to a few factors:

- The software image you select, either Firewall Threat Defense (FTD) or ASA software image.
- Willingness to use a cloud-based solution for management.
- Need for specific features or environment scale.

Local managers are included with both software options for single firewall deployments:

- ASDM is included with the ASA software image.
- Firewall Device Manager (FDM) is included with the Firewall Threat Defense software Image for all supported appliance models (Cisco Firepower 1000 Series, 4100 Series and 9300 Series; Cisco Secure Firewall 1200 Series, 200 Series and 3100 Series).

The Cisco Secure Firewall Threat Defense software image enables centralized management with either an on-premises, virtual or cloud-based manager - Cisco Secure Firewall Management Center.

Cisco Security Cloud Control unifies management across Cisco security solutions and incorporates the cloud-delivered version of Secure Firewall Management Center. This makes Cisco Security Cloud Control the best option for customers who want to use a cloud-based solution for the management of ASAs, FTDs or a mix of ASAs and FTDs from a single pane of glass.

Devices running the ASA software can be managed centrally by the Cisco Security Manager (on-premises) or Cisco Security Cloud Control (Cloud).

The following table can help guide you in which manager to select for your firewall deployment:

© 2026 Cisco and/or its affiliates. All rights reserved.

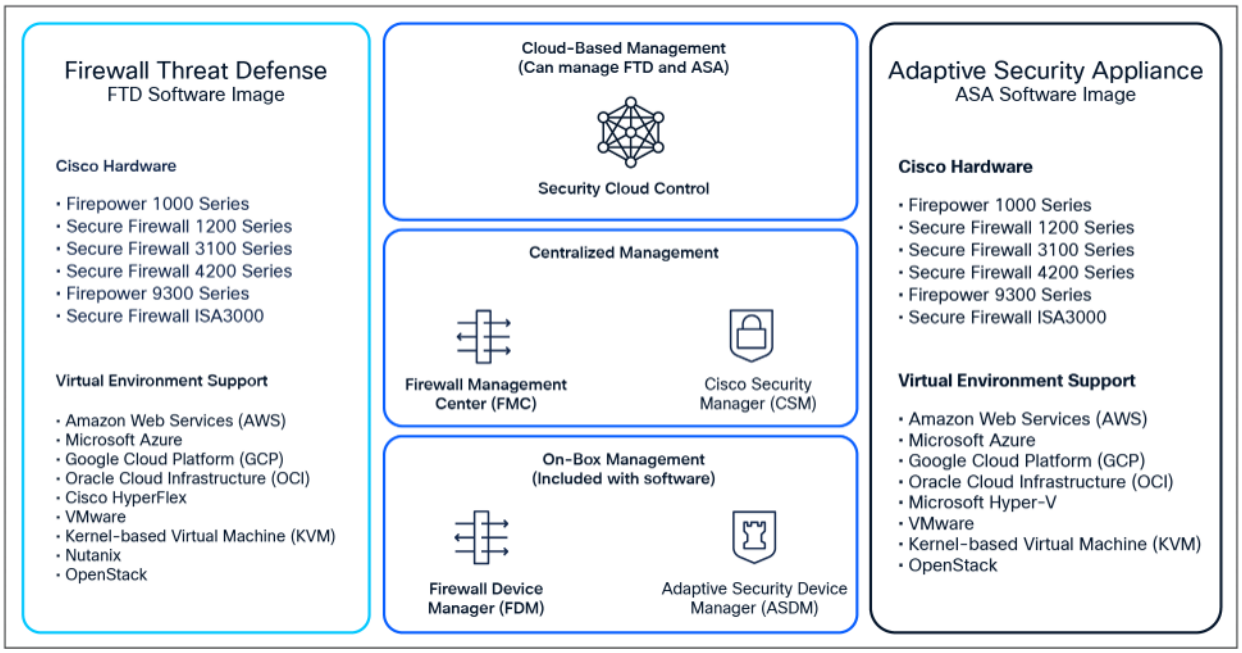



**Figure 1.**
Manager selection matrix

### Licensing

Smart Licensing is Cisco's licensing system. It enables customers to easily move licenses between similar systems in their organization, overcoming limitations associated with previous device-locked Product Authorization Key (PAK)-based licenses.

End customers must create a Smart Licensing account on Cisco's Smart Software Manager portal before ordering the Cisco Secure Firewall Threat Defense software or certain ASA appliances. Alternatively, Cisco or a partner can help create the Smart Licensing account on behalf of the end customer. The Smart Software Manager portal is available for customers to manage the efficient use of purchased smart licenses. When the order is placed, all ordered licenses are added to the customer's Smart Licensing account.

**Table 1.** Product licensing by product type

| Product | Licensing |
|---|---|
| **Cisco ASA Virtual appliances** | Cisco Smart Licensing |
| **Cisco Secure Firewall Threat Defense Virtual appliances** | Cisco Smart Licensing |
| **Cisco Secure DDOS Protection (Radware vDefensePro) on Cisco Firepower 9300 and 4100 Series appliances** | Supplied by Radware |
| **Cisco Secure Firewall Management Center** | None required |

© 2026 Cisco and/or its affiliates. All rights reserved.

| Product | Licensing |
|---|---|
| **Cisco Secure Firewall Management Center Virtual Appliance** | Cisco Smart Licensing |
| **Cisco Security Manager** | Cisco PAK Licensing |
| **Cisco Security Analytics and Logging** | Either Cisco Smart Licensing or Classic License |
| **Cisco ISE Passive Identity Connector (ISE-PIC)** | Either Cisco Smart Licensing or Classic License |

With the Cisco Smart License Manager, the customer can connect devices to the Smart Software Manager portal, so purchased licenses can be consumed as needed. These licenses can be relinquished back to the portal when a device is powered down or a user is finished using the license. With Smart Software Licensing, customers can easily check in and check out licenses to use on different platforms. Licenses are no longer locked to a specific platform.

A Smart Account can be created from Cisco Software Central. For more information on setting up a Smart Account, please refer to this Smart Licensing Deployment Guide.

**Table 2.** Additional Smart Licensing training, resources and support are available here

| Location | Description |
|---|---|
| https://www.cisco.com/site/us/en/buy/licensing/index.html | Cisco Software Licensing and Smart Accounts |
| Software Operation Exchange Page<br>Live Training Schedule<br>Orderable Smart Licensing SKU List | Additional Software training and informational resources |

#### ASA and Firewall Threat Defense License Terminology

This guide consistently uses the license terminology used in the Cisco Commerce tool. As of ASA 9.19.1 and FTD 7.3, new licensing terminology appears in the user interfaces of the management platforms. The differences are only in naming and are not different licenses per se.

**Table 3.** License terminology differences between Cisco Commerce and the user interfaces of the management platforms

| License Name Used in the Cisco Commerce tool | | License Name Seen in User Interface |
|---|---|---|
| **Base** | **Essentials** | |
| **Threat** | **IPS** | |
| **Malware** | **Malware Defense** | |
| **URL License** | | URL |

© 2026 Cisco and/or its affiliates. All rights reserved.

#### Cisco Secure DDoS Protection (Radware vDefensePro) Licensing

Licensing of the vDP and Vision will be administered directly by Radware. Once the order is shipped, Radware will send an email to the customer with their serial numbers. Please note the address of the person on the customer order who will receive the email. These serial numbers will be needed along with the MAC address for either vDP and/or Vision after installation. If the email with the serial numbers cannot be found, please open a TAC case to get them reissued. For detailed licensing instructions, please refer to Radware License Generator.

#### High Availability Pair Licensing

Cisco requires two (2) subscriptions for a High Availability (HA) pair of appliances running Firewall Threat Defense software image, which is configured for active-passive operation. The models available with this optional configuration include:

- Cisco Firepower 1000 Series
- Cisco Secure Firewall 1200 Series
- Cisco Secure Firewall 3100 Series
- Cisco Firepower 4100 Series
- Cisco Secure Firewall 4200 Series
- Cisco Firepower 9300 Series
- Cisco Secure Firewall Threat Defense Virtual appliances (except Public Cloud)
- Cisco ASA Virtual appliances (except Public Cloud)

We now offer specially configured bundle stock keeping units (SKUs) that enable the purchase of a High Availability pair of physical appliances and software subscriptions that includes 50% discounted pricing for the second software subscription in the two-appliance bundle.

The bundle consists of:

- Two (2) identically configured hardware appliances
- Two (2) identical software subscriptions

A 50% discount will be automatically applied to the second software subscription in the bundle. See the specific model section in this document for the appropriate bundle PID.

#### Renewing HA Bundle Software Subscriptions

The 50% pricing discount also applies to HA bundles at time of renewal.

#### Cisco Secure Client Licensing

Cisco Secure Client (formerly AnyConnect Plus, Apex, and VPN Only) licenses are required to use the Remote Access VPN (RA VPN) functions on all firewalls (physical and virtual) running the Secure Firewall ASA or Secure Firewall Threat Defense code base.

For information on purchasing Cisco Secure Client licenses and sharing the licenses with your Smart Account, please see the Cisco Secure Client Ordering Guide.

Instructions can also be found in the Cisco Secure Client License FAQ.

© 2026 Cisco and/or its affiliates. All rights reserved.

## Service and Support Offerings

### Software Application Support Plus Upgrades (SASU)

Cisco Secure Firewall Threat Defense software, ASA firewall, and Cisco Secure Firewall Management Center security licenses include software subscription support. SASU is essential to keeping your business-critical applications available, highly secure, and operating at optimal performance. For the term of your software subscription licenses, you will receive timely, uninterrupted access to the latest software updates and major upgrade releases, which may contain significant architectural changes and new features and functions. With software subscription support, you will have the latest software working to protect your business. You will also have access to a wide range of online tools and communities that can help you solve problems quickly, maintain business continuity, improve your competitiveness, and make the most of limited resources through increased productivity.

This support entitles customers to the services listed here for the full term of the purchased software subscription:

- Software updates and major upgrades, to keep applications performing optimally with the most current feature set.
- Access to the Cisco Technical Assistance Center (TAC), which provides fast, specialized support.
- Online tool building, to expand in-house expertise and boost business agility.
- Collaborative learning, to provide additional knowledge and training opportunities.

No additional products or fees are required to receive these services with a software subscription.

Cisco SASU includes:

- Registered access to Cisco.com.
- 24-hour access to the Cisco TAC and Cisco software specialists.
- Maintenance and minor software release updates.
- Major software upgrade releases.

Please refer to the following link for more detailed information regarding Cisco SASU: https://www.cisco.com/en/US/services/ps2827/ps2993/services_at_a_glance_sas_sasu.pdf.

### Cisco Smart Net Total Care Service

Customers require a Cisco Smart Net Total Care support contract with each appliance to download application signature updates. The Smart Net Total Care Service gives customers access to an abundance of Cisco support tools and expertise, providing them with greater network availability and performance while reducing operating costs. Technical service is required to be attached at the point of the product sale so that customers get the necessary support and entitlement and the best possible return on investment. When ordering Threat Defense software on select ASA hardware, the Management Center, the appropriate Smart Net Total Care service items are automatically added to your quote.

© 2026 Cisco and/or its affiliates. All rights reserved.

The Cisco Smart Net Total Care Service provides:

- Global 24-hour access to the Cisco TAC.
- Access to the online knowledge base, communities, and tools.
- Current hardware replacement option: next business day, where available.
- Operating system software updates.
- Smart, proactive diagnostics and real-time alerts on devices enabled with Cisco Smart Call Home.

Please refer to the following link for more detailed information regarding Cisco Smart Net Total Care Service: https://www.cisco.com/c/en/us/support/services/smart-net-total-care/index.html.

**Cisco Advanced Services**

The Cisco Global Security Solutions team provides comprehensive assessment, design, deployment, and migration assistance through the Cisco Advanced Services Transaction (AS-T) model, which involves the use of a Statement of Work (SOW). These Cisco AS-T offers are custom scoped and priced, and partners need to engage a Cisco Services account manager to purchase them.

Cisco Security Plan and Build Services help customers develop and deploy a comprehensive security strategy they can rely on to deliver the industry's most comprehensive advanced threat protection solution. This service incorporates a best practice review, deployment, and tune-up to help ensure that the system is alerting properly.

Cisco Security Migration Services help customers move from existing Cisco Source fire or competitive environments. Cisco performs an analysis of the current environment, develops a migration plan, tests the plan in a lab, and performs the migration in the production environment.

To order the customized Cisco Security Plan and Build Services and Migration Services, use the Cisco AS-T part numbers in the table below.

**Table 4.** Cisco AS-T ordering information

| Part numbers | Description | Price (US$) |
|---|---|---|
| **AS-SEC-CNSLT (-A, -L)** | Cisco Security Plan and Build Services | Custom priced |
| **AS-SEC-CNSLT (-A, -L)** | Cisco Security Migration Services | Custom priced |

**Cisco Technical Services**

Cisco Technical Services for Cisco products can be quoted and ordered in Cisco tools, including the Cisco Service Contract Center (SCC) and Cisco Commerce (CCW). Tool use varies depending on the service offer and partner type and whether the service is attached at the time of product purchase.

© 2026 Cisco and/or its affiliates. All rights reserved.

#### Partner Supported Services (PSS)

Customers who choose to purchase Partner Supported Services (PSS) from an authorized Cisco partner are also entitled to download application signature updates. For more details, visit https://www.cisco.com/go/partnerservices and the Partner Support Service Global Ordering Guide for Cisco 1-Tier Partners.

#### Cisco Talos Incident Response

Cisco Talos Incident Response (CTIR) provides a full suite of proactive and emergency services to help you prepare, respond and recover from a cyber security breach. CTIR enables 24-hour emergency response capabilities and direct access to Cisco Talos, the world's largest threat intelligence and research group.

You can order and transact CTIR while ordering specific Cisco Firepower 4K and 9K Series master bundles. This will provide you with yet another option to create a stronger security posture and stay protected in case of a security breach. The CTIR PID will be auto attached based on product order size. **The auto-attached SKU can be removed and is not mandatory.**

**Table 5.** CTIR option available in Cisco Firepower master bundles

| CTIR PID (Orderable PID) | CTIR SKU (Do not order without CTIR PID) | Description |
|---|---|---|
| **CTIR-NGFW-S=** | CON-CTIR-NGFW | Cisco Talos Incident Response Retainer-Small, Attach with NGFW |

To learn more on CTIR, follow this link: https://www.cisco.com/site/us/en/products/security/talos/incident-response-services/index.html.

## SKUs and ordering guidance for Cisco Secure Firewall Appliances

## Introduction

**Scope:** This section describes the pricing and ordering for the following products:

- Cisco Secure Firewall 200 Series
- Cisco Firepower 1000 Series
- Cisco Secure Firewall 1200 Series
- Cisco Secure Firewall 3100 Series
- Cisco Firepower 4100 Series
- Cisco Secure Firewall 4200 series
- Cisco Secure Firewall 6100 series
- Cisco Firepower 9300 Series

#### About the Cisco Secure Firewall Appliances

Cisco firewall appliances, when deployed as Layer 2-7 firewall sensors, use the Cisco Secure Firewall Threat Defense software image. The Cisco Secure Firewall Management Center provides unified management for both Next Generation Firewall and dedicated IPS. The on-device Firewall Device Manager is also available with Secure Firewall Threat Defense software. Alternatively, the Cisco Secure Firewall with Adaptive Security Appliance (ASA) software image is also supported on the Cisco Firepower and Secure

© 2026 Cisco and/or its affiliates. All rights reserved.

Firewall platforms. When running the ASA software image, the ADSM on-device manager is available. Cisco Firepower 4100 and 9300 series appliances are also available with Cisco Secure DDoS Protection. Alternatively, all Secure Firewalls are available with cloud-based Cisco Secure DDoS Protection.

**Cisco Secure Firewall 200 Series Appliances**

The Cisco® Secure Firewall 200 Series offers next-generation firewall capabilities specifically designed for distributed enterprises and small branch locations. It provides robust, cost-effective security and simplified management within a compact form factor, ensuring secure and optimized connectivity at the network edge. The 200 Series extends Cisco's Hybrid Mesh Firewall architecture to branch edges, providing AI-powered inspection and consistent security policies.

**Chassis Overview: Cisco Secure Firewall 220: Compact Model**

| | |
|---|---|
| **Front**<br>• Logo and label |  |
| **I/O**<br>4x 1000BASE-T ports<br>1x1G SFP port<br>USB Type-C and RJ-45 (Cisco serial)<br>1x USB 3 Type A port<br>1x 1000BASE-T Management port<br>Power input (uses external/brick AC power adapter) |  |

**Chassis Overview: Cisco Secure Firewall 240P: Compact Model**

| | |
|---|---|
| **Front**<br>• Logo and label |  |
| **I/O**<br>8x 1000BASE-T ports<br>2x1G SFP port<br>USB Type-C and RJ-45 (Cisco serial)<br>1x USB 3 Type A port<br>1x 1000BASE-T Management port<br>Power input (uses external/brick AC power adapter) |  |

**Cisco Firepower 1000 Series Appliances**

The Cisco Firepower 1000 Series is a family of threat-focused security appliances for branch, Distributed Enterprise and Internet Edge deployments. The 1000 Series hardware delivers superior threat defense, with greater throughput than earlier models such as the ASA-5506-X, ASA-5508-X and ASA-5516-X. The 1000 Series is available with ASA and FTD software images.

© 2026 Cisco and/or its affiliates. All rights reserved.

**Chassis Overview: Cisco Firepower 1010**

| | |
|---|---|
| **Front**<br>• Logo and label |  |
| **I/O**<br>8x 1000BASE-T ports<br>Console (Cisco RJ45 serial or mini-USB)<br>1x USB 2.0<br>1x 1000BASE-T Management Port<br>Power input (uses external/brick AC power adapter) |  |

**Chassis Overview: Cisco Firepower 1120 and 1140**

| | |
|---|---|
| **Front**<br>• Logo and label |  |
| **I/O**<br>8x 1000BASE-T ports<br>4x SFP ports (1Gbps)<br>Console (Cisco RJ45 serial or mini-USB)<br>1x USB 2.0<br>1x 1000BASE-T Management Port<br>FRU SSD |  |

**Chassis Overview: Cisco Firepower 1150**

| | |
|---|---|
| **Front**<br>• Logo and label |  |
| **I/O**<br>8x 1000BASE-T ports<br>2x SFP ports (1 Gbps)<br>2x SFP+ ports (10 Gbps)<br>Console (Cisco RJ45 serial or mini-USB)<br>1x USB 2.0<br>1x 1000BASE-T Management Port<br>FRU SSD |  |

**Cisco Secure Firewall 1200 Series Appliances**

The Cisco Secure Firewall 1200 Series is a family of threat-focused security appliances for the distributed enterprise. It extends high levels of inspection to branch locations to enable direct internet connectivity and SD-WAN.

© 2026 Cisco and/or its affiliates. All rights reserved.

The 1200 Series includes three compact models (1210CE, 1210CP, 1220CX) that can be installed in a variety of configurations (wall-mounted, on a desktop, rack-mounted, in a suitable cabinet). The family also includes three 1U rack-mount models (1230, 1240, 1250) for larger branches.

**Chassis Overview: Cisco Secure Firewall 1200 Series – Compact Models**

| | |
|---|---|
| **1210CE**<br>8x 1000BASE-T ports<br>Console (Cisco RJ45 serial or USB type-C)<br>1x USB 2.0<br>1x 1000BASE-T Management Port<br>Power input (uses external/brick AC power adapter) |  |
| **1210CP**<br>8x 1000BASE-T ports (PoE on 4 ports)<br>Console (Cisco RJ45 serial or USB type-C)<br>1x USB 2.0<br>1x 1000BASE-T Management Port<br>Power input (uses external/brick AC power adapter) |  |
| **1220CX**<br>8x 1000BASE-T ports (PoE on 4 ports)<br>2x SFP+ (10 Gbps)<br>Console (Cisco RJ45 serial or USB type-C)<br>1x USB 2.0<br>1x 1000BASE-T Management Port<br>Power input (uses external/brick AC power adapter) |  |

**Chassis Overview: Cisco Secure Firewall 1200 Series – Rack-mount Models**

| | |
|---|---|
| **1230 and 1240**<br>8x 1000BASE-T ports<br>4x SFP+ slots (1Gbps/10Gbps)<br>Console (Cisco RJ45 serial or USB type-C)<br>1x USB 3.0<br>1x 1000BASE-T Management Port<br>FRU SSD |  |
| **1250**<br>8x 2.5GBASE-T ports (PoE on 4 ports)<br>4x SFP+ slots (1Gbps/10Gbps)<br>Console (Cisco RJ45 serial or USB type-C)<br>1x USB 2.0 |  |

© 2026 Cisco and/or its affiliates. All rights reserved.

| | |
|---|---|
| 1x 1000BASE-T Management Port<br>FRU SSD | |

**Cisco Secure Firewall 3100 Series Appliances**

The Cisco Secure Firewall 3100 Series is a family of threat-focused security appliances. The 3100 Series addresses emerging hybrid mid-market and high-end use cases from the Internet edge to the data center, providing superior performance at a highly competitive price point.

**Chassis Overview: Cisco Secure Firewall 3100 Series**

| | |
|---|---|
| **Front**<br>8x 1000BASE-T ports<br>8x SFP+ 10Gbps ports (3105, 3110, 3120), or<br>8x SFP28 25Gbps ports (3130, 3140)<br>2x SSD bay (field-replaceable, 1 SSD included)<br>1x NetMod bay for FPR3K-XNM Gen2 modules<br>1x Management Ethernet port (SFP+ 10Gbps)<br>Console (Cisco RJ45 serial)<br>USB 2.0 |  |
| **Rear**<br>2x power supply bays (1 included)<br>2x fan module bays (2 included) |  |

**Cisco Firepower 4100 Series Appliances**

The Cisco Firepower 4100 Series comprises four threat-focused security appliances. The 4100 Series addresses use cases from the Internet edge to the data center. The 4100 Series hardware delivers superior threat defense, at faster speeds, with a smaller footprint. Also, the Cisco Firepower 4100 Series enables an upgrade path, on the customer's timeline, to the Cisco Secure Firewall Threat Defense software, even if the customer chooses the ASA image in the immediate term.

**Chassis Overview: Cisco Firepower 4100 Series**

| | |
|---|---|
| **Front view**<br>1. 8 SFP+ ports (require SFP optics module selection)<br>• 2 Network Module bays<br>• Optional Network Modules with optional optics modules<br>2. SSD bays (one occupied by default, second bay for future expansion) |  |
| **Rear view**<br>1. 2 power supply module bays<br>• 4112, and 4115: single AC default, dual AC or DC optional<br>• 4125 and 4145: dual AC default, DC optional |  |

© 2026 Cisco and/or its affiliates. All rights reserved.

| | |
|---|---|
| 2. 6 hot-swappable fans (default configuration, no options) | |

**Cisco Secure Firewall 4200 Series Appliances**

The Cisco Secure Firewall 4200 Series is a high-end firewall designed to meet the security requirements of large enterprises, datacenters, and service providers. It is available in three different performance models, offering superior threat defense within a compact 1 RU form factor. Key features and benefits of the appliance include:

- Cryptographic acceleration architecture preserves performance with SSL and VPN decryption.
- Save space and energy with 1RU form factor.
- Future-proof your investment with 16x node cluster.
- Flexibility of 2x interface module bays for additional interface support.
- Customize and future proof investment up to 400G interfaces.
- 2x SSD for event storage and malware analysis.
- Uptime/resilience with dual management interfaces.
- Fail-to-wire network modules, further enhancing its reliability and fault tolerance.

These platforms can be deployed in both firewall and dedicated IPS modes, providing versatile deployment options. For inline sets and passive interfaces, the 4200 Series supports Q-in-Q (stacked VLAN) with the ability to handle up to two 802.1Q headers in a packet.

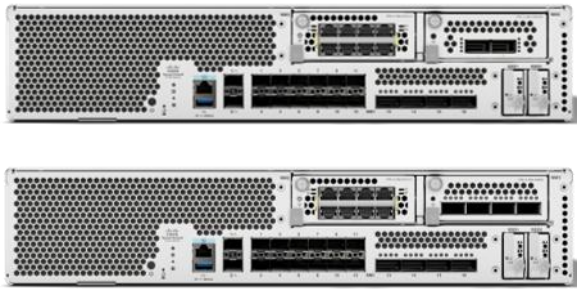
**Chassis Overview: Cisco Secure Firewall 4200 Series**

| | |
|---|---|
| **Front view**<br>1. 8 SFP28 ports (require transceiver selection)<br>2. Qty 2 Network Module bays<br>• Optional Network Modules<br>3. Qty 2 SSD bays (Both occupied by default) |  |
| **Rear view**<br>1. 2 power supply module bays<br>• 4215: single AC default, dual AC optional<br>• 4225 and 4245: dual AC default<br>2. 3 hot-swappable fan trays (default configuration, no options) |  |

**Cisco Secure Firewall 6100 Series Appliances**

The Cisco Secure Firewall 6100 Series is an AI-ready, ultra-high-end firewall engineered to deliver exceptional throughput and threat inspection in a 2-rack-unit (RU) form factor. Optimized for high-performing data center and telecommunications mobility infrastructure, its multi-core architecture and dedicated cryptographic modules provide industry-leading performance for both next-generation firewalling and encrypted traffic inspection. The 6100 Series supports both Firewall Threat Defense (FTD) and Adaptive Security Appliance (ASA) software, offering a versatile and powerful security solution.

© 2026 Cisco and/or its affiliates. All rights reserved.

| | |
|---|---|
| **Front view**<br>Fixed Ports: 12x 1/10/25/50 SFP56 Ethernet Ports + 4x 40/100/200 QSFP56 Ports<br>Network Modules: 2x Network Module bays supporting a wide range of interfaces from 1G copper up to 400G QSFP-DD, including fail-to-wire (FTW) options<br>Storage: 2x SSD bays (2 included, 3.6 TB each for 6160, 7.2 TB each for 6170)<br>Management: 2x 1/10/25/50 Gigabit Ethernet ports (SFP56)<br>Console: 1x RJ-45 console port<br>USB: 1x USB 3.0 port |  |
| **Rear view**<br>Power Supplies: 2x power supply bays (2 included, hot-swappable, 1+1 redundant AC or DC options)<br>Cooling: 4x field-replaceable fan modules (4 included) |  |

**Cisco Firepower 9300 Series Appliances**

The Cisco Firepower 9300 is a modular, scalable, carrier-grade appliance, available in Network Equipment Building System (NEBS) configurations, designed for service providers, data centers, campuses, supercomputing centers, high-frequency trading environments, and other environments requiring both low latency and the greatest throughput. In the service provider context, it is specifically designed for carriers, content providers, and cloud service providers to protect the Cisco Evolved Programmable Network, Cisco Evolved Services platform, and Cisco Application Centric Infrastructure architectures. (For more information, please see Cisco service provider security solutions.)

Tightly integrating threat-centric security services from Cisco and its partners, the 9300 appliance lowers integration costs and supports the full realization of highly secure, open, and programmable networks. In addition to providing class-leading security services, it offers low (less than 5-microsecond) latency, throughput for single flows exceeding 30 Gbps, and class-leading performance and port density on a per-rack-unit basis.

© 2026 Cisco and/or its affiliates. All rights reserved.

### Chassis Overview: Cisco Firepower 9300

Supervisor module (included with the 9300 chassis): provides overall chassis management and network interaction

- Network interface allocation and security module connectivity (960-Gbps internal fabric)

2 x Network Module bays

- 10, 40, and 100 Gigabit Ethernet network connectivity options



Security Modules: modular computing capability expands as your needs grow. Pictured are the three bays for Security Modules. A minimum of one must be ordered for standard operation.

With three SM-56 Security Modules, Cisco Firepower 9300 features up to:

- 190 Gbps of aggregate performance for NGFW inspection with FTD software use case; up to 0.87 Tbps aggregate performance when 16 service modules are clustered
- 235 Gbps of aggregate performance for stateful inspection with ASA software use case; up to 1 Tbps aggregate performance when 16 service modules are clustered

Also available: NEBS-compliant modules.

Pictured at right is the rear view of the Cisco Firepower 9300. Note that it is available with dual AC, DC, or HVDC power supplies. Also, the fan assemblies and power supplies are user replaceable.

Reminder: The Cisco Firepower 9300 is available with 10, 40, and 100 Gigabit Ethernet Network Modules.





### Special Guidelines for Quoting the Cisco Firepower 9300

Cisco Firepower 9300 ordering is highly customizable, and options are offered separately. You'll nevertheless find the ordering process straightforward.

The following table shows the four core components of a Cisco Firepower 9300 order.

**Table 6.** Components of a Cisco Firepower 9300 order

| Common hardware | Optional modules | Software licenses | Services and subscriptions |
|---|---|---|---|
| **Base Cisco Firepower 9300 Security Appliances include:**<br>• Chassis (1)<br>• Supervisor (1)<br>• Fans (4) | Choice of Security Modules—up to three bays per chassis:<br>• SM-40, 48, 56<br>Choice of network modules — two bays per chassis:<br>• 1/10/40/100Gbps options | Smart Licenses<br>ASA:<br>• ASA Standard<br>• Carrier<br>• Strong Encryption<br>• Security Contexts<br>Cisco Secure Firewall Threat Defense: | Smart Net Total Care Service<br>Cisco Secure Firewall Threat Defense Subscriptions<br>(1, 3, or 5 year terms)<br>• Threat (includes Security Intelligence, IPS) |

© 2026 Cisco and/or its affiliates. All rights reserved.

| Common hardware | Optional modules | Software licenses | Services and subscriptions |
|---|---|---|---|
| • Power supplies (2 – AC, DC or HVDC) | | • Threat Base (includes Application Visibility and Control – AVC)<br>• Threat license and subscription terms (see next column)<br>Third-party software:<br>• Cisco Secure DDOS Protection (Radware Virtual DefensePro) | • Malware defense<br>• URL |

**Common hardware** is bundled. However, your customer may wish to order extra fans and power supplies with the initial order, as these are hot-swappable, user-replaceable items. Please note that every order will require at least one, and up to three, **Security Modules. Network Modules** are also ordered separately.

Regarding **software licenses**, keep in mind that the Cisco Firepower 9300 runs either the ASA software image or the Cisco Secure Firewall Threat Defense image. Also, please note that the Encryption license is export controlled. It is available for most markets, to customers in countries where U.S. export control permits the export of strong cryptography. For more information, visit export compliance details.

In the **third-party software** category, Cisco Secure DDOS Protection (Radware Virtual DefensePro DDoS-mitigation capability) has been tightly integrated into the Cisco Firepower 9300 and 4100 Series with ASA software, is orderable from and supported directly by Cisco.

#### ASA Licensing for Cisco Firepower Appliances

The 9300 appliance, 6100 Series, 4200 Series, 4100 Series, 3100 Series, 1200 Series, 1000 Series and 200 Series are available with either the Cisco Secure Firewall Threat Defense (FTD) image or the Cisco Adaptive Security Appliance (ASA) image. Cisco Firepower appliances with ASA are available through Smart Licenses. They include a Base license and up to three optional licenses (Encryption, Security Contexts, and Carrier).

#### Base License (Free)

**L-F9K-ASA(=)** (for the Cisco Firepower 9300), **L-FPR4100-ASA(=)** (for the Cisco Firepower 4100 Series models), **L-FPR3100-ASA(=)** (for the Cisco Secure Firewall 3100 Series models), or **L-FPR1000-ASA(=)** (for the Cisco Firepower 1000 Series models) , **FPR42xx-BSE** (for the Cisco Secure Firewall 4200 Series models), **CSF2xx-BSE / L-CSF2xx-BSE=** (for the Cisco Secure Firewall 200 Series models) and **CSF61xx-BSE / L-CSF61xx-BSE=** (for the Cisco Secure Firewall 6100 Series models): Licensing on the ASA is simplified for the Cisco Firepower appliances. More than 50 ASA feature licenses are condensed into a single license. This license also includes the following security contexts by default: 10 security contexts for Firepower 9300, 10 security contexts for Firepower 4100 Series, 10 security contexts for Secure Firewall 4200, 2 security contexts for Secure Firewall 3100 Series, 2 security contexts for Firepower 1000 Series and 2 security contexts for Secure Firewall 6100.

© 2026 Cisco and/or its affiliates. All rights reserved.

#### Encryption License (Free)

**L-F9K-ASA-ENCR-K9(=)** (for the Cisco Firepower 9300), **L-FPR4K-ENC-K9(=)** (for Cisco Firepower 4100 Series models), **L-FPR3K-ENC-K9(=)** (for Cisco Secure Firewall 3100 Series models) or **L-FPR1K-ENC-K9(=)** (for Cisco Firepower 1000 Series models) , **FPR4200-ENC-K9/ L-FPR4200-ENC-K9=** (for Cisco Secure Firewall 4200 Series models), **CSF6100-ENC-K9/ L-CSF6100-ENC-K9=** (for Cisco Secure Firewall 6100 Series models) and **CSF200-ENC-K9/ L-CSF200-ENC-K9=** (for Cisco Secure Firewall 200 Series models): This license provides for strong encryption (K9) on the platform. The U.S. export of strong cryptography is not available to export-restricted regions. Cisco solutions and products with strong encryption may not be delivered to individuals or entities on the U.S. government's list of denied or restricted parties.

Please review the U.S. Bureau of Industry and Security's list of parties of concern at: https://www.bis.doc.gov/index.php/policy-guidance/lists-of-parties-of-concern.

#### Additional Security Contexts (Paid)

**L-F9K-ASA-SC-10(=)** (for the Cisco Firepower 9300), **L-FPR4K-ASASC-10(=)** (for the Cisco Firepower 4100 Series models), **L-FPR3K-ASASC-10(=)** (for the Cisco Secure Firewall 3100 Series models), **FPR4200-ASASC-10/ L-FPR4200-ASASC10=** (for the Cisco Secure Firewall 4200 Series models**), CSF6100-ASASC-10/ L-CSF6100-ASASC10=** (for the Cisco Secure Firewall 6100 Series models): This license adds 10 security contexts to an ASA instance on the 9300 appliance, 4100 appliance, 4200 appliance, 3100 appliance respectively.

#### Carrier License Option (Paid)

**L-F9K-ASA-CAR(=)** (for the Cisco Firepower 9300) or **L-FP4K-ASA-CAR=** (for Cisco Firepower 4100 Series models), **FPR42K-ASA-CAR/L-FPR42-ASA-CAR=** (for Cisco Secure Firewall 4200 Series models), or **L-FPR3K-ASA-CAR=** (for Cisco Secure Firewall 3100 Series models), **CSF6100-ASA-CAR/ L-CSF6100-ASA-CAR=** (for Cisco Secure Firewall 6100 Series models: This license covers carrier feature enablement that allows for inspection of Diameter, GTP/GPRS and SCTP protocols

#### Cisco Secure Firewall Threat Defense Licensing for Cisco Firepower Appliances

Figure 2 provided for general reference only, shows the typical order flow. Start with the primary bundle part numbers and the software image (ASA or Firewall Threat Defense), and then, in the case of the example, associated Cisco Secure Firewall Threat Defense–related licenses and subscriptions for functionality like Security Intelligence and IPS (“T”), Advanced Malware Protection (“M”), and URL Filtering (“C”). This example concludes with ordering the associated virtualized Cisco Secure Firewall Management Center. Note that Cisco Secure Firewall Threat Defense ships standard with the option to activate a 3-month trial license without activation of a Smart License account.

© 2026 Cisco and/or its affiliates. All rights reserved.

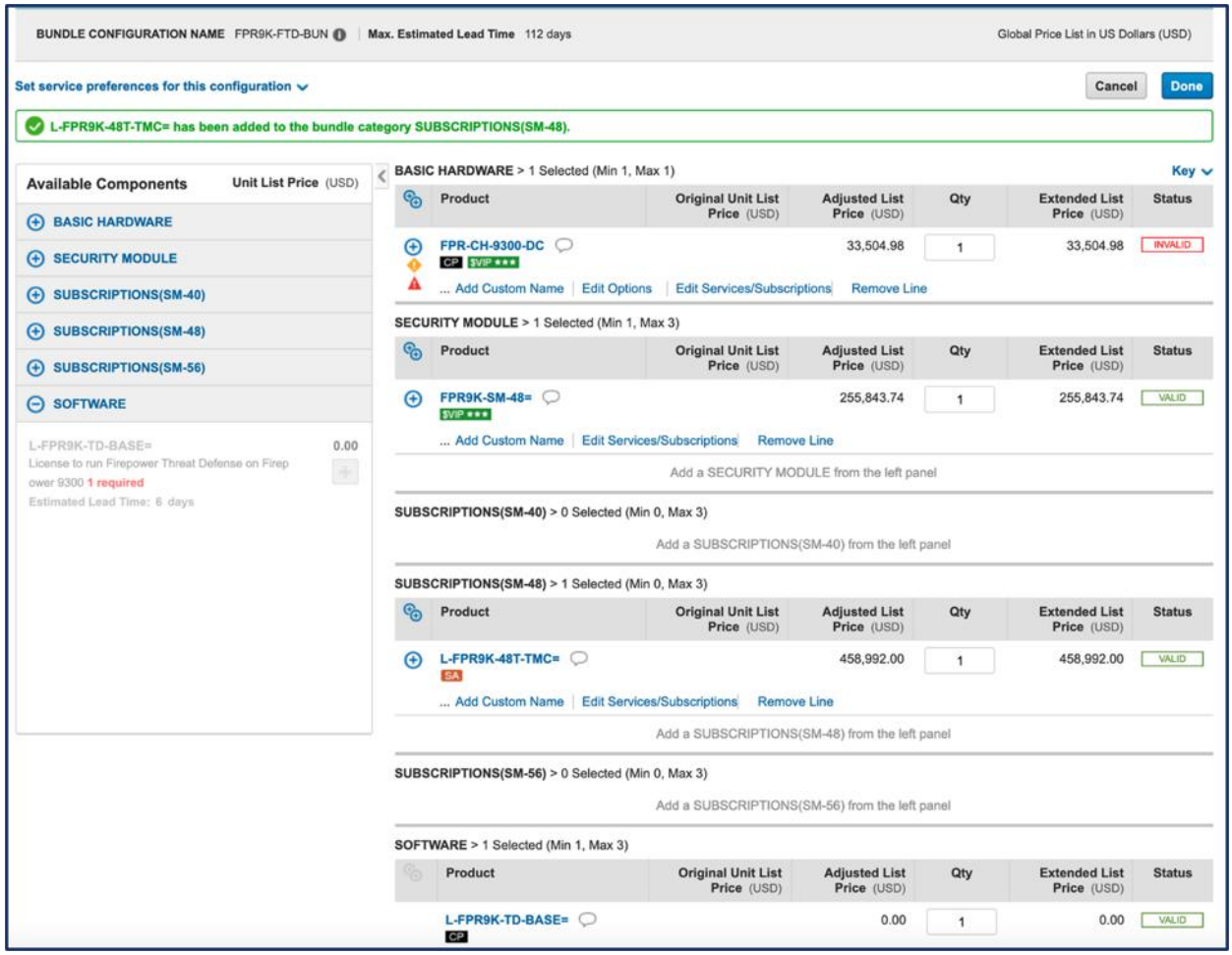



**Figure 2.**
Typical order flow

**Ordering Steps for Cisco Firepower 9300, FTD-Based Cisco Firepower 9300**

Start with one of the following FTD Bundle SKUs in CCW, example shown above is FPR9K-FTD-BUN.

Select Hardware Options and Quantity.

Chassis Type – AC, DC, or HVDC.

Chassis Options including Netmod, Sup, SFPs, power cables.

Security Module Quantity – up to 3 per chassis.

Select Subscriptions – T=, URL=, AMP=,TC=, TM=, TMC=.

Select Term – 1, 3 or 5 years.

Select Base Software License for each security module.

You can add additional features to the system. For example, starting with FTD release 7.3, you can add Carrier License to Firepower 3100 (**FPR3K-FTD-CAR**), Firepower 4100 (**FPR4K-FTD-CAR**), Firepower 9300 (**FPR9K-FTD-CAR**) and FTD virtual (**FTDV-CAR**) configurations. This license covers inspection of Diameter, GTP/GPRS and SCTP protocols.

© 2026 Cisco and/or its affiliates. All rights reserved.

Save and exit bundle configuration and select quantity of each bundle configured. Each bundle corresponds to a single-chassis configuration. After saving the configuration, you can change quantity for more than one chassis with the same configuration

#### Cisco ISE Passive Identity Connector (ISE-PIC)

Due to End-of-Life for the Cisco Firepower User Agent, FTD requires the use of either Cisco Identity Services Engine (ISE) or Cisco ISE Passive Identity Connector (ISE-PIC) to control policy based on Active Directory user. This section describes the procedure for ordering Cisco ISE Passive Identity Connector (ISE-PIC). For information on how to order of Cisco Identity Services Engine (ISE) please see the Cisco ISE Licensing Guide.

The Cisco Identity Services Engine (ISE) Passive Identity Connector centralizes, consolidates, and distributes identity information, including IP addresses, MAC addresses, and usernames. It centralizes the authentication information, becoming the single source of truth for its subscribers. Using the Cisco Platform Exchange Grid (pxGrid), the Cisco ISE Passive Identity Connector can support up to 20 subscribers. Further details on the capabilities of the Cisco ISE Passive Identity Connector (ISE-PIC) can be found on the Cisco ISE Passive Identity Connector Data Sheet.

**Table 7.** Cisco ISE-PIC ordering information

| SKU | Description | Services and subscriptions |
|---|---|---|
| **R-ISE-PIC-VM-K9=** | ISE Passive Identity Connector 3,000 session Virtual Machine | CON-ECMU-RISEPIVM |
| **L-ISE-PIC-UPG=** | ISE Passive Identity Connector – Upgrade to maximum 300,000 sessions | CON-ECMU-LISEPUPG |

**Note:** You may be entitled to ISE-PIC at no cost if you have a qualifying FMC and valid support contract. For more information see End-of-Life and End-of-Support for the Cisco Firepower User Agent.

#### Cisco Security Analytics and Logging

This section describes the procedure to enable extended logging and analytics by ordering Cisco Security Analytics and Logging as part of your firewall purchase. The detail ordering process is described here.

The Security Analytics and Logging offer has two distinct delivery mechanisms:

- **Security Analytics and Logging (SaaS):** A cloud-delivered, Software-as-a-Service (SaaS) offering with a Cloud Data Store.
- **Security Analytics and Logging (On prem):** An on-premises appliance-based software application with an On-premises Data Store.

Discounted Bundling When Attaching Firewall Subscriptions via CCW

a Begin by navigating to the firewall model to be ordered (FPR1150-NGFW-K9, for example).

b Make your software choice under the “Subscriptions” category at the top (wherever present) and navigate to the “Extended Logging and Analytics” category below.

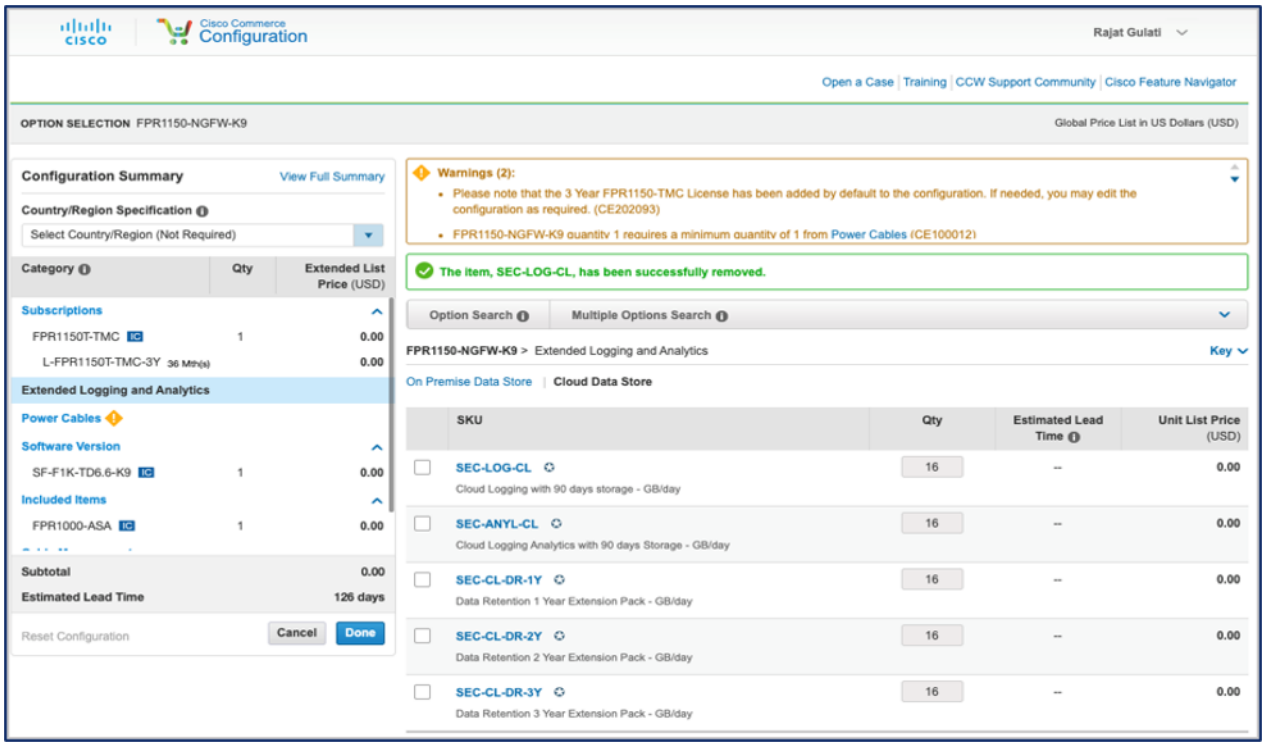
c You are presented with two options to the right: “On-Premises Data Store” or “Cloud Data Store.” Only one option can be selected per firewall being ordered, with either the same or different subscription term as the firewall subscription.

© 2026 Cisco and/or its affiliates. All rights reserved.

d The “Cloud Data Store” option allows selection of either the Logging License, **SEC-LOG-CL**, or the “Logging Analytics License,” **SEC-ANYL-CL**. Only one option needs to be chosen, as the Logging License is nested under Logging Analytics. Both Cloud licenses include access to a Cisco Security Cloud Control tenant for log viewing only, which can be requisitioned using the link here: https://www.ciscofeedback.vovici.com/se/6A5348A75C69D114.

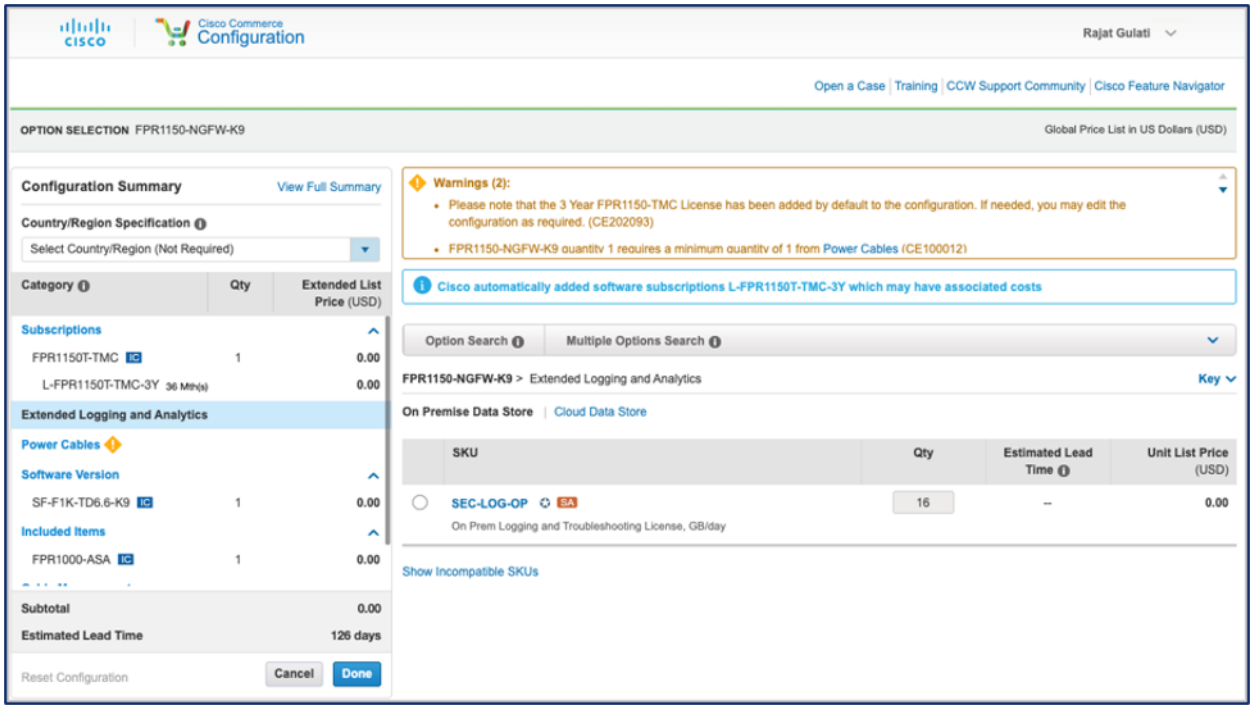
e Choosing either of the two data store options will attach a default logging volume in GB/day for that firewall model, based on expected daily volume per the Logging Volume Estimator Tool. Logging rate comes with a default retention of 90 days rolling storage for Cloud Logging.

f The last three optional licenses are Data Retention extensions, which extend log retention to 1, 2, or 3 years in the cloud.




© 2026 Cisco and/or its affiliates. All rights reserved.

g If SAL (Op) is desired, the “On-Premises Data Store” tab allows choosing the base Logging and Troubleshooting license, **SEC-LOG-OP**. This license supports remote query by FMC and is hosted on SNA appliance(s), as detailed in section 1.2.2.




h The process for bundling extended logging and analytics for Firewall FPR9K series devices is different, as the Security Modules (SM) configured as part of order determines the Logging quantity required. The Logging quantities needed are 190, 225 and 257 GBs/day for each SM-40, SM-48 and SM-56 respectively, and this quantity needs to be entered manually for the extended logging and analytics licenses. The system will display a warning of the logging quantities required for each Security Module, as shown below:




**Expected Retention Period**

The expected retention period for the SAL service under average deployment conditions (see note below table) is as follows:

**Table 8.** Retention Matrix

| Sustained Firewall Events per Second (eps) | Equivalent GB/day | On-premises | | | | | Cloud | | |
|---|---|---|---|---|---|---|---|---|---|
| | | Single node* 1TB Storage | Single node 2TB Storage | Single node 4TB Storage | Multinode** Virtual | Multinode HW | Single SEC | MultiSEC | Direct-to Cloud |
| **Expected Retention period in days (under average deployment conditions)** | | | | | | | | | |

© 2026 Cisco and/or its affiliates. All rights reserved.

| Sustained Firewall Events per Second (eps) | Equivalent GB/day | On-premises | | | | | Cloud | | |
|---|---|---|---|---|---|---|---|---|---|
| | | Single node* 1TB Storage | Single node 2TB Storage | Single node 4TB Storage | Multinode** Virtual | Multinode HW | Single SEC | MultiSEC | Direct-to Cloud |
| **5,000** | 562 | 50 | 100 | 200 | 300 | 600 | Up to 3 years<br>NA | Up to 3 years | Up to 3 years<br>Not recommended when individual device's logging rate exceeds 8,500 eps |
| **10,000** | 1,123 | 25 | 50 | 100 | 150 | 300 | | | |
| **20,000** | 2,246 | 12.5 | 25 | 50 | 75 | 150*** | | | |
| **50,000** | 5,616 | NA | NA | NA | 30 | 60 | | | |
| **75,000** | 8,424 | NA | NA | NA | NA | 40 | | | |
| **100,000** | 11,232 | NA | NA | NA | NA | 30 | | | |
| **200,000** | 22,464 | NA | NA | NA | NA | NA | | | |

**Note:** The on-premises log retention in days above are based on average deployment conditions, and may vary materially in different production environments.

* Single node = Repurposed SMC 2210 (HW or Virtual)

** Multi-node = SMC 2210 + FC 4210 + DS 6200 (All appliances HW or Virtual)

*** Compare FMC native logs retention ½ day @ 20,000 peak eps

**Cisco Secure DDoS Protection (formerly Radware Virtual DefensePro DDoS Mitigation Option)**

**Overview**

Cisco Secure DDoS Protection is provided by Radware Virtual DefensePro (vDP), available and supported directly from Cisco. It is available with the Cisco Firepower 9300 and select Cisco Firepower 4100 Series models running either the ASA or FTD software image. The following table details Firepower model and software image compatibility with Radware vDP.

**Table 9.** Cisco Secure DDOS Protection (Radware vDP) on Cisco Firepower running either ASA or FTD software image

| Firepower Series | ASA Compatibility | FTD Compatibility |
|---|---|---|
| **9300 Series – All Security Modules** | yes | yes |
| **4100 Series – All Models** | yes | yes |

## Performance

The performance figures in the tables below apply to all Cisco Firepower 9300 and 4100 Series model configurations running either the ASA or FTD software image.

**Table 10.** Key DDoS performance metrics for Cisco Firepower 4100 Series

© 2026 Cisco and/or its affiliates. All rights reserved.

| Parameter | Firepower 4100 Metric |
|---|---|
| **Maximum mitigation capacity/throughput** | 10 Gbps |
| **Maximum legitimate concurrent sessions** | 209,000 Connections Per Second (CPS) |
| **Maximum DDoS flood attack prevention rate** | 1,800,000 Packets Per Second (PPS) |

The performance figures in the following table are for Cisco Firepower 9300 with 1 to 3 Security Modules irrespective of Security Module type.

**Table 11.** Key DDoS performance metrics for Cisco Firepower 9300 with 1, 2, or 3 Security Modules

| Parameter | Firepower 9300 with 1 Security Module | Firepower 9300 with 2 Security Modules | Firepower 9300 with 3 Security Modules |
|---|---|---|---|
| **Maximum mitigation capacity/throughput** | 10 Gbps | 20 Gbps | 30 Gbps |
| **Maximum legitimate concurrent sessions** | 209,000 Connections Per Second (CPS) | 418,000 Connections Per Second (CPS) | 627,000 Connections Per Second (CPS) |
| **Maximum DDoS flood attack prevention rate** | 1,800,000 Packets Per Second (PPS) | 3,600,000 Packets Per Second (PPS) | 5,400,000 Packets Per Second (PPS) |

#### Capacity vs. Licensing

**Performance/Capacity/Throughput** is dependent on the number of cores assigned to the vDP virtual device:

- By default, Radware virtual DefensePro (vDP) installs using 6 cores (1 management, 5 software) across each of Cisco Firepower 9300's Security Modules and 4100 Series platforms.
- At install, the number of cores assigned to vDP can be adjusted from 2 to 10 to optimize the throughput performance of Cisco Firepower appliance depending on the customer need.
- While using the default 6 cores, the performance numbers for vDP are constant across platforms. The table below represents the relative performance level expected from ASA and FTD by removing 6 cores from the total available cores on the respective platforms (i.e. 24 cores minus 6 equals 75% of the total performance still available).

**Table 12.** Expected ASA or FTD image performance with 6 of the available cores assigned to vDP

| Cisco Firepower Model | Total vCores | Expected ASA or FTD Performance with vDP Active |
|---|---|---|
| **Firepower 9300 – SM-56** | 56 | 89.3% |
| **Firepower 9300 – SM-48** | 48 | 87.5% |
| **Firepower 9300 – SM-40** | 40 | 85.0% |
| **Firepower 4145** | 44 | 93.2% |
| **Firepower 4125** | 32 | 90.6% |
| **Firepower 4115** | 24 | 75.0% |

© 2026 Cisco and/or its affiliates. All rights reserved.

| Cisco Firepower Model | Total vCores | Expected ASA or FTD Performance with vDP Active |
|---|---|---|
| **Firepower 4112** | 24 | 75.0% |

**Licensing** is based on the amount of legitimate traffic, not the capacity of the VM to process information.

- Purchase vDP licenses based on the amount of the client's peak legitimate traffic flow.
- This approach differs from other vendors that charge based on attack volume. Radware licenses are based on **known** legitimate traffic rather than an **unknown** attack volume.

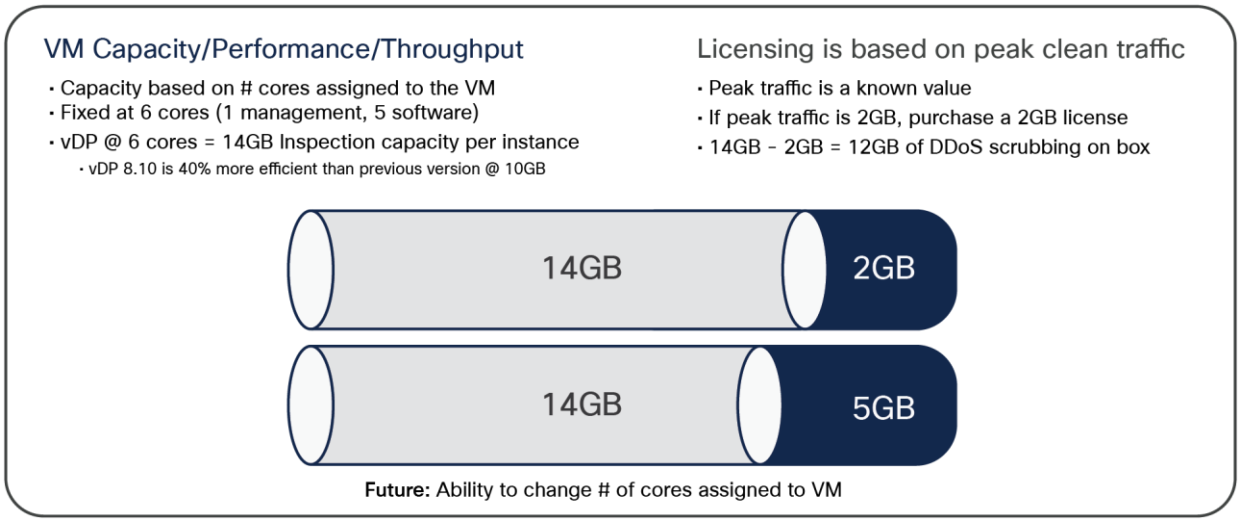



**Figure 3.**
Capacity vs. licensing

**Example 1:** Client has a 10-Gbps WAN link with a daily peak traffic flow of 2-Gbps.

- Purchase a 2-Gbps license or higher if the traffic is expected to increase in the near future.
- vDP will be able to mitigate a DDoS attack up to the capacity of the WAN link's 10-Gbps, after which a cloud scrubbing solution will have to take over at the ISP level.
  - Radware can be set up to automatically notify a cloud scrubber to take over.
  - Radware's Emergency Response Team (ERT) can assist in configuring vDP for each customer as part of the standard Cisco ECMU support contract for vDP.
  - Radware cloud availability on GPL is on the roadmap
  - **Warning: Do not over-purchase or over-quote the client's throughput needs. License is based on clean traffic only, not the capacity of the VM.**

© 2026 Cisco and/or its affiliates. All rights reserved.

**The vDP Software Licenses and Support SKUs**

The following tables outline the product information and SKUs for ordering. Cisco is only OEMing the Virtual License for Radware Manager Vision. Customers may want additional Manager Options that are provided directly by Radware.

**Table 13.** vDP spare SKUs: May be ordered separately

| SKU | Description | Service ECMU SKU |
|---|---|---|
| **L-FPR-RVDP-10G=** | Radware Virtual Defense Pro 10-Gbps license for Firepower | CON-ECMU-LFPRRVG1 |
| **L-FPR-RVDP-5G=** | Radware Virtual Defense Pro 5-Gbps license for Firepower | CON-ECMU-LFPR5RGV |
| **L-FPR-RVDP-2G=** | Radware Virtual Defense Pro 2-Gbps license for Firepower | CON-ECMU-LFPRRVG2 |
| **L-FPR-RVDP-1G=** | Radware Virtual Defense Pro 1-Gbps license for Firepower | CON-ECMU-LFPRRVGP |
| **L-FPR-RVDP-500M=** | Radware Virtual Defense Pro 500-Mbps license for Firepower | CON-ECMU-LFPR5RVD |
| **L-FPR-RVDP-200M=** | Radware Virtual Defense Pro 200-Mbps license for Firepower | CON-ECMU-LFPR0RVD |
| **L-RD-APV-VA-LIC==** | APSolute Vision - VA - Yearly Subscription | None |
| **L-RD-APV-RTU6-LIC** | APSolute Vision RTU - 6/30 - Yearly Subscription | None |

**Table 14.** Regular SKUs: Orderable with the Cisco Firepower platform

| SKU | Description | Service ECMU SKU |
|---|---|---|
| **FPR-RVDP-10G** | Radware Virtual Defense Pro 10-Gbps license for Firepower | CON-ECMU-LFPRRVG1 |
| **FPR-RVDP-5G** | Radware Virtual Defense Pro 5-Gbps license for Firepower | CON-ECMU-LFPR5RGV |
| **FPR-RVDP-2G** | Radware Virtual Defense Pro 2-Gbps license for Firepower | CON-ECMU-LFPRRVG2 |
| **FPR-RVDP-1G** | Radware Virtual Defense Pro 1-Gbps license for Firepower | CON-ECMU-LFPRRVGP |
| **FPR-RVDP-500M** | Radware Virtual Defense Pro 500-Mbps license for Firepower | CON-ECMU-LFPR5RVD |
| **FPR-RVDP-200M** | Radware Virtual Defense Pro 200-Mbps license for Firepower | CON-ECMU-LFPR0RVD |

Notes:

- Radware vDP license are based on legitimate traffic. Please refer to this deck for more details: Cisco Secure DDoS Protection
- L-RDWR-APV-VA includes both APSolute Vision with Security Reporter – 10 vDP
- The CON Service SKUs should automatically be added to the cart with a 12-month term
- Cisco will provide Level 0/1 to determine if problem is Cisco Firepower or vDP. All vDP issues will be escalated to Radware.
- Radware vDP clustering is currently only supported in the Cisco Firepower 9300 intrachassis configuration. This is clustering of multiple security modules (SM-40, SM-48, SM-56) within the same Cisco Firepower 9300 chassis.

© 2026 Cisco and/or its affiliates. All rights reserved.

- For High Availability (HA), Active-Active and Active-Standby modes are supported.
- Radware Vision Manager is a Virtual License and needs to be installed on its own server, not the Cisco Firepower platform. For version 4.6, VMware ESXi 5.1, 5.5, 6.0, 6.5, 6.7, 6.7U2 or VMware Workstation 8 or 11 are supported. Please check Cisco Secure Firewall Radware DefensePro DDoS Release Notes for details.
- Cisco Secure DDOS Protection (Radware vDP) Ordering Steps

**Ordering SPARE SKUs for existing equipment:**

Spare SKUs are provided (start with "L" and end in "=" sign) to allow you to order the vDP software license for existing equipment. These are L-FPR-RVDP-10G=. 5G=, and 2G=, respectively.

- Go to the Cisco Commerce home page.
- Create a new estimate or edit an old one.
- In the "Search by SKU" box, paste in one of the SPARE SKUs. Or click on the "Find Products and Solutions" link to the right of the "Search by SKU" box.
- Typing in "Radware" in search box will return all active Radware SPARE SKUs.




**Figure 4.**
Find products and solutions

- Once you find the SKU you need, then click the '+' sign to add it to the cart.
- Next click on the "Edit Service/Subscription" link and set the term of the service contract.




**Figure 5.**
Edit service/subscription

© 2026 Cisco and/or its affiliates. All rights reserved.

A 12-month (1y) ECME contract is selected by default, but that can be increased up to 60 months (5y).

**Note:** As of this writing, you have to visit the Edit Service/Subscription link and click done to accept the default 12-month service contract. Otherwise, the cart will produce an error.

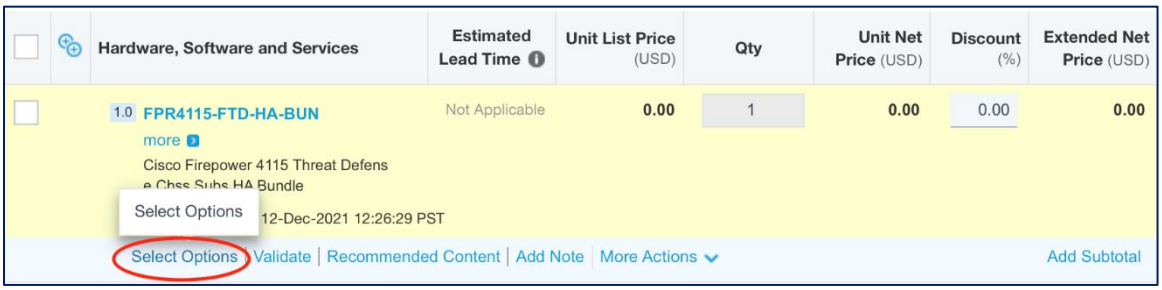
If you do not already own Radware Vision Manager, please add to your order SKU: L-RDWR-APV-VA=. This is the Radware Manager Vision and Security Reporter with support for 10 vDP instances.

#### Secure Workload Ordering Steps in Firewall Bundle

#### Ordering SPARE SKUs for existing equipment

A Workload SKU is provided to allow you to order workload within a firewall bundle, securing a multi-product discount. The SKU is C1-TAAS-XX-SW-K9 and is available for Firepower 4100 and 9300 bundles.

- Go to the Cisco Commerce home page.
- Select the firewall bundle to be ordered, for example FPR4115-FTD-HA-BUN.
- Click “Select Options” for the bundle to open the configurator.



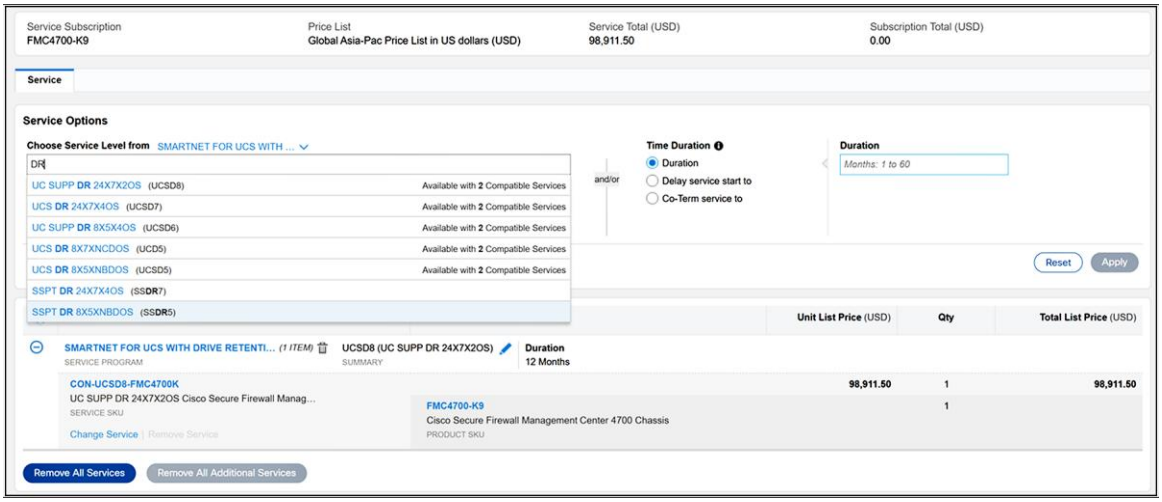

- Open the “Secure Workload” section on the left-hand side and add the license C1-TAAS-XX-SW-K9 to the bundle.
- Finalize the bundle configuration and proceed with the purchase.

#### Firewall Disk Retention Service/Subscription Ordering Steps

#### Disk Retention service allows customers to keep firewall/FMC disks during RMAs.

- Go to the Cisco Commerce home page
- Select the Firewall/FMC product to be ordered and add it to cart
- Click on “Edit Service/Subscription” link
- Search for "DR" in the "Service Options" section. It will show the list of all disk retention service PIDs available to the product
- After selecting the service option click on “Apply” to confirm the service

© 2026 Cisco and/or its affiliates. All rights reserved.




## Cisco Secure Firewall Small Business Edition License Pack

**Overview**

To meet real-world needs of small businesses, Cisco Secure Firewall Small Business Edition is tailor-made to simplify security. Secure Firewall Small Business Edition licenses are available in 2 types and can be ordered at the time of hardware purchase or as standalone license.

**Table 15.** Small Business Edition – Included Feature Set

| License Feature (Available in 3 Yr Term only) | SBE Lite | SBE Standard |
|---|---|---|
| **Threat Protection, Malware and URL Filtering** | Yes | Yes |
| **Cisco Security Cloud Control Firewall Management License** | Yes* | Yes* |
| **Cisco Secure Client - 50 Licenses (Secure Client Advantage for Mobile Devices and or Desktops)** | Yes | Yes |
| **Security Analytics and Logging (Logging and Troubleshooting)** | No | Yes |

## Platforms available

**Table 16.** Small Business Edition – Product Series Availability

| Product Series | SBE Lite | SBE Standard |
|---|---|---|
| **Firepower 1000 Series** | Yes – Only on FPR1010 | Yes – Only on FPR1010 |
| **All other platforms** | Not Available | Not Available |

*requires FWM-SEC-SUB-Cisco Security Cloud Control XaaS Subscription

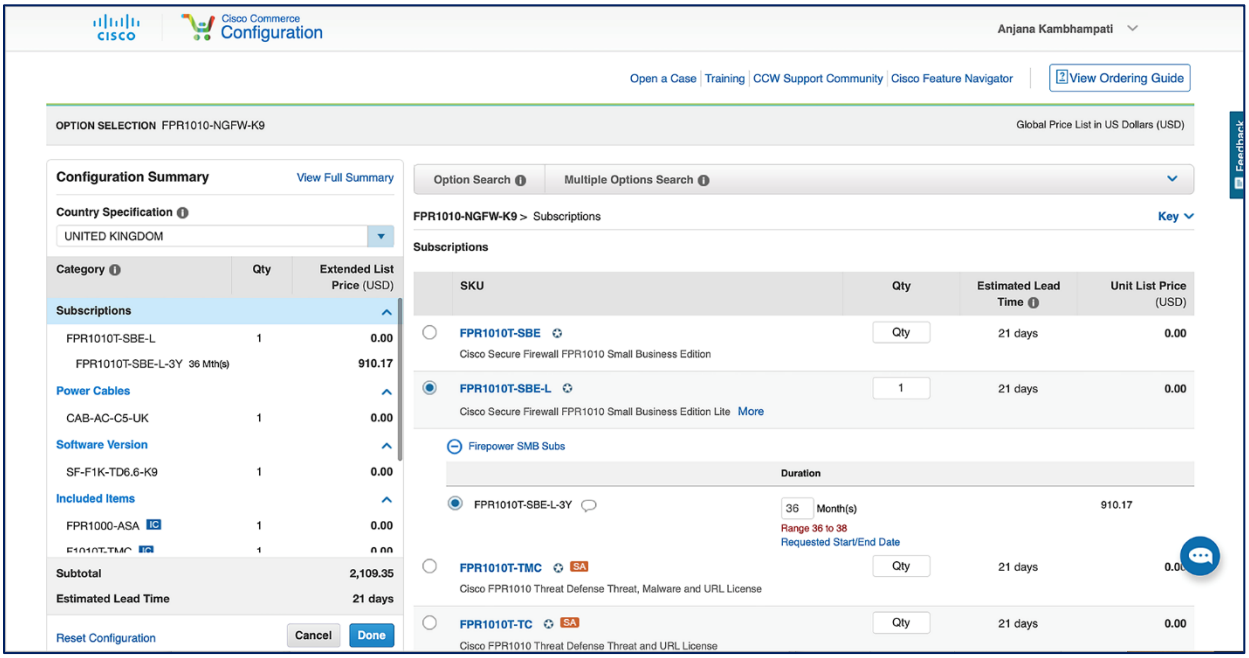
© 2026 Cisco and/or its affiliates. All rights reserved.

# SKUs and Ordering

**Table 17.** Small Business Edition – Part Numbers

| Part Number | Description |
|---|---|
| **FPR-SEC-TERM** | Cisco Secure Firewall Term Licenses - For Distributors/Drop Ship Orders |
| **FPR1010T-SBE** | Cisco Secure Firewall FPR1010 Small Business Edition |
| **FPR1010T-SBE-L** | Cisco Secure Firewall FPR1010 Small Business Edition Lite without Logging |
| **FPR1010T-SBE-3Y** | Cisco FPR1010 Small Business Edition, 3Y Subs |
| **FPR1010T-SBE-L-3Y** | Cisco FPR1010 Small Business Edition Lite, 3Y Subs |

**Ordering Steps for Cisco Secure Small Business Edition**




Start with one of the Firepower 1010 SKUs, for example - FPR1010-NGFW-K9.

Select “Edit Options”.

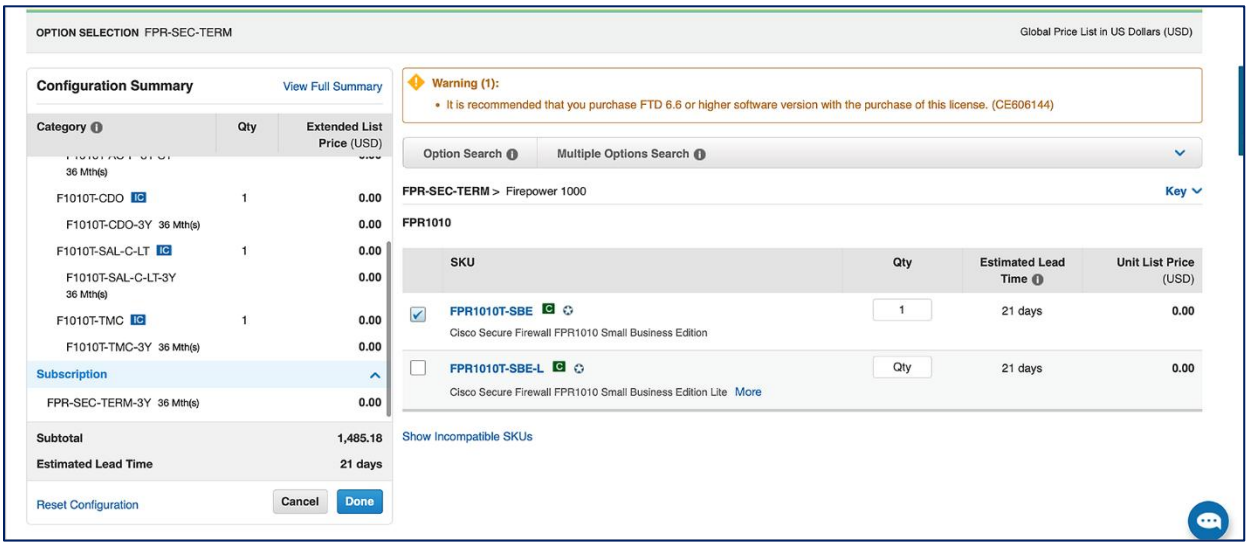
Select Subscription for Small Business Edition or Small Business Edition Lite: FPR1010T-SBE or FPR1010T-SBE-L.

Select Country.

Save and exit configuration.

© 2026 Cisco and/or its affiliates. All rights reserved.

**Ordering Steps for Cisco Secure Small Business Edition for Distributors**




Start with the following SKU in CCW FPR-SEC-TERM.

Select Subscription for Small Business Edition or Small Business Edition Lite: **FPR1010T-SBE** or **FPR1010T-SBE-L.**

Save and exit configuration.

## Ordering vDP with the Cisco Secure Firewall Platform

The non-spare versions of the SKUs are available options when ordering the 9300 or 4100 Cisco Firepower platform.

- Go to Cisco Commerce: https://apps.cisco.com/Commerce/home.
- Create a new estimate or edit an old one.
- Add Cisco Firepower 9300 or 4100 as desired (example is of a 4125) and configure appropriately.

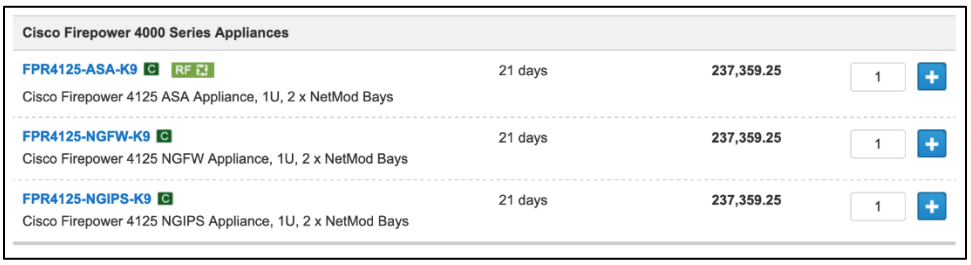



**Figure 6.**
Configuration options for Cisco Firepower 4125 platform

© 2026 Cisco and/or its affiliates. All rights reserved.

The Radware vDP SKUs are available under “Feature Licenses.” When configuring a Firepower 9300, you will need 1 license of equal size for **each** blade.

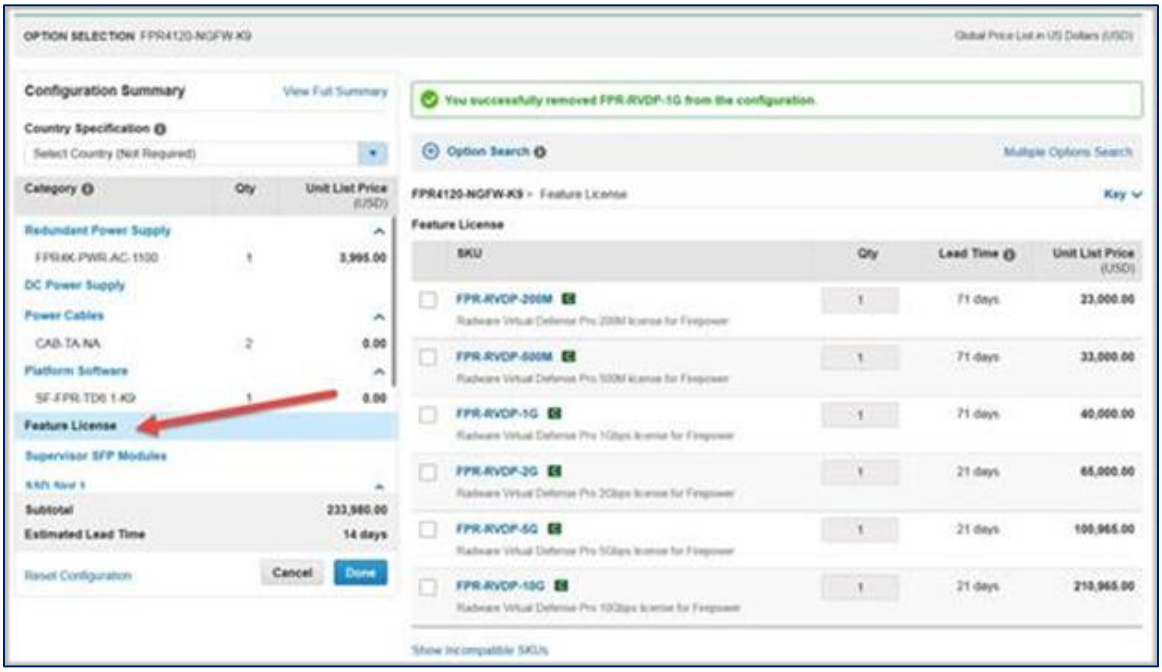



**Figure 7.**
Feature licenses

When you make your selection, you will see the Service Contract and the Right-to-Use licenses are automatically added to the cart. As with the SPARE license, you can change the length of the service contract by clicking the “Edit Service/Subscription” link. You will find the EMCU contract under the selected Radware SKU.

If you do not already own Radware Vision Manager, please add to your order SKU: L-RDWR-APV-VA=. This is the Radware Manager Vision and Security Reporter with support for 10 vDP instances.

### Links and Resources for Radware vDP

For Cisco internal questions, please send an email to: ask-radware@external.cisco.com

For Radware specific questions, please go to Cisco Technology Partnership with Radware.

#### Ordering the Cisco Firepower 1000 Series

The following tables outline the product part number information for the Cisco Firepower 1000 Series. Table 18A and 18B provide the top-level part numbers for chassis running ASA or Firewall Threat Defense software. Note that threat defense subscriptions can only be added to chassis running Firewall Threat Defense software.

© 2026 Cisco and/or its affiliates. All rights reserved.

**Table 18A.** 1000 Series Chassis Part Numbers

| Part Number | Description |
|---|---|
| **Bundles** | |
| **FPR1010-BUN** | Cisco Firepower 1010 Master Bundle (allows selection of ASA or FTD model) |
| **FPR1120-BUN** | Cisco Firepower 1120 Master Bundle (allows selection of ASA or FTD model) |
| **FPR1140-BUN** | Cisco Firepower 1140 Master Bundle (allows selection of ASA or FTD model) |
| **FPR1150-BUN** | Cisco Firepower 1150 Master Bundle (allows selection of ASA or FTD model) |
| **FPR1010-FTD-HA-BUN** | Cisco Firepower 1010 Two-Unit High Availability Bundle (will order 2 identical chassis and software subscriptions to be configured as a high-availability pair) |
| **FPR1120-FTD-HA-BUN** | Cisco Firepower 1120 Two-Unit High Availability Bundle (will order 2 identical chassis and software subscriptions to be configured as a high-availability pair) |
| **FPR1140-FTD-HA-BUN** | Cisco Firepower 1140 Two-Unit High Availability Bundle (will order 2 identical chassis and software subscriptions to be configured as a high-availability pair) |
| **FPR1150-FTD-HA-BUN** | Cisco Firepower 1150 Two-Unit High Availability Bundle (will order 2 identical chassis and software subscriptions to be configured as a high-availability pair) |
| **Appliances** | |
| **FPR1010-NGFW-K9** | Cisco Firepower 1010 NGFW Appliance, Desktop, PoE<br>(runs FTD software + optional subscriptions) |
| **FPR1010E-NGFW-K9** | Cisco Firepower 1010E NGFW Appliance, Desktop, no PoE<br>(runs FTD software + optional subscriptions) |
| **FPR1120-NGFW-K9** | Cisco Firepower 1120 NGFW Appliance, 1RU<br>(runs FTD software + optional subscriptions) |
| **FPR1140-NGFW-K9** | Cisco Firepower 1140 NGFW Appliance, 1RU<br>(runs FTD software + optional subscriptions) |
| **FPR1150-NGFW-K9** | Cisco Firepower 1150 NGFW Appliance, 1RU<br>(runs FTD software + optional subscriptions) |
| **FPR1010-ASA-K9** | Cisco Firepower 1010 NGFW Appliance, Desktop, PoE<br>(run ASA SW + Optional security plus license for High Availability) |
| **FPR1010E-ASA-K9** | Cisco Firepower 1010E NGFW Appliance, Desktop. no PoE<br>(run ASA SW + Optional security plus license for High Availability) |
| **FPR1120-ASA-K9** | Cisco Firepower 1120 NGFW Appliance, 1RU<br>(runs ASA software + optional security context license) |
| **FPR1140-ASA-K9** | Cisco Firepower 1140 NGFW Appliance, 1RU<br>(runs ASA software + optional security context license) |
| **FPR1150-ASA-K9** | Cisco Firepower 1150 NGFW Appliance, 1RU<br>(runs ASA software + optional security context license) |

© 2026 Cisco and/or its affiliates. All rights reserved.

**Table 18B.** 1000 Series ASA Licenses

| Part Number | Description |
|---|---|
| **ASA Standard License** | |
| **FPR1000-ASA** | Cisco Firepower 1000 Standard ASA License |
| **L-FPR1000-ASA=** | Cisco Firepower 1000 Standard ASA License |
| **Security Context Licenses** | |
| **L-FPR1K-ASASC-10=** | Cisco Firepower 1000 - Add 10 Security Context Licenses |
| **L-FPR1K-ASASC-5=** | Cisco Firepower 1000 - Add 5 Security Context Licenses |
| **Encryption Licenses** | |
| **L-FPR1K-ENC-K9=** | Cisco Firepower 1K Series ASA Strong Encryption (3DES/AES) |
| **FPR1010 Security Plus License (required for 2-box High-Availability configurations)** | |
| **L-FPR1010-SEC-PL=** | Cisco Firepower 1010 - Security Plus License |

**Table 19.** 1000 Series Accessories

| Part Number | Description |
|---|---|
| **FPR1K-CBL-MGMT=** | Cisco Firepower 1k Series Cable Mgmt Brackets 1120/1140/1150 |
| **FPR1K-DT-ACY-KIT=** | Cisco Firepower 1K Series Accessory Kit for FPR-1010 |
| **FPR1K-DT-PWR-AC=** | Cisco Firepower 1K Series 115W Power Adapter for FPR-1010 |
| **FPR1K-DT-FIPS-KIT=** | Cisco Firepower 1K Series FIPS Kit for FPR-1010 |
| **PWR-DT-150W-AC=** | Power supply, desktop, 150W, AC input |
| **FPR1010-RACK-MNT=** | Cisco Firepower 1K Series Rackmount Kit for FPR-1010 |
| **FPR1K-DT-RACK-MNT=** | Cisco Firepower 1K Series Rackmount Kit for FPR-1010 |
| **FPR1K-DT-WALL-MNT=** | Cisco Firepower 1K Series Wall Mount for FPR-1010 |
| **FPR1K-RM-ACY-KIT=** | Cisco Firepower 1K Series Accessory Kit for FPR-1120/1140/1150 |
| **FPR1K-RM-BRKT=** | Cisco Firepower 1K Series Rackmount Brackets - FPR-1120/1140/1150 |
| **FPR1K-RM-FIPS-KIT=** | Cisco Firepower 1K Series FIPS Kits for FPR-1120/1140/1150 |
| **FPR1K-RM-SSD200=** | Cisco Firepower 1K Series 200GB for FPR-1120/1140/1150 |

**Note:** Use these part numbers if the customer is ordering spare assemblies or mounting accessories

© 2026 Cisco and/or its affiliates. All rights reserved.

### SKUs for 1000 Series Licenses and Subscriptions

When ordering a 1000 Series with the Cisco Secure Firewall Threat Defense image, both licenses and a subscription to optional security services are required. Subscription terms are 1, 3, and 5 years, with discounts applied to multi-year terms. In the listed part numbers, the threat services are identified as follows:

**Table 20.** Threat Subscription Details

| Threat Subscription Abbreviations | Description |
|---|---|
| **T** | Threat (Security Intelligence and IPS) |
| **M or AMP*** | Malware defense |
| **C or URL*** | URL Filtering |
| **1Y** | **1-Year** Subscription |
| **3Y** | **3-Year** Subscription |
| **5Y** | **5-Year** Subscription |

*Note that Threat/IPS (T) License is a requirement for the use of Malware (M) or URL (C) license features.

**Table 21.** Cisco Firepower 1000 Series License Part Numbers for Configurations with the Cisco Secure Firewall Threat Defense Image

| Part Number | Description |
|---|---|
| **L-FPR1010T-AMP=** | Cisco Firepower 1010 Threat Defense Malware Protection License |
| **L-FPR1010T-T=** | Cisco Firepower 1010 Threat Defense Threat Protection License |
| **L-FPR1010T-TC=** | Cisco Firepower 1010 Threat Defense Threat and URL License |
| **L-FPR1010T-TM=** | Cisco Firepower 1010 Threat Defense Threat and Malware License |
| **L-FPR1010T-TMC=** | Cisco Firepower 1010 Threat Defense Threat, Malware, and URL License |
| **L-FPR1010T-URL=** | Cisco Firepower 1010 Threat Defense URL Filtering License |
| **L-FPR1120T-AMP=** | Cisco Firepower 1120 Threat Defense Malware Protection License |
| **L-FPR1120T-T=** | Cisco Firepower 1120 Threat Defense Threat Protection License |
| **L-FPR1120T-TC=** | Cisco Firepower 1120 Threat Defense Threat and URL License |
| **L-FPR1120T-TM=** | Cisco Firepower 1120 Threat Defense Threat and Malware License |
| **L-FPR1120T-TMC=** | Cisco Firepower 1120 Threat Defense Threat, Malware, and URL License |
| **L-FPR1120T-URL=** | Cisco Firepower 1120 Threat Defense URL Filtering License |
| **L-FPR1140T-AMP=** | Cisco Firepower 1140 Threat Defense Malware Protection License |

© 2026 Cisco and/or its affiliates. All rights reserved.

| Part Number | Description |
|---|---|
| **L-FPR1140T-T=** | Cisco Firepower 1140 Threat Defense Threat Protection License |
| **L-FPR1140T-TC=** | Cisco Firepower 1140 Threat Defense Threat and URL License |
| **L-FPR1140T-TM=** | Cisco Firepower 1140 Threat Defense Threat and Malware License |
| **L-FPR1140T-TMC=** | Cisco Firepower 1140 Threat Defense Threat, Malware, and URL License |
| **L-FPR1140T-URL=** | Cisco Firepower 1140 Threat Defense URL Filtering License |
| **L-FPR1150T-AMP=** | Cisco Firepower 1150 Threat Defense Malware Protection License |
| **L-FPR1150T-T=** | Cisco Firepower 1150 Threat Defense Threat Protection License |
| **L-FPR1150T-TC=** | Cisco Firepower 1150 Threat Defense Threat and URL License |
| **L-FPR1150T-TM=** | Cisco Firepower 1150 Threat Defense Threat and Malware License |
| **L-FPR1150T-TMC=** | Cisco Firepower 1150 Threat Defense Threat, Malware, and URL License |
| **L-FPR1150T-URL=** | Cisco Firepower 1150 Threat Defense URL Filtering License |

**Table 22.** Cisco Firepower 1000 Series Subscription Part Numbers for Configurations with the Firewall Threat Defense Image

| Part Number | Description |
|---|---|
| **L-FPR1010T-AMP-1Y** | Cisco Firepower 1010 Threat Defense Malware Protection 1Y Subscription |
| **L-FPR1010T-AMP-3Y** | Cisco Firepower 1010 Threat Defense Malware Protection 3Y Subscription |
| **L-FPR1010T-AMP-5Y** | Cisco Firepower 1010 Threat Defense Malware Protection 5Y Subscription |
| **L-FPR1010T-T-1Y** | Cisco Firepower 1010 Threat Defense Threat Protection 1Y Subscription |
| **L-FPR1010T-T-3Y** | Cisco Firepower 1010 Threat Defense Threat Protection 3Y Subscription |
| **L-FPR1010T-T-5Y** | Cisco Firepower 1010 Threat Defense Threat Protection 5Y Subscription |
| **L-FPR1010T-TC-1Y** | Cisco Firepower 1010 Threat Defense Threat and URL 1Y Subscription |
| **L-FPR1010T-TC-3Y** | Cisco Firepower 1010 Threat Defense Threat and URL 3Y Subscription |
| **L-FPR1010T-TC-5Y** | Cisco Firepower 1010 Threat Defense Threat and URL 5Y Subscription |
| **L-FPR1010T-TM-1Y** | Cisco Firepower 1010 Threat Defense Threat and Malware 1Y Subscription |
| **L-FPR1010T-TM-3Y** | Cisco Firepower 1010 Threat Defense Threat and Malware 3Y Subscription |
| **L-FPR1010T-TM-5Y** | Cisco Firepower 1010 Threat Defense Threat and Malware 5Y Subscription |
| **L-FPR1010T-TMC-1Y** | Cisco Firepower 1010 Threat Defense Threat, Malware, and URL 1Y Subscription |
| **L-FPR1010T-TMC-3Y** | Cisco Firepower 1010 Threat Defense Threat, Malware, and URL 3Y Subscription |

© 2026 Cisco and/or its affiliates. All rights reserved.

| Part Number | Description |
|---|---|
| **L-FPR1010T-TMC-5Y** | Cisco Firepower 1010 Threat Defense Threat, Malware, and URL 5Y Subscription |
| **L-FPR1010T-URL-1Y** | Cisco Firepower 1010 Threat Defense URL Filtering 1Y Subscription |
| **L-FPR1010T-URL-3Y** | Cisco Firepower 1010 Threat Defense URL Filtering 3Y Subscription |
| **L-FPR1010T-URL-5Y** | Cisco Firepower 1010 Threat Defense URL Filtering 5Y Subscription |
| **L-FPR1120T-AMP-1Y** | Cisco Firepower 1120 Threat Defense Malware Protection 1Y Subscription |
| **L-FPR1120T-AMP-3Y** | Cisco Firepower 1120 Threat Defense Malware Protection 3Y Subscription |
| **L-FPR1120T-AMP-5Y** | Cisco Firepower 1120 Threat Defense Malware Protection 5Y Subscription |
| **L-FPR1120T-T-1Y** | Cisco Firepower 1120 Threat Defense Threat Protection 1Y Subscription |
| **L-FPR1120T-T-3Y** | Cisco Firepower 1120 Threat Defense Threat Protection 3Y Subscription |
| **L-FPR1120T-T-5Y** | Cisco Firepower 1120 Threat Defense Threat Protection 5Y Subscription |
| **L-FPR1120T-TC-1Y** | Cisco Firepower 1120 Threat Defense Threat and URL 1Y Subscription |
| **L-FPR1120T-TC-3Y** | Cisco Firepower 1120 Threat Defense Threat and URL 3Y Subscription |
| **L-FPR1120T-TC-5Y** | Cisco Firepower 1120 Threat Defense Threat and URL 5Y Subscription |
| **L-FPR1120T-TM-1Y** | Cisco Firepower 1120 Threat Defense Threat and Malware 1Y Subscription |
| **L-FPR1120T-TM-3Y** | Cisco Firepower 1120 Threat Defense Threat and Malware 3Y Subscription |
| **L-FPR1120T-TM-5Y** | Cisco Firepower 1120 Threat Defense Threat and Malware 5Y Subscription |
| **L-FPR1120T-TMC-1Y** | Cisco Firepower 1120 Threat Defense Threat, Malware, and URL 1Y Subscription |
| **L-FPR1120T-TMC-3Y** | Cisco Firepower 1120 Threat Defense Threat, Malware, and URL 3Y Subscription |
| **L-FPR1120T-TMC-5Y** | Cisco Firepower 1120 Threat Defense Threat, Malware, and URL 5Y Subscription |
| **L-FPR1120T-URL-1Y** | Cisco Firepower 1120 Threat Defense URL Filtering 1Y Subscription |
| **L-FPR1120T-URL-3Y** | Cisco Firepower 1120 Threat Defense URL Filtering 3Y Subscription |
| **L-FPR1120T-URL-5Y** | Cisco Firepower 1120 Threat Defense URL Filtering 5Y Subscription |
| **L-FPR1140T-AMP-1Y** | Cisco Firepower 1140 Threat Defense Malware Protection 1Y Subscription |
| **L-FPR1140T-AMP-3Y** | Cisco Firepower 1140 Threat Defense Malware Protection 3Y Subscription |
| **L-FPR1140T-AMP-5Y** | Cisco Firepower 1140 Threat Defense Malware Protection 5Y Subscription |
| **L-FPR1140T-T-1Y** | Cisco Firepower 1140 Threat Defense Threat Protection 1Y Subscription |
| **L-FPR1140T-T-3Y** | Cisco Firepower 1140 Threat Defense Threat Protection 3Y Subscription |

© 2026 Cisco and/or its affiliates. All rights reserved.

| Part Number | Description |
|---|---|
| **L-FPR1140T-T-5Y** | Cisco Firepower 1140 Threat Defense Threat Protection 5Y Subscription |
| **L-FPR1140T-TC-1Y** | Cisco Firepower 1140 Threat Defense Threat and URL 1Y Subscription |
| **L-FPR1140T-TC-3Y** | Cisco Firepower 1140 Threat Defense Threat and URL 3Y Subscription |
| **L-FPR1140T-TC-5Y** | Cisco Firepower 1140 Threat Defense Threat and URL 5Y Subscription |
| **L-FPR1140T-TM-1Y** | Cisco Firepower 1140 Threat Defense Threat and Malware 1Y Subscription |
| **L-FPR1140T-TM-3Y** | Cisco Firepower 1140 Threat Defense Threat and Malware 3Y Subscription |
| **L-FPR1140T-TM-5Y** | Cisco Firepower 1140 Threat Defense Threat and Malware 5Y Subscription |
| **L-FPR1140T-TMC-1Y** | Cisco Firepower 1140 Threat Defense Threat, Malware, and URL 1Y Subscription |
| **L-FPR1140T-TMC-3Y** | Cisco Firepower 1140 Threat Defense Threat, Malware, and URL 3Y Subscription |
| **L-FPR1140T-TMC-5Y** | Cisco Firepower 1140 Threat Defense Threat, Malware, and URL 5Y Subscription |
| **L-FPR1140T-URL-1Y** | Cisco Firepower 1140 Threat Defense URL Filtering 1Y Subscription |
| **L-FPR1140T-URL-3Y** | Cisco Firepower 1140 Threat Defense URL Filtering 3Y Subscription |
| **L-FPR1140T-URL-5Y** | Cisco Firepower 1140 Threat Defense URL Filtering 5Y Subscription |
| **L-FPR1150T-AMP-1Y** | Cisco FPR1150 Threat Defense Malware Protection 1Y Subs |
| **L-FPR1150T-AMP-3Y** | Cisco FPR1150 Threat Defense Malware Protection 3Y Subs |
| **L-FPR1150T-AMP-5Y** | Cisco FPR1150 Threat Defense Malware Protection 5Y Subs |
| **L-FPR1150T-T-1Y** | Cisco FPR1150 Threat Defense Threat Protection 1Y Subs |
| **L-FPR1150T-T-3Y** | Cisco FPR1150 Threat Defense Threat Protection 3Y Subs |
| **L-FPR1150T-T-5Y** | Cisco FPR1150 Threat Defense Threat Protection 5Y Subs |
| **L-FPR1150T-TC-1Y** | Cisco FPR1150 Threat Defense Threat and URL 1Y Subs |
| **L-FPR1150T-TC-3Y** | Cisco FPR1150 Threat Defense Threat and URL 3Y Subs |
| **L-FPR1150T-TC-5Y** | Cisco FPR1150 Threat Defense Threat and URL 5Y Subs |
| **L-FPR1150T-TM-1Y** | Cisco FPR1150 Threat Defense Threat and Malware 1Y Subs |
| **L-FPR1150T-TM-3Y** | Cisco FPR1150 Threat Defense Threat and Malware 3Y Subs |
| **L-FPR1150T-TM-5Y** | Cisco FPR1150 Threat Defense Threat and Malware 5Y Subs |
| **L-FPR1150T-TMC-1Y** | Cisco FPR1150 Threat Defense Threat, Malware and URL 1Y Subs |
| **L-FPR1150T-TMC-3Y** | Cisco FPR1150 Threat Defense Threat, Malware and URL 3Y Subs |

© 2026 Cisco and/or its affiliates. All rights reserved.

| Part Number | Description |
|---|---|
| **L-FPR1150T-TMC-5Y** | Cisco FPR1150 Threat Defense Threat, Malware and URL 5Y Subs |
| **L-FPR1150T-URL-1Y** | Cisco FPR1150 Threat Defense URL Filtering 1Y Subs |
| **L-FPR1150T-URL-3Y** | Cisco FPR1150 Threat Defense URL Filtering 3Y Subs |
| **L-FPR1150T-URL-5Y** | Cisco FPR1150 Threat Defense URL Filtering 5Y Subs |

**Ordering Example: Cisco Firepower 1010 with FTD**

**Step 1:** Smart Software Licensing

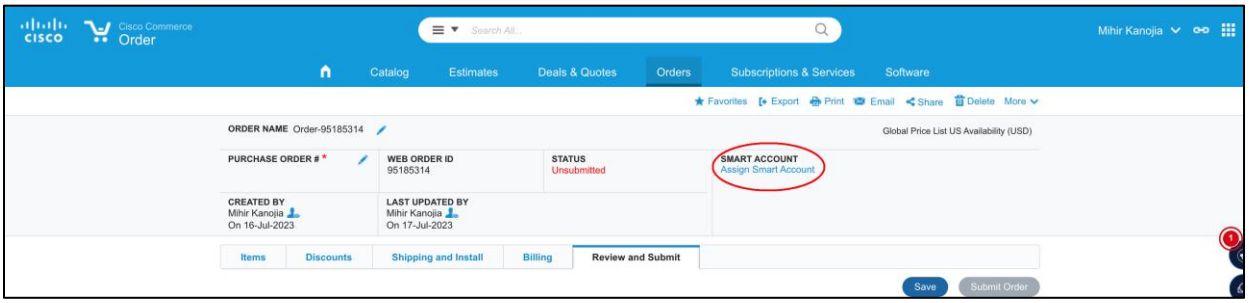
Before placing a Cisco Firepower 1010 order, the end customer must have a Cisco Smart Licensing account. For information about Smart Accounts and instructions on how to create an account, visit: https://www.cisco.com/web/ordering/smart-software-manager/index.html.

To associate the order's licenses with the customer's Smart Licensing account, or to begin the establishment of the Smart Licensing account, follow these steps. Note that if you are initiating the account, you can complete the order only if the account is initiated on the end customer's behalf and associated with the order.

Go to Cisco Commerce: https://www.cisco.com/go/ccw.

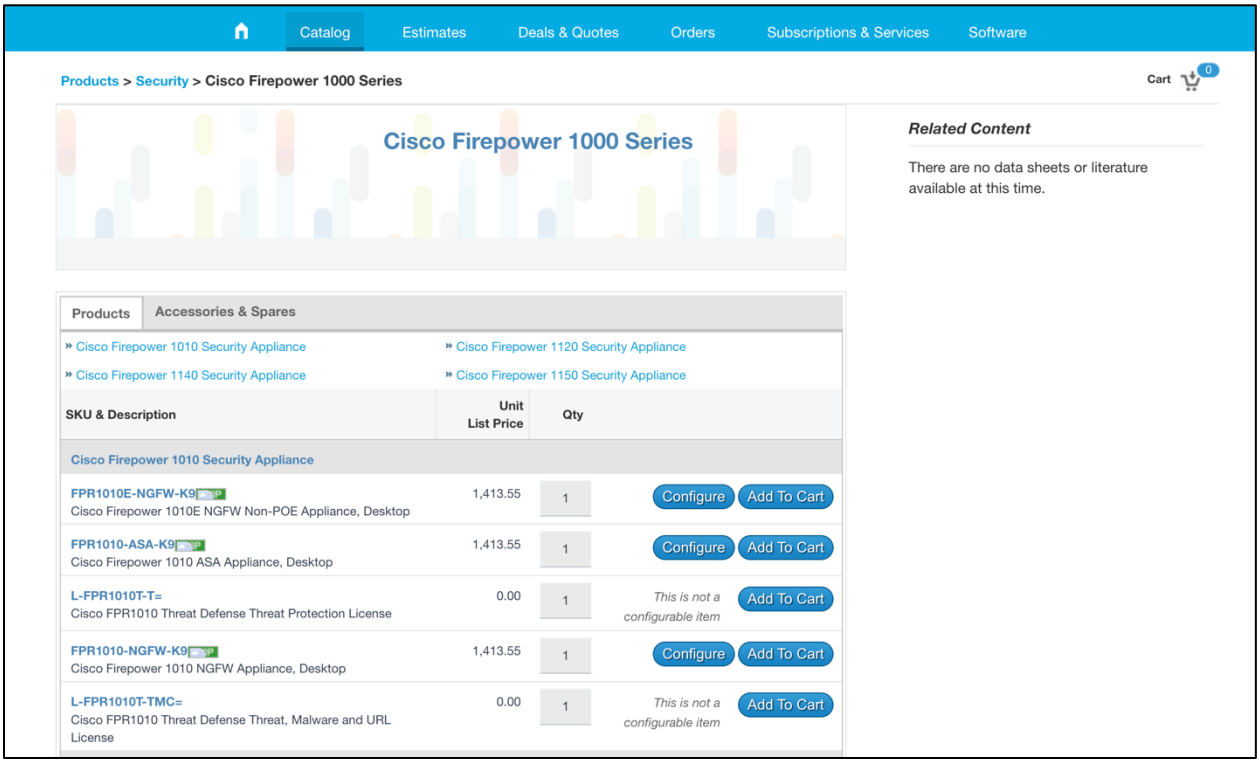
From the Orders pull-down menu, select Create Order.

Select Assign Smart Account and follow the subsequent prompts for Smart Licensing.

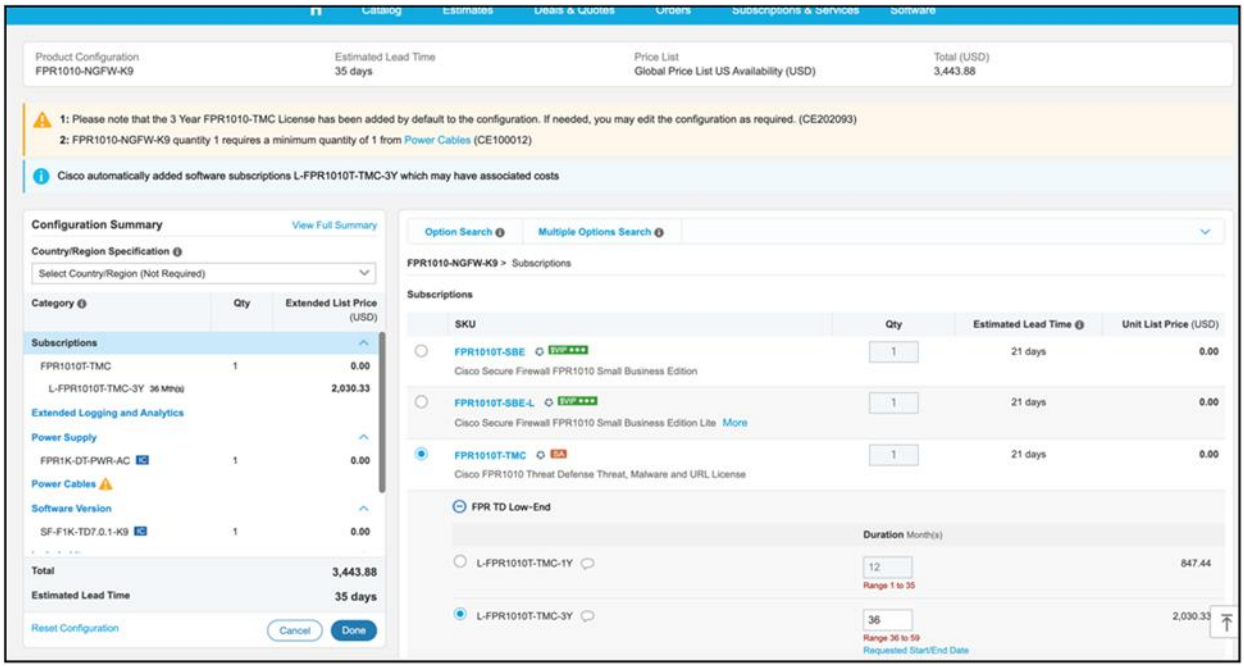



© 2026 Cisco and/or its affiliates. All rights reserved.

**Step 2:** Navigate to Catalog -> Products -> Security -> Firewalls -> Cisco Firepower 1000 Series. Select “Configure” for the FPR1010-NGFW-K9

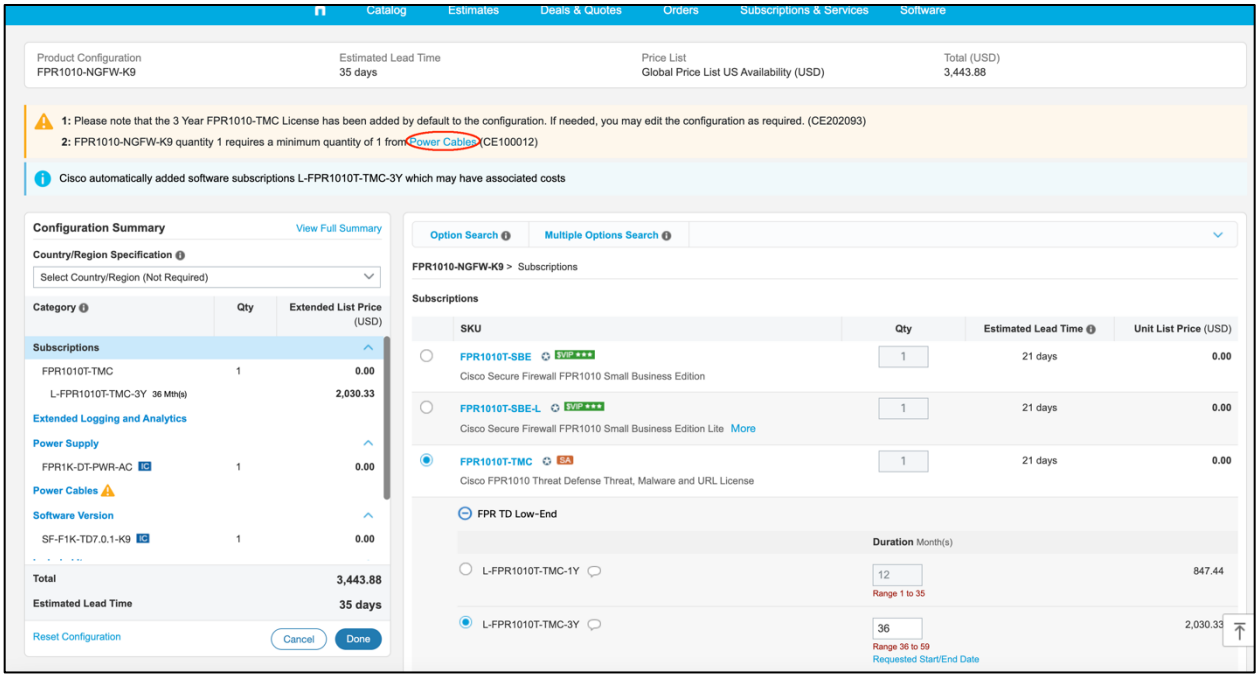


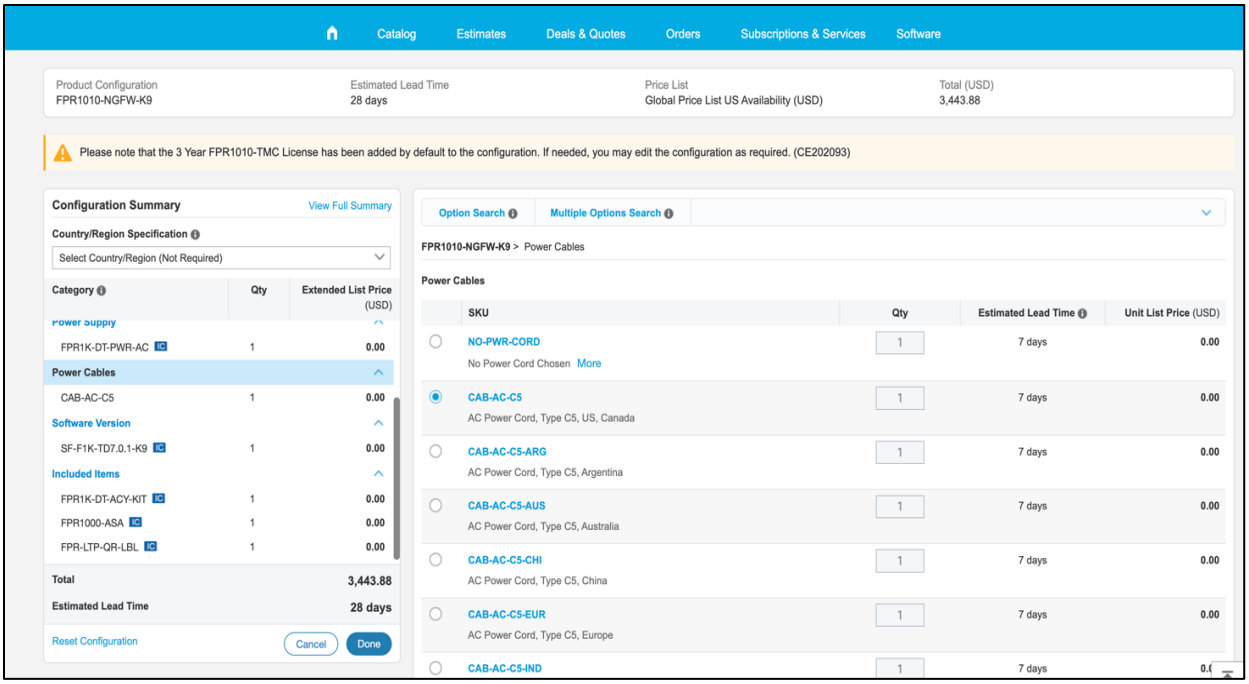

The Chassis is added on the cart along with the software subscription. By default, the 3 Year FPR1010-TMC license will be added to the configuration.




© 2026 Cisco and/or its affiliates. All rights reserved.

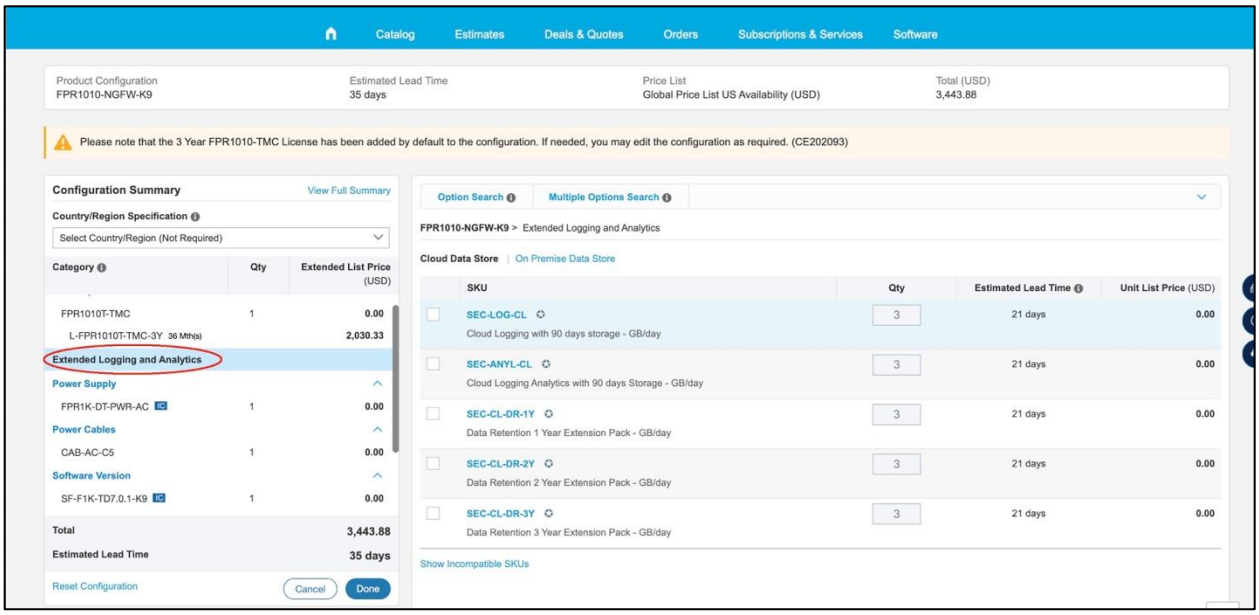
**Step 3:** Follow the instructions in the yellow box. First, click the power cables link and make the cable selection in the next screen.

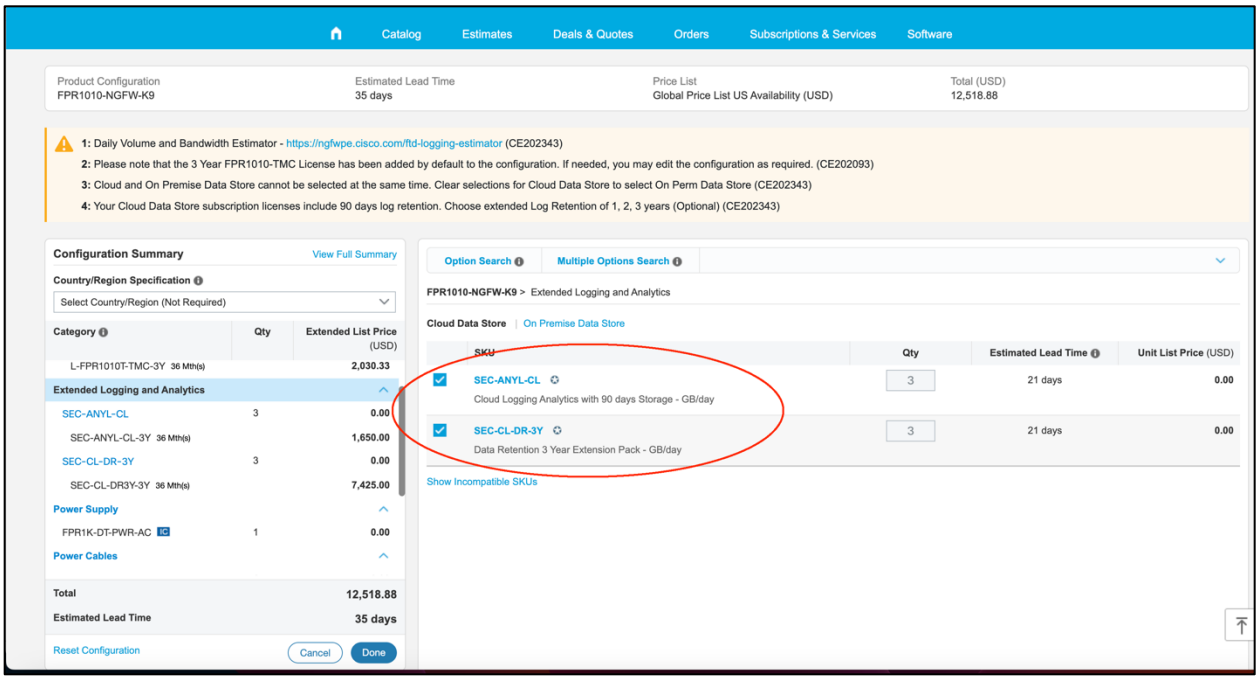



© 2026 Cisco and/or its affiliates. All rights reserved.

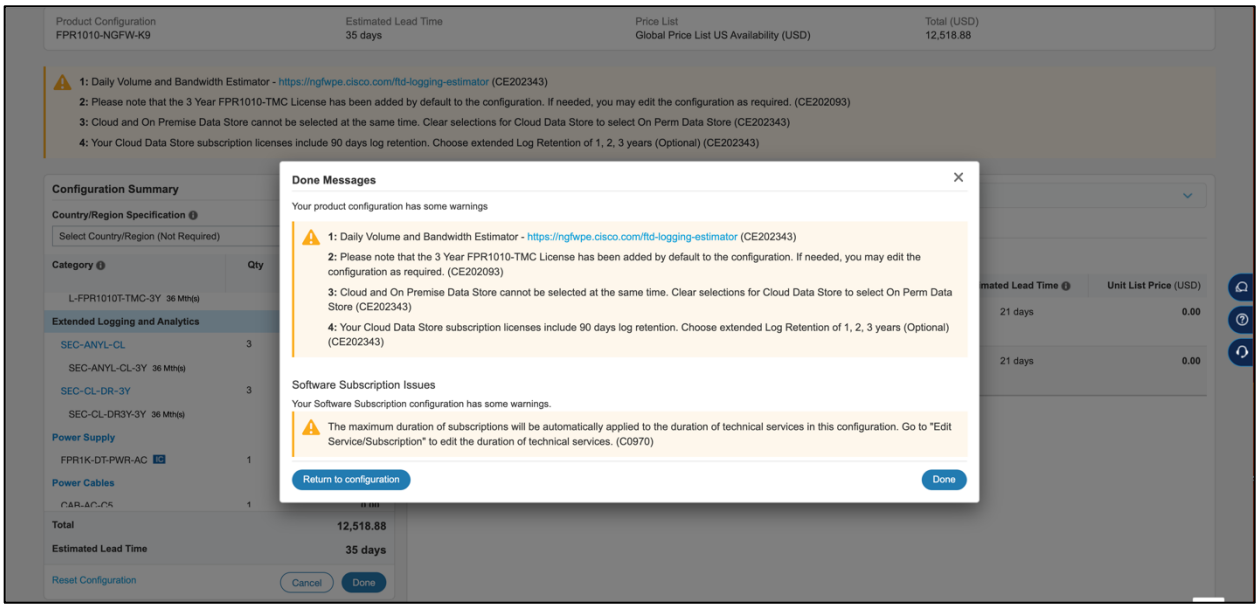
**Step 4:** After cable(s) selection, if there is a requirement for extended logging and analytics. Click on Extended logging and analytics on the configuration summary and add the cloud logging option along with the data retention SKU.



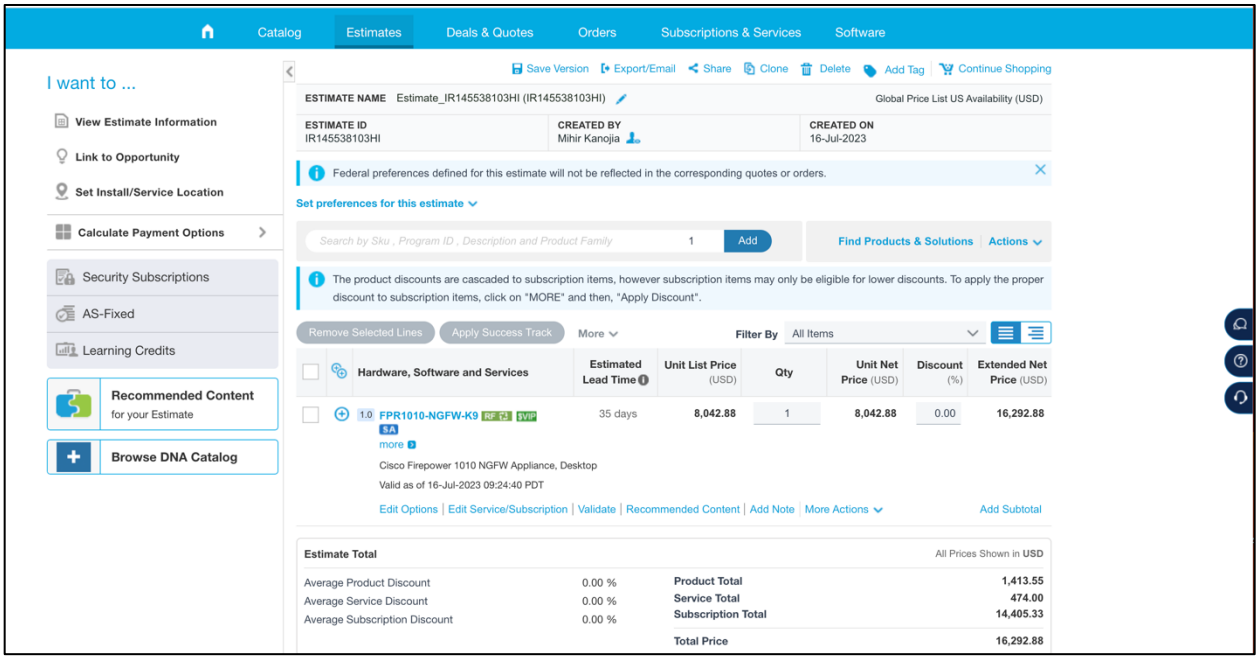




© 2026 Cisco and/or its affiliates. All rights reserved.

**Step 5:** After completing the selection of the Extended logging and analytics. Click “Done” to complete the configuration. An alert message appears to indicate to the user of the selected configuration. Click “Done” to proceed to the summary screen.




**Step 6:** After clicking done. The product configuration summary page will appear with all the selection.




### Ordering the Cisco Secure Firewall 1200 Series

The following tables provide product part numbers for the Cisco Secure Firewall 1200 Series. Start by selecting an appliance, then review the available options. Spare components and accessories can also be ordered separately.

© 2026 Cisco and/or its affiliates. All rights reserved.

**Table 23.** 1200 Series Appliances – Compact models

| Part Number | Description |
|---|---|
| **CSF1210CE-TD-K9** | Cisco Secure Firewall 1210 Compact Appliance, Threat Defense software |
| **CSF1210CP-TD-K9** | Cisco Secure Firewall 1210 Compact Appliance with PoE, Threat Defense software |
| **CSF1220CX-TD-K9** | Cisco Secure Firewall 1220 Compact Appliance with 10G SFP+, Threat Defense software |
| **CSF1210CE-ASA-K9** | Cisco Secure Firewall 1210 Compact Appliance, ASA software |
| **CSF1210CP-ASA-K9** | Cisco Secure Firewall 1210 Compact Appliance with PoE, ASA software |
| **CSF1220CX-ASA-K9** | Cisco Secure Firewall 1220 Compact Appliance with 10G SFP+, ASA software |

**Table 24.** 1200 Series Accessories – Compact Models

| Part Number | Description |
|---|---|
| **CSF1200C-PWR-AC=** | Secure Firewall 1200 Series power supply, compact models without PoE |
| **CSF1200CP-PWR-AC=** | Secure Firewall 1200 Series power supply, compact models with PoE |
| **CSF1200C-RACK-MNT=** | Secure Firewall 1200 Series rack-mount kit for compact models |
| **CSF1200C-WALL-MNT=** | Secure Firewall 1200 Series wall-mount kit for compact models |

**Table 25.** 1200 Series Appliances – 1U rack-mount models

| Part Number | Description |
|---|---|
| **CSF1230-TD-K9** | Cisco Secure Firewall 1230 Appliance, Threat Defense software |
| **CSF1240-TD-K9** | Cisco Secure Firewall 1240 Appliance, Threat Defense software |
| **CSF1250-TD-K9** | Cisco Secure Firewall 1250 Appliance, Threat Defense software |
| **CSF1230-ASA-K9** | Cisco Secure Firewall 1230 Appliance, ASA software |
| **CSF1240-ASA-K9** | Cisco Secure Firewall 1240 Appliance, ASA software |
| **CSF1250-ASA-K9** | Cisco Secure Firewall 1250 Appliance, ASA software |

© 2026 Cisco and/or its affiliates. All rights reserved.

**Table 26.** 1200 Series Accessories – 1U rack-mount models

| Part Number | Description |
|---|---|
| **CSF1200-SSD960=** | Secure Firewall 1200 Series SSD, 960 GB |
| **CSF1200-CBL-MGMT=** | Secure Firewall 1200 Series cable management accessory |

Threat Defense subscriptions provide signature updates for 1200 Series appliances with FTD software. Subscriptions are available with 1-year, 3-year and 5-year terms. Select a subscription package first, then select a subscription term.

A-la-carte subscription licenses can be ordered separately, or for renewals. A-la-carte part numbers are prefixed with L-, for example “L-CSF1210CET-T=” is the stand-alone equivalent of “CSF1210CET-T”

**Table 27.** 1200 Series Threat Defense Subscriptions

| Part Number | Description |
|---|---|
| **CSF1210CET-T** | CSF 1210CE Threat Defense IPS License |
| **CSF1210CET-TM** | CSF 1210CE Threat Defense IPS & Malware Defense License |
| **CSF1210CET-TC** | CSF 1210CE Threat Defense IPS & URL Filtering License |
| **CSF1210CET-TMC** | CSF 1210CE Threat Defense IPS, Malware & URL License |
| **CSF1210CET-AMP** | CSF 1210CE Threat Defense Malware Defense License |
| **CSF1210CET-URL** | CSF 1210CE Threat Defense URL Filtering License |
| **CSF1210CPT-T** | CSF 1210CP Threat Defense IPS License |
| **CSF1210CPT-TM** | CSF 1210CP Threat Defense IPS & Malware Defense License |
| **CSF1210CPT-TC** | CSF 1210CP Threat Defense IPS & URL Filtering License |
| **CSF1210CPT-TMC** | CSF 1210CP Threat Defense IPS, Malware & URL License |
| **CSF1210CPT-AMP** | CSF 1210CP Threat Defense Malware Defense License |
| **CSF1210CPT-URL** | CSF 1210CP Threat Defense URL Filtering License |
| **CSF1220CXT-T** | CSF 1220CX Threat Defense IPS License |
| **CSF1220CXT-TM** | CSF 1220CX Threat Defense IPS & Malware Defense License |
| **CSF1220CXT-TC** | CSF 1220CX Threat Defense IPS & URL Filtering License |
| **CSF1220CXT-TMC** | CSF 1220CX Threat Defense IPS, Malware & URL License |
| **CSF1220CXT-AMP** | CSF 1220CX Threat Defense Malware Defense License |
| **CSF1220CXT-URL** | CSF 1220CX Threat Defense URL Filtering License |
| **CSF12T-T** | CSF 1210CE Threat Defense IPS License |

© 2026 Cisco and/or its affiliates. All rights reserved.

| Part Number | Description |
|---|---|
| **CSF12CET-TM** | CSF 1210CE Threat Defense IPS & Malware Defense License |
| **CSF1210CET-TC** | CSF 1210CE Threat Defense IPS & URL Filtering License |
| **CSF1210CET-TMC** | CSF 1210CE Threat Defense IPS, Malware & URL License |
| **CSF1210CET-AMP** | CSF 1210CE Threat Defense Malware Defense License |
| **CSF1210CET-URL** | CSF 1210CE Threat Defense URL Filtering License |
| **CSF1230T-T** | CSF 1230 Threat Defense IPS License |
| **CSF1230T-TM** | CSF 1230 Threat Defense IPS & Malware Defense License |
| **CSF1230T-TC** | CSF 1230 Threat Defense IPS & URL Filtering License |
| **CSF1230T-TMC** | CSF 1230 Threat Defense IPS, Malware & URL License |
| **CSF1230T-AMP** | CSF 1230 Threat Defense Malware Defense License |
| **CSF1230T-URL** | CSF 1230 Threat Defense URL Filtering License |
| **CSF1240T-T** | CSF 1240 Threat Defense IPS License |
| **CSF1240T-TM** | CSF 1240 Threat Defense IPS & Malware Defense License |
| **CSF1240T-TC** | CSF 1240 Threat Defense IPS & URL Filtering License |
| **CSF1240T-TMC** | CSF 1240 Threat Defense IPS, Malware & URL License |
| **CSF1240T-AMP** | CSF 1240 Threat Defense Malware Defense License |
| **CSF1240T-URL** | CSF 1240 Threat Defense URL Filtering License |
| **CSF1250T-T** | CSF 1250 Threat Defense IPS License |
| **CSF1250T-TM** | CSF 1250 Threat Defense IPS & Malware Defense License |
| **CSF1250T-TC** | CSF 1250 Threat Defense IPS & URL Filtering License |
| **CSF1250T-TMC** | CSF 1250 Threat Defense IPS, Malware & URL License |
| **CSF1250T-AMP** | CSF 1250 Threat Defense Malware Defense License |
| **CSF1250T-URL** | CSF 1250 Threat Defense URL Filtering License |
| **CSF1260T-T** | CSF 1260 Threat Defense IPS License |
| **CSF1260T-TM** | CSF 1260 Threat Defense IPS & Malware Defense License |
| **CSF1260T-TC** | CSF 1260 Threat Defense IPS & URL Filtering License |
| **CSF1260T-TMC** | CSF 1260 Threat Defense IPS, Malware & URL License |

© 2026 Cisco and/or its affiliates. All rights reserved.

| Part Number | Description |
|---|---|
| **CSF1260T-AMP** | CSF 1260 Threat Defense Malware Defense License |
| **CSF1260T-URL** | CSF 1260 Threat Defense URL Filtering License |

**Ordering the Cisco Secure Firewall 200 Series**

The following tables provide product part numbers for the Cisco Secure Firewall 200 Series. Start by selecting an appliance, then review the available options. Spare components and accessories can also be ordered separately.

**Note:** '++' suffix denotes TAA compliant models.

**Table 28.** 200 Series Appliances – Compact models

| Part Number | Description |
|---|---|
| **CSF220-ASA-K9**<br>**CSF220-ASA-K9++** | Cisco Secure Firewall 220 Appliance, ASA |
| **CSF220-TD-K9**<br>**CSF220-TD-K9++** | Cisco Secure Firewall 220 Appliance, Threat Defense |
| **CSF240P-ASA-K9**<br>**CSF240P-ASA-K9++** | Cisco Secure Firewall 240P Appliance, POE, ASA |
| **CSF240P-TD-K9**<br>**CSF240P-TD-K9++** | Cisco Secure Firewall 240P Appliance, POE, Threat Defense |

**Table 29.** 200 Series Accessories – Compact Models

| Part Number | Description |
|---|---|
| **CSF200-WALL-MNT=** | Cisco Secure Firewall 200 Series Wall-Mount kit |
| **CSF200-RCKMNT-FX=** | Cisco Secure Firewall Rackmount Kit, w/Fixed Brackets for CSF220 / 240P |
| **CSF200-RCKMNT-SR=** | Cisco Secure Firewall Rackmount Kit, w/Slide Rails for CSF220 / 240P |
| **CAB-CONS-USB-C=** | Console cable, USB-C to USB-C, 6ft |
| **PWR-DT-30W-AC=** | Power supply, compact, 30W, AC input |
| **CSF200-CBL-MGMT=** | Cisco Secure Firewall 200 Series cable management |
| **PWR-DT-190W-AC=** | Cisco Secure Firewall Pwr Sup, Compact, 190W, AC input (POE) |
| **PWR-DT-230W-AC=** | Cisco Secure Firewall Pwr Sup, Compact, 230W (supported only for India region) |

© 2026 Cisco and/or its affiliates. All rights reserved.

Threat Defense subscriptions provide signature updates for 200 Series appliances with TD software. Subscriptions are available for 1-year, 3-year, and 5-year terms. Select a subscription package first, then select a subscription term.

A-la-carte subscription licenses can be ordered separately, or for renewals. A-la-carte part numbers are prefixed with L-, for example “L-CSF220T-T=” is the stand-alone equivalent of “CSF220T-T”

**Table 30.** Threat Subscription Details

| Threat Subscription Abbreviations | Description |
|---|---|
| **T** | Threat (Security Intelligence and IPS) |
| **M or AMP*** | Malware defense |
| **C or URL*** | URL Filtering |
| **1Y** | **1-Year** Subscription |
| **3Y** | **3-Year** Subscription |
| **5Y** | **5-Year** Subscription |

* Note that Threat/IPS (T) License is a requirement for the use of Malware (M) or URL (C) license features.

**Table 31.** 200 Series Threat Defense Subscriptions

| Part Number | Description |
|---|---|
| **CSF220T-T / L-CSF220T-T=** | CSF 220 Threat Defense IPS License |
| **CSF220T-TM / L-CSF220T-TM=** | CSF 220 Threat Defense IPS & Malware Defense License |
| **CSF220T-TC / L-CSF220T-TC=** | CSF 220 Threat Defense IPS & URL Filtering License |
| **CSF220T-TMC / L-CSF220T-TMC=** | CSF 220 Threat Defense IPS, Malware & URL License |
| **L-CSF220T-AMP=** | Cisco Secure Firewall 220 Adv Malware Protection License |
| **L-CSF220T-URL=** | Cisco Secure Firewall 220 URL Filtering License |
| **CSF240PT-T / L-CSF240PT-T=** | Cisco Secure Firewall 240P Threat Defense License |
| **CSF240PT-TC/ L-CSF240PT-TC=** | Cisco Secure Firewall 240P Threat Defense and URL License |
| **CSF240PT-TM / L-CSF240PT-TM=** | Cisco Secure Firewall 240P Threat Defense, Malware License |
| **CSF240PT-TMC / L-CSF240PT-TMC=** | Cisco Secure Firewall 240P TD, Malware and URL License |
| **L-CS240PT-AMP=** | Cisco Secure Firewall 240P Adv Malware Protection License |
| **L-CSF240PT-URL=** | Cisco Secure Firewall 240P URL Filtering License |

© 2026 Cisco and/or its affiliates. All rights reserved.

**Table 32.** 200 Series ASA software license

| Part Number | Description |
|---|---|
| **CSF200-ENC-K9** | Cisco Firewall 200 Series ASA Strong Encryption (3DES/AES) |
| **CSF200-ASA-CAR** | Cisco Firewall 200 ASA Carrier License |
| **L-CSF200-ASA-BPU=** | Cisco Firewall 200 ASA Universal License |

**Table 33.** Cisco Secure Firewall 200 Series subscription part numbers for configurations with the Threat Defense image

| Part Number | Description |
|---|---|
| **L-CSF220-AMP-1Y / 3Y / 5Y** | Cisco Secure Firewall 220 Adv Malware Protec Lic 1YR Subs / 3YR Subs / 5YR Subs |
| **L-CSF220-T-1Y / 3Y / 5Y** | Cisco Secure Firewall 220 Threat Defense 1Y Subscription / 3Y Subscription / 5Y Subscription |
| **L-CSF220-TC-1Y / 3Y / 5Y** | Cisco Secure Firewall 220 TD and URL Lic 1Y Subscription / 3Y Subscription / 5Y Subscription |
| **L-CSF220-TM-1Y / 3Y / 5Y** | Cisco Secure Firewall 220 TD, Malware Lic 1Y Subscription / 3Y Subscription / 5Y Subscription |
| **L-CSF220-TMC-1Y / 3Y / 5Y** | Cisco Secure Firewall 220 TD, Malware & URL Lic 1YR Subs / 3YR Subs / 5YR Subs |
| **L-CSF220-URL-1Y / 3Y / 5Y** | Cisco Secure Firewall 220 URL Filtering License 1YR Subs / 3YR Subs / 5YR Subs |
| **L-CSF240PT-AMP-1Y / 3Y / 5Y** | Cisco Secure Firewall 240P Adv Malware Protec Lic 1YR Subs / 3YR Subs / 5YR Subs |
| **L-CSF240PT-T-1Y / 3Y / 5Y** | Cisco Secure Firewall 240P Threat Defense 1Y Subscription / 3Y Subscription / 5Y Subscription |
| **L-CSF240PT-TC-1Y / 3Y / 5Y** | Cisco Secure Firewall 240P TD and URL Lic 1Y Subscription / 3Y Subscription / 5Y Subscription |
| **L-CSF240PT-TM-1Y / 3Y / 5Y** | Cisco Secure Firewall 240P TD, Malware Lic 1Y Subscription / 3Y Subscription / 5Y Subscription |
| **L-CSF240PT-TMC-1Y / 3Y / 5Y** | Cisco Secure Firewall 240P TD, Malware & URL Lic 1YR Subs / 3YR Subs / 5YR Subs |
| **L-CSF240PT-URL-1Y / 3Y / 5Y** | Cisco Secure Firewall 240P URL Filtering License 1YR Subs / 3YR Subs / 5YR Subs |

© 2026 Cisco and/or its affiliates. All rights reserved.

### SKUs and Ordering for Cisco Secure Firewall 3100 Series

The following tables provide part numbers for the Cisco Secure Firewall 3100 Series.

**Table 34.** 3100 Series chassis part numbers

| Part Number<br>PID | Description |
|---|---|
| **Bundles** | |
| **FPR3100-FTD-HA-BUN** | Cisco Secure Firewall 3100 series Two Unit High Availability Bundle<br>(will order 2 identical chassis and software subscriptions to be configured as a high-availability pair) |
| **Appliances** | |
| **FPR3105-NGFW-K9** | Cisco Secure Firewall 3105 Appliance with Threat Defense software |
| **FPR3110-NGFW-K9** | Cisco Secure Firewall 3110 Appliance with Threat Defense software |
| **FPR3120-NGFW-K9** | Cisco Secure Firewall 3120 Appliance with Threat Defense software |
| **FPR3130-NGFW-K9** | Cisco Secure Firewall 3130 Appliance with Threat Defense software |
| **FPR3140-NGFW-K9** | Cisco Secure Firewall 3140 Appliance with Threat Defense software, 1RU,<br>1 x Network Module Bays (runs FTD software + optional subscriptions) |
| **FPR3105-ASA-K9** | Cisco Secure Firewall 3105 ASA Appliance, 1RU (runs ASA software with optional security context license) |
| **FPR3110-ASA-K9** | Cisco Secure Firewall 3110 ASA Appliance, 1RU (runs ASA software with optional security context license) |
| **FPR3120-ASA-K9** | Cisco Secure Firewall 3120 ASA Appliance, 1RU (runs ASA software with optional security context license) |
| **FPR3130-ASA-K9** | Cisco Secure Firewall 3130 ASA Appliance, 1RU, 1 x Network Module Bays<br>(runs ASA software with optional security context license) |
| **FPR3140-ASA-K9** | Cisco Secure Firewall 3140 ASA Appliance, 1RU, 1 x Network Module Bays<br>(runs ASA software with optional security context license) |
| **Network Modules** | |
| **FPR3K-XNM-8X10G** | 3100 Series 8-port 1G/10G SFP+ Network Module |
| **FPR3K-XNM-8X10G=** | 3100 Series 8-port 1G/10G SFP+ Network Module (Spare) |
| **FPR3K-XNM-8X25G** | 3100 Series 8-port 1/10/25G ZSFP Network Module |
| **FPR3K-XNM-8X25G=** | 3100 Series 8-port 1/10/25G ZSFP Network Module (Spare) |

© 2026 Cisco and/or its affiliates. All rights reserved.

| Part Number<br>PID | Description |
|---|---|
| **FPR3K-XNM-4X40G** | 3100 Series 4-port 40G QSFP+ Network Module |
| **FPR3K-XNM-4X40G=** | 3100 Series 4-port 40G QSFP+ Network Module (Spare) |
| **FPR3K-XNM-2X100G** | 3100 Series 2-port 100G QSFP28 Network Module |
| **FPR3K-XNM-2X100G=** | 3100 Series 2-port 100G QSFP28 Network Module (Spare) |

**Table 35.** 3100 Series ASA software license SKUs

| Part Number | Description |
|---|---|
| **Multi-context License for ASA** | |
| **L-FPR3K-ASASC-10=** | Cisco Secure Firewall 3100 Add-on 10 security context licenses |
| **L-FPR3K-ASASC-5=** | Cisco Secure Firewall 3100 add-on 5 security context licenses |
| **Encryption License** | |
| **L-FPR3K-ENC-K9=** | License to enable strong encryption for ASA on Cisco Secure Firewall 3100 Series |

**Table 36.** 3100 Series accessories

| Part Number | Description |
|---|---|
| **FPR3K-PWR-AC-400=** | Cisco Secure Firewall 3100 Series 400W AC Power Supply |
| **FPR3K-PWR-DC-400=** | Cisco Secure Firewall 3100 Series 400W DC Power Supply |
| **FPR3K-FAN=** | Cisco Secure Firewall 3100 Series Fan Tray |
| **FPR3K-PSU-BLANK=** | Cisco Secure Firewall 3100 Series Chassis Power Supply Blank Slot Cover |
| **FPR3K-SSD-BLANK=** | Cisco Secure Firewall 3100 Series SSD Slot Carrier |
| **FPR3K-NM-BLANK=** | Cisco Secure Firewall 3100 Series Network Module Blank Slot Cover |
| **FPR3K-SSD900=** | Cisco Secure Firewall 3100 Series SSD for FPR 3100 Series |
| **FPR3K-BRKT=** | Cisco Secure Firewall 3100 Series Rackmount Brackets |
| **FPR3K-RAIL-BRKT=** | Cisco Secure Firewall 3100 Series Slide Rail Brackets |
| **FPR3K-CBL-MGMT=** | Cisco Secure Firewall 3100 Series Cable Management Brackets |
| **FPR3K-FIPS-KIT=** | Cisco Secure Firewall 3100 Series FIPS Kit |
| **FPR3K-SLIDE-RAILS=** | Cisco Secure Firewall 3100 Series Slide Rail Kit |
| **FPR3K-ACY-KIT** | Cisco Secure Firewall 3100 Series Accessory Kit |

© 2026 Cisco and/or its affiliates. All rights reserved.

### SKUs for 3100 Series Licenses and Subscriptions

When ordering a 3100 Series with the Cisco Secure Firewall Threat Defense image, both licenses and a subscription to optional security services are required. Subscription terms are 1, 3, and 5 years, with the greatest price discount at 5 years. In the listed part numbers, the threat services are identified as follows:

**Table 37.** Threat Subscription Details

| Threat Subscription Abbreviations | Description |
|---|---|
| **T** | Threat (Security Intelligence and IPS) |
| **M or AMP*** | Malware defense |
| **C or URL*** | URL Filtering |
| **1Y** | **1-Year** Subscription |
| **3Y** | **3-Year** Subscription |
| **5Y** | **5-Year** Subscription |

*Note that Threat/IPS (T) License is a requirement for the use of Malware (M) or URL (C) license features.

**Table 38.** Cisco Secure Firewall 3100 Series license part numbers for configurations with the Cisco Secure Firewall Threat Defense image

| Part Number | Description |
|---|---|
| **L-FPR3105T-AMP=** | Cisco Secure Firewall 3105 Threat Defense Malware Protection License |
| **L-FPR3105T-T=** | Cisco Secure Firewall 3105 Threat Defense Threat Protection License |
| **L-FPR3105T-TC=** | Cisco Secure Firewall 3105 Threat Defense Threat and URL License |
| **L-FPR3105T-TM=** | Cisco Secure Firewall 3105 Threat Defense Threat and Malware License |
| **L-FPR3105T-TMC=** | Cisco Secure Firewall 3105 Threat Defense Threat, Malware, and URL License |
| **L-FPR3105T-URL=** | Cisco Secure Firewall 3105 Threat Defense URL Filtering License |
| **L-FPR3110T-AMP=** | Cisco Secure Firewall 3110 Threat Defense Malware Protection License |
| **L-FPR3110T-T=** | Cisco Secure Firewall 3110 Threat Defense Threat Protection License |
| **L-FPR3110T-TC=** | Cisco Secure Firewall 3110 Threat Defense Threat and URL License |
| **L-FPR3110T-TM=** | Cisco Secure Firewall 3110 Threat Defense Threat and Malware License |
| **L-FPR3110T-TMC=** | Cisco Secure Firewall 3110 Threat Defense Threat, Malware, and URL License |
| **L-FPR3110T-URL=** | Cisco Secure Firewall 3110 Threat Defense URL Filtering License |
| **L-FPR3120T-AMP=** | Cisco Secure Firewall 3120 Threat Defense Malware Protection License |
| **L-FPR3120T-T=** | Cisco Secure Firewall 3120 Threat Defense Threat Protection License |

© 2026 Cisco and/or its affiliates. All rights reserved.

| Part Number | Description |
|---|---|
| **L-FPR3120T-TC=** | Cisco Secure Firewall 3120 Threat Defense Threat and URL License |
| **L-FPR3120T-TM=** | Cisco Secure Firewall 3120 Threat Defense Threat and Malware License |
| **L-FPR3120T-TMC=** | Cisco Secure Firewall 3120 Threat Defense Threat, Malware, and URL License |
| **L-FPR3120T-URL=** | Cisco Secure Firewall 3120 Threat Defense URL Filtering License |
| **L-FPR3130T-AMP=** | Cisco Secure Firewall 3130 Threat Defense Malware Protection License |
| **L-FPR3130T-T=** | Cisco Secure Firewall 3130 Threat Defense Threat Protection License |
| **L-FPR3130T-TC=** | Cisco Secure Firewall 3130 Threat Defense Threat and URL License |
| **L-FPR3130T-TM=** | Cisco Secure Firewall 3130 Threat Defense Threat and Malware License |
| **L-FPR3130T-TMC=** | Cisco Secure Firewall 3130 Threat Defense Threat, Malware, and URL License |
| **L-FPR3130T-URL=** | Cisco Secure Firewall 3130 Threat Defense URL Filtering License |
| **L-FPR3140T-AMP=** | Cisco Secure Firewall 3140 Threat Defense Malware Protection License |
| **L-FPR3140T-T=** | Cisco Secure Firewall 3140 Threat Defense Threat Protection License |
| **L-FPR3140T-TC=** | Cisco Secure Firewall 3140 Threat Defense Threat and URL License |
| **L-FPR3140T-TM=** | Cisco Secure Firewall 3140 Threat Defense Threat and Malware License |
| **L-FPR3140T-TMC=** | Cisco Secure Firewall 3140 Threat Defense Threat, Malware, and URL License |
| **L-FPR3140T-URL=** | Cisco Secure Firewall 3140 Threat Defense URL Filtering License |

**Table 39.** Cisco Secure Firewall 3100 Series subscription part numbers for configurations with the Firewall Threat Defense image

| Part Number | Description |
|---|---|
| **L-FPR3105T-AMP-1Y** | Cisco Secure Firewall 3105 Threat Defense Malware Protection 1Y Subscription |
| **L-FPR3105T-AMP-3Y** | Cisco Secure Firewall 3105 Threat Defense Malware Protection 3Y Subscription |
| **L-FPR3105T-AMP-5Y** | Cisco Secure Firewall 3105 Threat Defense Malware Protection 5Y Subscription |
| **L-FPR3105T-T-1Y** | Cisco Secure Firewall 3105 Threat Defense Threat Protection 1Y Subscription |
| **L-FPR3105T-T-3Y** | Cisco Secure Firewall 3105 Threat Defense Threat Protection 3Y Subscription |
| **L-FPR3105T-T-5Y** | Cisco Secure Firewall 3105 Threat Defense Threat Protection 5Y Subscription |
| **L-FPR3105T-TC-1Y** | Cisco Secure Firewall 3105 Threat Defense Threat and URL 1Y Subscription |
| **L-FPR3105T-TC-3Y** | Cisco Secure Firewall 3105 Threat Defense Threat and URL 3Y Subscription |
| **L-FPR3105T-TC-5Y** | Cisco Secure Firewall 3105 Threat Defense Threat and URL 5Y Subscription |

© 2026 Cisco and/or its affiliates. All rights reserved.

| Part Number | Description |
|---|---|
| **L-FPR3105T-TM-1Y** | Cisco Secure Firewall 3105 Threat Defense Threat and Malware 1Y Subscription |
| **L-FPR3105T-TM-3Y** | Cisco Secure Firewall 3105 Threat Defense Threat and Malware 3Y Subscription |
| **L-FPR3105T-TM-5Y** | Cisco Secure Firewall 3105 Threat Defense Threat and Malware 5Y Subscription |
| **L-FPR3105T-TMC-1Y** | Cisco Secure Firewall 3105 Threat Defense Threat, Malware, and URL 1Y Subscription |
| **L-FPR3105T-TMC-3Y** | Cisco Secure Firewall 3105 Threat Defense Threat, Malware, and URL 3Y Subscription |
| **L-FPR3105T-TMC-5Y** | Cisco Secure Firewall 3105 Threat Defense Threat, Malware, and URL 5Y Subscription |
| **L-FPR3105T-URL-1Y** | Cisco Secure Firewall 3105 Threat Defense URL Filtering 1Y Subscription |
| **L-FPR3105T-URL-3Y** | Cisco Secure Firewall 3105 Threat Defense URL Filtering 3Y Subscription |
| **L-FPR3105T-URL-5Y** | Cisco Secure Firewall 3105 Threat Defense URL Filtering 5Y Subscription |
| **L-FPR3110T-AMP-1Y** | Cisco Secure Firewall 3110 Threat Defense Malware Protection 1Y Subscription |
| **L-FPR3110T-AMP-3Y** | Cisco Secure Firewall 3110 Threat Defense Malware Protection 3Y Subscription |
| **L-FPR3110T-AMP-5Y** | Cisco Secure Firewall 3110 Threat Defense Malware Protection 5Y Subscription |
| **L-FPR3110T-T-1Y** | Cisco Secure Firewall 3110 Threat Defense Threat Protection 1Y Subscription |
| **L-FPR3110T-T-3Y** | Cisco Secure Firewall 3110 Threat Defense Threat Protection 3Y Subscription |
| **L-FPR3110T-T-5Y** | Cisco Secure Firewall 3110 Threat Defense Threat Protection 5Y Subscription |
| **L-FPR3110T-TC-1Y** | Cisco Secure Firewall 3110 Threat Defense Threat and URL 1Y Subscription |
| **L-FPR3110T-TC-3Y** | Cisco Secure Firewall 3110 Threat Defense Threat and URL 3Y Subscription |
| **L-FPR3110T-TC-5Y** | Cisco Secure Firewall 3110 Threat Defense Threat and URL 5Y Subscription |
| **L-FPR3110T-TM-1Y** | Cisco Secure Firewall 3110 Threat Defense Threat and Malware 1Y Subscription |
| **L-FPR3110T-TM-3Y** | Cisco Secure Firewall 3110 Threat Defense Threat and Malware 3Y Subscription |
| **L-FPR3110T-TM-5Y** | Cisco Secure Firewall 3110 Threat Defense Threat and Malware 5Y Subscription |
| **L-FPR3110T-TMC-1Y** | Cisco Secure Firewall 3110 Threat Defense Threat, Malware, and URL 1Y Subscription |
| **L-FPR3110T-TMC-3Y** | Cisco Secure Firewall 3110 Threat Defense Threat, Malware, and URL 3Y Subscription |
| **L-FPR3110T-TMC-5Y** | Cisco Secure Firewall 3110 Threat Defense Threat, Malware, and URL 5Y Subscription |
| **L-FPR3110T-URL-1Y** | Cisco Secure Firewall 3110 Threat Defense URL Filtering 1Y Subscription |
| **L-FPR3110T-URL-3Y** | Cisco Secure Firewall 3110 Threat Defense URL Filtering 3Y Subscription |
| **L-FPR3110T-URL-5Y** | Cisco Secure Firewall 3110 Threat Defense URL Filtering 5Y Subscription |

© 2026 Cisco and/or its affiliates. All rights reserved.

| Part Number | Description |
|---|---|
| **L-FPR3120T-AMP-1Y** | Cisco Secure Firewall 3120 Threat Defense Malware Protection 1Y Subscription |
| **L-FPR3120T-AMP-3Y** | Cisco Secure Firewall 3120 Threat Defense Malware Protection 3Y Subscription |
| **L-FPR3120T-AMP-5Y** | Cisco Secure Firewall 3120 Threat Defense Malware Protection 5Y Subscription |
| **L-FPR3120T-T-1Y** | Cisco Secure Firewall 3120 Threat Defense Threat Protection 1Y Subscription |
| **L-FPR3120T-T-3Y** | Cisco Secure Firewall 3120 Threat Defense Threat Protection 3Y Subscription |
| **L-FPR3120T-T-5Y** | Cisco Secure Firewall 3120 Threat Defense Threat Protection 5Y Subscription |
| **L-FPR3120T-TC-1Y** | Cisco Secure Firewall 3120 Threat Defense Threat and URL 1Y Subscription |
| **L-FPR3120T-TC-3Y** | Cisco Secure Firewall 3120 Threat Defense Threat and URL 3Y Subscription |
| **L-FPR3120T-TC-5Y** | Cisco Secure Firewall 3120 Threat Defense Threat and URL 5Y Subscription |
| **L-FPR3120T-TM-1Y** | Cisco Secure Firewall 3120 Threat Defense Threat and Malware 1Y Subscription |
| **L-FPR3120T-TM-3Y** | Cisco Secure Firewall 3120 Threat Defense Threat and Malware 3Y Subscription |
| **L-FPR3120T-TM-5Y** | Cisco Secure Firewall 3120 Threat Defense Threat and Malware 5Y Subscription |
| **L-FPR3120T-TMC-1Y** | Cisco Secure Firewall 3120 Threat Defense Threat, Malware, and URL 1Y Subscription |
| **L-FPR3120T-TMC-3Y** | Cisco Secure Firewall 3120 Threat Defense Threat, Malware, and URL 3Y Subscription |
| **L-FPR3120T-TMC-5Y** | Cisco Secure Firewall 3120 Threat Defense Threat, Malware, and URL 5Y Subscription |
| **L-FPR3120T-URL-1Y** | Cisco Secure Firewall 3120 Threat Defense URL Filtering 1Y Subscription |
| **L-FPR3120T-URL-3Y** | Cisco Secure Firewall 3120 Threat Defense URL Filtering 3Y Subscription |
| **L-FPR3120T-URL-5Y** | Cisco Secure Firewall 3120 Threat Defense URL Filtering 5Y Subscription |
| **L-FPR3130T-AMP-1Y** | Cisco Secure Firewall 3130 Threat Defense Malware Protection 1Y Subscription |
| **L-FPR3130T-AMP-3Y** | Cisco Secure Firewall 3130 Threat Defense Malware Protection 3Y Subscription |
| **L-FPR3130T-AMP-5Y** | Cisco Secure Firewall 3130 Threat Defense Malware Protection 5Y Subscription |
| **L-FPR3130T-T-1Y** | Cisco Secure Firewall 3130 Threat Defense Threat Protection 1Y Subscription |
| **L-FPR3130T-T-3Y** | Cisco Secure Firewall 3130 Threat Defense Threat Protection 3Y Subscription |
| **L-FPR3130T-T-5Y** | Cisco Secure Firewall 3130 Threat Defense Threat Protection 5Y Subscription |
| **L-FPR3130T-TC-1Y** | Cisco Secure Firewall 3130 Threat Defense Threat and URL 1Y Subscription |
| **L-FPR3130T-TC-3Y** | Cisco Secure Firewall 3130 Threat Defense Threat and URL 3Y Subscription |
| **L-FPR3130T-TC-5Y** | Cisco Secure Firewall 3130 Threat Defense Threat and URL 5Y Subscription |

© 2026 Cisco and/or its affiliates. All rights reserved.

| Part Number | Description |
|---|---|
| **L-FPR3130T-TM-1Y** | Cisco Secure Firewall 3130 Threat Defense Threat and Malware 1Y Subscription |
| **L-FPR3130T-TM-3Y** | Cisco Secure Firewall 3130 Threat Defense Threat and Malware 3Y Subscription |
| **L-FPR3130T-TM-5Y** | Cisco Secure Firewall 3130 Threat Defense Threat and Malware 5Y Subscription |
| **L-FPR3130T-TMC-1Y** | Cisco Secure Firewall 3130 Threat Defense Threat, Malware, and URL 1Y Subscription |
| **L-FPR3130T-TMC-3Y** | Cisco Secure Firewall 3130 Threat Defense Threat, Malware, and URL 3Y Subscription |
| **L-FPR3130T-TMC-5Y** | Cisco Secure Firewall 3130 Threat Defense Threat, Malware, and URL 5Y Subscription |
| **L-FPR3130T-URL-1Y** | Cisco Secure Firewall 3130 Threat Defense URL Filtering 1Y Subscription |
| **L-FPR3130T-URL-3Y** | Cisco Secure Firewall 3130 Threat Defense URL Filtering 3Y Subscription |
| **L-FPR3130T-URL-5Y** | Cisco Secure Firewall 3130 Threat Defense URL Filtering 5Y Subscription |
| **L-FPR3140T-AMP-1Y** | Cisco Secure Firewall 3140 Threat Defense Malware Protection 1Y Subscription |
| **L-FPR3140T-AMP-3Y** | Cisco Secure Firewall 3140 Threat Defense Malware Protection 3Y Subscription |
| **L-FPR3140T-AMP-5Y** | Cisco Secure Firewall 3140 Threat Defense Malware Protection 5Y Subscription |
| **L-FPR3140T-T-1Y** | Cisco Secure Firewall 3140 Threat Defense Threat Protection 1Y Subscription |
| **L-FPR3140T-T-3Y** | Cisco Secure Firewall 3140 Threat Defense Threat Protection 3Y Subscription |
| **L-FPR3140T-T-5Y** | Cisco Secure Firewall 3140 Threat Defense Threat Protection 5Y Subscription |
| **L-FPR3140T-TC-1Y** | Cisco Secure Firewall 3140 Threat Defense Threat and URL 1Y Subscription |
| **L-FPR3140T-TC-3Y** | Cisco Secure Firewall 3140 Threat Defense Threat and URL 3Y Subscription |
| **L-FPR3140T-TC-5Y** | Cisco Secure Firewall 3140 Threat Defense Threat and URL 5Y Subscription |
| **L-FPR3140T-TM-1Y** | Cisco Secure Firewall 3140 Threat Defense Threat and Malware 1Y Subscription |
| **L-FPR3140T-TM-3Y** | Cisco Secure Firewall 3140 Threat Defense Threat and Malware 3Y Subscription |
| **L-FPR3140T-TM-5Y** | Cisco Secure Firewall 3140 Threat Defense Threat and Malware 5Y Subscription |
| **L-FPR3140T-TMC-1Y** | Cisco Secure Firewall 3140 Threat Defense Threat, Malware, and URL 1Y Subscription |
| **L-FPR3140T-TMC-3Y** | Cisco Secure Firewall 3140 Threat Defense Threat, Malware, and URL 3Y Subscription |
| **L-FPR3140T-TMC-5Y** | Cisco Secure Firewall 3140 Threat Defense Threat, Malware, and URL 5Y Subscription |
| **L-FPR3140T-URL-1Y** | Cisco Secure Firewall 3140 Threat Defense URL Filtering 1Y Subscription |
| **L-FPR3140T-URL-3Y** | Cisco Secure Firewall 3140 Threat Defense URL Filtering 3Y Subscription |
| **L-FPR3140T-URL-5Y** | Cisco Secure Firewall 3140 Threat Defense URL Filtering 5Y Subscription |

© 2026 Cisco and/or its affiliates. All rights reserved.

**Ordering Example: Cisco Secure Firewall 3140 with FTD**

**Step 1:** Smart Software Licensing

Before placing a Cisco Secure Firewall 3100 order, a Smart Software Licensing account for the end customer must be initiated. If the customer already has a Smart Software Licensing account, that account must be associated with the order. More information on Smart Software Licensing account establishment is available in the Smart Software Licensing section of this ordering guide, and online at: https://www.cisco.com/web/ordering/smart-software-manager/index.html.

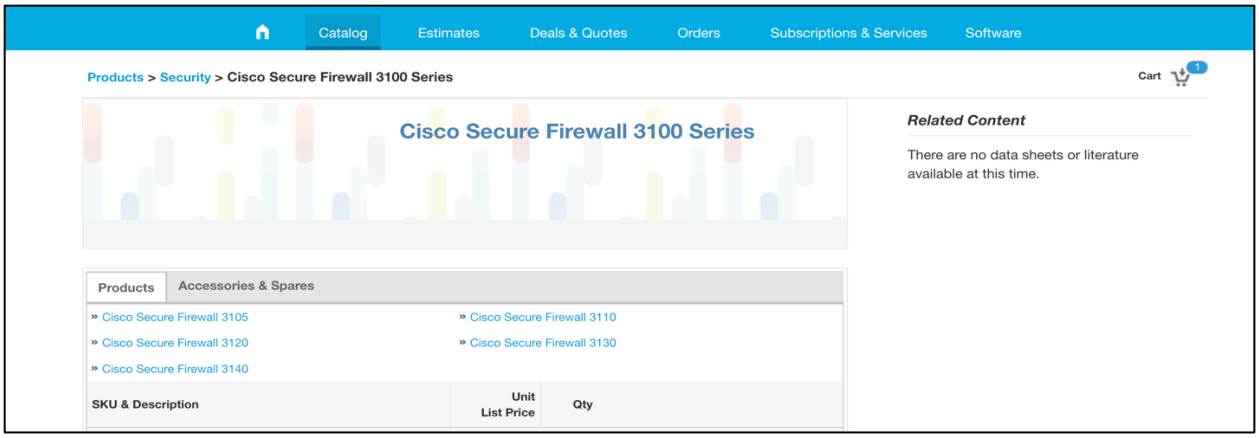
To associate the order's licenses with the customer's Smart Licensing account, or to begin the establishment of the Smart Licensing account, follow these steps. Note that if you are initiating the account, you can complete the order only if the account is initiated on the end customer's behalf and associated with the order.

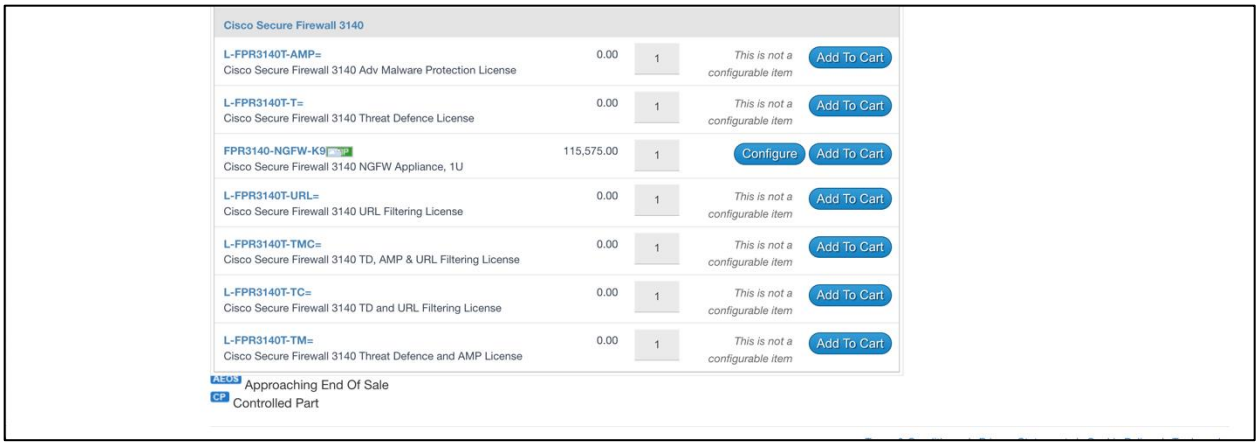
Go to Cisco Commerce: https://www.cisco.com/go/ccw.

From the Orders pull-down menu, select Create Order.

Select Assign Smart Account and follow the subsequent prompts for Smart Licensing.

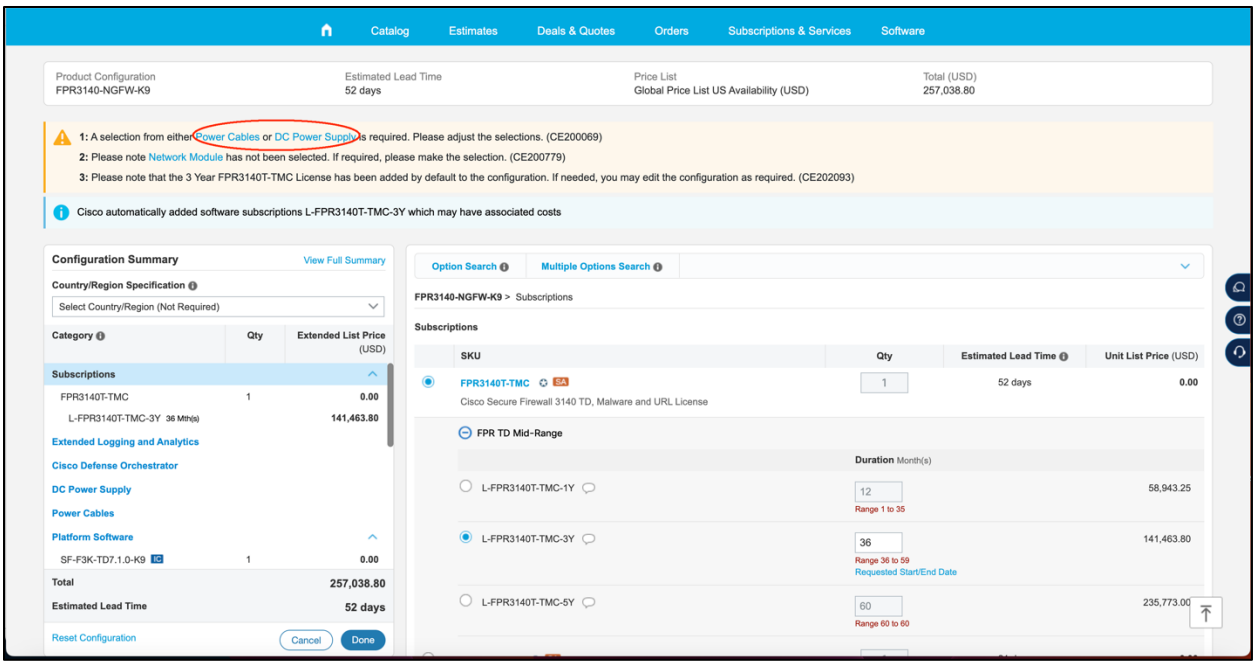
**Step 2:** Navigate to Products -> Security -> Cisco Secure Firewall 3100 series-> Cisco Secure Firewall 3140 -> FPR3140-NGFW-K9

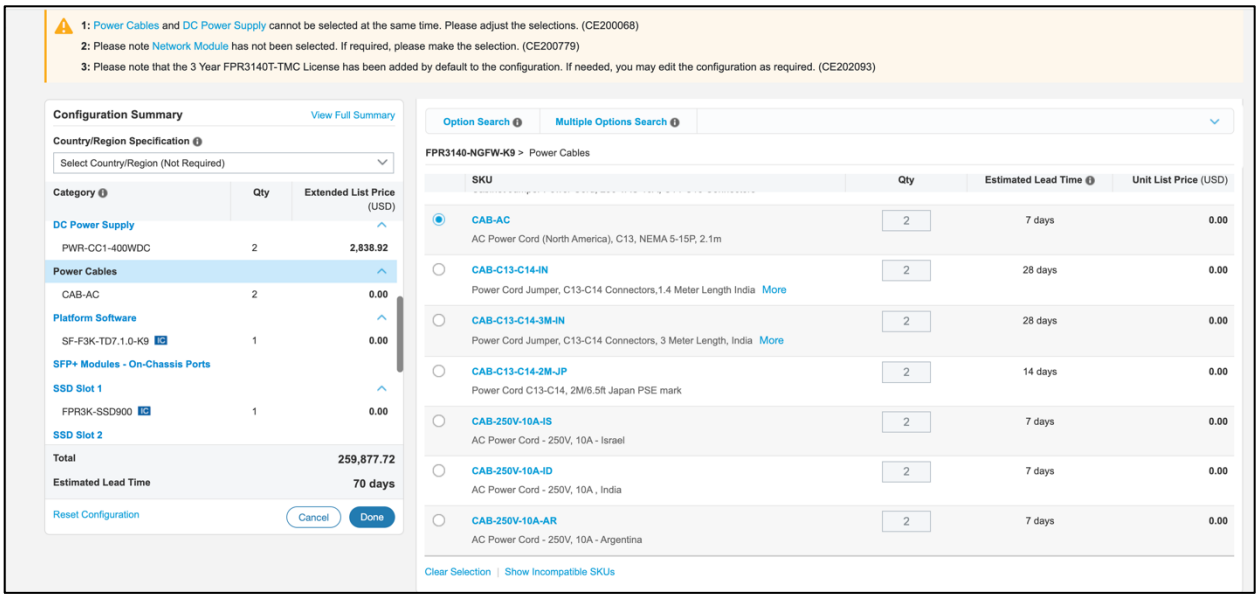



© 2026 Cisco and/or its affiliates. All rights reserved.

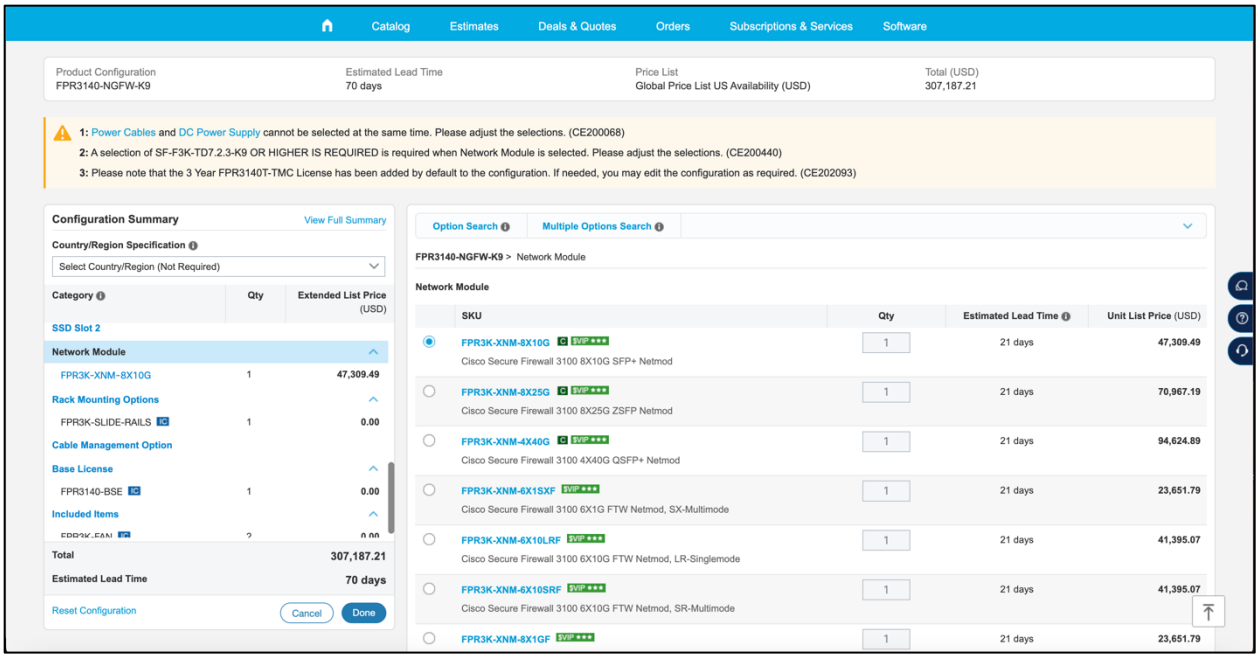
**Step 3:** Follow the instructions on the yellow box. Select the Power Cables or the DC Power Supply.



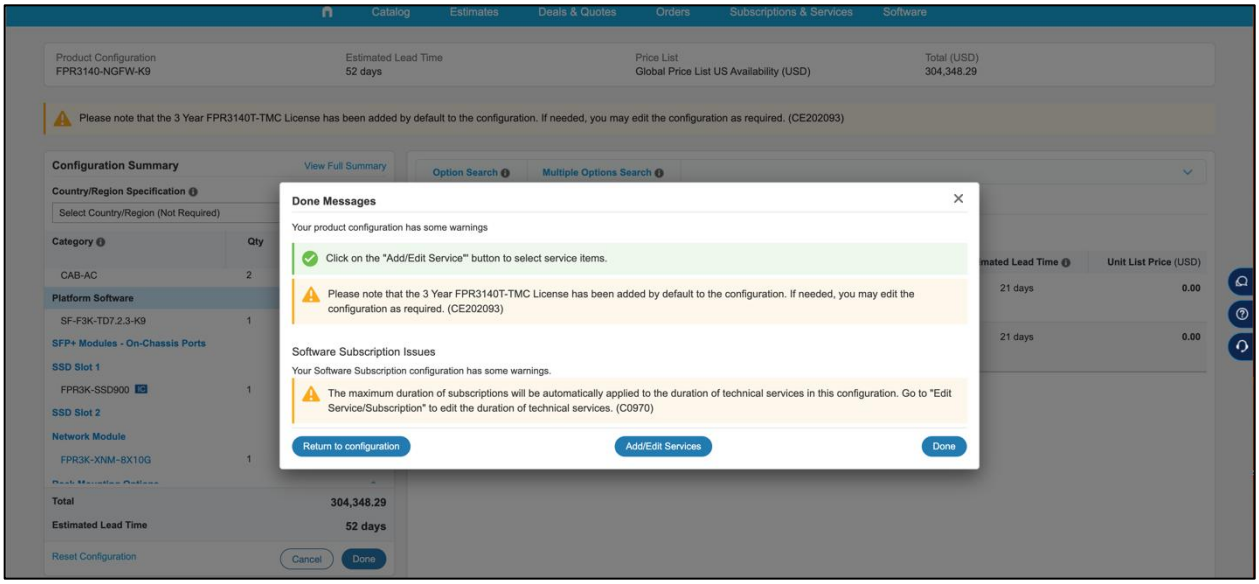




© 2026 Cisco and/or its affiliates. All rights reserved.

**Step 4:** After the cable selection is complete. Click on the Network module to add to the configuration.

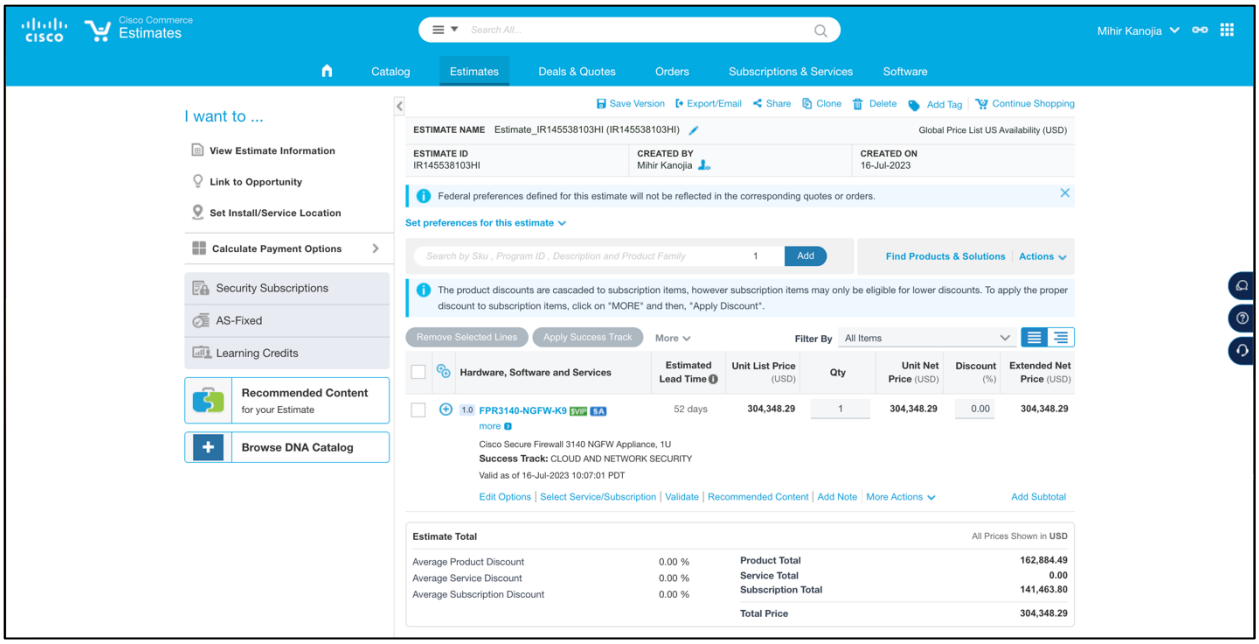



**Step 5:** Complete the configuration by clicking on done. An alert message appears for the user to confirm the selection.




© 2026 Cisco and/or its affiliates. All rights reserved.

**Step 6:** Product summary page appears with the selected configurations.




### SKUs and Ordering for Cisco Firepower 4100 Series

The following tables outline the product part number information for the Cisco Firepower 4100 Series. Note that the customer may want extra power supplies and fans.

**Table 40.** 4100 Series chassis part numbers

| Part Number | Description |
|---|---|
| **FPR4112-BUN** | Cisco Firepower 4112 Master Bundle |
| **FPR4115-BUN** | Cisco Firepower 4115 Master Bundle |
| **FPR4125-BUN** | Cisco Firepower 4125 Master Bundle |
| **FPR4145-BUN** | Cisco Firepower 4145 Master Bundle |
| **FPR4112-FTD-HA-BUN** | Cisco Firepower 4112 Two Unit High Availability Bundle (will order 2 identical chassis and software subscriptions to be configured as a high-availability pair) |
| **FPR4115-FTD-HA-BUN** | Cisco Firepower 4115 Two Unit High Availability Bundle (will order 2 identical chassis and software subscriptions to be configured as a high-availability pair) |
| **FPR4125-FTD-HA-BUN** | Cisco Firepower 4125 Two Unit High Availability Bundle (will order 2 identical chassis and software subscriptions to be configured as a high-availability pair) |
| **FPR4145-FTD-HA-BUN** | Cisco Firepower 4145 Two Unit High Availability Bundle (will order 2 identical chassis and software subscriptions to be configured as a high-availability pair) |
| **FPR4112-ASA-K9** | Cisco Firepower 4112 ASA Appliance, 1RU, 2 x Network Module Bays |
| **FPR4112-NGFW-K9** | Cisco Firepower 4112 NGFW Appliance, 1RU, 2 x Network Module Bays |
| **FPR4112-NGIPS-K9** | Cisco Firepower 4112 NGIPS Appliance, 1RU, 2 x Network Module Bays |

© 2026 Cisco and/or its affiliates. All rights reserved.

| Part Number | Description |
|---|---|
| **FPR4115-ASA-K9** | Cisco Firepower 4115 ASA Appliance, 1RU, 2 x Network Module Bays |
| **FPR4115-NGFW-K9** | Cisco Firepower 4115 NGFW Appliance, 1RU, 2 x Network Module Bays |
| **FPR4115-NGIPS-K9** | Cisco Firepower 4115 NGIPS Appliance, 1RU, 2 x Network Module Bays |
| **FPR4125-ASA-K9** | Cisco Firepower 4125 ASA Appliance, 1RU, 2 x Network Module Bays |
| **FPR4125-NGFW-K9** | Cisco Firepower 4125 NGFW Appliance, 1RU, 2 x Network Module Bays |
| **FPR4125-NGIPS-K9** | Cisco Firepower 4125 NGIPS Appliance, 1RU, 2 x Network Module Bays |
| **FPR4145-ASA-K9** | Cisco Firepower 4145 ASA Appliance, 1RU, 2 x Network Module Bays |
| **FPR4145-NGFW-K9** | Cisco Firepower 4145 NGFW Appliance, 1RU, 2 x Network Module Bays |
| **FPR4145-NGIPS-K9** | Cisco Firepower 4145 NGIPS Appliance, 1RU, 2 x Network Module Bays |

**Note:** Use the bundle part number unless you have an explicit reason not to. the bundle PID ensures that all necessary components are purchased.

**Table 41.** 4100 Series network module part numbers

| Part Number | Description |
|---|---|
| **FPR4K-NM-2X40G-F** | Cisco Firepower 2-port 40G SR FTW Network Module |
| **FPR4K-NM-2X40G-F=** | Cisco Firepower 2-port 40G SR FTW Network Module |
| **FPR4K-NM-4X40G** | Cisco Firepower 4-port QSFP+ Network Module |
| **FPR4K-NM-4X40G=** | Cisco Firepower 4-port QSFP+ Network Module |
| **FPR4K-NM-6X10LR-F** | Cisco Firepower 6-port 10G LR FTW Network Module |
| **FPR4K-NM-6X10LR-F=** | Cisco Firepower 6-port 10G LR FTW Network Module |
| **FPR4K-NM-6X10SR-F** | Cisco Firepower 6-port 10G SR FTW Network Module |
| **FPR4K-NM-6X10SR-F=** | Cisco Firepower 6-port 10G SR FTW Network Module |
| **FPR4K-NM-6X1SX-F** | Cisco Firepower 6-port 1G SX Fiber FTW Network Module |
| **FPR4K-NM-6X1SX-F=** | Cisco Firepower 6-port 1G SX Fiber FTW Network Module |
| **FPR4K-NM-8X10G** | Cisco Firepower 8-port SFP+ Network Module |
| **FPR4K-NM-8X10G=** | Cisco Firepower 8-port SFP+ Network Module |
| **FPR4K-NM-8X1G-F** | Cisco Firepower 8-port 1Gbps copper FTW Network Module |
| **FPR4K-NM-8X1G-F=** | Cisco Firepower 8-port 1Gbps copper FTW Network Module |
| **FPR4K-NM-2X100G=** | Cisco FirePower 2 port 100G Network Module |

© 2026 Cisco and/or its affiliates. All rights reserved.

**Table 42.** 4100 Series accessories part numbers

| Part Number | Description |
|---|---|
| **FPR4K-FAN** | Cisco Firepower 4000 Series Fan |
| **FPR4K-FAN=** | Cisco Firepower 4000 Series Fan |
| **FPR4K-NM-BLANK** | Cisco Firepower 4000 Series Network Module Blank Slot Cover |
| **FPR4K-NM-BLANK=** | Cisco Firepower 4000 Series Network Module Blank Slot Cover |
| **FPR4K-PSU-BLANK** | Cisco Firepower 4000 Series Chassis Power Supply Blank Slot Cover |
| **FPR4K-PSU-BLANK=** | Cisco Firepower 4000 Series Chassis Power Supply Blank Slot Cover |
| **FPR4K-PWR-AC-1100** | Cisco Firepower 4000 Series 1100W AC Power Supply |
| **FPR4K-PWR-AC-1100=** | Cisco Firepower 4000 Series 1100W AC Power Supply |
| **FPR4K-PWR-DC-950** | Cisco Firepower 4000 Series 950W DC Power Supply |
| **FPR4K-PWR-DC-950=** | Cisco Firepower 4000 Series 950W DC Power Supply |
| **FPR4K-RACK-MNT** | Cisco Firepower 4000 Series Rack Mount Kit |
| **FPR4K-RACK-MNT=** | Cisco Firepower 4000 Series Rack Mount Kit |
| **FPR4K-SSD-BBLKD** | Cisco Firepower 4000 Series SSD Slot Carrier |
| **FPR4K-SSD-BBLKD=** | Cisco Firepower 4000 Series SSD Slot Carrier |
| **FPR4K-SSD200** | Cisco Firepower 4000 Series SSD for 4110 and 4120 |
| **FPR4K-SSD200=** | Cisco Firepower 4000 Series SSD for 4110 and 4120 |
| **FPR4K-SSD400** | Cisco Firepower 4000 Series SSD for 4140 and 4150 |
| **FPR4K-SSD400=** | Cisco Firepower 4000 Series SSD for 4140 and 4150 |
| **FPR4K-SSD800** | Cisco Firepower 4000 Series 800GB SSD |
| **FPR4K-SSD800=** | Cisco Firepower 4000 Series 800GB SSD |
| **FPR4K-ACC-KIT** | Cisco Firepower 4000 Series Hardware Accessory Kit (Rack Mounts, Cables) |
| **FPR4K-ACC-KIT=** | Cisco Firepower 4000 Series Hardware Accessory Kit (Rack Mounts, Cables) |
| **FPR4K-ACC-KIT2** | Cisco Firepower 4115/25/45 Hardware Accessory Kit |
| **FPR4K-ACC-KIT2=** | Cisco Firepower 4115/25/45 Hardware Accessory Kit |
| **FPR4K-CBL-MGMT** | Cisco Firepower 4100 Series Cable Management Kit |
| **FPR4K-CBL-MGMT=** | Cisco Firepower 4100 Series Cable Management Kit |

**Note:** Use these part numbers if the customer is ordering spare fans, power supplies, or a rack mount kit.

© 2026 Cisco and/or its affiliates. All rights reserved.

**SKUs for 4100 Series Licenses and Subscriptions**

When ordering a 4100 Series firewall with the ASA configuration, a license is required. When ordering a 4100 Series hardware with the Cisco Secure Firewall Threat Defense image, both licenses and a subscription to optional security services are required. Subscription terms are 1, 3, and 5 years, with the greatest price discount at 5 years. In the listed part numbers, the threat services are identified as follows:

**Table 43.** Threat Subscription Details

| Threat Subscription Abbreviations | Description |
|---|---|
| **T** | Threat (Security Intelligence and IPS) |
| **M or AMP*** | Malware defense |
| **C or URL*** | URL Filtering |
| **1Y** | **1-Year** Subscription |
| **3Y** | **3-Year** Subscription |
| **5Y** | **5-Year** Subscription |

*Note that Threat/IPS (T) License is a requirement for the use of Malware (M) or URL (C) license features.

**Table 44.** Cisco Firepower 4100 Series license part numbers for configurations with the Cisco Secure Firewall Threat Defense image

| Part Number | Description |
|---|---|
| **L-FPR4112T-AMP=** | Cisco Firepower 4112 Threat Defense Malware Protection License |
| **L-FPR4112T-T=** | Cisco Firepower 4112 Threat Defense Threat Protection License |
| **L-FPR4112T-TC=** | Cisco Firepower 4112 Threat Defense Threat and URL License |
| **L-FPR4112T-TM=** | Cisco Firepower 4112 Threat Defense Threat and Malware License |
| **L-FPR4112T-TMC=** | Cisco Firepower 4112 Threat Defense Threat, Malware, and URL License |
| **L-FPR4112T-URL=** | Cisco Firepower 4112 Threat Defense URL Filtering License |
| **L-FPR4115T-AMP=** | Cisco Firepower 4115 Threat Defense Malware Protection License |
| **L-FPR4115T-T=** | Cisco Firepower 4115 Threat Defense Threat Protection License |
| **L-FPR4115T-TC=** | Cisco Firepower 4115 Threat Defense Threat and URL License |
| **L-FPR4115T-TM=** | Cisco Firepower 4115 Threat Defense Threat and Malware License |
| **L-FPR4115T-TMC=** | Cisco Firepower 4115 Threat Defense Threat, Malware, and URL License |
| **L-FPR4115T-URL=** | Cisco Firepower 4115 Threat Defense URL Filtering License |
| **L-FPR4125T-AMP=** | Cisco Firepower 4125 Threat Defense Malware Protection License |

© 2026 Cisco and/or its affiliates. All rights reserved.

| Part Number | Description |
|---|---|
| **L-FPR4125T-T=** | Cisco Firepower 4125 Threat Defense Threat Protection License |
| **L-FPR4125T-TC=** | Cisco Firepower 4125 Threat Defense Threat and URL License |
| **L-FPR4125T-TM=** | Cisco Firepower 4125 Threat Defense Threat and Malware License |
| **L-FPR4125T-TMC=** | Cisco Firepower 4125 Threat Defense Threat, Malware, and URL License |
| **L-FPR4125T-URL=** | Cisco Firepower 4125 Threat Defense URL Filtering License |
| **L-FPR4145T-AMP=** | Cisco Firepower 4145 Threat Defense Malware Protection License |
| **L-FPR4145T-T=** | Cisco Firepower 4145 Threat Defense Threat Protection License |
| **L-FPR4145T-TC=** | Cisco Firepower 4145 Threat Defense Threat and URL License |
| **L-FPR4145T-TM=** | Cisco Firepower 4145 Threat Defense Threat and Malware License |
| **L-FPR4145T-TMC=** | Cisco Firepower 4145 Threat Defense Threat, Malware, and URL License |
| **L-FPR4145T-URL=** | Cisco Firepower 4145 Threat Defense URL Filtering License |

**Table 45.** Cisco Firepower 4100 Series subscription part numbers for configurations with the Firewall Threat Defense image

| Part Number | Description |
|---|---|
| **L-FPR4112T-AMP-1Y** | Cisco Firepower 4112 Threat Defense Malware Protection 1Y Subscription |
| **L-FPR4112T-AMP-3Y** | Cisco Firepower 4112 Threat Defense Malware Protection 3Y Subscription |
| **L-FPR4112T-AMP-5Y** | Cisco Firepower 4112 Threat Defense Malware Protection 5Y Subscription |
| **L-FPR4112T-T-1Y** | Cisco Firepower 4112 Threat Defense Threat Protection 1Y Subscription |
| **L-FPR4112T-T-3Y** | Cisco Firepower 4112 Threat Defense Threat Protection 3Y Subscription |
| **L-FPR4112T-T-5Y** | Cisco Firepower 4112 Threat Defense Threat Protection 5Y Subscription |
| **L-FPR4112T-TC-1Y** | Cisco Firepower 4112 Threat Defense Threat and URL 1Y Subscription |
| **L-FPR4112T-TC-3Y** | Cisco Firepower 4112 Threat Defense Threat and URL 3Y Subscription |
| **L-FPR4112T-TC-5Y** | Cisco Firepower 4112 Threat Defense Threat and URL 5Y Subscription |
| **L-FPR4112T-TM-1Y** | Cisco Firepower 4112 Threat Defense Threat and Malware 1Y Subscription |
| **L-FPR4112T-TM-3Y** | Cisco Firepower 4112 Threat Defense Threat and Malware 3Y Subscription |
| **L-FPR4112T-TM-5Y** | Cisco Firepower 4112 Threat Defense Threat and Malware 5Y Subscription |
| **L-FPR4112T-TMC-1Y** | Cisco Firepower 4112 Threat Defense Threat, Malware, and URL 1Y Subscription |
| **L-FPR4112T-TMC-3Y** | Cisco Firepower 4112 Threat Defense Threat, Malware, and URL 3Y Subscription |

© 2026 Cisco and/or its affiliates. All rights reserved.

| Part Number | Description |
|---|---|
| **L-FPR4112T-TMC-5Y** | Cisco Firepower 4112 Threat Defense Threat, Malware, and URL 5Y Subscription |
| **L-FPR4112T-URL-1Y** | Cisco Firepower 4112 Threat Defense URL Filtering 1Y Subscription |
| **L-FPR4112T-URL-3Y** | Cisco Firepower 4112 Threat Defense URL Filtering 3Y Subscription |
| **L-FPR4112T-URL-5Y** | Cisco Firepower 4112 Threat Defense URL Filtering 5Y Subscription |
| **L-FPR4115T-AMP-1Y** | Cisco Firepower 4115 Threat Defense Malware Protection 1Y Subscription |
| **L-FPR4115T-AMP-3Y** | Cisco Firepower 4115 Threat Defense Malware Protection 3Y Subscription |
| **L-FPR4115T-AMP-5Y** | Cisco Firepower 4115 Threat Defense Malware Protection 5Y Subscription |
| **L-FPR4115T-T-1Y** | Cisco Firepower 4115 Threat Defense Threat Protection 1Y Subscription |
| **L-FPR4115T-T-3Y** | Cisco Firepower 4115 Threat Defense Threat Protection 3Y Subscription |
| **L-FPR4115T-T-5Y** | Cisco Firepower 4115 Threat Defense Threat Protection 5Y Subscription |
| **L-FPR4115T-TC-1Y** | Cisco Firepower 4115 Threat Defense Threat and URL 1Y Subscription |
| **L-FPR4115T-TC-3Y** | Cisco Firepower 4115 Threat Defense Threat and URL 3Y Subscription |
| **L-FPR4115T-TC-5Y** | Cisco Firepower 4115 Threat Defense Threat and URL 5Y Subscription |
| **L-FPR4115T-TM-1Y** | Cisco Firepower 4115 Threat Defense Threat and Malware 1Y Subscription |
| **L-FPR4115T-TM-3Y** | Cisco Firepower 4115 Threat Defense Threat and Malware 3Y Subscription |
| **L-FPR4115T-TM-5Y** | Cisco Firepower 4115 Threat Defense Threat and Malware 5Y Subscription |
| **L-FPR4115T-TMC-1Y** | Cisco Firepower 4115 Threat Defense Threat, Malware, and URL 1Y Subscription |
| **L-FPR4115T-TMC-3Y** | Cisco Firepower 4115 Threat Defense Threat, Malware, and URL 3Y Subscription |
| **L-FPR4115T-TMC-5Y** | Cisco Firepower 4115 Threat Defense Threat, Malware, and URL 5Y Subscription |
| **L-FPR4115T-URL-1Y** | Cisco Firepower 4115 Threat Defense URL Filtering 1Y Subscription |
| **L-FPR4115T-URL-3Y** | Cisco Firepower 4115 Threat Defense URL Filtering 3Y Subscription |
| **L-FPR4115T-URL-5Y** | Cisco Firepower 41154115 Threat Defense URL Filtering 5Y Subscription |
| **L-FPR4125T-AMP-1Y** | Cisco Firepower 4125 Threat Defense Malware Protection 1Y Subscription |
| **L-FPR4125T-AMP-3Y** | Cisco Firepower 4125 Threat Defense Malware Protection 3Y Subscription |
| **L-FPR4125T-AMP-5Y** | Cisco Firepower 4125 Threat Defense Malware Protection 5Y Subscription |
| **L-FPR4125T-T-1Y** | Cisco Firepower 4125 Threat Defense Threat Protection 1Y Subscription |
| **L-FPR4125T-T-3Y** | Cisco Firepower 4125 Threat Defense Threat Protection 3Y Subscription |

© 2026 Cisco and/or its affiliates. All rights reserved.

| Part Number | Description |
|---|---|
| **L-FPR4125T-T-5Y** | Cisco Firepower 4125 Threat Defense Threat Protection 5Y Subscription |
| **L-FPR4125T-TC-1Y** | Cisco Firepower 4125 Threat Defense Threat and URL 1Y Subscription |
| **L-FPR4125T-TC-3Y** | Cisco Firepower 4125 Threat Defense Threat and URL 3Y Subscription |
| **L-FPR4125T-TC-5Y** | Cisco Firepower 4125 Threat Defense Threat and URL 5Y Subscription |
| **L-FPR4125T-TM-1Y** | Cisco Firepower 4125 Threat Defense Threat and Malware 1Y Subscription |
| **L-FPR4125T-TM-3Y** | Cisco Firepower 4125 Threat Defense Threat and Malware 3Y Subscription |
| **L-FPR4125T-TM-5Y** | Cisco Firepower 4125 Threat Defense Threat and Malware 5Y Subscription |
| **L-FPR4125T-TMC-1Y** | Cisco Firepower 4125 Threat Defense Threat, Malware, and URL 1Y Subscription |
| **L-FPR4125T-TMC-3Y** | Cisco Firepower 4125 Threat Defense Threat, Malware, and URL 3Y Subscription |
| **L-FPR4125T-TMC-5Y** | Cisco Firepower 4125 Threat Defense Threat, Malware, and URL 5Y Subscription |
| **L-FPR4125T-URL-1Y** | Cisco Firepower 4125 Threat Defense URL Filtering 1Y Subscription |
| **L-FPR4125T-URL-3Y** | Cisco Firepower 4125 Threat Defense URL Filtering 3Y Subscription |
| **L-FPR4125T-URL-5Y** | Cisco Firepower 4125 Threat Defense URL Filtering 5Y Subscription |
| **L-FPR4140T-AMP-5Y** | Cisco Firepower 4140 Threat Defense Malware Protection 5Y Subscription |
| **L-FPR4140T-T-1Y** | Cisco Firepower 4140 Threat Defense Threat Protection 1Y Subscription |
| **L-FPR4145T-AMP-1Y** | Cisco Firepower 4145 Threat Defense Malware Protection 1Y Subscription |
| **L-FPR4145T-AMP-3Y** | Cisco Firepower 4145 Threat Defense Malware Protection 3Y Subscription |
| **L-FPR4145T-AMP-5Y** | Cisco Firepower 4145 Threat Defense Malware Protection 5Y Subscription |
| **L-FPR4145T-T-1Y** | Cisco Firepower 4145 Threat Defense Threat Protection 1Y Subscription |
| **L-FPR4145T-T-3Y** | Cisco Firepower 4145 Threat Defense Threat Protection 3Y Subscription |
| **L-FPR4145T-T-5Y** | Cisco Firepower 4145 Threat Defense Threat Protection 5Y Subscription |
| **L-FPR4145T-TC-1Y** | Cisco Firepower 4145 Threat Defense Threat and URL 1Y Subscription |
| **L-FPR4145T-TC-3Y** | Cisco Firepower 4145 Threat Defense Threat and URL 3Y Subscription |
| **L-FPR4145T-TC-5Y** | Cisco Firepower 4145 Threat Defense Threat and URL 5Y Subscription |
| **L-FPR4145T-TM-1Y** | Cisco Firepower 4145 Threat Defense Threat and Malware 1Y Subscription |
| **L-FPR4145T-TM-3Y** | Cisco Firepower 4145 Threat Defense Threat and Malware 3Y Subscription |
| **L-FPR4145T-TM-5Y** | Cisco Firepower 4145 Threat Defense Threat and Malware 5Y Subscription |

© 2026 Cisco and/or its affiliates. All rights reserved.

| Part Number | Description |
|---|---|
| **L-FPR4145T-TMC-1Y** | Cisco Firepower 4145 Threat Defense Threat, Malware, and URL 1Y Subscription |
| **L-FPR4145T-TMC-3Y** | Cisco Firepower 4145 Threat Defense Threat, Malware, and URL 3Y Subscription |
| **L-FPR4145T-TMC-5Y** | Cisco Firepower 4145 Threat Defense Threat, Malware, and URL 5Y Subscription |
| **L-FPR4145T-URL-1Y** | Cisco Firepower 4145 Threat Defense URL Filtering 1Y Subscription |
| **L-FPR4145T-URL-3Y** | Cisco Firepower 4145 Threat Defense URL Filtering 3Y Subscription |
| **L-FPR4145T-URL-5Y** | Cisco Firepower 4145 Threat Defense URL Filtering 5Y Subscription |

**Ordering Example: Cisco Firepower 4145 with ASA**

**Step 1:** Smart Software Licensing

Before placing a Cisco Firepower 4100 order, a Smart Software Licensing account for the end customer must be initiated. If the customer already has a Smart Software Licensing account, that account must be associated with the order. More information on Smart Software Licensing account establishment is available in the Smart Software Licensing section of this ordering guide, and online at: https://www.cisco.com/web/ordering/smart-software-manager/index.html.

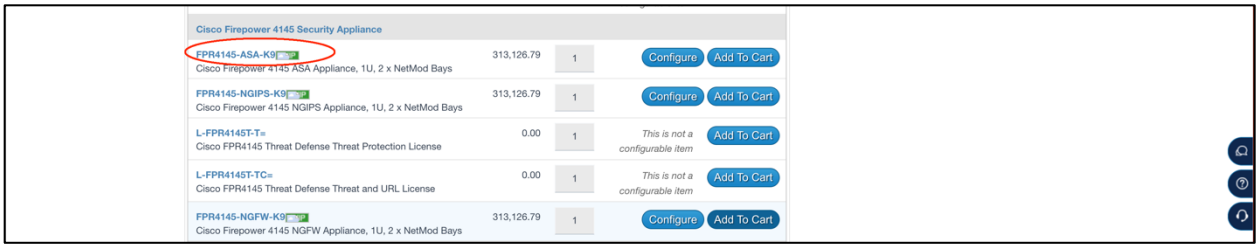
To associate the order's licenses with the customer's Smart Licensing account, or to begin the establishment of the Smart Licensing account, follow these steps. Note that if you are initiating the account, you can complete the order only if the account is initiated on the end customer's behalf and associated with the order.

Go to Cisco Commerce: https://www.cisco.com/go/ccw.

From the Orders pull-down menu, select Create Order.

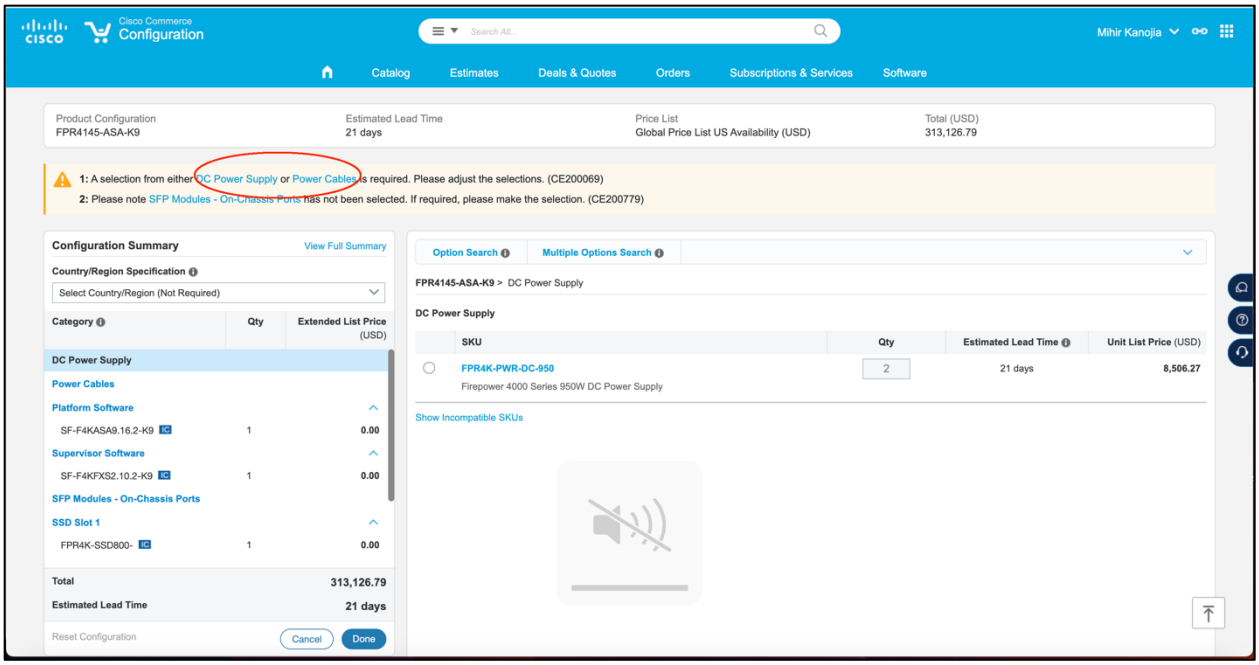
Select Assign Smart Account and follow the subsequent prompts for Smart Licensing.

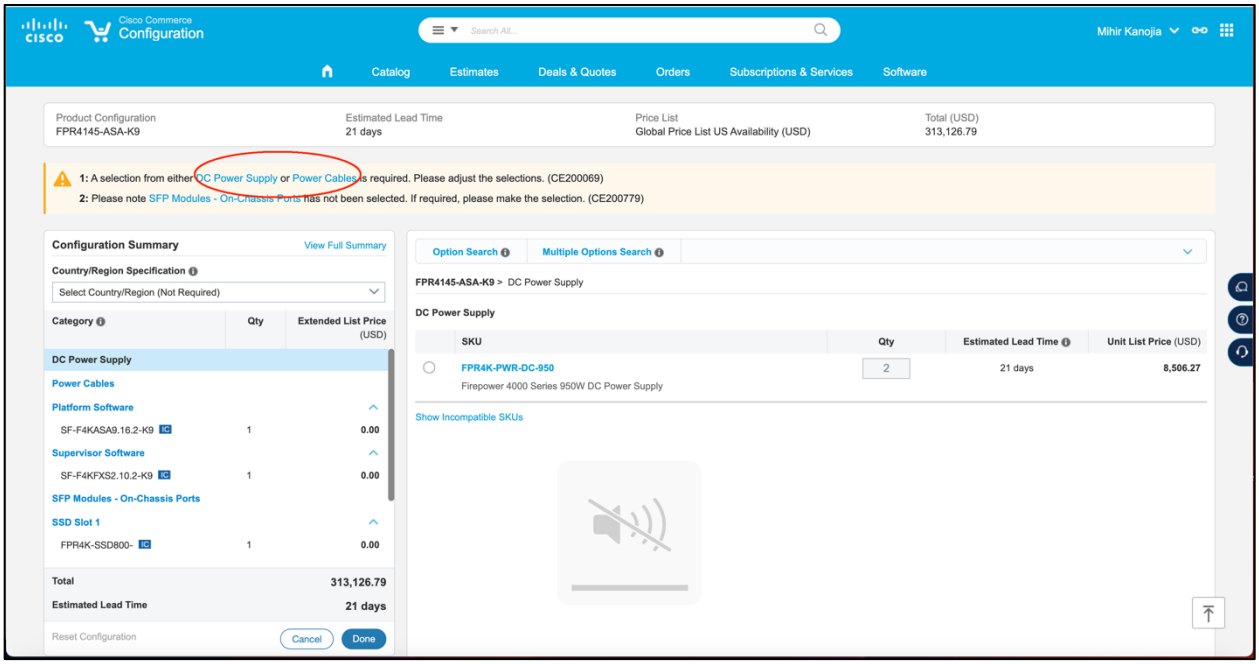
**Step 2:** Navigate to Products -> Security -> Cisco Firepower 4100 Series -> Cisco Firepower 4145 Security Appliance -> FPR4145-ASA-K9




© 2026 Cisco and/or its affiliates. All rights reserved.

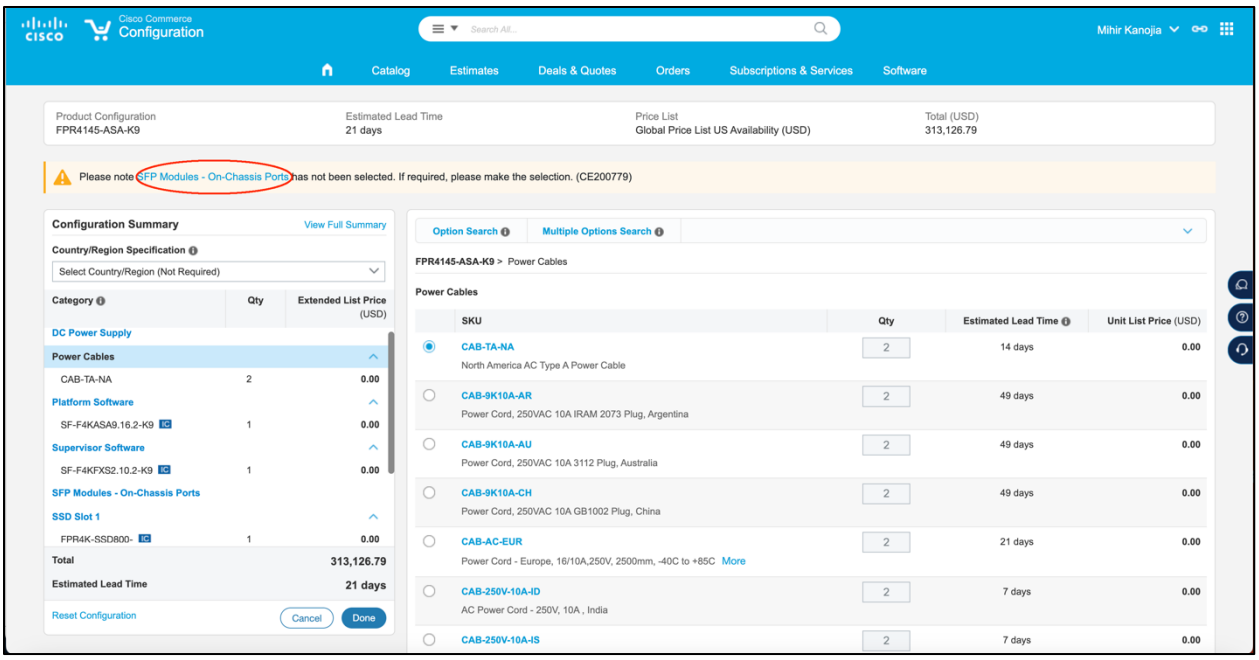
**Step 3:** Click on the Power cables to make the selection.

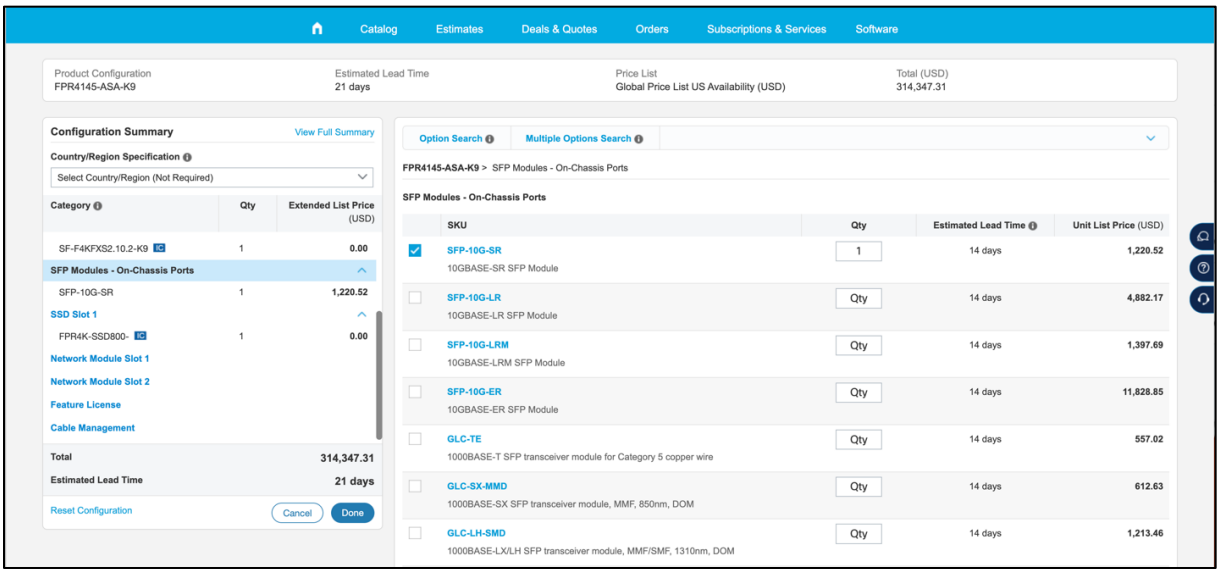



© 2026 Cisco and/or its affiliates. All rights reserved.

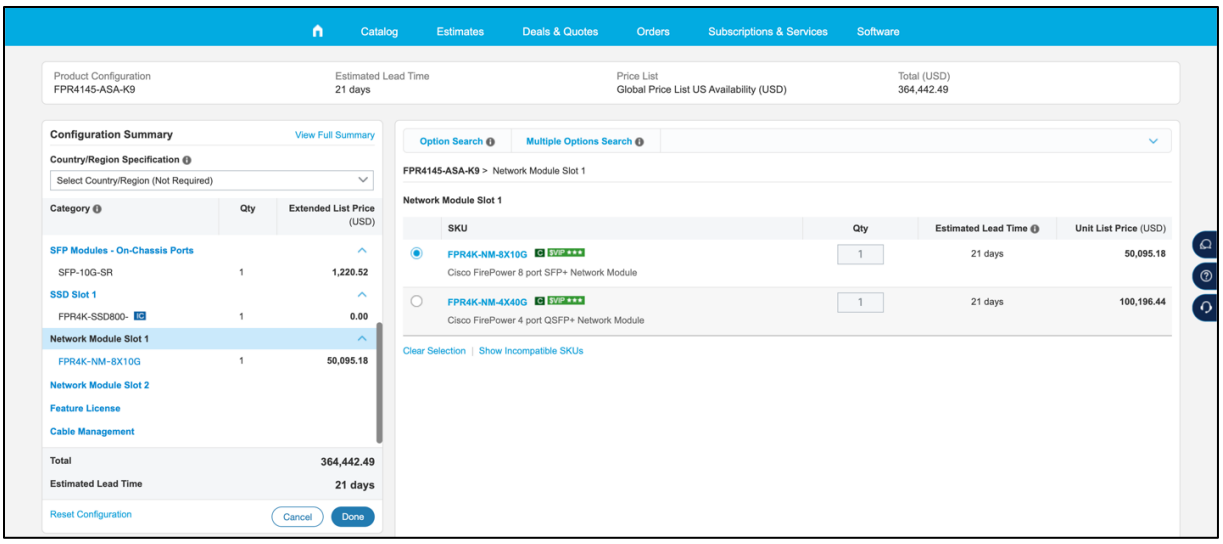
**Step 4:** Click on “SFP-Modules – On Chassis ports” to make the selection.

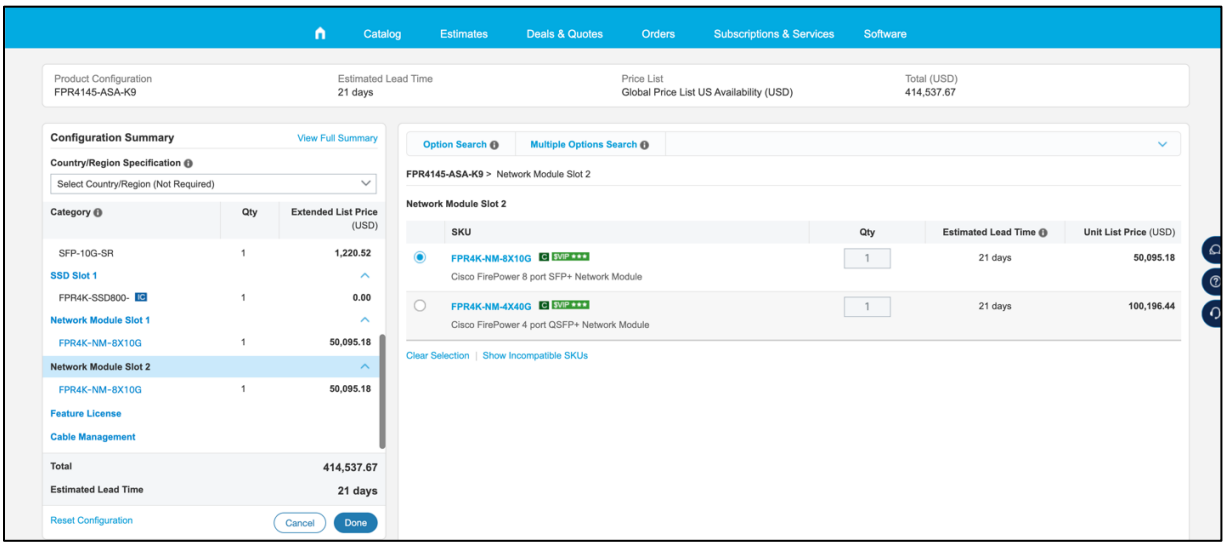



© 2026 Cisco and/or its affiliates. All rights reserved.

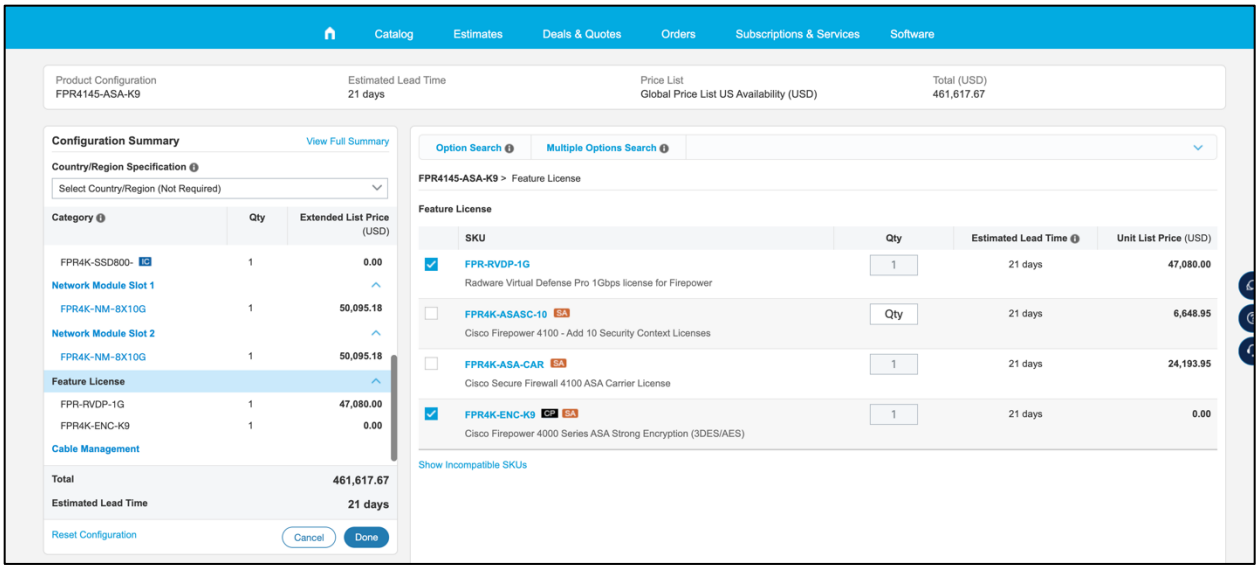
**Step 5:** Select the Network Modules – Slot 1 and Slot 2



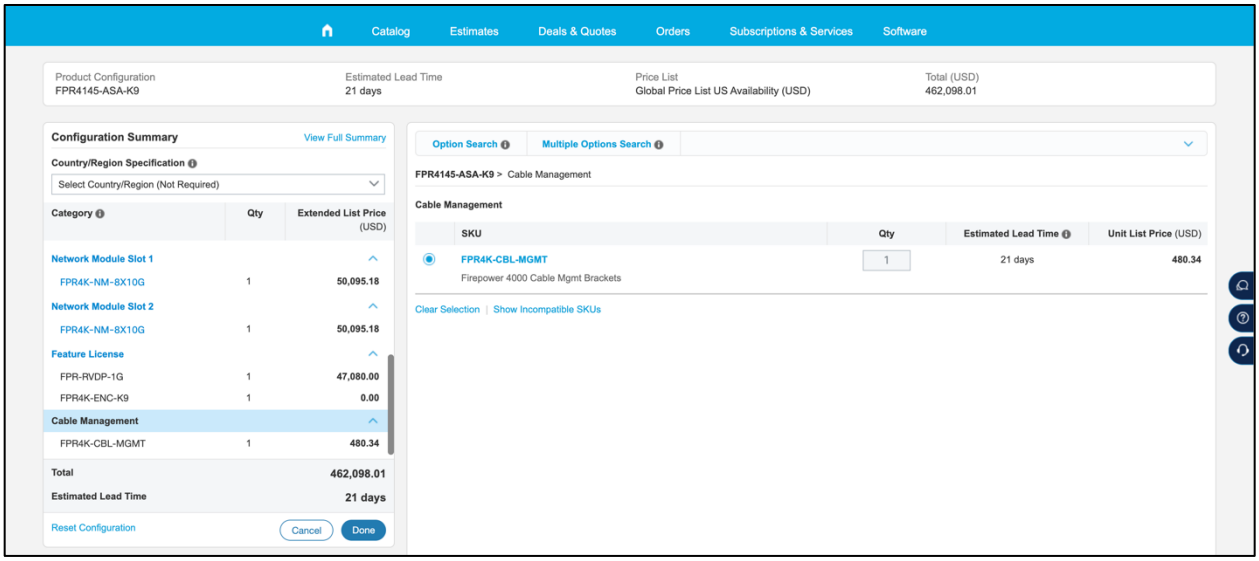




© 2026 Cisco and/or its affiliates. All rights reserved.

**Step 6:** Select Feature License




**Step 7:** Select Cables from Cable Management

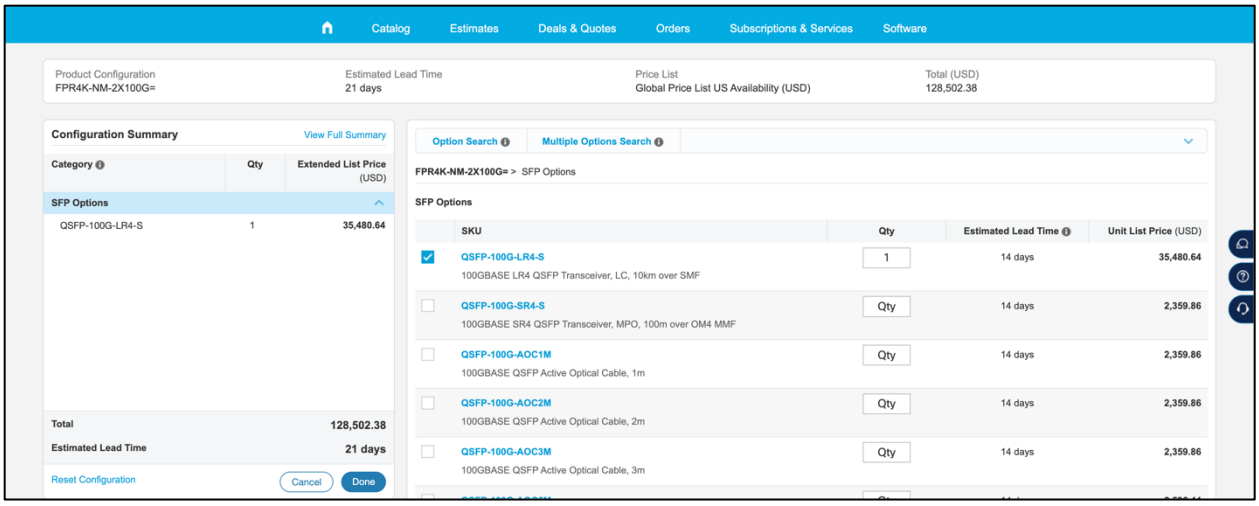



**Step 8:** Adding Spares. Navigate back to Products -> Security -> Cisco Firepower 4100 Series -> Accessories and Spares > Cisco Firepower 4145 Security Appliance -> FPR4K-NM-2X100G= -> Click Configure

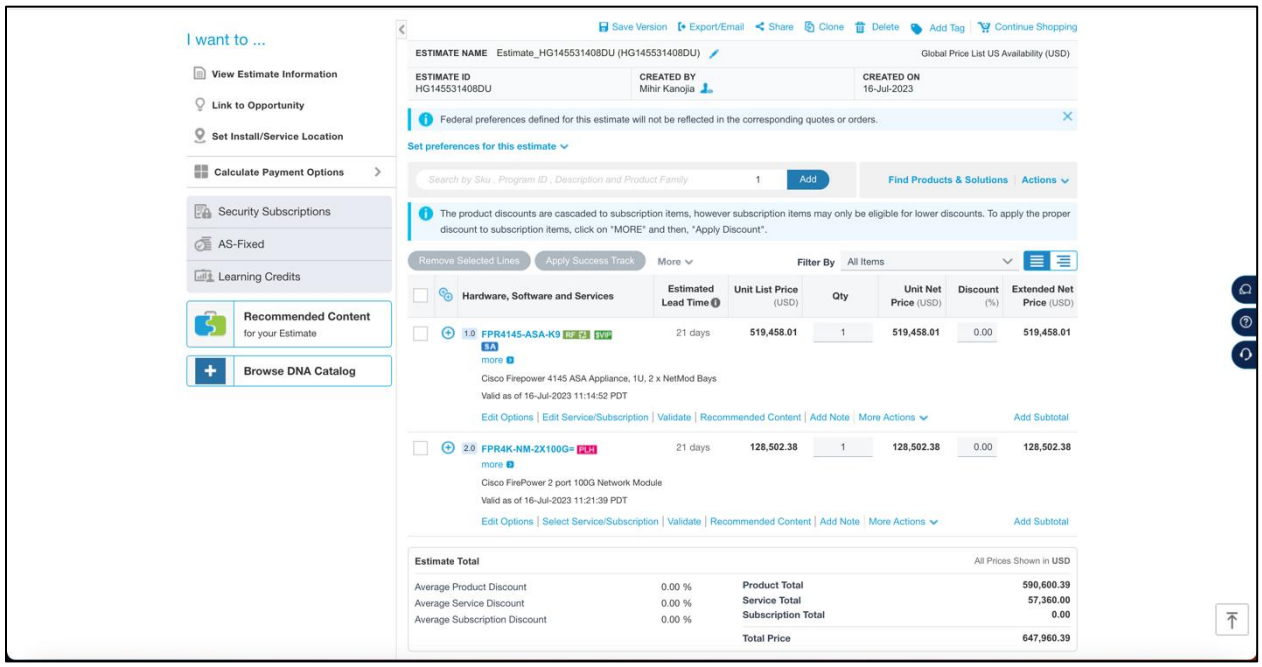



© 2026 Cisco and/or its affiliates. All rights reserved.

**Step 9:** Select the trans receiver for the SFP Option and click done.




**Step 10:** Final Product Summary configuration.




### SKUs and Ordering for Cisco Firepower 4200 Series

The following tables outline the product part number information for the Cisco Firepower 4200 Series. Note that the customer may want extra power supplies and fans.

**Table 46.** 4200 Series chassis part numbers

| Part Number | Description |
|---|---|
| **FPR4200-FTD-HA-BUN** | Cisco Secure Firewall 4200 series Two Unit High Availability Bundle (will order 2 identical chassis and software subscriptions to be configured as a high-availability pair) |
| **FPR4215-BUN** | Cisco Secure Firewall 4215 Master Bundle |

© 2026 Cisco and/or its affiliates. All rights reserved.

| Part Number | Description |
|---|---|
| **FPR4225-BUN** | Cisco Secure Firewall 4225 Master Bundle |
| **FPR4245-BUN** | Cisco Secure Firewall 4245 Master Bundle |
| **FPR4215-ASA-K9** | Cisco Secure Firewall 4215 ASA Appliance, 1U, 2x NetMod Bays |
| **FPR4215-NGFW-K9** | Cisco Secure Firewall 4215 NGFW Appliance, 1RU, 2 x Network Module Bays |
| **FPR4225-ASA-K9** | Cisco Secure Firewall 4225 ASA Appliance, 1RU, 2 x Network Module Bays |
| **FPR4225-NGFW-K9** | Cisco Secure Firewall 4225 NGFW Appliance, 1RU, 2 x Network Module Bays |
| **FPR4245-ASA-K9** | Cisco Secure Firewall 4125 ASA Appliance, 1RU, 2 x Network Module Bays |
| **FPR4245-NGFW-K9** | Cisco Secure Firewall 4125 NGFW Appliance, 1RU, 2 x Network Module Bays |

**Note:** Use the bundle part number unless you have an explicit reason not to. the bundle pid ensures that all necessary components are purchased.

**Table 47.** 4200 Series network module part numbers

| Part Number | Description |
|---|---|
| **FPR4K-XNM-2X400G** | Cisco Secure Firewall 4200 2X400G Netmod |
| **FPR4K-XNM-2X100G** | Cisco Secure Firewall 4200 2X100G QSFP28 Netmod |
| **FPR4K-XNM-4X200G** | Cisco Secure Firewall 4200 4X200G Netmod |
| **FPR4K-XNM-4X40G** | Cisco Secure Firewall 4200 4X40G QSFP+ Netmod |
| **FPR4K-XNM-6X10LRF** | Cisco Secure Firewall 4200 6X10G FTW Netmod, LR-Singlemode |
| **FPR4K-XNM-6X10SRF** | Cisco Secure Firewall 4200 6X10G FTW Netmod, SR-Multimode |
| **FPR4K-XNM-6X25LRF** | Cisco Secure Firewall 4200 6X25G FTW Netmod, LR-Singlemode |
| **FPR4K-XNM-6X25SRF** | Cisco Secure Firewall 4200 6X25G FTW Netmod, SR-Multimode |
| **FPR4K-XNM-8X10G** | Cisco Secure Firewall 4200 8X10G SFP+ Netmod |
| **FPR4K-XNM-8X25G** | Cisco Secure Firewall 4200 8X25G ZSFP Netmod |

**Table 48.** 4200 Series accessories part numbers

| Part Number | Description |
|---|---|
| **FPR4200-PWR-AC** | Cisco Secure Firewall 4200 Series AC Power Supply |
| **FPR4200-PWR-AC=** | Cisco Secure Firewall 4200 Series AC Power Supply |
| **FPR4200-SSD1800** | Cisco Secure Firewall 4200 Series 1.8TB SSD |

© 2026 Cisco and/or its affiliates. All rights reserved.

| Part Number | Description |
|---|---|
| **FPR4200-SSD1800=** | Cisco Secure Firewall 4200 Series 1.8TB SSD |
| **FPR4200-PSU-BLANK** | Cisco Secure Firewall 4200 Series Chassis PWR Blank Slot Cvr |
| **FPR4200-PSU-BLANK=** | Cisco Secure Firewall 4200 Series Chassis PWR Blank Slot Cvr |
| **FPR4200-NM-BLANK** | Cisco Secure Firewall 4200 Series NM Blank Slot Cover |
| **FPR4200-NM-BLANK=** | Cisco Secure Firewall 4200 Series NM Blank Slot Cover |
| **FPR4200-FAN** | Cisco Secure Firewall 4200 Series Fan |
| **FPR4200-FAN=** | Cisco Secure Firewall 4200 Series Fan |
| **FPR4200-ACC-KIT** | Cisco Secure Firewall 4200 HW Acc Kit (Rack Mounts, Cables) |
| **FPR4200-ACC-KIT=** | Cisco Secure Firewall 4200 HW Acc Kit (Rack Mounts, Cables) |
| **FPR4200-CBL-MGMT** | Cisco Secure Firewall 4200 Series Cable Management Brackets |
| **FPR4200-CBL-MGMT=** | Cisco Secure Firewall 4200 Series Cable Management Brackets |
| **FPR4200-FIPS-KIT** | Cisco Secure Firewall 4200 Series FIPS Kits |
| **FPR4200-FIPS-KIT=** | Cisco Secure Firewall 4200 Series FIPS Kits |
| **FPR4200-SLD-RAILS** | Cisco Secure Firewall 4200 Series Slide Rail Kit |
| **FPR4200-SLD-RAILS=** | Cisco Secure Firewall 4200 Series Slide Rail Kit |

**Note:** Use these part numbers if the customer is ordering spare fans, power supplies, or a rack mount kit.

© 2026 Cisco and/or its affiliates. All rights reserved.

**SKUs for 4200 Series Licenses and Subscriptions**

When ordering a 4200 Series firewall with the ASA configuration, a license is required. When ordering a 4200 Series hardware with the Cisco Secure Firewall Threat Defense image, both licenses and a subscription to optional security services are required. Subscription terms are 1, 3, and 5 years, with the greatest price discount at 5 years. In the listed part numbers, the threat services are identified as follows:

**Table 49.** Threat Subscription Details

| Threat Subscription Abbreviations | Description |
|---|---|
| **T** | Threat (Security Intelligence and IPS) |
| **M or AMP*** | Malware defense |
| **C or URL*** | URL Filtering |
| **1Y** | **1-Year** Subscription |
| **3Y** | **3-Year** Subscription |
| **5Y** | **5-Year** Subscription |

*Note that Threat/IPS (T) License is a requirement for the use of Malware (M) or URL (C) license features.

**Table 50.** Cisco Firepower 4200 Series license part numbers for configurations with the Cisco Secure Firewall Threat Defense image

| Part Number | Description |
|---|---|
| **L-FPR4215T-AMP=** | Cisco Secure Firewall 4215 Threat Defence License |
| **FPR4215T-T / L-FPR4215T-T=** | Cisco Secure Firewall 4215 TD and URL Filtering License |
| **FPR4215T-TC / L-FPR4215T-TC=** | Cisco Secure Firewall 4215 TD, AMP & URL Filtering License |
| **FPR4215T-TM / L-FPR4215T-TM=** | Cisco Secure Firewall 4215 TD, AMP & URL Filtering License |
| **FPR4215T-TMC / L-FPR4215T-TMC=** | Cisco Secure Firewall 4225 Threat Defence License |
| **L-FPR4215T-URL=** | Cisco Secure Firewall 4225 TD and URL Filtering License |
| **L-FPR4225T-AMP=** | Cisco Secure Firewall 4225 TD, AMP & URL Filtering License |
| **FPR4225T-T / L-FPR4225T-T=** | Cisco Secure Firewall 4225 TD, AMP & URL Filtering License |
| **FPR4225T-TC / L-FPR4225T-TC=** | Cisco Secure Firewall 4245 Threat Defence License |
| **FPR4225T-TM / L-FPR4225T-TM=** | Cisco Secure Firewall 4245 TD and URL Filtering License |
| **FPR4225T-TMC / L-FPR4225T-TMC=** | Cisco Secure Firewall 4245 TD, AMP & URL Filtering License |
| **L-FPR4225T-URL=** | Cisco Secure Firewall 4245 TD, AMP & URL Filtering License |
| **L-FPR4245T-AMP=** | Cisco Secure Firewall 4215 Adv Malware Protection License |
| **FPR4245T-T / L-FPR4245T-T=** | Cisco Secure Firewall 4215 Threat Defence License |

© 2026 Cisco and/or its affiliates. All rights reserved.

| Part Number | Description |
|---|---|
| **FPR4245T-TC / L-FPR4245T-TC=** | Cisco Secure Firewall 4215 TD and URL Filtering License |
| **FPR4245T-TM / L-FPR4245T-TM=** | Cisco Secure Firewall 4215 Threat Defence and AMP License |
| **FPR4245T-TMC / L-FPR4245T-TMC=** | Cisco Secure Firewall 4215 TD, AMP & URL Filtering License |
| **L-FPR4245T-URL=** | Cisco Secure Firewall 4215 URL Filtering License |

**Table 51.** Cisco Secure Firewall 4200 Series subscription part numbers for configurations with the FTD image

| Part Number | Description |
|---|---|
| **L-FPR4215T-T-1Y** | Cisco Secure Firewall 4215 Threat Defence 1Y Subs |
| **L-FPR4215T-T-3Y** | Cisco Secure Firewall 4215 Threat Defence 3Y Subs |
| **L-FPR4215T-T-5Y** | Cisco Secure Firewall 4215 Threat Defence 5Y Subs |
| **L-FPR4215T-TC-1Y** | Cisco Secure Firewall 4215 TD and URL Filtering 1Y Subs |
| **L-FPR4215T-TC-3Y** | Cisco Secure Firewall 4215 TD and URL Filtering 3Y Subs |
| **L-FPR4215T-TC-5Y** | Cisco Secure Firewall 4215 TD and URL Filtering 5Y Subs |
| **L-FPR4215T-TM-1Y** | Cisco Secure Firewall 4215 Threat Defence and AMP 1Y Subs |
| **L-FPR4215T-TM-3Y** | Cisco Secure Firewall 4215 Threat Defence and AMP 3Y Subs |
| **L-FPR4215T-TM-5Y** | Cisco Secure Firewall 4215 Threat Defence and AMP 5Y Subs |
| **L-FPR4215T-TMC-1Y** | Cisco Secure Firewall 4215 TD, AMP & URL Filtering 1Y Subs |
| **L-FPR4215T-TMC-3Y** | Cisco Secure Firewall 4215 TD, AMP & URL Filtering 3Y Subs |
| **L-FPR4215T-TMC-5Y** | Cisco Secure Firewall 4215 TD, AMP & URL Filtering 5Y Subs |
| **L-FPR4215T-AMP-1Y** | Cisco Secure Firewall 4215 Adv Malware Protection 1Y Subs |
| **L-FPR4215T-AMP-3Y** | Cisco Secure Firewall 4215 Adv Malware Protection 3Y Subs |
| **L-FPR4215T-AMP-5Y** | Cisco Secure Firewall 4215 Adv Malware Protection 5Y Subs |
| **L-FPR4215T-URL-1Y** | Cisco Secure Firewall 4215 URL Filtering 1Y Subs |
| **L-FPR4215T-URL-3Y** | Cisco Secure Firewall 4215 URL Filtering 3Y Subs |
| **L-FPR4215T-URL-5Y** | Cisco Secure Firewall 4215 URL Filtering 5Y Subs |
| **L-FPR4225T-T-1Y** | Cisco Secure Firewall 4225 Threat Defence 1Y Subs |
| **L-FPR4225T-T-3Y** | Cisco Secure Firewall 4225 Threat Defence 3Y Subs |
| **L-FPR4225T-T-5Y** | Cisco Secure Firewall 4225 Threat Defence 5Y Subs |

© 2026 Cisco and/or its affiliates. All rights reserved.

| Part Number | Description |
|---|---|
| **L-FPR4225T-TC-1Y** | Cisco Secure Firewall 4225 TD and URL Filtering 1Y Subs |
| **L-FPR4225T-TC-3Y** | Cisco Secure Firewall 4225 TD and URL Filtering 3Y Subs |
| **L-FPR4225T-TC-5Y** | Cisco Secure Firewall 4225 TD and URL Filtering 5Y Subs |
| **L-FPR4225T-TM-1Y** | Cisco Secure Firewall 4225 Threat Defence and AMP 1Y Subs |
| **L-FPR4225T-TM-3Y** | Cisco Secure Firewall 4225 Threat Defence and AMP 3Y Subs |
| **L-FPR4225T-TM-5Y** | Cisco Secure Firewall 4225 Threat Defence and AMP 5Y Subs |
| **L-FPR4225T-TMC-1Y** | Cisco Secure Firewall 4225 TD, AMP & URL Filtering 1Y Subs |
| **L-FPR4225T-TMC-3Y** | Cisco Secure Firewall 4225 TD, AMP & URL Filtering 3Y Subs |
| **L-FPR4225T-TMC-5Y** | Cisco Secure Firewall 4225 TD, AMP & URL Filtering 5Y Subs |
| **L-FPR4225T-AMP-1Y** | Cisco Secure Firewall 4225 Adv Malware Protection 1Y Subs |
| **L-FPR4225T-AMP-3Y** | Cisco Secure Firewall 4225 Adv Malware Protection 3Y Subs |
| **L-FPR4225T-AMP-5Y** | Cisco Secure Firewall 4225 Adv Malware Protection 5Y Subs |
| **L-FPR4225T-URL-1Y** | Cisco Secure Firewall 4225 URL Filtering 1Y Subs |
| **L-FPR4225T-URL-3Y** | Cisco Secure Firewall 4225 URL Filtering 3Y Subs |
| **L-FPR4225T-URL-5Y** | Cisco Secure Firewall 4225 URL Filtering 5Y Subs |
| **L-FPR4245T-T-1Y** | Cisco Secure Firewall 4245 Threat Defence 1Y Subs |
| **L-FPR4245T-T-3Y** | Cisco Secure Firewall 4245 Threat Defence 3Y Subs |
| **L-FPR4245T-T-5Y** | Cisco Secure Firewall 4245 Threat Defence 5Y Subs |
| **L-FPR4245T-TC-1Y** | Cisco Secure Firewall 4245 TD and URL Filtering 1Y Subs |
| **L-FPR4245T-TC-3Y** | Cisco Secure Firewall 4245 TD and URL Filtering 3Y Subs |
| **L-FPR4245T-TC-5Y** | Cisco Secure Firewall 4245 TD and URL Filtering 5Y Subs |
| **L-FPR4245T-TM-1Y** | Cisco Secure Firewall 4245 Threat Defence and AMP 1Y Subs |
| **L-FPR4245T-TM-3Y** | Cisco Secure Firewall 4245 Threat Defence and AMP 3Y Subs |
| **L-FPR4245T-TM-5Y** | Cisco Secure Firewall 4245 Threat Defence and AMP 5Y Subs |
| **L-FPR4245T-TMC-1Y** | Cisco Secure Firewall 4245 TD, AMP & URL Filtering 1Y Subs |
| **L-FPR4245T-TMC-3Y** | Cisco Secure Firewall 4245 TD, AMP & URL Filtering 3Y Subs |
| **L-FPR4245T-TMC-5Y** | Cisco Secure Firewall 4245 TD, AMP & URL Filtering 5Y Subs |

© 2026 Cisco and/or its affiliates. All rights reserved.

| Part Number | Description |
|---|---|
| **L-FPR4245T-AMP-1Y** | Cisco Secure Firewall 4245 Adv Malware Protection 1Y Subs |
| **L-FPR4245T-AMP-3Y** | Cisco Secure Firewall 4245 Adv Malware Protection 3Y Subs |
| **L-FPR4245T-AMP-5Y** | Cisco Secure Firewall 4245 Adv Malware Protection 5Y Subs |
| **L-FPR4245T-URL-1Y** | Cisco Secure Firewall 4245 URL Filtering 1Y Subs |
| **L-FPR4245T-URL-3Y** | Cisco Secure Firewall 4245 URL Filtering 3Y Subs |
| **L-FPR4245T-URL-5Y** | Cisco Secure Firewall 4245 URL Filtering 5Y Subs |

**Ordering Example: Cisco Secure Firewall 4225 with FTD**

**Step 1:** Smart Software Licensing

Before placing a Cisco Secure Firewall 4200 order, a Smart Software Licensing account for the end customer must be initiated. If the customer already has a Smart Software Licensing account, that account must be associated with the order. More information on Smart Software Licensing account establishment is available in the Smart Software Licensing section of this ordering guide, and online at: https://www.cisco.com/web/ordering/smart-software-manager/index.html.

To associate the order's licenses with the customer's Smart Licensing account, or to begin the establishment of the Smart Licensing account, follow these steps. Note that if you are initiating the account, you can complete the order only if the account is initiated on the end customer's behalf and associated with the order.

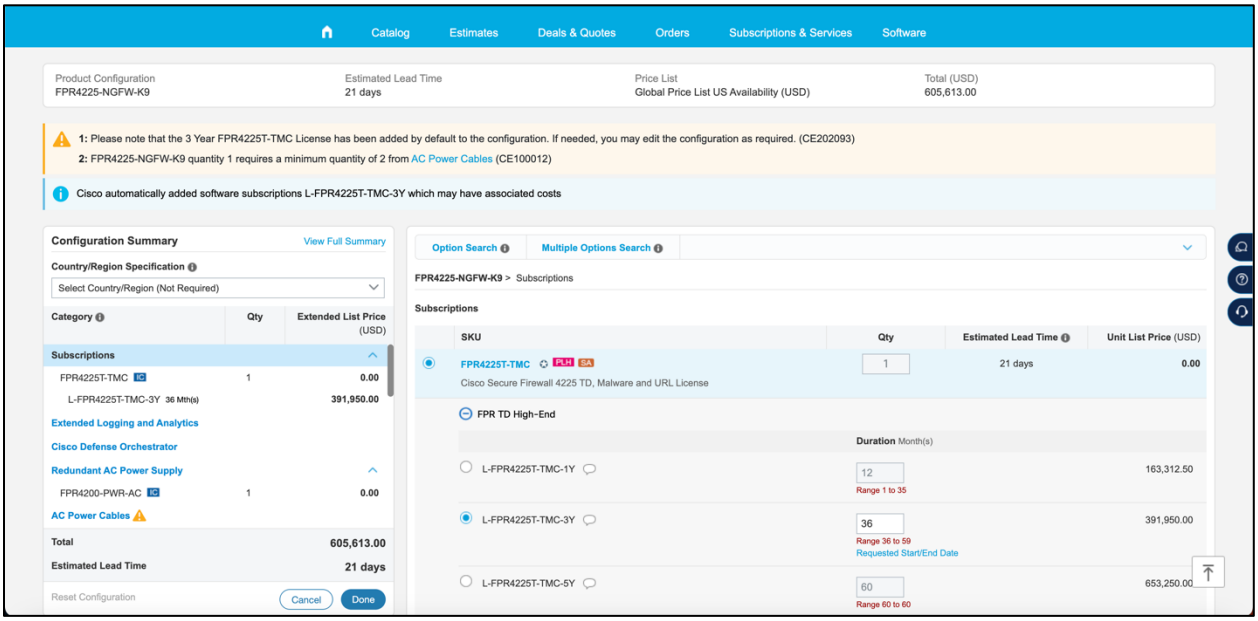
Go to Cisco Commerce: https://www.cisco.com/go/ccw.

From the Orders pull-down menu, select Create Order.

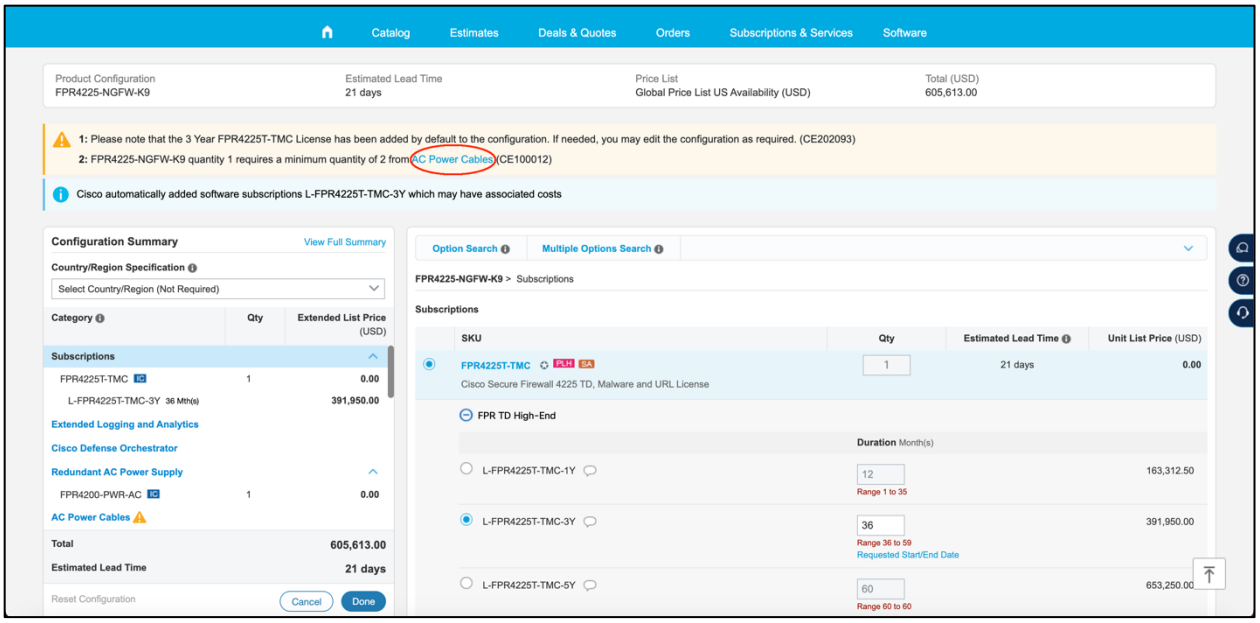
Select Assign Smart Account and follow the subsequent prompts for Smart Licensing.

© 2026 Cisco and/or its affiliates. All rights reserved.

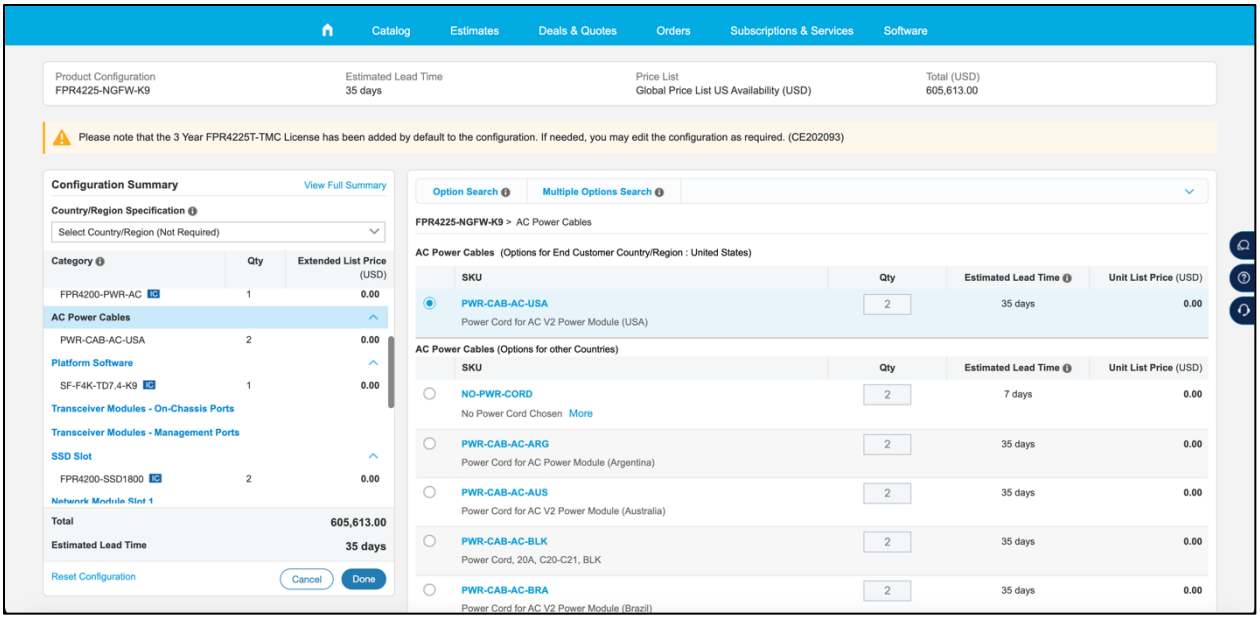
**Step 2:** Navigate to Products -> Security -> Cisco Secure Firewall 4200 Series -> Cisco Secure Firewall 4225 Security Appliance -> FPR4225-NGFW-K9



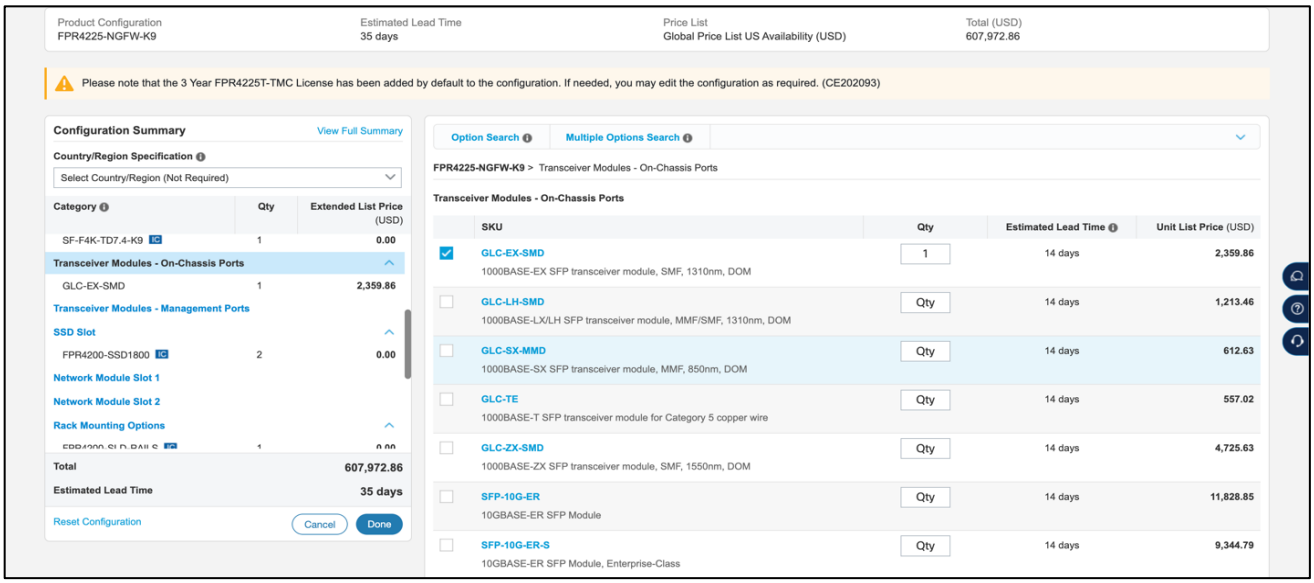

**Step 3:** Select the Power Cables




© 2026 Cisco and/or its affiliates. All rights reserved.

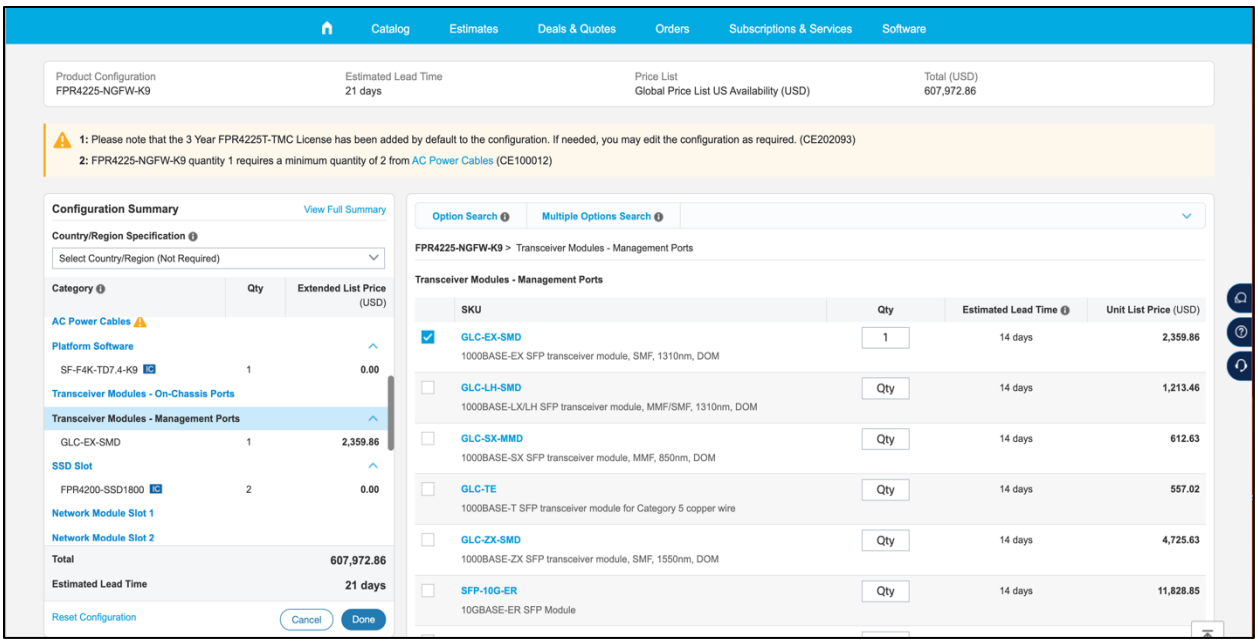



**Step 4:** Select Transceiver modules – On-Chassis Ports

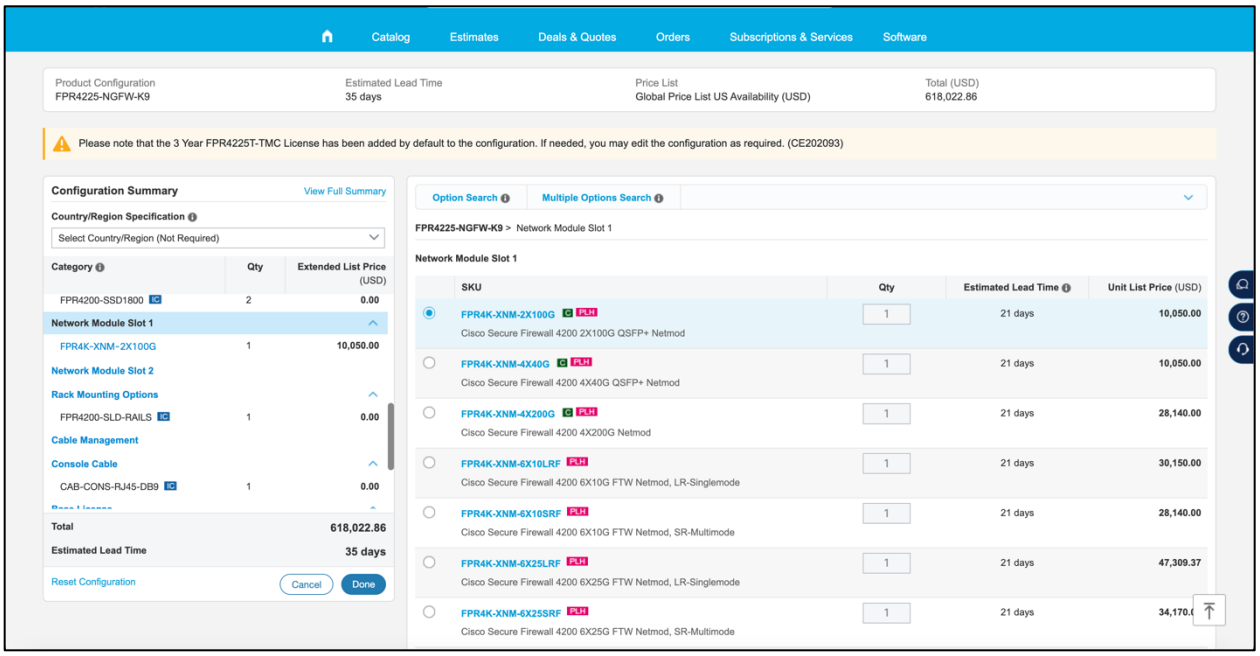



© 2026 Cisco and/or its affiliates. All rights reserved.

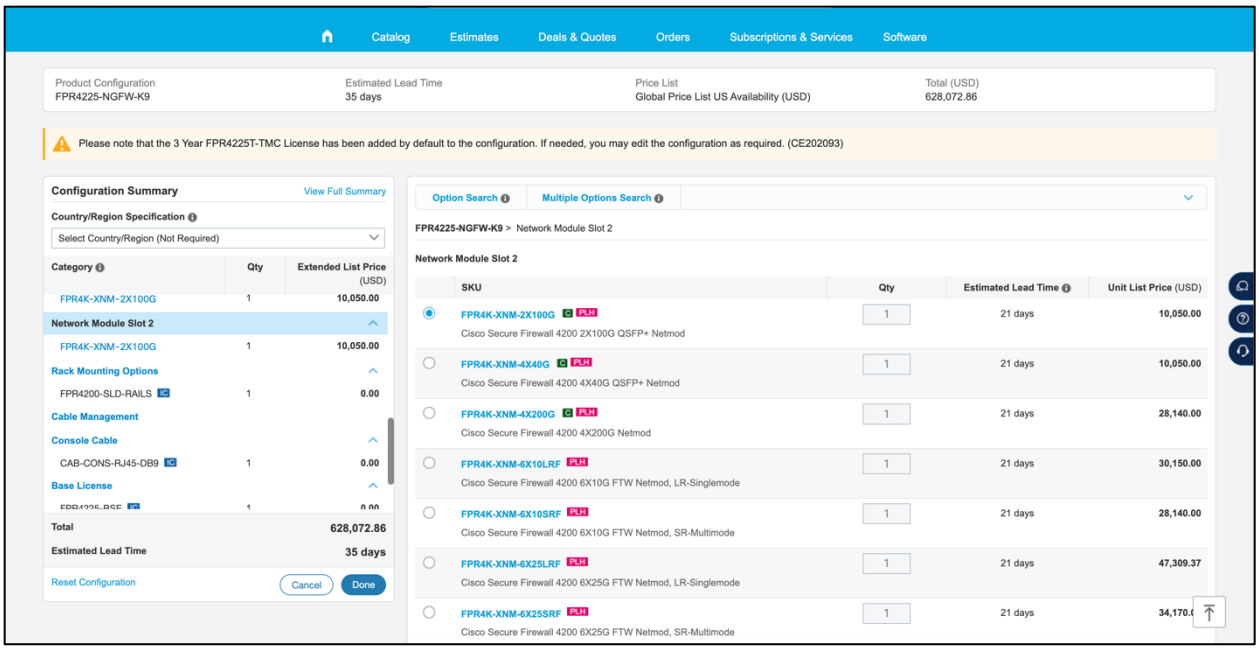
**Step 5:** Select Transceiver modules – Management Ports



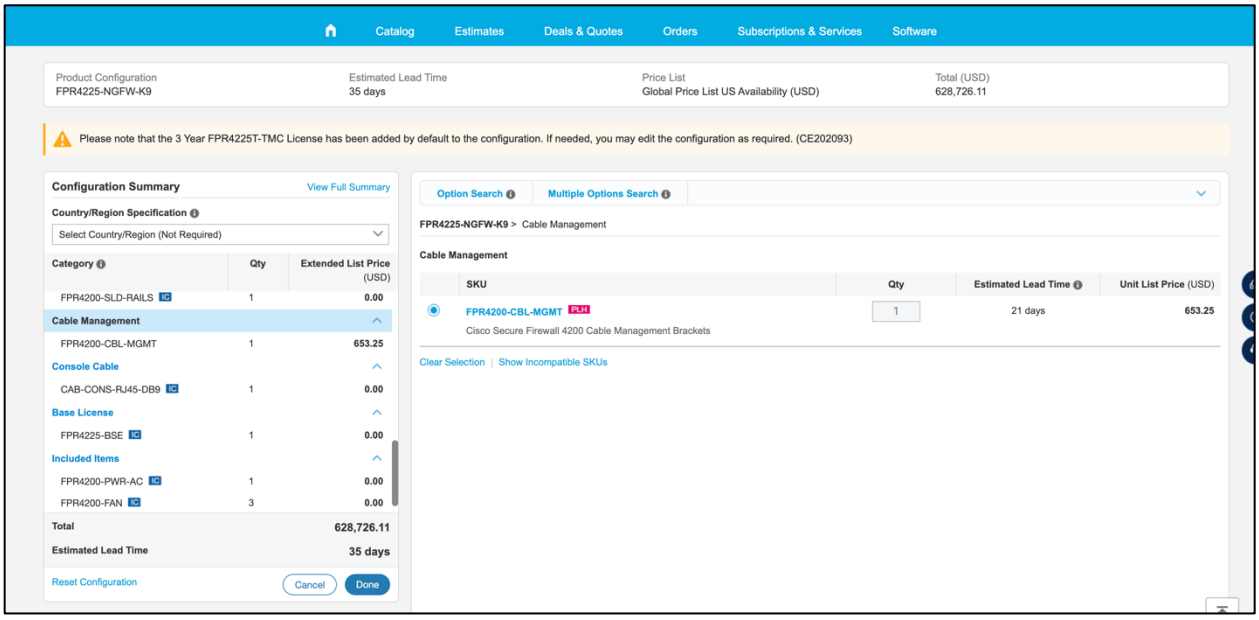

**Step 6:** Select Network Modules for Slot-1 and Slot-2




© 2026 Cisco and/or its affiliates. All rights reserved.

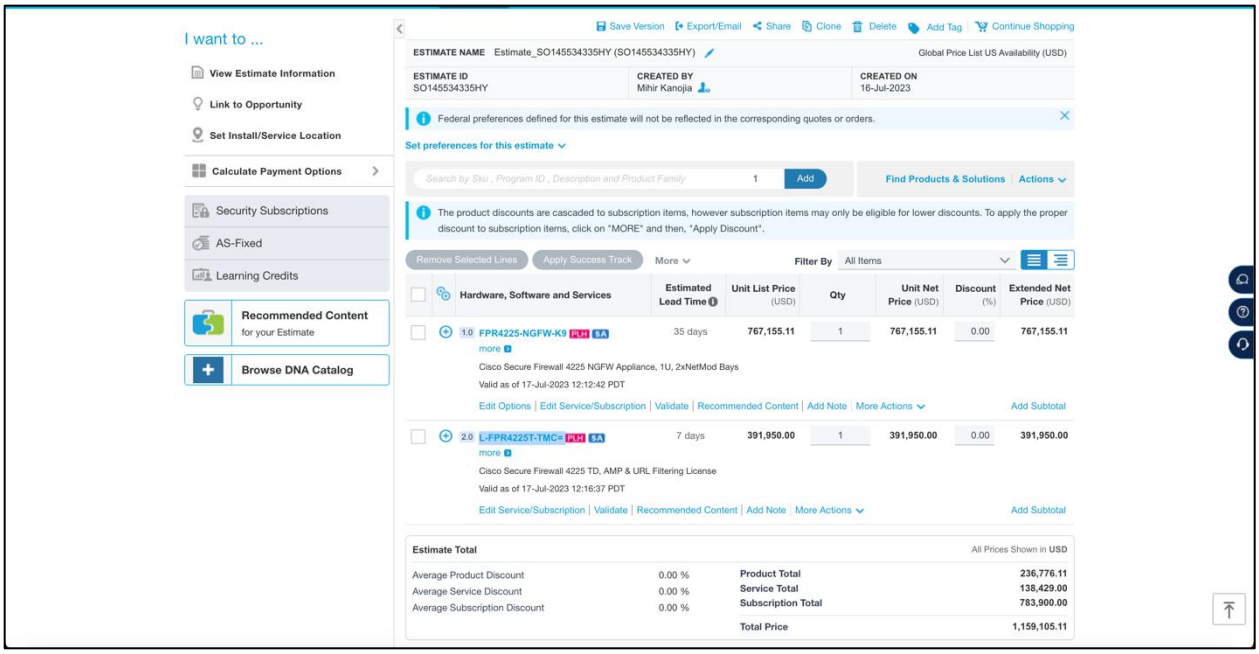



**Step 7:** Select the cables from Cable Management



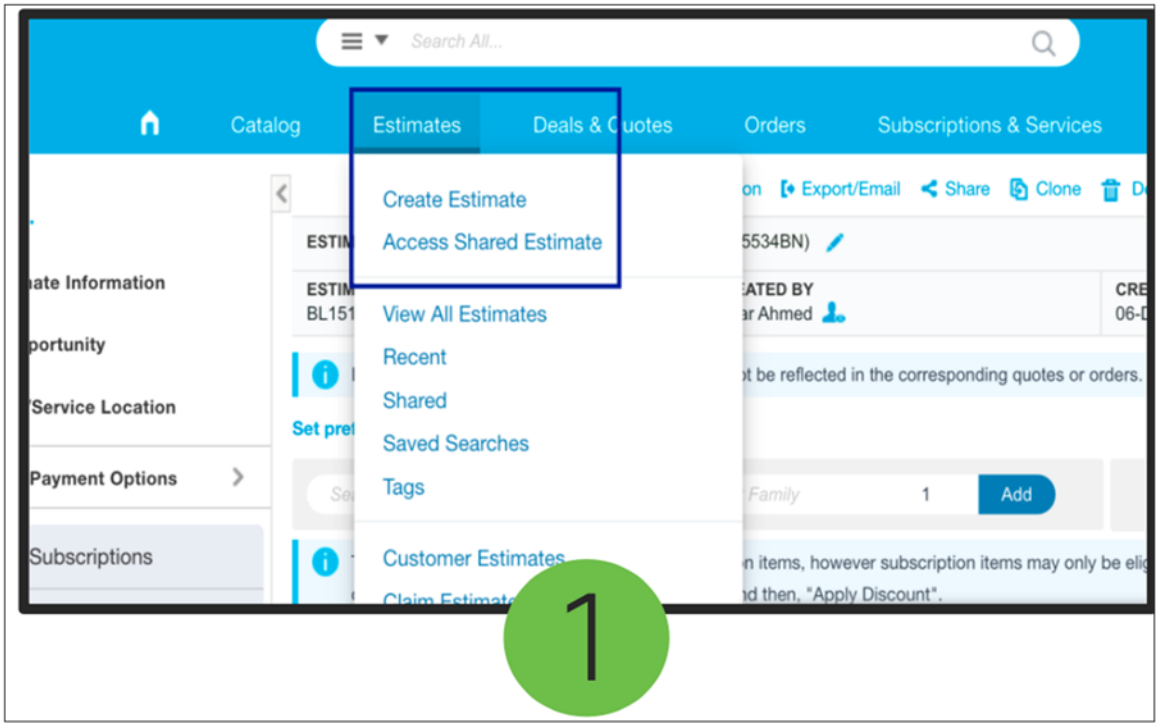

© 2026 Cisco and/or its affiliates. All rights reserved.

**Step 8:** Adding Spares. Navigate back to Products -> Security -> Cisco Secure Firewall 4200 Series -> Accessories and Spares -> Cisco Firepower 4225 Security Appliance -> Accessories and Spares -> L-FPR4225T-TMC= -> Click Add to Cart. The spare license is added to cart. The final product summary shown below.



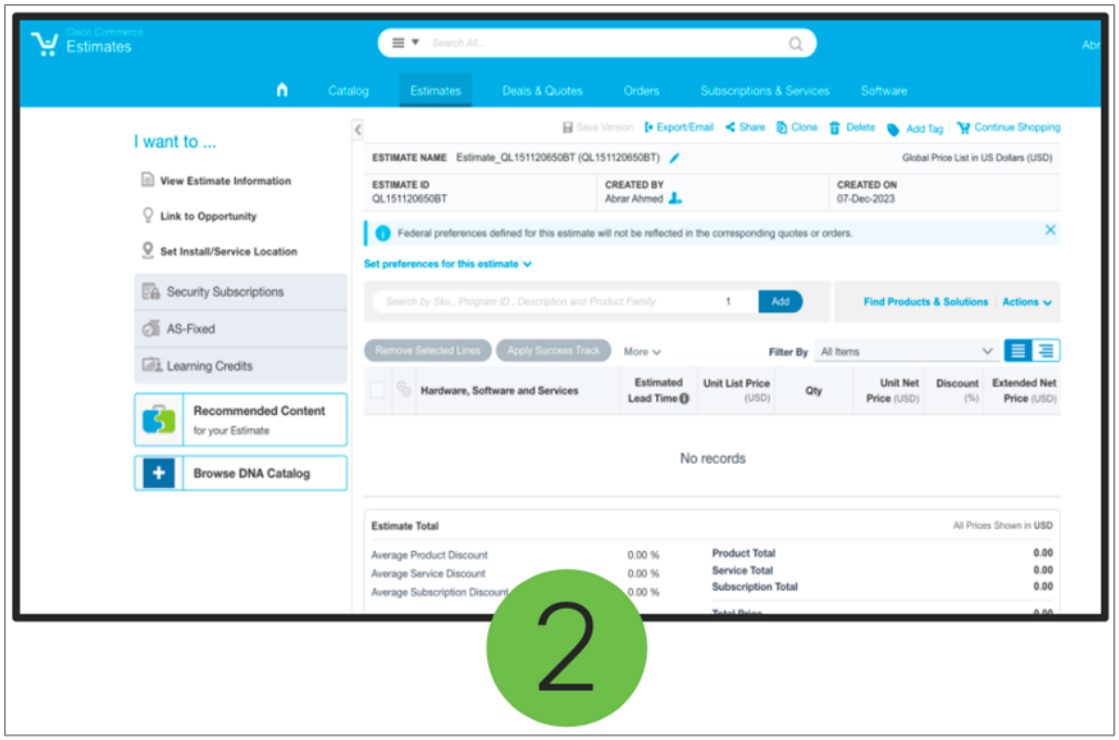

**4200 Firewall Solution Attached Services Ordering Example**

1. In Cisco Commerce Workspace (CCW), click Estimate dropdown. Select Create Estimate.

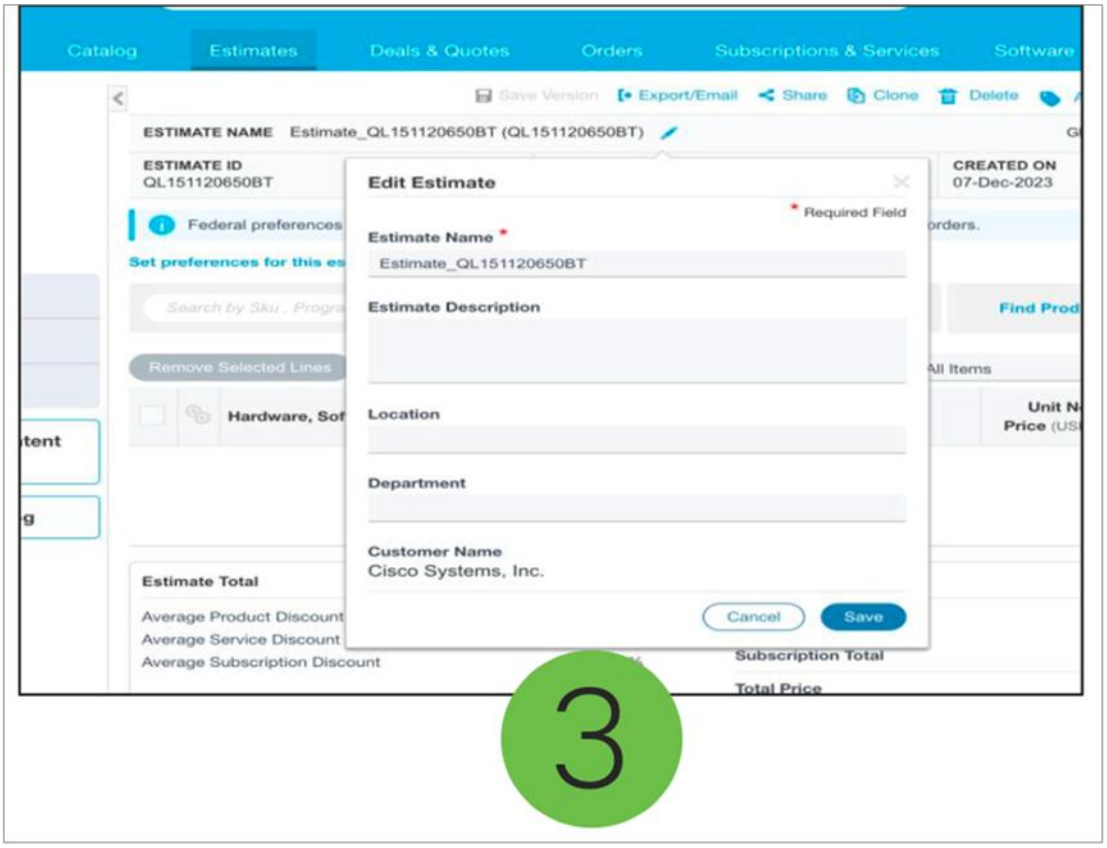



© 2026 Cisco and/or its affiliates. All rights reserved.

2. On the estimate page, complete all necessary fields



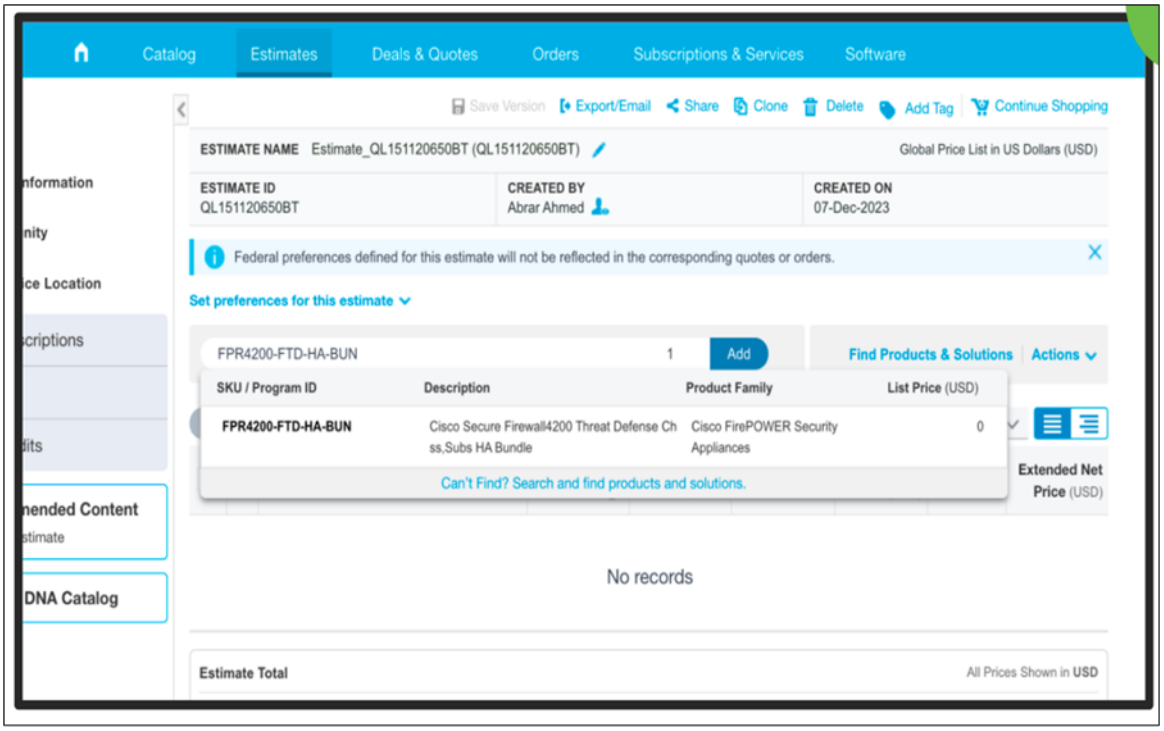

3. Click Edit Estimate tab. Complete fields on page. Click Save and Continue when done

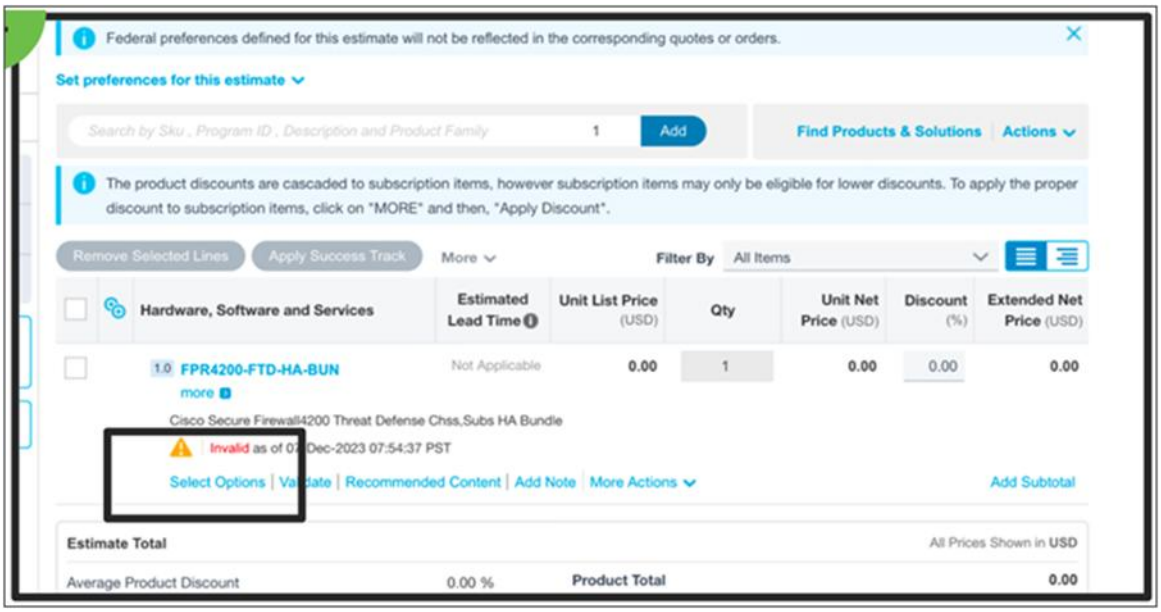



© 2026 Cisco and/or its affiliates. All rights reserved.

4. Under the Estimate tab:

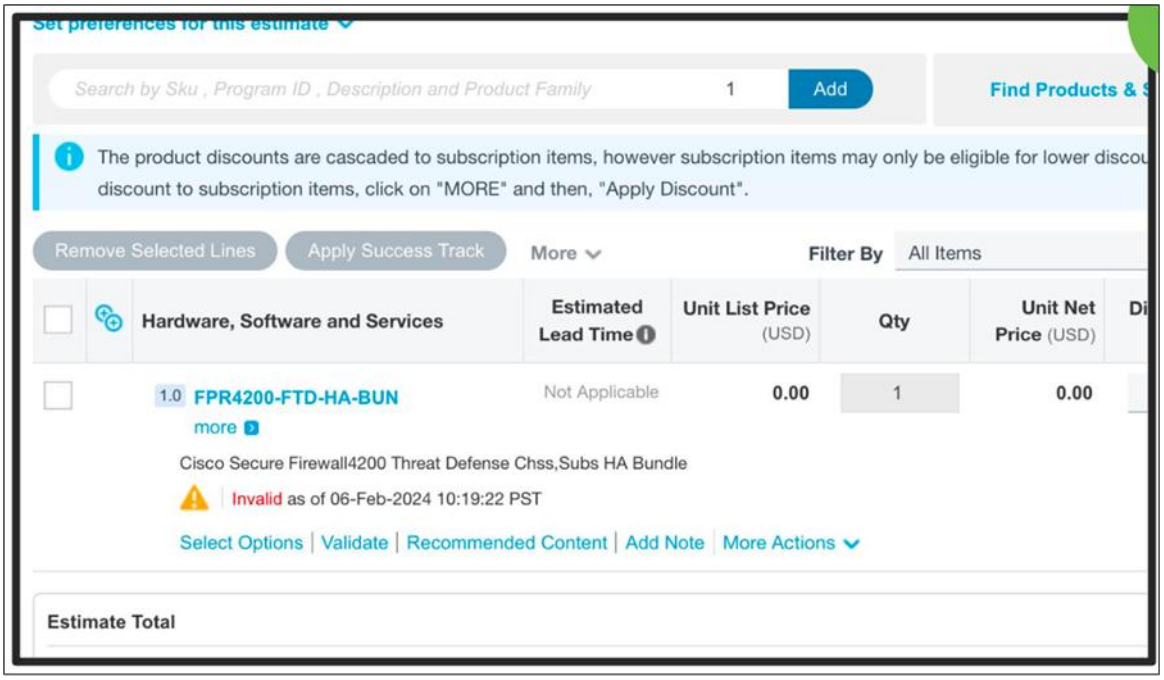
- Enter FPR4200-FTD-HA-BUN into Search field.
- Click Add.
- Select a Select Options.



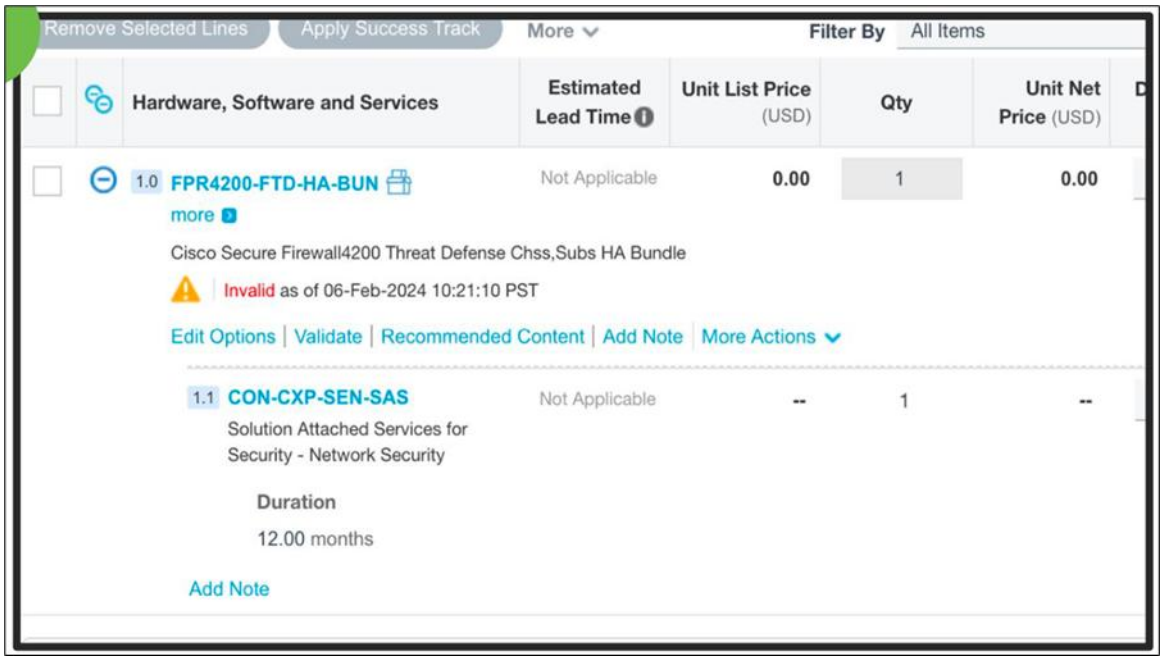

© 2026 Cisco and/or its affiliates. All rights reserved.

5. The CON-CXP-SEN-SAS SKU pricing will take a few seconds refresh and displays a message "The Advanced Services SKU in the bundle is being priced."




6. Click Save and Continue to price the MLB.

- Review the estimate pricing.
- Any additional changes made will require user to click Save and Continue again




**SKUs and Ordering for Cisco Secure Firewall 6100 Series**

The following tables outline the product part number information for the Cisco Secure Firewall 6100 Series. Note that the customer may want extra power supplies and fans.

© 2026 Cisco and/or its affiliates. All rights reserved.

**Table 52.** 6100 Series chassis part numbers

| Part Number | Description |
|---|---|
| **CSF6120-A-ASA-K9** | Cisco Secure Firewall 6120 Appliance, ASA |
| **CSF6130-A-ASA-K9** | Cisco Secure Firewall 6130 Appliance, ASA |
| **CSF6160-A-ASA-K9** | Cisco Secure Firewall 6160 Appliance, ASA |
| **CSF6160-A-TD-K9** | Cisco Secure Firewall 6160 Appliance, Threat Defense |
| **CSF6170-A-ASA-K9** | Cisco Secure Firewall 6170 Appliance, ASA |
| **CSF6170-A-TD-K9** | Cisco Secure Firewall 6170 Appliance, Threat Defense |

**Note:** Use the bundle part number unless you have an explicit reason not to. the bundle pid ensures that all necessary components are purchased.

**Table 53.** 6100 Series network module part numbers

| Part Number | Description | Spare |
|---|---|---|
| **CSF6K-XNM-8X10G** | Cisco Secure Firewall 6100 8x10G SFP+ Netmod | CSF6K-XNM-8X10G= |
| **CSF6K-XNM-8X25G** | Cisco Secure Firewall 6100 8x25G SFP28 Netmod | CSF6K-XNM-8X25G= |
| **CSF6K-XNM-4X40G** | Cisco Secure Firewall 6100 4x40G QSFP+ Netmod | CSF6K-XNM-4X40G= |
| **CSF6K-XNM-4X200G** | Cisco Secure Firewall 6100 4x200G QSFP56 Netmod | CSF6K-XNM-4X200G= |
| **CSF6K-XNM-2X100G** | Cisco Secure Firewall 6100 2x100G QSFP28 Netmod | CSF6K-XNM-2X100G= |
| **CSF6K-XNM-2X400G** | Cisco Secure Firewall 6100 2x400G QSFP-DD Netmod | CSF6K-XNM-2X400G= |
| **CSF6K-XNM-8X1GF** | Cisco Secure Firewall 6100 8x1G Copper FTW Netmod, RJ-45 | CSF6K-XNM-8X1GF= |
| **CSF6K-XNM-6X1SXF** | Cisco Secure Firewall 6100 6x1G FTW Netmod, SX multimode | CSF6K-XNM-6X1SXF= |
| **CSF6K-XNM-6X10SRF** | Cisco Secure Firewall 6100 6x10G FTW Netmod, SR multimode | CSF6K-XNM-6X10SRF= |
| **CSF6K-XNM-6X10LRF** | Cisco Secure Firewall 6100 6x10G FTW Netmod, LR single mode | CSF6K-XNM-6X10LRF= |

© 2026 Cisco and/or its affiliates. All rights reserved.

| Part Number | Description | Spare |
|---|---|---|
| **CSF6K-XNM-6X25SRF** | Cisco Secure Firewall 6100 6x25G FTW Netmod, SR multimode | CSF6K-XNM-6X25SRF= |
| **CSF6K-XNM-6X25LRF** | Cisco Secure Firewall 6100 6x25G FTW Netmod, LR single mode | CSF6K-XNM-6X25LRF= |
| **CSF6K-XNM-2X100SRF** | Cisco Secure Firewall 6100 2x100G FTW Netmod, SR4 multimode | CSF6K-XNM2X100SRF= |
| **CSF6100-NM-BLANK** | Cisco Secure Firewall 6100 Network Module Blank Slot Cover | CSF6100-NM-BLANK= |

**Table 54.** 6100 Series accessories part numbers

| Part Number | Description | Spare |
|---|---|---|
| **CSF6100-PWR-AC** | Cisco Secure Firewall 6100 Series AC/HVAC/HVDC Power Supply | CSF6100-PWR-AC= |
| **CSF6100-PWR-DC** | Cisco Secure Firewall 6100 Series 48V DC Power Supply | CSF6100-PWR-DC= |
| **–** | Cisco Secure Firewall 6100 Series Chassis Power Blank Slot Cover | CSF6100-PSU-BLANK= |
| **CSF6100-FAN** | Cisco Secure Firewall 6100 Series Fan | CSF6100-FAN= |
| **CSF6100-SSD1800** | Cisco Secure Firewall 6100 Series 1.8 TB SSD/SED | CSF6100-SSD1800= |
| **CSF6100-SSD3600** | Cisco Secure Firewall 6100 Series 3.6 TB SSD/SED | CSF6100-SSD3600= |
| **CSF6100-SSD7200** | Cisco Secure Firewall 6100 Series 7.2 TB SSD/SED | CSF6100-SSD7200= |
| **CSF6100-SSD1800-F** | Cisco Secure Firewall 6100 Series FIPS compliant 1.8 TB SSD/SED | CSF6100-SSD1800-F= |
| **CSF6100-SSD3600-F** | Cisco Secure Firewall 6100 Series FIPS compliant 3.6 TB SSD/SED | CSF6100-SSD3600-F= |
| **CSF6100-SSD7200-F** | Cisco Secure Firewall 6100 Series FIPS compliant 7.2 TB SSD/SED | CSF6100-SSD7200-F= |
| **CSF6100-MEM-C1X32** | Memory DIMM for Secure Firewall 6120 and 6130 CPU – 1x32 GB | CSF6100-MEM-C1X32= |
| **CSF6100-MEM-C1X64** | Memory DIMM for Cisco Secure Firewall 6160 CPU – 1x64 GB | CSF6100-MEM-C1X64= |
| **CSF6100-MEM-C1X96** | Memory DIMM for Cisco Secure Firewall 6170 CPU – 1x96 GB | CSF6100-MEM-C1X96= |
| **–** | Memory kit for Cisco Secure Firewall 6120 CPU – 12x32 GB | CSF61H-MEM-C12X32= |
| **–** | Memory kit for Cisco Secure Firewall 6130 CPU – 24x32 GB | CSF61H-MEM-C24X32= |
| **–** | Memory kit for Cisco Secure Firewall 6160 CPU – 24x64 GB | CSF61H-MEM-C24X64= |
| **–** | Memory kit for Cisco Secure Firewall 6170 CPU – 24x96 GB | CSF61H-MEM-C24X96= |
| **CSF6100-ACC-KIT** | Cisco Secure Firewall 6100 HW Accessory Kit (rack mounts, cables) | CSF6100-ACC-KIT= |
| **CSF6100-CBL-MGMT** | Cisco Secure Firewall 6100 Cable Management Brackets | CSF6100-CBL-MGMT= |
| **CSF6100-SLD-RAILS** | Cisco Secure Firewall 6100 Slide Rail Kit | CSF6100-SLD-RAILS= |

© 2026 Cisco and/or its affiliates. All rights reserved.

| Part Number | Description | Spare |
|---|---|---|
| **CSF6100-NM-BLANK** | Cisco Secure Firewall 6100 Network Module Blank Slot Cover | CSF6100-NM-BLANK= |
| **–** | Cisco Secure Firewall 6100 Series FIPS Kit | CSF6100-FIPS-KIT= |
| **–** | Cisco Secure Firewall 6100 Series Power Backplane Assembly | CSF6100-PBP= |

**Note:** Use these part numbers if the customer is ordering spare fans, power supplies, or a rack mount kit.

#### SKUs for 6100 Series Licenses and Subscriptions

When ordering a 6100 Series firewall with the ASA configuration, a license is required. When ordering a 6100 Series hardware with the Cisco Secure Firewall Threat Defense image, both licenses and a subscription to optional security services are required. Subscription terms are 1, 3, and 5 years, with the greatest price discount at 5 years. In the listed part numbers, the threat services are identified as follows:

**Table 55.** Cisco Secure Firewall 6100 Series license part numbers for configurations with the ASA image

| Part Number | Description |
|---|---|
| **CSF6100-ASASC-10** | Cisco Secure Firewall 6100 - Add 10 Security Context License |
| **CSF6100-ASA-CAR** | Cisco Secure Firewall 6100 ASA Carrier License |
| **CSF6100-ENC-K9** | Cisco Secure Firewall 6100 Strong Encryption (3DES/AES) |

**Table 56.** Threat Subscription Details

| Threat Subscription Abbreviations | Description |
|---|---|
| **T** | Threat (Security Intelligence and IPS) |
| **M or AMP*** | Malware defense |
| **C or URL*** | URL Filtering |
| **1Y** | **1-Year** Subscription |
| **3Y** | **3-Year** Subscription |
| **5Y** | **5-Year** Subscription |
| **CAR** | Carrier (GTP, SCTP and Diameter inspection) |

*Note that Threat/IPS (T) License is a requirement for the use of Malware (M) or URL (C) license features.

**Table 57.** Cisco Secure Firewall 6100 Series license part numbers for configurations with the Cisco Secure Firewall Threat Defense Image

| Part Number | Description |
|---|---|
| **L-CSF6160T-T=** | Cisco Secure Firewall 6160 Threat Defense License |

© 2026 Cisco and/or its affiliates. All rights reserved.

| Part Number | Description |
|---|---|
| **L-CSF6160T-TC=** | Cisco Secure Firewall 6160 Threat Defense and URL License |
| **L-CSF6160T-TM=** | Cisco Secure Firewall 6160 Threat Defense, Malware License |
| **L-CSF6160T-TMC=** | Cisco Secure Firewall 6160 TD, Malware and URL License |
| **L-CSF6160T-AMP=** | Cisco Secure Firewall 6160 Adv Malware Protection License |
| **L-CSF6160T-URL=** | Cisco Secure Firewall 6160 URL Filtering License |
| **L-CSF6170T-T=** | Cisco Secure Firewall 6170 Threat Defense License |
| **L-CSF6170T-TC=** | Cisco Secure Firewall 6170 Threat Defense and URL License |
| **L-CSF6170T-TM=** | Cisco Secure Firewall 6170 Threat Defense, Malware License |
| **L-CSF6170T-TMC=** | Cisco Secure Firewall 6170 TD, Malware and URL License |
| **L-CSF6170T-AMP=** | Cisco Secure Firewall 6170 Adv Malware Protection License |
| **L-CSF6170T-URL=** | Cisco Secure Firewall 6170 URL Filtering License |
| **L-CSF6100-FTD-CAR=** | Cisco Secure Firewall 6100 Threat Defense Carrier License |
| **L-CSF6100-TDENCK9=** | Cisco Secure Firewall 6100 Threat Defense Strong Encryption (3DES/AES) |
| **L-CSF6100-TDULRK9=** | Cisco Secure Firewall 6100 Threat Defense Universal License |

**Table 58.** Cisco Secure Firewall 6100 Series subscription part numbers for configurations with the Threat Defense image

| Part Number | Description |
|---|---|
| **L-CSF6160T-T-1Y/3Y/5Y** | Cisco Secure Firewall 6160 Threat Defense License subscription |
| **L-CSF6160T-TC-1Y/3Y/5Y** | Cisco Secure Firewall 6160 Threat Defense and URL License subscription |
| **L-CSF6160T-TM-1Y/3Y/5Y** | Cisco Secure Firewall 6160 Threat Defense, Malware License subscription |
| **L-CSF6160T-TMC-1Y/3Y/5Y** | Cisco Secure Firewall 6160 TD, Malware and URL License subscription |
| **L-CSF6160T-AMP-1Y/3Y/5Y** | Cisco Secure Firewall 6160 Malware Protection subscription |
| **L-CSF6160T-URL-1Y/3Y/5Y** | Cisco Secure Firewall 6160 URL Filtering subscription |
| **L-CSF6170T-T-1Y/3Y/5Y** | Cisco Secure Firewall 6170 Threat Defense License subscription |
| **L-CSF6170T-TC-1Y/3Y/5Y** | Cisco Secure Firewall 6170 Threat Defense and URL License subscription |
| **L-CSF6170T-TM-1Y/3Y/5Y** | Cisco Secure Firewall 6170 Threat Defense, Malware License subscription |
| **L-CSF6170T-TMC-1Y/3Y/5Y** | Cisco Secure Firewall 6170 TD, Malware and URL License subscription |
| **L-CSF6170T-AMP-1Y/3Y/5Y** | Cisco Secure Firewall 6170 Malware Protection subscription |

© 2026 Cisco and/or its affiliates. All rights reserved.

| Part Number | Description |
|---|---|
| **L-CSF6170T-URL-1Y/3Y/5Y** | Cisco Secure Firewall 6170 URL Filtering subscription |
| **CSF6100-FTD-CAR-1Y/3Y/5Y** | Cisco Secure Firewall 6100 Series Carrier License for FTD subscription |
| **CSF-NO-SUBS** | No Threat Defense Subscription |

**Table 59.** Cisco Secure Firewall 6100 Series power cords

| Part Number | Country and Description |
|---|---|
| **NO-PWR-CORD** | No power cord chosen |
| **CAB-AC-16A-SG-AR** | Argentina IRSM 2073 / Saf-D-Grid 250VAC 16A |
| **CAB-AC-16A-SG-AZ** | Australia and New Zealand AU20LS3 / Saf-D-Grid 250VAC 16A |
| **CAB-AC-16A-SG-BR** | Brazil EL224 / Saf-D-Grid 250VAC 16A |
| **CAB-AC-16A-SG-CH** | China GB 16C / Saf-D-Grid 250VAC 16A |
| **CAB-AC-16A-SG-EU** | Europe CEE 7-7 / Saf-D-Grid 250VAC 16A |
| **CAB-AC-16A-SG-IN** | India IEC60309 / Saf-D-Grid 250VAC 16A |
| **CAB-AC-16A-SG-IND** | India SABS 164-1 / Saf-D-Grid 250VAC 16A |
| **CAB-AC-16A-SG-IS** | Israel SI 16S3 / Saf-D-Grid 250VAC 16A |
| **CAB-AC-16A-SG-IT** | Italy CEI 23-50 / Saf-D-Grid to IEC-C19 250VAC 16A |
| **CAB-AC-16A-SG-SA** | South Africa EL / Saf-D-Grid 250VAC 16A |
| **CAB-AC-16A-SG-SK** | Korea Src / Saf-D-Grid 250VAC 16A |
| **CAB-AC-16A-SG-SW** | Switzerland SEV 5934-2 / Saf-D-Grid 250VAC 16A |
| **CAB-AC-16A-SG-UK** | United Kingdom IEC60309 / Saf-D-Grid 250VAC 16A |
| **CAB-AC-20A-NA** | Power cord, Saf-D-Grid / C20 20A |
| **CAB-AC-20A-SG-C20** | North America cabinet jumper PDU, IEC C20 / Saf-D-Grid 250VAC 20A |
| **CAB-AC-20A-SG-US** | North America straight blade, NEMA 5-20P / Saf-D-Grid 110VAC 20A |

© 2026 Cisco and/or its affiliates. All rights reserved.

| Part Number | Country and Description |
|---|---|
| **CAB-AC-20A-SG-US1** | North America twist lock, NEMA L5-20 / Saf-D-Grid 125VAC 20A |
| **CAB-AC-20A-SG-US2** | North America straight blade, NEMA 6-20 / Saf-D-Grid 250VAC 20A |
| **CAB-AC-20A-SG-US3** | North America twist lock, NEMA L6-20 / Saf-D-Grid 250VAC 20A |
| **CAB-AC-20A-SG-US4** | North America NEMA L7-20P / Saf-D-Grid 277VAC 20A |

**SKUs and Ordering for Cisco Firepower 9300**

The following tables outline the product part number information for the Cisco Firepower 9300. Note that the customer may want extra power supplies and fans. You can add these to the order separately. When you order, you choose between one and three security modules per chassis. Note that security module types cannot be mixed within a chassis.

**Table 60.** Chassis and sublevel assemblies and components included with each chassis

| Part Number (Chassis Hardware) | Description |
|---|---|
| **FPR-C9300-AC** | Cisco Firepower 9300 AC Chassis - includes 2 power supply units + 4 fans + rack-mount kit (3RU; accommodates up to three security modules) |
| **FPR-C9300-DC** | Cisco Firepower 9300 DC Chassis - includes 2 power supply units + 4 fans + rack-mount kit (3RU; accommodates up to three security modules) |
| **FPR-C9300-HVDC** | Cisco Firepower 9300 high-voltage DC Chassis - includes 2 power supply units + 4 fans + rack-mount kit (3RU; accommodates up to three security modules) |
| **FPR-C9300-AC=** | Cisco Firepower 9300 AC Chassis Spare – without power supply and fans |
| **FPR-C9300-DC=** | Cisco Firepower 9300 DC Chassis Spare – without power supply and fans |
| **FPR9K-PS-AC=** | Cisco Firepower 9000 Series AC Power Supply (order for spare only) |
| **FPR9K-PS-DC=** | Cisco Firepower 9000 Series DC Power Supply (order for spare only) |
| **FPR9K-FAN=** | Cisco Firepower 9000 Series Fan (order for spare only) |
| **FPR9K-RMK=** | Cisco Firepower 9000 Series Rack Mount Kit (order for spare only) |
| **FPR9K-SUP=** | Cisco Firepower 9000 Series Supervisor Spare |

| Part Number (Security Modules) | Description |
|---|---|
| **FPR9K-SM-40=** | Cisco Firepower 9000 Series, Security Module 40 Spare, includes 2 SSDs |
| **FPR9K-SM-48=** | Cisco Firepower 9000 Series, Security Module 48 Spare, includes 2 SSDs |
| **FPR9K-SM-56=** | Cisco Firepower 9000 Series, Security Module 56 Spare, includes 2 SSDs |
| **FPR9K-FTD-BUN** | Cisco FPR9300 Threat Defense Bundle for Security Modules |

© 2026 Cisco and/or its affiliates. All rights reserved.

| Part Number (Security Modules) | Description |
|---|---|
| **FPR9K-SM40-FTD-BUN** | Cisco FPR9300 SM-40 Threat Defense Chassis, Subs HA Bundle |
| **FPR9K-SM48-FTD-BUN** | Cisco FPR9300 SM-48 Threat Defense Chassis, Subs HA Bundle |
| **FPR9K-SM56-FTD-BUN** | Cisco FPR9300 SM-56 Threat Defense Chassis, Subs HA Bundle |
| **Breakout Cables** | Generic breakout cables can be used, please see: https://www.cisco.com/c/en/us/products/collateral/interfaces-modules/transceiver-modules/data_sheet_c78-660083.html |

**Note:** There are eight 10-Gbps ports on the supervisor module bundled by default with the chassis. However, customers that plan to use supervisor module ports will require connectors for both those ports as well as for the ports on the network modules. Only one 1-Gbps connector, for the management port, is included by default with each supervisor module.

**Table 61.** Cisco Firepower 9300 Network Modules

| Network Modules | Description |
|---|---|
| **FPR9K-NM-4X40G** | Firepower 9000 Series – 4 port QSFP+ Network Module |
| **FPR9K-NM-4X40G=** | Firepower 9000 Series – 4 port QSFP+ Network Module |
| **FPR9K-NM-8X10G** | Firepower 9000 Series – 8 port SFP+ Network Module |
| **FPR9K-NM-8X10G=** | Firepower 9000 Series – 8 port SFP+ Network Module |
| **FPR9K-DNM-2X100G** | Cisco FirePower 2 port 100G Network Module, Double Width |
| **FPR9K-DNM-2X100G=** | Cisco FirePower 2 port 100G Network Module, Double Width |
| **FPR9K-NM-2X100G** | Cisco FirePower 2 port 100G Network Module |
| **FPR9K-NM-2X100G=** | Cisco FirePower 2 port 100G Network Module |
| **FPR9K-NM-4X100G** | Cisco FirePower 4 port 100G Network Module |
| **FPR9K-NM-4X100G=** | Cisco FirePower 4 port 100G Network Module |
| **FPR9K-NM-6X10SR-F** | 10G Short range Fail to Wire Network Module (includes built-in SFP) |
| **FPR9K-NM-6X10SR-F=** | 10G Short range Fail to Wire Spare Network Module (includes built-in SFP) |
| **FPR9K-NM-6X10LR-F** | 10G Long range Fail to Wire Network Module (includes built-in SFP) |
| **FPR9K-NM-6X10LR-F=** | 10G Long range Fail to Wire Spare Network Module (includes built-in SFP) |

© 2026 Cisco and/or its affiliates. All rights reserved.

| Network Modules | Description |
|---|---|
| **FPR9K-NM-2X40G-F** | 40G Fail to Wire Network Module (includes built-in QSFP) |
| **FPR9K-NM-2X40G-F=** | 40G Fail to Wire Spare Network Module (includes built-in QSFP) |
| **FPR9K-NM-6X1SX-F** | Cisco Firepower 6-port 1G SX Fiber FTW Network Module (includes built-in SFP) |
| **FPR9K-NM-6X1SX-F=** | Cisco Firepower 6-port 1G SX Fiber FTW Network Module (Spare) (includes built-in SFP) |

**Table 62.** SFP module options for 10G netmod and 10G supervisor ports

| Part Number (SFP Modules) SKU | Description |
|---|---|
| **SFP-10G-SR** | 10GBASE-SR SFP Module |
| **SFP-10G-LR** | 10GBASE-LR SFP Module |
| **SFP-10G-SR-S** | 10GBASE-SR SFP Module, Enterprise-Class |
| **SFP-10G-LR-S** | 10GBASE-LR SFP Module, Enterprise-Class |
| **SFP-10G-LRM** | 10GBASE-LRM SFP Module |
| **SFP-10G-ER** | 10GBASE-ER SFP Module |
| **SFP-H10GB-CU1M** | 10GBASE-CU SFP+ Cable 1m |
| **SFP-H10GB-CU3M** | 10GBASE-CU SFP+ Cable 3m |
| **SFP-H10GB-CU5M** | 10GBASE-CU SFP+ Cable 5m |
| **SFP-H10GB-ACU7M** | Active Twinax cable assembly, 7m |
| **SFP-H10GB-ACU10M** | Active Twinax cable assembly, 10m |
| **SFP-10G-AOC1M** | 10GBASE Active Optical SFP+ Cable, 1m |
| **SFP-10G-AOC2M** | 10GBASE Active Optical SFP+ Cable, 2m |
| **SFP-10G-AOC3M** | 10GBASE Active Optical SFP+ Cable, 3m |
| **SFP-10G-AOC5M** | 10GBASE Active Optical SFP+ Cable, 5m |
| **SFP-10G-AOC7M** | 10GBASE Active Optical SFP+ Cable, 7m |
| **SFP-10G-AOC10M** | 10GBASE Active Optical SFP+ Cable, 10m |
| **GLC-SX-MMD** | 1000BASE-SX SFP transceiver module, MMF, 850nm, DOM |

© 2026 Cisco and/or its affiliates. All rights reserved.

| Part Number (SFP Modules) SKU | Description |
|---|---|
| **GLC-LH-SMD** | 1000BASE-LX/LH SFP transceiver module, MMF/SMF, 1310nm, DOM |
| **GLC-EX-SMD** | 1000BASE-EX SFP transceiver module, SMF, 1310nm, DOM |
| **GLC-ZX-SMD** | 1000BASE-ZX SFP transceiver module, SMF, 1550nm, DOM |

**Table 63.** SFP module options for 40G netmod

| Part Number (SFP Modules) | Description |
|---|---|
| **QSFP-40G-SR4** | 40GBASE-SR4 QSFP Transceiver Module with MPO Connector |
| **QSFP-40G-CSR4** | QSFP 4x10GBASE-SR Transceiver Module, MPO, 300M |
| **QSFP-40G-SR-BD** | QSFP40G BiDi Short-reach Transceiver |
| **QSFP-40G-LR4-S** | QSFP 40GBASE-LR4 Transceiver Mod, LC, 10km, Enterprise-Class |
| **QSFP-40G-LR4** | QSFP 40GBASE-LR4 OTN Transceiver, LC, 10km |
| **WSP-Q40GLR4L** | QSFP 40G Ethernet - LR4 Lite, LC, 2KM |
| **QSFP-H40G-CU1M** | 40GBASE-CR4 Passive Copper Cable, 1m |
| **QSFP-H40G-CU3M** | 40GBASE-CR4 Passive Copper Cable, 3m |
| **QSFP-H40G-CU5M** | 40GBASE-CR4 Passive Copper Cable, 5m |
| **QSFP-H40G-AOC1M** | 40GBASE Active Optical Cable, 1m |
| **QSFP-H40G-AOC2M** | 40GBASE Active Optical Cable, 2m |
| **QSFP-H40G-AOC3M** | 40GBASE Active Optical Cable, 3m |
| **QSFP-H40G-AOC5M** | 40GBASE Active Optical Cable, 5m |
| **QSFP-H40G-AOC7M** | 40GBASE Active Optical Cable, 7m |
| **QSFP-H40G-AOC10M** | 40GBASE Active Optical Cable, 10m |
| **QSFP-H40G-AOC15M** | 40GBASE Active Optical Cable, 15m |
| **QSFP-H40G-ACU7M** | 40GBASE-CR4 Active Copper Cable, 7m |
| **QSFP-H40G-AOC10M** | 40GBASE-CR4 Active Copper Cable, 10m |

© 2026 Cisco and/or its affiliates. All rights reserved.

**Table 64.** 100G network QSFP28 module options

| Part Number (SFP Modules) | Description |
|---|---|
| **QSFP-100G-LR4-S** | 100GBASE LR4 QSFP Transceiver, LC, 10km over SMF |

When ordering a Cisco Firepower 9300 firewall with the ASA configuration, a Standard (base) ASA license (LF9KASA) is required.

**Table 65.** Cisco Firepower 9300 power cables

| Part Number (Power Cables) | Country | Description |
|---|---|---|
| **CAB-AC-2500W-INT** | International | Power Cord, 250VAC 16A, INTL |
| **CAB-C19-CBN** | International | Cabinet Jumper Power Cord, 250VAC 16A, C20-C19 Connectors |
| **CAB-AC-C6K-TWLK** | [All Categories] | Power Cord, 250VAC 16A, twist lock NEMA L6-20 plug, US |
| **CAB-AC-2500W-US1** | North America and Japan | Power Cord, 250VAC 16A, straight blade NEMA 6-20 plug, US |
| **CAB-AC-16A-AUS** | Australia | Power Cord, 250VAC, 16A, Australia C19 |
| **CAB-AC16A-CH** | China | 16A AC Power Cord for China |
| **CAB-AC-2500W-ISRL** | People's Republic of China | Power Cord, 250VAC, 16A, Israel |
| **CAB-S132-C19-ISRL** | Israel | S132 to IEC-C19 14ft Israeli |
| **CAB-ACS-16** | Switzerland | AC Power Cord (Swiss) 16A |
| **CAB-IR2073-C19-AR** | Argentina | IRSM 2073 to IEC-C19 14ft Argentina |
| **CAB-BS1363-C19-UK** | United Kingdom | BS-1363 to IEC-C19 14ft UK |
| **CAB-SABS-C19-IND** | India | SABS 164-1 to IEC-C19 India |
| **CAB-C2316-C19-IT** | Italy | CEI 23-16 to IEC-C19 14ft Italy |
| **UCSB-CABL-C19-BRZ** | Brazil | NBR 14136 to C19 AC 14ft Power Cord, Brazil |
| **CAB-C19-C20-3M-JP** | Japan | Power Cord C19-C20, 3m/10ft Japan PSE mark |
| **CAB-AC-2500W-INT** | International | Power Cord, 250VAC 16A, INTL |

© 2026 Cisco and/or its affiliates. All rights reserved.

**SKUs for Cisco Firepower 9300 Series Licenses and Firewall Threat Defense Subscriptions**

When ordering a Cisco Firepower 9300 firewall with the ASA configuration, a Standard (base) ASA license (L-F9K-ASA) is required.

Alternatively, when ordering a 9300 Series with the Cisco Secure Firewall Threat Defense image, base AVC capability comes by default with Cisco Secure Firewall Threat Defense license (L-FPR9K-TD-BASE=). Additionally, subscriptions can be purchased (one license per security module) to add IPS, URL Filtering, and malware defense capabilities. Similarly, if the customer already has a Firepower 9300, the same PIDs are used to upgrade to the Cisco Secure Firewall Threat Defense image. Subscription terms are 1, 3, and 5 years, with the greatest price discount at 5 years. In the listed part numbers, the threat services are identified as follows:

**Table 66.** Threat subscription decoder

| Threat Subscription Abbreviations | Description |
|---|---|
| **T** | Threat (Security Intelligence and IPS) |
| **M or AMP*** | Malware defense |
| **C or URL*** | URL Filtering |
| **1Y** | **1-Year** Subscription |
| **3Y** | **3-Year** Subscription |
| **5Y** | **5-Year** Subscription |

*Note that Threat/IPS (T) License is a requirement for the use of Malware (M) or URL (C) license features.

**Table 67.** Cisco Firepower 9300 Series license part numbers and subscription terms for Cisco Secure Firewall Threat Defense on Security Module SM-40

| PID | Description |
|---|---|
| **L-FPR9K-40T-T=** | Cisco FPR9K SM-40 Threat Defense Threat Protection License |
| **L-FPR9K-40T-AMP=** | Cisco FPR9K SM-40 Threat Defense Malware Protection License |
| **L-FPR9K-40T-URL=** | Cisco FPR9K SM-40 Threat Defense URL Filtering License |
| **L-FPR9K-40T-TM=** | Cisco FPR9K SM-40 Threat Defense Threat and Malware License |
| **L-FPR9K-40T-TC=** | Cisco FPR9K SM-40 Threat Defense Threat and URL License |
| **L-FPR9K-40T-TMC=** | Cisco FPR9K SM-40 Threat Defense Threat, Malware and URL License |
| **L-FPR9K-40T-AMP-1Y** | Cisco FPR9K SM-40 Threat Defense Malware Protection 1Y Subs |
| **L-FPR9K-40T-AMP-3Y** | Cisco FPR9K SM-40 Threat Defense Malware Protection 3Y Subs |
| **L-FPR9K-40T-AMP-5Y** | Cisco FPR9K SM-40 Threat Defense Malware Protection 5Y Subs |
| **L-FPR9K-40T-URL-1Y** | Cisco FPR9K SM-40 Threat Defense URL Filtering 1Y Subs |

© 2026 Cisco and/or its affiliates. All rights reserved.

| PID | Description |
|---|---|
| **L-FPR9K-40T-URL-3Y** | Cisco FPR9K SM-40 Threat Defense URL Filtering 3Y Subs |
| **L-FPR9K-40T-URL-5Y** | Cisco FPR9K SM-40 Threat Defense URL Filtering 5Y Subs |
| **L-FPR9K-40T-T-1Y** | Cisco FPR9K SM-40 Threat Defense Threat Protection 1Y Subs |
| **L-FPR9K-40T-T-3Y** | Cisco FPR9K SM-40 Threat Defense Threat Protection 3Y Subs |
| **L-FPR9K-40T-T-5Y** | Cisco FPR9K SM-40 Threat Defense Threat Protection 5Y Subs |
| **L-FPR9K-40T-TM-1Y** | Cisco FPR9K SM-40 Threat Defense Threat and Malware 1Y Subs |
| **L-FPR9K-40T-TM-3Y** | Cisco FPR9K SM-40 Threat Defense Threat and Malware 3Y Subs |
| **L-FPR9K-40T-TM-5Y** | Cisco FPR9K SM-40 Threat Defense Threat and Malware 5Y Subs |
| **L-FPR9K-40T-TC-1Y** | Cisco FPR9K SM-40 Threat Defense Threat and URL 1Y Subs |
| **L-FPR9K-40T-TC-3Y** | Cisco FPR9K SM-40 Threat Defense Threat and URL 3Y Subs |
| **L-FPR9K-40T-TC-5Y** | Cisco FPR9K SM-40 Threat Defense Threat and URL 5Y Subs |
| **L-FPR9K-40T-TMC-1Y** | Cisco FPR9K SM-40 Threat Defense Threat, Malware, URL 1Y Sub |
| **L-FPR9K-40T-TMC-3Y** | Cisco FPR9K SM-40 Threat Defense Threat, Malware, URL 3Y Sub |
| **L-FPR9K-40T-TMC-5Y** | Cisco FPR9K SM-40 Threat Defense Threat, Malware, URL 5Y Sub |

**Table 68.** Cisco Firepower 9300 Series license part numbers and subscription terms for Cisco Secure Firewall Threat Defense on Security Module SM-48

| FPR9K-SM-48 | Firepower 9000 Series High Performance Security Module |
|---|---|
| **L-FPR9K-48T-T=** | Cisco FPR9K SM-48 Threat Defense Threat Protection License |
| **L-FPR9K-48T-AMP=** | Cisco FPR9K SM-48 Threat Defense Malware Protection License |
| **L-FPR9K-48T-URL=** | Cisco FPR9K SM-48 Threat Defense URL Filtering License |
| **L-FPR9K-48T-TM=** | Cisco FPR9K SM-48 Threat Defense Threat and Malware License |
| **L-FPR9K-48T-TC=** | Cisco FPR9K SM-48 Threat Defense Threat and URL License |
| **L-FPR9K-48T-TMC=** | Cisco FPR9K SM-48 Threat Defense Threat, Malware and URL License |
| **L-FPR9K-48T-AMP-1Y** | Cisco FPR9K SM-48 Threat Defense Malware Protection 1Y Subs |
| **L-FPR9K-48T-AMP-3Y** | Cisco FPR9K SM-48 Threat Defense Malware Protection 3Y Subs |
| **L-FPR9K-48T-AMP-5Y** | Cisco FPR9K SM-48 Threat Defense Malware Protection 5Y Subs |
| **L-FPR9K-48T-URL-1Y** | Cisco FPR9K SM-48 Threat Defense URL Filtering 1Y Subs |
| **L-FPR9K-48T-URL-3Y** | Cisco FPR9K SM-48 Threat Defense URL Filtering 3Y Subs |

© 2026 Cisco and/or its affiliates. All rights reserved.

| FPR9K-SM-48 | Firepower 9000 Series High Performance Security Module |
|---|---|
| **L-FPR9K-48T-URL-5Y** | Cisco FPR9K SM-48 Threat Defense URL Filtering 5Y Subs |
| **L-FPR9K-48T-T-1Y** | Cisco FPR9K SM-48 Threat Defense Threat Protection 1Y Subs |
| **L-FPR9K-48T-T-3Y** | Cisco FPR9K SM-48 Threat Defense Threat Protection 3Y Subs |
| **L-FPR9K-48T-T-5Y** | Cisco FPR9K SM-48 Threat Defense Threat Protection 5Y Subs |
| **L-FPR9K-48T-TM-1Y** | Cisco FPR9K SM-48 Threat Defense Threat and Malware 1Y Subs |
| **L-FPR9K-48T-TM-3Y** | Cisco FPR9K SM-48 Threat Defense Threat and Malware 3Y Subs |
| **L-FPR9K-48T-TM-5Y** | Cisco FPR9K SM-48 Threat Defense Threat and Malware 5Y Subs |
| **L-FPR9K-48T-TC-1Y** | Cisco FPR9K SM-48 Threat Defense Threat and URL 1Y Subs |
| **L-FPR9K-48T-TC-3Y** | Cisco FPR9K SM-48 Threat Defense Threat and URL 3Y Subs |
| **L-FPR9K-48T-TC-5Y** | Cisco FPR9K SM-48 Threat Defense Threat and URL 5Y Subs |
| **L-FPR9K-48T-TMC-1Y** | Cisco FPR9K SM-48 Threat Defense Threat, Malware, URL 1Y Sub |
| **L-FPR9K-48T-TMC-3Y** | Cisco FPR9K SM-48 Threat Defense Threat, Malware, URL 3Y Sub |
| **L-FPR9K-48T-TMC-5Y** | Cisco FPR9K SM-48 Threat Defense Threat, Malware, URL 5Y Sub |

**Table 69.** Cisco Firepower 9300 Series license part numbers and subscription terms for Cisco Secure Firewall Threat Defense on Security Module SM-56

| FPR9K-SM-56 | Firepower 9000 Series Security Module 56 |
|---|---|
| **L-FPR9K-56T-T=** | Cisco FPR9K SM-56 Threat Defense Threat Protection License |
| **L-FPR9K-56T-AMP=** | Cisco FPR9K SM-56 Threat Defense Malware Protection License |
| **L-FPR9K-56T-URL=** | Cisco FPR9K SM-56 Threat Defense URL Filtering License |
| **L-FPR9K-56T-TM=** | Cisco FPR9K SM-56 Threat Defense Threat and Malware License |
| **L-FPR9K-56T-TC=** | Cisco FPR9K SM-56 Threat Defense Threat and URL License |
| **L-FPR9K-56T-TMC=** | Cisco FPR9K SM-56 Threat Defense Threat, Malware and URL License |
| **L-FPR9K-56T-AMP-1Y** | Cisco FPR9K SM-56 Threat Defense Malware Protection 1Y Subs |
| **L-FPR9K-56T-AMP-3Y** | Cisco FPR9K SM-56 Threat Defense Malware Protection 3Y Subs |
| **L-FPR9K-56T-AMP-5Y** | Cisco FPR9K SM-56 Threat Defense Malware Protection 5Y Subs |
| **L-FPR9K-56T-URL-1Y** | Cisco FPR9K SM-56 Threat Defense URL Filtering 1Y Subs |
| **L-FPR9K-56T-URL-3Y** | Cisco FPR9K SM-56 Threat Defense URL Filtering 3Y Subs |
| **L-FPR9K-56T-URL-5Y** | Cisco FPR9K SM-56 Threat Defense URL Filtering 5Y Subs |

© 2026 Cisco and/or its affiliates. All rights reserved.

| FPR9K-SM-56 | Firepower 9000 Series Security Module 56 |
|---|---|
| **L-FPR9K-56T-T-1Y** | Cisco FPR9K SM-56 Threat Defense Threat Protection 1Y Subs |
| **L-FPR9K-56T-T-3Y** | Cisco FPR9K SM-56 Threat Defense Threat Protection 3Y Subs |
| **L-FPR9K-56T-T-5Y** | Cisco FPR9K SM-56 Threat Defense Threat Protection 5Y Subs |
| **L-FPR9K-56T-TM-1Y** | Cisco FPR9K SM-56 Threat Defense Threat and Malware 1Y Subs |
| **L-FPR9K-56T-TM-3Y** | Cisco FPR9K SM-56 Threat Defense Threat and Malware 3Y Subs |
| **L-FPR9K-56T-TM-5Y** | Cisco FPR9K SM-56 Threat Defense Threat and Malware 5Y Subs |
| **L-FPR9K-56T-TC-1Y** | Cisco FPR9K SM-56 Threat Defense Threat and URL 1Y Subs |
| **L-FPR9K-56T-TC-3Y** | Cisco FPR9K SM-56 Threat Defense Threat and URL 3Y Subs |
| **L-FPR9K-56T-TC-5Y** | Cisco FPR9K SM-56 Threat Defense Threat and URL 5Y Subs |
| **L-FPR9K-56T-TMC-1Y** | Cisco FPR9K SM-56 Threat Defense Threat, Malware, URL 1Y Sub |
| **L-FPR9K-56T-TMC-3Y** | Cisco FPR9K SM-56 Threat Defense Threat, Malware, URL 3Y Sub |
| **L-FPR9K-56T-TMC-5Y** | Cisco FPR9K SM-56 Threat Defense Threat, Malware, URL 5Y Sub |

**Ordering Example: Cisco Firepower 9300 with ASA**

**Step 1:** Smart Software Licensing

Before placing a Cisco Firepower 9300 order, a Smart Software Licensing account for the end customer must be initiated. If the customer already has a Smart Software Licensing account, that account must be associated with the order. More information on Smart Software Licensing account establishment is available in the Smart Software Licensing section of this ordering guide, and online at: https://www.cisco.com/web/ordering/smart-software-manager/index.html.

To associate the order's licenses with the customer's Smart Licensing account, or to begin the establishment of the Smart Licensing account, follow these steps. Note that if you are initiating the account, you are able to complete the order only if the account is initiated on the end customer's behalf and associated with the order.

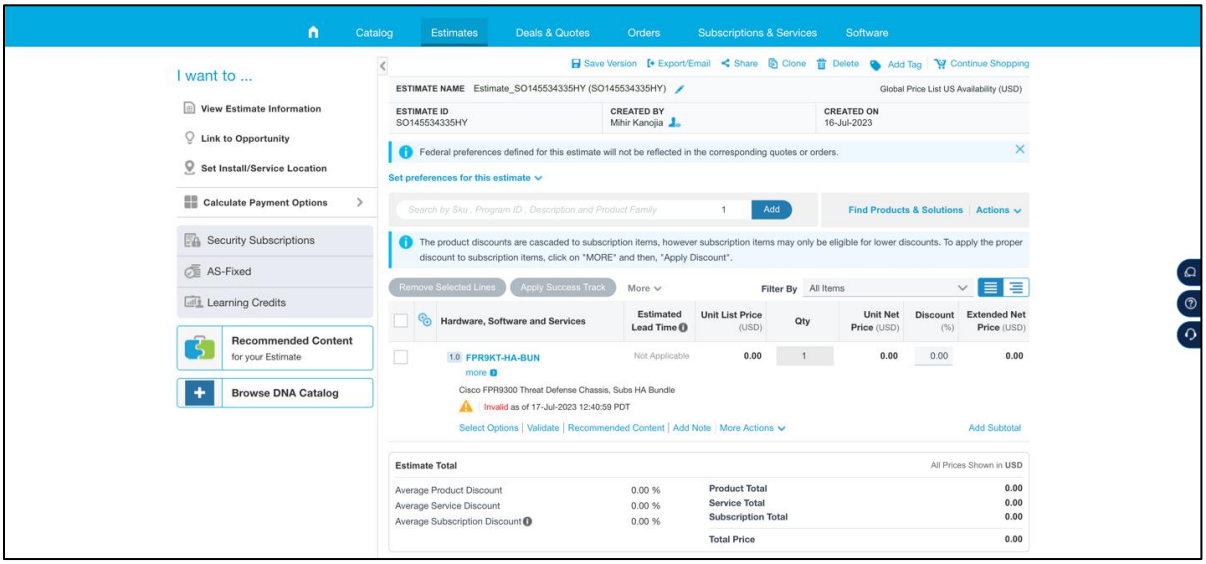
Go to Cisco Commerce: https://www.cisco.com/go/ccw.

From the Orders pull-down menu, select Create Order.

Select Assign Smart Account and follow the subsequent prompts for Smart Licensing.

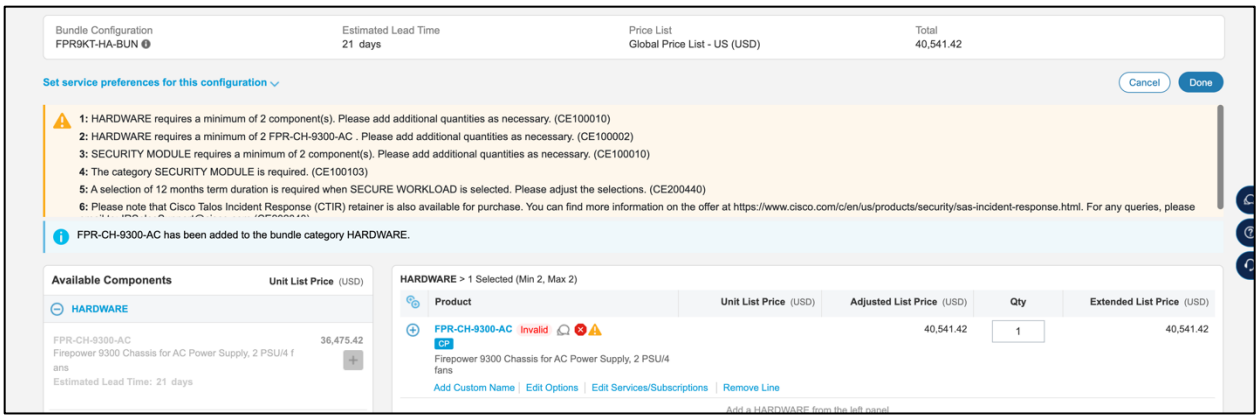
© 2026 Cisco and/or its affiliates. All rights reserved.

**Step 2:** Navigate to Catalog > Products > Security > Cisco Firepower 9300 Series -> Search for FPR9KT-HA-BUN. Add the chassis to the cart by clicking add.




**Step 3:** Check the box 1.0 FPR9KT-HA-BUN and select Options.

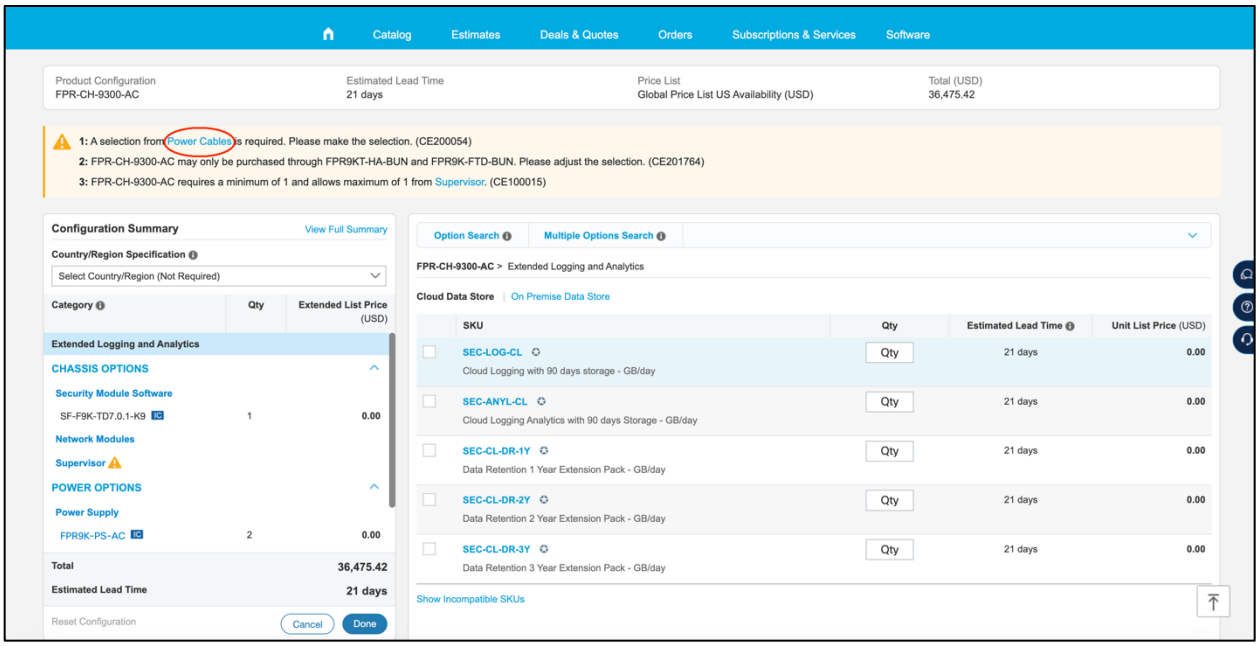
Follow the instructions in the yellow box. First click the hardware and make the selection.

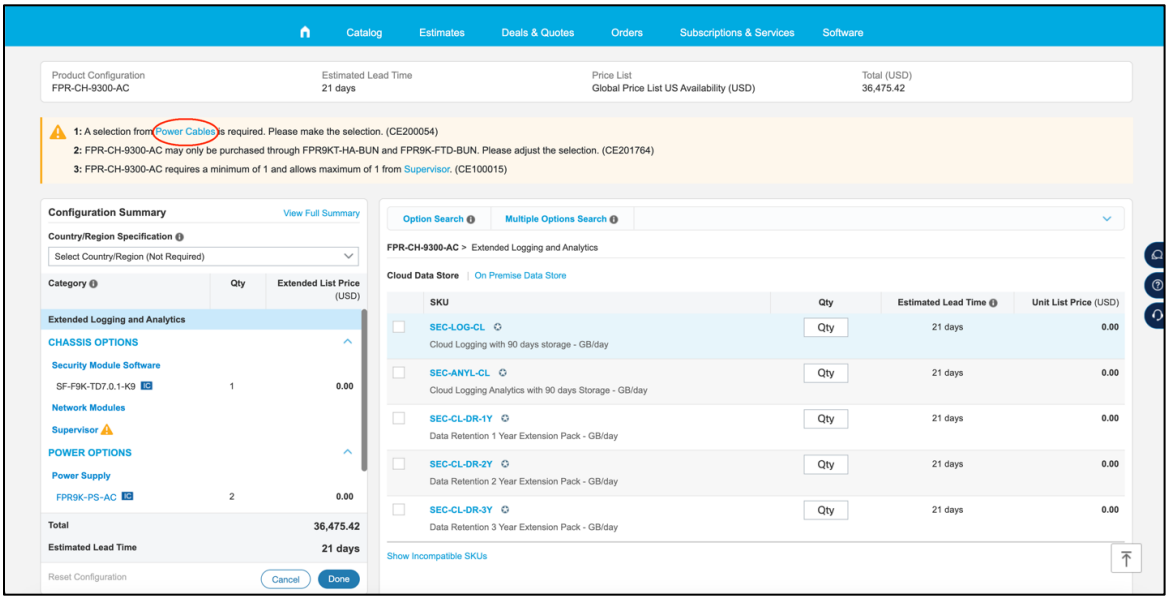



© 2026 Cisco and/or its affiliates. All rights reserved.

**Step 4:** Click on Edit Options in the FPR-CH-9300-AC Hardware and select the power cables, supervisor and network modules.

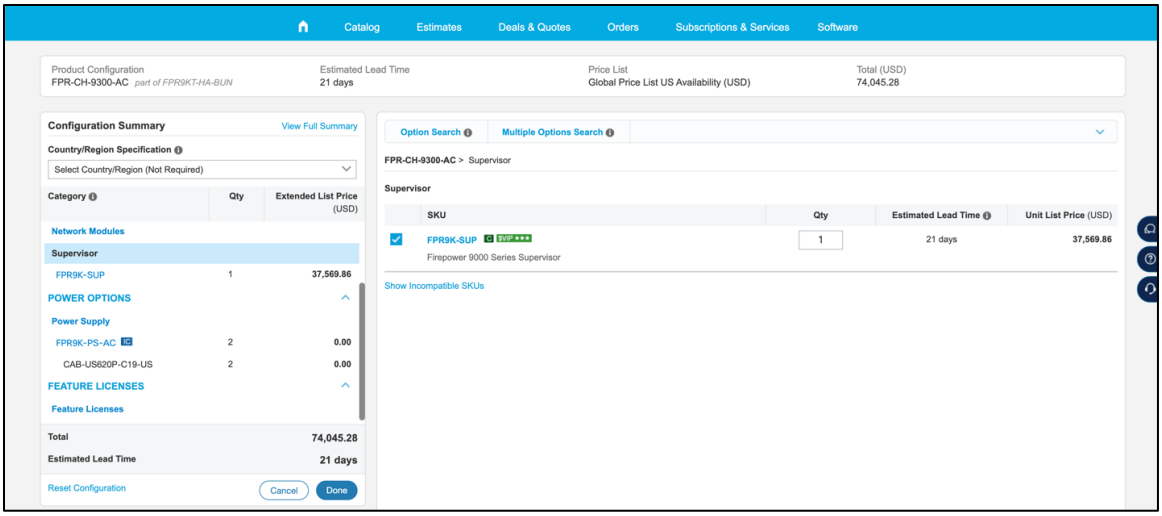
1. Power Cables Selection

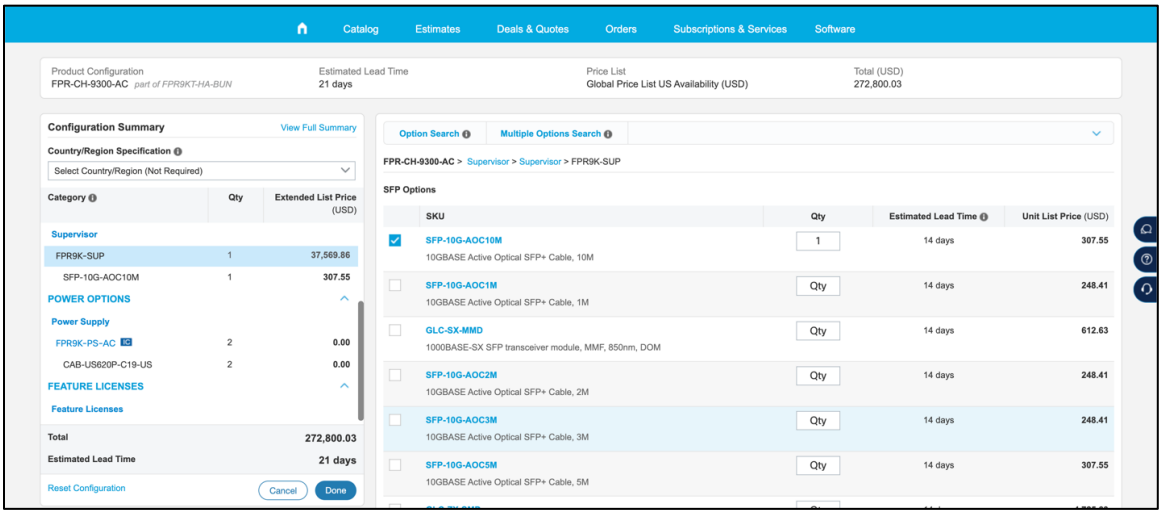


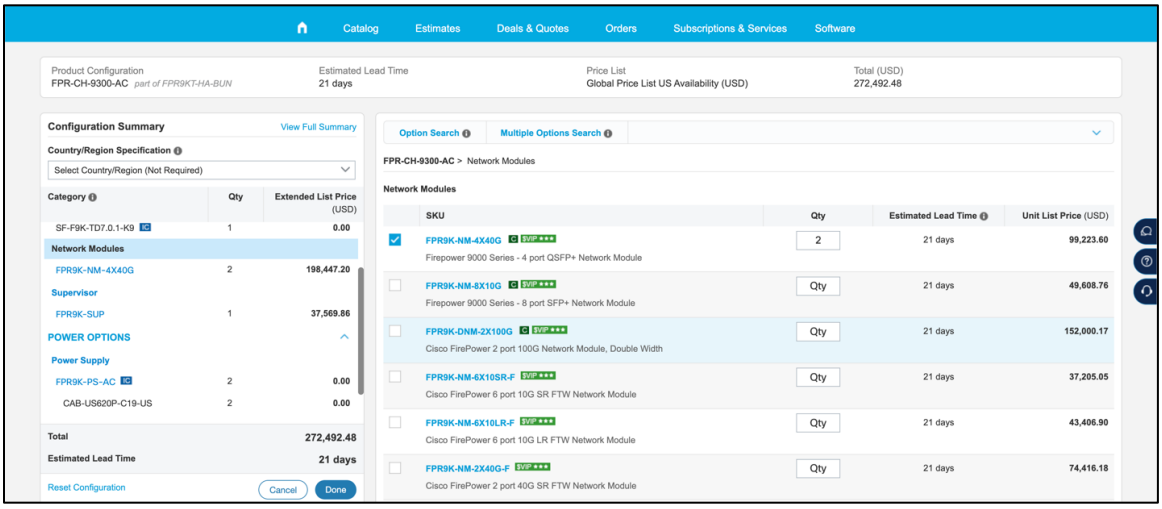

© 2026 Cisco and/or its affiliates. All rights reserved.

2. Supervisor Selection



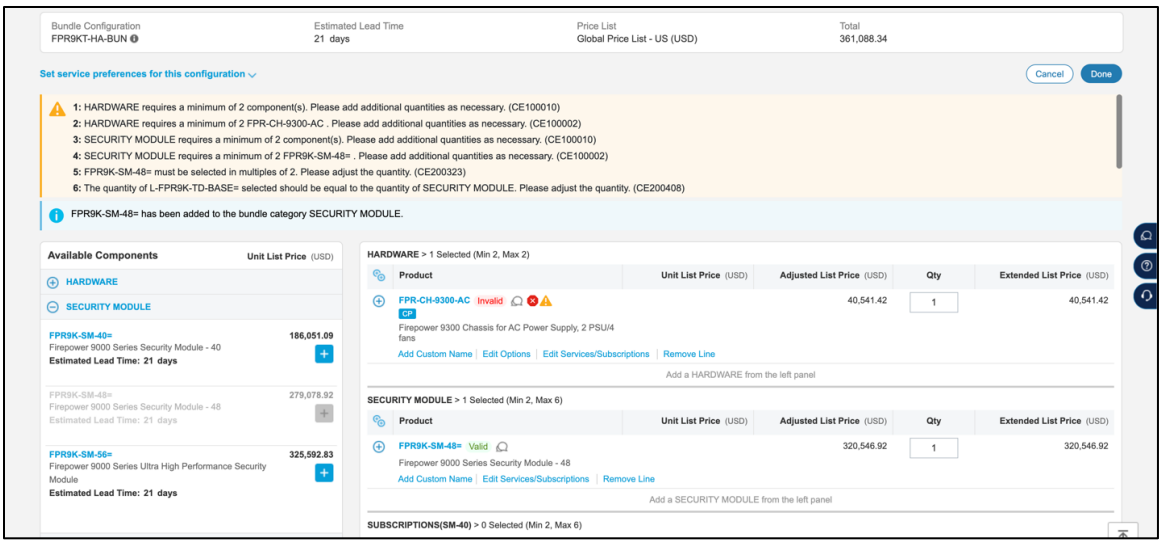




3. Network Module Selection

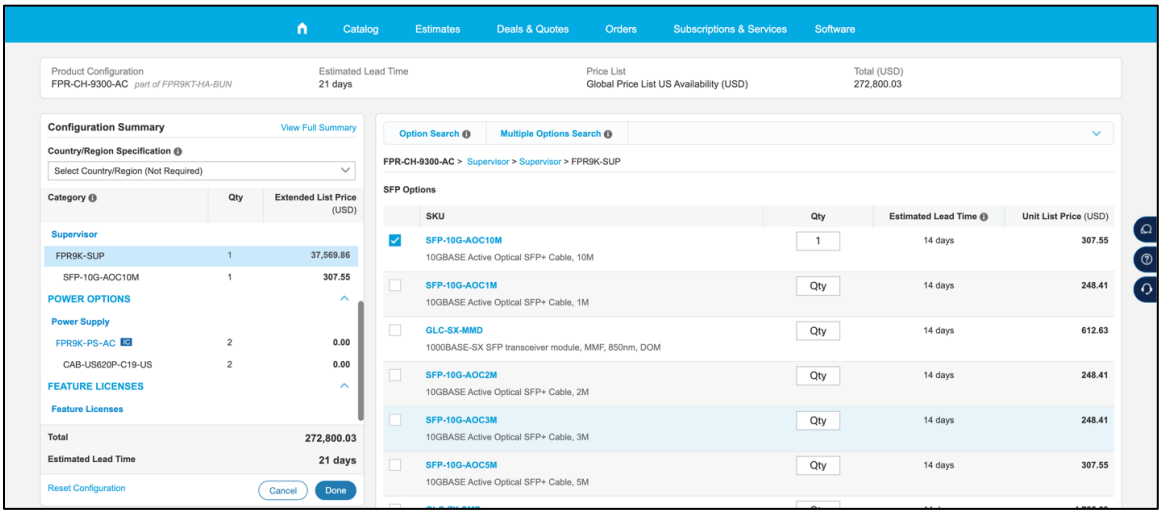



© 2026 Cisco and/or its affiliates. All rights reserved.

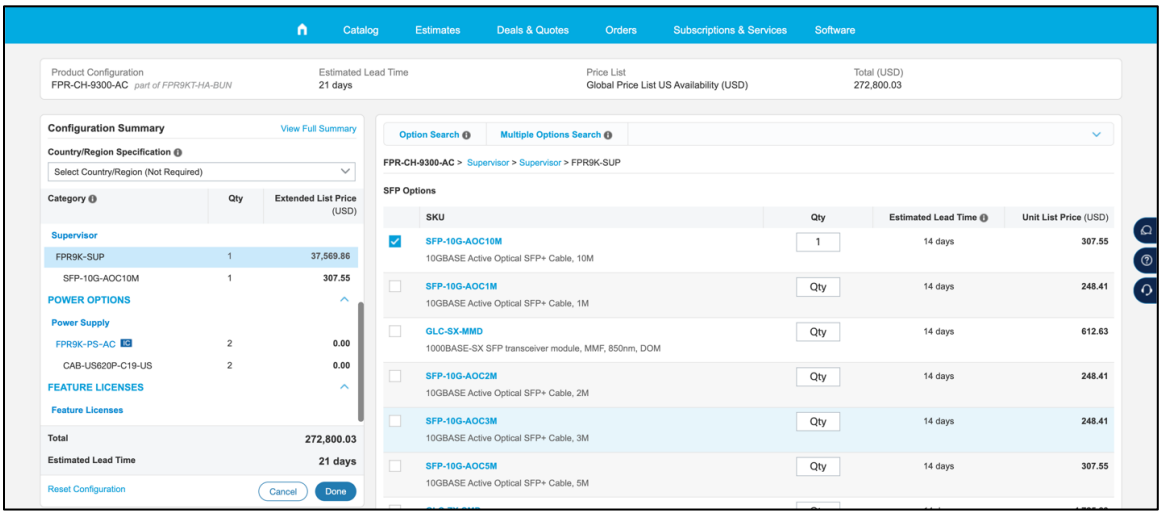
## **Step 5:** Add a Security Module




## **Step 6:** Add a Subscription License




## **Step 7:** Product Configuration Summary.




© 2026 Cisco and/or its affiliates. All rights reserved.

#### Example of Cisco Firepower Solution Configurations

Below tables show example configurations for ordering 9300 appliances. Note that these are high-level overviews and that actual orders will include additional items. Fully populated chassis with three SM-48 Security Modules for maximum I/O capability.

**Table 70.**

| Part Number | Description | Quantify |
|---|---|---|
| **FPR-C9300-AC** | Cisco Firepower 9300 AC Chassis + 2 PSU + 4 fans | 1 |
| **FPR9K-SUP** | Cisco Firepower 9000 Series Supervisor | 1 |
| **FPR9K-SM-48** | Cisco Firepower 9000 Series 48 Physical Core, Security Module includes 2 SSDs | 3 |
| **FPR9K-NM-4X40G** | Cisco Firepower 9000 Series - 4-port QSFP+ Network Module | 1 |
| **FPR9K-NM-8X10G** | Cisco Firepower 9000 Series - 8-port SFP+ Network Module | 1 |
| **CAB-AC-C6K-TWLK** | Power Cord, 250VAC 16A, twist-lock NEMA L6-20 plug, U | 1 |
| **L-F9K-ASA-SC-10=** | License to add 10 Security Contexts to ASA in Cisco Firepower 9000 | 3 |

**Table 71.** Chassis with one SM-40 Security Module

| Part Number | Description | Quantify |
|---|---|---|
| **FPR-C9300-AC** | Cisco Firepower 9300 AC Chassis + 2 PSU + 4 fans | 1 |
| **FPR9K-SUP** | Cisco Firepower 9000 Series Supervisor | 1 |
| **FPR9K-SM-40** | Cisco Firepower 9000 Series Enterprise, 40 Physical Core, Security Module (NEBS Ready) includes 2 SSDs | 1 |
| **CAB-AC-C6K-TWLK** | Power Cord, 250VAC 16A, twist lock NEMA L6-20 plug, U | 1 |

#### SKUs and Ordering Guidance for Cisco Secure Firewall Threat Defense Virtual

Cisco Secure Firewall Threat Defense Virtual is available where virtualized firewall and IPS capabilities are required, including in public cloud environments. It is the virtualized version of Firewall Threat Defense. It enables consistent security policies to follow workloads across your physical, virtual, and cloud environments, and between clouds. Complexity is further minimized with simple provisioning and a single console, the Firewall Management Center (FMC), which enables threat visibility, and automated defense, across your estate. FMC can manage both physical and virtual devices. See the Firewall Management Center section of this guide for FMC part numbers.

In Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform (GCP) and Oracle Cloud Infrastructure (OCI) environments, Cisco Secure Firewall Threat Defense Virtual devices can be managed either by an on-premises FMC, or in the respective public cloud with the virtualized FMC. When deployed in AWS and Microsoft Azure environments, two licensing models are available:

- Bring Your Own License (BYOL), where an existing Threat Defense Virtual license is required.
- Hourly billing (a pay-as-you-go model) is available through the AWS interface.

© 2026 Cisco and/or its affiliates. All rights reserved.

Google Cloud Platform (GCP) and Oracle Cloud Infrastructure (OCI) only support the Bring Your Own License (BYOL) licensing model.

For the supported private cloud platforms and Hyper Converged Infrastructure like Cisco Hyperflex and Nutanix AHV the same licenses can be used in the BYOL model.

Cisco Secure Firewall Threat Defense Virtual enables inter-VM and east-west traffic inspection, as well as at ingress and egress points to the cloud. It is designed to address security concerns in both traditional networks infrastructures and to be optionally inserted into Cisco's Application Centric Infrastructure (ACI) for flexible orchestration.

#### Firewall Threat Defense Virtual performance tiered Subscriptions

Performance tiered licensing is available starting from Firewall Threat Defense Virtual version 7.0. The new licensing model also includes Base License as a subscription. There are 6 tiers in the new performance tiered licensing model which can be ordered using the following SKU's.

**Table 72.** Cisco Secure Firewall Threat Defense Virtual Performance tiered Base Subscription and Threat, Malware and URL Filtering Subscription SKUs

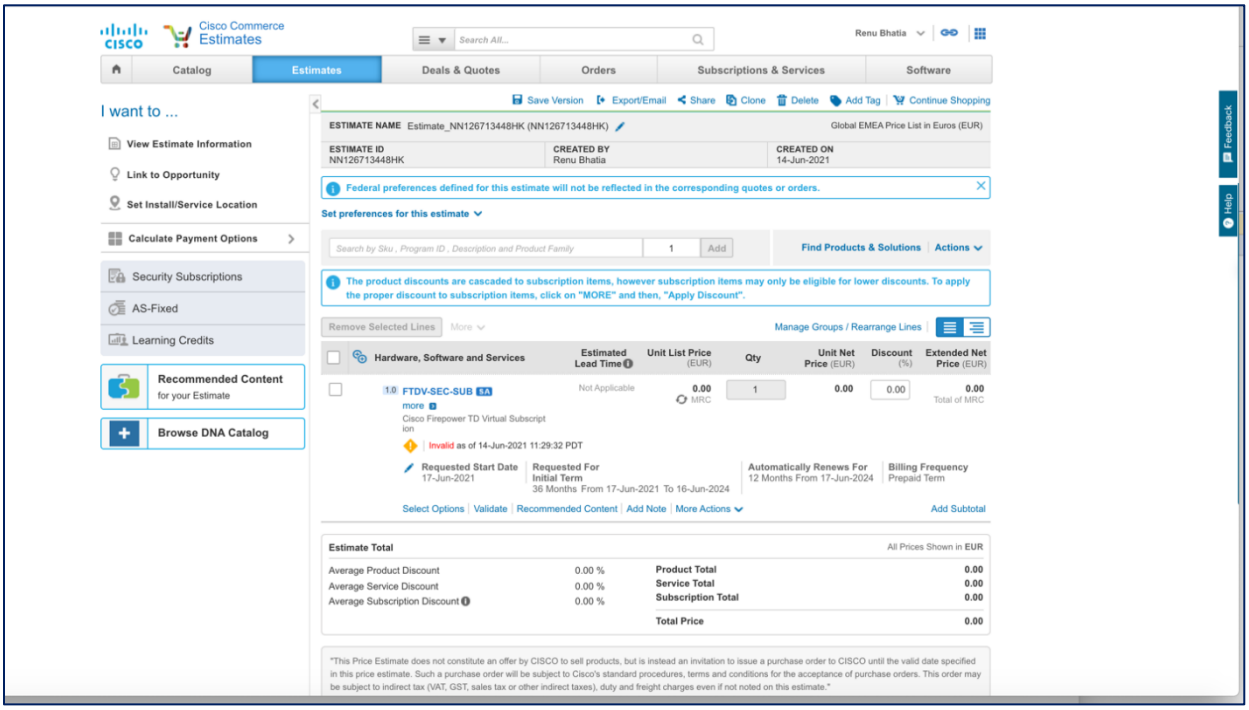
| Top level SKU | | |
|---|---|---|
| **License** | **Term Subscription** | **Description** |
| **FTDV-SEC-SUB** | 1,3 and 5 Year | Cisco Secure Firewall Threat Defense Virtual Subscription |

| Term Subscription 1, 3 and 5 year | | | | | | Description |
|---|---|---|---|---|---|---|
| **FTDv 5s** | **FTDv 10s** | **FTDv 20s** | **FTDv 30s** | **FTDv 50s** | **FTDv 100s** | |
| **FTD-V-5S-BSE-K9** | FTD-V-10S-BSE-K9 | FTD-V-20S-BSE-K9 | FTD-V-30S-BSE-K9 | FTD-V-50S-BSE-K9 | FTD-V-100S-BSE-K9 | Cisco Firepower TD Virtual Base License |
| **FTD-V-5S-TMC** | FTD-V-10S-TMC | FTD-V-20S-TMC | FTD-V-30S-TMC | FTD-V-50S-TMC | FTD-V-100S-TMC | Cisco Firepower TD Virtual Threat, Malware and URL Filtering License |
| **FTD-V-5S-TM** | FTD-V-10S-TM | FTD-V-20S-TM | FTD-V-30S-TM | FTD-V-50S-TM | FTD-V-100S-TM | Cisco Firepower TD Virtual Threat Protection, Malware License |
| **FTD-V-5S-TC** | FTD-V-10S-TC | FTD-V-20S-TC | FTD-V-30S-TC | FTD-V-50S-TC | FTD-V-100S-TC | Cisco Firepower TD Virtual Threat Protection, URL Filtering License |
| **FTD-V-5S-T** | FTD-V-10S-T | FTD-V-20S-T | FTD-V-30S-T | FTD-V-50S-T | FTD-V-100S-T | Cisco Firepower TD Virtual Threat Protection License |
| **FTD-V-5S-URL** | FTD-V-10S-URL | FTD-V-20S-URL | FTD-V-30S-URL | FTD-V-50S-URL | FTD-V-100S-URL | Cisco Firepower TD Virtual URL Filtering License |

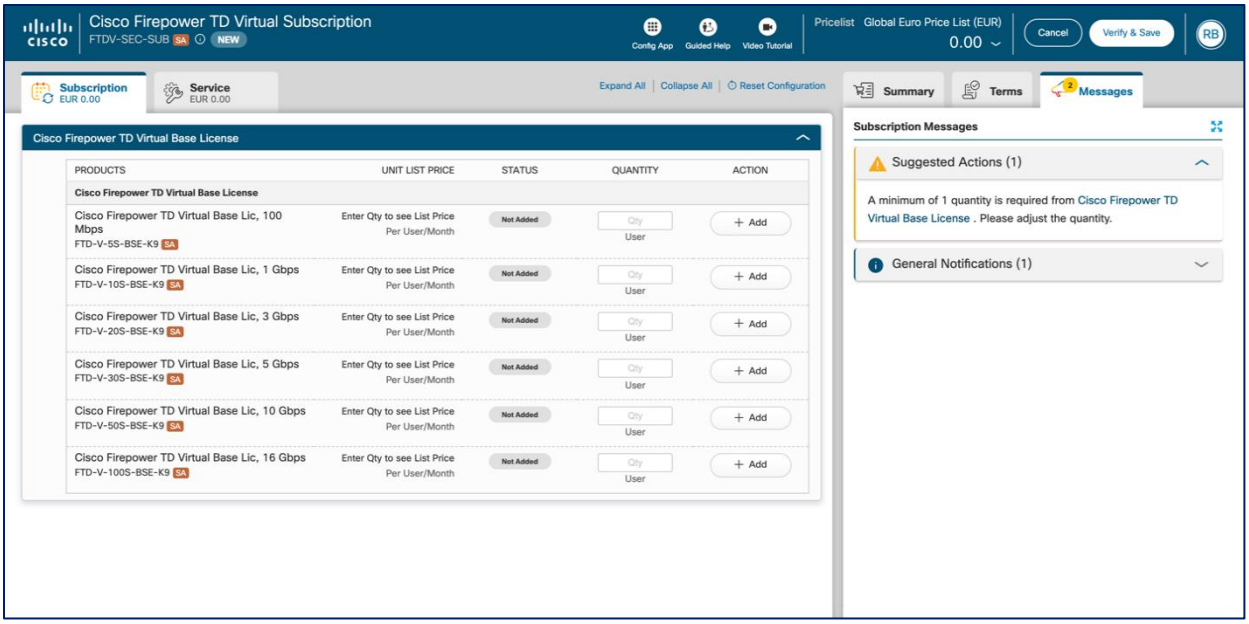
© 2026 Cisco and/or its affiliates. All rights reserved.

| Term Subscription 1, 3 and 5 year | | | | | | Description |
|---|---|---|---|---|---|---|
| FTDv 5s | FTDv 10s | FTDv 20s | FTDv 30s | FTDv 50s | FTDv 100s | |
| **FTD-V-5S-AMP** | FTD-V-10S-AMP | FTD-V-20S-AMP | FTD-V-30S-AMP | FTD-V-50S-AMP | FTD-V-100S-AMP | Cisco Firepower TD Virtual Malware License |

Search for the top level subscription SKU – FTDV-SEC-SUB and “Add”

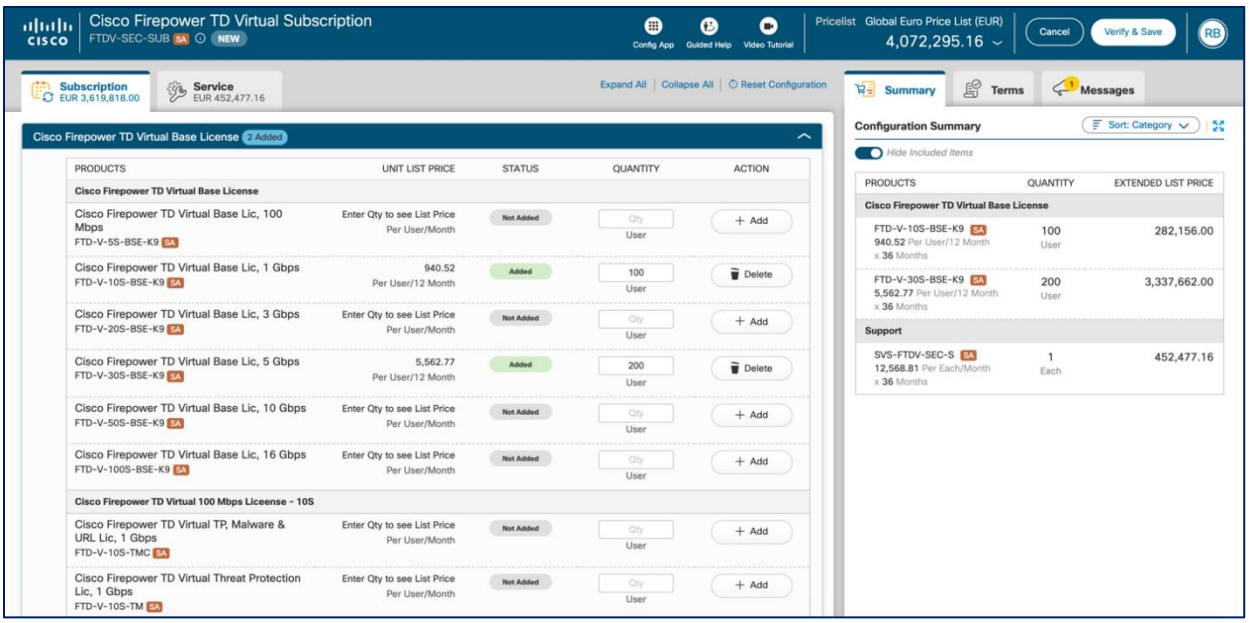



Add Base License quantity for the tiers required

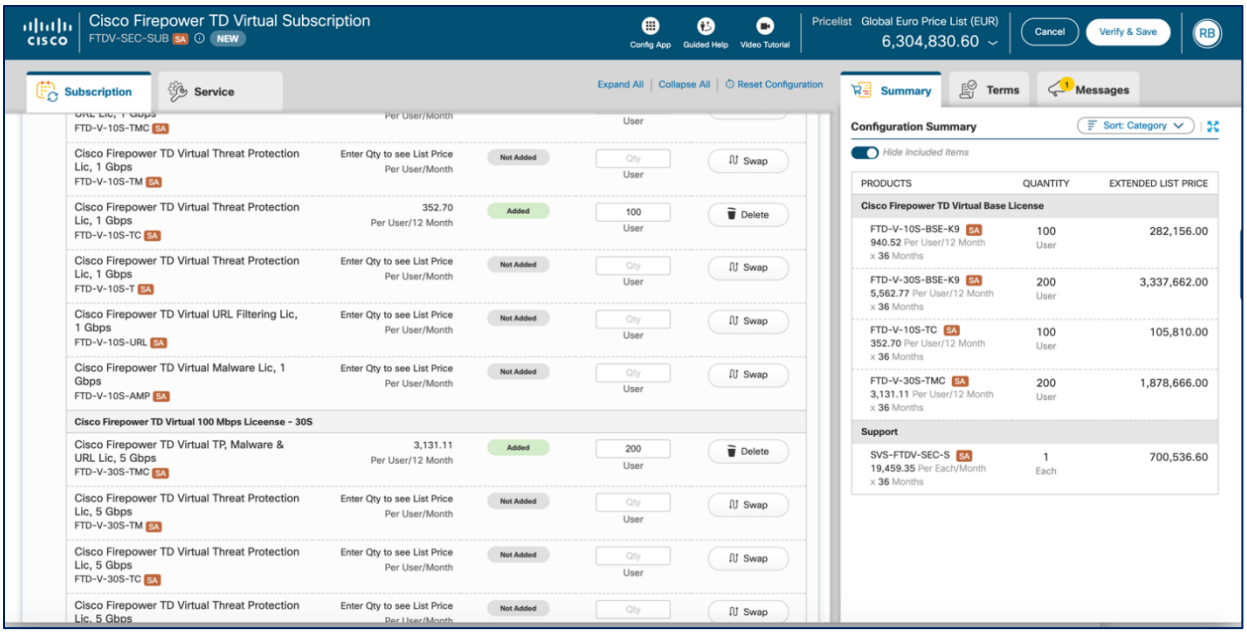



© 2026 Cisco and/or its affiliates. All rights reserved.

Then select the tier.

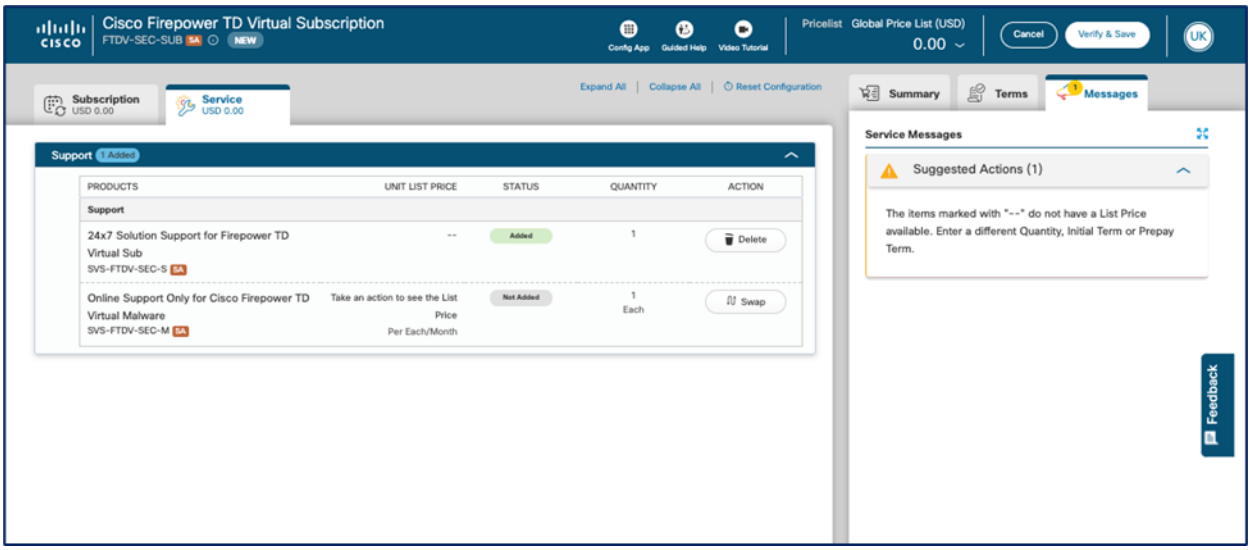



Select Additional features for each of Base license selected (Optional). Quantity should be aligned to Base License quantity

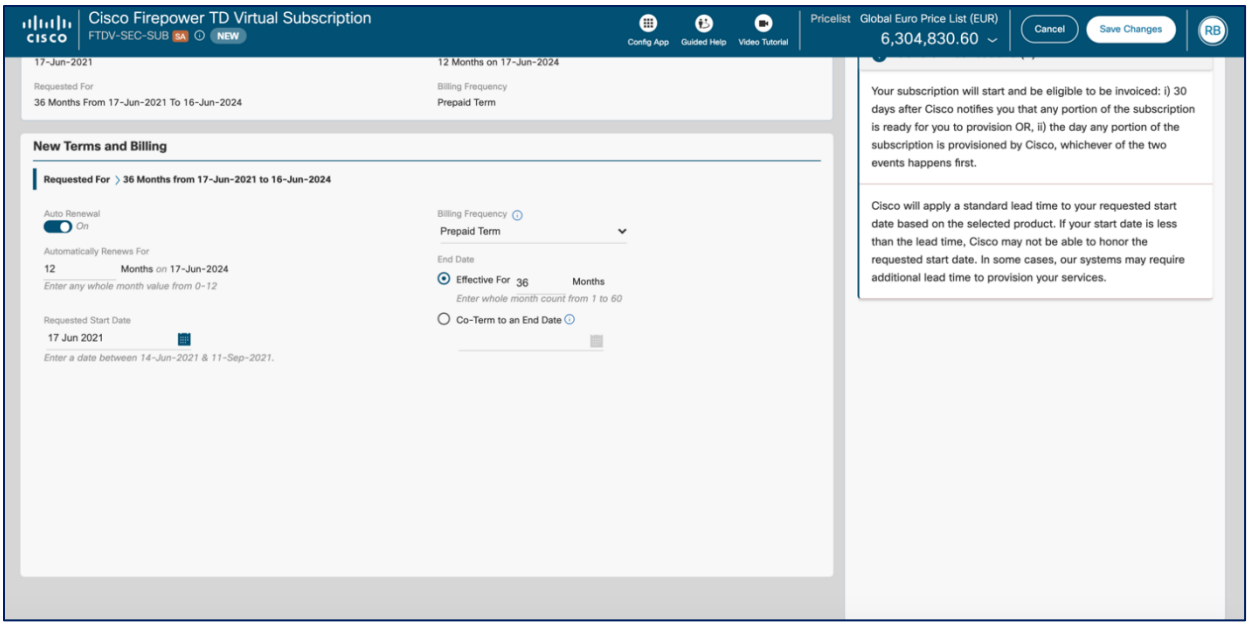



© 2026 Cisco and/or its affiliates. All rights reserved.

The Service tab shows the support options available. Cisco Solution Support is the default level of support for the Base and TMC subscription. It provides 24*7 technical phone support and is the recommended level of support. Included in the subscription at no additional cost is 8*5 online support which also provides Software upgrades.

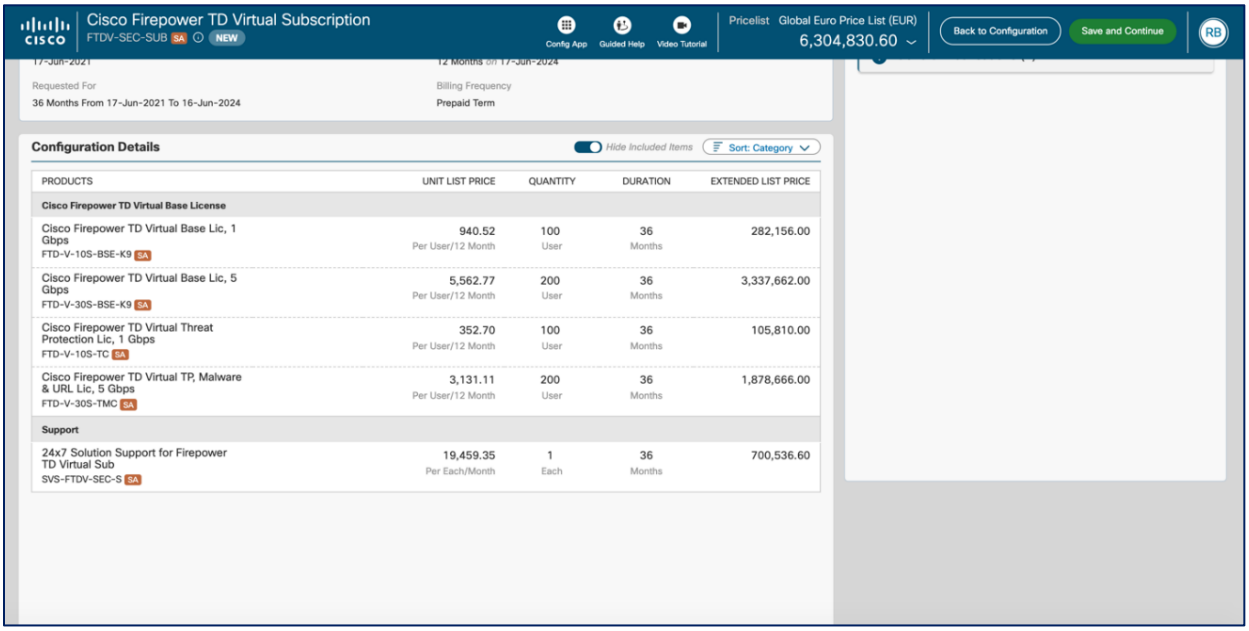



Default term is 3 Years which can be updated by clicking on Terms tab and editing duration. Click on Save Changes

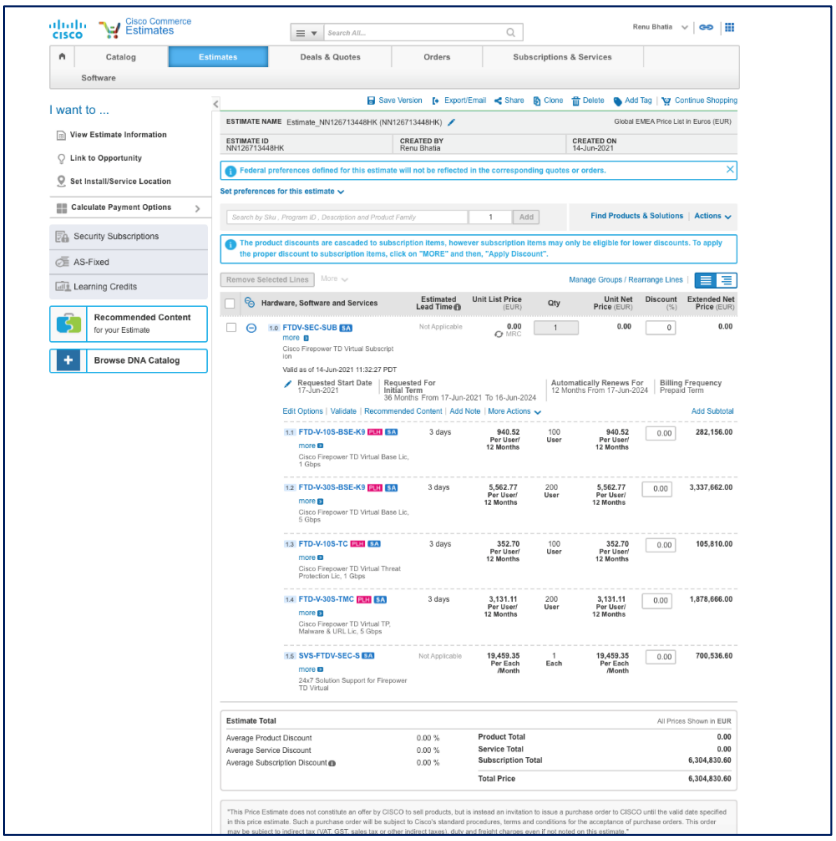



© 2026 Cisco and/or its affiliates. All rights reserved.

Once the changes are saved, the complete configuration is displayed. There is an option to switch from Solution support to basic support




Click on Save and Continue to review the complete configuration by clicking on Save and Continue. This will redirect to the main CCW screen.




Please note the older non tiered license with perpetual base will continue to work with 7.0. This can be selected as FTDv – Variable license on FMC UI during registration.

© 2026 Cisco and/or its affiliates. All rights reserved.

**Table 73.** Cisco Secure Firewall Threat Defense Virtual Perpetual Base

| SKUs | | |
|---|---|---|
| **Base License** | **Term Subscription** | **Description** |
| **FPRTD-V-K9** | | Cisco Firepower NGFWv Base License |

**Table 74.** Cisco Secure Firewall Threat Defense Subscription SKUs

| Term Licenses | Term Subscription | Description |
|---|---|---|
| **L-FPRTD-V-TMC=** | L-FPRTD-V-TMC-1Y | Cisco Firepower NGFWv Threat Defense Threat, Malware, and URL 1YR Subscription |
| **L-FPRTD-V-TMC=** | L-FPRTD-V-TMC-3Y | Cisco Firepower NGFWv Threat Defense Threat, Malware, and URL 3YR Subscription |
| **L-FPRTD-V-TMC=** | L-FPRTD-V-TMC-5Y | Cisco Firepower NGFWv Threat Defense Threat, Malware, and URL 5YR Subscription |
| **L-FPRTD-V-T=** | L-FPRTD-V-T-1Y | Cisco Firepower NGFWv Threat Defense Threat Protection 1YR Subscription |
| **L-FPRTD-V-T=** | L-FPRTD-V-T-3Y | Cisco Firepower NGFWv Threat Defense Threat Protection 3YR Subscription |
| **L-FPRTD-V-T=** | L-FPRTD-V-T-5Y | Cisco Firepower NGFWv Threat Defense Threat Protection 5YR Subscription |
| **L-FPRTD-V-URL=** | L-FPRTD-V-URL-1Y | Cisco Firepower NGFWv Threat Defense URL Filtering 1YR Subscription |
| **L-FPRTD-V-URL=** | L-FPRTD-V-URL-3Y | Cisco Firepower NGFWv Threat Defense URL Filtering 3YR Subscription |
| **L-FPRTD-V-URL=** | L-FPRTD-V-URL-5Y | Cisco Firepower NGFWv Threat Defense URL Filtering 5YR Subscription |
| **L-FPRTD-V-TC=** | L-FPRTD-V-TC-1Y | Cisco Firepower NGFWv Threat Defense Threat and URL 1Y Subscription |
| **L-FPRTD-V-TC=** | L-FPRTD-V-TC-3Y | Cisco Firepower NGFWv Threat Defense Threat and URL 3Y Subscription |
| **L-FPRTD-V-TC=** | L-FPRTD-V-TC-5Y | Cisco Firepower NGFWv Threat Defense Threat and URL 5Y Subscription |
| **L-FPRTD-V-TM=** | L-FPRTD-V-TM-1Y | Cisco Firepower NGFWv Threat Defense Threat and Malware Protection 1Y Subscription |
| **L-FPRTD-V-TM=** | L-FPRTD-V-TM-3Y | Cisco Firepower NGFWv Threat Defense Threat and Malware Protection 3Y Subscription |
| **L-FPRTD-V-TM=** | L-FPRTD-V-TM-5Y | Cisco Firepower NGFWv Threat Defense Threat and Malware Protection 5Y Subscription |

© 2026 Cisco and/or its affiliates. All rights reserved.

| Term Licenses | Term Subscription | Description |
|---|---|---|
| **L-FPRTD-V-AMP=** | L-FPRTD-V-AMP-1Y | Cisco Firepower NGFWv Threat Defense Malware Protection 1Y Subscription |
| **L-FPRTD-V-AMP=** | L-FPRTD-V-AMP-3Y | Cisco Firepower NGFWv Threat Defense Malware Protection 3Y Subscription |
| **L-FPRTD-V-AMP=** | L-FPRTD-V-AMP-5Y | Cisco Firepower NGFWv Threat Defense Malware Protection 5Y Subscription |

**SKUs and Ordering Guidance for Cisco Adaptive Security Virtual Appliance (ASAv)**

The Cisco ASAv brings the power of ASA to the virtual domain and private cloud environments. It runs the same software as the physical ASA appliance to deliver proven security functionality. You can use ASAv to protect virtual workloads within your data center. Later, you can expand, contract, or shift the location of these workloads over time and can span physical and virtual infrastructures. The Adaptive Security Virtual Appliance runs as a virtual machine inside a hypervisor in a virtual host. Most of the features that are supported on a physical ASA by Cisco software are supported on the virtual appliance as well, except for clustering and multiple contexts. The virtual appliance supports site-to-site VPN, remote-access VPN, and clientless VPN functionalities as supported by physical ASA devices. See the ASAv data sheet for more details.

ASAv is available in both subscription and perpetual licensing models.

**Table 75.** Cisco Adaptive Security Virtual Appliance (ASAv) Subscription License

| Part number | Description |
|---|---|
| **L-ASA-V-5S-K9=** | Cisco 100 Mbps entitlement (ASAv5) subscription |
| **L-ASA-V-10S-K9=** | Cisco 1 Gbps entitlement (ASAv10) subscription |
| **L-ASA-V-30S-K9=** | Cisco 2 Gbps entitlement (ASAv30) subscription |
| **L-ASA-V-50S-K9=** | Cisco 10 Gbps entitlement (ASAv50) subscription |
| **L-ASA-V-100S-K9=** | Cisco 20 Gbps entitlement (ASAv100) subscription* |

**Table 76.** Cisco Adaptive Security Virtual Appliance (ASAv) Perpetual License

| Cisco Adaptive Security Virtual Appliance (ASAv) | |
|---|---|
| **L-ASAV5S-K9=** | Cisco 100 Mbps entitlement (ASAv5) selection |
| **L-ASAV5S-STD-8** | 8-pack Cisco ASAv5(100 Mbps) with all firewall features licensed |
| **L-ASAV10S-K9=** | Cisco ASAv10 (1 Gbps) selection |
| **L-ASAV10S-STD** | Cisco ASAv10 (1 Gbps) with all firewall features licensed |
| **L-ASAV10S-STD-16** | 16-pack Cisco ASAv10 (1 Gbps) with all firewall features licensed |
| **L-ASAV30S-K9=** | Cisco ASAv30 (2 Gbps) selection |

© 2026 Cisco and/or its affiliates. All rights reserved.

| Cisco Adaptive Security Virtual Appliance (ASAv) | |
|---|---|
| **L-ASAV30S-STD** | Cisco ASAv30 (2 Gbps) with all firewall features licensed |
| **L-ASAV30S-STD-4** | 4-pack Cisco ASAv30 (2 Gbps) with all firewall features licensed |
| **L-ASAV50S-K9=** | Cisco ASAv50 selection |
| **L-ASAV50S-STD-4** | 4-Pack Cisco ASAv50 with all firewall features licensed |

**Note:** For ASAv, remote-access VPN functionality can be licensed separately as outlined in https://www.cisco.com/c/en/us/products/collateral/security/anyconnect-secure-mobility-client/guide-c07-732790.html.

#### Qualys Connector

The Qualys Connector is a software application that collects Qualys Guard vulnerability report data and sends it to the Cisco Secure Firewall Management Center. The Qualys vulnerability data is then aggregated with Cisco's vulnerability information found in the host map. Customers can choose to use Cisco or Qualys vulnerability data, or both, for Impact Flag calculations and automatic rule recommendations.

#### Firepower Product Licensing and License Activation

- The customer logs on to https://cisco.com/go/licensing and uses the Smart Licensing feature to request a token to be installed in the FMC or FDM. This license is then applied to the Cisco Secure Firewall Management Center that is going to manage the feature or appliance.
- Exception: Cisco Secure Endpoint (formerly AMP for Endpoints) does not require an activation key at this time.

#### High-Availability Configurations

Type 1: Secure Firewall High-Availability

- If the customer wants high availability for sensors, two appliances are required.
- Appliances must be of the same model and generation.
- Both appliances must be identically licensed and have support.
- Licenses will be applied to the same primary Cisco Secure Firewall Management Center managing the high-availability pair.

#### Snort Subscriber Rule Set: Subscription Options

**Personal:** This subscription type is for use in a home network environment. If you'd like to purchase a subscription online using a credit card, you may do so. For a personal subscription, please go to https://www.snort.org/products to place an order. It is not available to purchase on Cisco Commerce. As you approach the expiration date, renewal by way of Snort.org is automatic for credit card orders and is part of the license agreement.

© 2026 Cisco and/or its affiliates. All rights reserved.

**Business:** This subscription type is for use in businesses, nonprofit organizations, colleges and universities, government agencies, consultancies, and other venues where Snort sensors are in use in a production or lab environment. This subscription type does not include a license to redistribute the Snort Subscriber Rule Set except as described in section 2.1 of the Rule Set license agreement.

If you'd like to purchase a Rule subscription online using a credit card, you may do so. Customers or end users who cannot purchase by credit card are requested to contact a partner or distributor who can purchase on their behalf through Cisco Commerce. If you need assistance with a quote, contact snort-sub@cisco.com. Unlike Snort.org automatic renewals, orders placed in Cisco Commerce require a manual renewal to trigger another subscription. Important: Email address of the recipient of the subscription license needs to be included on the order for electronic delivery.

For more information, visit: https://www.snort.org/products.

## SKUs and ordering guidance for Cisco Security Manager

**Cisco Security Manager** provides scalable and centralized operations management for ASA functions, including policy and object management, event management, reporting, and troubleshooting for Cisco ASA firewall functions. The Security Manager can be used to manage:

- Cisco Firepower 1000, 200, 3100 4100, 4200, 6100 and 9300 series platforms with ASA software.
- Cisco Secure Firewall ASA Virtual on Private and Public Cloud.
- Cisco Secure Client (formerly AnyConnect Secure Mobility Client).

Security Manager is available in two feature levels: Standard and Professional (Table 64). Enterprise customers with numerous security devices will benefit from Security Manager Professional, and customers with fewer security device deployments will find Security Manager Standard an exceptional value. For small-scale and simple deployments, the Cisco Adaptive Security Device Manager (ASDM) is available to provide on-device, GUI-based firewall network operations management for Cisco ASA deployments.

**Note:** Modern server hardware is required. Please see the Cisco Security Manager data sheet for more details.

**Table 77.** Cisco Security Manager models

| E-Delivery Part Number | Description |
|---|---|
| **L-CSMST-5-K9** | Cisco Security Manager Standard - 5 Device License |
| **L-CSMST-10-K9** | Cisco Security Manager Standard - 10 Device License |
| **L-CSMST-25-K9** | Cisco Security Manager Standard - 25 Device License |
| **L-CSMPR-50-K9** | Cisco Security Manager Professional - 50 Device License |
| **L-CSMPR-100-K9** | Cisco Security Manager Professional - 100 Device License |
| **L-CSMPR-250-K9** | Cisco Security Manager Professional - 250 Device License |

© 2026 Cisco and/or its affiliates. All rights reserved.

| E-Delivery Part Number | Description |
|---|---|
| **Cisco Security Manager Professional Incremental Device Licenses** | |
| **L-CSMSTPR-U-K9** | Cisco Security Manager Upgrade License from 25 Device license (Standard) to 50 Device license (Professional) |
| **L-CSMPR-LIC-50** | 50 additional Devices on top of any Cisco Security Manager Professional license |
| **L-CSMPR-LIC-100** | 100 additional Devices on top of any Cisco Security Manager Professional license |
| **L-CSMPR-LIC-250** | 250 additional Devices on top of any Cisco Security Manager Professional license |

**Table 78.** Cisco Security Manager Software Application Support (SAS) SKUs

| **Cisco Security Manager** | | |
|---|---|---|
| **E-Delivery Part Number** | **Product Description** | **SKU** |
| **L-CSMST-5-K9** | Cisco Security Manager Standard - 5 Device License SAS (Minor Software Updates) | CON-SAS-LSMST5K9 |
| **L-CSMST-10-K9** | Cisco Security Manager Standard - 10 Device License SAS (Minor Software Updates) | CON-SAS-LSMST10K |
| **L-CSMST-25-K9** | Cisco Security Manager Standard - 25 Device License SAS (Minor Software Updates) | CON-SAS-LSMST25K |
| **L-CSMSTPR-U-K9** | Cisco Security Manager ST-25 To PR-50 Upgrade License SAS (Minor Software Updates) | CON-SAS-LCMSTPU9 |
| **Cisco Security Manager Enterprise Professional Incremental Device Licenses** | | |
| **L-CSMPR-50-K9** | Cisco Security Manager Professional - 50 Device License SAS (Minor Software Updates) | CON-SAS-LSMPR50K |
| **L-CSMPR-100-K9** | Cisco Security Manager Professional - 100 Device License SAS (Minor Software Updates) | CON-SAS-LSMPR100 |
| **L-CSMPR-250-K9** | Cisco Security Manager Professional - 250 Device License SAS (Minor Software Updates) | CON-SAS-LCMPR250 |

© 2026 Cisco and/or its affiliates. All rights reserved.

## SKUs and ordering guidance for Cisco Secure Firewall Management Center

The **Cisco Secure Firewall Management Center**, available as a physical or virtual appliance, provides unified management of:

- Cisco Secure Firewall Threat Defense software on the Cisco Firepower 1000 Series appliances.
- Cisco Secure Firewall Threat Defense software on the Cisco Secure Firewall 200 Series appliances.
- Cisco Secure Firewall Threat Defense software on the Cisco Firepower 3100 Series appliances.
- Cisco Secure Firewall Threat Defense software on the Cisco Firepower 4100 Series appliances.
- Cisco Secure Firewall Threat Defense software on the Cisco Firepower 4200 Series appliances.
- Cisco Secure Firewall Threat Defense Virtual.
- Cisco Secure Firewall Threat Defense software on the Cisco Firepower 9300.
- FirePOWER module of Cisco ASA with FirePOWER Services (up until release 7.4).
- Cisco Secure Intrusion Prevention System (IPS) and Cisco Secure Firewall malware defense solutions (up until release 7.0).
- Cisco Secure Firewall Threat Defense for Integrated Services Routers (ISR).

The Firewall Management Center provides a centralized management console and event database repository. It is available in a range of physical appliance models, as a virtual appliance for private and public cloud platforms or a cloud-delivered version that is delivered via Cisco Security Cloud Control. One physical or virtual management appliance can manage multiple appliances as long as all the appliances are running the compatible firewall configuration.

The appropriate Firewall Management Center hardware is selected based on the firewall configuration deployed and the number of appliances and events to be monitored. Firewall Management Center 1700, 1800, 2700, 2800, 4700 and 4800 physical appliances or the Firewall Management Center virtual appliance can be used to manage Cisco ASA with Firepower Services and the Firewall Threat Defense (FTD) software image. Cisco Security Manager is required to manage ASA physical or virtual appliance firewall functionality. Cisco Security Cloud Control delivers the cloud-delivered version of Firewall Management Center and a consistent and simplified cloud-based security policy management for ASA, ASA with FirePOWER Services, and FTD devices. For more details, visit Cisco Security Cloud Control home page. For Security Cloud Control ordering details, visit the Guidelines for Quoting Cisco Security Cloud Control Firewall Management.

**Table 79.** Cisco Secure Firewall Management Center SKUs

| **Cisco Secure Firewall Management Center (Hardware) Appliances** | |
|---|---|
| **Part Number** | Product Description |
| **FMC1700-K9** | Cisco Secure Firewall Management Center 1700 Chassis |
| **FMC2700-K9** | Cisco Secure Firewall Management Center 2700 Chassis |
| **FMC4700-K9** | Cisco Secure Firewall Management Center 4700 Chassis |
| **FMC1800-K9** | Cisco Secure Firewall Management Center 1800 Appliance |

© 2026 Cisco and/or its affiliates. All rights reserved.

| Cisco Secure Firewall Management Center (Hardware) Appliances | |
|---|---|
| **FMC2800-K9** | Cisco Secure Firewall Management Center 2800 Appliance |
| **FMC4800-K9** | Cisco Secure Firewall Management Center 4800 Appliance |
| **Cisco Secure Firewall Management Center (Hardware) Spare** | |
| **UCSC-PSU1-1050W=** | 1050W Power Supply Spare for FMC1700, 2700, 4700 |
| **UCSC-PSU1-1200W-D=** | 1200W Power Supply Spare for FMC1800, 2800, 4800 |

For new deployments, a compatible Management Center can be ordered with Firepower 3100 Series, 4100 Series, 4200 Series, and Secure Firewall 9300 devices. For small-scale FTD deployments, Firewall Device Manager on-device manager is included (except for CSF 4200).

**Note:** To manage network operations in large-scale deployments of devices running the ASA software image, using Cisco Security Manager or Cisco Security Cloud Control is highly recommended.

## SKUS and Ordering Guidance for Cisco Secure Firewall Management Center Virtual Appliance

The PAK-enabled, 2- and 10-device Firewall Management Center Virtual Appliances (FMCv) are part of a promotional offer to more cost-effectively manage FirePOWER Services or Firewall Threat Defense on small-scale deployments of low-end ASA-X Series appliances. However, the 2-, 10-, and 25-device FMCv Smart License or PAK SKUs do not have any limitations with respect to which appliances they can manage. For add-on licenses requirement for new devices on your FMCv, it is recommended to migrate to a higher FMCv model that supports additional devices.

**Table 80.** Smart Licensing-enabled Cisco Secure Firewall Management Center Virtual Appliance SKUs

| Cisco Secure Firewall Management Center (Software) Virtual Appliance | |
|---|---|
| **SF-FMC-VMW-K9** | Cisco Secure Firewall Management Center, for 25 devices |
| **SF-FMC-VMW-2-K9** | Cisco Secure Firewall Management Center, for 2 devices |
| **SF-FMC-VMW-10-K9** | Cisco Secure Firewall Management Center, for 10 devices |
| **SF-FMC-KVM-K9** | Cisco Secure Firewall Management Center, for 25 devices |
| **SF-FMC-KVM-2-K9** | Cisco Secure Firewall Management Center, for 2 devices |
| **SF-FMC-KVM-10-K9** | Cisco Secure Firewall Management Center, for 10 devices |
| **SF-FMC-VMW-300-K9** | Cisco Secure Firewall Management Center, Virtual for 300 devices Firepower License |
| **SF-FMC-VMW-25-300** | Upgrade SKU from FMCv25 to FMCv300 Cisco Secure Firewall Management Center, Virtual |

**Note:** FMCv SKUs are not tied to specific Private or Public Cloud platforms. The SKUs listed can be used with any supported Private or Public Cloud Deployment.

© 2026 Cisco and/or its affiliates. All rights reserved.

**Licensing Guidance for Cisco Secure Firewall Management Center**

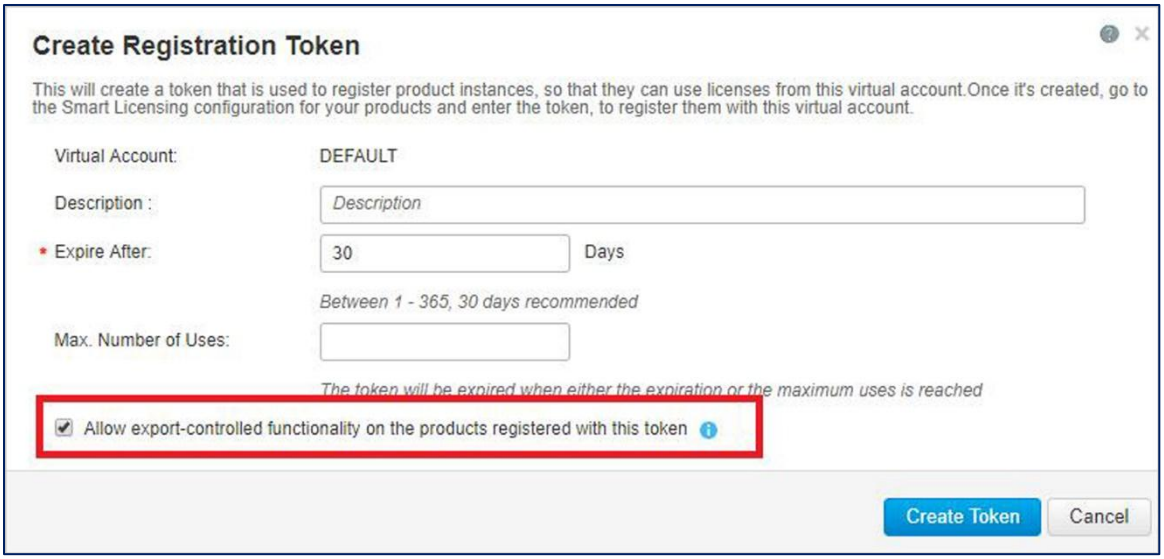
Firewall Management Center physical appliances do not require any separate management licenses. Firewall Management Center virtual appliances require only one of the licenses mentioned in the previous table based on the number of devices being managed. These licenses cannot be combined, for example, entitlement for management of four (4) managed devices, a minimum of one (1) Cisco Secure Firewall Management Center, for 10 devices is required. Use of two (2) Cisco Secure Firewall Management Center, for 2 devices licenses is not compliant for this use-case. Separate to the Firewall Management Center, the managed devices each require classic or Smart subscription feature licenses. Firewall Management Center Virtual Appliance Smart SKUs can manage any device running Firewall Threat Defense software.

**IMPORTANT: For version 6.3 and later:**

Enablement of strong crypto features (3DES/AES VPN) continues to happen automatically via Smart Licensing for those customers that are not subject to export restrictions or require an export license. However, those customers who are subject to export restrictions or require an export license will be asked to select a $0 strong crypto enablement key during configuration of any FMC device with version 6.3+.

For those customers who are subject to export restrictions or require an export license that upgrades an existing FMC to version 6.3+, there are spare versions of the PIDs available (those with "=" suffix).

To determine if you are subject to export restrictions or require an export license, customers can log in to CSSM and try to generate an installation token. For those customers that do NOT have export restrictions, this box will be checked by default. If you do NOT see this box or are NOT able to check the box, this means that your account is subject to export restrictions. See image below:




© 2026 Cisco and/or its affiliates. All rights reserved.

**Table 81.** Cisco Secure Firewall Management Center strong crypto enablement SKUs

| Firewall Management Center strong crypto | |
|---|---|
| **L-FMCVIR-ENC-K9=** | Cisco Virtual FMC Series Strong Encryption (3DES/AES) |
| **L-FMC1K-ENC-K9=** | Cisco FMC 1K Series Strong Encryption (3DES/AES) |
| **L-FMC2K-ENC-K9=** | Cisco FMC 2K Series Strong Encryption (3DES/AES) |
| **L-FMC4K-ENC-K9=** | Cisco FMC 4K Series Strong Encryption (3DES/AES) |

The standalone Cisco Secure Firewall Management Center is optimal for high-availability pairing. For the FMC, a high-availability or redundancy feature helps ensure continuity of operations. The secondary Management Center must be the same model as the primary appliance.

The Cisco Secure Firewall Management Center Virtual Appliance also supports High Availability on some Private and Public Cloid offerings. Use of High Availability for Cisco Secure Firewall Management Center Virtual requires an additional identical license.

Product high-availability configuration:

High availability for the Management Center

- If the customer wants high availability for the Management Center, an additional appliance is required.
- The secondary Management Center must be of the same model and generation as the primary one.
- License keys for all sensors, feature licenses (including Cisco Firepower), and subscriptions managed on the primary Management Center can be duplicated and loaded onto the secondary Management Center using the original activation keys.

High availability for the Management Center Virtual Appliance

- If the customer wants high availability for the Management Center Virtual Appliance, two (2) identical licenses (see Table 67) are required.
- High Availability support varies across Private and Public Cloud as well as model types, please review the latest guidance provided in the Cisco Secure Firewall Management Center Administration Guide for specific information.
- High availability for the Management Center Virtual Appliance is not supported by the Cisco Secure Firewall Management Center, for 2 devices license.

© 2026 Cisco and/or its affiliates. All rights reserved.

## Connect and protect bundle ordering

**Overview**

Partners can now order Cisco's security portfolio tailored for 3 specific customer use cases: Secure Campus, Secure Branch and Secure Hybrid Datacenter. The bundles include products that address the real-world needs of each use case. The bundles are designed to simplify ordering and provide an attrprice pointe-point.

Please contact your partner for eligibility and additional information.

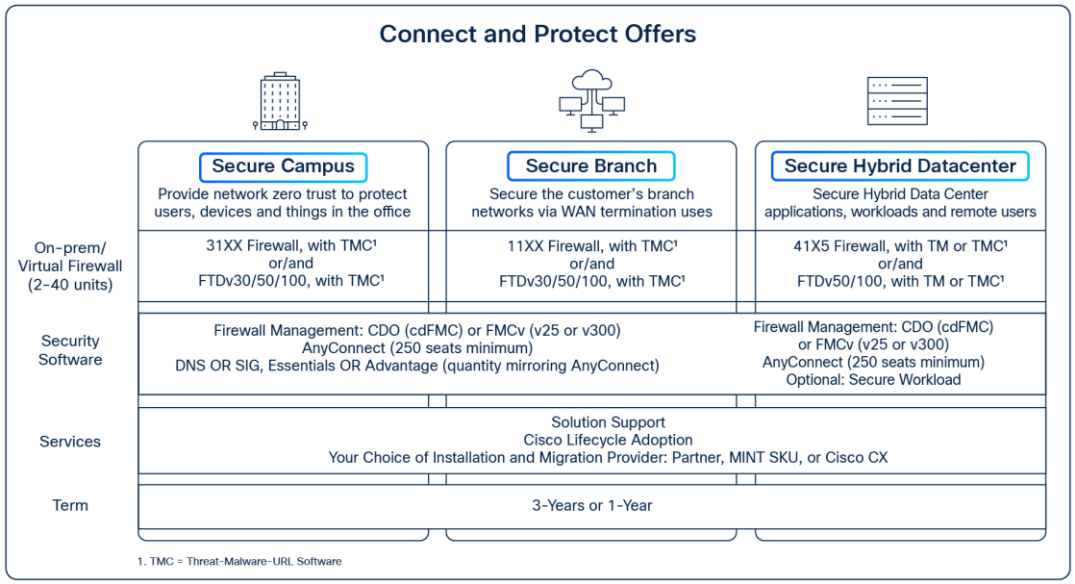



**Figure 8.**
Connect and Protect Offers – Included Products and Criteria

## SKUs and ordering

Adding the below to the estimate and configuring the required/optional sub-lines ("->") by clicking "select options" for the main line, following the indicated (minimum/maximum) quantities.

The hardware selection will need to happen as a separate line-item on the estimate. First, select and configure the use-case-specific bundle:

© 2026 Cisco and/or its affiliates. All rights reserved.

**Table 82.** Connect and Protect bundle components and options (Step 1)

| Product Category | Secure Campus | Secure Branch | Secure Hybrid Datacenter |
|---|---|---|---|
| **Bundle for Discount and Pre-Configuration** | FPR-SECURE-CAMPUS | FPR-SECURE-BRANCH | FPR-SECURE-DC |
| **Firewall HW (Quantity combined with virtual firewalls: 2-40)** | FPR31XX-NGFW-K9<br>• L-FPR31XXT-TMC=3Y (or<br>• L-FPR31XXT-TMC=1Y) | FPR11XX-NGFW-K9<br>• L-FPR11XXT-TMC=3Y (or<br>• L-FPR11XXT-TMC=1Y) | FPR41X5-NGFW-K9<br>• L-FPR41X5T-TM=3Y (or<br>• L-FPR41X5T-TM=1Y)<br>• L-FPR41X5T-TMC=3Y (or<br>• L-FPR41X5T-TMC=1Y) |
| **Technical support: Solution support must be purchased or attached appliance ordered** | CON-SSSNT-xxx | CON-SSSNT-xxx | CON-SSSNT-xxx |
| **Firewall Management (optional)** | SF-FMC-VMW-300-K9<br>SF-FMC-VMW-K9 | | |
| **Technical support: Solution support must be purchased or attached to the FMC** | CON-ECMUS-XXX | | |
| **SW Solution Support (Required- match the same quantity as HW or/and virtual appliance)** | FPR3K-SWSUPP-ENH= (top level)<br>CON-SWC1-TMC33XX | FPR1K-SWSUPP-ENH=<br>CON-SWS1-TMC11XX | FPR4K-SWSUPP-ENH=<br>CON-SWS1-TMC41X5 |
| **AnyConnect (Quantity: minimum 250)** | L-AC-APX-LIC= | L-AC-APX-LIC= | L-AC-APX-LIC= |

Next, configure the remaining items required for the respective bundles:

© 2026 Cisco and/or its affiliates. All rights reserved.

**Table 83.** Connect and Protect bundle components and options (Step 2)

| Product Category | Secure Campus | Secure Branch | Secure Hybrid Datacenter |
|---|---|---|---|
| **Bundle for Discount and Pre-Configuration** | FPR-CAMPUS-SUB | FPR-BRANCH-SUB | FPR-DC-SUB |
| **Virtual Firewalls (Quantity combined with hardware firewalls: 2-40)** | FTDv-SEC-SUB<br>• FTD-V-50S-BSE-K9 (or<br>• FTD-V-30S-BSE-K9 or<br>• FTD-V-100S-BSE-K9)<br>• SVS-FTDV-SEC-S | FTDv-SEC-SUB<br>• FTD-V-30S-BSE-K9 (or<br>• FTD-V-50S-BSE-K9 or<br>• FTD-V-100S-BSE-K9)<br>• SVS-FTDV-SEC-S | FTDv-SEC-SUB<br>• FTD-V-100S-BSE-K9 (or<br>• FTD-V-50S-BSE-K9)<br>• SVS-FTDV-SEC-S |
| **Security Cloud Control tenant if needed** | FWM-SEC-SUB<br>• FWM-BASE-LIC<br>• SVS-FWM-SUP-B | | |
| **Security Cloud Control Firewall Management license with unlimited logging and 90 days retention (Quantity matching firewall quantity if Security Cloud Control management selected)** | **FWM-ML-FP31xx-LIC** | **FWM-ML-FP11xx-LIC** | **FWM-ML-FP41x5-LIC** |
| **DNS Essentials or** | UMB-SEC-SUB<br>• UMB-[DNS or SIG]-ESS-K9 (quantity: minimum 250) | | NA |
| **DNS Advantage (optional upgrade to DNS Essentials)** | UMB-[DNS or SIG]-ADV-K9 (quantity: minimum 250)<br>• SVS-UMB-SUP-S or SVS-UMB-SUP-E or SVS-UMB-SUP-P | | |
| **Secure Workload (optional)** | NA | NA | C1-TAAS-SW-K9<br>• C1TAAS-WD-FND-k9<br>• SVS-TAAS-WP |
| **MINT Security (optional)** | MINT-SECURITY<br>• MINT-SECURITY-SVW | | |

For additional information regarding the ordering of Umbrella/DNS essentials or advantage, also see the Umbrella ordering guide.

© 2026 Cisco and/or its affiliates. All rights reserved.

## Additional resources

**Cisco Commerce**

Cisco Commerce is the primary tool used for ordering Cisco products and new services offered on the Cisco Price List. Three main steps are involved in creating an order: creating a quick quote, converting a quote to an order, and submitting an order.

Cisco Commerce Software Subscriptions and Services (CCW-R) is used to quote, order, and manage your service contracts and software subscriptions. Use CCW-R to create new or renew Technical Services (TS) and software subscription (Term-and-Content) quotes, submit approved orders, and manage your contracts.

## Cisco Capital Financing

The significant benefits offered by the Cisco Firepower 9300 make it the natural choice for service provider security and provisioning. As with any technology investment, the question is whether the new system is affordable. The answer is Cisco Capital financing. We can give customers the financing solution that works best for them. We offer both flexible repayments to help mitigate cash flow issues and operating leases to help negate capital expenditures.

Cisco Capital can help remove or reduce the barriers preventing organizations from obtaining the technology they need. Total solution financing programs help customers and partners:

- Achieve business objectives.
- Accelerate growth.
- Acquire technology to match current strategies and future needs.
- Remain competitive.

Cisco Capital also helps your customers achieve financial goals such as optimizing investment dollars, turning capital expenditures into operating expenses, and managing cash flow. And there's just one predictable payment. Cisco Capital operates in more than 100 countries, so regardless of location, customers and partners have access to a trusted means to secure Cisco products and services.

For more information about Cisco Capital financing, visit the following sites:

- For channel partners: https://www.ciscocapital.com/.
- For Cisco sales staff: https://wwwin.cisco.com/FinAdm/csc/.

**Our experts recommend**

- The Future of the Firewall White Paper.
- Cisco Secure Firewall At-a-Glance.


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 **https://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: https://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)



Printed in USA C07-737902-26 10/26



© 2026 Cisco and/or its affiliates. All rights reserved.