Cisco Secure Firewall Threat Defense (FTD) 7.4 with FMC 7.4 and Secure Client 5.1

Preparative Procedures & Operational User Guide for the Common Criteria Certified Configuration

Version 1.1

February 24, 2025

Prepared by:

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

Table of Contents

Table of Tables

1 Introduction

This document describes deployment of Cisco Secure Firewall Threat Defense (FTD) with FMC and Cisco Secure Client software in a manner consistent with its Common Criteria EAL4[1]+ certified configuration.

This document is a supplement to the Cisco administrative guidance, which is comprised of the installation and administration documents identified in section 1.7. This document supplements those manuals by specifying how to install, configure and operate this product in the Common Criteria (CC) evaluated configuration.

This guide provides an overview of configuration of these software components when installed to the allowed platforms listed in section 1.3.2:

- FMC 7.4 provides centralized management of one or more instances of FTD.
- FXOS 2.14: minimal FXOS build loads FTD applications on all platforms.
- FTD 7.4 provides firewall and VPN gateway functionality.
- Secure Client 5.1 provides VPN client functionality.

1.1 Audience

This document is written for administrators configuring the system components listed in section 1.3.2 into their CC-evaluated configuration. This document assumes you are familiar with networks and network terminology, that you are a trusted individual, and that you are trained to use the Internet and its associated terms and applications.

1.2 Common Criteria (CC) Evaluated Configuration

The following sections describe the scope of evaluation, required configuration, assumptions, and operational environment that the system must be in to ensure a secure deployment. To ensure the system is in the CC-evaluated configuration, system administrators must do the following:

1.3 Configure all the required system settings as documented in this guide, including disabling all features that would violate the claimed CC requirements as listed in section1.5 Secure Acceptance of the TOE

In order to ensure the correct FTD/FMC hardware is received, the hardware should be examined to ensure that that is has not been tampered with during delivery.

Verify that the TOE software and underlying hardware were not tampered with during delivery by performing the following actions:

[1] Common Criteria Evaluation Assurance Level 4.

1.3.1 Physical Acceptance of non-TOE hardware (supporting platforms)

Step 1 Before unpacking the appliance, inspect the physical packaging the equipment was delivered in. Verify that the external cardboard packing is printed with the Cisco Systems logo and motifs. If it is not, contact the supplier of the equipment (Cisco Systems or an authorized Cisco distributor/partner).

Step 2 Verify that the packaging has not obviously been opened and resealed by examining the tape that seals the package. If the package appears to have been resealed, contact the supplier of the equipment (Cisco Systems or an authorized Cisco distributor/partner).

Step 3 Verify that the box has a white tamper-resistant, tamper-evident Cisco Systems bar coded label applied to the external cardboard box. If it does not, contact the supplier of the equipment (Cisco Systems or an authorized Cisco distributor/partner). This label will include the Cisco product number, serial number, and other information regarding the contents of the box.

Step 4 Note the serial number of the appliance on the shipping documentation. The serial number displayed on the white label affixed to the outer box will be that of the device. Verify the serial number on the shipping documentation matches the serial number on the separately mailed invoice for the equipment. If it does not, contact the supplier of the equipment (Cisco Systems or an authorized Cisco distributor/partner).

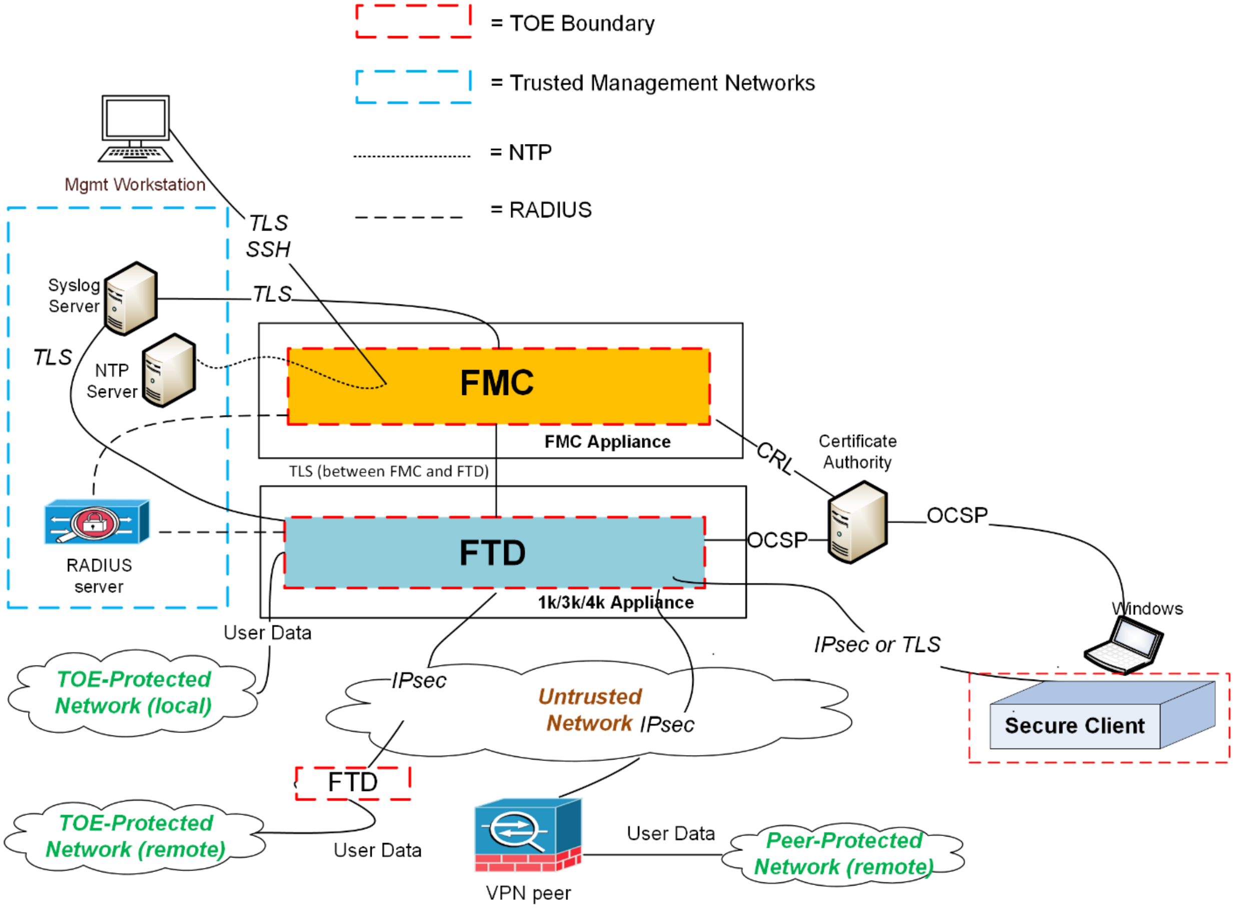
Step 5 Verify that the box was indeed shipped from the expected supplier of the equipment (Cisco Systems or an authorized Cisco distributor/partner). This can be done by verifying with the supplier that they shipped the box with the courier company that delivered the box and that the consignment note number for the shipment matches that used on the delivery. Also verify that the serial numbers of the items shipped match the serial numbers of the items delivered. This verification should be performed by some mechanism that was not involved in the actual equipment delivery, for example, phone/FAX or other online tracking service.

Step 6 Once the appliance is unpacked, inspect the unit. Verify that the serial number displayed on the unit itself matches the serial number on the shipping documentation and the invoice. If it does not, contact the supplier of the equipment (Cisco Systems or an authorized Cisco distributor/partner).

- Scope of Evaluation / Prohibited Features.
- Ensure the operational environment is consistent with section 1.6.1.
- Ensure all the environmental assumptions in section 1.6.2 are satisfied.

The CC-evaluated deployment is one which is similar to the one depicted below, in which the CC-evaluated components (the TOE, or Target of Evaluation) ensure traffic from protected networks (or the remote access VPN client, Secure Client) are not able to reach each other without passing traffic through an FTD appliance.

Figure 1 Depiction of a CC-Evaluated Deployment of Firepower and Secure Client



1.3.2 Security Requirements for the Operational Environment

To satisfy the security requirements in a manner consistent with the CC-evaluated configuration, ensure all administrators of FMC, FTD, and all VPN users adhere to the Administrator Responsibilities listed in the table in section 1.6.2 Environmental Assumptions such that all administrators and VPN users satisfy the operational environment security objective definitions as shown in the table.

1.3.3 Secure Parameters for Administrative Roles

In the context of the CC evaluation, all accounts that have access to any interactive administrative interface on FMC or FTD are considered to be ‘administrators’ of the system (or a ‘component’ of the system). The Secure Client component of the system does not enforce authentication, it relies on the underlying operating system to protect it, thus the accounts that manage the operating system must be trusted. The individuals who use Secure Client to initiate IPsec/TLS tunnels with FTD are considered VPN users, not administrators, and do not have any administrative access to FMC or FTD. The table below summarizes the administrative interfaces on each component of the system.

Table 1: Secure Parameters for Administrative Accounts

Administrative Interfaces	Administrative Roles	Permissions	Secure Parameters
FMC (Secure Firewall Management Center)			
CLI via console CLI via SSH	Default Administrative Role: • Config	See list of commands in section 3.8 Configure CLI Lockdown on FMC.	See bullet items in section 3.1 Configure Authentication.
WebUI via TLS	Default Administrative Roles: • Administrator • External Database User • Security Analyst • Security Analyst (Read Only) • Security Approver • Intrusion Admin • Access Admin • Network Admin • Maintenance User • Discovery Admin • Threat Intelligence Director (TID) User	See "Web Interface User Roles" in [FMC-AG].	See bullet items in section 3.1 Configure Authentication.
	Custom Administrative Roles • As created by someone with Administrator privileges.	See "Customize User Roles for the Web Interface" in [FMC-AG]	
FTD (Secure Firewall Threat Defense)			
CLI via console CLI via SSH	Default Administrative Roles: • Config • Basic	See section 5.3 Configure Authentication.	See section 5.3 Configure Authentication.
Secure Client			
None	None	n/a	n/a

1.4 Allowed Platforms

The table below lists the platforms allowed for use in this Common Criteria (CC) certified configuration.

Table 2: CC-Evaluated Software and Supported Hardware Platforms

Software	Supported Hardware Platforms
FTD release 7.4	FPR appliances supporting FTD 7.4: • FPR 1000 Series (the same installation and patch files are used for all models in this series: 1010, 1010E, 1120, 1140, and 1150) • Secure Firewall 3100 Series (the same installation and patch files are used for all models in this series: 3105, 3110, 3120, 3130 and 3140) • Secure Firewall 4200 Series (the same installation and patch files are used for all models in this series: 4215, 4225 and 4245)
FMC 7.4	FMC appliances that support FMC 7.4 (the same software build is used for all hardware models listed here): • FMC 1700

	• FMC 2700 • FMC 4700
Secure Client 5.1	The Secure Client client operates on any of the following OSs: Microsoft Windows 10/11 x64(64-bit)

1.5 Secure Acceptance of the TOE

In order to ensure the correct FTD/FMC hardware is received, the hardware should be examined to ensure that that is has not been tampered with during delivery.

Verify that the TOE software and underlying hardware were not tampered with during delivery by performing the following actions:

1.5.1 Physical Acceptance of non-TOE hardware (supporting platforms)

Step 1 Before unpacking the appliance, inspect the physical packaging the equipment was delivered in. Verify that the external cardboard packing is printed with the Cisco Systems logo and motifs. If it is not, contact the supplier of the equipment (Cisco Systems or an authorized Cisco distributor/partner).

Step 2 Verify that the packaging has not obviously been opened and resealed by examining the tape that seals the package. If the package appears to have been resealed, contact the supplier of the equipment (Cisco Systems or an authorized Cisco distributor/partner).

Step 3 Verify that the box has a white tamper-resistant, tamper-evident Cisco Systems bar coded label applied to the external cardboard box. If it does not, contact the supplier of the equipment (Cisco Systems or an authorized Cisco distributor/partner). This label will include the Cisco product number, serial number, and other information regarding the contents of the box.

Step 4 Note the serial number of the appliance on the shipping documentation. The serial number displayed on the white label affixed to the outer box will be that of the device. Verify the serial number on the shipping documentation matches the serial number on the separately mailed invoice for the equipment. If it does not, contact the supplier of the equipment (Cisco Systems or an authorized Cisco distributor/partner).

Step 5 Verify that the box was indeed shipped from the expected supplier of the equipment (Cisco Systems or an authorized Cisco distributor/partner). This can be done by verifying with the supplier that they shipped the box with the courier company that delivered the box and that the consignment note number for the shipment matches that used on the delivery. Also verify that the serial numbers of the items shipped match the serial numbers of the items delivered. This verification should be performed by some mechanism that was not involved in the actual equipment delivery, for example, phone/FAX or other online tracking service.

Step 6 Once the appliance is unpacked, inspect the unit. Verify that the serial number displayed on the unit itself matches the serial number on the shipping documentation and the invoice. If it does not, contact the supplier of the equipment (Cisco Systems or an authorized Cisco distributor/partner).

1.5.2 Scope of Evaluation / Prohibited Features

The list below identifies features or protocols that are not evaluated and must remain disabled. These features were not evaluated and/or validated by an independent third party.

The following features and protocols are not evaluated, and are prohibited from use:

- Use of telnet for management purposes. This functionality is disabled by default.

- Cisco Secure Firewall Device Manager (FDM). Cisco Secure Firewall Device Manager is a web-based local manager for FTD. FDM is automatically disabled on FTD when FTD is managed by FMC, as is the case with all Common Criteria evaluated TOE configurations.
- FMC REST API: Allows programmatic (non-interactive) configuration of FMC. The API is enabled by default but is administratively disabled in the CC-evaluated configuration.
- Smart Call Home. The Smart Call Home feature provides personalized, e-mail-based and web-based notification to customers about critical events involving their individual systems. Use of Smart Call Home is beyond the scope of this Common Criteria evaluation.
- Note: Use of DHCP to configure the IP address for any administrative interface on FMC or FTD. This is not supported in the CC-evaluated configuration because changing the management IP after installation could interfere with communications with managed FTD appliances.

1.5.3 FMC Features

The following features and services are disabled or unconfigured by default and must remain so in the CC-evaluated configuration. These features and services are related to security functionality claimed CC evaluation, but were beyond the scope of what was tested during the CC evaluation, and therefore must remain disabled or unconfigured in order to maintain conformance with the CC-evaluated configuration.

- eStreamer
- External Database Access
- Flex Config
- LDAP
- TACACS+
- User Role Escalation
- TCP State Bypass

The following features were not tested during the CC evaluation, but enabling them would not interfere with the CC-evaluated security claims.

- Advanced Access Control functionality, including:
  - Prefilter Policies
  - Security Intelligence (suspicious network lists, and suspicious URL lists)
  - HTTP Responses
  - SSL Policies (TLS proxy functionality)
  - Performance Settings, including:
    - Latency-Based Performance Settings
    - Firepower Threat Defense Service Policies
    - Intelligent Application Bypass Settings
    - Transport/Network Layer Preprocessing Settings
    - Detection Enhancement Settings
- Intrusion and Analysis functionality, including:
  - Intrusion Policies (including Network Analysis Policies)
  - Malware and File Policies
  - DNS Policies
  - Identity Policies
- Other functionality, including:
  - Smart Licensing
  - Stream Audit Log to an HTTP Server
  - Captive Portal (authenticated web proxy)
  - Alert Responses (via email, SNMP traps, or syslog)

1.5.4 FTD Features

The following features and services are disabled or unconfigured by default and must remain so in the CC-evaluated configuration. These features and services are related to security functionality claimed CC evaluation, but were beyond the scope of what was tested during the CC evaluation, and therefore must remain disabled or unconfigured in order to maintain conformance with the CC-evaluated configuration.

- Transmitting log messages via FTP (because use of FTP would require transmitting a password in plaintext): As would be configured via FMC under Devices > Platform Settings > Syslog > Logging Setup > Specify FTP Server Information.
- Unsupported features related to use of Secure Client with FTD:
    - Secure Client Customization and Localization support. The FTD device does not configure or deploy the files necessary to configure Secure Client for these capabilities.
    - Custom Attributes for the Secure Client client are not supported on the FTD. Hence all features that make use of Custom Attributes are not supported, such as Deferred Upgrade on desktop clients and Per-App VPN on mobile clients.
    - Local CA, the secure gateway cannot act as a Certificate Authority.
    - Local authentication; VPN users cannot be configured on the FTD secure gateway.
    - Single Sign-on using SAML 2.0.
    - TACACS, Kerberos (KCD Authentication and RSA SDI).
    - LDAP Authorization (LDAP Attribute Map).
    - Browser Proxy.
    - VPN load balancing.

1.5.5 Secure Client Features

The following features and services are disabled or unconfigured by default and must remain so in the CC-evaluated configuration. These features and services are related to security functionality claimed CC evaluation, but were beyond the scope of what was tested during the CC evaluation, and therefore must remain disabled or unconfigured in order to maintain conformance with the CC-evaluated configuration.

- Non-FIPS 140-2 mode of operation
- Secure Client Application Programming Interface (API) supports creation of a custom executable User Interface (UI).
- Some and-on Secure Client modules and their profiles, including:
    - Network Access Manager (NAM)
    - Network Visibility Module (NVM)
    - Secure Firewall Posture
    - ISE Posture (Endpoint Posture Assessment)
    - ThousandEyes

The following features were not tested during the CC evaluation, but using them would not interfere with the CC-evaluated security claims.

- Secure Client Profile Editor, provides a GUI to configure Secure Client VPN Client Policies.
- Umbrella, provides DNS-layer security when no VPN is active
- Secure Firewall Posture allows to create a remote access connection to the security appliance.
- ISE Posture, performs checks on endpoints that fails to satisfy all mandatory requirements.
- Diagnostics and Reporting Tool (DART), which bundles specified log files and diagnostic information for analyzing and debugging the client connection

- Start Before Logon (SBL) module (also called GINA), allows users to establish their VPN connection to the enterprise infrastructure before logging onto Windows. *Note: For SBL to be a viable option the authentication method defined within the remote access VPN policy must be one that can operate without human interaction (e.g. without entering a password), which in the CC-evaluated configuration would limit the authentication method to only an X.509 certificate, and would not include AAA/RADIUS.*

1.6 Operational Environment

This section describes the components in the environment and assumptions made about the environment.

1.6.1 Operational Environment Components

The system can be configured to rely on and utilize a number of other components in its operational environment.

- Management Workstation (**Required**) – The system supports Command Line Interface (CLI) and web access and as such an administrator would need a terminal emulator or SSH client (supporting SSHv2) or web browser (supporting HTTPS) to utilize those administrative interfaces.
- Audit (syslog) server – The system can be configured to deliver audit records to an external log server.
- Certificate Authority (CA) server – The system can be configured to import X.509v3 certificates from a CA, e.g., for TLS connection to syslog server.
- DNS server – The system supports domain name service in the network.
- NTP server – The system can be configured to use a master clock to synchronize the clocks on the systems in the evaluated configuration.
- RADIUS server – The system can be configured to use a RADIUS server to authenticate users.
- VPN Peer (another instance of the FTD, or a non-TOE VPN gateway)

1.6.2 Environmental Assumptions

The assumptions state the specific conditions that are expected to be met by the operational environment and administrators.

Table 3: Operational Environment Security Measures

Environment Security Objective	Operational Environment Security Objective Definition	Administrator Responsibilities

OE.NOEVIL	Authorized administrators are non-hostile and follow all administrator guidance; however, they are capable of error.	Do not act maliciously when configuring and maintaining the system, and adhere to all preparative and operational guidance contained within this document. Firepower/Secure Firewall administrators and VPN users are expected to understand and be familiar with the installation guides, configuration guides, release notes, and other documentation listed in the Documentation References (section 1.7) of this document. Firepower/Secure Firewall administrators are expected to have a solid understanding of firewall and VPN (IPsec and TLS) functionality. If needed, training is available through learningnetworkstore.cisco.com. VPN client (Secure Client) users do not need any special skills or training.
OE.PHYSEC	The hardware components on which the TOE components are installed are kept physically secure.	Ensure the underlying hardware of the system is in a secure location such that only authorized personnel have physical access.
OE.PROTRA	The workstations on which the TOE’ Secure Client component is installed are issued and managed by the same organization that manages the other TOE components and are kept secure through physical and/or cryptographic means (e.g. disk/drive encryption).	Ensure the underlying hardware and operating system of the Secure Client workstation is issued, installed and maintained securely to protect against loss of VPN user credentials. Ensure the organization that manages the Firepower/Secure Firewall components is also managing the Secure Client workstations. Ensure the workstations are protected by physical and/or cryptographic means (e.g. disk/drive encryption, such as the BitLocker drive encryption feature included with Windows 10/11).

OE.PROTENV	The operational environment servers on which the TOE relies, including NTP, syslog, CA/OCSP/CRL, and RADIUS servers remain physically and logically protected from malicious activity. The NTP, syslog, and RADIUS servers will be located on a trusted management network accessible from FMC and FTD.	Ensure the essential servers and services on which the system relies are trustworthy and maintained in a secure manner to protect them from malicious activity that may compromise their integrity. The servers should either be managed by the same organization that manages the Firepower/Secure Firewall components, or a memorandum of understanding (e.g. a contract or other agreement) should be in place to provide assurance that the servers are maintained securely.
OE.REMACC	Authorized administrators may access the TOE remotely from the internal and external networks.	Provide authentication credentials for administrative access only to trusted and trained personnel. Administrators are expected to have the knowledge, skills (and training as needed) as described for OE.NOEVIL. Ensure each remote administrative account has a unique password by following guidance in the document to force password resets at next login whenever one administrator creates or resets a password for another administrator.
OE.SINGEN	Information cannot flow among the internal and external networks unless it passes through the TOE.	Configure the networks around the system such that traffic that should traverse the system cannot bypass the system. For example, per the topology shown in Figure 1 Depiction of a CC-Evaluated Deployment of Firepower and Secure Client**Error! Reference source not found.**, ensure that traffic from one protected network (or a remote access VPN client workstation) is not able to reach (has no routable path to) another protected network without passing traffic through an FTD appliance.

1.7 Document References

Documentation References

The Cisco Firepower/Secure Firewall System documentation set includes online help and PDF files.

The following product guidance documents are provided online (see links provided below) or by request:

This Configuration Guide

Cisco Secure Firewall Threat Defense (FTD) 7.4 with FMC and Secure Client Preparative Procedures & Operational User Guide for the Common Criteria Certified Configuration (April 19)
This document is downloadable from:
https://www.cisco.com/c/en/us/solutions/industries/government/global-government-certifications/common-criteria.html

Secure Firewall Management Center (FMC) Appliances

[FMC-HIG] FMC Hardware Installation Guides:
Cisco Secure Firewall Management Center 1700, 2700, and 4700 Hardware Installation Guide (27-Nov-2023)

Secure Firewall Management Center (FMC)

[FMC-GS] FMC Getting Started Guides:
Cisco Secure Firewall Management Center 1700, 2700, and 4700 Getting Started Guide (28-Nov-2023)

[FMC-CG] FMC Configuration Guide
Cisco Secure Firewall Management Center Device Configuration Guide, 7.4 (7-Sep-2023)

[FMC-AG] FMC Administration Guide
Cisco Secure Firewall Management Center Administration Guide, 7.4 (7-Sep-2023)

[FMC-UG] FMC Upgrade Guide
Cisco Secure Firewall Threat Defense Upgrade Guide for Management Center, Version 7.4.1 (13-Dec-2023)

[FMC-RN] Firepower Release Notes, Version 7.4
Cisco Secure Firewall Threat Defense Release Notes, Version 7.4.x (10-Jan-2024)

Firepower/Secure Firewall 1000/1100, 3100 and 4200 Appliances

[FP1k-HIG] Firepower 1010/1100 Series Hardware Installation Guide
Cisco Firepower 1010 Series Hardware Installation Guide (24-Jul-2019)
Cisco Firepower 1100 Series Hardware Installation Guide (13-Nov-2019)

[FP3k-HIG] Secure Firewall 3100 Series Hardware Installation Guide
Cisco Secure Firewall 3100 Series Hardware Installation Guide (5-Feb-2024)

[FP4200-HIG] Firepower 4200 Series Hardware Installation Guides
Cisco Secure Firewall 4200 Series Hardware Installation Guide (16-May-2022)

Firepower/Secure Firewall Threat Defense (FTD)

[FTD-RG] Firepower Threat Defense Reimage Guide
Cisco Secure Firewall ASA and Secure Firewall Threat Defense Reimage Guide (11-Dec-2023)

[FP1k-GS] Firepower 1100 Getting Started Guide
Cisco Firepower 1010 Getting Started Guide (26-Jan-2024)

[FP3k-GS] Secure Firewall 3100 Getting Started Guide
Cisco Secure Firewall 3100 Getting Started Guide (26-Jan-2024)

[FP4200-GS] Secure Firewall 4200 Getting Started Guide
Cisco Secure Firewall 4200 Getting Started Guide (26-Jan-2024)

[FTD-CR] FTD Command Reference
Cisco Firepower Threat Defense Command Reference (04-Jan-2024)

[FTD-SYSLOG] FTD Syslog Messages:
Cisco Firepower Threat Defense Syslog Messages (13-Dec-2023)

Cisco Secure Client

[SC-INSTALL]
Cisco Secure Client (including AnyConnect) Administrator Guide, Release 5.1 (25-Mar-2024)

[SC-ADMIN]
Cisco Secure Client (including AnyConnect) Administrator Guide, Release 5.1 (25-Mar-2024)

[SC-RN]
Release Notes for Cisco Secure Client (including AnyConnect), Release 5.1 (13-DEC-2023)

The most up-to-date versions of the documentation can be accessed on the Cisco Support web site (http://www.cisco.com/c/en/us/support/index.html).

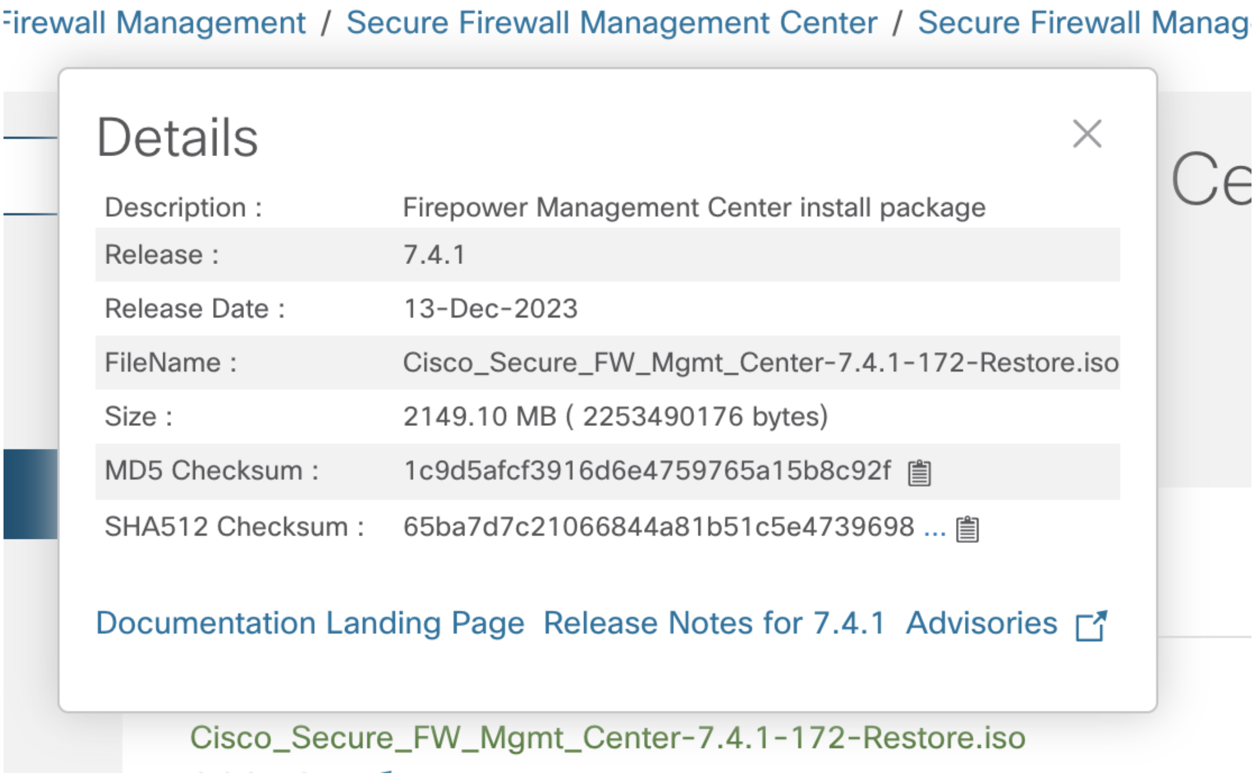
1.8 Obtaining and Verifying Cisco Software

All the Cisco software mentioned in this guide is available for download from https://software.cisco.com, using the procedures below.

- **FMC:** Search for “Secure Firewall Management Center” then select any model (all FMC models listed in section use the same software images), then select “7.4” and download “Firepower Management Center system software” or “Firepower Management Center upgrade”.
- **FTD on 1k:** Search for “Firepower 1000 Series” then select any model (all 1000/1100 series models use the same software images), then select “Firepower Threat Defense (FTD) Software” then select “7.4” and download the “Firepower Threat Defense install package for the Firepower 1000 series” or the “Firepower Threat Defense upgrade”.
- **FTD on 3k:** Search for “Secure Firewall 3100 Series” then select any model (all 3100 series models use the same software images), then select “Firepower Threat Defense (FTD) Software” then select “7.4” and download the “Firepower Threat Defense install and upgrade for the Firepower 3100 series”.
- **FTD on 4200:** Search for “Secure Firewall 4200 Series” (all 4200 series use the same software images), then select any model, then select “Firepower Threat Defense (FTD) Software” then select “7.4” and download the “Firepower Threat Defense install and upgrade package for the Firepower 4200 series”.

- **Secure Client:** Search for "Secure Client 5" then select "5.1" then download the "Cisco Secure Client Pre-Deployment Package (Windows) - includes individual MSI files".

When downloading each file, note the SHA512 checksum, which is visible by hovering a mouse pointer over each download link, and clicking the clipboard icon to copy the checksum to your computer's clipboard as shown in in the figure below. After downloading each software image, verify its integrity by calculating the SHA512 checksum of each downloaded by using checksum utilities available on your system (e.g. "sha512sum <filename>" on Linux, or "certutil -hashfile <filename> SHA512" on Windows), and confirm the calculated checksum of the downloaded file matches the expected checksum as shown on software.cisco.com.



irewall Management / Secure Firewall Management Center / Secure Firewall Manag

Details

Description :	Firepower Management Center install package
Release :	7.4.1
Release Date :	13-Dec-2023
FileName :	Cisco_Secure_FW_Mgmt_Center-7.4.1-172-Restore.iso
Size :	2149.10 MB (2253490176 bytes)
MD5 Checksum :	1c9d5afcf3916d6e4759765a15b8c92f
SHA512 Checksum :	65ba7d7c21066844a81b51c5e4739698 ...

Documentation Landing Page Release Notes for 7.4.1 Advisories

Cisco_Secure_FW_Mgmt_Center-7.4.1-172-Restore.iso

Figure 2: SHA512 Checksum on software.Cisco.com.

When installing FMC, the software integrity is verified through use of digital signature verification at the time of installation. The integrity of all updates and patches uploaded to FMC (FMC updates, and FTD updates) is also verified through use of digital signatures at the time of upload.

1.9 Modes of Operation

Note: Each TOE component is considered to be in a **pre-installation** state, and the CC-evaluated security functionality cannot be assumed to be in effect, until all procedures outlined in this document have been completed for each TOE component.

1.9.1 Modes of Operation for FMC

Startup: During normal startup the boot loader (LILO) mounts the file systems, runs file integrity verification of the kernel and binary files, and loads the kernel, which starts processes (applications including database, webserver, etc.). Near the end of the normal startup the administrative web server

WebUI may be remotely accessible, but instead of displaying a login prompt the web server will display a system message indicating that login is temporarily unavailable until startup completes. If the boot loader detects a file integrity error, the system will automatically restart. If any applications fail to load during startup the system will be in a partially failed state in which the console CLI, including local authentication mechanisms, will be accessible for troubleshooting purposes, but the web servers (administrative WebUI, and sftunnel) will remain inaccessible.

Shutdown: ***Normal shutdown*** can be initiated by an authorized administrator via the CLI or WebUI. Once initiated, system processes will be stopped in a pre-determined sequence to maintain integrity of all system information. Once the shutdown completes, the appliance will either automatically power off, or if the shutdown was initiated as a ***restart***, the system will automatically begin startup.

Operational: ***Normal operation*** consists of all essential processes running, including databases, web servers (remote administrative WebUI, and sftunnel connections with FTD), SSH server (if enabled), etc. The FMC would be in ***partially failed*** state if one or more essential processes halts or fails to start. If a process halts or fails to start the FMC will automatically attempt to restart it, and will display an error to the console indicating which process has failed to start. The FMC would be in a ***fully failed*** state in the event of loss power loss or in the event of a kernel crash. In the case of a kernel crash the FMC will automatically attempt to restart. In the case of power loss the FMC may require manual intervention to restore power, then press the power button on the appliance. With either type of full failure there is a risk of data corruption because much of the FMC data is stored in databases, and if the databases are not shutdown properly they can become corrupted. If data corruption occurs, contact Cisco TAC for assistance. FMC does support backup and restore procedures, but those procedures are beyond the scope of the Common Criteria certification, and were not tested during the CC evaluation.

1.9.2 Modes of Operation for FTD

Startup: During normal startup the boot loader runs file integrity verification of the system image, then loads the image. If the boot loader detects a file integrity error, the system will automatically restart. If any applications fail to load during startup the system will be in a partially failed state in which the console CLI, including local authentication mechanisms, will be accessible for troubleshooting purposes, As the startup completes the TLS communication with FMC, and SSH server (if enabled) become remotely accessible. Until startup completes, the FTD does not forward any traffic across any of its data interfaces.

Shutdown: ***Normal shutdown*** can be initiated by an authorized FTD administrator via the FTD CLI, or by and FMC administrator via the FMC WebUI. Once initiated, system processes will be stopped in a pre-determined sequence to maintain integrity of all system information. Once the shutdown completes, the appliance will either automatically power off, or if the shutdown was initiated as a ***restart***, the system will automatically begin startup.

Operational: ***Normal operation*** consists of all essential processes running, including the SSH server (if enabled), and enforcement of all Access Control Policies and VPN Policies. The FTD would be in ***partially failed*** state if one or more essential processes halts or fails to start. If a process halts or fails to start the FTD will automatically attempt to restart it, and will display an error to the console indicating which process has failed to start. The FTD would be in a ***fully failed*** state in the event of loss power loss or in the event of a kernel crash. In the case of a kernel crash or temporary loss of power the FTD will automatically attempt to restart.

1.9.3 Modes of Operation for Secure Client

Startup: During normal startup of the Secure Client client, Secure Client runs a self-test of its internal cryptographic library then runs an integrity check of its own binary (executable) files. If the self-tests or integrity tests fail, Secure Client will generate an error, and will not reach an operational state.

Operation: During normal operation, the Secure Client client state is either **connected** with or **disconnected** from the VPN gateway (FTD). Between being disconnected and connected the Secure Client client will be **authenticating** with the FTD. The process of authenticating will transfer the local client X.509v3 certificate to FTD, and will prompt the VPN user for a username and password (if the FTD indicates to Secure Client during authentication that such credentials are required). Once authentication has successfully completed, Secure Client receives from FTD hash (checksum) values of FTD's currently configured VPN Client Profile, and Secure Client version information, which Secure Client uses to determine whether it needs to download new versions from FTD (over TLS). If any update is required, Secure Client start initiate **downloading**. If the downloading included receipt of a new version of Secure Client, the new version of Secure Client will enter startup mode.

2 FMC Installation

2.1 FMC Fundamentals

FMC includes an operating system, and applications including an SSH server (for remote administration via CLI), a web server (for remote administration via WebUI from a web browser), and database (for storage of policies and audit messages). FMC is primarily configured via the WebUI, and in the CC-evaluated configuration the vast majority of CLI functionality is disabled. Regardless, it may occasionally be necessary to login to the CLI (via console) to perform some system maintenance, such as shutting down or restarting the appliance. Be aware that the default username for the CLI and the WebUI are the same, 'admin', and have the same default password, 'Admin123', but they are separate accounts, so when their default passwords are changed the new password for each admin account should be unique.

2.2 FMC Installation

To complete installation and initial configuration of FMC:

1) Refer to the correct FMC Hardware Installation Guide [FMC-HIG] for your hardware model to complete the tasks of mounting the appliance, connecting the console cable, and connecting power.
2) If the appliance was installed with an earlier version of FMC, follow instructions in the [FMC-UG] to upgrade to FMC 7.4.
3) Refer to the correct FMC Getting Started Guide [FMC-GS] for your hardware model and follow instructions.
    a) Follow "Configure Management Center Administrative Settings" to:
        i) Login to the WebUI.
        ii) Create Individual User Accounts (these are administrative accounts).
        iii) Configure Time Settings
        iv) Configure Smart Licensing for the FMC. (Use of either Smart Licensing or Universal Licenses will enable the FMC to allocate licenses automatically to any managed FTD.)
        v) (Optional) Schedule System Updates and Backups

b) (Skip) “Add Managed Devices to Management Center” (Skip this section for now because these steps will be covered later when one or more FTDs have is installed.)

   i) DO NOT follow the steps under “Set Up Lights Out Management User Access Configuration”. This feature uses the IPMI protocol for remote authentication, and the IPMI protocol is not secure enough to be used in the CC-evaluated configuration.

c) (Optional) Preconfigure FMCs

d) (Optional) Managing the Firepower Management Center User the System Restore Utility

e) DO NOT Erase the Hard Drive unless you intent to fully reinstall the appliance, or return it to Cisco, or dispose of it.

2.2.1 Check Installed Version

To check that the correct certified version of FMC is installed, you can execute one of the following commands:

- Version is shown in FMC GUI under: System > Updates.
- Version is shown in FMC CLI output of “show version”.

3 FMC Initial Configuration

3.1 Configure Authentication

FMC has two local user stores with separately maintained accounts, one set is used for CLI access, and the other is used for WebUI/GUI access. The default username and password for the CLI administrative and the GUI administrator are the same, the username is ‘admin’, and the default password is ‘Admin123’, but the default password is changed during initial setup, so after initial setup the passwords for each ‘admin’ account should continue to be unique.

To change the GUI admin password, or to create additional GUI accounts, refer to the “Add or Edit an Internal User” section in the “Users” chapter of [FMC-AG].

To enable RADIUS authentication, refer to the “Configure External Authentication for the Management Center” section in the “Users” chapter of [FMC-AG]. Enabling RADIUS on FMC is optional in the CC-evaluated configuration, but use of LDAP is outside the scope of evaluation, so enabling LDAP is prohibited.

> ***Note:*** *If the FMC will be configured to use RADIUS, the connection between the FMC and the RADIUS server should be protected from outside interference (e.g. attacks on the integrity or confidentiality of data-in-transit). The RADIUS server will be located on a trusted management network accessible from FMC.*

The bullets below summarize the secure settings required for FMC accounts. For more information refer to the “Requirements and Prerequisites for User Accounts” section of [FMC-AG].

Mandatory Security Parameters for FMC WebUI Accounts:

- Ensure that the “Maximum Number of Failed Logins” for each account is not disabled by ensuring the value is greater than zero (0). By default, for new accounts when CC mode is enabled is five (5) failed logins. For the CC-evaluated configuration, it is recommended to not exceed the 5-10 range for the failed login attempts.

- Configure the "Set Time in Minutes to Temporarily Lockout Users" to a non-zero number of minutes. The default is zero (0), which is a zero-duration lockout, essentially disabling lockout. The maximum is 1440 minutes (24 hours).
- When CC mode has been enabled on FMC (see section 3.7 below), FMC will enforce a minimum password length of 15 characters for all accounts. The minimum length will only be enforced when new passwords are set, including when new accounts are added, so change passwords for all existing accounts after enabling CC mode. Optionally, the value can be set higher than 15 individually for each account.

Optional Security Parameters for FMC WebUI Accounts

- Enabling a password strength check is optional, and can be enabled or disabled individually for each account.
- Setting the "Days Until Password Expiration" is optional. The default value is zero (0), which is unlimited.
- Setting the "Password Reuse Limit" is optional. The default is zero (0), which is unlimited.
- Setting the number of days to "Track Successful Logins" is optional. The default is zero (0), which is disabled (no tracking).
- Setting the "Password Reuse Limit" is optional. The default is zero (0), which is unlimited.
- To ensure each unique administrative account has a unique password that is not known to other administrators set the "Force Password Reset on Login" parameter whenever one administrator is creating a new account for another administrator or resetting a password for another administrator. This will force the other administrator to change their password at their next login.

Unconfigurable Security Parameters for FMC CLI Account:

- New passwords must meet password strength requirements (mixed-case, alpha-numeric, with a special character).

3.2 Configure the Pre-Login Banner

Create a custom login banner that will appear during login attempts via CLI or GUI. Banners can contain any printable characters except the less-than symbol (<) and the greater-than symbol (>). To configure the pre-login banner for FMC refer to the "Login Banner" section of [FMC-AG], which is summarized here:

1) Login to the FMC WebUI.
2) Navigate to **System > Configuration > Login Banner**.
3) In the **Custom Login Banner** field enter the login banner text you want to use.
4) Click **Save**.

3.3 Configure the Clock

Configure the clock manually or configure use of NTP. It's recommended to configure one or more NTP servers with which FMC will synchronize its clock. To configure the clock and NTP for FMC refer to the "Time Synchronization" section of [FMC-AG]. If the FMC is managing some FTD instances running on 4200 platforms, the FMC should be configured to use NTP servers to ensure the FMC and FTD instances maintain consistent clocks, particularly for writing timestamps into log messages.

> ***Note:*** *If the FMC will be configured to use NTP, the connection between the FMC and the NTP server should be protected from outside interference (e.g. attacks on the integrity of data-in-transit). The NTP server will be located on a trusted management network accessible from FMC.*

3.4 Configure Inactivity Timeout Settings

By default, all user sessions (web-based and CLI) automatically log out after 60 minutes (1 hour) of inactivity, though the limit is configurable separately for CLI sessions (shell timeout) and for WebUI sessions (browser session timeout). Users with Administrator Role can change the inactivity timeout value in the system policy to meet their security needs.

Note: The FMC WebUI supports the ability to exempt individual WebUI accounts that don't have the 'administrator' role from having the Browser Session Timeout apply to their sessions, but to adhere to the CC-evaluated configuration do not exempt any account from the Browser Session Timeout, regardless of the role(s) assigned to that account.

To configure the ShellTimeout (for CLI) and the Browser Session Timeout (for WebUI) for FMC refer to the "Configure Session Timeout" section of [FMC-AG], which is summarized here:

1) Login to the FMC WebUI.
2) Navigate to **System** > **Configuration** > **Session Timeout**.
3) Set the **Browser Session Timeout** value to any integer from 5-1440 minutes (24 hours) (default is 60 minutes, and for security reasons it's recommended to set the timeout value to no more than 60 minutes)
4) Set the **CLI Timeout** value to any integer from 5-1440 minutes (24 hours) (default is 60 minutes, and for security reasons it's recommended to set the timeout value to no more than 60 minutes)
5) Click **Save**.

3.5 Configure Logging (optional)

Audit messages on FMC are stored separately in two main categories: the "System Log" stores syslog messages (for system-level events, including CLI login/logout events); and the "Audit Log" stores messages as database records (for configuration changes via WebUI or CLI, and for IPS events). System messages are viewable via the WebUI under **System** > **Monitoring** > **Syslog**, and audit messages are viewable via the WebUI under **System** > **Monitoring** > **Audit**.

3.5.1 Configure Local Storage of Audit Log Messages (optional)

The local storage of system (syslog) messages (those viewable under **System** > **Monitoring** > **Syslog**) is not configurable.

To review the current storage limits for messages stored in the database (those viewable under **System** > **Monitoring** > **Audit**), look in the WebUI under **System** > **Configuration** > **Database**. The database that holds the events related to administrative actions via the WebUI are stored in the "Audit Event Database". To configure these values click on **Help** > **Online** while viewing that page, or refer to guidance in the "Configuring Database Event Limits" section of [FMC-AG].

3.5.2 Configure Use of a Remote Logging Server (optional)

The system (syslog) messages that are stored locally (those viewable under **System** > **Monitoring** > **Syslog**) cannot be transmitted to a remote logging server.

To enable transmission of audit messages to a remote server, navigate to **System** > **Configuration** > **Audit Log**, and follow the instructions in the "Stream Audit Logs to Syslog" section of [FMC-AG].

3.5.3 Configure Access Lists for Remote Administration (optional)

By default, FMC will accept incoming SSH and HTTPS connections from any source IP address, but FMC can be configured to allow incoming connections only from specified IP subnets or IP addresses, or to deny access from all access. To configure those rules, use the **System > Configuration > Access List** page of the WebUI, and refer to the "Configure an Access List" section of [FMC-AG] for further instructions.

To avoid disruption of HTTPS connectivity, it is recommended to new rules to allow HTTPS (port 443) from necessary subnets/addresses before deleting the default rule that allows those ports from all source addresses.

Inbound connectivity using SSH is enabled by default (permitted by a default Access List rule). To disable SSH access, delete all rules from the access list to port 22, then click the "Save" button.

Inbound connectivity using SNMP is disabled by default (not permitted by any Access List rule) and inbound SNMP access must remain disabled in the CC-evaluated confirmation, so do not create any rule that would allow inbound SNMP.

3.6 Disable the REST API

Use the FMC WebUI to disable the FMC REST API by unchecking the "Enable REST API" box under: **System > Configuration > REST API Preferences > Enable REST API**.

3.7 CC Mode and FIPS Mode

Enabling CC Mode on FMC is required to enable automated locking of the default 'admin' account when it's used to login remotely via the WebUI. For a summary of other characteristics of CC Mode, and for instructions to enable CC mode, refer to the "Security Certifications Compliance" section of [FMC-CG].

> ***Warning:*** *After enabling FIPS Mode or CC Mode on FMC those modes cannot be disabled. Disabling these modes would require reinstallation of FMC.*

3.8 Configure CLI Lockdown on FMC

During this initial configuration the CLI access will become greatly limited from the default behavior, and once that change has been made, nearly all administrative activity will be performed via the GUI. By default the default CLI shell is a Linux shell with ability to traverse the Linux file system. Access to that shell must be disabled in the CC-evaluated configuration. For further information about the FMC CLI, refer to the "Secure Firewall Management Center Command Line Reference" section of [FMC-AG].

To lock-down the CLI access, complete these steps:

1) Enable the custom FMC shell, which has limited functionality.
    a) Within the FMC GUI, navigate to **System > Configuration > Console Configuration**.
    b) The "Console" selection can be left at the default "Physical Serial Port" option, or can be changed to "VGA" but do not select "Lights Out Management".

> ***Note:*** *The Lights Out Management (LOM) option uses the IMPI protocol for remote serial-over-LAN (SOL) access to the CLI, and use of IMPI is not permitted in the CC-evaluated configuration.*

    c) Click "Save"

Note: Choosing “Enable CLI Access” changes the initial shell from the Linux filesystem shell to a limited shell that only provides the `following` commands:

```
> ?
configure  Change to Configuration mode
exit       Exit this CLI session
expert     Invoke a shell
show       Change to Show Mode
system     Change to System Mode
>
```

Warning: *Before completing the next step, ensure there is no need to access the Linux filesystem shell. Before completing the next step the Linux shell is still accessible by using the “expert” command. After completing the next step use of the “expert” command will be disabled.*

Note: *Note, access to the Linux shell is required for regenerating the SSH key pair.*

Note: *“system lockdown” does not disable Linux shell access for the current CLI session. The effects of the “system lockdown” command take affect on all subsequent CLI sessions.*

Warning: *If you need to access the Linux shell after this step, you need to contact Cisco TAC for assistance. Cisco TAC could use a challenge-response key to gain access to the Linux shell for troubleshooting purposes, or could install a ‘hotfix’ to re-enable use of the “expert” command, but use of that hotfix is prohibited in the CC-evaluated configuration.*

Note: *For the configuration changes to take effect, the administrator needs to logout and log back in.*

2) Login to the CLI (via console or SSH), and use the “system lockdown” command.

4 FTD Installation (all platforms)

4.1 Platform-Specific Differences

The CC-evaluated configuration includes deployment of FTD on multiple hardware platforms. All the platforms run an instance of FXOS that provides management of the hardware, and loads the FTD applications (firewall, VPN, and IPS). However, there are three separate sets of FTD images across the platforms, and there are some importance differences among those three images.

In the subsections below, headings will include platform-specific abbreviations (1k, 3k, 4200) wherever guidance is only applicable to a subset of platforms. Where no platform is specified in the section heading, the guidance is applicable to all platforms.

4.1.1 Image ‘Bundles’

4.1.1.1 Installation Images

FTD on 1k/3k/4200 (FXOS and FTD are bundled): FXOS and FTD are installed on 1k, 3k and 4200 platforms as a single image ‘bundle’ that includes FXOS and FTD. Once installed, the appliance can be reinstalled using the FXOS CLI, which would overwrite the FXOS and FTD images. Once FTD is being managed by an FMC, updates can be pushed from FMC to FTD, and updates can include updated code for FXOS as well as FTD.

4.1.1.2 Update Images (hotfixes, patches, updates, and upgrades)

FTD applications (firewall, VPN, IPS) on 1k/3k/4200: Once FTD has been installed on any platform, and FTD has been joined with an FMC such that the FMC is the 'manager' of the FTD, all FTD software updates are pushed to FTD directly from FMC, not from the FXOS on the 1k/3k/4200 chassis.

FXOS of FTD on 1k/3k/4200: Any updates to FXOS on 1k/3k/4200 are included in the FTD updates pushed to FTD from FMC.

4.1.2 Firepower Device Management (FDM) WebUI

Firepower Device Management is a WebUI (web-based user interface, accessible via a web browser) that can be used to manage a Firepower/Secure Firewall.

1k, 3k and 4200 platforms include a WebUI for managing FTD, called Firepower Device Manager (FDM), but FDM is only enabled if FTD is in a standalone configuration. When FTD is 'managed' by FMC, as FTD will always be the case in the CC-evaluated configured, the FDM is automatically disabled.

4.1.3 Fundamentals of 1k, 3k and 4200 Series Appliances

4.1.3.1 One 'admin' Account for the Platform

Multiple CLI shells on the 1k/3k/4200 platforms work in tandem to provide limited CLI functionality accessible via local serial console and via SSH. Regardless of whether the CLI accessed is initiated via console or SSH, the same authentication mechanism is used, using the same accounts, same credentials, and presenting the same customizable pre-login banner.

4.1.3.2 Multiple CLI Shells, All Limited

The CLI on the 1k. 3k and 4200 platforms provides three shells, the "fxos" shell, the "local-mgmt" shell, and the "ftd" shell, all of which provide different, and very limited configuration options. For example, the admin password can only be changed via the "ftd" shell, and the pre-login banner cannot be changed via any shell, it can only be configured via FMC.

When logging in to a 1k, 3k or 4200 appliance via the console, the initial shell is the "fxos" shell, whereas logging in via SSH will initially present the "ftd" shell. Once the administrator has logged in via console or SSH, the administrator can navigate among the three shells by using the commands "connect fxos", "connect local-mgmt", or "connect ftd". Typing "exit" will return to the previous shell, or will terminate the session if the administrator has already returned to the initial shell.

The fxos shell provides many commands to "set" configuration parameters, but changes are not saved without use of the "commit-buffer" command, and once FTD is being managed by FMC very few configuration changes can be saved via the "fxos" shell and most use of "commit-buffer" will result in, "Error: Changes not allowed. use: 'connect ftd' to make changes." The fxos shell blocks simple changes, such as changing the admin password (after first changing via the initialization wizard). Attempting to save changes via the fxos shell will display an error when attempting to commit those changes, as in this example:

```
Firepower /security # set password
Enter new password:
Confirm new password:
Firepower /security* # commit-buffer
Error: Changes not allowed. use: 'connect ftd' to make changes.
Firepower /security* #
```

The “local-mgmt” shell does not provide any commands that could result in changes to the configuration. This shell only provides limited commands for troubleshooting, such as “ping” and “traceroute”. The “ftd” shell allows some limited configuration changes, such as adding or deleting the FTD’s ‘manager’ (the FMC), changing the ‘admin’ password, and configuring some syslog settings, but no firewall or VPN configurations can be modified via the ftd shell (all Access Control Policies, Peer-to-Peer VPN policies, and Remote Access VPN policies must be configured and deployed via FMC). The following example shows how the ftd shell allows setting the IP addresses that are allowed to initiate SSH access to FTD, but does not allow configuring HTTP access because the WebUI of FTD, called Firepower Device Manager (FDM), is always automatically disabled when FTD is managed by an FMC (i.e. when the “local manager” of FTD is not active).

```
> configure ssh-access-list 10.0.0.0/8
The ssh access list was changed successfully.
> configure https-access-list 10.0.0.0/8
Changes to https access list can only be made when local manager is active.
>
```

4.1.3.3 *No WebUI Access*

Once the FTD on 1k/3k and 4200 platforms has been configured to be ‘managed’ by an FMC, the WebUI, called Firepower Device Manager (FDM) is always automatically disabled.

4.1.3.4 *Clock Synchronized with FMC*

Once the FTD on 1k/3k and 4200 is being managed by an FMC, the Platform Settings for the FTD (as configured via FMC) allow the FTD clock to be synchronized automatically with the FMC, and that is the recommended configuration. In this configuration, the FTD clock will receive clock updates from FMC and will automatically push those clock updates to FXOS. Optionally, the Platform Settings can be configured (via FMC) such that the platform will communicate directly with one or more NTP servers. In that configuration the FXOS will synchronize its clock with an external NTP server and the FXOS clock will automatically update the FTD clock.

4.2 FTD Installation and FTD Registration to FMC

4.2.1 Installing the FTD Image Bundle on 1k/3k/4200

Firepower 1010, 1010E:

a) Refer to the Cisco Firepower 1010 Hardware Installation Guide [FP1k-HIG] to mount the appliance, connect the console cable, and connect power.
b) If reimaging is required, refer to the “Reimage the Firepower 1000/2100; Secure Firewall 3100/4200” section of the Cisco ASA and Firepower Threat Defense Reimage Guide [FTD-RG].
c) Refer to the “Firepower Threat Defense Deployment with FMC” chapter of the Cisco Firepower 1010 Getting Started Guide [FP1k-GS] to connect power and cabling, complete the initial configuration, and register the FTD with an FMC.
d) To continue configuration of FTD refer to “FTD Post-Installation Configuration” (section 5) of this document.

Firepower 1120, 1140 and 1150:

a) Refer to the Cisco Firepower 1100 Series Hardware Installation Guide [FP1k-HIG] to mount the appliance, connect the console cable, and connect power.
b) If reimaging is required, refer to the “Reimage the Firepower 1000/2100; Secure Firewall 3100/4200” section of the Cisco ASA and Firepower Threat Defense Reimage Guide [FTD-RG].

c) Refer to the “Firepower Threat Defense Deployment with FMC” chapter of the Cisco Firepower 1100 Getting Started Guide [FP1k-GS] to connect power and cabling, complete the initial configuration, and register the FTD with an FMC.
d) To continue configuration of FTD refer to “FTD Post-Installation Configuration” (section 5) of this document.

Firepower 3105, 3110, 3120, 3130, and 3140:

a) Refer to the Cisco Secure Firewall 3100 Series Hardware Installation Guide [FPk-HIG] to mount the appliance, connect the console cable, and connect power.
b) If reimaging is required, refer to the “Reimage the Firepower 1000/2100; Secure Firewall 3100/4200” section of the Cisco ASA and Firepower Threat Defense Reimage Guide [FTD-RG].
c) Refer to the “Firepower Threat Defense Deployment with FMC” chapter of the Cisco Secure Firewall 3100 Getting Started Guide [FP3k-GS] to connect cabling, complete the initial configuration, and register the FTD with an FMC.
d) To continue configuration of FTD refer to “FTD Post-Installation Configuration” (section 5) of this document.

Firepower 4215, 4225 and 4245:

a) Refer to the Cisco Secure Firewall 4200 Series Hardware Installation Guide [FP4200-HIG] to mount the appliance, connect the console cable, and connect power.
b) If reimaging is required, refer to the “Reimage the Firepower 1000/2100; Secure Firewall 3100/4200” section of the Cisco Secure Firewall ASA and Secure Firewall Threat Defense Reimage Guide [FTD-RG].
c) Refer to the “Firepower Threat Defense Deployment with FMC” chapter of the Cisco Secure Firewall 4200 Getting Started Guide [FP4200-GS] to connect cabling, complete the initial configuration, and register the FTD with an FMC.
d) To continue configuration of FTD refer to “FTD Post-Installation Configuration” (section 5) of this document.

4.2.2 *Check Installed Version*

To check that the correct certified version of FTD is installed, you can execute one of the following commands:

- Version is shown in ***FMC*** GUI under: Devices > Device Management.
- Version is shown in FTD CLI output of “show version”.

5 FTD Post-Installation Configuration (all platforms)

Unless indicated otherwise within the text below, the instructions in this section are applicable to FTD running on all hardware platforms (Firepower 1000/1100 Series, 3100 Series and 4200 Series).

5.1 Ensure FTD is Managed by FMC

If the FTD ‘manager’ was not configured on FTD via the setup wizard that runs on FTD during initial login, the manager can be configured later using the “configure manager add” command. Refer to the “Firepower Threat Defense Deployment with FMC” chapter of the platform-specific Getting Started Guide [FMC-GS] to configure licensing, and register the FTD with an FMC.

Once an FTD has been joined with an FMC, removing the FTD from FMC (using the “configure manager delete” command on FTD) would remove the FTD from its CC-evaluated configuration. If it becomes necessary to remove an FTD from FMC, the FTD must be re-joined with the same or different FMC (configured in accordance with this guide), and the FTD Platform Policy must be deployed to the FTD to return the FTD to the CC-evaluated configuration.

5.2 Enable CC Mode and FIPS Mode

CC Mode is not enabled by default, but must be enabled in the CC-evaluated configuration. After CC Mode is enabled, the mode cannot be disabled nor changed to another mode. Enabling either CC Mode will implicitly also enable FIPS Mode. For an overview of the of the non-default security features enforced when CC Mode is enabled, refer to the "Security Certifications Compliance Characteristics" section of [FMC-CG].

> ***Warning:*** *After enabling FIPS Mode or CC Mode on FTD those modes cannot be disabled. Disabling these modes would require reinstallation of FTD.*

5.2.1 FIPS Mode

Enabling FIPS mode will limit algorithms used for HTTPS/TLS and SSH to ones which are permitted by FIPS 140-2, as listed in this CAVP certification: https://csrc.nist.gov/projects/cryptographic-algorithm-validation-program/details?product=740 To enable FIPS mode on FTD, enable CC Mode as described in the next subsection of this guide.

5.2.2 Common Criteria (CC) Mode

Enabling CC mode will limit algorithms used for HTTPS/TLS and SSH to ones listed below, and will implicitly enable FIPS Mode. To enable CC mode, refer to the "Enable Security Certifications Compliance" section of [FMC-CG] and follow instructions to configure the "FTD device" as summarized here:

1) In FMC, navigate to Devices > Platform Settings and create a Firepower Threat Defense Policy if one has not already been created for your FTD.
2) In FMC, navigate to Devices > Platform Settings > UCAPL/CC Compliance, and set the compliance mode to "CC".
3) Click "Save".
4) Deploy the Platform Policy to the FTD. This will result in rebooting the FTD, and regenerating SSH keys on the FTD.

SSH will be limited to SSHv2 with these algorithms:

- Encryption: aes128-cbc, aes256-cbc, AEAD_AES_128_GCM, AEAD_AES_256_GCM
- HMAC: hmac-sha1, hmac-sha2-256, hmac-sha2-512, AEAD_AES_128_GCM, AEAD_AES_256_GCM
- ECDH: ecdh-sha2-nistp384
- Key Exchange: ecdh-sha2-nistp384, kex-strict-s-v00@openssh.com

The TLS ciphersuites used between FTD and FMC are limited to:

- TLS_RSA_WITH_AES_128_CBC_SHA as defined in RFC 3268 (TLSv1.2)
- TLS_RSA_WITH_AES_256_CBC_SHA as defined in RFC 3268 (TLSv1.2)
- TLS_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246 (TLSv1.2)
- TLS_RSA_WITH_AES_256_CBC_SHA256 as defined in RFC 5246 (TLSv1.2)
- TLS_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5288 (TLSv1.2)
- TLS_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288 (TLSv1.2)
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA as defined in RFC 3268 (TLSv1.2)
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA as defined in RFC 3268 (TLSv1.2)

- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246 (TLSv1.2)
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 as defined in RFC 5246 (TLSv1.2)
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA as defined in RFC 4492 (TLSv1.2)
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA as defined in RFC 4492 (TLSv1.2)
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289 (TLSv1.2)
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289 (TLSv1.2)
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289 (TLSv1.2)
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289 (TLSv1.2)
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA as defined in RFC 4492 (TLSv1.2)
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA as defined in RFC 4492 (TLSv1.2)
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289 (TLSv1.2)
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289 (TLSv1.2)
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289 (TLSv1.2)
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289 (TLSv1.2)

The TLS ciphersuites used between FTD and a remote syslog server are limited to:

- TLS_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246 (TLSv1.2)
- TLS_RSA_WITH_AES_256_CBC_SHA256 as defined in RFC 5246 (TLSv1.2)
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289 (TLSv1.2)
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289 (TLSv1.2)
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289 (TLSv1.2)
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289 (TLSv1.2)
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289 (TLSv1.2)
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289 (TLSv1.2)
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289 (TLSv1.2)

Note: The web server on FTD (Firepower Device Manager, FDM) is disabled whenever FTD is managed by (has been registered to) an FMC.

Note: No TLS versions other than those listed above are supported on these products, thus there’s no risk of a remote client triggering a ‘downgrade’ to an older SSL/TLS version.

5.3 Configure Authentication

FTD supports multiple locally stored administrative accounts, each of which is assigned one of two roles, either “config” (read-write) or “basic” (read-only). Accounts can only be managed via the “ftd” shell. Each account can be configured with its own parameters.

RADIUS is not supported on FTD in the CC-evaluated configuration.

At minimum, to adhere to the CC-evaluated configuration, the default ‘admin’ account must be configured according to the settings listed below. To configure FTD accounts refer to the commands referenced below as descried in [FTD-CR]:

1) Access Level: Any setting is acceptable (either “config” or “basic”).
    a) The access level of the default ‘admin’ account cannot be changed, it’s set to ‘config’.
    b) If additional accounts are created, specify the access level by using the “configure user add” command.
2) Aging: Any setting is acceptable.
3) ForceReset: Any setting is acceptable. To ensure each unique administrative account has a unique password that is not known to other administrators set the “forcereset” parameter whenever one administrator is creating a new account for another administrator or resetting a password for another administrator. This will force the other administrator to change their password at their next login.

4) MaxFailedLogins: Set this limit using the "configure user maxfailedlogins" command.
   a) For the default 'admin' account, and another custom accounts, set the value to a positive integer (from 5-9999).
   b) If that limit of consecutive failed logins occurs, the account will be locked until unlocked by another administrative account that has its access level set to 'config', or when the unlock_time has been exceeded (if configured).
   c) (optional) To configure the unlock_time using the "configure unlock_time" command. The default unlock_time is 30 minutes, configurable from 1-9999 minutes.
5) MinPasswdLen: Set to eight (8) or greater using the "configure user minpasswdlen" command.
6) StrengthCheck: Set to either "enable" or "disable" using the "configure user strengthcheck" command. Once this setting is enabled for a user, the strength check will be enforced the next time that user resets their password (the strength check cannot be enforced on passwords that were set prior to enabling StrengthCheck for that user).

5.4 Configuration the Pre-Login Banner

Configure a pre-login banner that will be displayed prior to entering the administrator password during login to FTD. For an overview of Platform Settings, and how to assign Platform Settings to an FTD, refer to the "Platform Settings" chapter in [FMC-CG]. To configure a pre-login banner for FTD, in FMC navigate to **Devices > Platform Settings > Banner**, enter the login banner in the pre-login banner, and click Save, then deploy the updated Platform Settings to all FTD devices to which the Platform Settings have been assigned. For more detail, refer to the "Configure Banners" subsection of the "Platform Settings" section in [FMC-CG].

5.5 Configure the Clock

Configuring time synchronization for FTD offers 2 options. Synchronization via FMC or direct connection to NTP servers. In the evaluated configuration, "Via NTP from Management Center" (default setting) was tested. To change the default setting go to Devices > Platform Settings > (choose the platform to edit) > Time Synchronization and select "Via NTP from (IP address or FDQN of NTP server)

5.6 Configure Inactivity Timeout Settings

Enable inactivity timeouts for administrative sessions on FTD by following instructions in the "Timeouts" section of [FMC-CG], and adhere to these parameters:

- Set the "Console Timeout" to 5 or more minutes (configurable from 5-1440 minutes, though for security reasons it's recommended to set the timeout value to no more than 60 minutes).
- Setting any other timeout value is optional in the CC-evaluated configuration.

5.7 Disable the HTTP (HTTPS) Server

The FTD has a built-in web server with a WebUI for remote administration, but that interactive WebUI is disabled once the FTD is configured to be 'managed' by an FMC. Though the WebUI is remains enabled by default to support the ability for authenticated administrators to download packet capture files. Use the FMC WebUI to disable the FTD HTTP (HTTPS) server by unchecking the "Enable HTTP Server" box under: **Devices > Platform Settings >** (edit any and all applicable platform settings) **> HTTP > Enable HTTP Server** (uncheck the box), then click Save, then deploy the update to each applicable FTD.

5.8 Configure Logging (optional)

FTD generates audit messages from three internal sources, each of which uses a separate mechanism to transmit messages from FTD to another host:

1) System event messages: These messages include system-level events including clock changes, and authentication of administrators to the FTD CLI.
2) Firewall (Access Control Policy) and VPN messages: These messages can be viewed in the local logging buffer of FTD using the command "show logging".
3) IPS messages: These messages are automatically transmitted by FTD to FMC for storage, and are viewable via the "Audit Log" within FMC.

5.8.1 Transmit FTD System Messages to a Syslog Server (optional)

To transmit FTD system messages to a remote syslog server, follow these instructions:

1) (Optional) Configure use of certificates if enabling syslog-over-TLS:
   a) To display the syslog certificate if present: **show audit-cert**
   b) Import the certificates (the CA chain, the client cert and the client key): **configure audit_cert import**
      i) ***Note***: Import the audit certificate chain first (option 2) before importing the client certificate and private key (option 1).
   c) If necessary, delete the syslog server certs: **configure audit_cert delete**
   d) Optionally, configure use of CRLs for certificate revocation checking: **configure crl [*URL*]**
2) Configure one or more syslog servers:
   a) Display the current syslog server information if present: **show syslog-config**
   b) Configure the syslog server details on the FTD: **configure syslog_server setup**
      i) First it prompts for the server host.
      ii) Next if asks if you want TLS enabled.
      iii) Next it asks if you want Mutual Authentication enabled.
      iv) ***Note 1***: If the syslog server entry is defined by its FQDN, it must be resolvable via DNS.
      v) ***Note 2***: The syslog server must be configured correctly to receive syslog messages from FTD.
   c) If desired, disable the syslog config (server details remain on FTD, and can be re-enabled): **configure syslog_server disable**
   d) If desired, re-enable a syslog server, if it had been disabled: **configure syslog_server enable**
   e) If desired, disable the syslog server config and deletes the config: **configure syslog_server delete**

5.8.2 Transmit Firewall and VPN Messages to a Syslog Server (optional)

To configure firewall and VPN messages to be sent to a remote syslog server, refer to the "Configure Syslog Logging for FTD Devices" section of [FMC-CG], configuring at least the parameters summarized here:

1) In FMC, navigate to **Devices** > **Platform Settings** > **Syslog**.
2) On the "Logging Setup" tab, click the "Enable Logging" box.
3) On the "Logging Destinations" tab, configure at least one entry with the logging destination of "Syslog Servers".
4) On the "Syslog Servers" tab, add at least one syslog server.
    a) Use of either TCP syslog or UDP syslog is allowed in the CC-evaluated configuration.
    b) (Optional) Use of "secure syslog" (syslog-over-TLS) by clicking the "Enable secure syslog" box is allowed in the CC-evaluated configuration, but it has some constraints:
        i) Connections between the FTD and the syslog-over-TLS server cannot occur via the FTD's 'management' interface, these connections must use one of the FTD's data interfaces (specified as a "security zone" or a "named interface").
        ii) Use of X.509v3 certificates is required, including:
            (1) Generating a device certificate for the FTD. For instructions to load syslog server certificates, refer to the "Managing Threat Defense Certificates" section of [FMC-CG].
            (2) Installing the FTD's device certificate to the syslog server.

5.9 Configure CLI Lockdown on FTD

By default, the FTD shell allows use of the "expert" command to transmission from the 'ftd' shell to a Linux shell. This access must be disabled in the CC-evaluated configuration. Once this access is disabled, any future access to the Linux shell will require contacting Cisco TAC and completing a challenge-response key exchange that will temporarily re-enable access to the Linux shell for troubleshooting purposes. Once access to the Linux shell is reactivated the FTD is no longer considered to be in the CC-evaluated configuration.

To prohibit use of the 'expert' command, use the "system lockdown-sensor" command as described in [FTD-CR].

6 FTD Access Control Policies

6.1 FTD Interface Modes: Firewall, IPS-Only, or IDS-Only

FTD interfaces can be configured in firewall mode, which is the default mode for FTD interfaces (where the interface Mode is set to "None"); or FTD interfaces can be in an IPS (Inline Sets) or IDS mode (Passive). When configured as an IPS or IDS interface, the primary functionality of the interface is to provide IPS functionality such as deep packet inspection, IPS signature matching, malware detection, URL filtering, etc. Use of interfaces in IPS or IDS modes does not interfere with the security claims of the CC-evaluated configuration, which only makes traffic flow-control claims related to through-the-box (firewall) traffic, and VPN traffic, but does not make claims about the IPS or IDS functionality of FTD.

Configuring interfaces in IPS or IDS modes is not prohibited in the CC-evaluated configuration, but if any FTD interfaces are configured as IPS-only or IDS interfaces there some essential caveats to ensuring the FTD is operating in the CC-evaluated configuration:

1) The FTD must have at least two interfaces that are configured in firewall mode.
2) VPN gateway functionality is only supported on interfaces configured in firewall mode.

3) Interfaces configured as Inline sets can be configured to enforce CC-evaluated traffic flow controls with respect to firewall functionality, but not VPN gateway functionality.
4) Interfaces configured in Passive mode (or ERSPAN mode) do not violate CC-evaluated traffic flow controls because such interfaces do not forward traffic, nor to Passive interfaces support or enforce any CC-evaluated traffic flow controls because they cannot forward traffic and cannot function as VPN gateway endpoints.

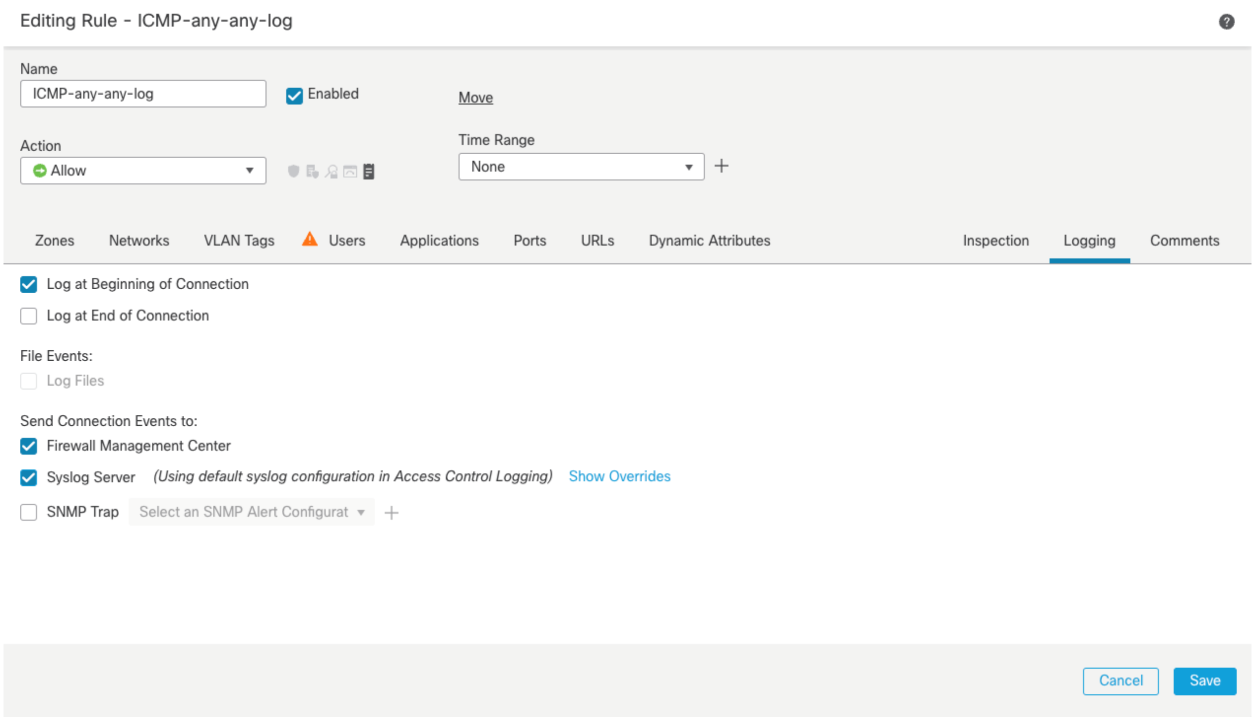
In a Passive mode, an FTD interface will only receive traffic, and will not forward that traffic to any other interface (thus functioning as a sensor interface of an IDS). When configured as an Inline set or in firewall mode, the interface will forward network traffic flows across the FTD (if such traffic is explicitly permitted by Access Control Policies (ACP). One FTD can have multiple interface configurations, for example, where two interfaces are configured as inline pair, and a third interface is configured as passive, and other interfaces are configured in regular firewall mode.

Traffic policies are defined in terms of network “zones”, also called “Security Zones,” which in turn are associated with FTD interfaces. So, an Access Control Policy may be defined to allow traffic from “zone0” to “zone1”, though those zones may be mapped to interfaces labeled “outside” and “inside” on one FTD and the same zones can also be mapped to interfaces labeled “int1” and “int2” of another FTD which enforces the same policy.

There are multiple types of policies that can be layered to apply to the same traffic flows (same zone-to-zone mappings). Having one type of policy applied to a zone/interface is sufficient to allow traffic flow. Traffic flow policy types include Prefilter, Access Control, and Intrusion policies.

Prefilter policies are sub-policies of Access Control policies, and every Access Control policy has an associated Prefilter policy, which is used to define rules for encapsulated traffic. There is no default action for nonencapsulated traffic; if a nonencapsulated connection does not match any prefilter rules, the system continues with applying rules in the Access Control policy. A Prefilter policy can contain multiple rules, which are enforced in the sequence they appear in the policy (the first rule that matches the traffic is the one that’s applied).

No FTD interface will forward traffic until policies have been configured an applied to that interface. Traffic will not be forwarded unless it’s explicitly permitted by at least one policy rule, thus an implicit “deny-all” rule is applied to all interfaces to which any traffic filtering rule has been applied. The implicit deny-all rule is executed after all admin-defined rules have been executed, and will result in dropping all traffic that has not been explicitly permitted, or explicitly denied. If an administrator wants to log all denied traffic, a rule entry should be added that denies all traffic and logs it, e.g. by either adding a rule at the end of a policy to explicitly drop and log all traffic, or by setting the Default Action for the policy to block all traffic, and enabling logging for the default rule, as show in this example:



Editing Rule - ICMP-any-any-log

Name: ICMP-any-any-log ☑ Enabled

Action: Allow

Time Range: None

☑ Log at Beginning of Connection

☐ Log at End of Connection

File Events:

☐ Log Files

Send Connection Events to:

☑ Firewall Management Center

☑ Syslog Server *(Using default syslog configuration in Access Control Logging)* Show Overrides

☐ SNMP Trap Select an SNMP Alert Configurat

6.1.1 *Firewall and VPN Gateway Interfaces*

FTD interfaces configured as firewall interfaces (including interface types labeled as ASA, Routed, or Switched), are interfaces that enforce the CC-evaluated traffic flow controls related to firewall functionality and VPN gateway functionality. Each of these interfaces will:

1) Be associated with a single Security Zone.
2) Enforce Access Control Policies, which are defined in terms of Security Zones.
3) Function as an VPN Gateway interface if an IP address has been assigned to the interface.

6.1.2 *Passive Interfaces (IDS-only interfaces)*

Through passive interfaces the FTD monitors traffic flowing across a network using a switch SPAN or mirror port. The SPAN or mirror port allows for traffic to be copied from other ports on the switch. This provides the system visibility within the network without being in the flow of network traffic. Passive interfaces receive all traffic unconditionally, and no traffic received on these interfaces is retransmitted.

6.1.3 *Inline Interface Sets (IPS-only interfaces)*

Inline Sets of interfaces on the FTD support traffic flows across the FTD, binding two ports together. This allows the system to be installed in any network environment without the configuration of adjacent network Devices. Inline interfaces receive all traffic unconditionally, but all traffic received on these interfaces is retransmitted out of an inline set unless explicitly dropped.

6.2 Configure Access Control Policies

An Access Control Policy (ACP) determines how the system handles traffic on the monitored network. Administrators can configure one or more access control policies, which they can then apply to one or more managed Devices. Each Device can have only one applied policy though. Access control rules can be added to a policy to provide granular control how traffic is handled and logged.

For each rule, administrator can specify a rule *action*, that is, whether to trust, block, or inspect matching traffic with an intrusion policy. Each rule contains a set of conditions that identify the specific traffic you want to control. Rules can be simple or complex, matching traffic by any combination of security zone, IP address, application, protocols, ports, etc. The system matches traffic to access control rules in order; the first matched rule handles the traffic.

6.2.1 Access Control Policies (ACP)

On the Access Control Policy page (**Policies > Access Control**) administrator can view all the current access control policies by name and optional description and the following status information:

- When a policy is up to date on targeted Devices, in green text.
- When a policy is out of date on targeted Devices, in red text.

The default access control policy blocks all traffic from entering your network.

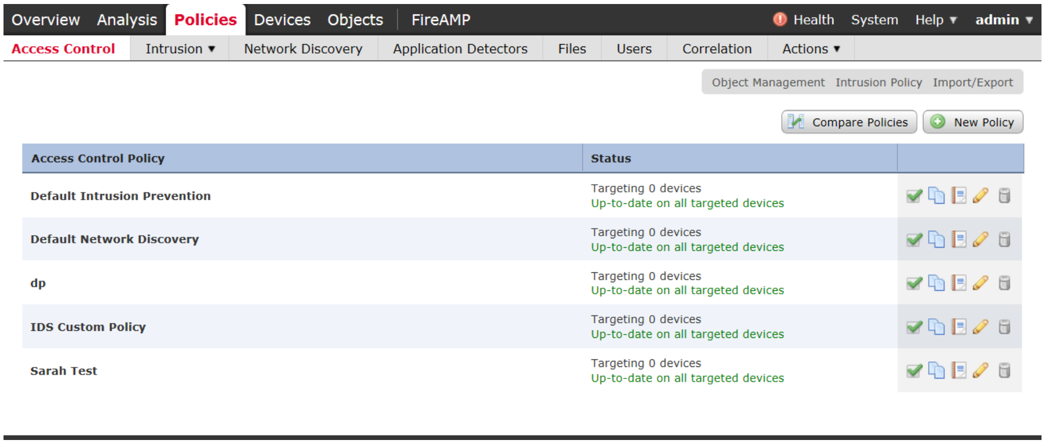
6.2.1.1 Essential ACP Elements for the CC-Evaluated Configuration

To satisfy the traffic flow control claims for the CC-evaluated configuration, every deployed ACP must at minimum include rules that define the “Network” (source and destination IP addresses), and *should* include “Ports” (source and/or destination port numbers), as well as identification of “Zones” (which are logical representations of networks, mapped to physical interfaces of each FTD to which the ACP can be applied). Any use of other ACP features (including VPN tags, Users, URL, etc.) is not relevant to supporting the CC-evaluated traffic flow control functionality, nor do any of those features interfere with Network-based or Port-based traffic flow control functionality.

6.2.1.2 Creating an Access Control Policy

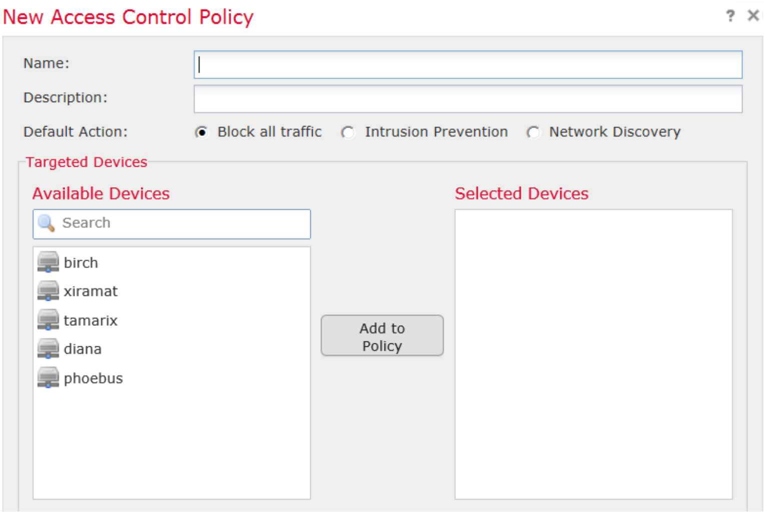
When you create a new access control policy you must, at minimum, give it a unique name and specify a default action. Although you are not required to identify the policy targets at policy creation time, you must perform this step before you can apply the policy.

1. Login with Administrator Role or Access Admin.
2. Select Policies > Access Control.



Access Control Policy	Status
Default Intrusion Prevention	Targeting 0 devices Up-to-date on all targeted devices
Default Network Discovery	Targeting 0 devices Up-to-date on all targeted devices
dp	Targeting 0 devices Up-to-date on all targeted devices
IDS Custom Policy	Targeting 0 devices Up-to-date on all targeted devices
Sarah Test	Targeting 0 devices Up-to-date on all targeted devices

3. Click New Policy.



New Access Control Policy

Name:

Description:

Default Action: ● Block all traffic ○ Intrusion Prevention ○ Network Discovery

Targeted Devices

Available Devices

Search

- birch
- xiramat
- tamarix
- diana
- phoebus

Selected Devices

4. In the **Name:** field, type a unique name for the new policy. Optionally, type a description in the **Description:** field.
5. Specify the default action.

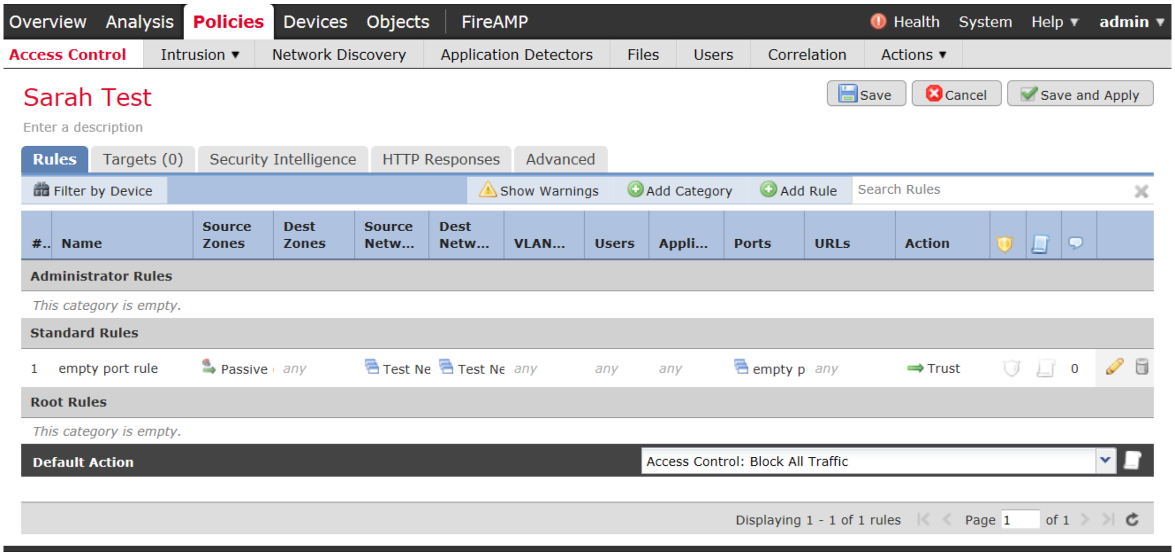
WARNING! Leave the default **Block all traffic** in the evaluated configuration.

6. Select the Devices where you want to apply the policy. Click on the managed Device(s) you want the policy to applied to. Then click on **Add to Policy** button.
7. Specify the initial **Default Action**:
   - Block all traffic creates a policy with the Access Control: Block All Traffic default action.
   - **Intrusion Prevention** creates a policy with the **Intrusion Prevention: Balanced Security and Connectivity** default action, associated with the default intrusion variable set.
8. Click **Save**.
9. Click **Deploy** and select the Device(s) you want to deploy the setting to and click **Deploy** again.

6.2.1.3 *Editing an Access Control Policy*

1. Login with Administrator Role.
2. Select Policies > Access Control.
3. Click the edit icon (✎) next to the access control policy you want to configure.

The Policy Edit page appears.



Sarah Test

Enter a description

#..	Name	Source Zones	Dest Zones	Source Netw...	Dest Netw...	VLAN...	Users	Appli...	Ports	URLs	Action			
Administrator Rules														
This category is empty.														
Standard Rules														
1	empty port rule	Passive	any	Test Ne	Test Ne	any	any	any	empty p	any	Trust			0
Root Rules														
This category is empty.														

Default Action: Access Control: Block All Traffic

Displaying 1 - 1 of 1 rules Page 1 of 1

4. Make changes to the policy and click **Save**.
5. Click **Deploy** and select the Device(s) you want to deploy the setting to and click **Deploy** again.

6.2.1.4 *Deleting an Access Control Policy*

1. Login with Administrator Role.
2. Select Policies > Access Control.
3. Click the delete icon (🗑) next to the policy you want to delete.
4. Click **OK** to confirm.

6.2.2 Access Control Rules

A set of access control rules is a key component of an access control policy. Access control rules allow administrator to manage, in a granular fashion, which traffic can enter the network, exit it, or cross from within without leaving it. Within an access control policy, the system matches traffic to rules in top-down order by rule number. In addition to its rule order and some other basic attributes, each rule has the following major components:

- A set of rule *conditions* that identifies the specific traffic you want to control.
- A rule *action*, which determines how the system handles traffic that meets the rule’s conditions.
- Intrusion *inspection* option, which allow you to examine allowed traffic with intrusion policy.
- The *logging* option, which allow you to keep a record (event log) of the matching traffic.

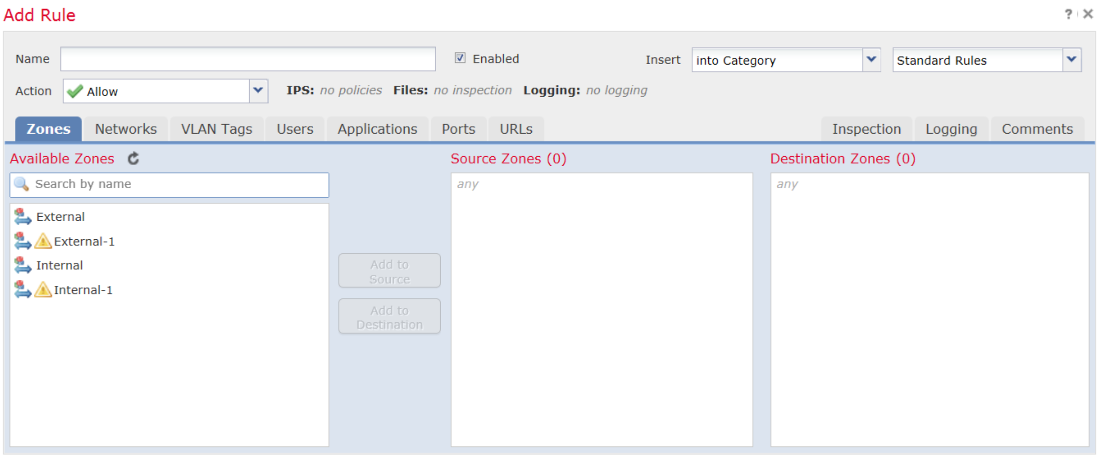
The access control policy’s default action defines the default action (for example, block all traffic) for the policy.

6.2.2.1 *Creating and Editing Access Control Rules*

1. Login with Administrator Role or Access Admin.
2. Select Policies > Access Control.

3. Click the edit icon (✎) next to the access control policy you want to configure.
4. Add a new rule or edit an existing rule:
   - To add a new rule, click **Add Rule**.
   - To edit an existing rule, click the edit icon (✎) next to the rule you want to edit.

Either the Add Rule or Editing Rule page appears.



Add Rule

Name:

☑ Enabled

Insert: into Category — Standard Rules

Action: ✓ Allow

IPS: *no policies* **Files:** *no inspection* **Logging:** *no logging*

Available Zones: External, External-1, Internal, Internal-1

Source Zones (0): any

Destination Zones (0): any

5. Configure the following rule components:
   - You must provide a unique rule **Name**.
   - Specify whether the rule is **Enabled**.
   - Specify the rule position.
   - Select a rule **Action**[2].
   - Configure the rule's conditions[3].
   - Configure the rule's **Inspection** option.
   - Specify **Logging** option.
   - Add Comments.
6. Click **Add** or **Save**.

Your changes are saved. You must deploy the updated ACP to an FTD for the changes to take effect.

6.2.2.2 *Understanding Rule Conditions*

Administrators can set an ACP rule to match traffic meeting any of the conditions described in the following table:

[2] The CC-evaluated actions are Allow and Block.

[3] The CC-evaluated conditions are Zones, Networks, and Ports. The other conditions are presented for completeness only.

Condition	Description
Zones	A configuration of one or more interfaces where you can apply policies. Zones provide a mechanism for classifying traffic on source and destination interfaces, and you can add source and destination zone conditions to rules.
Networks	Any combination of individual IPv4 and IPv6 addresses, CIDR blocks, and/or networks (by default, any). The system also supports Network Objects as described in Section 4, page 148 in the Cisco 3D System User Guide.
VLAN Tags	A number from 0 to 4094 that identifies traffic on your network by VLAN.
Applications	Applications provided by Cisco, user-defined applications, and application filters you create using the object manager.
Ports	Source and Destination ports. ICMPv4 and ICMPv6 type and code. Transport protocol ports, including individual and group port objects you create based on transport protocols[4]. The system supports Port Objects as described in Section 4, page 170 in the Cisco 3D System User Guide.
URLs	Cisco-provided URLs grouped by category and reputation, literal URLs, and any individual and group URL objects you create using the object manager.

IMPORTANT! Note that to use the Application tab for the access control rules, CONTROL license is required which requires PROTECTION license. This is needed to detect FTP and FTP data connections for dynamic rule. The CONTROL license is only supported for series 3 appliances.

To support the dynamic session establishment capability for FTP, you first need to create an access control rule that allows both FTP and FTP data. You can also configure the logging for this rule. This will enable the FTP application detector to allow the FTP data connection without an additional explicit rule.

6.2.2.3 *Deleting Access Control Rules*

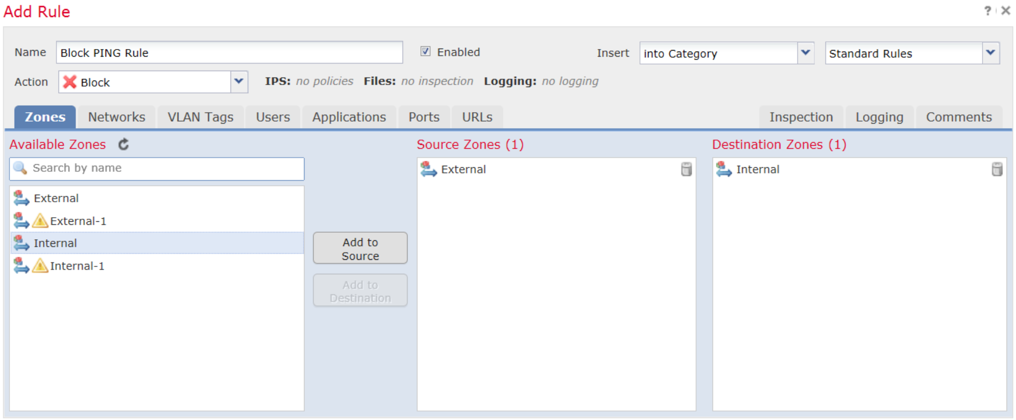
1. Login with Administrator Role.
2. Select Policies > Access Control.
3. Click the edit icon (✏) next to the access control policy you want to configure.
4. Click the delete icon (🗑) next to the access control rule you want to delete.
5. Click **OK** to confirm.
6. Click **Save**.

The following example demonstrates how to block all Ping (ICMP echo request) from the external network to internal network and log the connection attempt.

1. Login with Administrator Role.
2. Select Policies > Access Control.
3. Click the edit icon (✏) next to the access control policy you want to configure.
4. Click **Add Rule**.
5. Type a name for the rule.
6. Leave the **Enabled** checkbox selected.
7. Let the rule get inserted into standard rules.

[4] We support all the protocol-specific attributes required in the FWPP.

8. Select **Block** from drop-down list for the rule action.
9. On the **Zones** tab, select the **External** zone as the source zone and the **Internal** zone as the destination zone. You can click and drag or use the buttons.



Add Rule

Name: Block PING Rule ☑ Enabled Insert: into Category Standard Rules

Action: Block IPS: *no policies* Files: *no inspection* Logging: *no logging*

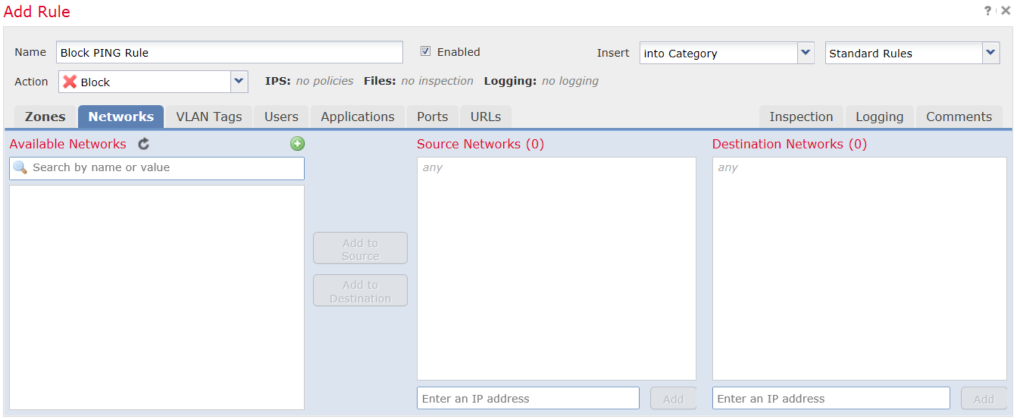
Available Zones: External, External-1, Internal, Internal-1

Source Zones (1): External

Destination Zones (1): Internal

10. On the **Networks** tab, select **any** as the source network and **any** as the destination network.

For granular control, you can enter IP address or range of IP addresses for source and destination networks. The system also supports IPv6 addresses as well.



Add Rule

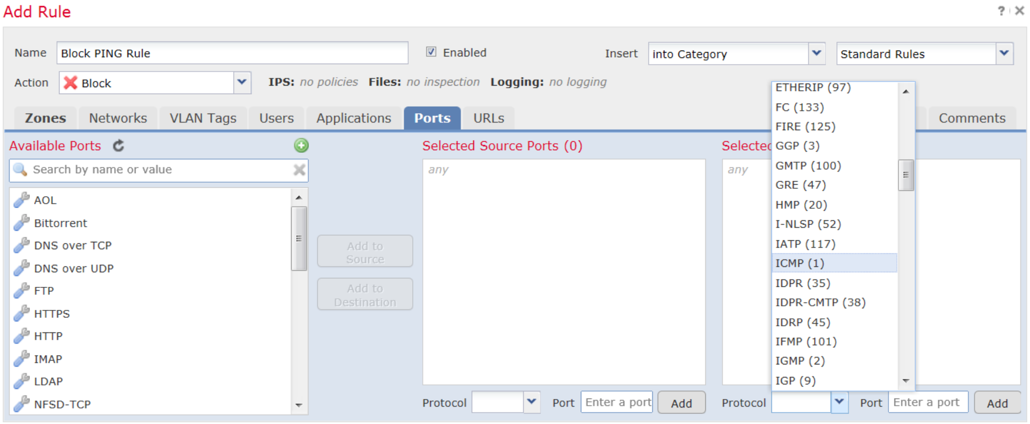
Name: Block PING Rule ☑ Enabled Insert: into Category Standard Rules

Action: Block IPS: *no policies* Files: *no inspection* Logging: *no logging*

Source Networks (0): *any*

Destination Networks (0): *any*

11. On the **Ports** tab, in the second **Protocol** fields, select **ICMP(1)**.



Add Rule

Name: Block PING Rule ☑ Enabled Insert: into Category Standard Rules

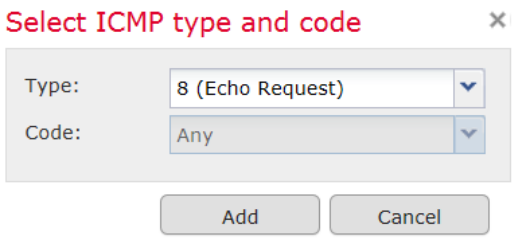
Action: Block IPS: *no policies* Files: *no inspection* Logging: *no logging*

Selected Source Ports (0): *any*

Selected Destination Ports: *any*

The Select ICMP type and code pop-up window appears.

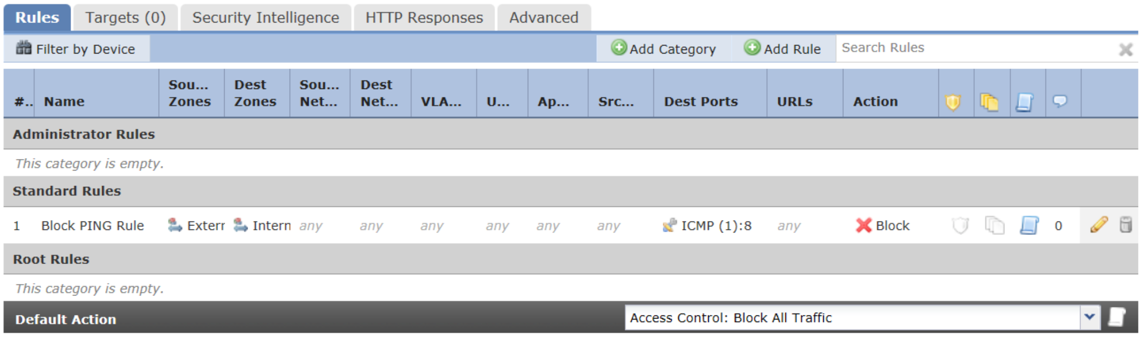
12. In the **Type:** field, select **8 (Echo Request)**.



Type: 8 (Echo Request)

Code: Any

13. Click **Add**.
14. On the Logging tab, check Log at Beginning of Connection.
15. In the Send Connection Events to: field, check the FMC.
16. Click **Add**.



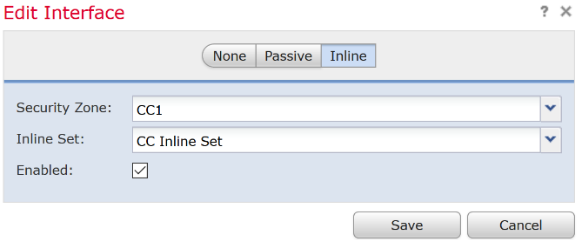
#..	Name	Sou... Zones	Dest Zones	Sou... Net...	Dest Net...	VLA...	U...	Ap...	Src...	Dest Ports	URLs	Action
Administrator Rules												
This category is empty.												
Standard Rules												
1	Block PING Rule	Exterr	Intern	any	any	any	any	any	any	ICMP (1):8	any	Block
Root Rules												
This category is empty.												

Default Action: Access Control: Block All Traffic

17. Click **Save**.

6.2.2.4 *Modification of Which Mode Is Active on an FTD Interface*

1. Login with Administrator Role.
2. Select Device > Device Management.
3. Edit an interface (e.g., eth1).



Security Zone: CC1

Inline Set: CC Inline Set

Enabled: ☑

4. To change an interface mode, change the interface from **Inline** to **Passive**.
5. Click **Save**.

7 FTD VPN Policies

7.1 FTD VPN Overview

A virtual private network (VPN) connection establishes a secure tunnel between endpoints over a public network such as the Internet. This chapter applies to Remote Access and Site-to-Site VPNs on FTD devices. It describes the Internet Protocol Security (IPsec), the Internet Security Association and Key Management Protocol (ISAKMP, or IKE) standards that are used to build site-to-site and remote access VPNs. For a more complete overview of IPsec VPN functionality in FTD, refer to the “VPN Overview” section of [FMC-CG].

7.1.1 Firepower VPN Licensing

There is no specific licensing for enabling FTD VPN, it is available by default.

The FMC determines whether to allow or block the usage of strong crypto on a FTD based on attributes provided by the smart licensing server. This is controlled by whether you selected the option to allow export-controlled functionality on the Device when you registered with Cisco Smart License Manager. If you are using the evaluation license, or you did not enable export-controlled functionality, you cannot use strong encryption.

7.1.2 Supported VPN Types

The FMC supports the following types of VPN connections:

7.1.2.1 Remote Access VPNs on FTD

Remote access VPNs are secure, encrypted connections, or tunnels, between remote users and your company’s private network. The connection consists of a VPN endpoint device, which is a workstation or mobile device with VPN client capabilities, and a VPN headend device, or secure gateway, at the edge of the corporate private network.

FTD can be configured (via FMC) to support Remote Access VPNs over TLS or IPsec IKEv2. Functioning as secure gateways in this capacity, they authenticate remote users, authorize access, and encrypt data to provide secure connections to your network. No other types of appliances, managed by the FMC, support Remote Access VPN connections.

FTD secure gateways support the Secure Client tunnel client. This client is required to provide secure IPsec IKEv2 or TLS connections for remote users.

7.1.2.2 Site-to-Site VPNs on FTD

A site-to-site VPN connects networks in different geographic locations. You can create site-to-site IPsec connections between managed Devices, and between managed Devices and other Cisco or third-party peers that comply with all relevant standards. These peers can have any mix of inside and outside IPv4 and IPv6 addresses. Site-to-Site tunnels are built using the Internet Protocol Security (IPsec) protocol suite and IKEv2, though the CC-evaluated configuration only allows use of IKEv2. After the VPN connection is established, the hosts behind the local gateway can connect to the hosts behind the remote gateway through the secure VPN tunnel.

7.2 VPN Basics

Tunneling makes it possible to use a public TCP/IP network, such as the Internet, to create secure connections between remote users and private corporate networks. Each secure connection is called a tunnel.

IPsec-based VPN technologies use the IKE and ESP protocols to build and manage tunnels. IKE and ESP accomplish the following:

- Negotiate tunnel parameters.
- Establish tunnels.

- Authenticate users and data.
- Manage security keys.
- Encrypt and decrypt data.
- Manage data transfer across the tunnel.
- Manage data transfer inbound and outbound as a tunnel endpoint or router.

A Device in a VPN functions as a bidirectional tunnel endpoint. It can receive plain packets from the private network, encapsulate them, create a tunnel, and send them to the other end of the tunnel where they are unencapsulated and sent to their final destination. It can also receive encapsulated packets from the public network, de-encapsulate them, and send them to their final destination on the private network.

After the site-to-site VPN connection is established, the hosts behind the local gateway can connect to the hosts behind the remote gateway through the secure VPN tunnel. A connection consists of the IP addresses and hostnames of the two gateways, the subnets behind them, and the method the two gateways use to authenticate to each other.

On an FTD, the system does not send VPN traffic until it has passed through the access control policy. Incoming tunnel packets are decrypted before being sent to the Snort process. Outgoing packets are processed by Snort before encryption. Identifying the protected networks for each endpoint node of a VPN tunnel determines which traffic is allowed to pass through the FTD and reach the internal hosts. In addition, the system does not send tunnel traffic to the public source when the tunnel is down.

7.2.1 Internet Key Exchange (IKE)

Internet Key Exchange (IKE) is a key management protocol that is used to authenticate IPsec peers, negotiate and distribute IPsec encryption keys, and to automatically establish IPsec security associations (SAs).

An IKE policy is a set of algorithms that two peers use to secure the IKE negotiation between them. IKE negotiation begins by each peer agreeing on a common (shared) IKE policy. This policy states which security parameters protect subsequent IKE negotiations.

To define an IKE policy, specify:

- A unique priority (1 to 65,543, with 1 the highest priority).
- An encryption method for the IKE negotiation, to protect the data and ensure privacy.
- A Hashed Message Authentication Codes (HMAC) method (called integrity algorithm in IKEv2) to ensure the identity of the sender, and to ensure that the message has not been modified in transit.
- For IKEv2, a separate pseudorandom function (PRF) used as the algorithm to derive keying material and hashing operations required for the IKEv2 tunnel encryption. The options are the same as those used for the hash algorithm.
- A Diffie-Hellman group to determine the strength of the encryption-key-determination algorithm. The Device uses this algorithm to derive the encryption and hash keys.
- An authentication method, to ensure the identity of the peers.
- A limit to the time the Device uses an encryption key before replacing it.

When IKE negotiation begins, the peer that starts the negotiation sends all of its policies to the remote peer, and the remote peer searches for a match with its own policies, in priority order. A match between IKE policies exists if they have the same encryption, hash (integrity and PRF for IKEv2), authentication, and Diffie-Hellman values, and an SA lifetime less than or equal to the lifetime in the policy sent. If the lifetimes are not identical, the shorter lifetime applies.

7.2.2 IPsec

IPsec is one of the most secure methods for setting up a VPN. IPsec provides data encryption at the IP packet level, offering a robust security solution that is standards-based. With IPsec, data is transmitted over a public network through tunnels. A tunnel is a secure, logical communication path between two peers. Traffic that enters an IPsec tunnel is secured by a combination of security protocols and algorithms.

7.2.3 Deciding Which Algorithms to Use

When deciding which encryption algorithms to use for the IKE policy or IPsec proposal, your choice is limited to algorithms supported by the IPsec endpoints. For IKEv2, you can configure multiple encryption algorithms. The system orders the settings from the most secure to the least secure and negotiates with the peer using that order. For IPsec proposals, the algorithm is used by the Encapsulating Security Protocol (ESP), which provides authentication, encryption, and anti-replay services. ESP is IP protocol type 50.

For the IKEv2 policy, FTD supports **AES-GCM-NULL-SHA-LATEST, AES-GCM-NULL-SHA, AES-SHA-SHA**, and DES-SHA-SHA, but the CC-evaluated configuration prohibits use of DES-SHA-SHA.

For the IKEv2 IPsec Proposal, FTD supports **AES-GCM-NULL-SHA-LATEST, AES-GCM, AES-SHA**, and DES-SHA-1, but in the CC-evaluated configuration selecting DES-SHA-1 is prohibited.

7.2.4 Deciding Which Diffie-Hellman Modulus Group to Use

You can use the following Diffie-Hellman key derivation algorithms to generate IPsec security association (SA) keys. Each group has a different size modulus. A larger modulus provides higher security, but requires more processing time. You must have a matching modulus group on both peers.

To implement the NSA Suite B cryptography specification, use IKEv2 and select one of the elliptic curve Diffie-Hellman (ECDH) options: 19, 20, or 21. Elliptic curve options and groups that use 2048-bit modulus are less exposed to attacks such as Logjam.

To select the Modulus Group for the tunnel, check the box to “Enable Perfect Forward Secrecy”, then select the Modulus Group to be used. In the CC-evaluated configuration, select one of **Modulus Group 14, 19, 20, or 24.**

7.2.5 Deciding Which Authentication Method to Use

Pre-shared keys and digital certificates are the methods of authentication available for VPNs, and site-to-site IKEv2 VPN connections can use both options. Remote Access VPN using IKEv2 supports digital certificate authentication only.

Pre-shared keys allow for a secret key to be shared between two peers and used by IKE during the authentication phase. The same shared key must be configured at each peer or the IKE SA cannot be established.

Digital certificates use RSA or ECDSA key pairs to sign and encrypt IKE key management messages. Certificates provide non-repudiation of communication between two peers, meaning that it can be proved that the communication actually took place. When using this authentication method, you need a Public Key Infrastructure (PKI) defined where peers can obtain digital certificates from a Certification Authority (CA). CAs manage certificate requests and issue certificates to participating network devices providing centralized key management for all of the participating devices.

Pre-shared keys do not scale well, using a CA improves the manage ability and scalability of your IPsec network. With a CA, you do not need to configure keys between all encrypting devices. Instead, each participating device is registered with the CA, and requests a certificate from the CA. Each device that has its own certificate and the public key of the CA can authenticate every other device within a given CA's domain.

7.2.6 PKI Infrastructure

A PKI provides centralized key management for participating network devices. It is a defined set of policies, procedures, and roles that support public key cryptography by generating, verifying, and revoking public key certificates commonly known as digital certificates.

In public key cryptography, each endpoint of a connection has a key pair consisting of both a public and a private key. The key pairs are used by the VPN endpoints to sign and encrypt messages. The keys act as complements, and anything encrypted with one of the keys can be decrypted with the other, securing the data flowing over the connection.

Generate a general-purpose RSA or ECDSA key pair, used for both signing and encryption, or you generate separate key pairs for each purpose. Separate signing and encryption keys help to reduce exposure of the keys. TLS uses a key for encryption but not signing, however, IKE uses a key for signing but not encryption. By using separate keys for each, exposure of the keys is minimized.

7.2.6.1 Digital Certificates

When you use Digital Certificates as the authentication method for VPN connections, peers are configured to obtain digital certificates from a Certificate Authority (CA). CAs are trusted authorities that "sign" certificates to verify their authenticity, there by guaranteeing the identity of the device or user.

CA servers manage public CA certificate requests and issue certificates to participating network devices as part of a Public Key Infrastructure (PKI), this activity is called Certificate Enrollment. These digital certificates, also called identity certificates contain:

- The digital identification of the owner for authentication, such as name, serial number, company, department, or IP address.
- A public key needed to send and receive encrypted data to the certificate owner.
- The secure digital signature of a CA.

Certificates also provide non-repudiation of communication between two peers, meaning that it they prove that the communication actually took place.

7.2.6.2 Certificate Authority Certificates

In order to validate a peer's certificate, each participating device must retrieve the CA's certificate from the server. A CA certificate is used to sign other certificates. It is self-signed and called a root certificate. This certificate contains the public key of the CA, used to decrypt and validate the CA's digital signature and the contents of the received peer's certificate. The CA certificate may be obtained by:

- Using the Simple Certificate Enrollment Protocol (SCEP) to retrieve the CA's certificate from the CA server
- Manually copying the CA's certificate from another participating device

Trustpoints

Once enrollment is complete, a trustpoint is created on the managed Device. It is the object representation of a CA and associated certificates. A trustpoint includes the identity of the CA, CA-specific parameters, and an association with a single enrolled identity certificate.

PKCS#12 File

A PKCS#12, or PFX, file holds the server certificate, any intermediate certificates, and the private key in one encrypted file. This type of file may be imported directly into a Device to create a trustpoint.

Revocation Checking

A CA may also revoke certificates for peers that no longer participate in your network. Revoked certificates are either managed by an Online Certificate Status Protocol (OCSP) server (OCSP responder), and the FTD may check the certificate revocation status before accepting a certificate from a VPN peer.

7.3 FTD Site-to-Site VPN

FTD site-to-site VPN supports the following features:

- FTD supports both IKEv1 & IKEv2, but the CC-evaluated configuration muse use IKEv2.
- Authentication methods can use PKI Certificates, automatic pre-shared keys, or manual pre-shared keys.

For a more complete explanation of this functionality in FTD, refer to the “Site-to-Site VPNs” section of [FMC-CG].

7.3.1 FTD Site-to-Site VPN Basics

7.3.1.1 IPsec and IKE

In the FMC, site-to-site VPNs are configured based on IKE policies and IPsec proposals that are assigned to VPN topologies. Policies and proposals are sets of parameters that define the characteristics of a site-to-site VPN, such as the security protocols and algorithms that are used to secure traffic in an IPsec tunnel. Several policy types may be required to define a full configuration image that can be assigned to a VPN topology.

7.3.1.2 Authentication

For authentication of VPN connections, configure a pre-shared key in the topology, or a trustpoint on each device. Pre-shared keys allow for a secret key, used during the IKE authentication phase, to be shared between two peers. A trustpoint includes the identity of the CA, CA-specific parameters, and an association with a single enrolled identity certificate.

7.3.1.3 Extranet Devices

Each topology type can include Extranet devices, devices that you do not manage in FMC. These include:

- Cisco devices that FMC supports, but for which your organization is not responsible. Such as spokes in networks managed by other organizations within your company, or a connection to a service provider or partner's network.
- Non-Cisco devices. You cannot use FMC to create and deploy configurations to non-Cisco devices

Add non-Cisco devices, or Cisco devices not managed by the FMC, to a VPN topology as "Other" devices. Also specify the IP address of each remote device.

7.3.2 Managing FTD Site-to-Site VPN

1) Login with Administrator Role.
2) For certificate authentication for your VPNs, you must prepare the Devices by allocating trustpoints as described in “Site-to-Site VPNs” section below.
3) Select **Devices > VPN > Site To Site** to manage your FTD Site-to-Site VPN configurations and deployments. Choose from the following:
    a) Add—To create a new VPN topology, click **+ Site to Site VPN**, and continue as instructed in “Configuring Site to Site VPNs” section below.
    b) Edit—To modify the settings of an existing VPN topology, click the edit icon (✎). Modifying is similar to configuring, continue as instructed above.
    c) Delete—To delete a VPN deployment, click the delete icon (🗑).
    d) Deploy—Click **Deploy**.

7.3.3 Configuring FTD Site-to-Site VPN

To configure a Site-to-Site VPN, follow this summary of steps. For a more complete overview of configurable options, refer to the “Configuring a Policy-based Site-to-Site VPNs” section of [FMC-CG].

1) Login with Administrator Role.
2) Choose **Devices > VPN > Site To Site. Then + Site to Site VPN**, or edit a listed VPN Topology.
3) Enter a unique **Topology Name**. We recommend naming your topology to indicate that it is a FTD VPN, and its topology type.
4) Choose the **Network Topology** for this VPN. For example, point to point topology.
5) To adhere to the CC-evaluated configuration, configure the tunnel parameters in accordance with the guidelines provided below. Where no specific guidance is provided here, any configurable option is acceptable in the CC-evaluated configuration.
    a) Choose the **IKEv2** as the version to use during IKE negotiations (the default is IKEv2).
    b) On the **Endpoint** tab, use any parameters as describe in the “FTD VPN Endpoint Options” section of [FMC-CG]. Add Endpoints for this VPN deployment by clicking the add icon (⊕) for each node in the topology.
    c) On the **IKE** tab, set the Policy to either **AES-GCM-NULL-SHA-LATEST, AES-GCM-NULL-SHA**, or **AES-SHA-SHA**. In the CC-evaluated configuration selecting the DES-SHA-SHA option is prohibited.
    d) On the **IPsec** tab:
        i) Set the IKEv2 IPsec Proposals to **AES-GCM**, and/or **AES-SHA**. In the CC-evaluated configuration selecting DES-SHA-1 is prohibited.
        ii) Click the “Enable Perfect Forward Secrecy” box, and set the Modulus Group to one of **14, 19, 20,** or **24**
    e) Click **Save**.
6) Deploy the updated VPN topology to all related FTD instances.

7.3.4 Certificate-Based Authentication for Site-to-Site VPN (optional)

7.3.4.1 Installing a certificate using manual enrollment.

1) Login with Administrator Role.
2) On the Devices > Certificates screen, choose Add > Add New Certificate to open the Add New Certificate dialog.
3) Choose a Device from the **Device** drop down list.
4) Associate a certificate enrollment object with this Device in one of the following ways:
    a) Choose a Certificate Enrollment Object of the appropriate type from the drop-down list.
    b) Click (+), to add a new Certificate Enrollment Object. Please see “Adding Certificate Enrollment Objects” section below.
5) Press **Install**, to initiate the manual enrollment process.

    The **CA Certificate** status will go from *In Progress* to *Available* as the FMC installs the CA certificate (provided in the enrollment object) on the managed Device, authenticates the CA Server, and creates a trustpoint on the managed Device.

    The **Identity Certificate** status will reach Pending state when the Certificate Signing Request (CSR) is generated by the managed Device and placed in the Identity Certificate field.
6) Execute the appropriate activity with your PKI CA Server to obtain an identity certificate.
    a) Click the Identity Certificate magnifying glass to view and copy the CSR.
    b) Execute the appropriate activity with your PKI CA Server to obtain an identity certificate using this CSR. This activity is completely independent of the FMC or the managed Device. When complete, You will have an Identity Certificate for the managed Device. You can copy it or place it in a file.
    c) To finish the manual process, install the obtained identity certificate on to the managed Device.
7) Return to the FMC dialog to paste the Identity Certificate into its field. Or, select **Browse** to choose the identity certificate file.
8) Select **Import** to import the Identity Certificate.

    The Identity Certificate status will be *Available* when the import complete.
9) Click the magnifying glass to view the **Identity Certificate** for this Device.

7.3.4.2 Installing a certificate by importing a PKCS12 file.

Note: A PKCS12 file size should not be larger than 24K.

1) Login with Administrator Role.
2) Go to **Devices > Certificates**, then click **+ Add > Import PKCS12 File** to open the Import PKCS12 File dialog.
3) Choose a pre-configured managed Device from the **Device** drop down list.
4) Specify a Certificate Enrollment type of PKCS12.
5) Select **Browse** to find and choose your PKCS#12 Certificate file.
6) Enter the **Passphrase** for decryption.

7) Press **Add**. For file import, the **CA Certificate** and **Identity Certificate** status will go from *In Progress* to *Available* as it installs the PKCS12 file on the Device.

8) Once *Available*, click the magnifying glass to view the Identity Certificate for this Device.

7.3.4.3 Adding Certificate Enrollment Objects

1) Login with Administrator Role.

2) Open the Add Cert Enrollment dialog:

   a) Directly from Object Management: In the **Objects > Object Management** screen, choose **PKI > Cert Enrollment** from the navigation pane, and press **Add Cert Enrollment**.

   b) While configuring a managed Device: In the **Devices > Certificates** screen, choose **Add > Add New Certificate** and click (+) for the **Certificate Enrollment** field.

3) Enter the **Name**, and optionally, a **Description** of this enrollment object. When enrollment is complete, this name is the name of the trustpoint on the managed Devices with which it is associated.

4) Open the **CA Information** tab and choose the **Enrollment Type**.

   a) **Self-Signed Certificate**—The managed Device, acting as a CA, generates its own self-signed root certificate. No other information is needed in this pane.

   b) **SCEP**—(Default) Simple Certificate Enrollment Protocol. Specify the SCEP information.

   c) **Manual**—Paste an obtained CA certificate in the **CA Certificate** field. You can obtain a CA certificate by copying it from another device.

   d) **PKCS12 File**—Import a PKCS12 file on a FTD managed Device that supports VPN connectivity. A PKCS#12, or PFX, file holds a server certificate, intermediate certificates, and a private key in one encrypted file.

5) Open the **Certificate Parameters** tab and specify the certificate contents. Specify additional information in certificate requests sent to the CA server.

   a) **Key Type**—RSA (default, and only supported option) or ECDSA

   b) **Key Name**—If the key pair you want to associate with the certificate already exists, this field specifies the name of that key pair. If the key pair does not exist, this field specifies the name to assign to the key pair that will be generated during enrollment. If you do not specify an RSA key pair, the fully qualified domain name (FQDN) key pair is used instead.

   c) **Key Size**—If the key pair does not exist, defines the desired key size (modulus), in bits. The recommended size is 2048 or greater.

6) (Optional) Click the **Revocation** tab, and specify the revocation options. Specify whether to check the revocation status of a certificate by choosing and configuring the method. Revocation checking is off by default, neither method (CRL or OCSP) is checked. Note: Use of CRLs was not tested during the CC evaluation, but its use would not interfere with the CC-evaluated configuration. Use of OCSP was validated for use in the CC-evaluated configuration, but is not required. Note: When both CRL and OCSP checking are enabled, the FTD will first attempt to use CRL, and will only attempt to use OCSP if the CRL could not be obtained (e.g. if the CRL distribution point was unavailable).

   a) (Optional) Enable Certificate Revocation Lists—Check to enable CRL checking.

      i) **Use CRL distribution point from the certificate**—Check to obtain the revocation lists distribution URL from the certificate.

ii) **Use static URL configured**—Check this to add a static, pre-defined distribution URL for revocation lists. Then add the URLs.

iii) **CRL Server URLs**—The URL of the server from which the CRL can be downloaded.

b) (Optional) **Enable Online Certificate Status Protocol (OCSP)** Check this box to enable OCSP checking.

i) **OCSP Server URL**—The URL of the OCSP server checking for revocation if you require OCSP checks. This URL must start with http://.

c) (Optional) **Consider the certificate valid if revocation information cannot be reached**—This box is checked by default. Uncheck the box if you want certificates to be considered invalid whenever the OCSP responder is not accessible.

7.3.4.4 FTD Certificate Map Object

Certificate Map objects are a named set of certificate matching rules. These objects are used to provide an association between a received certificate and a Remote Access VPN connection profile. Connection Profiles and Certificate Map objects are both part of a remote access VPN policy. If a received certificate matches the rules contained in the certificate map, the connection is "mapped", or associated with the specified connection profile. The rules are in priority order, they are matched in the order they are shown in the UI. The matching ends when the first rule within the Certificate Map object results in a match.

1) Login to FMC.

2) Open the **Objects > Object Management > VPN > Certificate Map**, click **Add Certificate Map,** and provide the necessary details.

a) **Map Name**—Identify this object so it can be referred to from other configurations, such as Remote-Access-VPN (names cannot contain spaces).

b) **Mapping Rule**—Specify the contents of the certificate to evaluate. If the certificate satisfies these rules, the user will be mapped to the connection profile containing this object.

i) **Field**—Select the field for the matching rule according to the Subject or the Issuer of the client certificate.

ii) **Component**—Select the component of the client certificate to use for the matching rule. If the Field is set to *Alternative Subject* or *Extended Key Usage* the Component will be frozen as *Whole* Field.

iii) **Operator**—Select *the* operator for the matching rule as follows:

(1) Equals—The certificate component must match the entered value. If they do not match exactly, the connection is denied.

(2) Contains—The certificate component must contain the entered value. If the component does not contain the value, the connection is denied.

(3) Does Not Equal—The certificate component cannot equal the entered value. For example, for a selected certificate component of Country, and an entered value of US, if the client county value equals US, then the connection is denied.

(4) Does Not Contain—The certificate component cannot contain the entered value. For example, for a selected certificate component of Country, and an entered value of US, if the client county value contains US, the connection is denied.

iv) **Valu**e—The value of the matching rule. The value entered is associated with the selected component and operator.

b) Click **Save**.

7.3.5 Configure IKEv2 Policy Objects

Use the IKEv2 policy dialog box to create, delete, and edit an IKEv2 policy object. These policy objects contain the parameters required for IKEv2 policies.

1) Login to FMC.
2) Choose **Objects > Object Management** and then **VPN > IKEv2 Policy** from the table of contents.
3) Choose ⊕**Add IKEv2 Policy** to create a new policy.
4) Enter a **Name** for this policy. The name of the policy object. A maximum of 128 characters is allowed.
5) Enter a **Description** for this policy. A description of the policy object. A maximum of 1024 characters is allowed.
6) Enter the **Priority**. The priority value of the IKE proposal. The priority value determines the order of the IKE proposals compared by the two negotiating peers when attempting to find a common security association (SA). If the remote IPsec peer does not support the parameters selected in your first priority policy, it tries to use the parameters defined in the next lowest priority policy. Valid values range from 1 to 65535. The lower the number, the higher the priority. If you leave this field blank, FMC assigns the lowest unassigned value starting with 1, then 5, then continuing in increments of 5.
7) Set the **Lifetime** of the security association (SA), in seconds. You can specify a value from 120 to 2,147,483,647 seconds. The default is 86400.
8) Choose the **Integrity Algorithms** portion of the Hash Algorithm used in the IKE policy. The Hash Algorithm creates a Message Digest, which is used to ensure message integrity.
9) Choose the **Encryption Algorithm** used to establish the Phase 1 SA for protecting Phase 2 negotiations.
10) Choose the PRF Algorithm.
11) Select and **Add** a **DH Group**.
12) Click **Save**.

7.3.6 Configure IKEv2 IPsec Proposal Objects

1) Login with Administrator Role.
2) Choose Objects > Object Management and then VPN > IKEv2 IPsec Proposal from the table of contents.
3) Choose ⊕**Add IKEv2 IPsec Proposal** to create a new Proposal.
4) Enter a **Name** for this Proposal. The name of the proposal object. A maximum of 128 characters is allowed.
5) Enter a **Description** for this Proposal. A description of the proposal object. A maximum of 1024 characters is allowed.
6) Choose the **ESP Hash** method, the hash or integrity algorithm to use in the Proposal for authentication.

7) Choose the **ESP Encryption** method. The Encapsulating Security Protocol (ESP) encryption algorithm for this Proposal.

8) Click **Save**.

7.3.7 Deploy Any Updated Site-to-Site VPN Policies

If any changes, additions, or deletions were made to any policy or object mentioned in the sections above, you must deploy those changes to any FTD that will use those policies or objects. In FMC, choose **Deploy** from the menu bar, then select all applicable FTD instances, then click **Deploy**.

7.4 FTD Remote Access VPN

FTD provides secure gateway capabilities that support remote access IPsec IKEv2 or TLS VPNs. The full tunnel client, Secure Client, provides secure TLS and IKEv2 IPsec connections to the security gateway for remote users, but the CC-evaluated configuration only allows use of IPsec for VPN connections. Secure Client is the only client supported on endpoint devices for remote VPN connectivity to FTD. The client gives remote users the benefits of a VPN client without the need for network administrators to install and configure clients on remote computers. The Secure Client is available for Windows, Mac, and Linux, but the CC-evaluated configuration only allows use of Secure Client on Windows 10/11.

Use the Remote Access VPN Policy wizard in the FMC to quickly and easily set up these two types of remote access VPNs with basic capabilities. Then, enhance the policy configuration if desired and deploy it to your FTD secure gateway devices.

7.4.1 Managing FTD Remote Access VPN

1) Login to FMC.

2) Choose **Devices > VPN > Remote Access**. The policies displayed in the list were created using the VPN Configuration Wizard, and possibly already edited. Out of date status indicates there is an older version of the remote access VPN policy on the targeted Devices. Deploy the latest remote access VPN policy to update the policy configuration.

3) Choose from the following actions:

   a) Add (⊕)—Creates a new Remote Access VPN Policy using a wizard that walks you through a basic policy configuration.

   b) Edit (✎)— Modify an existing Remote Access VPN policy. Click the edit icon or the VPN policy row to open the policy for editing.

   c) Delete (🗑)— Delete a Remote Access VPN configuration.

7.4.2 Editing a Remote Access VPN Policy

1) Login to FMC.

2) Choose **Devices > VPN > Remote Access**.

3) Select an existing Remote Access policy in the list and click the corresponding Edit icon (✎). The remote Access VPN Policy contains one or more Connection Profiles targeted for specific devices. These policies pertain to creating the tunnel itself, such as how authentication is accomplished, and how addresses are assigned (DHCP or Address Pools) to VPN clients. They also include user

attributes, which are identified in group policies configured on the FTD. A Device also provides a default connection profile named *DefaultWEBVPNGroup*. The connection profile that is configured using the wizard appears in the list.

4) The **Connection Profile** tab lists the profiles created under the Remote Access VPN policy. The table lists information about client address assignment, group policy, and authentication options. To add a connection profile, click the **Add (+)** icon and specify the following in the **Add Connection Profile** window:

    a) **Connection Profile**—Provide a name that the remote users will use for VPN connections. Specifies a set of parameters that define how the remote users connect to the VPN device. For more information about Connection Profile, see the "Adding and Editing FTD Remote Access VPN Connection Profile" section below.

    b) **Group Policy**—A collection of user-oriented attributes which are applied to the client when the VPN connectivity is established. Group policies configure common attributes for groups of users. For more information about Group Policy, see the "Configuring Group Policies" section below.

5) The **Access Interface** tab identifies the interface group or security zone to which the Remote Access Policy is applicable. Select the value from the drop-down list. The interface group or security zone must be a **Routed** type. Other interface types are not supported for Remote Access VPN connectivity. Associate the **Protocol** object with the access interface.

    a) For each Access Interface, click the **Edit** (pencil) icon to select which protocols are supported:

        i) Check **Enable IKEv2**—Select this option to enable IKEv2 settings or check **Enable SSL** to enabled TLS settings

    b) Select an IKEv2 Identity Certificate to be used by the FTD. Select Interface Identity Certificate from the drop-down list, or click the Add (+) icon to add a new one.

    c) Optional: The "Allow Users to select connection profile when logging in" checkbox can remain checked or unchecked.

    d) Optional: The "Bypass Access Control policy for decrypted traffic" checkbox can remain checked or unchecked. **Note:** Decrypted traffic is subjected to Access Control Policy by default. Enabling this option will bypasses inspection associated with the ACP, but VPN Filter ACL and authorization ACL downloaded from AAA server are still applied to VPN traffic.

6) The **Advanced** tab allows configuration of the remaining Remote Access Policy options:

    a) Configuring the **Secure Client Images**. The Cisco Secure Client client provides IPsec (IKEv2) and TLS connections to the FTD for remote users with full VPN profiling to corporate resources. Without a previously-installed client, remote users can enter the IP address of an interface configured to accept clientless VPN connections in their browser to download and install the Secure Client client. The FTD downloads the client that matches the operating system of the remote computer. After downloading, the client installs and establishes a secure connection. In the case of a previously installed client, when the user authenticates, the FTD, examines the revision of the client, and upgrades the client as necessary.

        i) Click the **Add (+)**icon in the **Available Secure Client Images** portion of the **Secure Client Images** dialog.

        ii) Enter then **Name**, **File Name**, and **Description** for the available Secure Client Image.

        iii) Click **Browse** to navigate to the location for selecting the client image to be uploaded.

        iv) Click **Save** to upload the image in the FMC.

b) Configuring the **Address Assignment Policy**. The FTD can use IPv4 or IPv6 policy for assigning IP addresses to Remote Access VPN client`s. If you configure more than one address assignment method, the FTD tries each of the options until it finds an IP address. You can use the IPv4 or IPv6 policy to find an IP address to the Remote Access VPN clients, though any selected IPv4 options will be attempted before any IPv6 options.

   i) **Use authorization server (RADIUS only)**. This option will allow the Secure Client client to obtain its IP address as part of AAA (RADIUS) authentication. Note: This option will only be viable if the one of the enabled Secure Client authentication methods (defined within the Connection Profile) includes "AAA" (either "AAA Only", or "Client Certificate & AAA").

   ii) **Use DHCP** (applicable to IPv4 only). This option will allow the Secure Client client to obtain an IP address from a DHCP server configured in a connection profile. You can also define the range of IP addresses that the DHCP server can use by configuring DHCP network scope in the group policy. If you use DHCP, configure the server in the **Objects > Object Management > Network** pane. This method is available for IPv4 assignment policies.

   iii) **Use an internal address pool**s. This option will allow the Secure Client client to obtain its IP address from the FTD's internally configured address pools. This is the easiest method of address pool assignment to configure, since the configuration does not rely on any non-Firepower component. If you use this method, create the IP address pools in **Objects > Object Management > Address Pools** pane and select the same in the connection profile. This method is available for both IPv4 and IPv6 assignment policies.

      (1) Optional: **Reuse an IP address after it is released.** This option delays the reuse of an IP address after its return to the address pool. Adding a delay helps to prevent problems firewall scan experience when an IP address is reassigned quickly. By default, the delay is set to zero, meaning the FTD does not impose a delay in reusing the IP address. If you want to extend the delay, enter the number of minutes in the range 0-480 to delay the IP address reassignment. This configurable element is available for IPv4 assignment policies.

c) Configuring the **Certificate Maps.** Certificate to connection profile maps are used for certificate authentication on secure gateways.

   i) Set the General Settings for Certificate Group Matching.

      (1) Select any, or all, of the following options to establish authentication and to determine to which connection profile (tunnel group) to map the client. Selections are priority-based, if a match is not found for the first selection matching continues down the list of options. When the rules are satisfied, the mapping is done. If the rules are not satisfied, the default connection profile (listed at the bottom) is used for this connection.

      (2) Use Group URL if Group URL and Certificate Map match different Connection profiles

      (3) Use the configured rules to match a certificate to a Connection Profile—Enable this to use the rules defined here in the Connection Profile Maps

   ii) Add Certificate to Connection Profile Mapping for this policy.

      (1) Click **Add**.

      (2) Choose or create a **Certificate Map** Object.

      (3) Specify the **Connection Profile** that is used if the rules in the certificate map object are satisfied.

      (4) Click **Save**.

d) Configuring Group Policies. A Group Policy is a set of attribute and value pairs, stored in a group policy object, that define the remote access VPN experience. For example, in the group policy object, you configure general attributes such as addresses, protocols, and connection settings.

   i) Select more group policies to associate with this Remote Access VPN policy. These are above and beyond the default group policy assigned at RAVPN policy creation time. Click **Add**. To create a group policy, please see “Configure Group Policy Object” section below.

   ii) Click **OK** when you have the **Selected Group Policy** window set as desired.

e) Configuring **IPsec:**

   i) The **Crypto Maps** page lists the interface groups on which IKEv2 protocol is enabled. Crypto Maps are auto generated for the interfaces on which IKEv2 protocol is enabled.

      (1) Select IPsec > Crypto Maps.

      (2) Click on **Interface Group**, the interface group on which IKEv2 protocol is enabled.

      (3) On **IKEv2 IPsec Proposals**, click **Edit** to specify the proposals for your chosen IKEv2 method. On the IKEv2 IPsec Proposal dialog box, select from the available Transform Sets, or create a new IKEv2 IPsec proposal. For the CC-certified configuration, the selected transform sets must not include DES_SHA-1, the allowed transform sets are **AES-GCM** and/or **AES-SHA**.

      (4) (Optional) **Enable Reverse Route Injection**—enables static routes to be automatically inserted into the routing process for those networks and hosts protected by a remote tunnel endpoint.

      (5) (Recommended) **Enable Perfect Forward Secrecy**—Whether to use Perfect Forward Secrecy (PFS) to generate and use a unique session key for each encrypted exchange. The unique session key protects the exchange from subsequent decryption, even if the entire exchange was recorded and the attacker has obtained the preshared or private keys used by the endpoint devices. If you select this option, also select the Diffie-Hellman key derivation algorithm to use when generating the PFS session key in the **Modulus Group** list.

      (6) **Lifetime Duration (seconds)**—The lifetime of the security association (SA), in seconds. When the lifetime is exceeded, the SA expires and must be renegotiated between the two peers. As a general rule, the shorter the lifetime (up to a point), the more secure your IKE negotiations will be. However, with longer lifetimes, future IPsec security associations can be setup more quickly than with shorter lifetimes. You can specify a value from 120 to 2147483647 seconds. The default is 28800 seconds. Any value is allowed in the CC-certified configuration.

      (7) (Optional) **ESPv3 Settings** are disabled by default, but enabling them with any configurable values is allowed in the CC-evaluated configuration.

   ii) The **IKE Policy** page specifies all of the IKEv2 policy objects applicable for this VPN policy when Secure Client endpoints connect via IPsec-IKEv2 protocol. **Note:** The policies listed on this page are named objects, which are also viewable under **Objects > Object Management > VPN > IKEv2 Policy**. There are three default IKEv2 policies which cannot be edited, but new policies can be created and assigned to the Remote Access Policy. The IKEv2 Policy that’s mapped by default to any Remote Access Policy is the “DES-SHA-SHA” policy, which is not permitted in the CC-evaluated configuration because it uses DES.

      (1) Click the Add (+) icon to modify the list of allowed IKEv2 Policies.

(2) Remove "DES-SHA-SHA" and add a policy that complies with the CC-evaluated configuration, which can be either of the other two default IKEv2 Policies (**AES-SHA-SHA, or AES-GCM-NULL-SHA**, **or AES-GCM-NULL-SHA-LATEST** where "null" indicates a null selection for integrity algorithm because GCM provides integrity), or create a new custom policy that contains any of the following options, and no other options:

(a) **Name**: Can be any name, but cannot include spaces.

(b) **Description**: Any description is allowed.

(c) **Priority**: Any priority is allowed.

(d) **Lifetime**: Any lifetime is allowed.

(e) **Integrity**: Can be any of SHA, SHA256, SHA384, or SHA512, or NULL only if the encryption algorithm is one of AES-GCM, AES-GCM-192, or AES-GCM-256.

(f) **Encryption:** Can be any of AES, AES-192, AES-256, AES-GCM, AES-GCM, or AES-GCM-256.

(g) **PRF Algorithms:** Can be blank, or can be any of SHA, SHA256, SHA384, or SHA512.

(h) **Diffie-Hellman Group**: Can be any of 14, 19, 20, or 24.

iii) The **IPsec/IKEv2 Parameters** tab allows configuration of the remaining options. Any of the configuration options are permitted in the CC-evaluated configuration, including:

(1) **IKEv2 Session Settings**

(a) Identity Sent to Peers is set to Auto by default, and can be changed to IP Address or Hostname.

(b) Enable Notification on Tunnel Disconnect is disabled by default.

(c) Do not allow device reboot until all sessions are terminated is disabled by default.

(2) **IKEv2 Security Association (SA) Settings**

(a) Cookie Challenge is set to Custom by default, with a default threshold of 50%.

(b) Number of SAs allowed in Negotiation is set to 100% by default.

(c) Maximum number of SAs allowed is set to Device Maximum by default.

(3) **IPsec Settings**

(a) Enable Fragmentation Before Encryption is enabled by default.

(b) Path Maximum Transmission Unit Aging is disabled by default.

(4) **NAT Transparency Settings**

(a) Enable IPsec over NAT-T is enabled by default.

7) Click **Save**.

8) Click **Deploy** to deploy the configuration changes on the FTD.

7.4.3 Adding a Remote Access VPN Policy

1) Login to FMC.

2) Choose **Devices > VPN > Remote Access**.
3) Click **Add (+)**.
4) Follow the steps in the **Remote Access VPN Policy Wizard**. Refer to section "Create a New Remote Access VPN Policy" in [FMC-CG] for more details. Any configurable values are acceptable in the CC-evaluated configuration except on the **Policy Assignment** step where the **VPN Protocol** must be **IPsec-IKEv2 or SSL**.

7.4.4 Configure Group Policy Object (optional)

1. Login to FMC using an Administrator Role.
2. Choose **Objects > Object Management > VPN > Group Policy**. Click **Add Group Policy** or choose a current policy to edit, then select the **Advanced** tab, which contains the following fields.
    1. **Access Hours**—Choose or create a time range object. This object specifies the range of time this group policy is available to be applied to a remote access user.
    2. **Idle Timeout/Alert Interval**—Specifies user's idle timeout period in minutes. If there is no communication activity on the user connection in this period, the system stops the connection. The minimum time is 1 minute. The default is 30 minutes. The Alert interval specifies the interval of time before idle time is reached to display a message to the user.

8 Secure Client Installation and Configuration

The Cisco Secure Client is a software application installed to a Windows 10/11 workstation that allows the workstation to establish an IPsec/TLS remote access VPN tunnel to an FTD appliance.

Once installed, Secure Client provides the VPN user with the following functions and interfaces:

- An icon on the Windows task bar. Right-clicking on the icon provides the option to open the Secure Client GUI.
- The Secure Client GUI allows the VPN user to:
    - Select a VPN gateway target (an alias name, hostname, FQDN, or IP address), or to type in an IP address or FQDN and click the "**Connect**" button to initiate an IPsec tunnel to the target.
    - Click a "**Disconnect**" button to terminate an established IPsec/TLS tunnel.
    - Click a status icon to see **stats** for the currently established tunnel, including duration of the connection, bytes sent, bytes received, etc.

8.1.1 For a basic overview of the essential GUI features, refer to "Check Installed Version

8.1.2 To check that the correct certified version of Secure Client is installed, you can execute one of the following commands:

Version is shown by clicking the "about" icon (lower-case "i" within a circle).

Version is shown in Windows CLI using: "vpncli.exe -v"

- Secure Client Connection to FTD" section 8.3.1 of this document. For a more through overview of Secure Client features, refer to [SC-ADMIN].

- The Secure Client CLI commands allow the VPN user to:

- Perform the same operations available via the GUI (via commands including: **connect**, **disconnect**, **stats**, etc.)
- For a full overview of CLI commands, refer to the "Use the Secure Client CLI Commands" section of [SC-ADMIN].

Note: The sections below explain that the IPsec/TLS remote access VPN functionality of Secure Client is provided by the "Core" component of the Secure Client suite of software (referred to as "Core & VPN" in the installer GUI, and referred to as the "core client" in [SC-ADMIN]). The core client is the only part of Secure Client that must be installed on the Windows workstation to support IPsec/TLS connectivity with FTD. Except where indicated, all references to "Secure Client" within this document refer only to the Core & VPN component of Secure Client. The "Secure Client Installation" section of this document (section 8.3 below) specifies which other components of the Secure Client suite of software may be installed with the Core & VPN component, and which components are prohibited to use with this CC-certified configuration of Secure Client.

8.2 Preparative Procedures the IT Environment

This section provides instructions for installing the required IT environment components to allow establishing remote access IPsec/TLS VPN connections between the Secure Client client and FTD. This requires a minimum of:

- one Certificate Authority (CA)
- one VPN Gateway (at least one FTD)
- one end-user Windows 10/11 workstation to which Secure Client will be installed

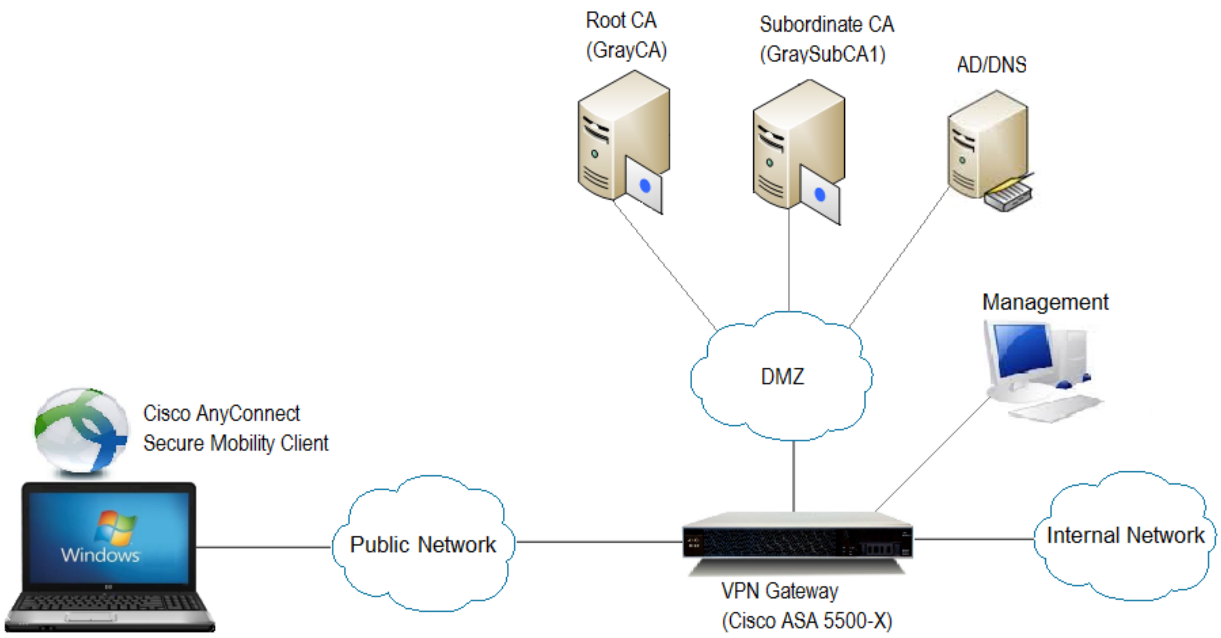
8.2.1 Install and Configure a Certificate Authority

To allow Secure Client clients to authenticate to FTD using X.509 certificates, a certificate authority (CA) must be available and accessible to the Secure Client client and also to FTD.

Any CA server that supports X.509v3 certificates can be used. To provide an example configuration, this section shows use of Microsoft Windows 2012 R2 Server as the CA server, but other CA products may be used other than Microsoft. Multi-chain PKI certificate structures are supported, but to provide a simplified example, this section shows a simple two-tier CA solution using an Offline Root CA and an Enterprise Subordinate CA.

A Root CA is configured as a standalone (Workgroup) server while the Subordinate CA is configured as part of a Microsoft domain with Active Directory services enabled. See Figure 3 below:

Figure 3: Secure Client Deployed with a Two-Tier CA Solution



The Subordinate CA issues X.509 digital certificates and provides a Certificate Revocation List (CRL) to the Windows host and VPN Gateway (FTD).

Alternatively, one (1) single root Enterprise CA could be deployed in the IT environment.

If using a Microsoft two-tier CA solution, install and configure a Root (GRAYCA) and Enterprise Subordinate Certificate Authority (GRAYSUBCA1) in accordance with the guidance from the vendor. The following is a step-by-step guide for the configuration of Microsoft Active Directory Certificate Services: https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/hh831348(v=ws.11)?redirectedfrom=MSDN

It is assumed both the Offline Root CA (GRAYCA) certificate and the Enterprise Subordinate CA (GRAYSUBCA1) certificates depicted in figure 1 are installed and trusted to ensure a trusted certificate chain is established.

If using a CA from a vendor other than Microsoft, follow that vendor's CA installation guidance.

Configuration Note:

Regardless of the CA product used, the ECDSA and RSA certificates on the FTD MUST have the following Key Usage and Extended Key Usage properties:

- Key Usage: Digital Signature, Key Agreement
- EKU: IP security IKE intermediate, IP end security system

The Subject Alternative Name (SAN) fields within ECDSA and RSA certificates on the FTD MUST match the connection information specified within the Secure Client profile on the client.

The Windows client needs to have following Key Usage and Extended Key Usage properties:

- Key Usage: Digital Signature, Key Agreement
- EKU: Client Authentication

8.2.2 Enroll the Secure Client Windows Host with the CA

The Microsoft "MMC" Certificate snap-in tool should be used to both generate a CSR and import certificates. Information on the use of MMC can be found here: http://technet.microsoft.com/en-us/library/dd632619.aspx

The Secure Client host administrator needs to follow the steps below from Microsoft to complete a manual CSR on a Windows machine: http://technet.microsoft.com/en-us/library/cc730929.aspx

Configuration Note: In step 4, select: **(No template) CNG key**

Configuration Note: In step 6, select: **PKCS #10**

Configuration Note: In step 8, the properties of the Certificate Request, ensure the following is selected:

- Click the Subject tab. Provide a Values for Subject name (at least Common Name = FQDN, and Country, plus typically State, Locality, Organization, and Organizational unit).
- Click the Private Key tab. Select one of:
  - RSA, Microsoft Software Key Storage Provider. If using RSA, select a key size of 2048 or greater under "Key options".
  - ECDSA_P256, Microsoft Software Key Storage Provider.
  - ECDSA_P384, Microsoft Software Key Storage Provider.
  - ECDSA_P521, Microsoft Software Key Storage Provider.
- Click the drop-down box to select the Hash Algorithm. Select one of Default Algorithm, sha256, sha384, or sha512 and click Apply.
- Click the **Extensions** tab
  - Click the drop-down box Under **Key usage** and select **Digital Signature** and select **Add** and **Apply**.
  - Click the drop-down box Under Extended Key Usage and Select Client Authentication, and select **Add** and **OK**.

After completing Step 9, save the CSR to a location and select "OK"

Configuration Note: The CSR will now need to be sent to the CA administrator and processed to obtain the Windows host identity certificate. If using a CA from a vendor other than Microsoft, follow that vendor's guidance for use of templates and certificate generation.

8.2.3 Import Certificates onto the Windows Host

Import the CA certificates and the Windows host identity certificate into the Windows certificate store. To import certificates, refer to the following instructions from Microsoft: http://technet.microsoft.com/en-us/library/cc754489.aspx

Configuration Note: The CA certificate must be in the Trusted Root Store.

8.2.4 Create a Secure Client VPN Client Profile (XML file)

The Windows host on which Secure Client is installed will need to contain an XML file, called an Secure Client VPN Client Profile (also called the Secure Client Profile, or just the Client Profile), which defines the how Secure Client will connect to FTD. These XML files can be created using the Secure Client

Profile Editor, which can be installed on the same Windows 10/11 workstation where the Secure Client client has been installed, or on a separate Windows workstation.

Once one or more Client VPN Profiles have been created using the Secure Client Profile Editor, they can be uploaded to FMC where they can be assigned to VPN Group Policies, which are deployed to FTD appliances. Once the XML profile has been associated with the Group Policy, the FTD will provide the SHA-1 checksum of the Client Policy to Secure Client at the start of the IPsec/TLS session and Secure Client will verify that its locally stored Client Policy is correct by comparing the received checksum to checksums of it's locally stored Client Policies. If the Secure Client client initiating connection to FTD doesn't have the Client Policy, the Secure Client client will request and receive the current Client Profile from FTD.

For more detailed information, refer to, "The Profile Editor" section of [SC-ADMIN]. Note that the Secure Client Administrator Guide expects that the VPN gateway to which Secure Client will be connected will be a Cisco ASA appliance, but in this case, for this CC-evaluated configuration, the VPN gateway will be an FTD appliance.

To install the Secure Client Profile Editor:

1. Download the installer from software.cisco.com by searching for Secure Client 5.1, and selecting the latest 5.1 version of the "Profile Editor (Windows)", e.g. tools-cisco-secure-client-win-5.1.2.42-profileeditor-k9.msi.
2. Install the *.msi file. Note: The Cisco Profile Editor 5.1.x cannot be installed on systems with JRE version lower than 8.

On the Windows 10/11 workstation running the Secure Client client, the Client Profile must be stored on the Windows 10/11 workstation running Secure Client. The file can be placed in the expected location manually, or it will be put in that location automatically when the Secure Client client connects to FTD. The file location is:

```
%ProgramData%\Cisco\Cisco Secure Client\VPN\Profile
```

8.3 Secure Client Installation

Follow the steps below to install the Secure Client client software on Windows 10/11. For more details refer to the "Predeploying to Windows" section of [SC-ADMIN] and Install Cisco Secure Client on a Windows Computer [SC-INSTALL].

1) Contact your Cisco sales representative and request a download link for the following Secure Client file:

   - cisco-secure-client-win-5.1.2.42-predeploy-k9.zip (Cisco Secure Client Pre-Deployment Package (Windows) - includes individual MSI

   - The zip file SHA-512 checksum is: 83e16e1a19a8b7c518e128dd366f79f1cba27a01984d205f6f8e2e6ae91219fc27b5ad93066c723f3a00648410f45dd6f94959415bc4c17e1992010b84b2df31

2) Download zip file.

3) Verify the integrity of the downloaded file by comparing the SHA512 checksum shown on the download page with one generated locally. Windows 10 includes a built-in utility to generate checksums, called certutil, where the syntax would be:

   - certutil -hashfile cisco-secure-client-win-5.1.2.42-predeploy-k9.zip SHA512

4) If the locally generated checksum matches the expected value, extract the *.zip file in a local folder. The zip contains multiple *.msi files, one for each add-on Secure Client module:

- *amp*.msi, *core*.msi, *dart*.msi, *gina*.msi, *iseposture*.msi, *nam*.msi, *nvm*.msi, *posture*.msi, *umbrella*.msi, and *websecurity*.msi.

5) Select which modules to install:

   a) Some add-on modules are allowed in the CC-evaluated configuration, and others are prohibited or not supported with FTD. Refer to section 1.5.5 of this document for a complete listing.

   b) Required module:

      i) Core & AnyConnect VPN (*core*.msi) is required to support IPsec VPN functionality.

   c) Allowed add-on modules:

      i) Diagnostic And Reporting Tool (*dart*.msi)

      ii) Start Before Login (*gina*.msi)

      iii) Umbrella (*umbrella*.msi)

   d) Prohibited (or not supported with FTD) add-on modules:

      i) Network Access Manager (*nam*.msi)

      ii) Network Visibility Module (*nvm*.msi)

      iii) Secure Firewall Posture (*Posture*.msi)

      iv) ThousandEyes (*thousandeyes*.msi)

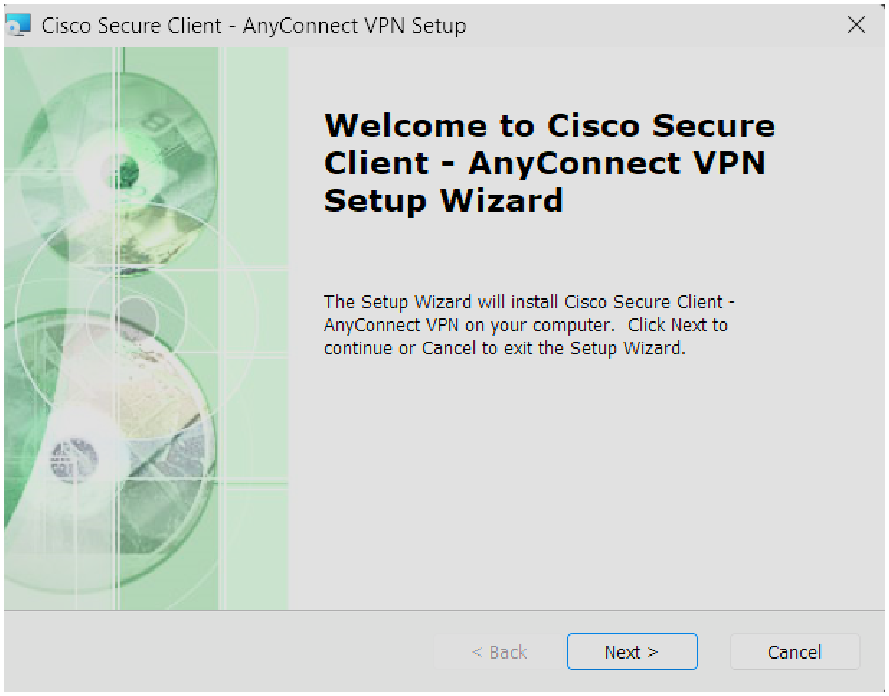
      v) ISE Posture (*iseposture*.msi)

6) Install the downloaded file by double-clicking the *core*.msi filename, or by running Setup.exe and selecting “Core & VPN” (see Figure 4 below).

   Note: *Upon installation, a digital signature verification check will automatically be performed. The authorized source for the digitally signed updates is "Cisco Systems, Inc." Verification includes a check that the certificate is valid and has a Code Signing Value of 1.3.6.1.5.5.7.3.3 in the EKU field. Should the installation abort stating the signature was not valid, do not continue the installation and contact Cisco Technical Support for assistance.*

7) If using the msi installer:

   a) The Cisco Secure Client Setup dialog box will appear.

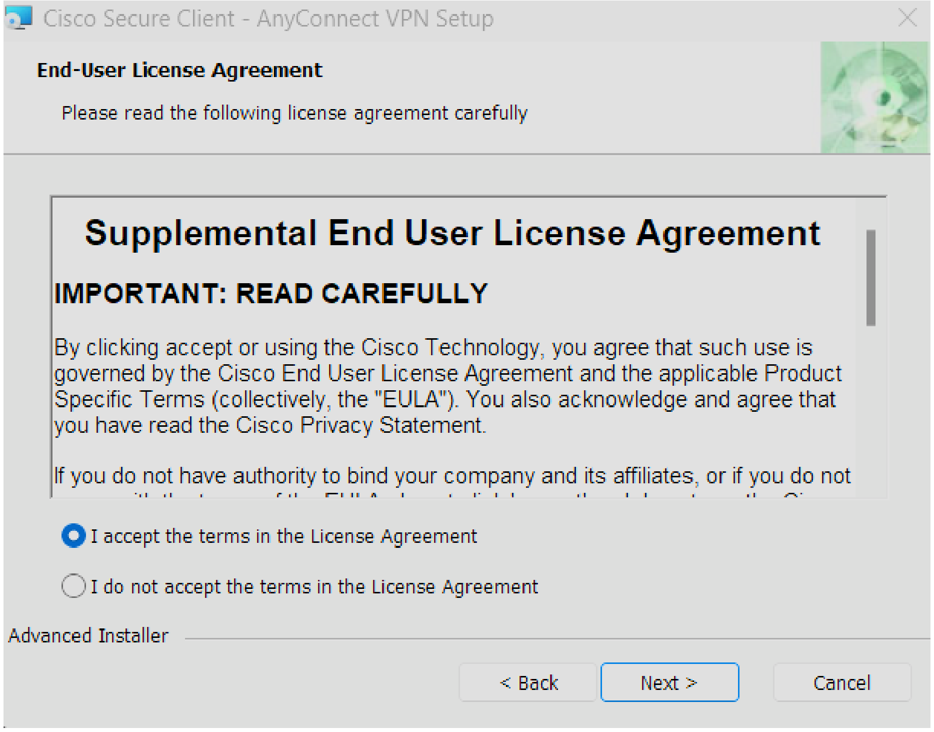


Cisco Secure Client - AnyConnect VPN Setup

Welcome to Cisco Secure Client - AnyConnect VPN Setup Wizard

The Setup Wizard will install Cisco Secure Client - AnyConnect VPN on your computer. Click Next to continue or Cancel to exit the Setup Wizard.

b) Click **Next** to continue.



Cisco Secure Client - AnyConnect VPN Setup

End-User License Agreement

Please read the following license agreement carefully

Supplemental End User License Agreement

IMPORTANT: READ CAREFULLY

By clicking accept or using the Cisco Technology, you agree that such use is governed by the Cisco End User License Agreement and the applicable Product Specific Terms (collectively, the "EULA"). You also acknowledge and agree that you have read the Cisco Privacy Statement.

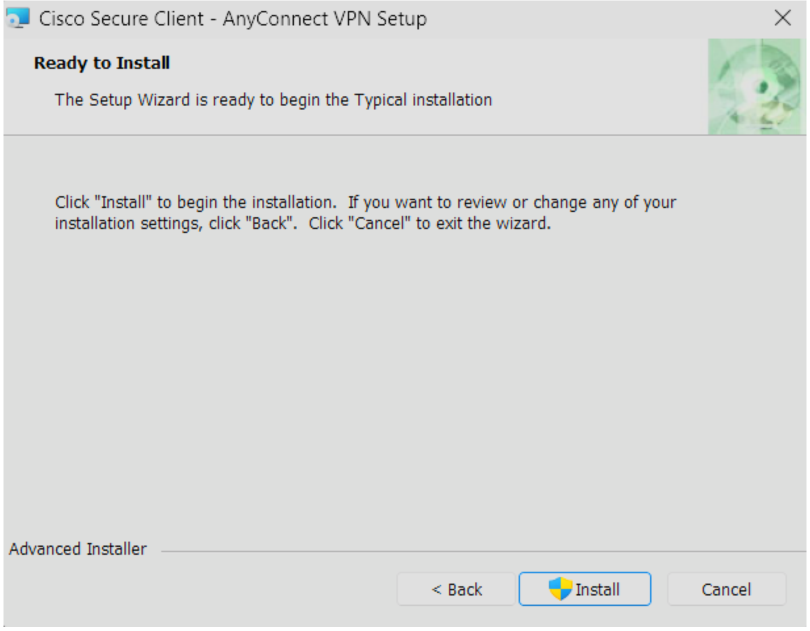
If you do not have authority to bind your company and its affiliates, or if you do not

● I accept the terms in the License Agreement

○ I do not accept the terms in the License Agreement

c) After reading the End-User License Agreement, click the radio button if you accept the terms in the agreement. Click **Next** to continue.

d) The “Ready to Install” dialogue box will appear.

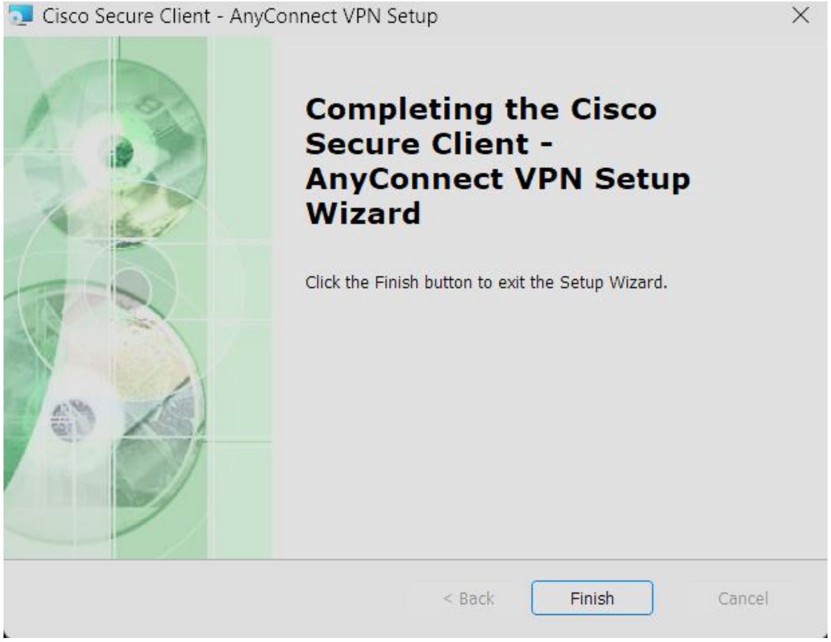


Ready to Install

The Setup Wizard is ready to begin the Typical installation

Click "Install" to begin the installation. If you want to review or change any of your installation settings, click "Back". Click "Cancel" to exit the wizard.

e) Click **Install** to Continue.



Completing the Cisco Secure Client - AnyConnect VPN Setup Wizard

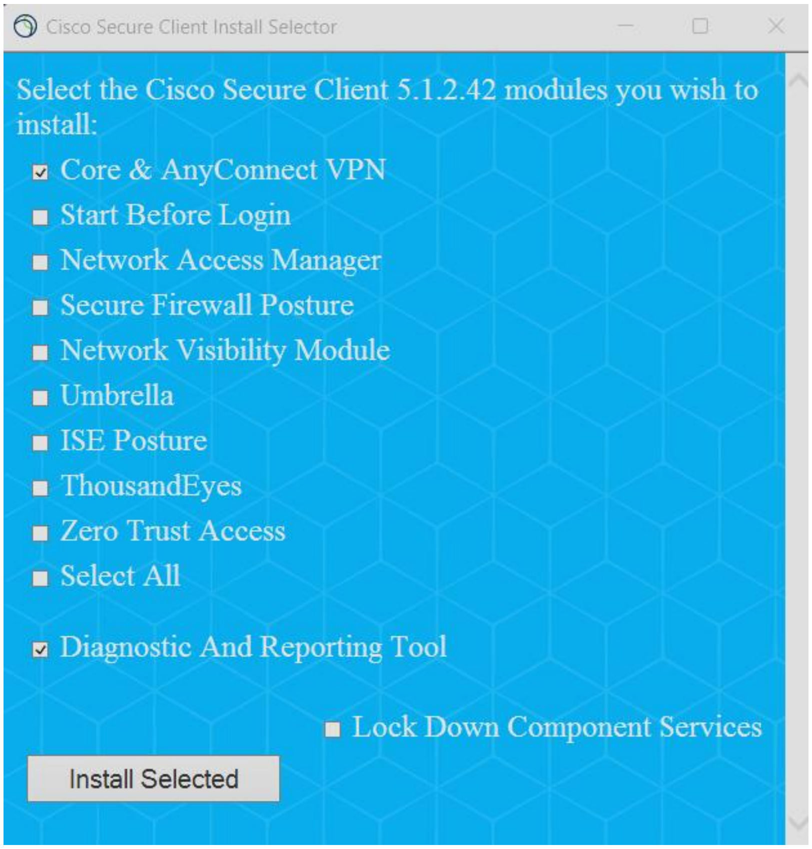
Click the Finish button to exit the Setup Wizard.

f) The software will install. Click **Finish** when complete.

8) If using Setup.exe it's possible to select multiple packages to be installed. Use of Setup.exe is optional instead of installing *.msi files individually.

   a) If using Setup.exe, checking "Lock Down Component Services" is optional (see Figure 4 below). Selecting that option will lock down the permissions of the Windows Services for each module that is installed. This will prevent any user from stopping the service, including local administrators.

Figure 4: Using Setup.exe to Install Secure Client



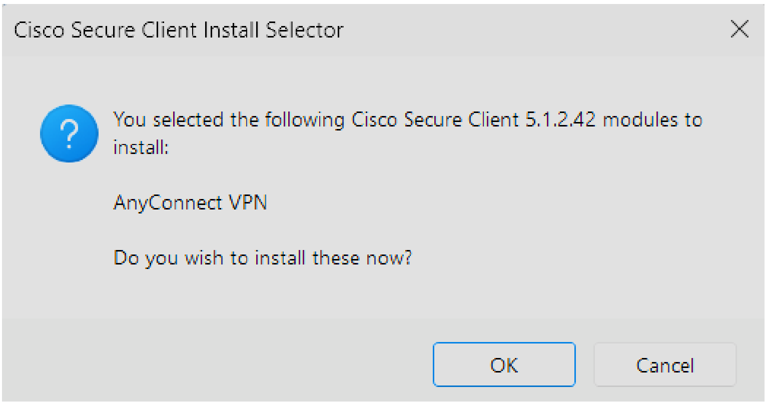
Select the Cisco Secure Client 5.1.2.42 modules you wish to install:

- ☑ Core & AnyConnect VPN
- □ Start Before Login
- □ Network Access Manager
- □ Secure Firewall Posture
- □ Network Visibility Module
- □ Umbrella
- □ ISE Posture
- □ ThousandEyes
- □ Zero Trust Access
- □ Select All

- ☑ Diagnostic And Reporting Tool

□ Lock Down Component Services

b) Check at least "**Core & AnyConnect VPN**" and click **Install Selected**.

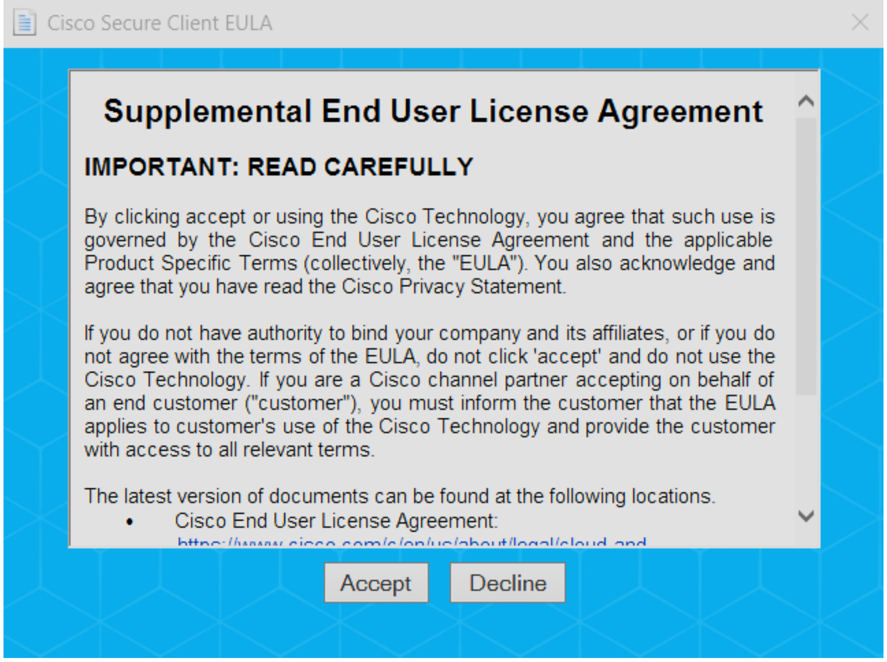


You selected the following Cisco Secure Client 5.1.2.42 modules to install:

AnyConnect VPN

Do you wish to install these now?

c) Click **OK** to confirm the selections.



Supplemental End User License Agreement

IMPORTANT: READ CAREFULLY

By clicking accept or using the Cisco Technology, you agree that such use is governed by the Cisco End User License Agreement and the applicable Product Specific Terms (collectively, the "EULA"). You also acknowledge and agree that you have read the Cisco Privacy Statement.

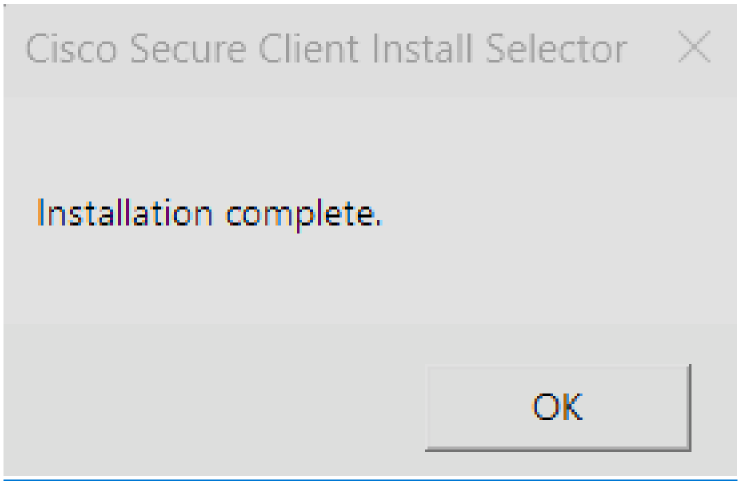
If you do not have authority to bind your company and its affiliates, or if you do not agree with the terms of the EULA, do not click 'accept' and do not use the Cisco Technology. If you are a Cisco channel partner accepting on behalf of an end customer ("customer"), you must inform the customer that the EULA applies to customer's use of the Cisco Technology and provide the customer with access to all relevant terms.

The latest version of documents can be found at the following locations.

- Cisco End User License Agreement: https://www.cisco.com/c/en/us/about/legal/cloud-and

d) After reading the End-User License Agreement, click **Accept** if you accept the terms in the agreement.

e) An installation progress box appears.



Installation complete.

f) When installation completes, click OK.

9) Navigate to **All Programs > Cisco > Cisco Secure Client** and click on the **Cisco Secure Client** icon.

10) Clicking the ‘About’ button will display version information.

8.3.1 Check Installed Version

To check that the correct certified version of Secure Client is installed, you can execute one of the following commands:

- Version is shown by clicking the “about” icon (lower-case “i” within a circle).
- Version is shown in Windows CLI using: “vpncli.exe -v”

8.4 Secure Client Connection to FTD

8.4.1 Preliminary Steps

Before proceeding:

- Ensure that a Secure Client VPN Client Policy has been created by completing all steps in section 8.2.4 of this document.
- Ensure that the VPN Remote Access policy has been created on FMC and deployed to one or more FTD by completing all steps in section 7.3.7 of this document.

8.4.2 Initiating the VPN Connection

1. Launch the Cisco Secure Client client. If a client policy has already been installed, and that policy contains a list of VPN gateways, that list will be visible in the drop-down box. Otherwise type the IP address or hostname of the VPN gateway, then click **Connect**.
2. Authentication of the VPN gateway:
   - If the VPN gateway certificate is valid and this is the first connection to the gateway you will be prompted to accept the certificate into the Windows certificate store.
3. Authentication of the Secure Client client:
   - If the VPN gateway (FTD) has been configured to only require certificate-based authentication, and the Secure Client host has been properly configured with an identity certificate, then the VPN will be established.
4. If the VPN gateway has been configured to require a secondary (RADIUS) authentication, the Secure Client client will prompt for the user credentials, and you must enter valid credentials before the VPN tunnel will be established.
5. Once the authentication steps have been completed, you can verify the status of the connection by clicking the Cisco Secure Client icon in the System Tray. You should see a green checkbox stating it is connected to the VPN gateway (Server).
6. To end the VPN Session, click the Disconnect Button.

Administrator Note: If the VPN gateway certificate is invalid or fails the CRL check, Secure Client will disallow the connection. If this situation occurs, the administrator will receive the following message:

Upon clicking OK, the connection attempt will show it failed.

If an IPsec/TLS session between Secure Client and a VPN gateway is unexpectedly interrupted, Secure Client will display a message that the VPN is disconnected. If this message appears, the user should re-initiate the IPsec/TLS VPN connection to the gateway.

9 System Monitoring and Audit Messages

9.1 FMC Audit Messages

The FMC and managed FTD devices log read-only auditing information for user activity. Audit logs are presented in a standard event view that allows administrator to view, sort, and filter audit log messages based on any item in the audit view. Administrator can delete and report on audit information and can view detailed reports of the changes that users make.

The audit log stores a maximum of 100,000 entries. When the number of audit log entries greatly exceeds 100,000, the appliance overwrites the oldest records from the database to reduce the number to 100,000.

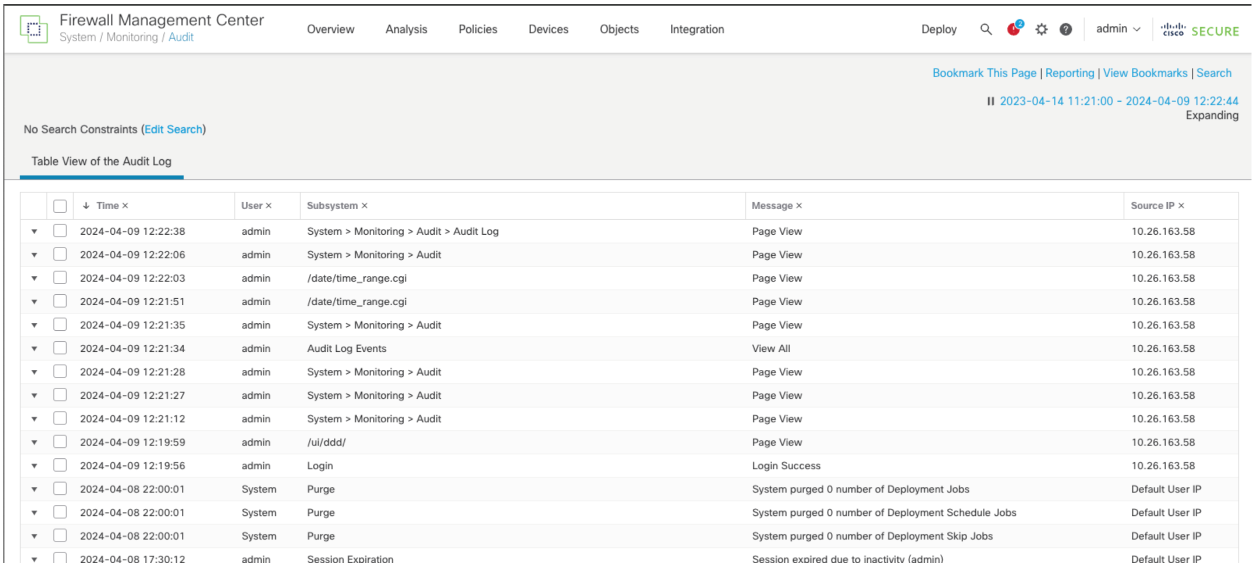
> **NOTE!** To change the maximum number of entries, go to System > Configuration > Database > Audit Event Database > Maximum Audit Events

The syslog is not stored in the same database as the audit logs. The number of syslog entries is based on the disk space so it varies based on the model. However, when the syslog storage space is full, it will overwrite the oldest logs with the newest logs via ‘logrotate’ implementation.

> **NOTE!** To prevent losing audit records, set up an audit server to send a copy of the audit and syslog records to.

The “Audit Log” on the FMC contains the log messages related to administrative actions performed on the FMC.

1. Login with Administrator Role.
2. Select System > Monitoring > Audit.



Firewall Management Center
System / Monitoring / Audit
Overview
Analysis
Policies
Devices
Objects
Integration
Deploy
admin
SECURE
Bookmark This Page | Reporting | View Bookmarks | Search
Table View of the Audit Log

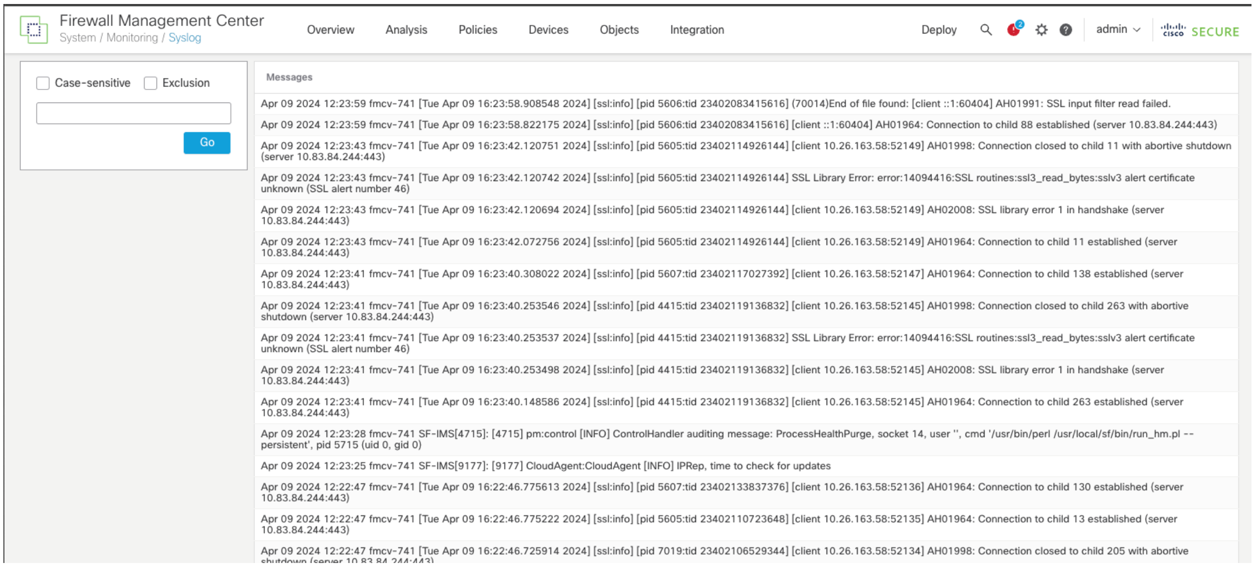
2023-04-14 11:21:00 - 2024-04-09 12:22:44
Expanding

No Search Constraints (Edit Search)

↓ Time ×	User ×	Subsystem ×	Message ×	Source IP ×
2024-04-09 12:22:38	admin	System > Monitoring > Audit > Audit Log	Page View	10.26.163.58
2024-04-09 12:22:06	admin	System > Monitoring > Audit	Page View	10.26.163.58
2024-04-09 12:22:03	admin	/date/time_range.cgi	Page View	10.26.163.58
2024-04-09 12:21:51	admin	/date/time_range.cgi	Page View	10.26.163.58
2024-04-09 12:21:35	admin	System > Monitoring > Audit	Page View	10.26.163.58
2024-04-09 12:21:34	admin	Audit Log Events	View All	10.26.163.58
2024-04-09 12:21:28	admin	System > Monitoring > Audit	Page View	10.26.163.58
2024-04-09 12:21:27	admin	System > Monitoring > Audit	Page View	10.26.163.58
2024-04-09 12:21:12	admin	System > Monitoring > Audit	Page View	10.26.163.58
2024-04-09 12:19:59	admin	/ui/ddd/	Page View	10.26.163.58
2024-04-09 12:19:56	admin	Login	Login Success	10.26.163.58
2024-04-08 22:00:01	System	Purge	System purged 0 number of Deployment Jobs	Default User IP
2024-04-08 22:00:01	System	Purge	System purged 0 number of Deployment Schedule Jobs	Default User IP
2024-04-08 22:00:01	System	Purge	System purged 0 number of Deployment Skip Jobs	Default User IP
2024-04-08 17:30:12	admin	Session Expiration	Session expired due to inactivity (admin)	Default User IP

3. The System log (syslog) page provides administrator with system log information for the appliance. The system log displays each message generated by the system. The following items are listed in order:
    - Date that the message was generated.
    - Time that the message was generated.
    - Host that generated the message.
    - The message itself[5].
4. Select System > Monitoring > Syslog.

[5] The message includes the user or source IP only if applicable. In most cases, the system generated the system log not the user and most of the time, the source IP address is the IP address of the appliance (i.e., system process resides on the system).



```
Apr 09 2024 12:23:59 fmcv-741 [Tue Apr 09 16:23:58.908548 2024] [ssl:info] [pid 5606:tid 23402083415616] (70014)End of file found: [client ::1:60404] AH01991: SSL input filter read failed.
Apr 09 2024 12:23:59 fmcv-741 [Tue Apr 09 16:23:58.822175 2024] [ssl:info] [pid 5606:tid 23402083415616] [client ::1:60404] AH01964: Connection to child 88 established (server 10.83.84.244:443)
Apr 09 2024 12:23:43 fmcv-741 [Tue Apr 09 16:23:42.120751 2024] [ssl:info] [pid 5605:tid 23402114926144] [client 10.26.163.58:52149] AH01998: Connection closed to child 11 with abortive shutdown
(server 10.83.84.244:443)
Apr 09 2024 12:23:43 fmcv-741 [Tue Apr 09 16:23:42.120742 2024] [ssl:info] [pid 5605:tid 23402114926144] SSL Library Error: error:14094416:SSL routines:ssl3_read_bytes:sslv3 alert certificate
unknown (SSL alert number 46)
Apr 09 2024 12:23:43 fmcv-741 [Tue Apr 09 16:23:42.120694 2024] [ssl:info] [pid 5605:tid 23402114926144] [client 10.26.163.58:52149] AH02008: SSL library error 1 in handshake (server
10.83.84.244:443)
Apr 09 2024 12:23:43 fmcv-741 [Tue Apr 09 16:23:42.072756 2024] [ssl:info] [pid 5605:tid 23402114926144] [client 10.26.163.58:52149] AH01964: Connection to child 11 established (server
10.83.84.244:443)
Apr 09 2024 12:23:41 fmcv-741 [Tue Apr 09 16:23:40.308022 2024] [ssl:info] [pid 5607:tid 23402117027392] [client 10.26.163.58:52147] AH01964: Connection to child 138 established (server
10.83.84.244:443)
Apr 09 2024 12:23:41 fmcv-741 [Tue Apr 09 16:23:40.253546 2024] [ssl:info] [pid 4415:tid 23402119136832] [client 10.26.163.58:52145] AH01998: Connection closed to child 263 with abortive
shutdown (server 10.83.84.244:443)
Apr 09 2024 12:23:41 fmcv-741 [Tue Apr 09 16:23:40.253537 2024] [ssl:info] [pid 4415:tid 23402119136832] SSL Library Error: error:14094416:SSL routines:ssl3_read_bytes:sslv3 alert certificate
unknown (SSL alert number 46)
Apr 09 2024 12:23:41 fmcv-741 [Tue Apr 09 16:23:40.253498 2024] [ssl:info] [pid 4415:tid 23402119136832] [client 10.26.163.58:52145] AH02008: SSL library error 1 in handshake (server
10.83.84.244:443)
Apr 09 2024 12:23:41 fmcv-741 [Tue Apr 09 16:23:40.148586 2024] [ssl:info] [pid 4415:tid 23402119136832] [client 10.26.163.58:52145] AH01964: Connection to child 263 established (server
10.83.84.244:443)
Apr 09 2024 12:23:28 fmcv-741 SF-IMS[4715]: [4715] pm:control [INFO] ControlHandler auditing message: ProcessHealthPurge, socket 14, user '', cmd '/usr/bin/perl /usr/local/sf/bin/run_hm.pl --
persistent', pid 5715 (uid 0, gid 0)
Apr 09 2024 12:23:25 fmcv-741 SF-IMS[9177]: [9177] CloudAgent:CloudAgent [INFO] IPRep, time to check for updates
Apr 09 2024 12:22:47 fmcv-741 [Tue Apr 09 16:22:46.775613 2024] [ssl:info] [pid 5607:tid 23402133837376] [client 10.26.163.58:52136] AH01964: Connection to child 130 established (server
10.83.84.244:443)
Apr 09 2024 12:22:47 fmcv-741 [Tue Apr 09 16:22:46.775222 2024] [ssl:info] [pid 5605:tid 23402110723648] [client 10.26.163.58:52135] AH01964: Connection to child 13 established (server
10.83.84.244:443)
Apr 09 2024 12:22:47 fmcv-741 [Tue Apr 09 16:22:46.725914 2024] [ssl:info] [pid 7019:tid 23402106529344] [client 10.26.163.58:52134] AH01998: Connection closed to child 205 with abortive
shutdown (server 10.83.84.244:443)
```

9.2 FTD Audit Messages

The audit events generated on FTD include log messages related to firewall and VPN activity. These messages can be configured to be transmitted directly from FTD to a remote syslog server (over UDP syslog, TCP syslog, or syslog-over TLS), and/or these messages can be transmitted to FMC for centralized storage and review. The log messages generated by FTD are in standard syslog format regardless of whether they're transmitted to a syslog server or to FMC.

To configure logging on FTD, refer to section 5.8 of this document.

To review audit messages transmitted to FMC from FTD, refer to the "System Log" in section 9.1 of this document.