Configuring FDM-Managed Devices

- Schedule a Security Database Update, on page 350
- Update FDM-Managed Device Security Databases, on page 351

Interfaces

You can use Cisco Defense Orchestrator (CDO) to configure and edit data interfaces or the management/diagnostic interface on an FDM-managed device.

At this time, CDO can only configure routed interfaces and bridge groups. It does not support the configuration passive interfaces.

Guidelines and Limitations for Firepower Interface Configuration

When you use Cisco Defense Orchestrator (CDO) to configure the device, there are several limitations to interface configuration. If you need any of the following features, you must use Firepower Management Center to configure the device.

Firewall

- Routed firewall mode only is supported. You cannot configure transparent firewall mode interfaces.
- Only physical firepower 1010 devices support interfaces configured for switch port mode. See Switch Port Mode Interfaces for an FDM-Managed Device for more information.

Passive

- At this time, Cisco Defense Orchestrator (CDO) does not identify passive interface mode in the interface table ad you cannot configure passive or ERSPAN interfaces. You must use the FDM-managed UI to configure and identify passive interfaces.

IPS-Only Mode

- You cannot configure interfaces to be inline (in an inline set), or inline tap, for IPS-only processing. IPS-only mode interfaces bypass many firewall checks and only support IPS security policy. In comparison, Firewall mode interfaces subject traffic to firewall functions such as maintaining flows, tracking flow states at both IP and TCP layers, IP defragmentation, and TCP normalization.
- Optionally, you can configure IPS functions for this firewall mode traffic according to your security policy.

EtherChannel

CDO supports read, create, and abilities for devices running Version 6.5 and later. To create Etherchannel interfaces, see Add an EtherChannel Interface for an FDM-Managed Device for more information. To create

- You can configure up to 48 EtherChannels on physical Firepower devices, although how many interfaces can be active at a time depends on your device model. For device-specific limitations, see Device-Specific Limitations.
- All interfaces in the channel group must be the same media type and capacity, and must be set to the same speed and duplex. The media type can be either RJ-45 or SFP; SFPs of different types (copper and

fiber) can be mixed. You cannot mix interface capacities (for example 1GB and 10GB interfaces) by setting the speed to be lower on the larger-capacity interface.

- The device to which you connect the EtherChannel must also support 802.3ad EtherChannels.
- The FDM-managed device does not support LACPDUs that are VLAN-tagged. If you enable native VLAN tagging on the neighboring switch using the Cisco IOS vlan dot1Q tag native command, then the FDM-managed device will drop the tagged LACPDUs. Be sure to disable native VLAN tagging on the neighboring switch.
- All FDM-managed device configuration refers to the logical EtherChannel interface instead of the member physical interfaces.

Note Interfaces set up as portchannels can only use physical interfaces, redundant interfaces, and subinterfaces are supported as bridge group member interfaces.

Bridge Groups

At this time, CDO supports the configuration of one bridge group. To determine if your device supports bridge groups, see Bridge Group Compatibility in FDM-Managed Configurations for more information.

When adding an interface to a bridge group, keep the following in mind:

- The interface must have a name.
- The interface cannot have any IPv4 or IPv6 addresses defined for it, either static or served through DHCP.
- BVI can have either VLAN interfaces or other routed interfaces as a member interface, but you cannot have both as member interfaces on a single BVI.
- BVI can have either VLAN interfaces or other routed interfaces as a member interface, but you cannot have both as member interfaces on a single BVI.
- The interface cannot be Point-to-Point Protocol over Ethernet (PPPoE)
- The interface cannot be associated with a security zone (if it is in a zone). You must delete any NAT rules for the interface before you can add it to a bridge group.
- Enable and disable the member interfaces individually. Thus, you can disable any unused interfaces without needing to remove them from the bridge group. The bridge group itself is always enabled.
- You can configure the interfaces that will be ***members*** of the bridge group. See Configure a Bridge Group for interface requirements and creation.

Point-to-Point Protocol over Ethernet

- You cannot configure Point-to-Point Protocol over Ethernet (PPPoE) for IPv4. If the Internet interface is connected to a DSL, cable modem, or other connection to your ISP, and your ISP uses PPPoE to provide your IP address, you must use the FDM to configure these settings.

VLAN

To configure VLAN interfaces and VLAN members, see Configure an FDM-Managed Device VLAN for more information. To configure VLAN for switch port mode, see Configure an FDM-Managed Device VLAN for Switch Port Mode for more information.

- The interface must be physical.
- The interface cannot be management-only.
- The interface cannot be associated as any other type of interface, including BVI, subinterfaces, another VLAN interface, EtherChannel, etc.
- The interface cannot be a BVI member or an etherchannel member.
- Device models support varying numbers of VLAN members. See Maximum Number of VLAN Members by Device Model for more information.

Note To configure VLAN for your environment, see Configure Firepower VLAN Subinterfaces and 802.1Q Trunking for more information.

Network Module Cards

Optional network module installations are limited to the ASA 5515-X, 5525-X, 5545-X, and 5555-X, and the Firepower 2100 series devices.

- Cards are only discovered during bootstrap (that is, initial installation or reimage, or when switching between local/remove management). CDO sets the correct defaults for speed and duplex for these interfaces. If you replace an optional card with one that changes the speed/duplex options for the interfaces, without changing the total number of interfaces available, reboot the device so that the system recognizes the correct speed/duplex values for the replaced interfaces. From an SSH or Console session with the device, enter the reboot command. Then, using CDO, edit each physical interface that had capability changes and select valid speed and duplex options, as the system does not automatically correct your original settings. Deploy your changes right away to ensure correct system behavior.
- You cannot enable or disable network modules or perform breakout online insertion and removal (OIR) of interfaces on FDM-managed Secure Firewall 3100 series devices.

Note Replacing a card with one that changes the total number of interfaces, or removing interfaces that were referred to by other objects, can result in unexpected problems. If you need to make this kind of change, please first remove all references to the interfaces you will remove, such as security zone membership, VPN connections, and so forth. We also suggest you do a backup prior to making the change.

Interfaces on Virtual FDM-Managed Devices

- You cannot add or remove interfaces without reinitializing a virtual FDM-managed device. You must execute these actions in an FDM-managed device.

Note If you replace interfaces with ones that have different speed/duplex capabilities, reboot the device so that the system recognizes the new speed/duplex values with the following procedure: from the device's CLI console, enter the reboot command. Then, in CDO, edit each interface that had capability changes and select valid speed and duplex options, as the system does not automatically correct your original settings. Deploy your changes right away to ensure correct system behavior.

Maximum Number of VLAN Members by Device Model

The device model limits the maximum number of VLAN subinterfaces that you can configure. Note that you can configure subinterfaces on data interfaces only, you cannot configure them on the management interface. The following table explains the limits for each device model.

Model	Maximum VLAN Subinterfaces
Firepower 1010	60
Firepower 1120	512
Firepower 1140, Firepower 1150	1024
Firepower 2100	1024
Secure Firewall 3100	1024
Firepower 4100	1024
Firepower 9300	1024
ASA 5508-X	50
ASA 5515-X	100
ASA 5516-X	100
ASA 5525-X	200
ASA 5545-X	300
ASA 5555-X	500
ISA 3000	100

Firepower Data Interfaces

Cisco Defense Orchestrator (CDO) supports configuring routed interfaces and bridge virtual interfaces on FDM-managed devices.

Routed Interfaces

Each Layer 3 routed interface (or subinterface) requires an IP address on a unique subnet. You would typically attach these interfaces to switches, a port on another router, or to an ISP/WAN gateway.

You can assign a static address, or you can obtain one from a DHCP server. However, if the DHCP server provides an address on the same subnet as a statically-defined interface on the device, the system will disable the DHCP interface. If an interface that uses DHCP to get an address stops passing traffic, check whether the address overlaps the subnet for another interface on the device.

You can configure both IPv6 and IPv4 addresses on a routed interface. Make sure you configure a default route for both IPv4 and IPv6. This task will need to be performed on the FDM-managed device using Firepower Device Manager. See "Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager, Version x.x.x", **The Basics > Routing** for information about configuring a default route.

Bridge Groups and Bridge Virtual Interfaces

A bridge group is a group of interfaces that the FDM-managed device bridges instead of routes. Bridged interfaces belong to a bridge group, and all interfaces are on the same network. The bridge group is represented by a Bridge Virtual Interface (BVI) that has an IP address on the bridge network. Interfaces included in the bridge group are called "members."

You can route between routed interfaces and BVIs, if you name the BVI. In this case, the BVI acts as the gateway between member interfaces and routed interfaces. If you do not name the BVI, traffic on the bridge group member interfaces cannot leave the bridge group. Normally, you would name the interface so that you can route member interfaces to the Internet.

FDM-managed devices only support one bridge group, therefore, CDO can only manage that one bridge group and cannot create additional bridge groups on the device. CDO can only manage BVIs on FDM-managed devices installed directly on hardware, not on virtual FDM-managed device instances.

One use for a bridge group in routed mode is to use extra interfaces on the FDM-managed device instead of an external switch. You can attach endpoints directly to bridge group member interfaces. You can also attach switches to add more endpoints to the same network as the BVI.

Passive Interfaces

Passive interfaces monitor traffic flowing across a network using a switch SPAN (Switched Port Analyzer) or mirror port. The SPAN or mirror port allows for traffic to be copied from other ports on the switch. This function provides the system visibility within the network without being in the flow of network traffic. When configured in a passive deployment, the system cannot take certain actions such as blocking or shaping traffic. Passive interfaces receive all traffic unconditionally and no traffic received on these interfaces is retransmitted.

At this time, CDO has limited support for managing passive interfaces on the FDM-managed device:

- Passive interfaces must be configured on the FDM-managed device.
- Routed interfaces cannot be changed to passive interfaces and passives interfaces cannot be changed to routed interfaces using CDO.
- CDO does not identify passive interfaces in the interface table.

Related Information:

- IPv6 Addressing for Firepower Interfaces
- Guidelines and Limitations for Firepower Interface Configuration

- Configure a Physical Firepower Interface

Management/Diagnostic Interface

The physical port labeled Management (or for FDM-managed device virtual, the Management 0/0 virtual interface) actually has two separate interfaces associated with it.

- **Management virtual interface**-This IP address is used for system communication. This is the address the system uses for Smart Licensing and to retrieve database updates. You can open management sessions to it (Firepower Device Manager and CLI). You must configure a management address, which is defined on **System Settings** > **Management Interface**.
- **Diagnostic physical interface**-The physical Management port is actually named Diagnostic. You can use this interface to send syslog messages to an external syslog server. Configuring an IP address for the Diagnostic physical interface is optional. The only reason to configure the interface is if you want to use it for syslog. This interface appears, and is configurable, on the **Inventory** > **Interfaces** page. The Diagnostic physical interface only allows management traffic, and does not allow through traffic.

(Hardware devices.) The recommended way to configure Management/Diagnostic is to not wire the physical port to a network. Instead, configure the Management IP address only, and configure it to use the data interfaces as the gateway for obtaining updates from the Internet. Then, open the inside interfaces to HTTPS/SSH traffic (by default, HTTPS is enabled) and open Firepower Device Manager using the inside IP address. This task you must perform on Firepower Device Manager directly. See "Configuring the Management Access List" in the Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager for instructions.

For FDM-managed device virtual, the recommended configuration is to attach Management0/0 to the same network as the inside interface, and use the inside interface as the gateway. Do not configure a separate address for Diagnostic.

Note **For special instructions on how to edit the Management interface see** Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager for Firepower version 6.4 or higher. Open the guide and navigate to **The Basic** > **Interfaces** > **Management/Diagnostic Interface**. Management interface configuration should be done on the Firepower Device Manager.

Interface Settings

Use these topics to configure interface settings.

Use of Security Zones in Firepower Interface Settings

Each interface can be assigned to a single security zone. You then apply your security policy based on zones. For example, you can assign the inside interface to the inside zone; and the outside interface to the outside zone. You can configure your access control policy to enable traffic to go from inside to outside, but not from outside to inside, for example.

Each zone has a mode, either routed or passive. This relates directly to the interface mode. You can add routed and passive interfaces only to the same mode security zone.

Bridge Virtual Interfaces (BVIs) are not added to security zones. Only member interfaces are added to security zones.

You do not include the Diagnostic or Management interface in a zone. Zones apply to data interfaces only.

CDO does not currently support the management, monitoring, or use of Virtual Tunnel Interface (VTI) tunnels on ASA or FDM-managed devices. Devices with configured VTI tunnels can be onboarded to CDO but it ignores VTI interfaces. If a security zone or static route references a VTI, CDO reads the security zone and static route without the VTI reference. CDO support for VTI tunnels is coming soon.

See Security Zone Object for more information about security zones.

Assign an FDM-Managed Device Interface to a Security Zone

Before you Begin

An interface has the following limitations when adding a security zone:

- The interface must have a name.
- The interface cannot be management-only. This option is enabled and disabled from the Advanced tab of the interface.
- You cannot assign a security zone to a bridge group interface.
- You cannot assign a security zone to an interface configured for switchport mode.
- CDO does not currently support the management, monitoring, or use of Virtual Tunnel Interface (VTI) tunnels on ASA or FDM-managed devices. Devices with configured VTI tunnels can be onboarded to CDO but it ignores VTI interfaces. If a security zone or static route references a VTI, CDO reads the security zone and static route without the VTI reference. CDO support for VTI tunnels is coming soon.

Assign a Firepower Interface to a Security Zone

Use the following procedure to associate a security zone to an existing interface:

Procedure

Step 1 Log into CDO.

Step 2 In the navigation pane, click **Inventory**.

Step 3 Click the **Devices** tab to locate the device or the **Templates** tab to locate the model device.

Step 4 Click the **FTD** device and select the FDM-managed device you want to modify.

Step 5 In the **Management** pane located to the right, click **Interfaces**.

Step 6 Select the interface you want to add a security zone to and click **Edit**.

Step 7 Use the **Security Zone** drop-down menu and select the security zone you want associated with this interface.

Note If need to, ceate a new security zone from this drop-down menu by clicking **Create New**.

Step 8 Click **Save**.

Step 9 Deploy Configuration Changes from CDO to FDM-Managed Device.

Related Information:

- Security Zone Object

- Create or Edit a Firepower Security Zone Object
- Guidelines and Limitations for Firepower Interface Configuration

Use of Auto-MDI/MDX in Firepower Interface Settings

For RJ-45 interfaces, the default auto-negotiation setting also includes the Auto-MDI/MDIX feature. Auto-MDI/MDIX eliminates the need for crossover cabling by performing an internal crossover when a straight cable is detected during the auto-negotiation phase. Either the speed or duplex must be set to auto-negotiate to enable Auto-MDI/MDIX for the interface. If you explicitly set both the speed and duplex to a fixed value, thus disabling auto-negotiation for both settings, then Auto-MDI/MDIX is also disabled. For Gigabit Ethernet, when the speed and duplex are set to 1000 and full, then the interface always auto-negotiates; therefore Auto-MDI/MDIX is always enabled and you cannot disable it.

These settings are configured on the Advanced tab when editing an interface.

Use of MAC Addresses in Firepower Interface Settings

You can manually configure Media Access Control (MAC) addresses to override the default value.

For a high availability configuration, you can configure both the active and standby MAC address for an interface. If the active unit fails over and the standby unit becomes active, the new active unit starts using the active MAC addresses to minimize network disruption.

Active and standby MAC addresses are configured on the Advanced tab when configuring an interface.

Default MAC Addresses

Default MAC address assignments depend on the type of interface.

- **Physical interfaces** - The physical interface uses the burned-in MAC address.
- **Subinterfaces** - All subinterfaces of a physical interface use the same burned-in MAC address. You might want to assign unique MAC addresses to subinterfaces. For example, your service provider might perform access control based on the MAC address. Also, because IPv6 link-local addresses are generated based on the MAC address, assigning unique MAC addresses to subinterfaces allows for unique IPv6 link-local addresses.

Use of MTU Settings in Firepower Interface Settings

About the MTU

The MTU specifies the maximum frame payload size that the FDM-managed device can transmit on a given Ethernet interface. The MTU value is the frame size without Ethernet headers, VLAN tagging, or other overhead. For example, when you set the MTU to 1500, the expected frame size is 1518 bytes including the headers, or 1522 when using VLAN. Do not set the MTU value higher to accommodate these headers.

Path MTU Discovery

The FDM-managed device supports Path MTU Discovery (as defined in RFC 1191), which lets all devices in a network path between two hosts coordinate the MTU so they can standardize on the lowest MTU in the path.

MTU and Fragmentation

For IPv4, if an outgoing IP packet is larger than the specified MTU, it is fragmented into 2 or more frames. Fragments are reassembled at the destination (and sometimes at intermediate hops), and fragmentation can cause performance degradation. For IPv6, packets are typically not allowed to be fragmented at all. Therefore, your IP packets should fit within the MTU size to avoid fragmentation.

For UDP or ICMP, the application should take the MTU into account to avoid fragmentation.

Note The FDM-managed device can receive frames larger than the configured MTU as long as there is room in memory.

MTU and Jumbo Frames

A larger MTU lets you send larger packets. Larger packets might be more efficient for your network. See the following guidelines:

- Matching MTUs on the traffic path: We recommend that you set the MTU on all FDM-managed device interfaces and other device interfaces along the traffic path to be the same. Matching MTUs prevents intermediate devices from fragmenting the packets.
- Accommodating jumbo frames: A jumbo frame is an Ethernet packet larger than the standard maximum of 1522 bytes (including Layer 2 header and VLAN header), up to 9216 bytes. You can set the MTU up to 9198 bytes to accommodate jumbo frames. The maximum is 9000 for FDM-managed virtual.

Note Increasing the MTU assigns more memory for jumbo frames, which might limit the maximum usage of other features, such as access rules. If you increase the MTU above the default 1500 on ASA 5500-X series devices or FDM-managed virtual, you must reboot the system. You do not need to reboot Firepower 2100 series devices, where jumbo frame support is always enabled.

Jumbo frame support is enabled by default on Firepower 3100 devices.

IPv6 Addressing for Firepower Interfaces

You can configure two types of unicast IPv6 addresses for Firepower physical interfaces.

- **Global**—The global address is a public address that you can use on the public network. For a bridge group, you configure the global address on the Bridge Virtual Interface (BVI), not on each member interface. You cannot specify any of the following as a global address.
  - Internally reserved IPv6 addresses: fd00::/56 (from=fd00:: to= fd00:0000:0000:00ff:ffff:ffff:ffff:ffff)
  - An unspecified address, such as ::/128
  - The loopback address, ::1/128
  - Multicast addresses, ff00::/8
  - Link-local addresses, fe80::/10

- **Link-local**—The link-local address is a private address that you can only use on the directly-connected network. Routers do not forward packets using link-local addresses; they are only for communication on a particular physical network segment. They can be used for address configuration or for the Network Discovery functions such as address resolution and neighbor discovery. Each interface must have its own address because the link-local address is only available on a segment, and is tied to the interface MAC address.

At a minimum, you need to configure a link-local address for IPv6 to operate. If you configure a global address, a link-local address is automatically configured on the interface, so you do not also need to specifically configure a link-local address. If you do not configure a global address, then you need to configure the link-local address, either automatically or manually.

Configuring Firepower Interfaces

When you attach a cable to an interface connection (physically or virtually), you need to configure the interface. At minimum, you need to name the interface and enable it for traffic to pass through it. If the interface is a member of a bridge group, naming the interface is sufficient. If the interface is a bridge virtual interface (BVI), you need to assign the BVI an IP address. If you intend to create VLAN subinterfaces rather than a single physical interface on a given port, you would typically configure the IP addresses on the subinterface, not on the physical interface. VLAN subinterfaces let you divide a physical interface into multiple logical interfaces that are tagged with different VLAN IDs.

The interface list shows the available interfaces, their names, addresses, and states. You can change the state of an interface, on or off, or edit an interface, by selecting the interface row and clicking **Edit** in the Actions pane. The list shows the interface characteristics based on your configuration. Expand an interface row to see subinterfaces or bridge group member.

Related Information:

- Interfaces
- Configure a Physical Firepower Interface
- Configure Advanced Firepower Interface Options, on page 18
- Configure Firepower VLAN Subinterfaces and 802.1Q Trunking
- Configure an FDM-Managed Device VLAN for Switch Port Mode

Configure a Physical Firepower Interface

At a minimum, you must enable a physical interface to use it. You would also typically name it and configure IP addressing; however, you would not configure IP addressing if you intend to create VLAN subinterfaces, if you are configuring a passive mode interface, or if you intend to add the interface to a bridge group.

Note You cannot configure IP addresses on bridge group member interfaces or passive interfaces, although you can modify advanced settings, that are not related to IPv6 addressing.

You can disable an interface to temporarily prevent transmission on the connected network. You do not need to remove the interface's configuration. At this time, Cisco Defense Orchestrator (CDO) can only configure

routed interfaces and bridge groups. CDO lists passive interfaces but you cannot reconfigure them as active interfaces from CDO.

Note **Note**: CDO does not support Point-to-Point Protocol over Ethernet (PPPoE) configurations for IPv4. Configuring this option in an FDM-managed devicemay cause isses in the CDO UI; if you **must** configure PPPoE for your device, you must make the appropriate changes in an FDM-managed device.

Procedure

Procedure

Step 1 On the **Inventory** page, click the device whose interfaces you want to configure and click **Interfaces** in the Management pane on the right.

Step 2 On the Interfaces page, select the physical interface you want to configure.

Step 3 In the Actions pane on the right, click **Edit**.

Step 4 Give the physical interface a **Logical Name** and, optionally, a **Description**. Unless you configure subinterfaces, the interface should have a name.

Note If you change the name, the change is automatically reflected everywhere you used the old name, including security zones, syslog server objects, and DHCP server definitions. However, you cannot remove the name until you first remove all configurations that use the name, because you typically cannot use an unnamed interface for any policy or setting.

Step 5 Pick one of these options:

- If you intend to add sub-interfaces:

If you intend to configure subinterfaces for this physical interface, you are probably done. Click **Save** and continue with Configure Firepower VLAN Subinterfaces and 802.1Q Trunking ; otherwise, continue.

Note Even when configuring subinterfaces, it is valid to name the interface and supply IP addresses. This is not the typical setup, but if you know that is what you need, you can configure it.

- If you do not intend to add a sub-interface, continue with either or both, Configure IPv4 Addressing for the Physical Interface and Configure IPv6 Addressing for the Physical Interface.

Configure IPv4 Addressing for the Physical Interface

Warning After you configure and save a DHCP address pool, the DHCP address pool is bound to the interface's configured IP address(es). If you edit the interface's subnet mask after you configure a DHCP address pool, deployments to the FDM-managed device fail. Also, if you edit the DHCP address pool in the FDM-managed console and read the configuration from an FDM-managed device to Cisco Defense Orchestrator, the read fails.

Procedure

Step 1 In the "Editing Physical Interface" dialog, click the **IPv4 Address** tab.

Step 2 Select one of the following options from the Type field:

- **Static**-Choose this option if you want to assign an address that should not change. Enter in the interface's IP address and the subnet mask for the network attached to the interface. For example, if you attach the 10.100.10.0/24 network, you could enter 10.100.10.1/24. Ensure that the address you enter is not the network ID or the broadcast address for the network and the address is not already used on the network.
  - **Standby IP Address and Subnet Mask -** If you configured high availability, and you are monitoring this interface for HA, also configure a standby IP address on the same subnet. The standby address is used by this interface on the standby device. If you do not set the standby IP address, the active unit cannot monitor the standby interface using network tests; it can only track the link state.
  - **(Optional) DHCP Address Pool** - Enter a a single DHCP Server IP address, or an IP address range. The range of IP addresses must be on the same subnet as the selected interface and cannot include: the IP address of the interface itself, the broadcast address, or the subnet network address. Specify the start and end address for the pool, separated by a hyphen. To temporarily disable this DHCP server, edit the server in the **DHCP Servers** section of the Configure DHCP Servers page.
- **Dynamic (DHCP)**-Choose this option if the address should be obtained from the DHCP server on the network. Change the following options if necessary:
  - **Obtain Default Route**-Whether to get the default route from the DHCP server. You would normally check this option.
  - **DHCP Route Metric**-If you obtain the default route from the DHCP server, enter the administrative distance to the learned route, between 1 and 255.

    Note If there is a DHCP server configured for the interface, you are shown the configuration. You can edit or delete the DHCP address pool. If you change the interface IP address to a different subnet, you must either delete the DHCP server, or configure an address pool on the new subnet, before you can save the interface changes.

Step 3 Click **Save** if you are done or continue with one of these procedures:

- Configure IPv6 Addressing for the Physical Interface if you intend to assign an IPv6 address to this interface as well as an IPv4 address.
- Configure Advanced Firepower Interface Options, on page 18. The advanced settings have defaults that are appropriate for most networks. Edit them only if you are resolving network issues.
- If you saved the interface, and you don't want to continue advanced interface options, continue to Enable the Physical Interface.

Configure IPv6 Addressing for the Physical Interface

Procedure

Step 1 In the "Editing Physical Interface" dialog, click the IPv6 Address tab.

Step 2 **State**-To enable IPv6 processing and to automatically configure the link-local address when you do not configure the global address, click the **State** slider to enable it. The link-local address is generated based on the interface MAC addresses (Modified EUI-64 format).

Note Disabling IPv6 does not disable IPv6 processing on an interface that is configured with an explicit IPv6 address or that is enabled for auto configuration.

Step 3 **Address Auto Configuration**-Check this option to have the address automatically configured. IPv6 stateless autoconfiguration will generate a global IPv6 address only if the link on which the device resides has a router configured to provide IPv6 services, including the advertisement of an IPv6 global prefix for use on the link. If IPv6 routing services are not available on the link, you will get a link-local IPv6 address only, which you cannot access outside of the device's immediate network link. The link local address is based on the Modified EUI-64 interface ID.

Although RFC 4862 specifies that hosts configured for stateless autoconfiguration do not send Router Advertisement messages, the FDM-managed device does send Router Advertisement messages in this case. Select **Suppress RA** to suppress messages and conform to the RFC.

Step 4 **Suppress RA**-Check this box if you want to suppress router advertisements. The Firepower Threat Defense device can participate in router advertisements so that neighboring devices can dynamically learn a default router address. By default, router advertisement messages (ICMPv6 Type 134) are periodically sent out each IPv6 configured interface.

Router advertisements are also sent in response to router solicitation messages (ICMPv6 Type 133). Router solicitation messages are sent by hosts at system startup so that the host can immediately autoconfigure without needing to wait for the next scheduled router advertisement message.

You might want to suppress these messages on any interface for which you do not want the Firepower Threat Defense device to supply the IPv6 prefix (for example, the outside interface).

Step 5 **Link-Local Address**-If you want to use the address as link local only, enter it in the Link-Local Address field. Link local addresses are not accessible outside the local network. You cannot configure a link-local address on a bridge group interface.

Note A link-local address should start with FE8, FE9, FEA, or FEB, for example fe80::20d:88ff:feee:6a82. Note that we recommend automatically assigning the link-local address based on the Modified EUI-64 format. For example, if other devices enforce the use of the Modified EUI-64 format, then a manually-assigned link-local address may cause packets to be dropped.

Step 6 **Standby Link-Local Address**-Configure this address if the interface connects a high availability pair of devices. Enter the link-local address of the interface on the other FDM-managed device, to which this interfaces is connected.

Step 7 **Static Address/Prefix**â€”If you do not use stateless autoconfiguration, enter the full static global IPv6 address and network prefix. For example, 2001:0DB8::BA98:0:3210/48. For more information on IPv6 addressing, see IPv6 Addressing for Firepower Interfaces.

Step 8 **Standby IP Address**-If you configure high availability, and you are monitoring this interface for HA, also configure a standby IPv6 address on the same subnet. The standby address is used by this interface on the standby device. If you do not set the standby IP address, the active unit cannot monitor the standby interface using network tests; it can only track the link state.

Step 9 Click **Save** if you are done or continue with one of these procedures:

- Configure Advanced Firepower Interface Options, on page 18. The advanced settings have defaults that are appropriate for most networks. Edit them only if you are resolving network issues.
- If you saved the interface, and you don't want to continue advanced interface options, continue to Enable the Physical Interface.

Enable the Physical Interface

Procedure

Step 1 Select the interface you want to enable.

Step 2 Slide the **State** slider at the top right of the window, associated with the interface's logical name to blue.

Step 3 Preview and Deploy Configuration Changes for All Devices now the changes you made, or wait and deploy multiple changes at once.

Configure Firepower VLAN Subinterfaces and 802.1Q Trunking

VLAN subinterfaces let you divide a physical interface into multiple logical interfaces that are tagged with different VLAN IDs. An interface with one or more VLAN subinterfaces is automatically configured as an 802.1Q trunk. Because VLANs allow you to keep traffic separate on a given physical interface, you can increase the number of interfaces available to your network without adding additional physical interfaces or devices.

Create subinterfaces if you attach the physical interface to a trunk port on a switch. Create a subinterface for each VLAN that can appear on the switch trunk port. If you attach the physical interface to an access port on the switch, there is no point in creating a subinterface.

Note You cannot configure IP addresses on bridge group member interfaces, although you can modify advanced settings as needed.

Before You Begin

Prevent untagged packets on the physical interface. If you use subinterfaces, you typically do not also want the physical interface to pass traffic, because the physical interface passes untagged packets. Because the physical interface must be enabled for the subinterface to pass traffic, ensure that the physical interface does not pass traffic by not naming the interface. If you want to let the physical interface pass untagged packets, you can name the interface as usual.

Procedure

Procedure

Step 1 In the navigation pane, click **Inventory**.

Step 2 Click the **Devices** tab to locate the device or the **Templates** tab to locate the model device.

Step 3 Click the **FTD** tab and click the device whose interfaces you want to configure.

Step 4 Click **Interfaces** in the **Management** pane at the right.

Step 5 On the Interfaces page, select the physical interface you want to configure and in the Actions pane at the right, click **+ New Subinterface**.

Notice that the **Parent Interface** field shows the name of the physical interface for which you are creating this subinterface. You cannot change the parent interface after you create the subinterface.

Step 6 Give the subinterface a **logical name** and, optionally, a **description**. Without a logical name, the rest of the interface configuration is ignored.

Note If you change the name, the change is automatically reflected everywhere you used the old name, including security zones, syslog server objects, and DHCP server definitions. However, you cannot remove the name until you first remove all configurations that use the name, because you typically cannot use an unnamed interface for any policy or setting.

Step 7 Configure the VLAN ID and Subinterface ID:

- **VLAN ID** - Enter a VLAN ID between 1 and 4094 that will be used to tag the packets on this subinterface.
- **Subinterface ID** - Enter the subinterface ID as an integer between 1 and 4294967295. The number of subinterfaces allowed Maximum Number of VLAN Members by Device Model. You cannot change the subinterace ID after you create the subinterface.

Continue with Configure IPv4 Addressing for the Subinterface and Configure IPv6 Addressing for the Subinterface .

Configure IPv4 Addressing for the Subinterface

Procedure

Step 1 In the "Adding Subinterface" dialog, click the **IPv4 Address** tab.

Step 2 Select one of the following options from the Type field:

- **Static**-Choose this option if you want to assign an address that should not change.

  Enter in the interface's **IP address and the subnet mask** for the network attached to the interface. For example, if you attach the 10.100.10.0/24 network, you could enter 10.100.10.1/24. Ensure that the address you enter is not the network ID or the broadcast address for the network and the address is not already used on the network.

- Enter a **Standby IP Address** and Subnet Mask only if this interface is being used in a high availability pair of devices.

- **Dynamic (DHCP)**-Choose this option if the address should be obtained from the DHCP server on the network. Change the following options if necessary:
  - **Obtain Default Route**-Whether to get the default route from the DHCP server. You would normally check this option.
  - **DHCP Route Metric**-If you obtain the default route from the DHCP server, enter the administrative distance to the learned route, between 1 and 255.

    See Configure DHCP Servers.

    Note If there is a DHCP server configured for the interface, you are shown the configuration. You can edit or delete the DHCP address pool. If you change the interface IP address to a different subnet, you must either delete the DHCP server, or configure an address pool on the new subnet, before you can save the interface changes.

Step 3 Click **Create** if you are done or continue with one of these procedures:

- Continue to "Configure IPv6 Addressing for the Physical Interface" if you want to assign an IPv6 address to this interface as well as an IPv4 address.
- Configure Advanced Firepower Interface Options, on page 18. The advanced settings have defaults that are appropriate for most networks. Edit them only if you are resolving network issues.
- If you created the subinterface, go to Enable the Physical Interface .

Configure IPv6 Addressing for the Subinterface

Procedure

Step 1 Click the IPv6 Address tab.

Step 2 **Enable IPv6 processing**-To enable IPv6 processing and to automatically configure the link-local address when you do not configure the global address, move the **State** slider to blue. The link-local address is generated based on the interface MAC addresses (Modified EUI-64 format).

Note Disabling IPv6 does not disable IPv6 processing on an interface that is configured with an explicit IPv6 address or that is enabled for auto configuration.

Step 3 **Address Auto Configuration**-Check this option to have the address automatically configured. IPv6 stateless auto configuration will generate a global IPv6 address only if the link on which the device resides has a router configured to provide IPv6 services, including the advertisement of an IPv6 global prefix for use on the link. If IPv6 routing services are not available on the link, you will get a link-local IPv6 address only, which you cannot access outside of the device's immediate network link. The link local address is based on the Modified EUI-64 interface ID.

Step 4 **Suppress RA**-Check this box if you want to suppress router advertisements. The Firepower Threat Defense device can participate in router advertisements so that neighboring devices can dynamically learn a default router address. By default, router advertisement messages (ICMPv6 Type 134) are periodically sent out each IPv6 configured interface.

Router advertisements are also sent in response to router solicitation messages (ICMPv6 Type 133). Router solicitation messages are sent by hosts at system startup so that the host can immediately autoconfigure without needing to wait for the next scheduled router advertisement message.

You might want to suppress these messages on any interface for which you do not want the Firepower Threat Defense device to supply the IPv6 prefix (for example, the outside interface).

Step 5 **Link-Local Address**-If you want to use the address as link local only, enter it in the Link-Local Address field. Link local addresses are not accessible outside the local network.

Note A link-local address should start with FE8, FE9, FEA, or FEB, for example fe80::20d:88ff:feee:6a82. Note that we recommend automatically assigning the link-local address based on the Modified EUI-64 format. For example, if other devices enforce the use of the Modified EUI-64 format, then a manually-assigned link-local address may cause packets to be dropped.

Step 6 **Standby Link-Local Address**-Configure this address if your interface connects a high availability pair of devices.

Step 7 **Static Address/Prefix**-If you do not use stateless autoconfiguration, enter the full static global IPv6 address and network prefix. For example, 2001:0DB8::BA98:0:3210/48. For more information on IPv6 addressing, see IPv6 Addressing, on page 136.

Step 8 **Standby IP Address**-If you configure high availability, and you are monitoring this interface for HA, also configure a standby IPv6 address on the same subnet. The standby address is used by this interface on the standby device. If you do not set the standby IP address, the active unit cannot monitor the standby interface using network tests; it can only track the link state.

Step 9 Click **Create** if you are done or continue with one of these procedures:

- Click the Advanced tab to Configure Advanced Firepower Interface Options, on page 18. The advanced settings have defaults that are appropriate for most networks. Edit them only if you are resolving network issues.
- If you created the subinterface, go to Enable the Physical Interface .

Enable the Physical Interface

Procedure

Step 1 To enable the subinterface, slide the State slider, associated with the subinterface's logical name to blue.

Step 2 Preview and Deploy Configuration Changes for All Devices now the changes you made, or wait and deploy multiple changes at once.

Configure Advanced Firepower Interface Options

Advanced interface options have default settings that are appropriate for most networks. Configure them only if you are resolving networking problems.

The following procedure assumes the interface is already defined. You can also edit these settings while initially editing or creating the interface.

This procedure and all of the steps in it are optional.

Limitations:

- You cannot set MTU, duplex, or speed for the Management interface on a Firepower 2100 series device.
- The MTU of an unnamed interface **must** be set to 1500 bytes.

Procedure

Step 1 In the navigation pane, click **Inventory**.

Step 2 Click the **Devices** tab to locate the device or the **Templates** tab to locate the model device.

Step 3 Click the **FTD** tab and click the device whose interfaces you want to configure.

Step 4 Click **Interfaces** in the **Management** pane at the right.

Step 5 On the Interfaces page, select the physical interface you want to configure and in the Actions pane at the right, click **Edit**.

Step 6 Click the **Advanced** tab.

Step 7 **Enable for HA Monitoring** is automatically enabled. When this is enabled, the device includes the health of the interface as a factor when the HA pair decides whether to fail over to the peer unit in a high availability configuration. This option is ignored if you do not configure high availability. It is also ignored if you do not configure a name for the interface.

Step 8 To make a data interface management only, check **Management Only**.

A management only interface does not allow through traffic, so there is very little value in setting a data interface as a **management only** interface. You cannot change this setting for the Management/Diagnostic interface, which is always management only.

Step 9 Modify the IPv6 DHCP configuration settings.

- **Enable DHCP for IPv6 address configuration** - Whether to set the Managed Address Configuration flag in the IPv6 router advertisement packet. This flag informs IPv6 autoconfiguration clients that they should use DHCPv6 to obtain addresses, in addition to the derived stateless autoconfiguration address.
- **Enable DHCP for IPv6 non-address configuration** - Whether to set the Other Address Configuration flag in the IPv6 router advertisement packet. This flag informs IPv6 autoconfiguration clients that they should use DHCPv6 to obtain additional information from DHCPv6, such as the DNS server address.

Step 10 Configure **DAD Attempts** - How often the interface performs Duplicate Address Detection (DAD), from 0 - 600. The default is 1. During the stateless auto configuration process, DAD verifies the uniqueness of new unicast IPv6 addresses before the addresses are assigned to interfaces. If the duplicate address is the link-local address of the interface, the processing of IPv6 packets is disabled on the interface. If the duplicate address is a global address, the address is not used. The interface uses neighbor solicitation messages to perform Duplicate Address Detection. Set the value to 0 to disable duplicate address detection (DAD) processing.

Step 11 Change the MTU (maximum transmission unit) to the desired value.

The default MTU is 1500 bytes. You can specify a value from 64 - 9198 (or 9000, for Firepower Threat Defense Virtual). Set a high value if you typically see jumbo frames on your network. See Use of MTU Settings in Firepower Interface Settings for more information.

Note If you increase MTU above 1500 on ASA 5500-X series devices, ISA 3000 series devices, or Firepower Threat Defense Virtual, you must reboot the device. Log into the CLI and use the reboot command. You do not need to reboot the Firepower 2100 or Secure Firewall 3100 series devices, where jumbo frame support is always enabled.

Step 12 (Physical interface only.) Modify the **speed** and **duplex** settings.

The default is that the interface negotiates the best duplex and speed with the interface at the other end of the wire, but you can force a specific duplex or speed if necessary. The options listed are only those supported by the interface. Before setting these options for interfaces on a network module, please read Guidelines and Limitations for Firepower Interface Configuration.

- **Duplex**- Choose Auto , Half , Full , or Default . Auto is the default when the interface supports it. For example, you cannot select Auto for the SFP interfaces on a Firepower 2100 or Secure Firewall 3100 series device. Select Default to indicate that Firepower Device Manager should not attempt to configure the setting.

  Any existing configuration is left unchanged.

- **Speed**- Choose Auto to have the interface negotiate the speed (this is the default), or pick a specific speed: 10 , 100 , 1000 , 10000 Mbps. You can also select these special options:

  Any existing configuration is left unchanged.

  The type of interface limits the options you can select. For example, the SFP+ interfaces on a Firepower 2100 series device support 1000 (1 Gbps) and 10000 (10 Gpbs) only, and the SFP interfaces support 1000 (1 Gbps) only, whereas GigabitEthernet ports do not support 10000 (10 Gpbs). SPF interfaces on other devices might require No Negotiate . Consult the hardware documentation for information on what the interfaces support.

Step 13 (Optional, recommended for subinterfaces and high availability units.) Configure the MAC address.

MAC Address-The Media Access Control in H.H.H format, where H is a 16-bit hexadecimal digit. For example, you would enter the MAC address 00-0C-F1-42-4C-DE as 000C.F142.4CDE. The MAC address must not have the multicast bit set, that is, the second hexadecimal digit from the left cannot be an odd number.)

Standby MAC Address-For use with high availability. If the active unit fails over and the standby unit becomes active, the new active unit starts using the active MAC addresses to minimize network disruption, while the old active unit uses the standby address.

Step 14 Click **Create**.

Configure a Bridge Group

A bridge group is a virtual interface that groups one or more interfaces. The main reason to group interfaces is to create a group of switched interfaces. Thus, you can attach workstations or other endpoint devices directly to the interfaces included in the bridge group. You do not need to connect them through a separate physical switch, although you can also attach a switch to a bridge group member.

The group members do not have IP addresses. Instead, all member interfaces share the IP address of the Bridge Virtual Interface (BVI). If you enable IPv6 on the BVI, member interfaces are automatically assigned unique link-local addresses.

You typically configure a DHCP server on the bridge group interface (BVI), which provides IP addresses for any endpoints connected through member interfaces. However, you can configure static addresses on the

endpoints connected to the member interfaces if you prefer. All endpoints within the bridge group must have IP addresses on the same subnet as the bridge group IP address.

Note For ISA 3000, the device comes pre-configured with bridge group BVI, named inside, which includes all data interfaces except for the outside interface. Thus, the device is pre-configured with one port used for linking to the Internet or other upstream network, and all other ports enabled and available for direct connections to endpoints. If you want to use an inside interface for a new subnet, you must first remove the needed interfaces from BVI.

FDM-managed devices only support one bridge group; therefore, Cisco Defense Orchestrator can only manage that one bridge group and cannot create additional bridge groups on the device.

After you create a bridge group on CDO, you will not know the bridge group ID until after the configuration is deployed to the FDM-managed device. FDM-managed device assigns the bridge group ID, for example, BVI1. If the interface is deleted and a new bridge group is created, the new bridge group receives an incremented number, for example, BVI2.

Before you Begin

Configure the interfaces that will be ***members*** of the bridge group. Specifically, each ***member*** interface must meet the following requirements:

- The interface must have a name.
- The interface cannot be configured as **management-only**.
- The interface cannot be configured for passive mode.
- The interface cannot be an EtherChannel interface or an EtherChannel subinterface.
- The interface cannot have any IPv4 or IPv6 addresses defined for it, either static or served through DHCP. If you need to remove the address from an interface that you are currently using, you might also need to remove other configurations for the interface, such as static routes, DHCP server, or NAT rules, that depend on the interface having an address. If you try to add an interface with an IP address to a bridge group, CDO will warn you. If you continue to add the interface to the bridge group, CDO will remove the IP address from the interface configuration.
- BVI can have either VLAN interfaces or other routed interfaces as a member interface, but you cannot have both as member interfaces on a single BVI.
- The interface cannot be Point-to-Point Protocol over Ethernet (PPPoE)
- The interface cannot be associated with a security zone (if it is in a zone). You must delete any NAT rules for the interface before you can add it to a bridge group.
- Enable and disable the member interfaces individually. Thus, you can disable any unused interfaces without needing to remove them from the bridge group. The bridge group itself is always enabled.
- Bridge groups do not support clustering.

Note Bridge groups are not supported on Firepower 2100 devices in routed mode or on VMware with bridged ixgbevf interfaces.

Configure the Name of the Bridge Group Interface and Select the Bridge Group Members

In this procedure you give the bridge group interface (BVI) a name and select the interfaces to add to the bridge group:

Procedure

Step 1 In the navigation bar, click **Inventory**.

Step 2 Click the **Devices** tab to locate the device or the **Templates** tab to locate the model device.

Step 3 Click the **FTD** tab and select the device for which you want to create a bridge group.

Step 4 Do one of the following:

- Select the BVI bridge group and click **Edit** in the Actions pane.
- Click the plus button and select Bridge Group Interface.

Note You can create and configure a single bridge group. If you already have a bridge group defined, you should edit that group instead of trying to create a new one. If you need to create a new bridge group, you must first delete the existing bridge group.

Step 5 Configure the following:

- **Logical Name**-You must give the bridge group a name. It can be up to 48 characters. Alphabetic characters must be lower case. For example, inside or outside. Without a name, the rest of the interface configuration is ignored.

Note If you change the name, the change is automatically reflected everywhere you used the old name, including security zones, syslog server objects, and DHCP server definitions. However, you cannot remove the name until you first remove all configurations that use the name, because you typically cannot use an unnamed interface for any policy or setting.

- (Optional) **Description**-The description can be up to 200 characters on a single line, without carriage returns.

Step 6 Click the **Bridge Group Member** tab. A bridge group can have up to 64 interfaces or subinterfaces to a single bridge group.

- Check an interface to add it to the bridge group.
- Uncheck an interface you want to remove from the bridge group.

Step 7 Click **Save**.

The BVI now has a name and member interfaces. Continue with the following tasks to configure the bridge group interface. You are not performing these tasks for the member interfaces themselves:

- Configure the IPv4 Address for the BVI if you are assigning an IPv4 address to the BVI.
- Configure the IPv6 Address for the BVI if you are assigning an IPv6 address to the BVI.

- Configure Advanced Interface Options for the bridge group interface.

Configure the IPv4 Address for the BVI

Procedure

Step 1 Select the device for which you want to create a bridge group.

Step 2 Select the BVI in the list of interfaces and click **Edit** in the Actions pane.

Step 3 Click the IPv4 Address tab to configure the IPv4 address.

Step 4 Select one of the following options from the Type field:

- **Static**-Choose this option if you want to assign an address that should not change. Type in the bridge group's IP address and the subnet mask. All attached endpoints will be on this network. For models with a pre-configured bridge group, the default for the BVI "inside" network is 192.168.1.1/24 (i.e. 255.255.255.0). Ensure that the address is not already used on the network.

  If you configured high availability, and you are monitoring this interface for HA, also configure a standby IP address on the same subnet. The standby address is used by this interface on the standby device. If you do not set the standby IP address, the active unit cannot monitor the standby interface using network tests; it can only track the link state.

  Note If there is a DHCP server configured for the interface, you are shown the configuration. You can edit or delete the DHCP address pool. If you change the interface IP address to a different subnet, you must either delete the DHCP server, or configure an address pool on the new subnet, before you can save the interface changes. See Configuring DHCP Server.

- **Dynamic (DHCP)**-Choose this option if the address should be obtained from the DHCP server on the network. This is not the typical option for bridge groups, but you can configure it if needed. You cannot use this option if you configure high availability. Change the following options if necessary:
  - Route Metricâ€”If you obtain the default route from the DHCP server, the administrative distance to the learned route, between 1 and 255. The default is 1.
  - Obtain Default Routeâ€”Check this option to get the default route from the DHCP server. You would normally select this option, which is the default.

Step 5 Continue with one of the following procedures:

- Configure the IPv6 Address for the BVI if you are assigning an IPv4 address to the BVI.
- Configure Advanced Interface Options.
- Click **Save** and deploy the changes to the Firepower device. See Deploy Configuration Changes from CDO to FDM-Managed Device for more information.

Configure the IPv6 Address for the BVI

Procedure

Step 1 Click the IPv6 Address tab to configure IPv6 addressing for the BVI.

Step 2 Configure these aspects of IPv6 addressing:

Step 3 **Enable IPv6 processing**-To enable IPv6 processing and to automatically configure the link-local address when you do not configure the global address, slide the **State** slider to blue. The link local address is generated based on the interface MAC addresses (Modified EUI-64 format).

Note Disabling IPv6 does not disable IPv6 processing on an interface that is configured with an explicit IPv6 address or that is enabled for autoconfiguration.

Step 4 **Suppress RA**-Whether to suppress router advertisements. The Firepower Threat Defense device can participate in router advertisements so that neighboring devices can dynamically learn a default router address. By default, router advertisement messages (ICMPv6 Type 134) are periodically sent out each IPv6 configured interface.

Router advertisements are also sent in response to router solicitation messages (ICMPv6 Type 133). Router solicitation messages are sent by hosts at system startup so that the host can immediately auto-configure without needing to wait for the next scheduled router advertisement message.

You might want to suppress these messages on any interface for which you do not want the FDM-managed device to supply the IPv6 prefix (for example, the outside interface).

Step 5 **Static Address/Prefix**-If you do not use stateless auto configuration, enter the full static global IPv6 address and network prefix. For example, 2001:0DB8::BA98:0:3210/48. For more information on IPv6 addressing, see IPv6 Addressing.

Step 6 **Standby IP Address**-If you configure high availability, and you are monitoring this interface for HA, also configure a standby IPv6 address on the same subnet. The standby address is used by this interface on the standby device. If you do not set the standby IP address, the active unit cannot monitor the standby interface using network tests; it can only track the link state.

Step 7 Continue with one of the following procedures:

- Configure Advanced Interface Options.
- Click **Save** and deploy the changes to the Firepower device. See Deploy Configuration Changes from CDO to FDM-Managed Device for more information.

Configure Advanced Interface Options

You configure most advanced options on bridge group ***member*** interfaces, but some are available for the bridge group interface itself.

Procedure

Step 1 The advanced settings have defaults that are appropriate for most networks. Edit them only if you are resolving network issues.

Step 2 Click **OK**.

Step 3 Click **Save** and deploy the changes to the Firepower device. See Deploy Configuration Changes from CDO to FDM-Managed Device for more information.

What to do next

- Ensure that all member interfaces that you intend to use are enabled.
- Configure a DHCP server for the bridge group. See Configure DHCP Servers.
- Add the member interfaces to the appropriate security zones.
- Ensure that policies, such as identity, NAT, and access, supply the required services for the bridge group and member interfaces.

Bridge Group Compatibility in FDM-Managed Configurations

In various configurations, where you can specify an interface, sometimes you will be able to specify a bridge virtual interface (BVI) and sometimes you will be able to specify a member of the bridge group. This table explains when a BVI can be used and when a member interface can be used.

Firepower Threat Defense Configuration Type	BVI can be used	BVI member can be used
DHCP server	Yes	No
DNS Server	Yes	Yes
Management access	Yes	No
NAT (Network Address Translation)	No	Yes
Security Zone	No	Yes
Site-to-Site VPN access point	No	Yes
Syslog Server	Yes	No

Delete a Bridge Group

When you delete a bridge group, its members become standard routed interfaces, and any NAT rules or security zone membership are retained. You can edit the interfaces to give them IP addresses. If you need to create a new bridge group, you must first delete the existing bridge group.

Procedure

Step 1 In the navigation pane, click **Inventory**.

Step 2 Click the **Devices** tab.

Step 3 Click the **FTD** tab and select the device from which you want to delete the bridge group.

Step 4 Select the BVI bridge group and click **Remove** in the Actions pane.

Step 5 Preview and Deploy Configuration Changes for All Devices now the changes you made, or wait and deploy multiple changes at once.

Add an EtherChannel Interface for an FDM-Managed Device

EtherChannel Interface Limitations

An EtherChannel, depending on the device model, can include multiple member interfaces of the same media type and capacity and must be set to the same speed and duplex. You cannot mix interface capacities (for example 1GB and 10GB interfaces) by setting the speed to be lower on the larger-capacity interface. The Link Aggregation Control Protocol (LACP) aggregates interfaces by exchanging the Link Aggregation Control Protocol Data Units (LACPDUs) between two network devices.

EtherChannel interfaces have a number of limitations based on physical configuration and software versions. See the sections below for more information.

General Interface Limitations

- EtherChannels are only available on devices running FDM-managed Version 6.5 and later.
- Cisco Defense Orchestrator supports EtherChannel interface configuration on the following Firepower devices: 1010, 1120, 1140, 1150, 2110, 2120, 2130, 2140, 3110, 3120, 3130, and 3140. For interface limitations per device model, see Device-Specific Limitations.
- All interfaces in the channel group must be the same media type and capacity, and must be set to the same speed and duplex. The media type can be either RJ-45 or SFP; SFPs of different types (copper and fiber) can be mixed. You cannot mix interface capacities (for example 1GB and 10GB interfaces) by setting the speed to be lower on the larger-capacity interface.
- The device to which you connect the EtherChannel must also support 802.3ad EtherChannels.
- The FDM-managed device does not support LACPDUs that are VLAN-tagged. If you enable native VLAN tagging on the neighboring switch using the Cisco IOS vlan dot1Q tag native command, then the FDM-managed device will drop the tagged LACPDUs. Be sure to disable native VLAN tagging on the neighboring switch.
- All FDM-managed device configuration refers to the logical EtherChannel interface instead of the member physical interfaces.
- Portchannel interfaces are displayed as physical interfaces.

Device-Specific Limitations

The following devices have specific interface limitations:

1000 Series

- Firepower 1010 supports up to 8 EtherChannel interfaces.
- Firepower 1120,1140,1150 supports up to 12 EtherChannel interfaces.
- 1000 series do not support LACP rate fast; LACP always uses the normal rate. This setting is not configurable.

2100 Series

- Firepower 2110 and 2120 models supports up to 12 EtherChannel interfaces.
- Firepower 2130 and 2140 models support up to 16 EtherChannel interfaces.
- 2100 series do not support LACP fast rate; LACP always uses the normal rate. This setting is not configurable.

Secure Firewall 3100 Series

- All Secure Firewall 3100 models support up to 16 EtherChannel interfaces.
- The Secure Firewall 3100 models support LACP fast rate.
- The Secure Firewall 3100 series models do not support enabling or disabling of network modules and breakout online insertion and removal (OIR) of interfaces.

4100 Series and 9300 Series

- You cannot create or configure EtherChannels on the 4100 and 9300 series. Etherchannels for these devices must be configured in the FXOS chassis.
- Etherchannels on the 4100 and 9300 series appear in Cisco Defense Orchestrator as physical interfaces.

Add an EtherChannel Interface

Use the following procedure to add an EtherChannel to your FDM-managed device:

Note If you want to immediately create another EtherChannel, check the **Create another** checkbox and then click **Create**.

Procedure

Step 1 In the navigation pane, click **Inventory**.

Step 2 Click the **Devices** tab.

Step 3 Click the **FTD** tab and select the device you want to add an EtherChannel to.

Step 4 In the **Management** pane located to the right, select **Interfaces**.

Step 5 Click the blue plus button  and select **EtherChannel**.

Step 6 (Optional) Enter a **Logical Name**.

Step 7 (Optional) Enter a description.

Step 8 Enter the **EtherChannel ID**.

For Firepower 1010 series, enter a value between 1 and 8.

For the Firepower 2100, 3100, 4100, and 9300 series, enter a value between 1 and 48.

Step 9 Click the drop-down button for **Link Aggregation Control Protocol** and select one of the two options:

- **Active** - Sends and receives LACP updates. An active EtherChannel can establish connectivity with either an active or a passive EtherChannel. You should use the active mode unless you need to minimize the amount of LACP traffic.
- **On** - The EtherChannel is always on, and LACP is not used. An **on** EtherChannel can only establish a connection with another EtherChannel that is also configured to be **on**.

Step 10 Search for and select the interfaces you want to include in the EtherChannel as memebers. You **must** include at least one interface.

Warning: If you add an EtherChannel interface as a member and it already has an IP address configured, CDO removes the IP address of the member.

Step 11 Click **Create**.

Related Information:

- Edit Or Remove an EtherChannel Interface for FDM-Managed Device
- Add a Subinterface to an EtherChannel Interface
- Edit or Remove a Subinterface from an EtherChannel
- Guidelines and Limitations for Firepower Interface Configuration
- Assign an FDM-Managed Device Interface to a Security Zone
- Add an EtherChannel Interface for an FDM-Managed Device, on page 26

Edit Or Remove an EtherChannel Interface for FDM-Managed Device

Use the following procedures to either modify an existing EtherChannel interface, or remove an EtherChannel interface from an FDM-managed device.

Edit an EtherChannel

Note that EtherChannels have several limitations you must be aware of when modifying. See EtherChannel for more information.

Note EtherChannels must have at least one member.

Use the following procedure to edit an existing EtherChannel:

Procedure

Step 1 In the navigation pane, click **Inventory**.

Step 2 Click the **Devices** tab.

Step 3 Click the **FTD** tab and select the threat defense associated with the Etherchannel you want to modify.

Step 4 In the **Management** pane located to the right, click **Interfaces**.

Step 5 On the **Interfaces** page, select the EtherChannel interface you want to edit. In the Actions pane located to the right, click the edit icon .

Step 6 Modify any of the following items:

- Logical name.
- State.
- Description.
- Security Zone assignment.
- Link Aggregation Control Protocol status.
- IP address configuration in either the **IPv4**, **IPv6**, or **Advanced** tabs.
- EtherChannel members.

Warning **Warning**: If you add an EtherChannel interface as a member and it already has an IP address configured, CDO removes the IP address of the member.

Step 7 Click **Save**.

Remove an EtherChannel Interface

Note EtherChannel interfaces associated with a high availability (HA) or any other configuration. You must manually remove the EtherChannel interface from all configurations before deleting it from CDO.

Use the following procedure to remove an EtherChannel interface from an FDM-managed device:

Procedure

Step 1 In the navigation pane, click **Inventory**.

Step 2 Click the **Devices** tab.

Step 3 Click the **FTD** tab and the threat defense associated with the Etherchannel you want to delete.

Step 4 In the **Management** pane located to the right, select **Interfaces**.

Step 5 On the **Interfaces** page, select the EtherChannel interface you want to edit. In the Actions pane located to the right, click **Remove**.

Step 6 Confirm you want to delete the EtherChannel interface and click **OK**.

Add a Subinterface to an EtherChannel Interface

EtherChannel Subinterfaces

The **Interfaces** page allows you to view which interfaces of a device have subinterfaces by expanding each interface. This expanded view also shows you the unique logical name, enabled/disabled state, any associated security zones, and mode of the subinterface. The interface type and mode of the subinterface is determined by the parent interface.

General Limitations

CDO does not support subinterfaces for the following interface types:

- Interface configured for management-only.
- Interface configured for switch port mode.
- Passive interfaces.
- VLAN interfaces.
- Bridge virtual interfaces (BVI).
- Interfaces that are already a member of another EtherChannel interface.

You **can** create subinterfaces for the following:

- Bridge group members.
- EtherChannel interfaces.
- Physical interfaces.

Add a Subinterface to an EtherChannel Interface

Use the following procedure to add a subinterface to an existing interface:

Note If you want to immediately create another subinterface, check the **Create another** checkbox and then click **Create**.

Procedure

Step 1 In the navigation pane, click **Inventory**.

Step 2 Click the **Devices** tab.

Step 3 Click the **FTD** tab and select the threat defense you want to add an EtherChannel to. In the Management pane located to the right, select **Interfaces**.

Step 4 Select the interface you want to group the subinterface under. In the Action pane located to the right, click the + New Subinterface button.

Step 5 (Optional) Enter a **Logical Name**.

Step 6 (Optional) Enter a description.

Step 7 (Optional) Assign a security zone to the subinterface. Note that you cannot assign a security zone if the subinterface does not have a logical name.

Step 8 Enter a VLAN ID.

Step 9 Enter the **EtherChannel ID**. Use a value between 1 and 48; use values between 1 and 8 for the Firepower 1010 series.

Step 10 Select the **IPv4**, **IPv6**, or **Advanced** tab to configure the IP address of the subinterface.

Step 11 Click **Create**.

Edit or Remove a Subinterface from an EtherChannel

Use the following procedures to either modify an existing subinterface, or remove a subinterface from an Etherchannel interface.

Note Subinterfaces and EtherChannel interfaces have a series of guidelines and limitations that may affect your configuration. See the General Limitations for more information.

Edit a Subinterface

Use the following procedure to edit an existing subinterface associated with an EtherChannel interface:

Procedure

Step 1 Log into CDO.

Step 2 In the navigation pane, click **Inventory**.

Step 3 Click the **Devices** tab.

Step 4 Click the **FTD** tab and select the threat defense associated with the EtherChannel and subinterface you want to edit.

Step 5 In the **Management** pane located to the right, select **Interfaces**.

Step 6 Locate and expand the Etherchannel interface that the subinterface is a member of.

Step 7 Select the desired subinterface you want to edit. In the Action pane located to the right, click the edit icon .

Step 8 Modify any of the following items:

- Logical name.
- State.
- Description.
- Security Zone assignment.
- VLAN ID
- IP address configuration in either the IPv4, IPv6, or Advanced tabs.

Step 9 Click **Save**.

Remove a Subinterface from an EtherChannel

Use the following procedure to remove an existing subinterface from an EtherChannel interface:

Procedure

Step 1 In the navigation pane, click **Inventory**.

Step 2 Click the **Devices** tab.

Step 3 Click the **FTD** tab and select the threat defense associated with the EtherChannel and subinterface you want to edit. In the Management pane located to the right, select **Interfaces**.

Step 4 Locate and expand the Etherchannel interface that the subinterface is a member of.

Step 5 Select the desired subinterface you want to delete.

Step 6 In the Actions pane located to the right, click **Remove**.

Step 7 Confirm you want to delete the subinterface interface and click **OK**.

Add Interfaces to a Virtual FDM-Managed Device

When you deploy a virtual FDM-managed device, you assign interfaces to the virtual machine. Then, from within an FDM-managed device, you configure those interfaces using the same methods you would use for a hardware device.

However, you cannot add more virtual interfaces to the virtual machine and then have FDM automatically recognize them. If you need more physical-interface equivalents for a virtual FDM-managed device, you basically have to start over. You can either deploy a new virtual machine, or you can use the following procedure.

Caution Adding interfaces to a virtual machine requires that you completely wipe out the virtual FDM-managedconfiguration. The only part of the configuration that remains intact is the management address and gateway settings.

Before You Begin

Do the following in an FDM-managed device:

- Examine the virtual FDM-managed device configuration and make notes on settings that you will want to replicate in the new virtual machine.
- Select **Devices** > **Smart License** > **View Configuration** and disable all feature licenses.

Procedure

Step 1 Power off the virtual FDM-managed device.

Step 2 Using the virtual machine software, add the interfaces to the virtual FDM-managed device. For VMware, virtual appliances use e1000 (1 Gbit/s) interfaces by default. You can also use vmxnet3 or ixgbe (10 Gbit/s) interfaces

Step 3 Power on the virtual FDM-managed device.

Step 4 Open the virtual FDM-managed device console, delete the local manager, then enable the local manager. Deleting the local manager, then enabling it, resets the device configuration and gets the system to recognize the new interfaces. The management interface configuration does not get reset. The following SSH session shows the commands.

```
> show managers
Managed locally.
> configure manager delete
If you enabled any feature licenses, you must disable them in Firepower Device Manager
before deleting the local manager. Otherwise, those licenses remain assigned to the device
 in Cisco Smart Software Manager.
Do you want to continue[yes/no] yes
DCHP Server Disabled
> show managers
No managers configured.
> configure manager local
>
```

Step 5 Open a browser session to an FDM-managed device, complete the device setup wizard, and configure the device. See the "Complete the Initial Configuration" section of the Getting Started chapter of Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager, Version x.x.x, guide for more instructions.

Switch Port Mode Interfaces for an FDM-Managed Device

For each physical Firepower 1010 interface, you can set its operation as a firewall interface or as a switch port. Switch ports forward traffic at Layer 2, using the switching function in hardware. Switch ports on the same VLAN can communicate with each other using hardware switching, and traffic is not subject to the FDM-managed device security policy. Access ports accept only untagged traffic, and you can assign them to a single VLAN. Trunk ports accept untagged and tagged traffic, and can belong to more than one VLAN. For devices that have been reimaged to Version 6.4, Ethernet 1/2 through 1/8 are configured as access switch ports on VLAN 1; devices that are manually upgraded to Version 6.4 (and later), the ethernet configuration maintains the configuration prior ot upgrading. Note that switch ports on the same VLAN can communicate with each other using hardware switching, and traffic is not subject to the FDM-managed device security policy.

Access or Trunk

A physical interface configured as a switch port can be assigned as either an access port or a trunk port.

Access ports forward traffic to only one VLAN and accept only untagged traffic. We strongly recommend this option if you intend to forward traffic to a single host or device. You must also specify the VLAN you would like to be associated with the interface, otherwise it will default to VLAN 1.

Trunk ports forward traffic to multiple VLANs. You must assign one VLAN interface as the native trunk port and at least one VLAN as an associated trunk port. You can select up to 20 interfaces to be associated with the switch port interface, which enables traffic from different VLAN IDs to pass through the switch port interface. If an untagged traffic is passed through the switch port then the traffic is tagged with the VLAN ID of the native VLAN interface. Note that the default Fiber Distributed Data Interface (FDDI) & Token RING ID between 1002 and 1005 cannot be used for VLAN ID.

Change the Port Mode

If you select an interface that is configured for routed mode as a VLAN member, CDO automatically converts the interface to switch port mode and configures the interface as an access port by default. As a result the logical name and the associated static IP addresses are removed from the interface.

Configuration Limitations

Be aware of the following limitations:

- Only physical Firepower 1010 devices support switch port mode configuration. Virtual FDM-managed devices do not support switch port mode.
- The Firepower 1010 device allows a maximum of 60 VLANs.
- VLAN interfaces configured for switch port mode must be unnamed. This means the MTU **must** be configured to 1500 bytes.
- You **cannot** delete an interface configured as a switch port mode. You must manually change the interface mode from **switch port** mode to **routed** mode.
- Interfaces configured for switch port mode do not support IP addresses. If the interface is currently referenced in or configured for VPN, DHCP, or is associated with a static route, you **must** manually remove the IP address.
- You cannot use any member of the bridge group interface as a a switch port.
- The MTU for a VLAN interface **must** be 1500 bytes. Unnamed VLAN interfaces do not support any other configuration.
- Switch port mode does not support the following:
  - Diagnostic interface.
  - Dynamic, multicast, or Equal-Cost Multi-Path (ECMP) routing.
  - Passive interfaces.
  - Port etherchannels, or using an interface that is a member of an etherchannel.
  - Subinterfaces.
  - Failover and state link.

High Availability and Switch Port Mode Interfaces

You should not use the switch port functionality when using High Availability. Because the switch ports operate in hardware, they continue to pass traffic on both the active *and* the standby units. High Availability is designed to prevent traffic from passing through the standby unit, but this feature does not extend to switch ports. In a normal High Availability network setup, active switch ports on both units will lead to network loops. We suggest that you use external switches for any switching capability. Note that VLAN interfaces can be monitored by failover, while switch ports cannot.

Note You can only use a firewall interface as the failover link.

Switch Port Mode Configurations in Templates

You can create templates of devices with interfaces configured for switch port mode. Beware the following scenarios when mapping interfaces from the template to a device:

- If a template interface does not contain any VLAN members prior to applying the template, CDO automatically maps it to an available device interface that has the same properties.
- If a template interface that does not contain a VLAN member is mapped to a device interface that is configured as **N/A**, CDO automatically creates an interface on the device the template is to be applied to
- If a template interface containing a VLAN member is mapped to a device interface that is not present, applying a template will **fail**.
- Templates do not support mapping more than one template interface to the same device interface.
- The template's management interface must be mapped to the device's management interface.

Configure an FDM-Managed Device VLAN

You must first configure a VLAN interface if you intend to configure subinterfaces or switch ports.

Note An FDM-managed device supports a maximum of 60 VLAN interfaces.

Procedure

Step 1 In the navigation pane, click **Inventory**.

Step 2 Click the **Devices** tab to locate the device or the **Templates** tab to locate the model device.

Step 3 Click the **FTD** tab and select the desired device you want to create a VLAN on.

Step 4 In the **Management** pane at the right, click **Interfaces**.

Step 5 On the **Interfaces** page, click the  button.

Step 6 Configure the following:

- **Parent Interface** - The parent interface is the physical interface to which you want to add the subinterface. You cannot change the parent interface after you create the subinterface.
- (Optional) **Logical Name**-Set the name for the VLAN, up to 48 characters. Alphabetic characters must be lower case. If you do not want to route between the VLAN and other VLANs or firewall interfaces, then leave the VLAN interface name empty.

  Note If you do not enter a name, the MTU in the **Advanced Options** must be set to 1500. If you change the MTU to something other than 1500, the VLAN must be unnamed.

- (Optional) **Description**-The description can be up to 200 characters on a single line, without carriage returns.

- (Optional) **Security Zone** - Assign the subinterface to a security zone. Note that you cannot assign a subinterface if it does not have a Logical Name. You ca also assign a security zone after creating a subinterface. See Use of Security Zones in Firepower Interface Settings for more information.
- (Optional) **VLAN ID**-Enter the VLAN ID between 1 and 4070 that will be used to tag the packets on this subinterface.

  Note VLAN interfaces are routed by default. If you add this VLAN interface to a bridge group at a later date, Cisco Defense Orchestrator (CDO) automatically changes the mode to **BridgeGroupMember**. Similarly, if you change this VLAN interface to switch port mode, CDO automatically changes the mode to **Switch Port**.

- (Optional) **Subinterface ID** - Enter the subinterface ID as an integer between 1 and 4294967295. This ID is appended to the interface ID; for example Ethernet1/1.100. You can match the VLAN ID for convenience, but it is not required. You cannot change the ID after you create the subinterface.

Step 7 Click the **IPv4 Address** tab and select one of the following options from the Type field:

- **Static** - Choose this option if you want to assign an address that should not change. Type in the interface's IP address and the subnet mask for the network attached to the interface. For example, if you attach the 10.100.10.0/24 network, you could enter 10.100.10.1/24. Ensure that the address is not already used on the network.

  If you configured high availability, and you are monitoring this interface for HA, also configure a standby IP address on the same subnet. The standby address is used by this interface on the standby device. If you do not set the standby IP address, the active unit cannot monitor the standby interface using network tests; it can only track the link state.

  Note If there is a DHCP server configured for the interface, you are shown the configuration. You can edit or delete the DHCP address pool. If you change the interface IP address to a different subnet, you must either delete the DHCP server, or configure an address pool on the new subnet, before you can save the interface changes. See Configure DHCP Servers for more information.

- **Dynamic (DHCP)**-Choose this option if the address should be obtained from the DHCP server on the network. You cannot use this option if you configure high availability. Change the following options if necessary:
  - **Route Metric**-If you obtain the default route from the DHCP server, the administrative distance to the learned route, between 1 and 255. The default is 1.
  - **Obtain Default Route**-Check this option to get the default route from the DHCP server. You would normally select this option, which is the default.

- **DHCP Address Pool** - If there is a DHCP server configured for the interface, you are shown the configuration. You can edit or delete the DHCP address pool. If you change the interface IP address to a different subnet, you must either delete the DHCP server, or configure an address pool on the new subnet, before you can save the interface changes.

Step 8 (Optional) Click the **IPv6 Address** tab and configure the following:

- **State** - To enable IPv6 processing and to automatically configure the link-local address when you do not configure the global address, slide the State slider to blue. The link local address is generated based on the interface MAC addresses (Modified EUI-64 format).

Note Disabling IPv6 does not disable IPv6 processing on an interface that is configured with an explicit IPv6 address or that is enabled for autoconfiguration.

- **Address Auto Configuration** - Check this option to have the address automatically configured. IPv6 stateless autoconfiguration will generate a global IPv6 address only if the link on which the device resides has a router configured to provide IPv6 services, including the advertisement of an IPv6 global prefix for use on the link. If IPv6 routing services are not available on the link, you will get a link-local IPv6 address only, which you cannot access outside of the device's immediate network link. The link local address is based on the Modified EUI-64 interface ID.
- **Suppress RA**-Whether to suppress router advertisements. Threat Defense can participate in router advertisements so that neighboring devices can dynamically learn a default router address. By default, router advertisement messages (ICMPv6 Type 134) are periodically sent out each IPv6 configured interface.

  Router advertisements are also sent in response to router solicitation messages (ICMPv6 Type 133). Router solicitation messages are sent by hosts at system startup so that the host can immediately auto-configure without needing to wait for the next scheduled router advertisement message.

  We suggest suppressing these messages on any interface for which you do not want the FDM-managed device to supply the IPv6 prefix (for example, the outside interface).
- **Static Address/Prefix**-If you do not use stateless auto configuration, enter the full static global IPv6 address and network prefix. For example, 2001:0DB8::BA98:0:3210/48. For more information on IPv6 addressing, see IPv6 Addressing for Firepower Interfaces.
- **Standby IP Address**-If you configure high availability, and you are monitoring this interface for HA, also configure a standby IPv6 address on the same subnet. The standby address is used by this interface on the standby device. If you do not set the standby IP address, the active unit cannot monitor the standby interface using network tests; it can only track the link state.

Step 9 (Optional) Click the **Advanced** tab.

- Select **Enable** for **HA Monitoring** if you want the health of the interface to be a factor when the system decides whether to fail over to the peer unit in a high availability configuration.

  This option is ignored if you do not configure high availability. It is also ignored if you do not configure a name for the interface.
- Select **Management Only** to make a data interface management only.

  A management only interface does not allow through traffic, so there is very little value in setting a data interface as management only. You cannot change this setting for the Management/Diagnostic interface, which is always management only.
- Modify the IPv6 Configuration settings.
  - **Enable DHCP for IPv6 address configuration**-Whether to set the Managed Address Configuration flag in the IPv6 router advertisement packet. This flag informs IPv6 autoconfiguration clients that they should use DHCPv6 to obtain addresses, in addition to the derived stateless autoconfiguration address.
  - **Enable DHCP for IPv6 non-address configuration**-Whether to set the Other Address Configuration flag in the IPv6 router advertisement packet. This flag informs IPv6 autoconfiguration clients that they should use DHCPv6 to obtain additional information from DHCPv6, such as the DNS server address.

- **DAD Attempts**-How often the interface performs Duplicate Address Detection (DAD), from 0 - 600. The default is 1. During the stateless autoconfiguration process, DAD verifies the uniqueness of new unicast IPv6 addresses before the addresses are assigned to interfaces. If the duplicate address is the link-local address of the interface, the processing of IPv6 packets is disabled on the interface. If the duplicate address is a global address, the address is not used. The interface uses neighbor solicitation messages to perform Duplicate Address Detection. Set the value to 0 to disable duplicate address detection (DAD) processing.

- Change the **MTU** (maximum transmission unit) to the desired value.

  The default MTU is 1500 bytes. You can specify a value from 64 - 9198 (or 9000 for virtual FDM-managed devices and 9184 for the Firepower 4100/9300). Set a high value if you typically see jumbo frames on your network.

  Note If you increase MTU above 1500 on ASA 5500-X series devices, ISA 3000 series devices, or virtual FDM-managed devices, the VLAN must be unnamed **and** you must reboot the device. Log into the CLI and use the reboot command. If the device is configured for HA, you must also reboot the standby device. You do not need to reboot Firepower models, where jumbo frame support is always enabled.

- (Optional for subinterface and HA pairs) Configure the **MAC address**.

  By default, the system uses the MAC address burned into the network interface card (NIC) for the interface. Thus, all subinterfaces on an interface use the same MAC address, so you might want to create unique addresses per subinterface. Manually configured active/standby MAC addresses are also recommended if you configure high availability. Defining the MAC addresses helps maintain consistency in the network in the event of failover.

  - **MAC Address**-The Media Access Control in H.H.H format, where H is a 16-bit hexadecimal digit. For example, you would enter the MAC address 00-0C-F1-42-4C-DE as 000C.F142.4CDE. The MAC address must not have the multicast bit set, that is, the second hexadecimal digit from the left cannot be an odd number.)

  - **Standby MAC Address**-For use with HA pairs. If the active unit fails over and the standby unit becomes active, the new active unit starts using the active MAC addresses to minimize network disruption, while the old active unit uses the standby address.

Step 10 If you intend to create another subinterface for this device, check **Create another** prior to completing the subinterface configuration.

Step 11 (Optional) Activate the subinterface upon creation by toggling the **State** slider in the upper right corner of the pop-up window from grey to blue.

Step 12 Click **OK**.

Step 13 Preview and Deploy Configuration Changes for All Devices now the changes you made, or wait and deploy multiple changes at once.

Configure an FDM-Managed Device VLAN for Switch Port Mode

Be sure to read the limitations for switch port mode prior to configuration; see Switch Port Mode Interfaces for an FDM-Managed Device for more information.

Note You can assign or edit a VLAN member to a physical interface at any time. Be sure to deploy the changes to the device after you confirm the new configuration.

Create a VLAN Interface for Switch Port Mode

Procedure

Step 1 In the navigation pane, click **Inventory**.

Step 2 Click the **Devices** tab to locate the device or the **Templates** tab to locate the model device.

Step 3 Click the **FTD** tab and select the device you want to configure interfaces for.

Step 4 In the **Management** pane on the right, click **Interfaces**.

Step 5 On the **Interfaces** page, click the  button and choose **VLAN Interface**.

Step 6 View the **VLAN Members** tab and select the desired physical interfaces.

Note If you chose to add a member that references a VLAN interface configured for either Access or Native Trunk, you can only select one VLAN as a member. Physical interfaces that references a VLAN interface configured for Associated Trunk supports up to 20 interfaces as members.

Step 7 Configure the rest of the VLAN interface, as described in Configure an FDM-Managed Device VLAN.

Step 8 Click **Save**. Confirm that you want to reset the VLAN configuration and reassign an IP address to the interface.

Step 9 Preview and Deploy Configuration Changes for All Devicesnow the changes you made, or wait and deploy multiple changes at once.

Configure an Existing Physical Interface for Switch Port Mode

Procedure

Step 1 In the navigation pane, click **Inventory**.

Step 2 Click the **Devices** tab to locate the device or the **Templates** tab to locate the model device.

Step 3 Click the **FTD** tab and select the device you want to configure interfaces for.

Step 4 In the **Management** pane on the right, click **Interfaces**.

Step 5 On the **Interfaces** page, select the physical interface you want to modify. In the Action Pane on the right, click the edit icon  .

Step 6 Interfaces configured for switch port mode do not support logical names. If the interface has a logical name, delete it.

Step 7 Locate the **Mode** and use the drop-down menu to select **Switch Port**.

Step 8 Configure the physical interface for switch port mode:

- (Optional) Check the **Protected Port** check box to set this switch port as protected, so you can prevent the switch port from communicating with other protected switch ports on the same VLAN. You might

want to prevent switch ports from communicating with each other if: the devices on those switch ports are primarily accessed from other VLANs; you do not need to allow intra-VLAN access; and you want to isolate the devices from each other in case of infection or other security breach. For example, if you have a DMZ that hosts three web servers, you can isolate the web servers from each other if you apply this option to each switch port. The inside and outside networks can both communicate with all three web servers, and vice versa, but the web servers cannot communicate with each other.

- For the Usage Type, select **Access** or **Trunk**. See Switch Port Mode Interfaces for an FDM-Managed Device to determine which port type you need.
  - If you select **Trunk**, you must select one VLAN interface as the **Native Trunk VLAN** to forward untagged traffic and at least one **Associated VLAN** to forward tagged traffic. Click the + icon to view the existing physical interfaces. You can select up to 20 VLAN interfaces as associated VLANs.
  - You can create a new VLAN interface set to Access mode by clicking **C reate new VLAN**.

Step 9 Click **Save**. Confirm that you want to reset the VLAN configuration and reassign an IP address to the interface.

Step 10 Preview and Deploy Configuration Changes for All Devices now the changes you made, or wait and deploy multiple changes at once.

Viewing and Monitoring Firepower Interfaces

To view firepower interfaces, follow these steps:

Procedure

Step 1 In the navigation pane, click **Inventory**.

Step 2 Click the **Devices** tab to locate the device or the **Templates** tab to locate the model device.

Step 3 Click the **FTD** tab and the device whose interfaces you want to view.

Step 4 Select **Interfaces** in the Management pane on the right.

Step 5 In the Interfaces table, select an interface.

- If you expand the interface row, you see subinterface information.
- On the right, you see detailed interface information.

Monitoring Interfaces in the CLI

You can view some basic information, behavior, and statistics about interfaces by connecting to the device using SSH and running the command below.

For an easy to connect to the device using SSH, onboard the FDM-managed device you want to monitor as an SSH device and then use the >_ Command Line Interface in CDO.

- **`show interface`** displays interface statistics and configuration information. This command has many keywords you can use to get to the information you need. Use ? as a keyword to see the available options.
- **`show ipv6 interface`** displays IPv6 configuration information about the interfaces.
- **`show bridge-group`** displays information about Bridge Virtual Interfaces (BVI), including member information and IP addresses.
- **`show conn`** displays information about the connections currently established through the interfaces.
- **`show traffic`** displays statistics about traffic flowing through each interface.
- **`show ipv6 traffic`** displays statistics about IPv6 traffic flowing through the device.
- **`show dhcpd`** displays statistics and other information about DHCP usage on the interfaces, particularly about the DHCP servers configured on interfaces.

Synchronizing Interfaces Added to a Firepower Device using FXOS

If an interface is added to a Firepower device by using the Firepower eXtensible Operating System (FXOS) Chassis Manager, on the Firepower 4100 series or 9300 series devices, Cisco Defense Orchestrator does *not* recognize that configuration change and report a configuration conflict.

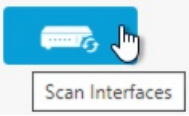
To see the newly added interface in CDO, follow this procedure:

Procedure

Step 1 Log in to an FDM-managed device.

Step 2 From the FDM-managed main page, click **View All Interfaces** in the Interfaces panel.

Step 3 Click the **Scan Interfaces** button:



Step 4 Wait for the interfaces to scan, and then click **OK**.

Step 5 Deploy your changes on an FDM-managed device.

Step 6 Log in to CDO as an Admin or SuperAdmin.

Step 7 In the navigation pane, click **Inventory**.

Step 8 Click the **Devices** tab to locate the device or the **Templates** tab to locate the model device.

Step 9 Click the **FTD** tab and select the device with the expected new interface configuration.

Step 10 Click **Check for Changes** to immediately compare the copy of the configuration on the device with the copy of the configuration stored on CDO. CDO will detect the interface change and report a "Conflict Detected" state on the **Inventory** page for the device.

Step 11 Resolve the Conflict Detected by clicking **Review Conflict** and then accepting the out of band changes.

Routing

Routing is the act of moving information across a network from a source to a destination. Along the way, at least one intermediate node is typically encountered. Routing involves two basic activities: determining optimal routing paths and transporting packets through a network.

Using Cisco Defense Orchestrator (CDO), you can define a default route, and other static routes, for your FDM-managed devices. The following topics explain routing basics and how to use CDO to configure static routing on your FDM-managed device:

- About Static Routing and Default Routes
- The Routing Table and Route Selection
- Configure Static and Default Routes for FDM-Managed Devices
- Monitoring Routing

About Static Routing and Default Routes

To route traffic to a non-connected host or network, you must define a route to that host or network. That defined route is a static route. Consider also configuring a default route. A default route is for all traffic that is not routed by other means to a default network gateway, typically the next hop router.

Related Information:

- Default Route
- Static Routes

Default Route

If you do not know a route to a specific network, the simplest option is to configure a default route that sends all traffic to an upstream router, relying on that router to route the traffic for you. A default route identifies the gateway IP address to which the FDM-managed device sends all IP packets for which you did not define a static route. A default route is simply a static route with 0.0.0.0/0 (IPv4) or ::/0 (IPv6) as the destination IP address.

Static Routes

A static route is a route from one network to another network that you define and enter manually into the routing table. You might want to use static routes in the following cases:

- Your network is small and stable and you can easily manage manually adding and changing routes between devices.
- Your networks use an unsupported router discovery protocol.
- You do not want the traffic or CPU overhead associated with routing protocols.
- In some cases, a default route is not enough. The default gateway might not be able to reach the destination network, so you must also configure more specific static routes. For example, if the default gateway is

outside, then the default route cannot direct traffic to any inside networks that are not directly connected to the FDM-managed device.

- You are using a feature that does not support dynamic routing protocols.

Limitations:

- CDO does not currently support the management, monitoring, or use of Virtual Tunnel Interface (VTI) tunnels on ASA or FDM-managed devices. Devices with configured VTI tunnels can be onboarded to CDO but it ignores the VTI interfaces. If a security zone or static route references a VTI, CDO reads the security zone and static route without the VTI reference. CDO support for VTI tunnels is coming soon.
- FDM-managed device running on software version 7.0 or later allows configuring Equal-Cost Multi-Path (ECMP) traffic zones. When the FDM-managed device is onboarded to CDO, it can read but cannot modify the ECMP configuration available in the global VRF routes because it does not allow a route to the same destination network with an identical metric value. You can create and modify ECMP traffic zones through FDM and then read it into CDO. For more information on ECMP, see the "Equal-Cost Multi-Path (ECMP) Routing" section in the "Routing Basics and Static Routes" chapter of Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager, Version 7.0 or later.

The Routing Table and Route Selection

When NAT translations (xlates) and rules do not determine the egress interface, the system uses the routing table to determine the path for a packet.

Routes in the routing table include a metric called "administrative distance" that provides a relative priority to a given route. If a packet matches more than one route entry, the one with the lowest distance is used. Directly connected networks (those defined on an interface) have the distance 0, so they are always preferred. Static routes have a default distance of 1, but you can create them with any distance between 1-254.

Routes that identify a specific destination take precedence over the default route (the route whose destination is 0.0.0.0/0 or ::/0).

How the Routing Table is Populated

The FDM-managed device routing table can be populated with statically defined routes and directly connected routes. It is possible that the same route is entered in more than one manner. When two routes to the same destination are put into the routing table, the one that remains in the routing table is determined as follows:

- If the two routes have different network prefix lengths (network masks), then both routes are considered unique and are entered into the routing table. The packet forwarding logic then determines which of the two to use.

For example, assume the following routes are entered in the routing table:

- 192.168.32.0/24
- 192.168.32.0/19

Even though the 192.168.32.0/24 route has the longer network prefix, both routes are installed in the routing table because each of these routes has a different prefix length (subnet mask). They are considered different destinations and the packet forwarding logic determines which route to use.

- If multiple paths to the same destination are entered in the routing table, the route with the better metric, as entered with the static route, is entered into the routing table.

Metrics are values associated with specific routes, ranking them from most preferred to least preferred. The parameters used to determine the metrics differ for different routing protocols. The path with the lowest metric is selected as the optimal path and installed in the routing table. If there are multiple paths to the same destination with equal metrics, load balancing is done on these equal cost paths.

Related Information:

- How Forwarding Decisions are Made

How Forwarding Decisions are Made

Forwarding decisions are made in this order:

- Use NAT translations (xlates) and rules to determine the egress interface. If the NAT rules do not determine the egress interface, the system uses the routing table to determine the path for a packet.
- If the destination does not match an entry in the routing table, the packet is forwarded through the interface specified for the default route. If a default route has not been configured, the packet is discarded.
- If the destination matches a single entry in the routing table, the packet is forwarded through the interface associated with that route.
- If the destination matches more than one entry in the routing table, then the packet is forwarded out of the interface associated with the route that has the longer network prefix length. For example, a packet destined for 192.168.32.1 arrives on an interface with the following routes in the routing table:
- 192.168.32.0/24 gateway 10.1.1.2
- 192.168.32.0/19 gateway 10.1.1.3

In this case, a packet destined to 192.168.32.1 is directed toward 10.1.1.2, because 192.168.32.1 falls within the 192.168.32.0/24 network. It also falls within the other route in the routing table, but 192.168.32.0/24 has the longer prefix within the routing table (24 bits verses 19 bits). Longer prefixes are always preferred over shorter ones when forwarding a packet.

Note Existing connections continue to use their established interfaces even if a new similar connection would result in different behavior due to a change in routes.

Configure Static and Default Routes for FDM-Managed Devices

Define static routes on an FDM-managed device so it knows where to send packets bound for networks not directly connected to the interfaces on the system.

Consider creating a default route. This is the route for network 0.0.0.0/0. This route defines where to send packets whose egress interface cannot be determined by existing NAT translations, static NAT rules, or other static routes.

You might need other static routes if the default gateway cannot be used to get to all networks. For example, the default route is usually an upstream router on the outside interface. If there are additional inside networks

that are not directly connected to the device, and they cannot be accessed through the default gateway, you need static routes for each of those inside networks.

You cannot define static routes for the networks that are directly connected to system interfaces. The system automatically creates these routes.

Procedure

Procedure

Step 1 In the navigation pane, click **Inventory**.

Step 2 Click the **Devices** tab to locate the device or the **Templates** tab to locate the model device.

Step 3 Click the **FTD** device and select the device on which you want to define static routes.

Step 4 In the **Management** pane at the right, click **Routing**.

Step 5 On the Static Routing page, do one of the following:

- To add a new static route, click the plus button  .
- Click the edit icon for the route you want to edit.

If you no longer need a route, click the trash can icon for the route to delete it.

Step 6 Configure the route properties

- **Protocol**-Select whether the route is for an IPv4 or IPv6 address.
- **Interface**-Select the interface through which you want to send traffic. The gateway address needs to be accessible through this interface.
- **Gateway**-Select the network object that identifies the IP address for the gateway to the destination network. Traffic is sent to this address.
- **Metric**-The administrative distance for the route, between 1 and 254. The default is for static routes is 1. If there are additional routers between the interface and the gateway, enter the number of hops as the administrative distance.

  Administrative distance is a parameter used to compare routes. The lower the number, the higher precedence the route is given. Connected routes (networks directly connected to an interface on the device) always take precedence over static routes.
- **Destination Network**-Select the network object(s), that identifies the destination network, that contains the host(s), that uses the gateway in this route.

  To define a default route, use the pre-defined any-ipv4 or any-ipv6 network objects, or create an object for the 0.0.0.0/0 (IPv4) or ::/0 (IPv6) network.

Step 7 Click **OK**.

Step 8 Preview and Deploy Configuration Changes for All Devices now the changes you made, or wait and deploy multiple changes at once.

Static Route Example

See the Static Route Network Diagram for the addresses used in this example.

The goal is to create a static route that allows return traffic to the host at 20.30.1.2 in destination network 20.30.1.0/24.

The packet can take any path to reach the destination. When a network receives a packet on an interface, it determines where to forward the packet for the best route to a destination.

Note The DMZ does not have a static route as it is connected directly to the interface.

For example, consider the following two routes for reaching the destination.

Route 1:

Procedure

Step 1 Packets come back to the outside interface, **209.165.201.0/27**, looking for **20.30.1.2.**

Step 2 We direct the packets to use the **inside** interface to get to the gateway 192.168.1.2, which is on the same network as the destination.

Step 3 From there, we identify the destination network by the **gateway address** for that network, 20.30.1.1.

Step 4 The IP address 20.30.1.2 is on the same subnet as 20.30.1.1. The router forwards the packet to the switch, the switch forwards the packet to 20.30.1.2.

Interface:Inside Destination_N/W:20.30.1.0/24 Gateway: 192.168.1.2 Metric: 1

Route 2:

Procedure

Step 1 Packets come back to the outside interface, **209.165.201.0/27**, looking for **20.30.1.2**.

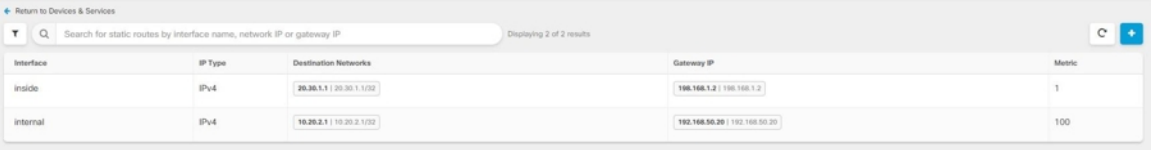
Step 2 We direct the packets to use the **internal** interface to get to the gateway 192.168.50.20, which is multiple hops away from the destination network.

Step 3 From there, we identify the destination network by the **gateway address** for that network, 20.30.1.1.

Step 4 The IP address 20.30.1.2 is on the same subnet as 20.30.1.0. The router forwards the packet to the switch, the switch forwards the packet to 20.30.1.2.

Interface:Inside Destination_N/W:20.30.1.0/24 Gateway: 192.168.50.20 Metric: 100

Here is what the completed Add Static Route table would like for these routes.



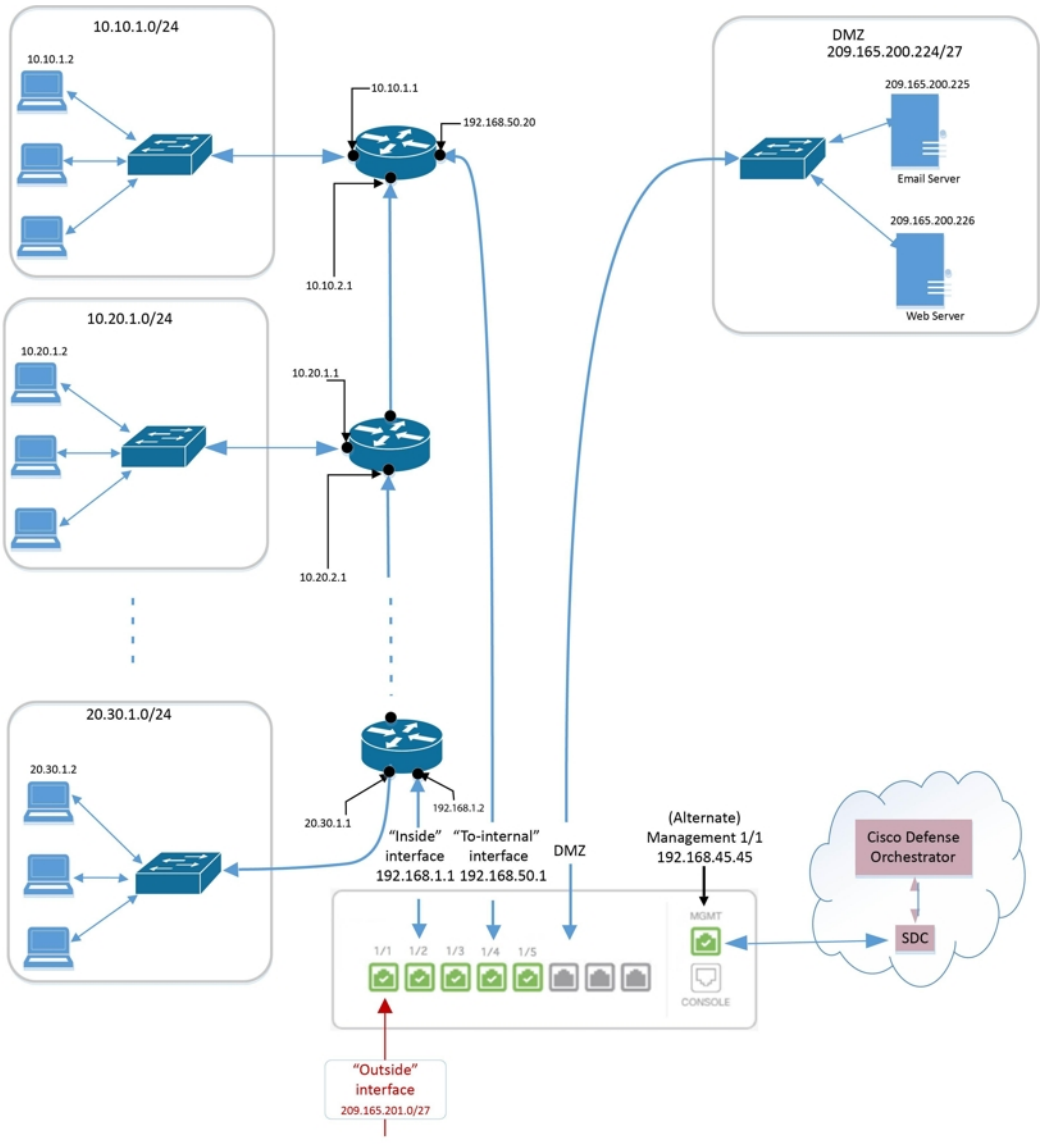
Monitoring Routing

To monitor and troubleshoot routing, open Firewall Device Manager for the device and open the CLI console or log into the device CLI using SSH and use the following commands:

- `show route` displays the routing table for the data interfaces, including routes for directly-connected networks.
- `show ipv6 route` displays the IPv6 routing table for the data interfaces, including routes for directly-connected networks.
- `show network` displays the configuration for the virtual management interface, including the management gateway. Routing through the virtual interface is not handled by the data interface routing table, unless you specify data-interfaces as the management gateway.
- `show network-static-routes` displays static routes configured for the virtual management interface using the `configure network static-routes` command. Normally, there will not be any static routes, as the management gateway suffices for management routing in most cases. These routes are not available to traffic on the data interfaces. This command is not available in the CLI console.

Static Route Network Diagram

We refer to this network diagram when discussing Configure Static and Default Routes for FDM-Managed Devices:



About Virtual Routing and Forwarding

About VRF

Virtual routing and forwarding (VRF) allow multiple instances of a routing table to exist in a router. Firepower Version 6.6 introduces the ability to have a default VRF table and user-created VRF tables. A single VRF table can handle multiple types of varying routing protocols, such as EX, OSPF, BGP, IGRP, etc. Each routing protocol within a VRF table is listed as an entry. In addition to handling multiple types of common routing protocols, you can configure a routing protocol to reference an interface from another VRF. This allows you to segment network paths without using multiple devices.

See About Virtual Routers and Virtual Routing and Forwarding (VRF) for more information.

VRF in Cisco Defense Orchestrator

This feature is new to Firepower Version 6.6. When the FDM-managed device is onboarded to CDO, the device routing page reads and supports only the VRFs defined on the global router of the FDM-managed device. To view the global VRF in CDO, select the device from the **Inventory** page and select **Routing** from the **Management** pane located to the right of the window. From here, you can view, modify, and delete the global VRF; note that CDO retains the name of the VRF when reading the configuration from FDM.

CDOfirewall device manager doesn't read VRFs configured in the user-defined virtual routers. You must create and manage VRF tables through firewall device manager.

For information on global and user-defined routes, see the "Managing Virtual Routers" section in the "Virtual Routers" chapter of Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager, Version 7.0 or later.

Objects

An object is a container of information that you can use in one or more security policies. Objects make it easy to maintain policy consistency. You can create a single object, use it different policies, modify the object, and that change is propagated to every policy that uses the object. Without objects, you would need to modify all the policies, individually, that require the same change.

When you onboard a device, CDO recognizes all the objects used by that device, saves them, and lists them on the **Objects** page. From the **Objects** page, you can edit existing objects and create new ones to use in your security policies.

CDO calls an object used on multiple devices a **shared object** and identifies them in the **Objects** page with this badge .

Sometimes a shared object develops some "issue" and is no longer perfectly shared across multiple policies or devices:

- **Duplicate objects** are two or more objects on the same device with different names but the same values. These objects usually serve similar purposes and are used by different policies. Duplicate objects are identified by this issue icon:
- **Inconsistent objects** are objects on two or more devices with the same name but different values. Sometimes users create objects in different configurations with same name and content but over time the values of these objects diverge which creates the inconsistency. Inconsistent objects are identified by this issue icon:
- **Unused objects** are objects that exist in a device configuration but are not referenced by another object, an access-list, or a NAT rule. Unused objects are identified by this issue icon:

You can also create objects for immediate use in rules or policies. You can create an object that is unassociated with any rule or policy.

You can view the objects managed by CDO by navigating to the **Objects** menu or by viewing them in the details of a network policy.

CDO allows you to manage network and service objects across supported devices from one location. With CDO, you can manage objects in these ways:

- Search for and filter all your objects based on a variety of criteria.

- Find duplicate, unused, and inconsistent objects on your devices and consolidate, delete, or resolve those object issues.
- Find unassociated objects and delete them if they are unused.
- Discover shared objects that are common across devices.
- Evaluate the impact of changes to an object on a set of policies and devices before committing the change.
- Compare a set of objects and their relationships with different policies and devices.
- Capture objects in use by a device after it has been on-boarded to CDO.

If you have issues with creating, editing, or reading objects from an onboarded device, see Troubleshoot Cisco Defense Orchestrator for more information.

Objects

An object is a container of information that you can use in one or more security policies. Objects make it easy to maintain policy consistency. You can create a single object, use it different policies, modify the object, and that change is propagated to every policy that uses the object. Without objects, you would need to modify all the policies, individually, that require the same change.

When you onboard a device, CDO recognizes all the objects used by that device, saves them, and lists them on the **Objects** page. From the **Objects** page, you can edit existing objects and create new ones to use in your security policies.

CDO calls an object used on multiple devices a **shared object** and identifies them in the **Objects** page with this badge .

Sometimes a shared object develops some "issue" and is no longer perfectly shared across multiple policies or devices:

- **Duplicate objects** are two or more objects on the same device with different names but the same values. These objects usually serve similar purposes and are used by different policies. Duplicate objects are identified by this issue icon:
- **Inconsistent objects** are objects on two or more devices with the same name but different values. Sometimes users create objects in different configurations with same name and content but over time the values of these objects diverge which creates the inconsistency. Inconsistent objects are identified by this issue icon:
- **Unused objects** are objects that exist in a device configuration but are not referenced by another object, an access-list, or a NAT rule. Unused objects are identified by this issue icon:

You can also create objects for immediate use in rules or policies. You can create an object that is unassociated with any rule or policy.

You can view the objects managed by CDO by navigating to the **Objects** menu or by viewing them in the details of a network policy.

CDO allows you to manage network and service objects across supported devices from one location. With CDO, you can manage objects in these ways:

- Search for and filter all your objects based on a variety of criteria.

- Find duplicate, unused, and inconsistent objects on your devices and consolidate, delete, or resolve those object issues.
- Find unassociated objects and delete them if they are unused.
- Discover shared objects that are common across devices.
- Evaluate the impact of changes to an object on a set of policies and devices before committing the change.
- Compare a set of objects and their relationships with different policies and devices.
- Capture objects in use by a device after it has been on-boarded to CDO.

If you have issues with creating, editing, or reading objects from an onboarded device, see Troubleshoot Cisco Defense Orchestrator for more information.

Object Types

The following table describes the objects that you can create for your devices and manage using CDO.

Table 1: FDM-Managed Device Object Types

Object	Description
Application Filter	An application filter object defines the applications used in an IP connection, or a filter that defines applications by type, category, tag, risk, or business relevance. You can use these objects in policies to control traffic instead of using port specifications.
Upload RA VPN AnyConnect Client Profile	AnyConnect Client Profile objects are file objects and represent files used in configurations, typically for remote access VPN policies. They can contain an AnyConnect Client Profile and AnyConnect Client Image files.
Certificate Filter	Digital certificates provide digital identification for authentication. Certificates are used for SSL (Secure Socket Layer), TLS (Transport Layer Security), and DTLS (Datagram TLS) connections, such as HTTPS and LDAPS.
DNS Group	DNS servers are needed to resolve fully-qualified domain names (FQDN), such as www.example.com, to IP addresses. You can configure different DNS group objects for management and data interfaces.
Geolocation	A geolocation object defines countries and continents that host the device that is the source or destination of traffic. You can use these objects in policies to control traffic instead of using IP addresses.
IKEv1 Policy	An IKEv1 policy object contain the parameters required for IKEv1 policies when defining VPN connections.

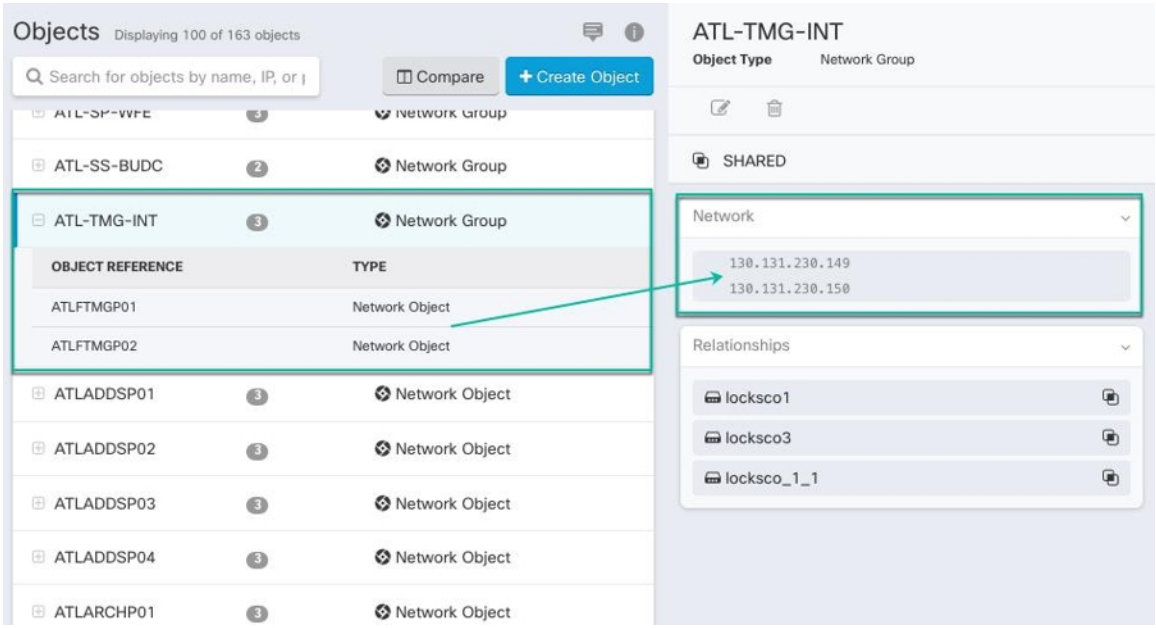
Object	Description
IKEv2 Policy	An IKEv2 policy objects contain the parameters required for IKEv2 policies when defining VPN connections.
IKEv1 IPSEC Proposal	IPsec Proposal objects configure the IPsec proposal used during IKE Phase 1 negotiations. The IPsec proposal defines the combination of security protocols and algorithms that secure traffic in an IPsec tunnel.
IKEv2 IPSEC Proposal	IPsec Proposal objects configure the IPsec proposal used during IKE Phase 2 negotiations. The IPsec proposal defines the combination of security protocols and algorithms that secure traffic in an IPsec tunnel.
Network	Network groups and network objects (collectively referred to as network objects) define the addresses of hosts or networks.
Security Zone	A security zone is a grouping of interfaces. Zones divide the network into segments to help you manage and classify traffic.
Service	Service objects, service groups, and port groups are reusable components that contain protocols or ports considered part of the TCP/IP protocol suite.
SGT Group	A SGT dynamic object identifies source or destination addresses based on an SGT assigned by ISE and can then be matched against incoming traffic.
Syslog Server	A syslog server object identifies a server that can receive connection-oriented or diagnostic system log (syslog) messages.
URL	Use URL objects and groups (collectively referred to as URL objects) to define the URL or IP addresses of web requests. You can use these objects to implement manual URL filtering in access control policies or blocking in Security Intelligence policies.

Shared Objects

Cisco Defense Orchestrator (CDO) calls objects on multiple devices with the same name and same contents, **shared objects**. Shared objects are identified by this icon

on the **Objects** page. Shared objects make it easy to maintain policies because you can modify an object in one place and that change affects all the other policies that use that object. Without shared objects, you would need to modify all the policies individually that require the same change.

When looking at a shared object, CDO shows you the contents of the object in the object table. Shared objects have exactly the same contents. CDO shows you a combined or "flattened" view of the elements of the object in the details pane. Notice that in the details pane, the network elements are flattened into a simple list and not directly associated with a named object.

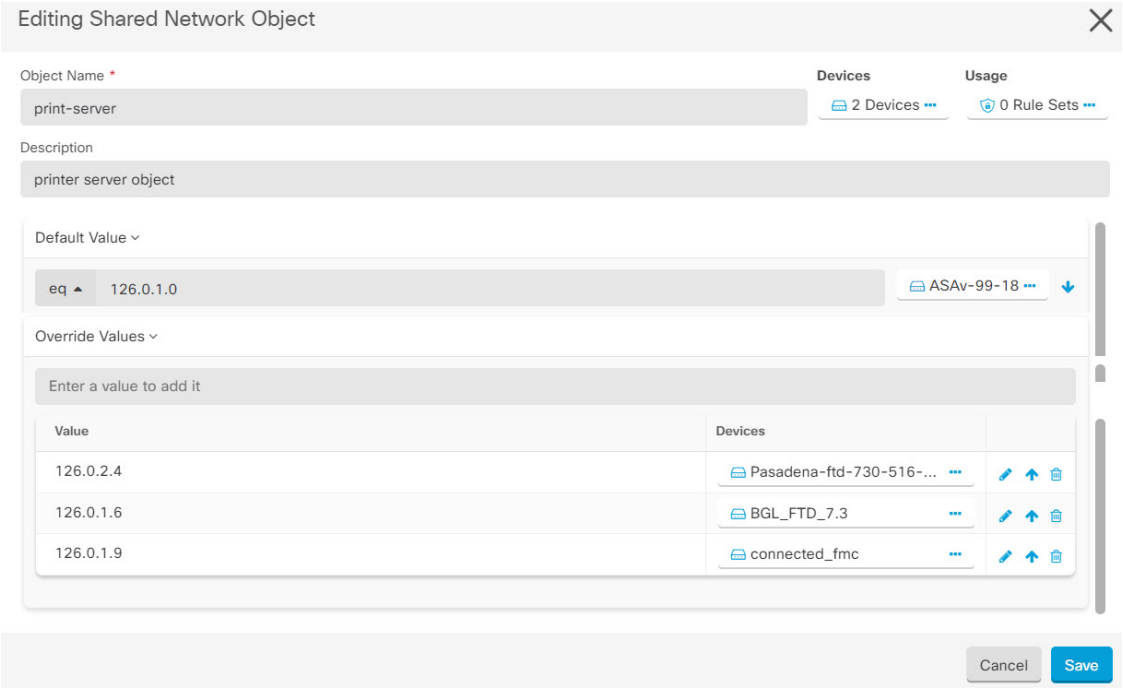


Object Overrides

An object override allows you to override the value of a shared network object on specific devices. CDO uses the corresponding value for the devices that you specify when configuring the override. Although the objects are on two or more devices with the same name but different values, CDO doesn't identify them as **Inconsistent objects** only because these values are added as overrides.

You can create an object whose definition works for most devices, and then use overrides to specify modifications to the object for the few devices that need different definitions. You can also create an object that needs to be overridden for all devices, but its use allows you to create a single policy for all devices. Object overrides allow you to create a smaller set of shared policies for use across devices without giving up the ability to alter policies when needed for individual devices.

For example, consider a scenario where you have a printer server in each of your offices, and you have created a printer server object `print-server`. You have a rule in your ACL to deny printer servers from accessing the internet. The printer server object has a default value that you want to change from one office to another. You can do this by using object overrides and maintain rule and "printer-server" object consistent across all locations, although their values may be different.



Note CDO allows you to override objects associated with the rules in a ruleset. When you add a new object to a rule, you can override it only after you attach a device to the ruleset and save the changes. See Configure Rulesets for a Device for more information.

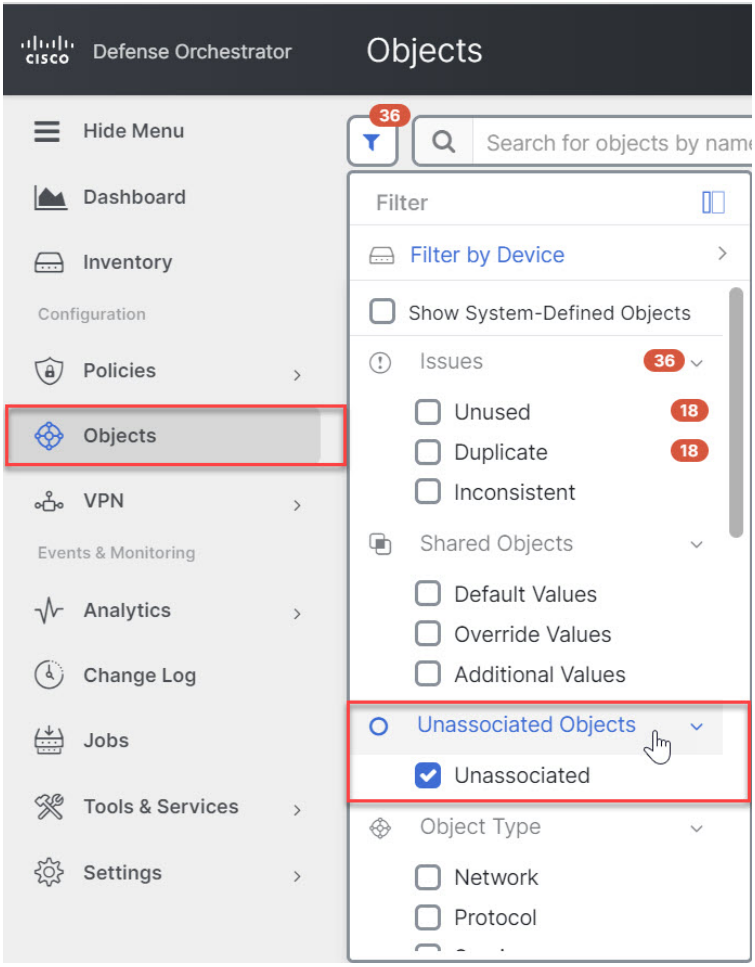
Note If there are inconsistent objects, you can combine them into a single shared object with overrides. See Resolve Inconsistent Object Issues for more information.

Unassociated Objects

You can create objects for immediate use in rules or policies. You can also create an object that is unassociated with any rule or policy. When you use that unassociated object in a rule or policy, CDO creates a copy of it and uses the copy. The original unassociated object remains among the list of available objects until it is either deleted by a nightly maintenance job, or you delete it.

Unassociated objects remain in CDO as a copy to ensure that not all configurations are lost if the rule or policy associated with the object is deleted accidentally.

To view unassociated objects click in the left-hand pane of the Objects tab and check the **Unassociated** checkbox.



Compare Objects

Procedure

Step 1 In the CDO navigation bar on the left, click **Objects** and choose an option.

Step 2 Filter the objects on the page to find the objects you want to compare.

Step 3 Click the **Compare** button 

.

Step 4 Select up to three objects to compare.

Step 5 View the objects, side-by-side, at the bottom of the screen.

- Click the up and down arrows in the Object Details title bar to see more or less of the Object Details.
- Expand or collapse the Details and Relationships boxes to see more or less information.

Step 6 (Optional) The Relationships box shows how an object is used. It may be associated with a device or a policy. If the object is associated with a device, you can click the device name and then click **View Configuration**

to see the configuration of the device. CDO shows you the device's configuration file and highlights the entry for that object.

Filters

You can use many different filters on the **Inventory** and **Objects** pages to find the devices and objects you are looking for.

To filter, click in the left-hand pane of the Inventory, Policies, and Objects tabs:

The Inventory filter allows you to filter by device type, hardware and software versions, snort version, configuration status, connection states, conflict detection, and secure device connectors, and labels. You can apply filters to find devices within a selected device type tab. You can use filters to find devices within the selected device type tab.

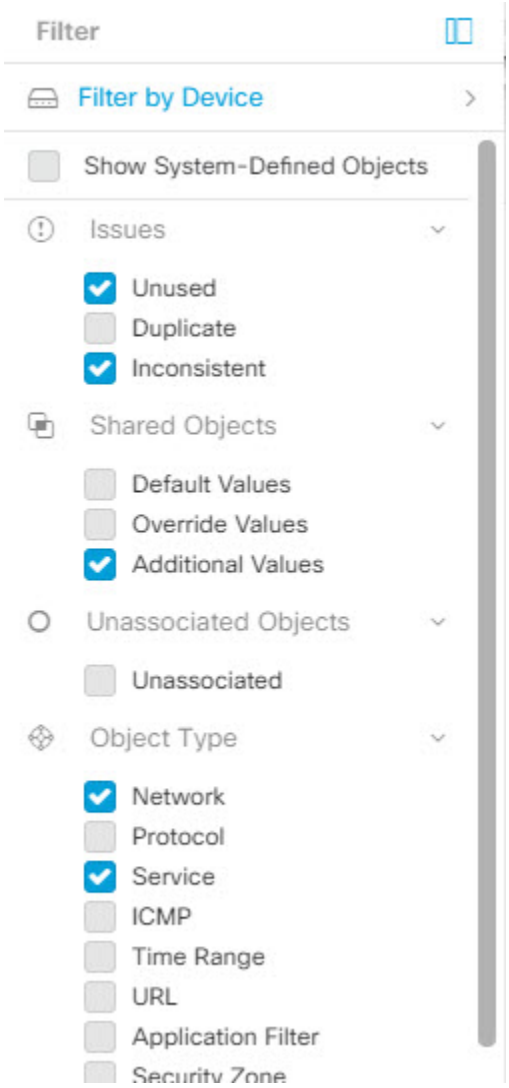
Note When the **FTD** tab is opened, the filter pane provides filters to show FDM-managed devices based on the management application through which the devices are accessed from CDO.

- FDM: Devices managed using FTD API or FDM.
- FMC-FTD: Devices managed using Firepower Management Center.
- FTD: Devices managed using FTD Management.

The object filter allows you to filter by device, issue type, shared objects, unassociated objects, and object type. You can include system objects in your results or not. You can also use the search field to search for objects in the filter results that contain a certain name, IP address, or port number.

When filtering devices and objects, you can combine your search terms to create several potential search strategies to find relevant results.

In the following example, filters are applied to search objects that are "Issues (Used OR Inconsistent) AND Shared Objects with Additional Values AND Objects of type Network OR Service.



Object Filters

To filter, click in the left-hand pane of the Objects tab:

- **All Objects** – This filter provides you all the objects available from all the devices you have on-boarded in CDO. This filter is useful to browse all your objects, or as a starting point to search or further apply sub-filters.
- **Shared Objects** – This quick filter shows you all the Objects that CDO has found to be shared on more than one device.
- **Objects By Device** – Lets you pick a specific device so that you can see objects found on the selected device.

Sub filters – Within each main filter, there are sub-filters you can apply to further narrow down your selection. These sub-filters are based on Object Type – Network, Service, Protocol, etc.

The selected filters in this filter bar would return objects that match the following criteria:

***** Objects that are on one of two devices. (Click **Filter by Device** to specify the devices.) AND are

*** Inconsistent** objects AND are

*** Network** objects OR **Service** objects AND

***** Have the word "**group**" in their object naming convention

Because **Show System Objects** is checked, the result would include both system objects and user-defined objects.

Show System Objects Filter

Some devices come with pre-defined objects for common services. These system objects are convenient because they are already made for you and you can use them in your rules and policies. There can be many system objects in the objects table. System objects cannot be edited or deleted.

Show System Objects is **off** by default. To display system objects in the object table, check **Show System Objects** in the filter bar. To hide system objects in the object table, leave Show System Objects unchecked in the filter bar.

If you hide system objects, they will not be included in your search and filtering results. If you show system objects, they will be included in your object search and filtering results.

Configure Object Filters

You can filter on as few or as many criteria as you want. The more categories you filter by, the fewer results you should expect.

Procedure

Step 1 In the CDO navigation bar on the left, click **Objects** and choose an option.

Step 2 Open the filter panel by clicking the filter icon at the top of the page. Uncheck any filters that have been checked to make sure no objects are inadvertently filtered out. Additionally, look at the search field and delete any text that may have been entered in the search field.

Step 3 If you want to restrict your results to those found on particular devices:

a. Click **Filter By Device**.

b. Search all the devices or click a device tab to search for only devices of a certain kind.

c. Check the device you want to include in your filter criteria.

d. Click **OK**.

Step 4 Check **Show System Objects** to include system objects in your search results. Uncheck **Show System Objects** to exclude system objects from your search results.

Step 5 Check the object **Issues** you want to filter by. If you check more than one issue, objects in any of the categories you check are included in your filter results.

Step 6 Check **Ignored** issues if you want to see the object that had issues but was ignored by the administrator.

Step 7 Check the required filter in **Shared Objects** if you are filtering for objects shared between two or more devices.

- **Default Values**: Filters objects having only the default values.

- **Override Values**: Filters objects having overridden values.
- **Additional Values**: Filters objects having additional values.

Step 8 Check **Unassociated** if you are filtering for objects that are not part of any rule or policy.

Step 9 Check the **Object Types** you want to filter by.

Step 10 You can also add an object name, IP address, or port number to the Objects search field to find objects with your search criteria among the filtered results.

When to Exclude a Device from Filter Criteria

When adding a device to filtering criteria, the results show you the objects on a device but not the relationships of those objects to other devices. For example, assume **ObjectA** is shared between ASA1 and ASA2. If you were to filter objects to find shared objects on ASA1, you would find **ObjectA** but the **Relationships** pane would only show you that the object is on ASA1.

To see all the devices to which an object is related, don't specify a device in your search criteria. Filter by the other criteria and add search criteria if you choose to. Select an object that CDO identifies and then look in the Relationships pane. You will see all the devices and policies the object is related to.

Unignore Objects

One way to resolve unused, duplicate, or inconsistent objects is to ignore them. You may decide that though an object is unused, a duplicate, or inconsistent, there are valid reasons for that state and you choose to leave the object issue unresolved. At some point in the future, you may want to resolve those ignored objects. As CDO does not display ignored objects when you search for object issues, you will need to filter the object list for ignored objects and then act on the results.

Procedure

Step 1 In the CDO navigation bar on the left, click **Objects** and choose an option.

Step 2 Filter and search for ignored objects.

Step 3 In the **Object** table, select the object you want to unignore. You can unignore one object at a time.

Step 4 Click **Unignore** in the details pane.

Step 5 Confirm your request. Now, when you filter your objects by issue, you should find the object that was previously ignored.

Deleting Objects

You can delete a single object or mulitple objects.

Delete a Single Object

Caution If cloud-delivered Firewall Management Center is deployed on your tenant:

Changes you make to network objects and groups on the or **Objects > FDM Objects** page are reflected in the corresponding cloud-delivered Firewall Management Center network object or group on the **Objects > Other FTD Objects** page. In addition, an entry is created in the **Devices with Pending Changes** page for each on-prem management center with **Discover & Manage Network Objects** enabled, from which you can choose and deploy the changes to the on-prem management center on which you have these objects.

Deleting a network object or group from either page deletes the object or group from both pages.

Procedure

Step 1 In the CDO navigation bar on the left, choose **Objects** and choose an option.

Step 2 Locate the object you want to delete by using object filters and the search field, and select it.

Step 3 Review the **Relationships** pane. If the object is used in a policy or in an object group, you cannot delete the object until you remove it from that policy or group.

Step 4 In the Actions pane, click the **Remove** icon .

Step 5 Confirm that you want to delete the object by clicking **OK**.

Step 6 Preview and Deploy Configuration Changes for All Devices the changes you made, or wait and deploy multiple changes at once.

Delete a Group of Unused Objects

As you onboard devices and start resolving object issues, you find many unused objects. You can delete up to 50 unused objects at a time.

Procedure

Step 1 Use the **Issues** filter to find **unused** objects. You can also use the Device filter to find objects that are not associated with a device by selecting **No Device**. Once you have filtered the object list, the object checkboxes appear.

Step 2 Check the **Select all** checkbox in the object table header to select all the objects found by the filter that appear in the object table; or, check individual checkboxes for individual objects you want to delete.

Step 3 In the Actions pane, click the **Remove** icon .

Step 4 Preview and Deploy Configuration Changes for All Devices now the changes you made, or wait and deploy multiple changes at once.

Network Objects

A network object can contain a host name, a network IP address, a range of IP addresses, a fully qualified domain name (FQDN), or a subnetwork expressed in CIDR notation. **Network groups** are collections of

network objects and other individual addresses or subnetworks you add to the group. Network objects and network groups are used in access rules, network policies, and NAT rules. You can create, update, and delete network objects and network groups using CDO.

Table 2: Pemitted Values of Network Objects

Device type	IPv4 / IPv6	Single Address	Range of addresses	Fully Qualified Domain Name	Subnet using CIDR Notation
FTD	IPv4 and IPv6	Yes	Yes	Yes	Yes

Table 3: Pemitted Contents of a Network Group

Device type	IP Value	Network Object	Network Groups
FTD	No	Yes	Yes

Reusing Network Objects Across Products

If you have a Cisco Defense Orchestrator tenant with a cloud-delivered Firewall Management Center and one or more on-prem management centers onboarded to your tenant:

- When you create a Secure Firewall Threat Defense, FDM-managed threat defense, ASA, or Meraki network object or group, a copy of the object is also added to the objects list on the **Objects > Other FTD Objects** page used when configuring cloud-delivered Firewall Management Center, and vice versa.
- When you create a Secure Firewall Threat Defense, FDM-managed threat defense, or ASA network object or group, an entry is created in the **Devices with Pending Changes** page for each On-Prem Firewall Management Center for which **Discover & Manage Network Objects** is enabled. From this list, you can choose and deploy the object to the on-prem management center on which you want to use the object and discard the ones that you do not want. Navigate **Tools & Services** > **Firewall Management Center**, select the on-prem management center, and click **Objects** to see your objects in the On-Prem Firewall Management Center user interface and assign them to policies.

Changes you make to network objects or groups on either page apply to the object or group instance on both pages. Deleting an object from one page also deletes the corresponding copy of the object from the other page.

Exceptions:

- If a network object of the same name already exists for cloud-delivered Firewall Management Center, the new Secure Firewall Threat Defense, FDM-managed threat defense, ASA, or Meraki network object will not be replicated on the **Objects > Other FTD Objects** page of Cisco Defense Orchestrator
- Network objects and groups in onboarded threat defense devices that are managed by on-premises Secure Firewall Management Center are not replicated on the **Objects > Other FTD Objects** page and cannot be used in cloud-delivered Firewall Management Center.

  Note that for on-premises Secure Firewall Management Center instances that have been *migrated* to cloud-delivered Firewall Management Center, network objects and groups *are* replicated to the CDO objects page if they are used in policies that were deployed to FTD devices.
- Sharing Network Objects between CDO and cloud-delivered Firewall Management Center is automatically enabled on new tenants but must be requested for existing tenants. If your network objects are not being shared with cloud-delivered Firewall Management Center, contact TAC to have the features enabled on your tenant.

- Sharing network objects between CDO and On-Prem Management Center is not automatically enabled on CDO for new on-prem management centers onboarded to CDO. If your network objects are not being shared with On-Prem Management Center, ensure **Discover & Manage Network Objects** toggle button is enabled for the on-prem management center in **Settings** or contact TAC to have the features enabled on your tenant.

Viewing Network Objects

Network objects you create using CDO and those CDO recognizes in an onboarded device's configuration are displayed on the Objects page. They are labeled with their object type. This allows you to filter by object type to quickly find the object you are looking for.

When you select a network object on the Objects page, you see the object's values in the Details pane. The Relationships pane shows you if the object is used in a policy and on what device the object is stored.

When you click on a network group you see the contents of that group. The network group is a conglomerate of all the values given to it by the network objects.

Related Information:

- Create or Edit a Firepower Network Object or Network Group

Create or Edit a Firepower Network Object or Network Groups

A Firepower network object can contain a hostname, an IP address, or a subnet address expressed in CIDR notation. **Network groups** are conglomerates of network objects and network groups that are used in access rules, network policies, and NAT rules. You can create, read, update, and delete network objects and network groups using Cisco Defense Orchestrator (CDO).

Firepower network objects and groups can be used by ASA, threat defense, FDM-managed, and Meraki devices. See Reusing Network Objects Across Products.

Note If cloud-delivered Firewall Management Center is deployed on your tenant:

When you create a network object or group on the or **Objects > FDM Objects** page, a copy of the object is automatically added to the **Objects > Other FTD Objects** page and vice-versa. In addition, an entry is created in the **Devices with Pending Changes** page for each on-prem management center with **Discover & Manage Network Objects** enabled, from which you can choose and deploy the objects to the on-prem management center on which you want these objects.

Caution If cloud-delivered Firewall Management Center is deployed on your tenant:

Changes you make to network objects and groups on the or **Objects > FDM Objects** page are reflected in the corresponding cloud-delivered Firewall Management Center network object or group on the **Objects > Other FTD Objects** page. In addition, an entry is created in the **Devices with Pending Changes** page for each on-prem management center with **Discover & Manage Network Objects** enabled, from which you can choose and deploy the changes to the on-prem management center on which you have these objects.

Deleting a network object or group from either page deletes the object or group from both pages.

Table 4: IP addresses that can be added to network objects

Device type	IPv4 / IPv6	Single Address	Range of addresses	Partially Qualified Domain Name (PQDN)	Subnet using CIDR Notation
Firepower	IPv4 / IPv6	Yes	Yes	Yes	Yes

Related Information:

- Create a Firepower Network Object
- Edit a Firepower Network Object
- Add Additional Values to a Shared Network Group
- Edit Additional Values in a Shared Network Group

Create a Firepower Network Object

Note If cloud-delivered Firewall Management Center is deployed on your tenant:

When you create a network object or group on the or **Objects > FDM Objects** page, a copy of the object is automatically added to the **Objects > Other FTD Objects** page and vice-versa. In addition, an entry is created in the **Devices with Pending Changes** page for each on-prem management center with **Discover & Manage Network Objects** enabled, from which you can choose and deploy the objects to the on-prem management center on which you want these objects.

Procedure

Step 1 In the CDO navigation bar on the left, click **Objects > FDM Objects**.

Step 2 Click the blue plus button to create an object.

Step 3 Click **FTD** > **Network**.

Step 4 Enter an **Object Name**.

Step 5 Select **Create a network object**.

Step 6 In the **Value** section:

- Select **eq** and enter a single IP address, a subnet address expressed in CIDR notation, or a Partially Qualified Domain Name (PQDN).
- Select **range** and enter an IP address range.

Note Do not set a host bit value. If you enter a host bit value other than 0, CDO unsets it while creating the object, because the cloud-delivered Firewall Management Center only accepts IPv6 objects with host bits not set.

Step 7 Click **Add**.

Attention: The newly created network objects aren't associated with any FDM-managed device as they aren't part of any rule or policy. To see these objects, select the **Unassociated** objects category in object filters. For more information, see Object Filters. Once you use the unassociated objects in a device's rule or policy, such objects are associated with that device.

Create a Firepower Network Group

A **network group** can contain network objects and network groups. When you create a new network group, you can search for existing objects by their name, IP addresses, IP address range, or FQDN and add them to the network group. If the object isn't present, you can instantly create that object in the same interface and add it to the network group.

Note If cloud-delivered Firewall Management Center is deployed on your tenant:

When you create a network object or group on the or **Objects > FDM Objects** page, a copy of the object is automatically added to the **Objects > Other FTD Objects** page and vice-versa. In addition, an entry is created in the **Devices with Pending Changes** page for each on-prem management center with **Discover & Manage Network Objects** enabled, from which you can choose and deploy the objects to the on-prem management center on which you want these objects.

Procedure

Step 1 In the CDO navigation bar on the left, click **Objects > FDM Objects**.

Step 2 Click the blue plus button to create an object.

Step 3 Click **FTD** > **Network**.

Step 4 Enter an **Object Name**.

Step 5 Select **Create a network group**.

Step 6 In the **Values** field, enter a value or name. When you start typing, CDO provides object names or values that match your entry.

Step 7 You can choose one of the existing objects shown or create a new one based on the name or value that you have entered.

Step 8 If CDO finds a match, to choose an existing object, click **Add** to add the network object or network group to the new network group.

Step 9 If you have entered a value or object that is not present, you can perform one of the following:

- Click **Add as New Object With This Name** to create a new object with that name. Enter a value and click the checkmark to save it.
- Click **Add as New Object** to create a new object. The object name and value are the same. Enter a name and click the checkmark to save it.

It's is possible to create a new object even though the value is already present. You can make changes to those objects and save them.

Note: You can click the edit icon to modify the details. Clicking the delete button doesn't delete the object itself; instead, it removes it from the network group.

Step 10 After adding the required objects, click **Save** to create a new network group.

Step 11 Preview and Deploy Configuration Changes for All Devices.

Edit a Firepower Network Object

Caution If cloud-delivered Firewall Management Center is deployed on your tenant:

Changes you make to network objects and groups on the or **Objects > FDM Objects** page are reflected in the corresponding cloud-delivered Firewall Management Center network object or group on the **Objects > Other FTD Objects** page. In addition, an entry is created in the **Devices with Pending Changes** page for each on-prem management center with **Discover & Manage Network Objects** enabled, from which you can choose and deploy the changes to the on-prem management center on which you have these objects.

Deleting a network object or group from either page deletes the object or group from both pages.

Procedure

Step 1 In the CDO navigation bar on the left, click **Objects > FDM Objects**.

Step 2 Locate the object you want to edit by using object filters and search field.

Step 3 Select the network object and click the edit icon  in the **Actions** pane.

Step 4 Edit the values in the dialog box in the same fashion that you created them in "Create a Firepower Network Group".

Note Click the delete icon next to remove the object from the network group.

Step 5 Click **Save**. CDO displays the devices that will be affected by the change.

Step 6 Click **Confirm** to finalize the change to the object and any devices affected by it.

Edit a Firepower Network Group

Caution If cloud-delivered Firewall Management Center is deployed on your tenant:

Changes you make to network objects and groups on the or **Objects > FDM Objects** page are reflected in the corresponding cloud-delivered Firewall Management Center network object or group on the **Objects > Other FTD Objects** page. In addition, an entry is created in the **Devices with Pending Changes** page for each on-prem management center with **Discover & Manage Network Objects** enabled, from which you can choose and deploy the changes to the on-prem management center on which you have these objects.

Deleting a network object or group from either page deletes the object or group from both pages.

Procedure

Step 1 In the CDO navigation bar on the left, click **Objects** > **FDM Objects**.

Step 2 Locate the network group you want to edit by using object filters and search field.

Step 3 Select the network group and click the edit icon in the **Actions** pane.

Step 4 Change the object name and description if needed.

Step 5 If you want to change the objects or network groups that are already added to the network group, perform the following steps:

a. Click the edit icon appearing beside the object name or network group to modify them.

b. Click the checkmark to save your changes. **Note**: You can click the remove icon to delete the value from a network group.

Step 6 If you want to add new network objects or network groups to this network group, you have to perform the following steps:

a. In the **Values** field, enter a new value or the name of an existing network object. When you start typing, CDO provides object names or values that match your entry. You can choose one of the existing objects shown or create a new one based on the name or value that you have entered.

b. If CDO finds a match, to choose an existing object, click **Add** to add the network object or network group to the new network group.

c. If you have entered a value or object that is not present, you can perform one of the following:

- Click **Add as New Object With This Name** to create a new object with that name. Enter a value and click the checkmark to save it.
- Click **Add as New Object** to create a new object. The object name and value are the same. Enter a name and click the checkmark to save it.

It's is possible to create a new object even though the value is already present. You can make changes to those objects and save them.

Step 7 Click **Save**. CDO displays the policies that will be affected by the change.

Step 8 Click **Confirm** to finalize the change to the object and any devices affected by it.

Step 9 Preview and Deploy Configuration Changes for All Devices.

Add an Object Override

Caution If cloud-delivered Firewall Management Center is deployed on your tenant:

Changes you make to network objects and groups on the or **Objects > FDM Objects** page are reflected in the corresponding cloud-delivered Firewall Management Center network object or group on the **Objects > Other FTD Objects** page. In addition, an entry is created in the **Devices with Pending Changes** page for each on-prem management center with **Discover & Manage Network Objects** enabled, from which you can choose and deploy the changes to the on-prem management center on which you have these objects.

Deleting a network object or group from either page deletes the object or group from both pages.

Procedure

Step 1 In the CDO navigation bar on the left, click **Objects > FDM Objects**.

Step 2 Locate the object to which you want to add an override, using object filters and search field.

Step 3 Select the network object and click the edit icon in the **Actions** pane.

Step 4 Enter the value in the **Override Values** dialog box and click **+ Add Value**.

Important The override you are adding must have the same type of value that the object contains. For example, to a network object, you can configure an override only with a network value and not a host value.

Step 5 Once you see that the value is added, click the cell in the **Devices** column in **Override Values**.

Step 6 Click **Add Devices**, and choose the device to which you want the override to be added. The device you select must contain the object to which you are adding the override.

Step 7 Click **Save**. CDO displays the devices that will be affected by the change.

Step 8 Click **Confirm** to finalize the addition of the override to the object and any devices affected by it.

Note You can add more than one override to an object. However, you must select a different device, which contains the object, each time you are adding an override.

Step 9 See Object Overrides to know more about object overrides and Edit Object Overrides to edit an existing override.

Edit Object Overrides

You can modify the value of an existing override as long as the object is present on the device.

Procedure

Step 1 In the CDO navigation bar on the left, click **Objects > FDM Objects**.

Step 2 Locate the object having override you want to edit by using object filters and search field.

Step 3 Select the object having override and click the edit icon in the Actions pane.

Step 4 Modify the override value:

- Click the edit icon to modify the value.
- Click on the cell in the **Devices** column in **Override Values** to assign new devices. You can select an already assigned device and click **Remove Overrides** to remove overrides on that device.
- Click arrow in **Override Values** to push and make it as the default value of the shared object.
- Click the delete icon next to the override you want to remove.

Step 5 Click **Save**. CDO displays the devices that will be affected by the change.

Step 6 Click **Confirm** to finalize the change to the object and any devices affected by it.

Step 7 Preview and Deploy Configuration Changes for All Devices.

Add Additional Values to a Shared Network Group

The values in a shared network group that are present on all devices associated with it are called "default values". CDO allows you to add "additional values" to the shared network group and assign those values to some devices associated with that shared network group. When CDO deploys the changes to the devices, it determines the contents and pushes the "default values" to all devices associated with the shared network group and the "additional values" only to the specified devices.

For example, consider a scenario where you have four AD main servers in your head office that should be accessible from all your sites. Therefore, you have created an object group named "Active-Directory" to use in all your sites. Now you want to add two more AD servers to one of your branch offices. You can do this by adding their details as additional values specific to that branch office on the object group "Active-Directory". These two servers do not participate in determining whether the object "Active-Directory" is consistent or shared. Therefore, the four AD main servers are accessible from all your sites, but the branch office (with two additional servers) can access two AD servers and four AD main servers.

Note If there are inconsistent shared network groups, you can combine them into a single shared network group with additional values. See Resolve Inconsistent Object Issues for more information.

Caution If cloud-delivered Firewall Management Center is deployed on your tenant:

Changes you make to network objects and groups on the or **Objects > FDM Objects** page are reflected in the corresponding cloud-delivered Firewall Management Center network object or group on the **Objects > Other FTD Objects** page. In addition, an entry is created in the **Devices with Pending Changes** page for each on-prem management center with **Discover & Manage Network Objects** enabled, from which you can choose and deploy the changes to the on-prem management center on which you have these objects.

Deleting a network object or group from either page deletes the object or group from both pages.

Procedure

Step 1 In the CDO navigation bar on the left, click **Objects > FDM Objects**.

Step 2 Locate the shared network group you want to edit by using object filters and search field.

Step 3 Click the edit icon in the **Actions** pane.

- The **Devices** field shows the devices the shared network group is present.
- The **Usage** field shows the rulesets associated with the shared network group.
- The **Default Values** field specifies the default network objects and their values associated with the shared network group that was provided during their creation. Next to this field, you can see the number of devices that contain this default value, and you can click to see their names and device types. You can also see the rulesets associated with this value.

Step 4 In the **Additional Values** field, enter a value or name. When you start typing, CDO provides object names or values that match your entry.

Step 5 You can choose one of the existing objects shown or create a new one based on the name or value that you have entered.

Step 6 If CDO finds a match, to choose an existing object, click **Add** to add the network object or network group to the new network group.

Step 7 If you have entered a value or object that is not present, you can perform one of the following:

- Click **Add as New Object With This Name** to create a new object with that name. Enter a value and click the checkmark to save it.
- Click **Add as New Object** to create a new object. The object name and value are the same. Enter a name and click the checkmark to save it.

It's is possible to create a new object even though the value is already present. You can make changes to those objects and save them.

Step 8 In the **Devices** column, click the cell associated with the newly added object and click **Add Devices**.

Step 9 Select the devices that you want and click **OK**.

Step 10 Click **Save**. CDO displays the devices that will be affected by the change.

Step 11 Click **Confirm** to finalize the change to the object and any devices affected by it.

Step 12 Preview and Deploy Configuration Changes for All Devices.

Edit Additional Values in a Shared Network Group

Caution If cloud-delivered Firewall Management Center is deployed on your tenant:

Changes you make to network objects and groups on the or **Objects > FDM Objects** page are reflected in the corresponding cloud-delivered Firewall Management Center network object or group on the **Objects > Other FTD Objects** page. In addition, an entry is created in the **Devices with Pending Changes** page for each on-prem management center with **Discover & Manage Network Objects** enabled, from which you can choose and deploy the changes to the on-prem management center on which you have these objects.

Deleting a network object or group from either page deletes the object or group from both pages.

Procedure

Step 1 In the CDO navigation bar on the left, click **Objects** > **FDM Objects**.

Step 2 Locate the object having the override you want to edit by using object filters and search field.

Step 3 Click the edit icon in the **Actions** pane.

Step 4 Modify the override value:

- Click the edit icon to modify the value.
- Click the cell in the **Devices** column to assign new devices. You can select an already assigned device and click **Remove Overrides** to remove overrides on that device.
- Click arrow in **Default Values** to push and make it an additional value of the shared network group. All devices associated with the shared network group are automatically assigned to it.
- Click arrow in **Override Values** to push and make it as default objects of the shared network group.
- Click the delete icon next to remove the object from the network group.

Step 5 Click **Save**. CDO displays the devices that will be affected by the change.

Step 6 Click **Confirm** to finalize the change to the object and any devices affected by it.

Step 7 Preview and Deploy Configuration Changes for All Devices.

Deleting Network Objects and Groups in CDO

If Cloud-delivered Firewall Management Center is deployed on your tenant:

Deleting a network object or group from the or **Objects** > **FDM Objects** page deletes the replicated network object or group from the **Objects** > **Other FTD Objects** page and vice-versa.

URL Objects

URL objects and URL groups are used by Firepower devices. Use URL objects and groups (collectively referred to as URL objects) to define the URL or IP addresses of web requests. You can use these objects to implement manual URL filtering in access control policies or blocking in Security Intelligence policies. A URL object defines a single URL or IP address, whereas a URL group defines more than one URL or IP address.

Before You Begin

When creating URL objects, keep the following points in mind:

- If you do not include a path (that is, there is no / character in the URL), the match is based on the server's hostname only. The hostname is considered a match if it comes after the :// separator, or after any dot in the hostname. For example, ign.com matches ign.com and www.ign.com, but it does not match verisign.com.
- If you include one or more / character, the entire URL string is used for a substring match, including the server name, path, and any query parameters. However, we recommend that you do not use manual URL filtering to block or allow individual web pages or parts of sites, as servers can be reorganized and pages

moved to new paths. Substring matching can also lead to unexpected matches, where the string you include in the URL object also matches paths on unintended servers or strings within query parameters.

- The system disregards the encryption protocol (HTTP vs HTTPS). In other words, if you block a website, both HTTP and HTTPS traffic to that website is blocked, unless you use an application condition to target a specific protocol. When creating a URL object, you do not need to specify the protocol when creating an object. For example, use example.com rather than http://example.com.
- If you plan to use a URL object to match HTTPS traffic in an access control rule, create the object using the subject common name in the public key certificate used to encrypt the traffic. Also, the system disregards subdomains within the subject common name, so do not include subdomain information. For example, use example.com rather than www.example.com.

  However, please understand that the subject common name in the certificate might be completely unrelated to a web site's domain name. For example, the subject common name in the certificate for youtube.com is *.google.com (this of course might change at any time). You will get more consistent results if you use the SSL Decryption policy to decrypt HTTPS traffic so that URL filtering rules work on decrypted traffic.

Note URL objects will not match HTTPS traffic if the browser resumes a TLS session because the certificate information is no longer available. So even if you carefully configure the URL object, you might get inconsistent results for HTTPS connections.

Create or Edit an FDM-Managed URL Object

URL objects are reusable components that specify a URL or IP address.

To create a URL object, follow these steps:

Procedure

Step 1 In the Cisco Defense Orchestrator navigation bar on the left, click **Objects > FDM Objects**.

Step 2 Click **Create Object** > **FTD** > **URL**.

Step 3 Enter an object name and description.

Step 4 Select **Create a URL object.**

Step 5 Enter the specific URL or IP address for your object.

Step 6 Click **Add**.

Create a Firepower URL Group

A URL group can be made up of one or more URL objects representing one or more URLs or IP addresses. The Firepower Device Manager and Firepower Management Center also refer to these objects as "URL Objects."

Procedure

Step 1 In the CDO navigation bar on the left, click **Objects > FDM Objects**.

Step 2 Click **Create Object** > **FTD** > **URL**.

Step 3 Enter an object name and description.

Step 4 Select **Create a URL group.**

Step 5 Add an existing object by clicking **Add Object,** selecting an object, and clicking **Select**. Repeat this step to add more objects.

Step 6 Click **Add** when you are done adding URL objects to the URL group.

Edit a Firepower URL Object or URL Group

Procedure

Step 1 In the CDO navigation bar on the left, click **Objects > FDM Objects**.

Step 2 Filter the objects to find the object you want to edit and then select the object in the object table.

Step 3 In the details pane, click  to edit.

Step 4 Edit the values in the dialog box in the same fashion that you created them in the procedures above.

Step 5 Click **Save**.

Step 6 CDO displays the policies that will be affected by the change. Click **Confirm** to finalize the change to the object and any policy affected by it.

Application Filter Objects

Application filter objects are used by Firepower devices. An application filter object defines the applications used in an IP connection, or a filter that defines applications by type, category, tag, risk, or business relevance. You can use these objects in policies to control traffic instead of using port specifications.

Although you can specify individual applications, application filters simplify policy creation and administration. For example, you could create an access control rule that identifies and blocks all high risk, low business relevance applications. If a user attempts to use one of those applications, the session is blocked.

You can select applications and application filters directly in a policy without using application filter objects. However, an object is convenient if you want to create several policies for the same group of applications or filters. The system includes several pre-defined application filters, which you cannot edit or delete.

Note Cisco frequently updates and adds additional application detectors via system and vulnerability database (VDB) updates. Thus, a rule blocking high risk applications can automatically apply to new applications without you having to update the rule manually.

Note When an FDM-managed device is onboarded to CDO, it converts the application filters to application filter objects without altering the rule defined in Access Rule or SSL Decryption. Because of a configuration change, the device's configuration status is changed to 'Not Synced' and requires configuration deployment from CDO. In general, FDM does not convert the application filters to application filter objects until you manually save the filters.

Related Information:

- Create and Edit a Firepower Application Filter Object
- Deleting Objects

Create and Edit a Firepower Application Filter Object

An application filter object allows you to target hand-picked applications or a group of applications identified by the filters. This application filter objects can be used in policies.

Create a Firepower Application Filter Object

To create an application filter object, follow this procedure:

Procedure

Step 1 In the CDO navigation bar on the left, click **Objects > FDM Objects**.

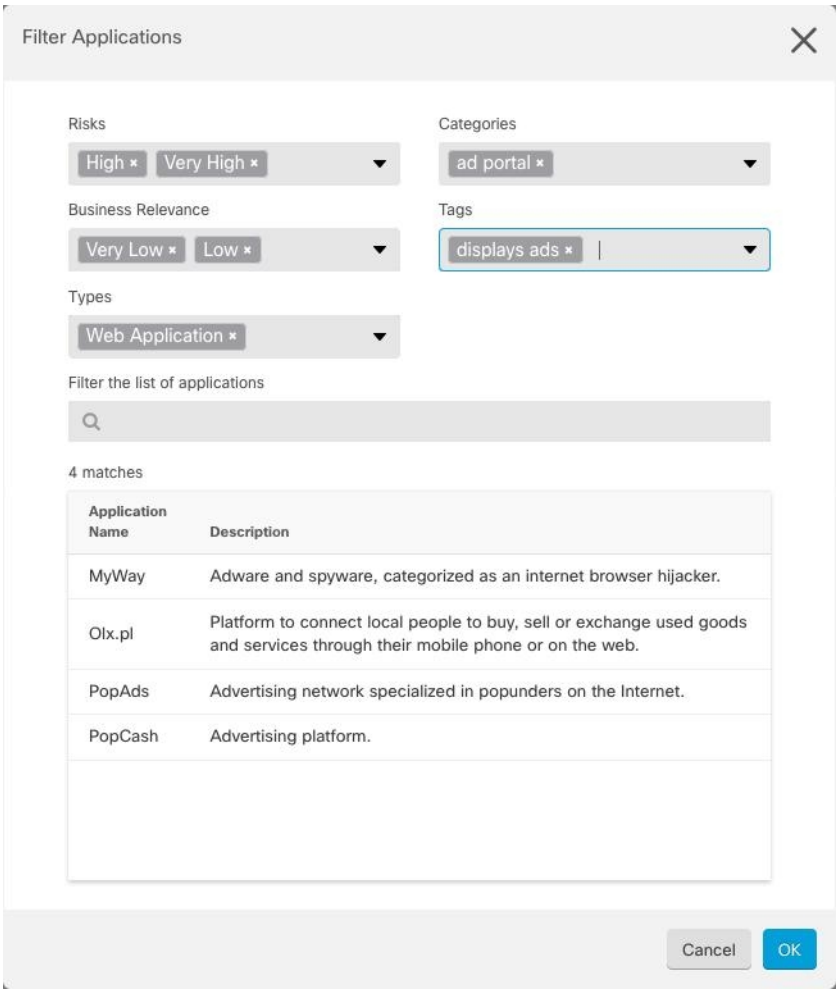
Step 2 Click **Create Object > FTD > Application Service**.

Step 3 Enter an **object name** for the object and optionally, a **description**.

Step 4 Click **Add Filter** and select the applications and filters to add to the object.

The initial list shows applications in a continually scrolling list. Click **Advanced Filter** to see the filter options and to get an easier view for selecting applications. Click **Add** when you have made your selections. You can repeat the process to add additional applications or filters.

Note Multiple selections within a single filter criteria have an OR relationship. For example, Risk is High OR Very High. The relationship between filters is AND, so Risk is High OR Very High, AND Business Relevance is Low OR Very Low. As you select filters, the list of applications in the display updates to show only those that meet the criteria. You can use these filters to help you find applications that you want to add individually, or to verify that you are selecting the desired filters to add to the rule.



Risks: The likelihood that the application is used for purposes that might be against your organization's security policy, from very low to very high.

Business Relevance: The likelihood that the application is used within the context of your organization's business operations, as opposed to recreationally, from very low to very high.

Types: The type of application.

- **Application Protocol:** Application protocols such as HTTP and SSH, which represent communications between hosts.
- **Client Protocol:** Clients such as web browsers and email clients, which represent software running on the host.
- **Web Application:** Web applications such as MPEG video and Facebook, which represent the content or requested URL for HTTP traffic.

Categories: A general classification for the application that describes its most essential function.

Tags: Additional information about the application, similar to category.

For encrypted traffic, the system can identify and filter traffic using only the applications tagged SSL Protocol. Applications without this tag can only be detected in unencrypted or decrypted traffic. Also, the system assigns

the decrypted traffic tag to applications that the system can detect in decrypted traffic only, not encrypted or unencrypted.

Applications List (bottom of the display): This list updates as you select filters from the options above the list, so you can see the applications that currently match the filter. Use this list to verify that your filter is targeting the desired applications when you intend to add filter criteria to the rule. To add a specific application or applications to your object, select them from the filtered list. Once you select the applications, the filter will no longer apply. If you want the filter itself to be the object, do not select an application from the list. Then the object will represent ever application identified by the filter.

Step 5 Click **OK** to save your changes.

Edit a Firepower Application Filter Object

Procedure

Step 1 In the CDO navigation bar on the left, click **Objects > FDM Objects**.

Step 2 Locate the object you want to edit by using object filters and search field.

Step 3 Select the object you want to edit.

Step 4 Click the edit icon  in the Actions pane of the details panel.

Step 5 Edit the values in the dialog box in the same fashion that you created them in the procedures above.

Step 6 Click **Save**.

Step 7 CDO displays the policies that will be affected by the change. Click **Confirm** to finalize the change to the object and any policy affected by it.

Related Information:

- Objects
- Object Filters
- Delete a Firepower Object

Geolocation Objects

A geolocation object defines countries and continents that host the device that is the source or destination of traffic. You can use these objects in policies to control traffic instead of using IP addresses. For example, using geographical location, you could easily restrict access to a particular country without needing to know all of the potential IP addresses used there.

You can typically select geographical locations directly in a policy without using geolocation objects. However, an object is convenient if you want to create several policies for the same group of countries and continents.

Update Geolocation Database

To ensure that you are using up-to-date geographical location data to filter your traffic, Cisco strongly recommends that you regularly update the geolocation database (GeoDB). At this time, this is not a task that you can perform using Cisco Defense Orchestrator. See the following sections of the Cisco Firepower Threat

Defense Configuration Guide for Firepower Device Manager for the version your device is running to learn more about the GeoDB and how to update it.

- Updating System Databases and Feeds
- Updating System Databases

Create and Edit a Firepower Geolocation Filter Object

You can create a geolocation object by itself on the object page or when creating a security policy. This procedure creates a geolocation object from the object page.

To create a geolocation object, follow these steps:

Procedure

Step 1 In the CDO navigation bar on the left, click **Objects > FDM Objects**.

Step 2 Click **Create Object** > **FTD** > **Geolocation**.

Step 3 Enter an **object name** for the object and optionally, a **description**.

Step 4 In the filter bar, start typing the name of a country or a region and you are presented with a list of possible matches.

Step 5 Check the country, countries, or regions that you want to add to the object.

Step 6 Click **Add**.

Edit a Geolocation Object

Procedure

Step 1 In the CDO navigation bar on the left, click **Objects > FDM Objects**.

Step 2 Use the filter panes and search field to locate your object.

Step 3 In the Actions pane, click **Edit**.

Step 4 You can change the name of the object and add or remove countries and regions to your object.

Step 5 Click **Save**.

Step 6 You will be notified if any devices are impacted. Click **Confirm**.

Step 7 If a device or policy was impacted, open the **Inventory** page and **Preview and Deploy** the changes to the device.

DNS Group Objects

Domain Name System (DNS) groups define a list of DNS servers and some associated attributes. DNS servers are needed to resolve fully-qualified domain names (FQDN), such as www.example.com, to IP addresses. You can configure different DNS group objects for management and data interfaces.

FDM-managed devices must have a DNS server configured prior to creating a new DNS Group Object. You can either add a DNS Server to theConfigure DNS Server in Cisco Defense Orchestrator (CDO) or create a

DNS server in firewall device manager and then sync the FDM-managed configuration to CDO. To create or modify the DNS server settings in firewall device manager, see **Configuring DNS for Data and Management Interfaces** in the Cisco Firepower Device Manager Configuration Guide, Version 6.4. or later.

Create a DNS Group Object

Use the following procedure to create a new DNS group object in CDO:

Procedure

Step 1 In the CDO navigation bar on the left, click **Objects > FDM Objects**.

Step 2 Click the blue plus button  to create an object.

Step 3 Click **FTD** > **DNS Group**.

Step 4 Enter an **Object Name**.

Step 5 (Optional) Add a description.

Step 6 Enter the IP address of a **DNS server**. You can add up to six DNS servers; click the **Add DNS Server**. If you want to remove a server address, click the delete icon.

Note The list is in priority order: the first server in the list is always used, and subsequent servers are used only if a response is not received from the servers above it. Although you can add up to six servers, only the first 3 servers listed will be used for the management interface.

Step 7 Enter the **Domain Search Name**. This domain is added to hostnames that are not fully-qualified, for example, serverA instead of serverA.example.com.

Step 8 Enter the amount of **Retries**. The number of times, from 0 to 10, to retry the list of DNS servers when the system does not receive a response. The default is 2. This setting applies to DNS groups used on the data interfaces only.

Step 9 Enter the **Timeout** value. The number of seconds, from 1 to 30, to wait before trying the next DNS server. The default is 2 seconds. Each time the system retries the list of servers, this timeout doubles. This setting applies to DNS groups used on the data interfaces only.

Step 10 Click **Add**.

Edit a DNS Group Object

You can edit a DNS group object that was created in Cisco Defense Orchestrator or in firewall device manager. Use the following procedure to edit an existing DNS group object:

Procedure

Step 1 In the CDO navigation bar on the left, click **Objects > FDM Objects**.

Step 2 Locate the **DNS Group Object** you want to edit by using object filters and search field.

Step 3 Select the object and click the edit icon  in the **Actions** pane.

Step 4 Edit any of the following entries:

- Object Name.
- Description.
- DNS Server. You can edit, add, or remove DNS servers from this list.
- Domain Search Name.
- Retries.
- Timeout.

Step 5 Click **Save**.

Step 6 Preview and Deploy Configuration Changes for All Devices.

Delete a DNS Group Object

Use the following procedure to delete a DNS Group Object from CDO:

Procedure

Step 1 In the CDO navigation bar on the left, click **Objects** > **FDM Objects**.

Step 2 Locate the **DNS Group Object** you want to edit by using object filters and search field.

Step 3 Select the object and click the **Remove** icon .

Step 4 Confirm you want to delete the DNS group object and click **Ok**.

Step 5 Preview and Deploy Configuration Changes for All Devices.

Add a DNS Group Object as an FDM-Managed DNS Server

You can add a DNS group object as the preferred DNS Group for either the **Data Interface** or the **Management Interface**. See FDM-Managed Device Settings for more information.

Certificate Objects

Digital certificates provide digital identification for authentication. Certificates are used for SSL (Secure Socket Layer), TLS (Transport Layer Security), and DTLS (Datagram TLS) connections, such as HTTPS and LDAPS.

See the **About Certificates** and **Configuring Certificates** following sections of the Resuable Objects chapter of the Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager for the version your device is running.

About Certificates

Digital certificates provide digital identification for authentication. A digital certificate includes information that identifies a device or user, such as the name, serial number, company, department, or IP address. A digital certificate also includes a copy of the public key for the user or device. Certificates are used for SSL (Secure Socket Layer), TLS (Transport Layer Security), and DTLS (Datagram TLS) connections, such as HTTPS and LDAPS.

You can create the following types of certificate:

- **Internal certificates**—Internal identity certificates are certificates for specific systems or hosts. You can generate these yourself using the OpenSSL toolkit or get them from a Certificate Authority. You can also generate a self-signed certificate.

  The system comes with the following pre-defined internal certificates, which you can use as is or replace: **DefaultInternalCertificate** and **DefaultWebServerCertificate**

- **Internal Certificate Authority (CA)** certificates—Internal CA certificates are certificates that the system can use to sign other certificates. These certificates differ from internal identity certificates with respect to the basic constraints extension and the CA flag, which are enabled for CA certificates but disabled for identity certificates. You can generate these yourself using the OpenSSL toolkit or get them from a Certificate Authority. You can also generate a self-signed internal CA certificate. If you configure self-signed internal CA certificates, the CA runs on the device itself.

  The system comes with the following pre-defined internal CA certificate, which you can use as is or replace: **NGFW-Default-InternalCA**

- **Trusted Certificate Authority (CA)** certificates—A trusted CA certificate is used to sign other certificates. It is self-signed and called a root certificate. A certificate that is issued by another CA certificate is called a subordinate certificate.

  Certificate Authorities (CAs) are trusted authorities that "sign" certificates to verify their authenticity, thereby guaranteeing the identity of the device or user. CAs issue digital certificates in the context of a PKI, which uses public-key or private-key encryption to ensure security. A CA can be a trusted third party, such as VeriSign, or a private (in-house) CA that you establish within your organization. CAs are responsible for managing certificate requests and issuing digital certificates.

  The system includes many trusted CA certificates from third party Certificate Authorities. These are used by SSL decryption policies for Decrypt Re-Sign actions.

For more information, see the **Certificate Types Used by Feature** section of the Reusable Objects chapter of the Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager for the version your device is running.

Certificate Types Used by Feature

You need to create the right type of certificate for each feature. The following features require certificates.

Identity Policies (Captive Portal)—Internal Certificate

(Optional.) Captive portal is used in identity policies. Users must accept this certificate when authenticating to the device for purposes of identifying themselves and receiving the IP address associated with their usernames. If you do not supply a certificate, the device uses an automatically generated certificate.

SSL Decryption Policy—Internal, Internal CA, and Trusted CA Certificates.

(Required.) The SSL decryption policy uses certificates for the following purposes:

- Internal certificates are used for known key decryption rules.
- Internal CA certificates are used for decrypt re-sign rules when creating the session between the client and FDM-managed device.
- Trusted CA certificates
  - They are used indirectly for decrypt re-sign rules when creating the session between the FDM-managed device and server. Unlike the other certificates, you do not directly configure these

certificates in the SSL decryption policy; they simply need to be uploaded to the system. The system includes a large number of trusted CA certificates, so you might not need to upload any additional certificates.

- When creating an Active Directory Realm object and configuring the directory server to use encryption.

Configuring Certificates

Certificates used in identity policies or SSL decryption policies must be an X509 certificate in PEM or DER format. You can use OpenSSL to generate certificates if needed, obtain them from a trusted Certificate Authority, or create self-signed certificates.

Use these procedures to configure certificate objects:

- Uploading Internal and Internal CA Certificates
- Uploading Trusted CA Certificates
- Generating Self-Signed Internal and Internal CA Certificate
- To view or edit a certificate, click either the edit icon or the view icon for the certificate.
- To delete an unreferenced certificate, click the trash can icon (delete icon) for the certificate. See Deleting Objects.

Uploading Internal and Internal CA Certificates

Internal identity certificates are certificates for specific systems or hosts. You can generate these yourself using the OpenSSL toolkit or get them from a Certificate Authority. You can also generate a self-signed certificate.

Internal Certificate Authority (CA) certificates (Internal CA certificates) are certificates that the system can use to sign other certificates. These certificates differ from internal identity certificates with respect to the basic constraints extension and the CA flag, which are enabled for CA certificates but disabled for identity certificates. You can generate these yourself using the OpenSSL toolkit or get them from a Certificate Authority. You can also generate a self-signed internal CA certificate. If you configure self-signed internal CA certificates, the CA runs on the device itself.

For information on the features that use these certificates, see Certificate Type Used by Feature.

Procedure

This procedure creates an internal or internal CA certificate by uploading a certificate file or pasting existing certificate text into a text box. If you want to generate a self signed certificate, see Generating Self-Signed Internal and Internal CA Certificates.

To create an internal or internal CA certificate object, or when adding a new certificate object to a policy, follow this procedure:

Procedure

Step 1 Do one of the following:

- Create the certificate object in the Objects page:

a. In the CDO navigation bar on the left, click **Objects** > **FDM Objects**.

b. Click the plus button  and select **FTD** > **Certificate**

- Click **Create New Object** when adding a new certificate object to a policy.

Step 2 Enter a **Name** for the certificate. The name is used in the configuration as an object name only, it does not become part of the certificate itself.

Step 3 In step 1, select **Internal Certificate** or **Internal CA.**

Step 4 In step 2, select **Upload** to upload the certificate file.

Step 5 In step 3, in the **Server Certificate** area, paste the certificate contents in the text box or upload the certificate file as explained in the wizard. If you paste the certificate into the text box, the certificate must include the BEGIN CERTIFICATE and END CERTIFICATE lines. For example:

```
-----BEGIN CERTIFICATE-----
 MIICMTCCAZoCCQDdUV3NGK/cUjANBgkqhkiG9w0BAQsFADBdMQswCQYDVQQGEwJV
UzETMBEGA1UECAwKU29tZS1TdGF0ZTEhMB8GA1UECgwYSW50ZXJuZXQgV2lkZ2l0
(...5 lines removed...)
shGJDReRYJQqilhHZrYTWZAYTrD7NQPHutK+ZiJng67cPgnNDuXEn55UwMOQoHBp
HMUwmhiGZlzJM8BpX2Js2yQ3ms30pr8rO+gPCPMCAwEAATANBgkqhkiG9w0BAQsF
AAOBgQCB02CebA6YjJCGr2CJZrQSeUwSveRBpmOuoqm98o2Z+5gJM5CkqgfxwCUn
RV7LRfQGFYd76V/5uor4Wx2ZCjqy6+zuQEm4ZxWNSZpA9UBixFXJCs9MBO4qkG5D
vlk3WYJfcgyJ10h4E4b0W2xiixBU+xoOTLRATnbKY36EWAG5cw==
-----END CERTIFICATE-----
```

Step 6 In step 3, in the **Certificate Key** area, paste the key contents into the Certificate Key text box or upload the key file as explained in the wizard. If you paste the key into the text box, the key must include the BEGIN PRIVATE KEY or BEGIN RSA PRIVATE KEY and END PRIVATE KEY or END PRIVATE KEY lines.

Note The key cannot be encrypted.

Step 7 Click **Add**.

Uploading Trusted CA Certificates

A trusted Certificate Authority (CA) certificate is used to sign other certificates. It is self-signed and called a root certificate. A certificate that is issued by another CA certificate is called a subordinate certificate.

For information on the features that use these certificates, see Certificate Type Used by Feature.

Obtain a trusted CA certificate from an external certificate authority, or create one using your own internal CA, for example, with OpenSSL tools. Then, use the following procedure to upload the certificate.

Procedure

Procedure

Step 1 Do one of the following:

- Create the certificate object in the Objects page:

  a. In the CDO navigation bar on the left, click **Objects** > **FDM Objects**.

b. Click the plus button  and select **FTD** > **Certificate**.

- Click **Create New Object** when adding a new certificate object to a policy.

Step 2 Enter a **Name** for the certificate. The name is used in the configuration as an object name only, it does not become part of the certificate itself.

Step 3 In step 1, select **External CA Certificate** and click **Continue**. The wizard advances to step 3.

Step 4 In step 3, in the **Certificate Contents** area, paste the certificate contents in the text box or upload the certificate file as explained in the wizard.

The certificate must follow these guidelines:

- The name of the server in the certificate must match the server Hostname / IP Address. For example, if you use 10.10.10.250 as the IP address but ad.example.com in the certificate, the connection fails.
- The certificate must be an X509 certificate in PEM or DER format.
- The certificate you paste must include the BEGIN CERTIFICATE and END CERTIFICATE lines. For example:

```
-----BEGIN CERTIFICATE-----
MIIFgTCCA2mgAwIBAgIJANvdcLnabFGYMA0GCSqGSIb3DQEBCwUAMFcxCzAJBgNV
BAYTAlVTMQswCQYDVQQIDAJUWDEPMA0GA1UEBwwGYXVzdGluMRQwEgYDVQQKDAsx
OTIuMTY4LjEuMTEUMBIGA1UEAwwLMTkyLjE2OC4xLjEwHhcNMTYxMDI3MjIzNDE3
WhcNMTcxMDI3MjIzNDE3WjBXMQswCQYDVQQGEwJVUzELMAkGA1UECAwCVFgxDzAN
BgNVBAcMBmF1c3RpbjEUMBIGA1UECgwLMTkyLjE2OC4xLjExFDASBgNVBAMMCzE5
Mi4xNjguMS4xMIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEA5NceYwtP
ES6Ve+S9z7WLKGX5JlF58AvH82GPkOQdrixn3FZeWLQapTpJZt/vgtAI2FZIK31h
(...20 lines removed...)
hbr6HOgKlOwXbRvOdksTzTEzVUqbgxt5Lwupg3b2ebQhWJz4BZvMsZX9etveEXDh
PY184V3yeSeYjbSCF5rP71fObG9Iu6+u4EfHp/NQv9s9dN5PMffXKieqpuN20Ojv
2b1sfOydf4GMUKLBUMkhQnip6+3W
-----END CERTIFICATE-----
```

Step 5 Click **Add**.

Generating Self-Signed Internal and Internal CA Certificates

Internal identity certificates are certificates for specific systems or hosts. You can generate these yourself using the OpenSSL toolkit or get them from a Certificate Authority. You can also generate a self-signed certificate.

Internal Certificate Authority (CA) certificates (Internal CA certificates) are certificates that the system can use to sign other certificates. These certificates differ from internal identity certificates with respect to the basic constraints extension and the CA flag, which are enabled for CA certificates but disabled for identity certificates. You can generate these yourself using the OpenSSL toolkit or get them from a Certificate Authority. You can also generate a self-signed internal CA certificate. If you configure self-signed internal CA certificates, the CA runs on the device itself.

You can also create these certificates using OpenSSL, or obtain them from a trusted CA, and upload them. For more information, see Uploading Internal and Internal CA Certificates.

For information on the features that use these certificates, see Certificate Type Used by Feature.

Note New self-signed certificates are generated with a 5-year validity term. Be sure to replace certificates before they expire.

Warning Upgrading devices that have self-signed certificates may experience issues; see New Certificate Detected for more information.

Procedure

This procedure generates a self-signed certificate by entering the appropriate certificate field values in a wizard. If you want to create an internal or internal CA certificate by uploading a certificate file, see Uploading Internal and Internal CA Certificates.

To generate a self-signed certificate, follow this procedure:

Procedure

Step 1 Do one of the following:

- Create the certificate object in the Objects page:
  a. In the CDO navigation bar on the left, click **Objects > FDM Objects**.
  b. Click the plus button and select **FTD** > **Certificate**.
- Click **Create New Object** when adding a new certificate object to a policy.

Step 2 Enter a **Name** for the certificate. The name is used in the configuration as an object name only, it does not become part of the certificate itself.

Step 3 In step 1, select **Internal Certificate** or **Internal CA.**

Step 4 In step 2, select **Self-Signed** to create the self-signed certificate in this step.

Step 5 Configure at least one of the following for the certificate subject and issuer information.

- Country (C)— Select the country code from the drop-down list.
- State or Province (ST)— The state or province to include in the certificate.
- Locality or City (L)— The locality to include in the certificate, such as the name of the city.
- Organization (O)— The organization or company name to include in the certificate.
- Organizational Unit (Department) (OU)— The name of the organization unit (for example, a department name) to include in the certificate.
- Common Name (CN)— The X.500 common name to include in the certificate. This could be the name of the device, web site, or another text string. This element is usually required for successful connections. For example, you must include a CN in the internal certificate used for remote access VPN.

Step 6 Click **Add**.

About IPsec Proposals

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 called a transform set. During the IPsec security association (SA) negotiation, peers search for a transform set that is the same at both peers.

There are separate IPsec proposal objects based on the IKE version, IKEv1, or IKEv2:

- When you create an IKEv1 IPsec proposal, you select the mode in which IPsec operates, and define the required encryption and authentication types. You can select single options for the algorithms. If you want to support multiple combinations in a VPN, create and select multiple IKEv1 IPsec Proposal objects.
- When you create an IKEv2 IPsec proposal, you can select all of the encryption and hash algorithms allowed in a VPN. The system orders the settings from the most secure to the least secure and negotiates with the peer until a match is found. This allows you to potentially send a single proposal to convey all the allowed combinations instead of the need to send each allowed combination individually as with IKEv1.

The Encapsulating Security Protocol (ESP) is used for both IKEv1 and IKEv2 IPsec proposals. It provides authentication, encryption, and antireplay services. ESP is IP protocol type 50.

Note We recommend using both encryption and authentication on IPsec tunnels.

The following topics explain how to configure IPsec proposals for each IKE version:

- Create and Edit IKEv1 IPsec Proposal Object
- Create and Edit IKEv2 IPsec Proposal Object

Managing an IKEv1 IPsec Proposal Object

IPsec Proposal objects configure the IPsec proposal used during IKE Phase 2 negotiations. The IPsec proposal defines the combination of security protocols and algorithms that secure traffic in an IPsec tunnel. There are separate objects for IKEv1 and IKEv2. Currently, Cisco Defense Orchestrator (CDO) supports IKEv1 IPsec proposal objects.

The Encapsulating Security Protocol (ESP) is used for both IKEv1 and IKEv2 IPsec proposals. It provides authentication, encryption, and anti-replay services. ESP is IP protocol type 50.

Note We recommend using both encryption and authentication on IPsec tunnels.

Related Topics

Create an IKEv1 IPsec Proposal Object, on page 213

Create or Edit an IKEv1 IPsec Proposal Object

There are several pre-defined IKEv1 IPsec proposals. You can also create new proposals to implement other combinations of security settings. You cannot edit or delete system-defined objects.

The following procedure explains how you can create and edit objects directly through the Objects page. You can also create IKEv1 IPsec Proposals objects while editing the IKEv1 IPsec settings in a Site-to-Site VPN connection by clicking the **Create New IKEv1 Proposal** link shown in the object list.

Procedure

Step 1 In the CDO navigation bar on the left, click **Objects > FDM Objects**.

Step 2 Do one of these things:

- Click the blue plus button and select **FTD > IKEv1 IPsec Proposal** to create the new object.
- In the object page, select the IPsec proposal you want to edit and click **Edit** in the Actions pane at the right.

Step 3 Enter an **object name** for the new object.

Step 4 Select the Mode in which the IKEv1 IPsec Proposal object operates.

- **Tunnel mode** encapsulates the entire IP packet. The IPSec header is added between the original IP header and a new IP header. This is the default. Use tunnel mode when the firewall is protecting traffic to and from hosts positioned behind the firewall. Tunnel mode is the normal way regular IPSec is implemented between two firewalls (or other security gateways) that are connected over an untrusted network, such as the Internet.
- **Transport mode** encapsulates only the upper-layer protocols of an IP packet. The IPSec header is inserted between the IP header and the upper-layer protocol header (such as TCP). Transport mode requires that both the source and destination hosts support IPSec, and can only be used when the destination peer of the tunnel is the final destination of the IP packet. Transport mode is generally used only when protecting a Layer 2 or Layer 3 tunneling protocol such as GRE, L2TP, and DLSW.

Step 5 Select the **ESP Encryption** (Encapsulating Security Protocol encryption) algorithm for this proposal. For an explanation of the options, see Deciding Which Encryption Algorithm to Use, on page 194.

Step 6 Select the **ESP Hash** or integrity algorithm to use for authentication. For an explanation of the options, see Deciding Which Hash Algorithms to Use, on page 195.

Step 7 Click **Add**.

Managing an IKEv2 IPsec Proposal Object

IPsec Proposal objects configure the IPsec proposal used during IKE Phase 2 negotiations. The IPsec proposal defines the combination of security protocols and algorithms that secure traffic in an IPsec tunnel.

When you create an IKEv2 IPsec proposal, you can select all of the encryption and hash algorithms allowed in a VPN. The system orders the settings from the most secure to the least secure and negotiates with the peer until a match is found. This allows you to potentially send a single proposal to convey all the allowed combinations instead of the need to send each allowed combination individually as with IKEv1.

Related Topics

Create or Edit an IKEv2 IPsec Proposal Object, on page 214

Create or Edit an IKEv2 IPsec Proposal Object

There are several pre-defined IKEv2 IPsec proposals. You can also create new proposals to implement other combinations of security settings. You cannot edit or delete system-defined objects.

The following procedure explains how you can create and edit objects directly through the Objects page. You can also create IKEv2 IPsec Proposals objects while editing the IKEv2 IPsec settings in a VPN connection by clicking the Create New IPsec Proposal link shown in the object list.

Procedure

Step 1 In the CDO navigation bar on the left, click **Objects** > **FDM Objects**.

Step 2 Do one of these things:

- Click the blue plus button  and select **FTD** > **IKEv2 IPsec Proposal** to create the new object.
- In the object page, select the IPsec proposal you want to edit and click **Edit** in the Actions pane at the right.

Step 3 Enter an **object name** for the new object.

Step 4 Configure the IKE2 IPsec proposal objects:

- **Encryption**—The Encapsulating Security Protocol (ESP) encryption algorithm for this proposal. Select all the algorithms that you want to allow. The system negotiates with the peer, starting from the strongest to the weakest algorithm until a match is agreed upon. For an explanation of the options, see Deciding Which Encryption Algorithm to Use, on page 194.
- **Integrity Hash**—The hash or integrity algorithm to use for authentication. Select all the algorithms that you want to allow. The system negotiates with the peer, starting from the strongest to the weakest algorithm until a match is agreed upon. For an explanation of the options, see Deciding Which Hash Algorithms to Use, on page 195.

Step 5 Click **Add**.

About Global IKE Policies

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

The IKE negotiation comprises two phases. Phase 1 negotiates a security association between two IKE peers, which enables the peers to communicate securely in Phase 2. During Phase 2 negotiation, IKE establishes SAs for other applications, such as IPsec. Both phases use proposals when they negotiate a connection. An IKE proposal is a set of algorithms that two peers use to secure the negotiation between them. IKE negotiation begins by each peer agreeing on a common (shared) IKE policy. This policy states which security parameters are used to protect subsequent IKE negotiations.

IKE policy objects define the IKE proposals for these negotiations. The objects that you enable are the ones used when the peers negotiate a VPN connection: you cannot specify different IKE policies per connection. The relative priority of each object determines which of these policies are tried first, with the lower number being a higher priority. The connection is not established if the negotiation fails to find a policy that both peers can support.

To define the global IKE policy, you select which objects to enable for each IKE version. If the pre-defined objects do not satisfy your requirements, create new policies to enforce your security policy.

The following procedure explains how to configure the global policy through the Objects page. You can also enable, disable, and create policies when editing a VPN connection by clicking Edit for the IKE Policy settings.

The following topics explain how to configure IKE policies for each version:

- Configuring IKEv1 Policies
- Configuring IKEv2 Policies

Managing IKEv1 Policies

About IKEv1 Policy

Internet Key Exchange (IKE) version 1 policy objects contain the parameters required for IKEv1 policies when defining VPN connections. IKE is a key management protocol that facilitates the management of IPsec-based communications. It is used to authenticate IPsec peers, negotiate and distribute IPsec encryption keys, and automatically establish IPsec security associations (SAs).

There are several pre-defined IKEv1 policies. If any suit your needs, simply enable them by clicking the State toggle. You can also create new policies to implement other combinations of security settings. You cannot edit or delete system-defined objects.

Related Topics

Create an IKEv1 Policy, on page 209

Create or Edit an IKEv1 Policy

The following procedure explains how you can create and edit objects directly through the Objects page. You can also create an IKEv1 policy while editing the IKE settings in a Site-to-Site VPN connection by clicking the **Create New IKEv1 Policy** link shown in the object list.

Procedure

Step 1 In the CDO navigation bar on the left, click **Objects > FDM Objects**.

Step 2 Do one of these things:

- Click the blue plus button  and select **FTD > IKEv1 Policy** to create a new IKEv1 policy.
- In the object page, select the IKEv1 policy you want to edit and click **Edit** in the Actions pane at the right.

Step 3 Enter an **object name**, up to 128 characters.

Step 4 Configure the IKEv1 properties.

- **Priority**—The relative priority of the IKE policy, from 1 to 65,535. The priority determines the order of the IKE policy 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 highest priority policy, it tries to use the parameters defined in the next lowest priority. The lower the number, the higher the priority.
- **Encryption**—The encryption algorithm used to establish the Phase 1 security association (SA) for protecting Phase 2 negotiations. For an explanation of the options, see Deciding Which Encryption Algorithm to Use.
- **Diffie-Hellman Group**—The Diffie-Hellman group to use for deriving a shared secret between the two IPsec peers without transmitting it to each other. A larger modulus provides higher security but requires more processing time. The two peers must have a matching modulus group. For an explanation of the options, see Deciding Which Diffie-Hellman Modulus Group to Use.
- **Lifetime**—The lifetime of the security association (SA), in seconds, from 120 to 2147483647 or blank. 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 set up more quickly than with shorter lifetimes. The default is 86400. To specify an unlimited lifetime, enter no value (leave the field blank).
- **Authentication**—The method of authentication to use between the two peers. For more information, see Deciding Which Authentication Method to Use, on page 196.
  - **Preshared Key**—Use the preshared key that is defined on each device. These keys allow for a secret key to be shared between two peers and to be used by IKE during the authentication phase. If the peer is not configured with the same preshared key, the IKE SA cannot be established.
  - **Certificate**—Use the device identity certificates for the peers to identify each other. You must obtain these certificates by enrolling each peer in a Certificate Authority. You must also upload the trusted CA root and intermediate CA certificates used to sign the identity certificates in each peer. The peers can be enrolled in the same or a different CA. You cannot use self-signed certificates for either peer.
- **Hash**—The hash algorithm for creating a message digest, which is used to ensure message integrity. For an explanation of the options, see Encryption and Hash Algorithms Used in VPN, on page 194.

Step 5 Click **Add**.

Managing IKEv2 Policies

About IKEv2 Policy

Internet Key Exchange (IKE) version 2 policy objects contain the parameters required for IKEv2 policies when defining VPN connections. IKE is a key management protocol that facilitates the management of IPsec-based communications. It is used to authenticate IPsec peers, negotiate and distribute IPsec encryption keys, and automatically establish IPsec security associations (SAs).

There are several pre-defined IKEv2 policies. If any suit your needs, simply enable them by clicking the State toggle. You can also create new policies to implement other combinations of security settings. You cannot edit or delete system-defined objects.

Related Topics

Create an IKEv2 Policy, on page 211

Create or Edit an IKEv2 Policy

The following procedure explains how you can create and edit objects directly through the Objects page. You can also create an IKEv2 policy while editing the IKE settings in a Site-to-Site VPN connection by clicking the **Create New IKEv2 Policy** link shown in the object list.

Procedure

Step 1 In the CDO navigation bar on the left, click **Objects > FDM Objects**.

Step 2 Do one of these things:

- Click the blue plus button  and select **FTD > IKEv2 Policy** to create a new IKEv2 policy.
- In the object page, select the IKEv2 policy you want to edit and click **Edit** in the Actions pane at the right.

Step 3 Enter an **object name**, up to 128 characters.

Step 4 Configure the IKEv2 properties.

- **Priority**—The relative priority of the IKE policy, from 1 to 65,535. The priority determines the order of the IKE policy 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 highest priority policy, it tries to use the parameters defined in the next lowest priority. The lower the number, the higher the priority.
- **State**—Whether the IKE policy is enabled or disabled. Click the toggle to change the state. Only enabled policies are used during IKE negotiations.
- **Encryption**—The encryption algorithm used to establish the Phase 1 security association (SA) for protecting Phase 2 negotiations. Select all algorithms that you want to allow, although you cannot include both mixed-mode (AES-GCM) and normal mode options in the same policy. (Normal mode requires that you select an integrity hash, whereas mixed-mode prohibits a separate integrity hash selection.) The system negotiates with the peer, starting from the strongest to the weakest algorithm until a match is agreed upon. For an explanation of the options, see Deciding Which Encryption Algorithm to Use, on page 194.
- **Diffie-Hellman Group**—The Diffie-Hellman group to use for deriving a shared secret between the two IPsec peers without transmitting it to each other. A larger modulus provides higher security but requires more processing time. The two peers must have a matching modulus group. Select all the algorithms that you want to allow. The system negotiates with the peer, starting from the strongest to the weakest group until a match is agreed upon. For an explanation of the options, see Deciding Which Diffie-Hellman Modulus Group to Use, on page 195.
- **Integrity Hash**—The integrity portion of the hash algorithm for creating a message digest, which is used to ensure message integrity. Select all the algorithms that you want to allow. The system negotiates with the peer, starting from the strongest to the weakest algorithm until a match is agreed upon. The integrity hash is not used with the AES-GCM encryption options. For an explanation of the options, see Encryption and Hash Algorithms Used in VPN, on page 194.

- **Pseudo-Random Function (PRF) Hash**—The pseudo-random function (PRF) portion of the hash algorithm, which is used as the algorithm to derive keying material and hashing operations required for the IKEv2 tunnel encryption. In IKEv1, the Integrity and PRF algorithms are not separated, but in IKEv2, you can specify different algorithms for these elements. Select all the algorithms that you want to allow. The system negotiates with the peer, starting from the strongest to the weakest algorithm until a match is agreed upon. For an explanation of the options, see Encryption and Hash Algorithms Used in VPN, on page 194.
- **Lifetime**—The lifetime of the security association (SA), in seconds, from 120 to 2147483647 or blank. 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 set up more quickly than with shorter lifetimes. The default is 86400. To specify an unlimited lifetime, enter no value (leave the field blank).

Step 5 Click **Add**.

RA VPN Objects

Security Zone Object

A security zone is a grouping of interfaces. Zones divide the network into segments to help you manage and classify traffic. You can define multiple zones, but a given interface can be in one zone only.

The Firepower system creates the following zones during initial configuration and they are displayed in Defense Orchestrator's object page. You can edit zones to add or remove interfaces, or you can delete the zones if you no longer use them.

- **inside_zone**-Includes the inside interface. This zone is intended to represent internal networks.
- **outside_zone**-Includes the outside interface. This zone is intended to represent networks external to your control, such as the internet.

Typically, you would group interfaces by the role they play in your network. For example, you would place the interface that connects to the internet in the **outside_zone** security zone, and all of the interfaces for your internal networks in the **inside_zone** security zone. Then, you could apply access control rules to traffic coming from the outside zone and going to the inside zone.

Before creating zones, consider the access rules and other policies you want to apply to your networks. For example, you do not need to put all internal interfaces into the same zone. If you have 4 internal networks, and you want to treat one differently than the other three, you can create two zones rather than one. If you have an interface that should allow outside access to a public web server, you might want to use a separate zone for the interface.

Related Information:

- Create or Edit a Firepower Security Zone Object
- Assign a Firepower Interface to a Security Zone
- Deleting Objects

Create or Edit a Firepower Security Zone Object

A security zone is a grouping of interfaces. Zones divide the network into segments to help you manage and classify traffic. You can define multiple zones, but a given interface can be in one zone only. For more information see, Security Zone Object.

A security zone object is not associated with a device unless it is used in a rule for that device.

Create a Security Zone Object

To create a security zone object, follow these instructions:

Procedure

Step 1 In the CDO navigation bar on the left, click **Objects > FDM Objects**.

Step 2 Click the blue plus button  and select **FTD** > **Security Zone** to create the object.

Step 3 Give the object a name and, optionally, a description.

Step 4 Select the interfaces to put in the security zone.

Step 5 Click **Add.**

Edit a Security Zone Object

After onboarding an FDM-managed device, you will find there are already at least two security zones, one is the inside_zone and the other is the outside_zone. These zones can be edited or deleted. To edit any security zone object, follow these instructions:

Procedure

Step 1 In the CDO navigation bar on the left, click **Objects > FDM Objects**.

Step 2 Find the object you want to edit:

- If you know the name of the object, you can search for it in the Objects page:
  - Filter the list by security zone.
  - Enter the name of the object in the search field.
  - Select the object.
- If you know the object is associated with a device, you can search for it starting on the **Inventory** page.
  - In the navigation pane, click **Inventory**.
  - Click the **Devices** tab.
  - Click the apporpriate tab.
  - Use the device filter and search bar to locate your device.
  - Select the device.

- In the Management pane at the right, click  **Objects.**
- Use the object filter and search bar to locate the object you are looking for.

Note If the security zone object you created is not associated with a rule in a policy for your device, it is considered "unassociated" and you will not see it among the search results for a device.

Step 3 Select the object.

Step 4 Click the **Edit** icon in the Actions pane at the right.

Step 5 After editing any of the attributes of the object. Click **Save**.

Step 6 After clicking Save you receive a message explaining how these changes will affect other devices. Click **Confirm** to save the changes or Cancel.

Service Objects

Firepower Service Objects

FTD service objects, service groups, and port groups are reusable components that contain protocols or ports considered part of the IP protocol suite.

FTD service groups are collections of service objects. A service group may contain objects for one or more protocols. You can use the objects and groups in security policies for purposes of defining network traffic matching criteria, for example, to use access rules to allow traffic to specific TCP ports. The system includes several pre-defined objects for common services. You can use these objects in your policies; however, you cannot edit or delete system-defined objects.

Firepower Device Manager and Firepower Management Center refer to service objects as port objects and service groups and port groups.

See Create and Edit Firepower Threat Defense Service Objects for more information.

Protocol Objects

Protocol objects are a type of service object that contain less-commonly used or legacy protocols. Protocol objects are identified by a name and protocol number. CDO recognizes these objects in ASA and Firepower (FDM-managed device) configurations and gives them their own filter of "Protocols" so you can find them easily.

See Create and Edit Firepower Threat Defense Service Objects for more information.

ICMP Objects

An Internet Control Message Protocol (ICMP) object is a service object specifically for ICMP and IPv6-ICMP messages. CDO recognizes these objects in ASA and Firepower configurations when those devices are onboarded and CDO gives them their own filter of "ICMP" so you can find the objects easily.

Using CDO, you can rename or remove ICMP objects from an ASA configuration. You can use CDO to create, update, and delete ICMP and ICMPv6 objects in a Firepower configuration.

Note For the ICMPv6 protocol, AWS does not support choosing specific arguments. Only rules that allow all ICMPv6 messages are supported.

See Create and Edit Firepower Threat Defense Service Objects for more information.

Related Information:

- Deleting Objects

Create and Edit Firepower Service Objects

To create a firepower service object, follow these steps:

firewall device manager (FDM-managed) service objects are reusable components that specify a TCP/IP protocol and a port. The firewall device manager, On-Prem Firewall Management Center and Cloud-delivered Firewall Management Center refer to these objects as "Port Objects."

Procedure

Step 1 In the CDO navigation bar on the left, click **Objects > FDM Objects**.

Step 2 Click the blue button  on the right to create an object, and select **FTD** > **Service**.

Step 3 Enter an object name and description.

Step 4 Select **Create a service object.**

Step 5 Click the **Service Type** button and select the protocol for which you want to create an object.

Step 6 Configure the protocol as follows:

- **TCP**, **UDP**
  - Select **eq** and then enter either a port number or a protocol name. For example, you could enter 80 as a port number or HTTP as the protocol name.
  - You can also select **range** and then enter a range of port numbers, for example, **1 65535** (to cover all ports).
- **ICMP**, **IPv6-ICMP**-Select the ICMP **Type.** Select **Any** for the type to apply to all ICMP messages. For information on the types and codes, see the following pages:
  - ICMP-http://www.iana.org/assignments/icmp-parameters/icmp-parameters.xml
  - ICMPv6-http://www.iana.org/assignments/icmpv6-parameters/icmpv6-parameters.xml
- **Other**-Select the desired protocol.

Step 7 Click **Add**.

Step 8 Preview and Deploy Configuration Changes for All Devices the changes you made now, or wait and deploy multiple changes at once.

Create a Firepower Service Group

A service group can be made up of one or more service objects representing one or more protocols. The service objects need to be created before they can be added to the group. The Firepower Device Manager and Firepower Management Center refer to these objects as "Port Objects."

Procedure

Step 1 In the CDO navigation bar on the left, click **Objects** > **FDM Objects**.

Step 2 Click the blue button  on the right to create an object, and select **FTD** > **Service**.

Step 3 Enter an object name and description.

Step 4 Select **Create a service group.**

Step 5 Add an object to the group by clicking **Add Object.**

- Click **Create** to create a new object as you did above in Create a Firepower Service Object above.
- Click **Choose** to add an existing service object to the group. Repeat this step to add more objects.

Step 6 Click **Add** when you are done adding service objects to the service group.

Step 7 Preview and Deploy Configuration Changes for All Devices the changes you made now, or wait and deploy multiple changes at once.

Edit a Firepower Service Object or Service Group

Procedure

Step 1 In the CDO navigation bar on the left, click **Objects** > **FDM Objects**.

Step 2 Filter the objects to find the object you want to edit and then select the object in the object table.

Step 3 In the Actions pane, click **Edit**  .

Step 4 Edit the values in the dialog box in the same fashion that you created them in the procedures above.

Step 5 Click **Save**.

Step 6 CDO displays the policies that will be affected by the change. Click **Confirm** to finalize the change to the object and any policy affected by it.

Step 7 Preview and Deploy Configuration Changes for All Devices the changes you made now, or wait and deploy multiple changes at once.

Security Group Tag Group

Security Group Tags

About Security Group Tags

If you use Cisco Identity Services Engine (ISE) to define and use **security group tag** (SGT) for classifying traffic in a Cisco TrustSec network, you can write access control rules that use SGT as matching criteria. Thus, you can block or allow access based on security group membership rather than IP addresses.

In ISE, you can create a SGT and assign host or network IP addresses to each tag. If you assign an SGT to a user's account, the SGT is assigned to the user's traffic. After you configure FDM-managed device to connect to an ISE server and create the SGT, you can create SGT groups in Cisco Defense Orchestrator and build access control rules around them. Note that you must configure ISE's SGT Exchange Protocol (SXP) mapping before you can associate an SGT to an FDM-managed device. See **Security Group Tag Exchange Protocol** in the Cisco Identity Services Engine Administrator Guide of the version you are currently running for more information.

When an FDM-managed device evaluates SGT as a traffic matching criteria for an access control rule, it uses the following priority:

1. The source SGT defined in the packet, if any. No destination matching is done using this technique. For the SGT to be in the packet, the switches and routers in the network must be configured to add them. See the ISE documentation for information on how to implement this method.
2. The SGT assigned to the user session, as downloaded from the ISE session directory. You need to enable the option to listen to session directory information for this kind of SGT matching, but this option is on by default when you first create the ISE identity source. The SGT can be matched to source or destination. Although not required, you would also normally set up a passive authentication identity rule, using the ISE identity source along with an AD realm, to collect user identity information.
3. The SGT-to-IP address mapping downloaded using SXP. If the IP address is within the range for an SGT, then the traffic matches the access control rule that uses the SGT. The SGT can be matched to source or destination.

Note You cannot use the information retrieved from ISE directly in an access control rule. Instead, you need to create SGT groups, which refer to the downloaded SGT information. Your SGT groups can refer to more than one SGT, so you can apply policy based on a relevant collections of tags if that is appropriate.

Version Support

CDO currently supports SGT and SGT groups on FDM-managed devices running Version 6.5 and later. an FDM-managed device allows you to configure and connect to an ISE server in Version 6.5 and later but not does not support SGT configuration in the UI until Version 6.7.

From the FDM-managed UI, this means that an FDM-managed device running Version 6.5 or later can download SXP mappings of SGTs but cannot be manually added to objects or access control rules. To make changes to the SGTs for devices running Version 6.5 or Version 6.6, you must use the ISE UI. If the device running Version 6.5 is onboarded to Cisco Defense Orchestrator, however, you can see the current SGTs associated with the device and create SGT groups.

SGT in CDO

Security Group Tags

SGTs are read-only in CDO. You cannot create or edit an SGT in CDO. To create an SGT, see the Cisco Identity Services Engine Administrator Guide of the version your are currently running.

SGT Groups

Note An FDM-managed device refers to groups of SGTs as SGT dynamic objects. In CDO, these lists of tags are currently called SGT groups. You can create an SGT group in CDO without referring to the FDM-managed device or ISE UI.

Use SGT groups to identify source or destination addresses based on an SGT assigned by ISE. You can then use the objects in access control rules for purposes of defining traffic matching criteria. You cannot use the information retrieved from ISE directly in an access control rule. Instead, you need to create SGT groups, which refer to the downloaded SGT information.

Your SGT groups can refer to more than one SGT, so you can apply policy based on relevant collections of tags if that is appropriate.

In order to create an SGT group in CDO, you must have at least one SGT already configured and SGT mappings from an ISE server configured for the FDM-managed console of the device you want to use. Note that if more than one FDM-managed device is associated with the same ISE server, an SGT or SGT group can be applied to more than one device. If a device is not associated with an ISE server, you cannot include SGT objects in your access control rule, or apply an SGT group to that device configuration.

SGT Groups in Rules

SGT groups can be added to access control rules; they appear as source or destination network objects. For more information about how networks work in rules, see Source and Destination Criteria in an FDM-Managed Access Control Rule.

You can create an SGT group from the Objects page. See Create an SGT Group for more information.

Create an SGT Group

To create an SGT group that can be used for an access control rule, use the following procedure:

Before you begin

You must have the following configurations or environments configured prior to creating a security group tag (SGT) group:

- FDM-managed device must be running at least Version 6.5.
- You must configure the ISE identity source to subscribe to SXP mappings and enable deploy changes. To manage SXP mappings, see **Configure Security Groups and SXP Publishing in ISE** of the Firepower Device Manager Configuration Guide for the version you're using, Version 6.7 and later.
- All SGTs must be created in ISE. To create an SGT, see the Cisco Identity Services Engine Configuration Guide of the version your are currently running.

Procedure

Step 1 In the CDO navigation bar on the left, click **Objects** > **FDM Objects**.

Step 2 Click the blue plus button  to create an object.

Step 3 Click **FTD** > **Network**.

Step 4 Enter an **Object Name**.

Step 5 (Optional) Add a description.

Step 6 Click **SGT** and use the drop-down menu to check all the applicable SGTs you want included in the group. You can sort the list by SGT name.

Step 7 Click **Save**.

Note You cannot create or edit SGTs in CDO, you can only add or remove them from an SGT group. To create or edit an SGT, see the Cisco Identity Services Engine Configuration Guide of the version you are currently running.

Edit an SGT Group

To edit an SGT group, use the following procedure:

Procedure

Step 1 In the CDO navigation bar on the left, click **Objects** > **FDM Objects**.

Step 2 Locate the SGT group you want to edit by using object filters and search field.

Step 3 Select the SGT group and click the edit icon  in the **Actions** pane.

Step 4 Modify the SGT group. Edit the name, description, or the SGTs associated with the group.

Step 5 Click **Save**.

Note You cannot create or edit SGTs in CDO, you can only add or remove them from an SGT group. To create or edit an SGT, see the Cisco Identity Services Engine Configuration Guide of the version you are currently running.

Add an SGT Group to an Access Control Rule

To add an SGT group to an access control rule, use the following procedure:

Procedure

Step 1 In the navigation pane, click **Inventory**.

Step 2 Click the **Devices** tab to locate the device or the **Templates** tab to locate the model device.

Step 3 Click the **FTD** tab and select the device you want to add the SGT group to.

Step 4 In the**Management** pane, select **Policy**.

Step 5 Click the blue plus button  for either the **Source** or **Destination** objects and select **SGT Groups**.

Step 6 Locate the SGT group(s) you want to edit by using object filters and search field.

Step 7 Click **Save**.

Step 8 Preview and Deploy Configuration Changes for All Devices.

Note If you need to create an additional SGT group, click **Create New Object**. Fill in the required information mentioned in Create an FTD SGT Group and **Add** the SGT group to the rule.

Syslog Server Objects

FDM-managed devices have a limited capacity to store events. To maximize storage for events, you can configure an external server. A system log (syslog) server object identifies a server that can receive connection-oriented or diagnostic syslog messages. If you have a syslog server set up for log collection and analysis, you can use the Cisco Defense Orchestrator to create objects to define them and use the objects in the related policies.

Create and Edit Syslog Server Objects

To create a new syslog server object, follow these steps:

Procedure

Step 1 In the CDO navigation bar on the left, click **Objects** > **FDM Objects**.

Step 2 Click the **Create Object** button  .

Step 3 Select **Syslog Server** under FDM-managed device object types

Step 4 Configure the syslog server object properties:

- **IP Address**—Enter the IP address of the syslog server.
- **Protocol Type**—Select the protocol that your syslog server uses to receive messages. If you select TCP, the system can recognize when the syslog server is not available, and stops sending events until the server is available again.
- **Port Number**—Enter a valid port number to use for syslog. If your syslog server uses default ports, enter 514 as the default UDP port or 1470 as the default TCP port. If the server does not use default ports, enter the correct port number. The port must be in the range 1025 to 65535.
- **Select an interface**—Select which interface should be used for sending diagnostic syslog messages. Connection and intrusion events always use the management interface. Your interface selection determines the IP address associated with syslog messages. Note that you can only select **one** of the options listed below. You cannot select both. Select one of the following options:
  - **Data Interface**—Use the data interface you select for diagnostic syslog messages. Select an interface from the generated list. If the server is accessible through a bridge group member interface, select the bridge group interface (BVI). If it is accessible through the Diagnostic interface (the physical management interface), we recommend that you select Management Interface instead of this option.

You cannot select a passive interface. For connection and intrusion syslog messages, the source IP address will either be for the management interface, or for the gateway interface if you route through data interfaces.

- **Management Interface**—Use the virtual management interface for all types of syslog messages. The source IP address will either be for the management interface, or for the gateway interface if you route through data interfaces.

Step 5 Click **Add**.

Step 6 Preview and Deploy Configuration Changes for All Devices now the changes you made, or wait and deploy multiple changes at once.

Edit Syslog Server Objects

To edit an existing syslog server object, follow these steps:

Procedure

Step 1 In the CDO navigation bar on the left, click **Objects > FDM Objects**.

Step 2 Locate the desired syslog server object and select it. You can **filter** the object list by the syslog server object type.

Step 3 In the Actions pane, click **Edit**.

Step 4 Make the desired edits and click **Save**.

Step 5 Confirm the changes you made.

Step 6 Preview and Deploy Configuration Changes for All Devices now the changes you made, or wait and deploy multiple changes at once.

Related Information:

- Deleting Objects

Create a Syslog Server Object for Secure Logging Analytics (SaaS)

Create a syslog server object with the IP address, TCP port, or UDP port of the Secure Event Connector (SEC) you want to send events to. You would create one syslog object for every SEC that you have onboarded to your tenant but you would only send events from one rule to one syslog object representing one SEC.

Prerequisite

This task is part of a larger workflow. See Implementing Secure Logging Analytics (SaaS) for FDM-Managed Devices before you begin.

Procedure

Procedure

Step 1 In the CDO navigation bar on the left, click **Objects** > **FDM Objects**.

Step 2 Click the **Create Object** button  .

Step 3 Select **Syslog Server** under FDM-managed device object types.

Step 4 Configure the syslog server object properties. To find these properties of the SEC, from the navigation pane on the left, choose **Tools & Services** > **Secure Connectors**. Then select the Secure Event Connector you want to configure the syslog object for and look in the Details pane on the right.

- **IP Address**—Enter the IP address of the SEC.
- **Protocol Type**—Select TCP or UDP.
- **Port Number**—Enter port 10125 if you selected TCP or 10025 if you selected UDP.
- **Select an interface**—Select the interface configured to reach the SEC.

Note FDM-managed device supports one syslog object per IP address so you will have to choose between using TCP and UDP.

Step 5 Click **Add**.

What to do next

Continue with Step 3 of Existing CDO Customer Workflow to Implement Secure Logging Analytics (SaaS) and Send Events through the Secure Event Connector to the Cisco Cloud.

Manage Security Policies in CDO

Security policies examine network traffic with the ultimate goal of allowing the traffic to its intended destination or dropping it if a security threat is identified. You can use CDO to configure security policies on many different types of devices.

- FDM Policy Configuration, on page 100
- Network Address Translation, on page 179

FDM Policy Configuration

Security policies examine network traffic with the ultimate goal of allowing the traffic to its intended destination or dropping it if a security threat is identified. Use CDO to manage all the components of FDM-managed device's security policies.

FDM-Managed Access Control Policy

You can use Cisco Defense Orchestrator to manage the access control policy of an FDM-managed device. The access control policy controls access to network resources by evaluating network traffic against access control rules. The FDM-managed device compares the criteria of the access control rules, in the order they appear in the access control policy, to the network traffic. When all the traffic conditions in an access control rule are

- **Trust**—Allow traffic without further inspection of any kind.
- **Allow**—Allow the traffic subject to the intrusion and other inspection settings in the policy.
- **Block**—Drop the traffic unconditionally. The traffic is not inspected.

If none of the rules in the access control policy match the network traffic, the FDM-managed device takes the default action listed below the access control rules.

Read an FDM-Managed Access Control Policy

Procedure

Step 1 In the navigation pane, click **Inventory**.

Step 2 Click the **Devices** tab to locate the device or the **Templates** tab to locate the model device.

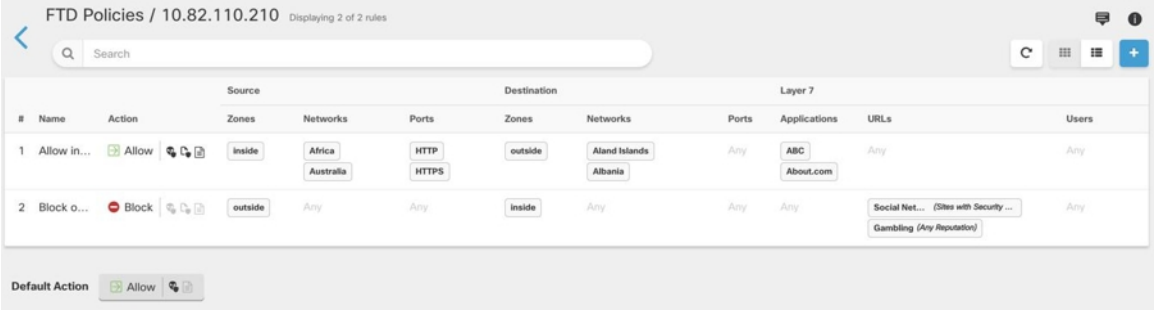
Step 3 Click the **FTD** tab and select the device whose policy it is you want to read.

Step 4 In the **Management** pane at the right, select **Policy**.

Step 5 To ensure that you see the whole policy, click **Show All** in the Filter panel.

Step 6 Toggle the rule column display to view the rules with more or fewer column. If you are used to viewing access control rules in an FDM-managed device, toggle the rule column display to show more columns.

Here is an example of how to read a rule in a policy. All traffic is evaluated against rule 1 first for a match. If the traffic matches rule 1, the action for that rule is applied to the traffic. Traffic that originates from the inside zone, AND originates from Africa OR Australia, AND originates from HTTP or HTTPS ports, AND arrives at the outside zone, AND arrives at the Aland Islands OR Albania, AND arrives at any port, AND arrives at ABC OR About.com is allowed to flow from the source to the destination. We can also see that an intrusion policy and a file policy are applied to the rule and that events from the rule are being logged.



Related Information:

- Configure the FDM Access Control Policy

Configure the FDM Access Control Policy

FDM-managed devices have a single policy. A section of that policy has access control rules. For ease of discussion, we refer to the section of the policy that has access control rules as the *access control policy*. After onboarding the FDM-managed device, you add rules to, or edit rules in, the access control policy.

If you are onboarding a new FDM-managed device, it may be that there are no rules in the policy that was imported. In that case, when you open the FDM Policy page, you will see the message, "No results found." If you see that message, you can start adding rules to the FDM-Managed Device Policy and then deploy them to the device from CDO.

Tips Before you Begin

When adding conditions to access control rules, consider the following tips:

- You can create custom objects for some of the conditions at the time you add them to the rule. Look in the dialog boxes for a link to create custom objects.
- You can configure multiple conditions per rule. Traffic must match all the conditions in the rule for the rule to apply to traffic. For example, you can use a single rule to perform URL filtering for specific hosts or networks.
- For each condition in a rule, you can add up to 50 criteria. Traffic that matches any of a condition's criteria satisfies the condition. For example, you can use a single rule to apply application control for up to 50 applications or application filters. Thus, there is an OR relationship among the items in a single condition, but an AND relationship between condition types (for example, between source/destination and application).
- Some features require that you have enabled the appropriate Firepower licenses.
- Some editing tasks may not require you to enter the edit mode. From the policy page, you can modify a condition in the rule by clicking the + button within that condition column and select the desired object or element in the popup dialog box. You can also click the **x** on an object or element to remove it from the rule.

Create or Edit an FDM-Managed Access Control Policy

Use this procedure to edit an FDM-managed access control policy using Cisco Defense Orchestrator:

Procedure

Step 1 In the navigation pane, click **Inventory**.

Step 2 Click the **Devices** tab to locate the device or the **Templates** tab to locate the model device.

Step 3 Click the **FTD** tab and whose access control whose policy you want to edit.

Step 4 In the **Management** pane at the right, select **Policy**.

Step 5 Do any of the following:

- To create a new rule, click the blue plus button .
- To edit an existing rule, select the rule and click the edit icon in the **Actions** pane. (Simple edits may also be performed inline without entering edit mode.)
- To delete a rule you no longer need, select the rule and click the remove icon in the Actions pane.
- To move a rule within the policy, select the rule in the access control table and click the up or down arrow at the end of the rule row to move the rule.

When editing or adding a rule, continue with the remaining steps in this procedure.

Step 6 In the **Order** field, select the position for the rule within the policy. Network traffic is evaluated against the list of rules in numerical order, 1 to "last."

Rules are applied on a first-match basis, so you must ensure that rules with highly specific traffic matching criteria appear above policies that have more general criteria that would otherwise apply to the matching traffic.

The default is to add the rule to the end of the list. If you want to change a rule's location later, edit this option.

Step 7 Enter the rule name. You can use alphanumeric characters, spaces, and these special characters: + . _ -

Step 8 Select the action to apply if the network traffic is matched by the rule:

- **Trust**—Allow traffic without further inspection of any kind.
- **Allow**—Allow the traffic subject to the intrusion and other inspection settings in the policy.
- **Block**—Drop the traffic unconditionally. The traffic is not inspected.

Step 9 Define the traffic matching criteria by using any combination of attributes in the following tabs:

- **Source**—Click the **Source** tab and add or remove security zones (interfaces), networks (which include networks, continents, and custom geolocations), or ports from which the network traffic originated. The default value is "Any."
- **Destination**—Click the **Destination** tab and add or remove the security zones (interfaces), networks (which include networks, continents and custom geolocations), or ports on which the traffic arrives. The default value is "Any." See Source and Destination Criteria in an FDM-Managed Access Control Rule.
- **Applications**—Click the **Application** tab and add or remove a web application, or a filter that defines applications by type, category, tag, risk, or business relevance. The default is any application. See Application Criteria in an FDM-Managed Access Control Rule

- **URLs**—Click the **URL** tab and add or remove a URL or URL category of a web request. The default is any URL. See URL Conditions in an FDM-Managed Access Control Rule to learn how to fine-tune this condition using URL categories and reputation filters.
- **Users**—Active Directory realm objects, special identities (failed authentication, guest, no authentication required, unknown), and user groups added to the rule from firewall device manager are visible in the rule row but it is not yet editable in CDO.

  Caution Individual user-objects are not yet visible in an access control policy rule in CDO. Log in to an FDM-managed device to see how an individual user-object may affect an access control policy rule.

Step 10 (Optional, for rules with the Allow action) Click the **Intrusion Policy** tab to assign an intrusion inspection policy to inspect traffic for intrusions and exploits. See Intrusion Policy Settings in an FDM-Managed Access Control Rule.

a. **To log Intrusion events** generated by intrusion policy rules, see " FDM-Managed Device Settings" for the device.

Step 11 (Optional, for rules with the Allow action) Click the **File Policy** tab to assign a file policy that inspects traffic for files that contain malware and for files that should be blocked. See File Policy Settings in an FDM-Managed Access Control Rule.

a. **To log file events** enerated by file policy rules, see "FDM-Managed Device Settings" for the device.

Step 12 (Optional) Click the logging tab to enable logging and collect **connection events** reported by the access control rule.

See Logging Settings in an FDM-Managed Access Control Rule for more information on logging settings.

If you subscribe to Cisco Security Analytics and Logging, you can configure connection events in CDO and send them to the Secure Event Connector (SEC) by configuring a syslog object with the SEC's IP address and port. See Cisco Security Analytics and Logging for more information about this feature. You would create one syslog object for every SEC that you have onboarded to your tenant, but you would only send events generated by one rule, to one syslog object, representing one SEC.

Step 13 Click **Save**. You are now done configuring a specific rule in the security policy.

Step 14 You can now configure the **Default Action** for the security policy as a whole. The Default Action defines what happens if network traffic does not match any of the rules in the access control policy, intrusion policy, or file/malware policy.

Step 15 Click the Default Action for the policy.

Step 16 Configure an intrusion policy as you did in step 9, above.

Step 17 Configure logging connection events generated by the Default Action.

If you subscribe to Cisco Security Analytics and Logging, you can send events generated by the default action to a Secure Event Connector (SEC) by configuring a syslog object with the SEC's IP address and port. See Cisco Security Analytics and Logging for more information about this feature. You would create one syslog object for every SEC that you have onboarded to your tenant, but you would only send events generated by rule to one syslog object, representing one SEC.

Step 18 (Optional) For any rule that you created, you can select it and add a comment about it in the Add Comments field. To learn more about rule comments see, Adding Comments to Rules in Policies and Rulesets.

Step 19 Preview and Deploy Configuration Changes for All Devices now the changes you made, or wait and deploy multiple changes at once.

Configuring Access Policy Settings

You can configure settings that apply to the access policy, rather than to specific rules within the policy.

Procedure

These settings apply to the access policy as a whole, rather than to specific rules within the policy.

Procedure

Step 1 In the navigation pane, click **Inventory**.

Step 2 Click the **Devices** tab to locate the device or the **Templates** tab to locate the model device.

Step 3 Click the **FTD** tab and whose access control whose policy you want to edit.

Step 4 In the **Management** pane at the right, select **Policy**.

Step 5 Click the **Settings** icon and configure these settings:

- **TLS Server Identity Discovery** - TLS 1.3 certificates are encrypted. For traffic encrypted with TLS 1.3 to match access rules that use application or URL filtering, the system must decrypt the TLS 1.3 certificate. We recommend that you enable this option to ensure encrypted connections are matched to the right access control rule. The setting decrypts the certificate only; the connection remains encrypted. Enabling this option is sufficient to decrypt TLS 1.3 certificates; you do not need to create a corresponding SSL decryption rule. Available for FDM-managed devices running software version 6.7 or later.
- **Reputation Enforcement on DNS Traffic** - Enable this option to apply your URL filtering category and reputation rules to DNS lookup requests. If the fully-qualified domain name (FQDN) in the lookup request has a category and reputation that you are blocking, the system blocks the DNS reply. Because the user does not receive a DNS resolution, the user cannot complete the connection. Use this option to apply URL category and reputation filtering to non-web traffic. For more information, see DNS Request Filtering. Available for FDM-managed devices running software version 7.0 and later.

Step 6 Click **Save**.

About TLS Server Identity Discovery

Typically, the TLS 1.3 certificates are encrypted. For traffic encrypted with TLS 1.3 to match access rules that use application or URL filtering, the system must decrypt the TLS 1.3 certificate. We recommend that you enable early application detection and URL categorization to ensure encrypted connections are matched to the right access control rule. This setting decrypts the certificate only; the connection remains encrypted.

Note This feature is currently available for FDM-managed devices running on software version 6.7 or later.

Procedure

Step 1 In the navigation pane, click **Inventory**.

Step 2 Click the **Devices** tab to locate the device or the **Templates** tab to locate the model device.

Step 3 Click the **FTD** tab and whose access control whose policy you want to edit.

Step 4 In the **Management** pane at the right, select **Policy**.

Step 5 Click the settings button.

Step 6 Click the slider next to **TLS Server Identity Discovery** to enable early application detection and URL categorization for encrypted connections.

Step 7 Click **Save**.

Copy FDM-Managed Access Control Rules

Use this procedure to copy access control rules by copying it from their current position and pasting them to a new position in the same policy or by pasting them to the policy of a different FDM-managed device. You can paste the rule before or after other rules in the policy, so the rule evaluates that network traffic in its proper order within the policy.

Copy Rules within the Device

To copy rules within an FDM-managed device, follow this procedure:

Procedure

Step 1 In the navigation pane, click **Inventory**.

Step 2 Click the **Devices** tab to locate the device or the **Templates** tab to locate the model device.

Step 3 Click the **FTD** tab and select the FDM-managed device you whose policy it is you want to edit.

Step 4 In the **Management** pane on the right, click **Policy**.

Step 5 Select one or more access control rules you want to copy and click **Copy** in the **Actions** pane on the right.

Step 6 In the policy where you want to paste the rule(s), select the rule that your copied rule(s) should precede or follow and, in the **Actions** pane, click one fo the following options:

- **Paste Before**automatically pastes one or more copied rules above the selected rule, so the copied rule is ordered above it.
- **Paste After**automatically pastes one or more copied rules below the selected rule, so the copied rule is ordered below it.

The paste operation can be performed multiple times at any required position.

Note When pasting rules within an FDM-managed device, if a rule with the same name exists, '- Copy' is appended to the original name. If the renamed name also exists, '- Copy n' is appended to the original name. For example, 'rule name - Copy 2'.

Step 7 Review your changes and Deploy Configuration Changes from CDO to FDM-Managed Device now or wait and deploy multiple changes at once.

Copy Rules from One FDM-Managed Device Policy to Another FDM-Managed Device Policy

When copying rules from one FDM-managed device policy to another FDM-managed device policy, objects associated with those rules are copied to the new FDM-managed device as well.

CDO validates some conditions when pasting the rules. For more information, see Behavior of Objects when Pasting Rules to Another Device.

Important **Important**: CDO allows you to copy rules from one FDM-managed device to another FDM-managed device only if the same software versions on both devices are the same. If the software version is different, the "Rules could not be pasted because they are not compatible with the version of this device" error appears when you attempt to paste the rules. You can click the **Details** link to know the details.

To copy rules to another FDM-managed device, follow this procedure:

Procedure

Step 1 In the navigation pane, click **Inventory**.

Step 2 Click the **Devices** tab to locate the device or the **Templates** tab to locate the model device.

Step 3 Click the **FTD** tab and select the device you want to copy the rule from.

Step 4 In the **Management** pane on the right, click **Policy**.

Step 5 Select one or more access control rules you want to copy and click **Copy** in the **Actions** pane on the right.

Step 6 Click **Inventory** and navigate to the FDM-managed device you want to paste the rules to.

Step 7 In the **Management** pane on the right, click **Policy**.

Step 8 In the policy where you want to paste the rule(s) you just copied, select the rule that your copied rule(s) should precede or follow and, in the **Actions** pane, click **Paste Before** or **Paste After**.

Step 9 Select any access control rule you want for pasting the copied rules around it and in the **Actions** pane, click one of the following options:

- **Paste Before** automatically one or more rules above the selected rule, so the copied rules evaluate network traffic before the selected rule.
- **Paste After** automatically one or more rules below the selected rule, so the copied rules evaluate network traffic after the selected rule.

The paste operation can be performed multiple times at any required position.

Note When pasting rules to another FDM-managed device, if a rule with the same name exists, '-Copy' is appended to the original name. If the renamed name also exists, '-Copy n' is appended to the original name. For example, 'rule name-Copy 2'.

Step 10 When you copy rules from one FDM-managed device to another, the **Configuration Status** of the destination device is in 'Not Synced' state. Review your changes and Deploy Configuration Changes from CDO to FDM-Managed Device now or wait and deploy multiple changes at once.

Related Information:

- Move FDM-Managed Access Control Rules
- Behavior of Objects when Pasting Rules to Another Device

Move FDM-Managed Access Control Rules

Use this feature to move access control rules by cutting it from their current position in a policy and pasting them to a new position in the same policy or to the policy of a different FDM-managed device. You can paste the rule before or after other rules in a policy, so the rule evaluates that network traffic in its proper order within the policy.

Move Rules within the Device

To move rules within an FDM-managed device, follow this procedure:

Procedure

Step 1 In the navigation pane, click **Inventory**.

Step 2 Click the **Devices** tab to locate the device or the **Templates** tab to locate the model device.

Step 3 Click the **FTD** tab and select the FDM-managed device whose policy it is you want to edit.

Step 4 In the **Management** pane on the right, click **Policy**.

Step 5 Select one or more access control rules you want to move and click **Cut**in the Actions pane on the right. The selected rules are highlighted in yellow. **Note**: If you want to cancel your selection, select any rule and click **Copy**.

Step 6 In the policy where you want to paste the rule(s) you just cut, select the rule that the cut rule(s) should precede or follow and, in the **Actions** pane, click one of the following options:

- **Paste Before** automatically pastes one or more rules above the selected rule, so the cut rules evaluate network traffic before the selected rule.
- **Paste After** automatically pastes one or more rules below the selected rule, so the cut rules evaluate network traffic after the selected rule.

The paste operation can be performed multiple times at any required position.

Note When pasting rules within an FDM-managed device, if a rule with the same name exists, '- Copy' is appended to the original name. If the renamed name also exists, '- Copy n' is appended to the original name. For example, 'rule name - Copy 2'.

Step 7 Review your changes and Deploy Configuration Changes from CDO to FDM-Managed Device now or wait and deploy multiple changes at once.

Move a Rule from One FDM-Managed Device Policy to Another FDM-Managed Device Policy

When moving rules from one FDM-managed device policy to another FDM-managed device policy, objects associated with those rules are copied to the new FDM-managed device as well.

CDO validates some conditions when pasting the rules. For more information on those conditions, see Behavior of Objects when Pasting Rules to Another Device.

To move rules to another FDM-managed device, follow this procedure:

Procedure

Step 1 In the navigation pane, click **Inventory**.

Step 2 Click the **Devices** tab to locate the device or the **Templates** tab to locate the model device.

Step 3 Click the **FTD** tab and select the FDM-managed device you want to copy the rule from.

Step 4 In the **Management** pane on the right, click **Policy**.

Step 5 Select one or more access control rules you want to move and click **Cut** in the **Actions** pane on the right.

Step 6 Click **Inventory** and navigate to the FDM-managed device you want to move one or more selected rules to.

Step 7 In the **Management** pane on the right, click **Policy**.

Step 8 In the policy where you want to paste the rule(s) you just cut, select the rule that your cut rule should precede or follow and, in the **Actions** pane, click **Paste Before** or **Paste After**.

- **Paste Before** automatically one or more rules above the selected rule, so the cut rules evaluate network traffic before the selected rule.
- **Paste After** automatically one or more rules below the selected rule, so the cut rules evaluate network traffic after the selected rule.

The paste operation can be performed multiple times at any required position.

Note When pasting rules within an FDM-managed device, if a rule with the same name exists, '-Copy' is appended to the original name. If the renamed name also exists, '- Copy n' is appended to the original name. For example, 'rule name - Copy 2'.

Step 9 When you copy rules from one FDM-managed device to another, the **Configuration Status** of source and destination devices are in 'Not Synced' state. Review your changes and Deploy Configuration Changes from CDO to FDM-Managed Device now or wait and deploy multiple changes at once.

Related Information:

- Copy FDM-Managed Access Control Rules
- Behavior of Objects when Pasting Rules to Another Device

Behavior of Objects when Pasting Rules to Another Device

If the rules you cut or copied contain objects, and you paste those rules into another FDM-managed device policy, CDO copies the objects in those rules to the destination FDM-managed device when any of the following conditions are met:

For all types of objects (except security zone)

- The destination device does not contain the object; in that case, CDO creates the object in the destination device first and then pastes the rule.
- The destination device contains the object with the same name and the same values as the source device.

For security zone objects

- The destination device contains the security zone object with the same name and the same interfaces as the source.
- The destination device does not contain the same security zone object and has interfaces for use on the destination.
- The destination device contains the security zone object, which is empty and has interfaces for use on the destination.

For objects with Active Directory (AD) realm

- CDO pastes the rule with Active Directory (AD) realm objects only if the realm with the same name already present on the target device.

Important The paste operation fails in the following conditions:

- If there are differences in the vulnerability, geolocation, intrusion, or URL databases between the two device versions, CDO cannot paste the rules into the target device. You need to recreate the rules manually in the new device.
- If the rule you are adding has a security zone that contains the interface of type 'management-only'.

Related Information:

- Copy FDM-Managed Access Control Rules
- Move FDM-Managed Access Control Rules

Source and Destination Criteria in an FDM-Managed Access Control Rule

The Source and Destination criteria of an access rule define the security zones (interfaces) through which the traffic passes, the IP addresses or the country or continent (geographical location) for the IP address, or the protocols and ports used in the traffic. The default is any zone, address, geographical location, protocol, and port.

To modify the source or destination conditions in an access control rule you can edit the rule using the procedure in Configure the FDM Access Control Policy. Simple edits may be performed without entering edit mode. From the policy page, you can modify a condition in the rule by selecting the rule and clicking the + button within the source or destination condition column and selecting a new object or element in the popup dialog box. You can also click the **x** on an object or element to remove it from the rule.

You can use the following criteria to identify the source and destination to match in the rule.

Source Zones, Destination Zones

The security zone objects that define the interfaces through which the traffic passes. You can define one, both, or neither criteria: any criteria not specified applies to traffic on any interface.

- To match traffic leaving the device from an interface in the zone, add that zone to the Destination Zones.
- To match traffic entering the device from an interface in the zone, add that zone to the Source Zones.
- If you add both source and destination zone conditions to a rule, matching traffic must originate from one of the specified source zones and egress through one of the destination zones.

Use this criteria when the rule should apply based on where the traffic enters or exits the device. For example, if you want to ensure that all traffic going to inside hosts gets intrusion inspection, you would select your inside zone as the Destination Zones while leaving the source zone empty. To implement intrusion filtering in the rule, the rule action must be Allow, and you must select an intrusion policy in the rule.

Note You cannot mix passive and routed security zones in a single rule. In addition, you can specify passive security zones as source zones only, you cannot specify them as destination zones.

Source Networks, Destination Networks

The network objects or geographical locations that define the network addresses or locations of the traffic.

- To match traffic from an IP address or geographical location, configure the Source Networks.
- To match traffic to an IP address or geographical location, configure the Destination Networks.
- If you add both source and destination network conditions to a rule, matching traffic must originate from one of the specified IP addresses and be destined for one of the destination IP addresses.

When you add this criteria, you select from the following tabs:

- Network—Select the network objects or groups that define the source or destination IP addresses for the traffic you want to control. You can use objects that define the address using the fully-qualified domain name (FQDN); the address is determined through a DNS lookup.
- Geolocation—Select the geographical location to control traffic based on its source or destination country or continent. Selecting a continent selects all countries within the continent. Besides selecting geographical location directly in the rule, you can also select a geolocation object that you created to define the location. Using geographical location, you could easily restrict access to a particular country without needing to know all of the potential IP addresses used there.

Note To ensure that you are using up-to-date geographical location data to filter your traffic, Cisco strongly recommends that you regularly update the geolocation database (GeoDB).

Source Ports, Destination Ports/Protocols

The port objects that define the protocols used in the traffic. For TCP/UDP, this can include ports. For ICMP, it can include codes and types.

- To match traffic from a protocol or port, configure the **Source Ports**. Source ports can be TCP/UDP only.
- To match traffic to a protocol or port, configure the **Destination Ports/Protocols**. If you add only destination ports to a condition, you can add ports that use different transport protocols. ICMP and other non-TCP/UDP specifications are allowed in destination ports only; they are not allowed in source ports.
- To match traffic both originating from specific TCP/UDP ports and destined for specific TCP/UDP ports, configure both. If you add both source and destination ports to a condition, you can only add ports that share a single transport protocol, TCP or UDP. For example, you could target traffic from port TCP/80 to port TCP/8080.

URL Conditions in an FDM-Managed Access Control Rule

The URL conditions of an access control rule defines the URL used in a web request, or the category to which the requested URL belongs. For category matches, you can also specify the relative reputation of sites to allow or block. The default is to allow all URLs.

URL categories and reputations allow you to quickly create URL conditions for access control rules. For example, you could block all Gaming sites, or all high risk Social Networking sites. If a user attempts to browse to any URL with that category and reputation combination, the session is blocked.

Using category and reputation data also simplifies policy creation and administration. It grants you assurance that the system will control web traffic as expected. Finally, because Cisco's threat intelligence is continually updated with new URLs, as well as new categories and risks for existing URLs, you can ensure that the system uses up-to-date information to filter requested URLs. Malicious sites that represent security threats such as malware, spam, botnets, and phishing may appear and disappear faster than you can update and deploy new policies.

To modify the URL and URL Category conditions in an access control rule, you can edit the rule using the procedure in Configure the FDM Access Control Policy. Simple edits may be performed without entering edit mode. From the policy page, you can modify a URL condition in the rule by selecting the rule and clicking the + button within the URL condition column and selecting a new object, element, URL reputation, or URL category from the popup dialog box. You can also click the **x** on an object or element to remove it from the rule.

Click the blue plus icon  and select URL objects, groups, or URL categories and click **Save**. You can click Create New Object if the URL object you require does not exist. See Create or Edit FDM URL Objects for more information about URL objects.

License Requirement for URL Filtering

To use URL filtering, you need to have the **URL** license enabled on your FDM-managed device.

Specifying a Reputation for a URL Category Used in a Rule

By default, all URLs in a URL category are treated by a rule the same way. For example, if you have a rule that blocks Social Network URLs, you will block all of them regardless of reputation. You can adjust that setting so that you block only high-risk Social Network sites. Likewise, you could allow all URLs from a URL category except the high-risk sites.

Use this procedure to use a reputation filter on a URL category in an access control rule:

Procedure

Step 1 From the FDM Policy page, select the rule you want to edit.

Step 2 Click **Edit**.

Step 3 Click the **URLs** tab.

Step 4 Click the blue plus button  and select a URL Category.

Step 5 Click **Apply Reputation to Selected Categories** or the **Any Reputation** link on the URL Category you just picked.

Step 6 Uncheck the **Any Reputation** check box.

Step 7 Filter URLs by reputation:

- If the rule has a blocking action, slide the reputation slider to the right to block only the sites with the reputations marked in red. For example, if you slide the slider to "Sites with Security Risks," a blocking rule would block "Sites with Security Risks," "Suspicious Sites," and "High-Risk sites" but it would allow traffic from "Well-known Sites" and "Benign Sites."
- If the rule has an allow action, slide the reputation slider to the right to allow only the sites with the reputations marked in green. For example, if you slide the slider to "Benign Sites," the rule will allow traffic from "Well-Known Sites" and "Benign Sites" but not allow traffic from "Sites with Security Risks," "Suspicious Sites," and "High-Risk sites."

Step 8 Click **Save**.

Step 9 Click **Select**.

Step 10 Click **Save**.

Step 11 Preview and Deploy Configuration Changes for All Devices now the changes you made, or wait and deploy multiple changes at once.

Intrusion Policy Settings in an FDM-Managed Access Control Rule

Cisco delivers several intrusion policies with the Firepower system. These policies are designed by the Cisco Talos Security Intelligence and Research Group, who set the intrusion and preprocessor rule states and advanced settings.

License and Action Requirements for Intrusion Policies

- **Licenses**-To add intrusion policies to a rule, you need to enable an license on the FDM-managed device
- **Rule action**-you can configure intrusion and file policies on rules that **allow** traffic only. Inspection is not performed on rules set to **trust** or **block** traffic. In addition, if the default action for the access control policy is **allow**, you can configure an intrusion policy but not a file policy.

Available Intrusion Policies for an Access Control Rule

For access control rules that allow traffic, you can select one of the following intrusion policies to inspect traffic for intrusions and exploits. An intrusion policy examines decoded packets for attacks based on patterns, and can block or alter malicious traffic.

The policies are listed from least to most secure:

- **Connectivity over Security**—This policy is built for organizations where connectivity (being able to get to all resources) takes precedence over network infrastructure security. The intrusion policy enables far fewer rules than those enabled in the Security over Connectivity policy. Only the most critical rules that block traffic are enabled. Select this policy if you want to apply some intrusion protection but you are fairly confident in the security of your network.
- **Balanced Security and Connectivity**—This policy is designed to balance overall network performance with network infrastructure security. This policy is appropriate for most networks. Select this policy for most situations where you want to apply intrusion prevention.
- **Security over Connectivity**—This policy is built for organizations where network infrastructure security takes precedence over user convenience. The intrusion policy enables numerous network anomaly intrusion rules that could alert on or drop legitimate traffic. Select this policy when security is paramount or for traffic that is high risk.
- **Maximum Detection**—This policy is built for organizations where network infrastructure security is given even more emphasis than is given by the Security Over Connectivity policy, with the potential for even greater operational impact. For example, the intrusion policy enables rules in a large number of threat categories including malware, exploit kit, old and common vulnerabilities, and known in-the-wild exploits. If you select this policy, carefully evaluate whether too much legitimate traffic is being dropped.

Related Information

- Intrusion, File, and Malware Inspection in FDM-Managed Access Control Policies

File Policy Settings in an FDM-Managed Access Control Rule

Use file policies to detect malicious software, or *malware*, using Advanced Malware Protection for Firepower (AMP for Firepower). You can also use file policies to perform file control, which allows control over all files of a specific type regardless of whether the files contain malware.

AMP for Firepower uses the AMP cloud to retrieve dispositions for possible malware detected in network traffic, and to obtain local malware analysis and file pre-classification updates. The management interface must have a path to the Internet to reach the AMP cloud and perform malware lookups. When the device detects an eligible file, it uses the file's SHA-256 hash value to query the AMP cloud for the file's disposition. The possible dispositions are:

- Malware—The AMP cloud categorized the file as malware. An archive file (e.g. a zip file) is marked as malware if any file within it is malware.
- Clean—The AMP cloud categorized the file as clean, containing no malware. An archive file is marked as clean if all files within it are clean.
- Unknown—The AMP cloud has not assigned a disposition to the file yet. An archive file is marked as unknown if any file within it is unknown.
- Unavailable—The system could not query the AMP cloud to determine the file's disposition. You may see a small percentage of events with this disposition; this is expected behavior. If you see a number of "unavailable" events in succession, ensure that the Internet connection for the management address is functioning correctly.

License and Action Requirements for File Policies

Licenses-To add file policies to a rule, you need to enable two licenses on the Firepower Device Manager:

- license
- Malware license

Rule action-You can configure file policies on rules that allow traffic only. Inspection is not performed on rules set to trust or block traffic. In addition, if the default action for the access control policy is allow, you can configure an intrusion policy but not a file policy.

Available File Policies for an Access Control Rule

- **None**—Do not evaluate transmitted files for malware and do no file-specific blocking. Select this option for rules where file transmissions are trusted or where they are unlikely (or impossible), or for rules where you are confident your application or URL filtering adequately protects your network.
- **Block Malware All**—Query the AMP cloud to determine if files traversing your network contain malware, then block files that represent threats.
- **Cloud Lookup All**—Query the AMP cloud to obtain and log the disposition of files traversing your network while still allowing their transmission.
- **Block Office Document and PDF Upload, Block Malware Others**—Block users from uploading Microsoft Office documents and PDFs. Additionally, query the AMP cloud to determine if files traversing your network contain malware, then block files that represent threats.
- **Block Office Documents Upload, Block Malware Others**—Block users from uploading Microsoft Office documents. Additionally, query the AMP cloud to determine if files traversing your network contain malware, then block files that represent threats.

Releated Information:

- Intrusion Policy Settings in an FDM-Managed Access Control Rule

Logging Settings in an FDM-Managed Access Control Rule

Logging Settings for Access Control Rule

The logging settings for an access rule determine whether connection events are issued for traffic that matches the rule.

You should log connections according to the security and compliance needs of your organization. If your goal is to limit the number of events you generate and improve performance, only enable logging for the connections critical to your analysis. However, if you want a broad view of your network traffic for profiling purposes, you can enable logging for additional connections.

Caution Logging blocked TCP connections during a Denial of Service (DoS) attack can affect system performance and overwhelm the database with multiple similar events. Before you enable logging for a Block rule, consider whether the rule is for an Internet-facing interface or other interface vulnerable to DoS attack.

Procedure

Procedure

Step 1 Configure the FDM Access Control Policy and click the **Logging** tab.

Step 2 Specify the log action:

- **Log at Beginning and End of Connection**—Issue events at the start and end of a connection. Because end-of-connection events contain everything that start-of-connection events contain, plus all of the information that could be gleaned during the connection, Cisco recommends that you do not select this option for traffic that you are allowing. Logging both events can impact system performance. However, this is the only option allowed for blocked traffic.
- **Log at End of Connection**—Select this option if you want to enable connection logging at the end of the connection, which is recommended for allowed or trusted traffic.
- **Log None**—Select this option to disable logging for the rule. This is the default.

Note When an intrusion policy, invoked by an access control rule, detects an intrusion and generates an intrusion event, the system automatically logs the end of the connection where the intrusion occurred, regardless of the logging configuration of the rule. For connections where an intrusion was blocked, the action for the connection in the connection log is **Block**, with a reason of **Intrusion Block**, even though to perform intrusion inspection you must use an Allow rule.

Step 3 Specify where to send connection events:

If you want to send a copy of the events to an external syslog server, select the server object that defines the syslog server. If the required object does not already exist, you will need to create one. See Create and Edit Syslog Server Objects for more information.

Because event storage on the device is limited, sending events to an external syslog server can provide more long-term storage and enhance your event analysis.

For Cisco Security Analytics and Logging subscribers:

- If you send events to the Cisco cloud through a Secure Event Connector (SEC), specify an SEC as your syslog server. You will then be able to see these events alongside file policy and malware policy connection events.
- If you send events directly to the Cisco cloud without an SEC, specify when to log events (at the beginning or end of the connection) but do not specify the SEC as the syslog server.

Step 4 File Events

Check **Log Files** if you want to enable logging of prohibited files or malware events. You must select a file policy in the rule to configure this option. The option is enabled by default if you select a file policy for the rule. We recommend you leave this option enabled.

When the system detects a prohibited file, it automatically logs one of the following types of event to the FDM-managed internal buffer.

- File events, which represent detected or blocked files, including malware files.
- Malware events, which represent detected or blocked malware files only.

- Retrospective malware events, which are generated when the malware disposition for a previously detected file changes.

For connections where a file was blocked, the action for the connection in the connection log is Block even though to perform file and malware inspection you must use an Allow rule. The connection's Reason is either File Monitor (a file type or malware was detected), or Malware Block or File Block (a file was blocked)

Step 5 Click **Save**.

Step 6 Preview and Deploy Configuration Changes for All Devices now the changes you made, or wait and deploy multiple changes at once.

Security Group Tags

About Security Group Tags

If you use Cisco Identity Services Engine (ISE) to define and use **security group tag** (SGT) for classifying traffic in a Cisco TrustSec network, you can write access control rules that use SGT as matching criteria. Thus, you can block or allow access based on security group membership rather than IP addresses.

In ISE, you can create a SGT and assign host or network IP addresses to each tag. If you assign an SGT to a user's account, the SGT is assigned to the user's traffic. After you configure FDM-managed device to connect to an ISE server and create the SGT, you can create SGT groups in Cisco Defense Orchestrator and build access control rules around them. Note that you must configure ISE's SGT Exchange Protocol (SXP) mapping before you can associate an SGT to an FDM-managed device. See **Security Group Tag Exchange Protocol** in the Cisco Identity Services Engine Administrator Guide of the version you are currently running for more information.

When an FDM-managed device evaluates SGT as a traffic matching criteria for an access control rule, it uses the following priority:

1. The source SGT defined in the packet, if any. No destination matching is done using this technique. For the SGT to be in the packet, the switches and routers in the network must be configured to add them. See the ISE documentation for information on how to implement this method.
2. The SGT assigned to the user session, as downloaded from the ISE session directory. You need to enable the option to listen to session directory information for this kind of SGT matching, but this option is on by default when you first create the ISE identity source. The SGT can be matched to source or destination. Although not required, you would also normally set up a passive authentication identity rule, using the ISE identity source along with an AD realm, to collect user identity information.
3. The SGT-to-IP address mapping downloaded using SXP. If the IP address is within the range for an SGT, then the traffic matches the access control rule that uses the SGT. The SGT can be matched to source or destination.

Note You cannot use the information retrieved from ISE directly in an access control rule. Instead, you need to create SGT groups, which refer to the downloaded SGT information. Your SGT groups can refer to more than one SGT, so you can apply policy based on a relevant collections of tags if that is appropriate.

Version Support

CDO currently supports SGT and SGT groups on FDM-managed devices running Version 6.5 and later. an FDM-managed device allows you to configure and connect to an ISE server in Version 6.5 and later but not does not support SGT configuration in the UI until Version 6.7.

From the FDM-managed UI, this means that an FDM-managed device running Version 6.5 or later can download SXP mappings of SGTs but cannot be manually added to objects or access control rules. To make changes to the SGTs for devices running Version 6.5 or Version 6.6, you must use the ISE UI. If the device running Version 6.5 is onboarded to Cisco Defense Orchestrator, however, you can see the current SGTs associated with the device and create SGT groups.

SGT in CDO

Security Group Tags

SGTs are read-only in CDO. You cannot create or edit an SGT in CDO. To create an SGT, see the Cisco Identity Services Engine Administrator Guide of the version your are currently running.

SGT Groups

Note An FDM-managed device refers to groups of SGTs as SGT dynamic objects. In CDO, these lists of tags are currently called SGT groups. You can create an SGT group in CDO without referring to the FDM-managed device or ISE UI.

Use SGT groups to identify source or destination addresses based on an SGT assigned by ISE. You can then use the objects in access control rules for purposes of defining traffic matching criteria. You cannot use the information retrieved from ISE directly in an access control rule. Instead, you need to create SGT groups, which refer to the downloaded SGT information.

Your SGT groups can refer to more than one SGT, so you can apply policy based on relevant collections of tags if that is appropriate.

In order to create an SGT group in CDO, you must have at least one SGT already configured and SGT mappings from an ISE server configured for the FDM-managed console of the device you want to use. Note that if more than one FDM-managed device is associated with the same ISE server, an SGT or SGT group can be applied to more than one device. If a device is not associated with an ISE server, you cannot include SGT objects in your access control rule, or apply an SGT group to that device configuration.

SGT Groups in Rules

SGT groups can be added to access control rules; they appear as source or destination network objects. For more information about how networks work in rules, see Source and Destination Criteria in an FDM-Managed Access Control Rule.

You can create an SGT group from the Objects page. See Create an SGT Group for more information.

Create an SGT Group

To create an SGT group that can be used for an access control rule, use the following procedure:

Before you begin

You must have the following configurations or environments configured prior to creating a security group tag (SGT) group:

- FDM-managed device must be running at least Version 6.5.
- You must configure the ISE identity source to subscribe to SXP mappings and enable deploy changes. To manage SXP mappings, see **Configure Security Groups and SXP Publishing in ISE** of the Firepower Device Manager Configuration Guide for the version you're using, Version 6.7 and later.
- All SGTs must be created in ISE. To create an SGT, see the Cisco Identity Services Engine Configuration Guide of the version your are currently running.

Procedure

Step 1 In the CDO navigation bar on the left, click **Objects > FDM Objects**.

Step 2 Click the blue plus button  to create an object.

Step 3 Click **FTD > Network**.

Step 4 Enter an **Object Name**.

Step 5 (Optional) Add a description.

Step 6 Click **SGT** and use the drop-down menu to check all the applicable SGTs you want included in the group. You can sort the list by SGT name.

Step 7 Click **Save**.

Note You cannot create or edit SGTs in CDO, you can only add or remove them from an SGT group. To create or edit an SGT, see the Cisco Identity Services Engine Configuration Guide of the version you are currently running.

Edit an SGT Group

To edit an SGT group, use the following procedure:

Procedure

Step 1 In the CDO navigation bar on the left, click **Objects > FDM Objects**.

Step 2 Locate the SGT group you want to edit by using object filters and search field.

Step 3 Select the SGT group and click the edit icon  in the **Actions** pane.

Step 4 Modify the SGT group. Edit the name, description, or the SGTs associated with the group.

Step 5 Click **Save**.

Note You cannot create or edit SGTs in CDO, you can only add or remove them from an SGT group. To create or edit an SGT, see the Cisco Identity Services Engine Configuration Guide of the version you are currently running.

Add an SGT Group to an Access Control Rule

To add an SGT group to an access control rule, use the following procedure:

Procedure

Step 1 In the navigation pane, click **Inventory**.

Step 2 Click the **Devices** tab to locate the device or the **Templates** tab to locate the model device.

Step 3 Click the **FTD** tab and select the device you want to add the SGT group to.

Step 4 In the**Management** pane, select **Policy**.

Step 5 Click the blue plus button  for either the **Source** or **Destination** objects and select **SGT Groups**.

Step 6 Locate the SGT group(s) you want to edit by using object filters and search field.

Step 7 Click **Save**.

Step 8 Preview and Deploy Configuration Changes for All Devices.

Note If you need to create an additional SGT group, click **Create New Object**. Fill in the required information mentioned in Create an FTD SGT Group and **Add** the SGT group to the rule.

Application Criteria in an FDM-Managed Access Control Rule

The Application criteria of an access rule defines the application used in an IP connection, or a filter that defines applications by type, category, tag, risk, or business relevance. The default is any application.

Although you can specify individual applications in the rule, application filters simplify policy creation and administration. For example, you could create an access control rule that identifies and blocks all high risk, low business relevance applications. If a user attempts to use one of those applications, the session is blocked.

In addition, Cisco frequently updates and adds additional application detectors via system and vulnerability database (VDB) updates. Thus, a rule blocking high risk applications can automatically apply to new applications without you having to update the rule manually.

You can specify applications and filters directly in the rule, or create application filter objects that define those characteristics. The specifications are equivalent, although using objects can make it easier to stay within the 50-items-per-criteria system limit if you are creating a complex rule. See Create and Edit a Firepower Application Filter Object for more information about creating an application filter object.

To modify the application and application filters used in a rule, you can edit the rule using the procedure in FDM-Managed Access Control Policy. Simple edits may be performed without entering edit mode. From the policy page, you can modify an application condition in the rule by selecting the rule and clicking the + button within the application condition column and selecting a new object or element in the popup dialog box. You can also click the **x** on an object or element to remove it from the rule.

Intrusion, File, and Malware Inspection in FDM-Managed Access Control Policies

Intrusion and file policies work together as the last line of defense before traffic is allowed to its destination:

- Intrusion policies govern the system's intrusion prevention capabilities.
- File policies govern the system's file control and AMP for Firepower capabilities.

All other traffic handling occurs before network traffic is examined for intrusions, prohibited files, and malware. By associating an intrusion or file policy with an access control rule, you are telling the system that before it passes traffic that matches the access control rule's conditions, you first want to inspect the traffic with an intrusion policy, a file policy, or both.

You can configure intrusion and file policies on rules that allow traffic only. Inspection is not performed on rules set to trust or block traffic. In addition, if the default action for the access control policy is allow, you can configure an intrusion policy but not a file policy.

For any single connection handled by an access control rule, file inspection occurs before intrusion inspection. That is, the system does not inspect files blocked by a file policy for intrusions. Within file inspection, simple blocking by type takes precedence over malware inspection and blocking. Until a file is detected and blocked in a session, packets from the session may be subject to intrusion inspection.

Note By default, the system disables intrusion and file inspection of encrypted payloads. This helps reduce false positives and improve performance when an encrypted connection matches an access control rule that has intrusion and file inspection configured. Inspection works with unencrypted traffic only.

Related Information:

- Intrusion Policy Settings in an FDM-Managed Access Control Rule
- File Policy Settings in an FDM-Managed Access Control Rule

Custom IPS Policy in an FDM-Managed Access Control Rule

You cannot have more than one instance of the same custom IPS policy associated to a single device.

Note Associating an IPS policy with an access control rule means that passing traffic is submitted to deep packet inspection. The only supported rule action for an access control rule with an IPS policy is **Allow**.

Use the following procedure to associate a custom IPS policy to an FDM-managed device:

Procedure

Step 1 Create a custom IPS policy. See Configure Firepower Custom IPS Policies for more information.

Step 2 From the Cisco Defense Orchestrator Navigation pane, select **Policies**. Click **FTD / Meraki / AWS Policies**.

Step 3 Scroll or filter through the list of FDM-managed device policies and select the policy you want to associate with a custom IPS policy.

Step 4 Click the blue plus button  .

Step 5 In the **Order** field, select the position for the rule within the policy. Network traffic is evaluated against the list of rules in numerical order, 1 to "last."

Step 6 Enter the rule name. You can use alphanumeric characters, spaces, and these special characters: + . _ -

Step 7 Select the **Intrusion Policy** tab. Expand the drop-down menu to see all the available intrusion policies and select the desired custom IPS policy.

Step 8 Define the traffic matching criteria by using any combination of attributes in the remaining tabs: **Source/Destination**, **URLs**, **Applications**, and **File Policy**.

Step 9 (Optional) Click the logging tab to enable logging and collect **connection events** reported by the access control rule.

Step 10 Click **Save**.

Step 11 Preview and Deploy Configuration Changes for All Devices now the changes you made, or wait and deploy multiple changes at once.

TLS Server Identity Discovery in Firepower Threat Defense

You can now perform improved URL filtering and application control on traffic with threat defense's unique TLS Server Identity Discovery that allows control and precision when it comes to your environment. You do not have decrypt the traffic for this feature to work.

Note Support for the Server Identity Discovery feature is limited to Version 6.7 and later.

Enable the TLS Server Identity Discovery

Use the following procedure to enable, or disable, the TLS Server Identity Discovery feature for your FDM-managed access control policies:

Procedure

Step 1 In the navigation pane, click **Inventory**.

Step 2 Click the **Devices** tab to locate the device or the **Templates** tab to locate the model device.

Step 3 Click the **FTD** tab and select the device.

Step 4 In the **Management** pane located to the right, select **Policy**.

Step 5 Click the Access Policy Settings gear icon  in the upper right corner of the table .

Step 6 Slide the toggle to enable TLS Server Identity Discovery.

Step 7 Click **Save**.

Intrusion Prevention System

The Cisco Talos Intelligence Group (Talos) detects and correlates threats in real time and maintains a reputation disposition on billions of files. The Cisco IOS Intrusion Prevention System (IPS) is an inline, deep-packet inspection feature that mitigates attacks on your network by using the threat intelligence data from Talos to accurately identify, classify, and drop malicious traffic in real time.

Cisco Defense Orchestrator (CDO) provides the ability to activate and tune the IPS feature on FDM-managed devices that run software versions 6.4.x.x through 6.6.0.x and 6.6.1.x.

Note CDO currently does not support IPS rule tuning on version 6.7.

On the CDO menu bar, navigate **Policies > Signature Overrides** to perform these tasks:

- Resolve inconsistencies in overrides across multiple devices.
- View and hide threat events.
- Override how a threat event is handled by changing the rule action.

Related Information:

- Firepower Intrusion Policy Signature Overrides
- Threat Events
- Troubleshoot Intrusion Prevention System

Threat Events

A threat event report is a report of traffic that has been dropped, or that has generated an alert, after matching one of Cisco Talos' intrusion policies. In most cases, there's no need to tune IPS rules. If necessary, you have the option to override how an event is handled by changing the matching rule action in Cisco Defense Orchestrator.

Note the following behaviors of the Threats page:

- Threat events that are displayed are not live. Devices are polled hourly for additional Threat events.
- Threat events that are not included in the Live or Historical view are not part of Cisco Security Analytics and Logging.
- To see Threat events that you've hidden from view, click the filter icon and check the **view hidden** option.
- If you are a subscriber to Cisco Security Analytics and Logging , the events you see in Threat Events table do not contain events sent to the Secure Event Connector.

Procedure

Step 1 From the navigation pane, select **Monitoring** > **Threats**. You can filter what events are shown and search by source IP address.

Step 2 Click on a threat event to expand the details panel on the right.

a) For more information on the rule, click the **Rule Document** URL in the **Rule Details** section.
b) To hide this event, check the toggle switch for **Hide Events**. The event handling continues as is, but you won't see it here, unless you click **View Hidden** or un-hide this event.
c) To edit rule overrides, click **Tune Rule**. When you change a rule action in CDO, the override applies to all the pre-defined policies. This is different than in the FDM-managed device where each rule can be different from policy to policy.

Note CDO provides the ability to tune rules on FDM-managed devices that run software versions 6.4.x.x through 6.6.0.x and 6.6.1.x. CDO currently does not support rule tuning on FDM-managed Version 6.7.

- In the **Override All** devices pull-down, select an action and click **Save**.
  - **Drop**-This choice creates an event when this rule matches traffic and then drops the connection. Use this action to tighten security of certain rules. For example, specifying Drop would make security stricter when the Talos rule is matched even if the "Connectivity over Security" policy is specified for the access control rule.
  - **Alert**-This choice creates an event when this rule matches traffic, but it does not drop the connection. A use case for "Alert" is when traffic is blocked, but the customer wants to allow, it and look at the alerts before disabling the rule.
  - **Disabled**-This choice prevents traffic from being matched to the rule. No events are generated. The use case for "Disabled" is to stop false positives in reports, or remove rules that do not apply to your environment, like disabling Apache httpd rules if you don't use httpd.
  - **Default**-This choice returns a rule to the default action it was assigned by Talos, for the intrusion policy it is listed in. For example, when you return an intrusion rule to "Default" that may mean its action returns to "Alert" in the "Connectivity over Security" policy and "Block" in the "Balanced Security and Connectivity" policy.
- To edit rule overrides by device, check the **Advanced Options** slider. This section shows you the configured rule action for each device, which you can change by checking the affected device, selecting an override action, and clicking **Save**.
- **Affected Devices** does not indicate the source devices. Instead, it shows the FDM-managed devices reporting the event.

Note
- Click the refresh ( ) button to refresh the table that shows threats based on the current search filters.
- Click the export ( ) button to download the current summary of the threats to a comma-separated value (.csv) file. You can open the .csv file in a spreadsheet application such as Microsoft Excel to sort and filter the items on your list. CDO exports the basic threat details to the file except for additional information such as time, source, and device.

Step 3 Preview and Deploy Configuration Changes for All Devices now the changes you made, or wait and deploy multiple changes at once.

Firepower Intrusion Policy Signature Overrides

In most cases, there's no need to tune any IPS rules. If necessary, you have the option to override how an event is handled by changing the matching rule action in CDO. CDO gives you options to resolve issues with the overrides.

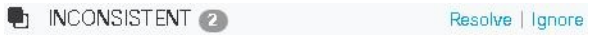
Manage Signature Overrides

Procedure

Step 1 From the main navigation bar, click **Policies > Signature Overrides**. You can filterwhat devices and policy override policies are shown. You can also search for intrusion policies by name or intrusion rule SID.

Step 2 Click on the name of policy override policy to expand the details panel on the right.

Step 3 In the **Issues** pane, a badge indicates the overrides are inconsistent across the devices. You can see the INCONSISTENT field with the number of devices affected:



a) **To ignore the issue**, click **Ignore**. This doesn't change the issue but removes the indicator badge from the **Issues** column.

b) **To resolve the issue**, click **Resolve**. In the left panel, select the policies to compare and show their consistent and inconsistent overrides.

- To merge the policies together:
  1. Click **Resolve by Merging** to combine them into a single policy with the same overrides on all its devices.
  2. Click **Confirm**.
- To rename a policy:
  1. In the policy's section, click **Rename** and give it a different name.
  2. Click **Confirm**.
- To ignore a policy:
  1. In the policy's section, click **Ignore**.
  2. Click **Confirm**.
- To ignore all the inconsistencies, click **Ignore All**.

Step 4 If there are individual Talos intrusion rules that were changed on the device using an FDM-managed device you will see them in the **Overrides** pane. You can change the override action for an intrusion rule by clicking **Tune** link and choosing an override action. This action will be applied to that rule in all of the Talos intrusion policies it's used in. Note that if you choose to restore the default action rule (**Default**), you cannot tune the intrusion rule again until it is triggered by the environment.

- Connectivity over Security
- Balanced Security and Connectivity

- Security over Connectivity
- Maximum Detection

For consistency across devices, the override action will be saved to every device associated with the intrusion override policy.

These are the effects of the override action:

- **Drop**-This choice creates an event when this rule matches traffic and then drops the connection. Use this action to tighten security of certain rules. For example, specifying Drop would make security stricter when the Talos rule is matched even if the "Connectivity over Security" policy is specified for the access control rule.
- **Alert**-This choice creates an event when this rule matches traffic, but it does not drop the connection. A use case for "Alert" is when traffic is blocked, but the customer wants to allow, it and look at the alerts before disabling the rule.
- **Disabled**-This choice prevents traffic from being matched to the rule. No events are generated. The use case for "Disabled" is to stop false positives in reports, or remove rules that do not apply to your environment, like disabling Apache httpd rules if you don't use httpd.
- **Default**-This choice is only applicable if the rule's default action is different in the Talos intrusion policy levels. For example, when you return an intrusion rule to "Default" that may mean its action returns to "Alert" in the "Connectivity over Security" policy and "Block" in the "Balanced Security and Connectivity" policy.
- Edit rule overrides with the following options:
  - **Override for all devices** - This option sets the required action to all the devices managed by CDO. Select an option from the drop-down menu. If the rule has different override values for different intrusion override policies, the drop-down option is "Multiple" by default.
  - **Edit rule overrides by device** - check the **Advanced Options** slider and select the **Overrides by Devices** tab. This option shows you the configured rule action for each device, which you can change by checking the affected device, selecting an override action, and clicking **Save**.
  - **Edit rule overrides by policy** - check the **Advanced Options** slider and select the **All Overrides** tab. This section is only applicable if your tenant has more than one IPS policy configured. You can manage all IPs policies from this page, including policies that have more than one device associated to it.

Step 5 Preview and Deploy Configuration Changes for All Devices now the changes you made, or wait and deploy multiple changes at once.

Create A Signature Override

You can only create signature overrides for IPS rules that are already triggered on an FDM-managed device. When you create a signature override in CDO, the override is automatically applies the configured action (**Drop**, **Alert**, **Disabled**, **Default**) to all of the policy levels.

Procedure

Step 1 From the main navigation bar, click **Monitoring> Threats**.

Step 2 Select a threat from the table and expand it. In the Tune Actions pane, click **Tune**.

Step 3 Tune the rules as described in **step 4** in the Firepower Intrusion Policy Signature Overrides procedure.

Step 4 Preview and Deploy Configuration Changes for All Devices now the changes you made, or wait and deploy multiple changes at once.

Remove A Signature Override

Procedure

Step 1 From the main navigation bar, click **Policies > Signature Overrides**.

Step 2 Click on the name of override to expand the details panel on the right.

Step 3 Expand the Overrides pane and select the override you want to remove, then click **Tune**.

Step 4 Set the default action to **Default**.

Step 5 Preview and Deploy Configuration Changes for All Devices now the changes you made, or wait and deploy multiple changes at once.

Custom Firepower Intrusion Prevention System Policy

About Custom IPS Policies

With the introduction of version 6.7, the improved Snort 3 processing engine allows you to create and customize Intrusion Prevention System (IPS) policies using rules provided by the Cisco Talos Intelligence Group (Talos). The best practice is to create your own policy based on the provided Talos policy templates and change that if you need to adjust rule actions.

Note At this time, CDO does not support custom IPS rules. You can create and modify custom IPS policies with rules that are provided by Talos, but you cannot create your own IPS rules and apply them to custom IPS policies.

The base templates include the same list of intrusion rules (also known as signatures), but they differ in the actions taken for each rule. For example, a rule might be enabled in one policy, but disabled in another policy.For another example, you may find that a particular rule is giving you too many false positives, where the rule is blocking traffic that you do not want blocked; you can disable the rule without needing to switch to a less-secure intrusion policy. You could alternatively change it to alert on matches without dropping traffic.

IPS Policy Base Template

The base templates include the same list of intrusion rules (also known as signatures), but they differ in the actions taken for each rule. For example, a rule might be enabled in one policy, but disabled in another policy. For another example, you may find that a particular rule is giving you too many false positives, where the

rule is blocking traffic that you do not want blocked; you can disable the rule without needing to switch to a less-secure intrusion policy. You could alternatively change it to alert on matches without dropping traffic.

The base templates provided are suggested configurations based on the type of protection your network might need. You can use any of the following templates as the base when you create a new policy:

Caution Do **not** modify the default IPS policies provided with an FDM-managed device enabled with Snort 3. We **strongly** recommend creating new custom IPS policies based on the templates below, and to use a unique name for the new policy that is different from the names of the default IPS policies listed below. If you need to troubleshoot your policies, Cisco TAC can easily locate the custom policy and revert to a default policy; this keeps your network protected without losing your customized changes.

The base templates provided are suggested configurations based on the type of protection your network might need. You can use any of the following templates as the base when you create a new policy:

- **Maximum Detection** - These policies are built for networks where network infrastructure security is given even more emphasis than is given by the Security Over Connectivity policies, with the potential for even greater operational impact.
- **Security Over Connectivity** - These policies are built for networks where network infrastructure security takes precedence over user convenience. The intrusion policy enables numerous network anomaly intrusion rules that could alert on or drop legitimate traffic.
- **Balanced Security and Connectivity** - These policies are built for both speed and detection. Used together, they serve as a good starting point for most networks and deployment types.
- **Connectivity Over Security** - These policies are built for networks where connectivity, the ability to get to all resources, takes precedence over network infrastructure security. Only the most critical rules that block traffic are enabled.
- **No Rules Active** - The rules included in the policy are disabled by default.

Tip The **Maximum Detection** base template requires a considerable amount of memory and CPU to work effectively. CDO recommends deploying IPS policies using this template to models such as the 2100, 4100, or virtual device.

As new vulnerabilities become known, Talos releases intrusion rule updates. These rule updates can modify any Cisco-provided network analysis or intrusion policy, and may provide new and updated intrusion rules and preprocessor rules that are automatically applies to existing rules and policy settings. Rule updates might also delete rules from the existing template bases and provide new rule categories, as well as modify the default variable set.

IPS Policy Mode

By default, all intrusion policies operate in **Prevention** mode to implement an IPS. In the Prevention inspection mode, if a connection matches an intrusion rule whose action is to drop traffic, the connection is actively blocked.

If you instead want to test the effect of the intrusion policy on your network, you can change the mode to **Detection**, which implements an Intrusion Detection System (IDS). In this inspection mode, drop rules are

treat like alert rules, where you are notified of matching connections, but the action result becomes **Would Have Blocked**, and connections are never in fact blocked.

IPS Rule Group Security Level

CDO allows you to modify the security level of the rule groups included in your policy. Note that this security level is applied to all the rules in the rule group and not to individual rules.

Note Changes made a rule group's security level are automatically submitted and cannot be reverted. You do not have to click **Save** to submit security level modifications. You must manually change the security level back.

IPS Rule Action

Modify the actions of an individual rule or multiple rules within a rule group at any time. IPS rules can be set as the following options:

- **Disabled**—Do not match traffic against this rule. No events are generated.
- **Alert**—Create an event when this rule matches traffic, but do not drop the connection.
- **Drop**—Create an event when this rule matches traffic, and also drop the connection.

FDM Templates and Custom IPS Policy

Templates derived from a device with Snort 3 enabled can only be applied to devices that also have Snort 3 enabled. Due to the variability in rules supported and processed by Snort 2 and Snort 3, a template configured with Snort 3 cannot fully support and protect a device configured with Snort 2. See Switching from Snort 2 to Snort 3 for more information.

If you happen to use the ASA Migration tool to create an FDM template from an ASA configuration, we **strongly** recommend not configuring, or un-configuring any IPS policies. ASA devices do not support the Snort engine and migrating IPS policies from an ASA configuration to an FDM-managed device configuration may cause issues. If you do use the ASA migration tool, we recommend creating custom IPS policies for the device after creating and deploying the template.

See FDM-Managed Device Templates for more information about templates.

Rulesets and Custom IPS Policy

Rulesets are not yet support on devices configured for Snort 3. The following limitations apply:

- You cannot attach rulesets to Snort 3-enabled devices.
- You cannot create a ruleset from an existing device that has Snort 3 installed.
- You cannot associate a custom IPS policy to a ruleset.

Prerequisites

You can view the available IPS policies from the **Intrusion policies** page, but you cannot create or modify custom IPS policies without the following prerequisites:

Device Support

- Firepower 1000 series
- Firepower 2100 series
- Firepower 4100 series
- Threat Defense virtual with AWS
- Threat Defense virtual with Azure

Software Support

s

Devices **must** be running at least version 6.7 and Snort 3.

If your device is running a version prior to 6.7, upgrade your device. See Upgrade an FDM-Managed Device for more information.

If your device is running version 6.7 with Snort 2, please note that some intrusion rules in Snort 2.0 might not exist in Snort 3.0. See Switching from Snort 2 to Snort 3 for more information.

Note To find out what version of software version and Snort engine your device is running, simply locate and select the device on the **Inventory** page and look at the **Device Details**

Related Information:

- Configure Firepower Custom IPS Policies
- Custom IPS Policy in an FDM-Managed Access Control Rule

Configure Firepower Custom IPS Policies

Before you create or modify a custom IPS policy for your FDM-managed device in CDO, be sure to read the Custom Firepower Intrusion Prevention System Policy.

At this time, CDO does **not** support custom IPS rules. You can create and modify custom IPS policies with rules that are provided by Talos, but you cannot create your own IPS rules and apply them to custom IPS policies.

If you experience issues creating or editing IPS policies in CDO, see Troubleshoot Intrusion Prevention System for more information.

Note You cannot delete or reorder the rules within a custom IPS policy's rule group.

Create a Custom IPS Policy

Use the following procedure to create a new custom IPS policy with the IPS rules provided by Talos:

Procedure

Step 1 From the CDO navigation pane, click **Policies**.

Step 2 Select **Intrusion Policies**.

Step 3 Click the blue plus button  .

Step 4 Expand the drop-down menu of the **Base Template**. If your device is running version 7.2 with Snort 3, you must expand the drop-down and then click **Choose** to select the template.If the device is running version 7.1.x and earlier, simply expand the drop-down menu and select one of the following templates:

- **Maximum Detection** - These policies are built for networks where network infrastructure security is given even more emphasis than is given by the Security Over Connectivity policies, with the potential for even greater operational impact.

  Tip The **Maximum Detection** base template requires a considerable amount of memory and CPU to work effectively. CDO recommends deploying IPS policies using this template to models such as the 2100, 3100, 4100, or threat defense virtual.

- **Security Over Connectivity** - These policies are built for networks where network infrastructure security takes precedence over user convenience. The intrusion policy enables numerous network anomaly intrusion rules that could alert on or drop legitimate traffic.
- **Balanced Security and Connectivity** - These policies are built for both speed and detection. Used together, they serve as a good starting point for most networks and deployment types.
- **Connectivity Over Security** - These policies are built for networks where connectivity, the ability to get to all resources, takes precedence over network infrastructure security. Only the most critical rules that block traffic are enabled.
- **No Rules Active** - The rules included in the policy are disabled by default.

Step 5 Enter a **Name** for the policy.

We **strongly** recommend using a name that is unique and different from the default base templates. If you ever need to troubleshoot your IPS policy, Cisco TAC can easily locate the custom policy and revert to a default policy; this keeps your network protected without losing your customized changes.

Step 6 (Optional) Enter a **Description** for the policy.

Step 7 Select the **IPS Mode**:

- **Prevention** - If a connection matches an intrusion rule whose action is to drop traffic, the connection is actively blocked.
- **Detection** - If a connection matches an intrusion rule whose action is to drop traffic, the action result becomes **Would Have Blocked** and no action is taken.

Step 8 Click **Save**.

What's Next?

Add your IPS policy to an FDM-managed device access control rule. See Custom IPS Policy in an FDM-Managed Access Control Rule for more information.

Edit a Custom IPS Policy

You can edit an existing IPS policy if you have onboarded an FDM-managed device that already has an IPS policy, if you created an IPS policy in FDM and CDO reads the policy from the deployed configuration, or if you just created a new IPS policy.

Use the following procedure to modify an existing custom IPS policy:

Procedure

Step 1 From the CDO navigation pane, click **Policies**.

Step 2 Select **Intrusion Policies**.

Step 3 Identify the IPS policy you want to edit. Click **Edit**.

Step 4 At the top of the page, click the edit icon  .

Step 5 Edit the following desired fields:

- Base Template.
- Name.
- Description.
- IPS Mode.

Step 6 Click **Save**.

Step 7 Preview and Deploy Configuration Changes for All Devices now the changes you made, or wait and deploy multiple changes at once.

Edit Rule Groups in a Custom IPS Policy

You can override the default action of a rule within a rule group. Use the following procedure to edit the rules contained within the rule group

Procedure

Step 1 From the CDO Navigation pane, click **Policies**.

Step 2 Select **Intrusion Policies**.

Step 3 Identify the IPS policy you want to edit. Click **Edit**.

Step 4 From the Rule Group tab located to the left, expand the desired rule group. From the expanded list, select the group.

Step 5 Edit the rule group:

a) Edit the **Security Level** of the entire rule group by selecting the security level bar. Manually drag the security level to the type of security you want applied to the entire rule group. Click **Submit**

b) Edit the **Rule Action** of an individual rule by expanding the rule's drop-down menu located to the right.

c) Edit the **Rule Action** of multiple rules by selecting the checkboxes of the desired rules and expanding the drop-down menu located above the table of rules. This selection impacts all selected rules.

d) Edit the **Rule Action** of all the rules by selecting the checkbox in the title row of the table and expanding the drop-down menu located above the table of rules. This selection impacts all the rules in the rule group.

Step 6 Click **Save** at the top of the policy page.

Step 7 Preview and Deploy Configuration Changes for All Devices now the changes you made, or wait and deploy multiple changes at once.

Delete a Custom IPS policy

Use the following procedure to delete a custom IPS policy from CDO:

Procedure

Step 1 From the CDO Navigation pane, click **Policies**.

Step 2 Select **Intrusion Policies**.

Step 3 Identify the IPS policy you want to edit. Click **Delete**.

Step 4 Click **OK** to delete the policy.

Step 5 Preview and Deploy Configuration Changes for All Devices now the changes you made, or wait and deploy multiple changes at once.

Security Intelligence Policy

About Security Intelligence

The Security Intelligence policy gives you an early opportunity to drop unwanted traffic based on source/destination IP address or destination URL. The system drops the traffic on the blocked list before evaluating it with the access control policy, thus reducing the amount of system resources used.

You can block traffic based on the following:

- **Cisco Talos feeds**—Cisco Talos provides access to regularly updated security intelligence feeds. Sites representing security threats such as malware, spam, botnets, and phishing appear and disappear faster than you can update and deploy custom configurations. The system downloads feed updates regularly, and thus new threat intelligence is available without requiring you to redeploy the configuration.

Note Cisco Talos feeds are updated by default every hour. You can change the update frequency, and even update the feeds on demand, by logging into Firepower Device Manager and navigating from the home page: Device > Updates > View Configuration.

- **Network and URL objects**—If you know of specific IP addresses or URLs you want to block, you can create objects for them and add them to the Blocked list or the Allowed list.

You create separate blocked and allowed lists for IP addresses (networks) and URLs.

License Requirements for Security Intelligence

You must enable the license on the FDM-managed device to use Security Intelligence.

For more information, see the **Security Intelligence Feed Categories** section of the Security Policies chapter of the appropriate Cisco FTD Configuration Guide for Firepower Device Manager.

Configure the Firepower Security Intelligence Policy

The Security Intelligence policy gives you an early opportunity to drop unwanted traffic based on source/destination IP address or destination URL. Any allowed connections are still evaluated by access control policies and might eventually be dropped. You must enable the license to use Security Intelligence.

Configure Firepower Security Intelligence Policy

Procedure

Step 1 In the navigation pane, click **Inventory**.

Step 2 Click the **Devices** tab to locate the device or the **Templates** tab to locate the model device.

Step 3 Click the **FTD** tab and select the FDM-managed device for which you are going to create or edit a security intelligence policy.

Step 4 In the **Management** pane at the right, click **Policy.**

Step 5 In the FDM-managed device Policies page, click **Security Intelligence** in the policy bar.

Step 6 If the policy is not enabled, click the Security Intelligence slider to enable it or click **Enable** in the About Security Intelligence information box.

Note You can disable Security Intelligence at any time by clicking the Security Intelligence toggle off. Your configuration is preserved, so that when you enable the policy again you do not need to reconfigure it.

Step 7 Select the row for **Blocked List**. Notice that, depending on your table view, there are plus signs in the networks, network objects, network feeds, URLs, URL objects, and URL feeds columns.

- In the **Add Networks to Blocked List** dialog box and **Add URL Object to Blocked List** dialog box, you can search for an existing object or create one to suit your needs. Check the object you want to block and then click **Select**.

  Note Security Intelligence ignores IP address blocks using a /0 netmask. This includes the any-ipv4 and any-ipv6 network objects. Do not select these objects for network block-listing.

- In the **Add URL Objects to Blocked List** and **Add Network Feeds to Blocked List** dialog, check a feed that you want to block and click **Select**. You can read the description of the feed by clicking the down arrow at the end of the feed row. They are also described in Security Intelligence Feeds for Firepower Security Intelligence Policies.

Step 8 If you know there are networks, IP addresses, or URLs that are included in the any of the network groups, network feeds, URL objects, or URL feeds you specified in the previous step, that you want to make an exception for, click the row for the **Allowed List**.

Step 9 Select or create objects for the networks, IP addresses, and URLs that you want to make exceptions for. When you click **Select** or **Add** they are added to the Allowed List row.

Step 10 (Optional) To log events generated by the Security Intelligence policy:

a) Click the Logging Settings  icon to configure logging. If you enable logging, any matches to blocked list entries are logged. Matches to exception entries are not logged, although you get log messages if exempted connections match access control rules with logging enabled.

b) Enable event logging by clicking the **Connection Events Logging** toggle.

c) Choose where to send your events:

- Clicking **None** saves events to your FDM-managed device. They are visible in the FDM Events viewer. Storage space on the FDM-managed device is very limited. It is best to store your connection events on a syslog server, by defining a syslog server object, instead of choosing None.
- Clicking **Create** or **Choose** allows you to create or choose a syslog server, represented by a syslog server object, to send logging events to. Because event storage on the device is limited, sending events to an external syslog server can provide more long-term storage and enhance your event analysis.

If you have a subscription to Cisco Security Analytics and Logging, send events to a Secure Event Connector by configuring a syslog object with the SEC's IP address and port. See Cisco Security Analytics and Logging for more information about this feature.

Step 11 (Optional) For any rule that you created, you can select it and add a comment about it in the Add Comments field. To learn more about rule comments see, Adding Comments to Rules in Policies and Rulesets.

Step 12 Preview and Deploy Configuration Changes for All Devices now the changes you made, or wait and deploy multiple changes at once.

Making Exceptions to the Firepower Security Intelligence Policy Blocked Lists

For each blocked list you create in a Configure the Firepower Security Intelligence Policy, you can create an associated allowed list. The only purpose of the allowed list is to make an exception for IP addresses or URLs that appear in the blocked list. That is, if you find an address or URL you need to use, and you know to be safe, is in a feed configured on the blocked list, you can exempt that address or URL by putting in the allowed list. This way, you don't need to remove an entire feed from the blocked list for the sake of one address or URL.

After passing through the security intelligence policy, allowed traffic is subsequently evaluated by the access control policy. The ultimate decision on whether the connections are allowed or dropped is based on the access control rule the connections match. The access rule also determines whether intrusion or malware inspection is applied to the connection.

Security Intelligence Feeds for Firepower Security Intelligence Policies

The following table describes the categories available in the Cisco Talos feeds. These categories can be entered in both the network and URL blocked list.

Category	Description
attackers	Active scanners and block-listed hosts known for outbound malicious activity.

Category	Description
bogon	Bogon networks and unallocated IP addresses.
bots	Sites that host binary malware droppers.
CnC	Sites that host command-and-control servers for botnets.
dga	Malware algorithms used to generate a large number of domain names acting as rendezvous points with their command-and-control servers.
exploitkit	Software kits designed to identify software vulnerabilities in clients.
malware	Sites that host malware binaries or exploit kits.
open_proxy	Open proxies that allow anonymous web browsing.
open_relay	Open mail relays that are known to be used for spam.
phishing	Sites that host phishing pages.
response	IP addresses and URLs that are actively participating in malicious or suspicious activity.
spam	Mail hosts that are known for sending spam.
suspicious	Files that appear to be suspicious and have characteristics that resemble known malware.
tor_exit_node	Tor exit nodes.

FDM-Managed Device Identity Policy

Identity Policy Overview

Use identity policies to collect user identity information from connections. You can then view usage based on user identity in the dashboards, and configure access control based on user or user group. By linking network behavior, traffic, and events directly to individual users and groups, the system can help you identify the source of policy breaches, attacks, or network vulnerabilities.

For example, you can identify who owns the host targeted by an intrusion event, and who initiated an internal attack or port scan. You can also identify high bandwidth users and users who are accessing undesirable web sites or applications.

You can then view usage based on user identity in the dashboards, and configure access control based on Active Directory (AD) realm object (which matches all users on that AD), special identities (such as failed authentication, guest, no authentication required, or unknown identity), or user groups.

You can obtain user identity using the following methods:

- Passive authentication—For all types of connections, obtain user identity from other authentication services without prompting for username and password.
- Active authentication—For HTTP connections only, prompt for username and password and authenticate against the specified identity source to obtain the user identity for the source IP address.

Establishing User Identity Through Passive Authentication

Passive authentication gathers user identity without prompting the user for username and password. The system obtains the mappings from the identity sources you specify.

You can passively obtain user-to-IP address mappings from the following sources:

- Remote access VPN logins. The following user types are supported for passive identity:
  - User accounts defined in an external authentication server.
  - Local user accounts that are defined in FDM-managed device.
- Cisco Identity Services Engine (ISE); Cisco Identity Services Engine Passive Identity Connector (ISE PIC).

If a given user is identified through more than one source, the remote access VPN login identity takes precedence.

Establishing User Identity through Active Authentication

Authentication is the act of confirming the identity of a user.

With active authentication, when an HTTP traffic flow comes from an IP address for which the system has no user-identity mapping, you can decide whether to authenticate the user who initiated the traffic flow against the directory configured for the system. If the user successfully authenticates, the IP address is considered to have the identity of the authenticated user.

Failure to authenticate does not prevent network access for the user. Your access rules ultimately decide what access to provide these users.

Dealing with Unknown Users

When you use an FDM-managed device to configure the directory server for the identity policy, FDM-managed downloads user and group membership information from the directory server. The Active Directory information is refreshed every 24 hours at midnight or whenever you edit and save the directory configuration (even if you do not make any changes).

If a user succeeds in authenticating when prompted by an active authentication identity rule, but the user's name is not in the downloaded user identity information, the user is marked as Unknown. You will not see the user's ID in identity-related dashboards, nor will the user match group rules.

However, any access control rules for the Unknown user will apply. For example, if you block connections for Unknown users, these users are blocked even though they succeeded in authenticating (meaning that the directory server recognizes the user and the password is valid).

Thus, when you make changes to the directory server, such as adding or deleting users, or changing group membership, these changes are not reflected in policy enforcement until the system downloads the updates from the directory.

If you do not want to wait until the daily midnight update, you can force an update by editing the directory realm information (login to an FDM-managed device and navigate Objects > Identity Sources, then edit the realm). Click **OK**, then deploy changes. The system will immediately download the updates.

Note You can check whether new or deleted user information is on the FDM-managed system by logging in to an FDM-managed device and navigating **Policies > Access Control**, clicking the **Add Rule** (+) button, and looking at the list of users on the Users tab. If you cannot find a new user, or you can find a deleted user, then the system has old information

How to Implement an Identity Policy

If you want to manage identity policies for your FDM-managed device using Cisco Defense Orchestrator (CDO) you need to create identity sources first. You can configure the remaining settings using Defense Orchestrator.

When configured correctly, you will be able to see usernames in the monitoring dashboards and events in FDM. You will also be able to use user identity in access control and SSL decryption rules as a traffic-matching criteria.

Note At this time, CDO can not configure some of the components needed to implement identity policies such as remote access VPN and Cisco Identity Services Engine. These components must be configured in FDM, which is the local manager of the device. Some of the steps in the procedure below indicate that you must use FDM to configure some identity components to implement identity policies.

Procedure

The following procedure provides an overview of what you must configure to get identity policies to work:

Procedure

Step 1 Create the AD identity realm. Whether you collect user identity actively or passively, you need to configure the Active Directory (AD) server that has the user identity information. See Create an FTD Active Directory Realm Object for more information.

Step 2 If you want to use passive authentication identity rules, configure the passive identity sources **using FDM**.

You can configure any of the following, based on the services you are implementing in the device and the services available to you in your network.

- Remote access VPN—If you intend to support remote access VPN connections to the device, user logins can provide the identity based on the AD server or on local users (those defined within an FDM-managed device). For information on configuring remote access VPN, see the Configuring Remote Acces VPNs chapter of the Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager for the version running on your device.
- Cisco Identity Services Engine (ISE) or Cisco Identity Services Engine Passive Identity Connector (ISE PIC)—If you use these products, you can configure the device as a pxGrid subscriber, and obtain user identity from ISE. See the Configure Identity Services Engine chapter of the Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager for instructions.

Step 3 **Using Defense Orchestrator**, enable the identity policy and configure passive or active authentication. See Configure Identity Policy Settings for more information.

Step 4 **Using Defense Orchestrator**, Configure the Identity Policy Default Action. If your intention is to use passive authentication only, you can set the default action to passive authentication and there is no need to create specific rules.

Step 5 **Using Defense Orchestrator**, Configure Identity Rules. Create rules that will collect passive or active user identities from the relevant networks.

Step 6 (Optional) For any rule that you created, you can select it and add a comment about it in the Add Comments field. To learn more about rule comments see, Adding Comments to Rules in Policies and Rulesets.

Step 7 Preview and Deploy Configuration Changes for All Devices now the changes you made, or wait and deploy multiple changes at once.

Configure Identity Policies

You can use identity policies to collect user identity information from connections. You can then view usage based on user identity in the FDM dashboards, and configure access control based on user or user group.

The following is an overview of how to configure the elements required to obtain user identity through identity policies:

Procedure

Procedure

Step 1 In the navigation pane, click **Inventory**.

Step 2 Click the **Devices** tab to locate the device or the **Templates** tab to locate the model device.

Step 3 Click the **FTD** tab and select the device for which you are configuring an identity policy, and click **Policy** in the **Management** pane at the right.

Step 4 Click **Identity** in the Policy bar.

Step 5 If you have not yet enabled an identity policy, read about passive and active authentication and click **Enable**. You are enabling an identity policy, *not* a passive authentication policy or an active authentication policy. The rules in the policy will specify active or passive authentication.

Step 6 Manage the identity policy:

After you configure identity settings, this page lists all rules in order. Rules are matched against traffic from top to bottom with the first match determining the action to apply. You can do the following from this page:

- **To enable or disable the identity policy**, click the identity toggle. See Configure Identity Policy Settings for more information.
- **To read the passive authentication settings**, click the button next to the **Passive Auth** label on the identity bar. See Configure Identity Policy Settings for more information.
- **To enable active authentication,** click the button next to the **Active Auth** label on the identity bar. See Configure Identity Policy Settings for more information.
- **To change the default action**, click the default action button and select the desired action. See Configure the Identity Policy Default Action.

- **To move a rule in the table**, select the rule and click the up or down arrow at the end of the rule's row in the rule table.
- **To move a rule in the table**, select the rule and click the up or down arrow at the end of the rule's row in the rule table.
- **To configure rules**:
  - To create a new rule, click the plus  button.
  - To edit an existing rule, select the rule and click **Edit** in the Actions pane. You can also selectively edit a rule property by clicking on the property in the table.
  - To delete a rule you no longer need, select the rule and click **Remove** in the Actions pane.

For more information on creating and editing identity rules, see Configure Identity Rules.

Step 7 (Optional) For any rule that you created, you can select it and add a comment about it in the Add Comments field. To learn more about rule comments see, Adding Comments to Rules in Policies and Rulesets.

Step 8 Preview and Deploy Configuration Changes for All Devices now the changes you made, or wait and deploy multiple changes at once.

Configure Identity Policy Settings

For identity policies to work, you must configure the sources that provide user identity information. The settings you must configure differ based on the type of rules you configure: passive, active, or both.

Note At this time, CDO can not configure some of the components needed to implement identity policies such as active directory identity realms, remote access VPN, and Cisco Identity Services Engine. These components must be configured in FDM, which is the local manager of the device. Some of the steps in the procedure below indicate that you must use FDM to configure some identity components to implement identity policies.

Procedure

Before you begin

Ensure that time settings are consistent among the directory servers, FDM-managed device, and clients. A time shift among these devices can prevent successful user authentication. "Consistent" means that you can use different time zones, but the time should be the same relative to those zones; for example, 10 AM PST = 1 PM EST.

Procedure

Step 1 In the navigation pane, click **Inventory**.

Step 2 Click the **Devices** tab to locate the device or the **Templates** tab to locate the model device.

Step 3 Click the **FTD** tab and select the device for which you are configuring an identity policy, and click **Policy** in the **Management** pane at the right.

Step 4 **Enable Identity policies** by clicking the Identity toggle. Or, you can click the button, review the descriptions of passive and active authentication and click **Enable** in the dialog.

Step 5 **Read the Passive Authentication** settings. Click the **Passive Auth** button on the identity bar.

The Passive Authentication button shows **Enabled** if you have configured remote access VPN or Cisco Identity Services engine using Firepower Device Manager.

You must have configured at least one passive identity source to create passive authentication rules.

Step 6 **Configure Active Authentication.** When an identity rule requires active authentication for a user, the user is redirected to the captive portal port on the interface through which they are connected and then they are prompted to authenticate.

a) Click the **Active Auth** button on the Identity bar.

b) If you have not already, enable SSL Description by clicking the **Enable** link. If you don't see the Enable link, skip to step "c".

1. From the **Select Decrypt Re-Sign Certificate** menu, select the internal CA certificate to use for rules that implement decryption with re-signed certificates.

   You can use the pre-defined **NGFW-Default-InternalCA** certificate, or click the menu and select Create or Choose to create a new certificate or select one you have already uploaded to the FDM-managed device.

   If you have not already installed the certificate in client browsers, click the download button to obtain a copy. See the documentation for each browser for information on how to install the certificate. Also see Downloading the CA Certificate for Decrypt Re-Sign Rules.

   Note You are prompted for SSL Decryption settings only if you have not already configured the SSL decryption policy. To change these settings after enabling the identity policy, edit the SSL decryption policy settings.

2. Click **Save**.

c) Click the **Server Certificate** menu to select (choose) the internal certificate to present to users during active authentication. If you have not already created the required certificate, click **Create**. Users will have to accept the certificate if you do not upload a certificate that their browsers already trust.

d) In the **Port** field, enter the port number for the captive portal. The default is 885 (TCP). If you configure a different port, it must be in the range 1025-65535.

Note For the HTTP Basic, HTTP Response Page, and NTLM authentication methods, the user is redirected to the captive portal using the IP address of the interface. However, for HTTP Negotiate, the user is redirected using the fully-qualified DNS name firewall-hostname.AD-domain-name . If you want to use HTTP Negotiate, you must also update your DNS server to map this name to the IP addresses of all inside interfaces where you are requiring active authentication. Otherwise, the redirection cannot complete, and users cannot authenticate.

e) Click **Save**.

Step 7 Continue with Configure the Identity Policy Default Action.

Configure the Identity Policy Default Action

The identity policy has a default action, which is implemented for any connections that do not match any individual identity rules.

In fact, having no rules is a valid configuration for your policy. If you intend to use passive authentication on all traffic sources, then simply configure Passive Authentication as your default action.

Procedure

Procedure

Step 1 In the navigation pane, click **Inventory**.

Step 2 Click the **Devices** tab to locate the device or the **Templates** tab to locate the model device.

Step 3 Click the **FTD** tab and select the device for which you are configuring an identity policy, and click **Policy** in the **Management** pane at the right.

Step 4 Click **Identity** in the Policy bar.

Step 5 Configure Identity Policy Settings if you have not done so already.

Step 6 At the bottom of the screen, click the Default Action button and choose one of the following:

- **Passive Auth**—User identity will be determined using all configured passive identity sources for connections that do not match any identity rules. If you do not configure any passive identity sources, using Passive Auth as the default is the same as using No Auth.
- **No Auth**—User identity will not be determined for connections that do not match any identity rules.

Step 7 Preview and Deploy Configuration Changes for All Devices now the changes you made, or wait and deploy multiple changes at once.

Configure Identity Rules

Identity rules determine whether user identity information should be collected for matching traffic. You can configure No Authentication if you do not want to collect user identity information for matching traffic.

Keep in mind that regardless of your rule configuration, active authentication is performed on HTTP traffic only. Thus, you do not need to create rules to exclude non-HTTP traffic from active authentication. You can simply apply an active authentication rule to all sources and destinations if you want to get user identity information for all HTTP traffic.

Note Also keep in mind that a failure to authentication has no impact on network access. Identity policies collect user identity information only. You must use access rules if you want to prevent users who failed to authenticate from accessing the network.

Procedure

Procedure

Step 1 In the navigation pane, click **Inventory**.

Step 2 Click the **Devices** tab to locate the device or the **Templates** tab to locate the model device.

Step 3 Click the **FTD** tab and select the device for which you are configuring an identity policy, and click **Policy** in the **Management** pane at the right.

Step 4 Click **Identity** in the policy bar.

Step 5 Do any of the following:

- To create a new rule, click the plus button. To understand identity source objects and how they could affect your rules, see Configure Identity Sources for FDM-Managed Device for more information.
- To edit an existing rule, click the rule you want to edit and click **Edit** in the Actions pane at the right.
- To delete a rule you no longer need, click the rule you want to delete and click **Remove** in the Actions pane at the right.

Step 6 In **Order**, select where you want to insert the rule in the ordered list of rules.

Rules are applied on a first-match basis, so you must ensure that rules with highly specific traffic matching criteria appear above policies that have more general criteria that would otherwise apply to the matching traffic.

The default is to add the rule to the end of the list. If you want to change a rule's location later, edit this option.

Step 7 In **Name**, enter a name for the rule.

Step 8 Select the **Action** that the FDM-managed device should apply on a match and if necessary, an Active Directory (AD) Identity Source.

You must select the AD identity realm that includes the user accounts for passive and active authentication rules. choose one of the following:

- **Passive Auth**—Use passive authentication to determine user identity. All configured identity sources are shown. The rule automatically uses all configured sources.
- **Active Auth**Use active authentication to determine user identity. Active authentication is applied to HTTP traffic only. If any other t—ype of traffic matches an identity policy that requires or allows active authentication, then active authentication will not be attempted.
- **No Auth**—Do not obtain user identity. Identity-based access rules will not be applied to this traffic. These users are marked as No Authentication Required.

Note For both **Passive Auth** and **Active Auth**, you can opt to select an AD Realm identity source. If you do not have any identity source objects readily prepared, click **Create new object** to launch the identity source object wizard. See Create or Edit an Active Directory Realm Object for more information.

Step 9 (Active Authentication only.) Click the **Active authentication** tab and select the authentication method (Type) supported by your directory server:

- **HTTP Basic**—Authenticate users using an unencrypted HTTP Basic Authentication connection. Users log in to the network using their browser's default authentication popup window. This is the default.
- **NTLM**—Authenticate users using an NT LAN Manager (NTLM) connection. This selection is only available when you select an AD realm. Users log in to the network using their browser's default authentication popup window, although you can configure Internet Explorer and Firefox browsers to transparently authenticate using their Windows domain login. That task is done in FDM, see Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager > Security Policies > Identity Policies > **Enabling Transparent User Authentication** for instructions.
- **HTTP Negotiate**—Allow the device to negotiate the method between the user agent (the application the user is using to initiate the traffic flow) and the Active Directory server. Negotiation results in the strongest commonly supported method being used, in order, NTLM, then basic. Users log in to the network using their browser's default authentication popup window.
- **HTTP Response Page**Prompt users to authenticate using a system-provided web page. This is a form of HTTP Basic authentication.

Note For the HTTP Basic, HTTP Response Page, and NTLM authentication methods, the user is redirected to the captive portal using the IP address of the interface. However, for HTTP Negotiate, the user is redirected using the fully-qualified DNS name *firewall-hostname.AD-domain-name* . If you want to use HTTP Negotiate, you must also update your DNS server to map this name to the IP addresses of all inside interfaces where you are requiring active authentication. Otherwise, the redirection cannot complete, and users cannot authenticate.

Step 10 (Active authentication only.) Select **Fall Back as Guest > On/Off** to determine whether users who fail active authentication are labeled as Guest users.

Users get 3 chances to successfully authenticate. If they fail, your selection for this option determines how the user is marked. You can deploy access rules based on these values.

- Fall Back as Guest > **On**—Users are marked as Guest.
- Fall Back as Guest > **Off**—Users are marked as Failed Authentication.

Step 11 Define the traffic matching criteria on the **Source** and **Destination** tabs for Passive authentication, Active authentication, or No Authentication rule actions.

Keep in mind that active authentication will be attempted with HTTP traffic only. Therefore, there is no need to configure No Auth rules for non-HTTP traffic, and there is no point in creating Active Authentication rules for any non-HTTP traffic. However, passive authentication is valid for any type of traffic.

The Source/Destination criteria of an identity rule define the security zones (interfaces) through which the traffic passes, the IP addresses or the country or continent (geographical location) for the IP address, or the protocols and ports used in the traffic. The default is any zone, address, geographical location, protocol, and port.

To modify a condition, you click the  button within that condition, select the desired object or element, and click OK in the popup dialog box. If the criterion requires an object, you can click **Create New Object** if the object you require does not exist.

To remove an object from a condition, hover over the object and click the X.

You can configure the following traffic matching criteria.

Source Zones, Destination Zones

The security zone objects that define the interfaces through which the traffic passes. You can define one, both, or neither criteria: any criteria not specified applies to traffic on any interface.

- To match traffic leaving the device from an interface in the zone, add that zone to the Destination Zones.
- To match traffic entering the device from an interface in the zone, add that zone to the Source Zones.
- If you add both source and destination zone conditions to a rule, matching traffic must originate from one of the specified source zones and egress through one of the destination zones.

Use this criteria when the rule should apply based on where the traffic enters or exits the device. For example, if you want to ensure that user identity is collected from all traffic originating from inside networks, select an inside zone as the Source Zones while leaving the destination zone empty.

Note You cannot mix passive and routed security zones in a single rule. In addition, you can specify passive security zones as source zones only, you cannot specify them as destination zones.

Source Networks, Destination Networks

The network objects or geographical locations that define the network addresses or locations of the traffic.

- To match traffic from an IP address or geographical location, configure the Source Networks.
- To match traffic to an IP address or geographical location, configure the Destination Networks.
- If you add both source and destination network conditions to a rule, matching traffic must originate from one of the specified IP addresses and be destined for one of the destination IP addresses.

When you add this criteria, you select from the following tabs:

- **Network**â€”Select the network objects or groups that define the source or destination IP addresses for the traffic you want to control.
- **Country/Continent**-Select the geographical location to control traffic based on its source or destination country or continent. Selecting a continent selects all countries within the continent. Besides selecting geographical location directly in the rule, you can also select a geolocation object that you created to define the location. Using geographical location, you could easily restrict access to a particular country without needing to know all of the potential IP addresses used there.
- **Custom Geolocation**â€”Select (or create) a geolocation object that has exactly the countries and continents you specify.

Note To ensure you are using up-to-date geographical location data to filter your traffic, Cisco strongly recommends that you regularly update the geolocation database (GeoDB). See Update Geolocation Database for more information.

Source Ports, Destination Ports/Protocols

The port objects that define the protocols used in the traffic. For TCP/UDP, this can include ports.

- To match traffic from a protocol or port, configure the Source Ports. Source ports can be TCP/UDP only.
- To match traffic to a protocol or port, configure the Destination Ports/Protocols.
- To match traffic both originating from specific TCP/UDP ports and destined for specific TCP/UDP ports, configure both. If you add both source and destination ports to a condition, you can only add ports that

share a single transport protocol, TCP or UDP. For example, you could target traffic from port TCP/80 to port TCP/8080.

Step 12 Click **Save**.

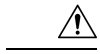
Step 13 Return to the **Inventory** page.

Step 14 Select the device to which you added these rules to the identity policy.

Step 15 Preview and Deploy Configuration Changes for All Devices now the changes you made, or wait and deploy multiple changes at once.

SSL Decryption Policy

Some protocols, such as HTTPS, use Secure Sockets Layer (SSL) or its follow-on version, Transport Layer Security (TLS), to encrypt traffic for secure transmissions. Because the system cannot inspect encrypted connections, you must apply SSL decryption policy to decrypt them if you want to apply access rules that consider higher-layer traffic characteristics to make access decisions.



Caution Keep in mind that decrypting and then re-encrypting traffic adds a processing load on the device, which will reduce overall system performance.

Continue with these topics:

- About SSL Decryption
- How to Implement and Maintain the SSL Decryption Policy
- Configure SSL Decryption Policies
- Configure Certificates for Known Key and Re-Sign Decryption
- Downloading the CA Certificate for Decrypt Re-Sign Rules
- Troubleshooting SSL Decryption Issues

How to Implement and Maintain the SSL Decryption Policy

You can use SSL decryption policies to turn encrypted traffic into plain text traffic, so that you can then apply URL filtering, intrusion and malware control, and other services that require deep packet inspection. If your policies allow the traffic, the traffic is re-encrypted before it leaves the device.

The SSL decryption policy applies to encrypted traffic only. No unencrypted connections are evaluated against SSL decryption rules.

Unlike some other security policies, you need to monitor and actively maintain the SSL decryption policy, because certificates can expire or even be changed on destination servers. Additionally, changes in client software might alter your ability to decrypt certain connections, because the decrypt re-sign action is indistinguishable from a man-in-the-middle attack.

The following procedure explains the end-to-end process of implementing and maintaining the SSL decryption policy.

Procedure

Procedure

Step 1 If you will implement Decrypt Re-sign rules, create the required internal CA certificate.

You must use an internal Certificate Authority (CA) certificate. You have the following options. Because users must trust the certificate, either upload a certificate client browsers are already configured to trust, or ensure that the certificate you upload is added to the browser trust stores.

- Create a self-signed internal CA certificate, which is signed by the device itself. See Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager > Reusable Objects > Certificates > Generating Self-Signed Internal and Internal CA Certificates.
- Upload an internal CA certificate and key signed by an external trusted CA or by a CA inside your organization. See Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager > Reusable Objects > Certificates > Uploading Internal and Internal CA Certificates.

Step 2 If you will implement Decrypt Known Key rules, collect the certificate and key from each of the internal servers.

You can use Decrypt Known Key only with servers that you control, because you must obtain the certificate and key from the server. Upload these certificates and keys as internal certificates (not internal CA certificates). See Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager > Reusable Objects > Certificates > Uploading Internal and Internal CA Certificates.

Step 3 Configure SSL Decryption Policies.

When you enable the policy, you also configure some basic settings.

Step 4 Configure the Default SSL Decryption Action

If in doubt, select Do Not Decrypt as the default action. Your access control policy can still drop traffic that matches the default SSL decryption rule if appropriate.

Step 5 Configure SSL Decryption Rules.

Identify traffic to decrypt and the type of decryption to apply.

Step 6 If you configure known key decryption, edit the SSL decryption policy settings to include those certificates. See Configure Certificates for Known Key and Re-Sign Decryption.

Step 7 If necessary, download the CA certificate used for Decrypt Re-sign rules and upload it to the browser on client workstations.

For information on downloading the certificate and distributing it to clients, see Downloading the CA Certificate for Decrypt Re-Sign Rules.

Step 8 Periodically, update re-sign known key certificates.

- Re-sign certificate—Update this certificate before it expires. If you generate the certificate through Firepower Device Manager, it is valid for 5 years. To determine when a certificate expires, click the view icon for the certificate from the Objects page.
- Known-key certificate—For any known-key decryption rules, you need to ensure that you have uploaded the destination server's current certificate and key. Whenever the certificate and key changes on supported

servers, you must also upload the new certificate and key (as an internal certificate) and update the SSL decryption settings to use the new certificate.

Step 9 Upload missing trusted CA certificates for external servers.

The system includes a wide range of trusted CA root and intermediate certificates issued by third parties. These are needed when negotiating the connection between FDM-managed devices and the destination servers for decrypt re-sign rules.

Upload all certificates within a root CA's chain of trust to the list of trusted CA certificates, including the root CA certificate and all intermediate CA certificates. Otherwise, it is more difficult to detect trusted certificates issued by intermediate CAs. Upload certificates on the Objects > Certificates page. See See Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager > Reusable Objects > Certificates > Uploading Trusted CA Certificates.

About SSL Decryption

Normally, the access control policy determines if network connections should be allowed or blocked. However, if you enable the SSL decryption policy, encrypted connections are first sent through the SSL decryption policy to determine if they should be decrypted or blocked. Any connections that were not blocked, whether or not decrypted, then go through the access control policy for a final allow/block decision.

Note You must enable the SSL decryption policy in order to implement active authentication rules in the identity policy. If you enable SSL decryption to enable identity policies, but do not otherwise want to implement SSL decryption, select Do Not Decrypt for the default action in the SSL Decryption page and do not create additional SSL decryption rules. The identity policy automatically generates whatever rules it needs.

The following topics explain encrypted traffic flow management and decryption in more detail.

- Why Implement SSL Decryption?
- Automatically Generated SSL Decryption Rules
- Handling Undecryptable Traffic

Why Implement SSL Decryption?

Encrypted traffic, such as HTTPS connections, cannot be inspected. Many connections are legitimately encrypted, such as connections to banks and other financial institutions. Many web sites use encryption to protect privacy or sensitive data. For example, your connection to Firepower Device Manager is encrypted. However, users can also hide undesirable traffic within encrypted connections.

By implementing SSL decryption, you can decrypt connections, inspect them to ensure they do not contain threats or other undesirable traffic, and then re-encrypt them before allowing the connection to proceed. (The decrypted traffic goes through your access control policy and matches rules based on inspected characteristics of the decrypted connection, not on the encrypted characteristics.) This balances your need to apply access control policies with the user's need to protect sensitive information.

You can also configure SSL decryption rules to block encrypted traffic of types you know you do not want on your network.

Caution Keep in mind that decrypting and then re-encrypting traffic adds a processing load on the device, which will reduce overall system performance.

Actions You Can Apply to Encrypted Traffic

When configuring SSL decryption rules, you can apply the actions described in the following topics. These actions are also available for the default action, which applies to any traffic that does not match an explicit rule.

- Decrypt Re-Sign
- Decrypt Known Key
- Do Not Decrypt
- Block

Note Any traffic that passes through the SSL decryption policy must then pass through the access control policy. Except for traffic you drop in the SSL decryption policy, the ultimate allow or drop decision rests with the access control policy.

Decrypt Re-Sign

If you elect to decrypt and re-sign traffic, the system acts as a man-in-the-middle.

For example, the user types in https://www.cisco.com in a browser. The traffic reaches the FDM-managed device, the device then negotiates with the user using the CA certificate specified in the rule and builds an SSL tunnel between the user and the FDM-managed device. At the same time the device connects to https://www.cisco.com and creates an SSL tunnel between the server and the FDM-managed device.

Thus, the user sees the CA certificate configured for the SSL decryption rule instead of the certificate from www.cisco.com. The user must trust the certificate to complete the connection. The FDM-managed device then performs decryption/re-encryption in both directions for traffic between the user and destination server.

Note If the client does not trust the CA used to re-sign the server certificate, it warns the user that the certificate should not be trusted. To prevent this, import the CA certificate into the client trusted CA store. Alternatively, if your organization has a private PKI, you can issue an intermediate CA certificate signed by the root CA which is automatically trusted by all clients in the organization, then upload that CA certificate to the device.

If you configure a rule with the Decrypt Re-Sign action, the rule matches traffic based on the referenced internal CA certificate's signature algorithm type, in addition to any configured rule conditions. Because you can select a single re-sign certificate for the SSL decryption policy, this can limit traffic matching for resign rules.

For example, outgoing traffic encrypted with an elliptic curve (EC) algorithm matches a Decrypt Re-Sign rule only if the re-sign certificate is an EC-based CA certificate. Similarly, traffic encrypted with an RSA algorithm matches Decrypt Re-Sign rules only if the global re-sign certificate is RSA; outgoing traffic encrypted with an EC algorithm does not match the rule, even if all other configured rule conditions match.

Decrypt Known Key

If you own the destination server, you can implement decryption with a known key. In this case, when the user opens a connection to https://www.cisco.com, the user sees the actual certificate for www.cisco.com, even though it is the FDM-managed device that is presenting the certificate.

Your organization must be the owner of the domain and certificate. For the example of cisco.com the only possible way to have the end user see Cisco's certificate would be if you actually own the domain cisco.com (i.e. you are Cisco Systems) and have ownership of the cisco.com certificate signed by a public CA. You can only decrypt with known keys for sites that your organization owns.

The main purpose of decrypting with a known key is to decrypt traffic heading to your HTTPS server to protect your servers from external attacks. For inspecting client side traffic to external HTTPS sites, you must use decrypt re-sign as you do not own the servers.

Note To use known key decryption, you must upload the server's certificate and key as an internal identity certificate, and then add it to the list of known-key certificates in the SSL decryption policy settings. Then, you can deploy the rule for known-key decryption with the server's address as the destination address. For information on adding the certificate to the SSL decryption policy, see Configure SSL Decryption Policies.

Do Not Decrypt

If you elect to bypass decryption for certain types of traffic, no processing is done on the traffic. The encrypted traffic proceeds to the access control policy, where it is allowed or dropped based on the access control rule it matches.

Block

You can simply block encrypted traffic that matches an SSL decryption rule. Blocking in the SSL decryption policy prevents the connection from reaching the access control policy.

When you block an HTTPS connection, the user does not see the system default block response page. Instead, the user sees the browser's default page for a secure connection failure. The error message does not indicate the site was blocked due to policy. Instead, errors might indicate that there are no common encryption algorithms. It will not be obvious from this message that you blocked the connection on purpose.

Automatically Generated SSL Decryption Rules

Whether you enable the SSL decryption policy, FDM-managed device automatically generates Decrypt Re-sign rules for each identity policy rule that implements active authentication. This is required to enable active authentication for HTTPS connections.

When you enable the SSL decryption policy, you see these rules under the Identity Policy Active Authentication Rules heading. These rules are grouped at the top of the SSL decryption policy. The rules are read only. You can change them only by altering your identity policy

Handling Undecryptable Traffic

There are several characteristics that make a connection undecryptable. If a connection has any of the following characteristics, the default action is applied to the connection regardless of any rule the connection would otherwise match. If you select Block as your default action (rather than Do Not Decrypt), you might run into issues, including excessive drops of legitimate traffic.

- Compressed session—Data compression was applied to the connection.
- SSLv2 session—The minimum supported SSL version is SSLv3.
- Unknown cipher suite—The system does not recognize the cipher suite for the connection.
- Unsupported cipher suite—The system does not support decryption based on the detected cipher suite.
- Session not cached—The SSL session has session reuse enabled, the client and server reestablished the session with the session identifier, and the system did not cache that session identifier.
- Handshake errors—An error occurred during the SSL handshake negotiation.
- Decryption errors—An error occurred during the decryption operation.
- Passive interface traffic—All traffic on passive interfaces (passive security zones) is undecryptable.

License Requirements for SSL Decryption Policies

You do not need a special license to use the SSL decryption policy.

However, you do need the URL license to create rules that use URL categories and reputations as match criteria. For information on configuring licenses, see Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager> Licensing the System > Enabling or Disabling Optional Licenses.

Guidelines for SSL Decryption

Keep the following in mind when configuring and monitoring SSL decryption policies:

- The SSL Decryption policy is bypassed for any connections that match access control rules set to trust or block if those rules:
  - Use security zone, network, geolocation, and port only as the traffic matching criteria.
  - Come before any other rules that require inspection, such as rules that match connections based on application or URL, or allow rules that apply intrusion or file inspection.
- When using URL category matching, note that there are cases where the login page for a site is in a different category than the site itself. For example, Gmail is in the "Web based email" category, whereas the login page is in the "Internet Portals" category. To get connections to these sites decrypted, you must include both categories in the rule.

- You cannot disable the SSL decryption policy if you have any active authentication rules. To disable the SSL decryption policy, you must either disable the identity policy, or delete any identity rules that use active authentication.

Configure SSL Decryption Policies

You can use SSL decryption policies to turn encrypted traffic into plain text traffic, so that you can then apply URL filtering, intrusion and malware control, and other services that require deep packet inspection. If your policies allow the traffic, the traffic is re-encrypted before it leaves the device.

The SSL decryption policy applies to encrypted traffic only. No unencrypted connections are evaluated against SSL decryption rules.

Caution Keep in mind that decrypting and then re-encrypting traffic adds a processing load on the device, which will reduce overall system performance.

Note VPN tunnels are decrypted before the SSL decryption policy is evaluated, so the policy never applies to the tunnel itself. However, any encrypted connections within the tunnel are subject to evaluation by the SSL decryption policy.

The following procedure explains how to configure the SSL decryption policy. For an explanation of the end-to-end process of creating and managing SSL decryption, see How to Implement and Maintain the SSL Decryption Policy.

Procedure

Before you begin

The SSL decryption rules table contains two sections:

- **Identity Policy Active Authentication Rules**—If you enable the identity policy and create rules that use active authentication, the system automatically creates the SSL decryption rules needed to make those policies work. These rules are always evaluated before the SSL decryption rules you create yourself. You can alter these rules only indirectly, by making changes to the identity policy.
- **SSL Native Rules**—These are rules that you have configured. You can add rules to this section only.

Procedure

Step 1 In the navigation pane, click **Inventory**.

Step 2 Click the **Devices** tab to locate the device or the **Templates** tab to locate the model device.

Step 3 Click the **FTD** tab and select the device you want to create the SSL policy.

Step 4 Click **Policy** in the **Management** pane at the right.

Step 5 Click **SSL Decryption** in the policy bar.

Step 6 If you have not yet enabled the policy, click **Enable SSL Decryption** and configure policy settings, as described in Enable the SSL Decryption Policy.

Step 7 Configure the default action for the policy. The safest choice is Do Not Decrypt. For more information, see **Configure the Default SSL Decryption Action** section of the Security Policies chapter of the Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager for the version your device is running.

Step 8 Manage the SSL decryption policy.

After you configure SSL decryption settings, this page lists all rules in order. Rules are matched against traffic from top to bottom with the first match determining the action to apply. You can do the following from this page:

- To disable the policy, click the SSL Decryption Policy toggle. You can re-enable it by clicking Enable SSL Decryption.
- To edit policy settings, including the list of certificates used in the policy, click the configuration button on the SSL toolbar: 

. You can also download the certificate used with decrypt re-sign rules so that you can distribute it to clients. See the following sections of the Security Policies chapter in the Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager of the version your device is running:
  - Configure Certificates for Known Key and Re-Sign Decryption
  - Downloading the CA Certificate for Decrypt Re-Sign Rules
- To configure rules:
  - To create a new rule and log events it generates, click the blue plus button  . See Configure SSL Decryption Rules.
  - To edit an existing rule, click the rule in the rule table and click **Edit** in the Actions pane. You can also selectively edit a rule property by clicking on the property in the table.
  - To delete a rule you no longer need, click the rule in the rule table and click **Remove** in the Actions pane.
  - To move a rule, hover over it in the rule table. At the end of the row use the up and down arrows to move its position with the rule table.
  - (Optional) For any rule that you created, you can select it and add a comment about it in the Add Comments field. To learn more about rule comments see, Adding Comments to Rules in Policies and Rulesets.

Step 9 Continue to Enable the SSL Decryption Policy.

Enable the SSL Decryption Policy

Before you can configure SSL decryption rules, you must enable the policy and configure some basic settings. The following procedure explains how to enable the policy directly. You can also enable it when you enable identity policies. Identity policies require that you enable the SSL decryption policy.

Procedure

Before you begin

If you upgraded from a release that did not have SSL decryption policies, but you had configured the identity policy with active authentication rules, the SSL decryption policy is already enabled. Ensure that you select the Decrypt Re-Sign certificate you want to use, and optionally enable pre-defined rules.

Review Configure SSL Decryption Policies if you have not already.

Procedure

Step 1 In the navigation pane, click **Inventory**.

Step 2 Click the **Devices** tab to locate the device or the **Templates** tab to locate the model device.

Step 3 Click the **FTD** tab and the device for which you want to enable the SSL Decryption policy.

Step 4 Click **Policy** in the **Management** pane at the right.

Step 5 Click **SSL Decryption** in the policy bar.

Step 6 Click the **SSL Decryption** toggle in the SSL bar to enable the SSL Decryption policy.

- If this is the first time you enabled the policy, read the description of Decrypt Known-Key and Decrypt Re-Sign SSL decryption and click enable.
- If you have already configured the policy once and then disabled it, the policy is simply enabled again with your previous settings and rules. You can click the SSL decryption configuration button 

Configure Certificates for Known Key and Re-Sign Decryption and configure settings as described in .

Step 7 For **Select Decrypt Re-Sign Certificate**, select the internal CA certificate to use for rules that implement decryption with re-signed certificates.

You can use the pre-defined NGFW-Default-InternalCA certificate, or one that you created or uploaded. If the certificate does not yet exist, click **Create** to add an FDM-managed device internal CA certificate.

If you have not already installed the certificate in client browsers, click the download button  to obtain a copy. See the documentation for each browser for information on how to install the certificate. Also see Downloading the CA Certificate for Decrypt Re-Sign Rules

Step 8 Click **Save.**

Step 9 Continue with Configure the Default SSL Decryption Action to set the default action for the policy.

Configure the Default SSL Decryption Action

If an encrypted connection does not match a specific SSL decryption rule, it is handled by the default action for the SSL decryption policy.

Procedure

Before you begin

If you have not already, review these procedures and follow the procedures in them:

1. Configure SSL Decryption Policies
2. Enable the SSL Decryption Policy

Procedure

Step 1 In the navigation pane, click **Inventory**.

Step 2 Click the **Devices** tab to locate the device or the **Templates** tab to locate the model device.

Step 3 Click the **FTD** tab and select the device for which you want to configure the default SSL decryption action.

Step 4 Click **Policy** in the **Management** pane at the right.

Step 5 Click **SSL Decryption** in the policy bar.

Step 6 Click the **Default Action** button.

Step 7 Select the action to apply to matching traffic:

- **Do Not Decrypt**—Allow the encrypted connection. The access control policy then evaluates the encrypted connection and drops or allows it based on access control rules.
- **Block**—Drop the connection immediately. The connection is not passed on to the access control policy.

Step 8 (Optional.) Configure logging for the default action. You must enable logging to capture events from SSL Decryption policies. Select from these options:

- **At End of Connection**—Generate an event at the conclusion of the connection.
  - Send Connection Events Toâ€”If you want to send a copy of the events to an external syslog server, select the server object that defines the syslog server. If the required object does not already exist, click Create New Syslog Server and create it. (To disable logging to a syslog server, select Any from the server list.)

    Because event storage on the device is limited, sending events to an external syslog server can provide more long term storage and enhance your event analysis.

    If you have a subscription to Cisco Security Analytics and Logging, specify or create the syslog server using a Secure Event Connector's IP address and port. See Cisco Security Analytics and Logging for more information about this feature.

- **No Logging**—Do not generate any events.

Step 9 Click **Save.**

Step 10 Preview and Deploy Configuration Changes for All Devices now the changes you made, or wait and deploy multiple changes at once.

Configure SSL Decryption Rules

Use SSL decryption rules to determine how to handle encrypted connections. Rules in the SSL decryption policy are evaluated from top to bottom. The rule applied to traffic is the first one where all the traffic criteria are matched.

You can create and edit rules in the SSL Native Rules section only.

Caution Keep in mind that decrypting and then re-encrypting traffic adds a processing load on the device, which will reduce overall system performance.

Note Traffic for your VPN connections (both site-to-site and remote access) is decrypted before the SSL decryption policy evaluates connections. Thus, SSL decryption rules are never applied to VPN connections, and you do not need to consider VPN connections when creating these rules. However, any use of encrypted connections within a VPN tunnel are evaluated. For example, an HTTPS connection to an internal server through an RA VPN connection is evaluated by SSL decryption rules, even though the RA VPN tunnel itself is not (because it is decrypted already)

Procedure

Before you begin

If you have not already, review Configure SSL Decryption Policies, Enable the SSL Decryption Policy, and Configure the Default SSL Decryption Action to configure the SSL decryption policy your rules will be added to.

If you are creating a decrypt known-key rule, ensure that you upload the certificate and key for the destination server (as an internal certificate) and also edit the SSL decryption policy settings to use the certificate. Known-key rules typically specify the destination server in the destination network criteria of the rule. For more information, see Configure Certificates for Known Key and Re-Sign Decryption.

Procedure

Step 1 In the navigation pane, click **Inventory**.

Step 2 Click the **Devices** tab to locate the device or the **Templates** tab to locate the model device.

Step 3 Click the **FTD** tab and select the device for which you want to enable the SSL Decryption policy.

Step 4 Click **Policy** in the Management pane at the right.

Step 5 Click **SSL Decryption** in the policy bar.

Step 6 Do any of the following:

- To create a new rule, click the blue plus button.
- To edit an existing rule, click the edit icon for the rule.
- To delete a rule you no longer need, click the remove icon for the rule.

Step 7 In **Order**, select where you want to insert the rule in the numbered list of rules.

You can insert rules into the SSL Native Rules section only. The Identity Policy Active Authentication Rules are automatically generated from your identity policy and are read-only.

Rules are applied on a first-match basis, so you must ensure that rules with highly specific traffic matching criteria appear above policies that have more general criteria that would otherwise apply to the matching traffic.

The default is to add the rule to the end of the list. If you want to change a rule's location later, edit this option.

Step 8 In **Name**, enter a name for the rule.

The name cannot contain spaces. You can use alphanumeric characters and these special characters: + . _ -

Step 9 Select the action to apply to matching traffic. For a detailed discussion of each option, see the following:

- Decrypt Re-Sign
- Decrypt Known Key
- Do Not Decrypt
- Block

Step 10 Define the traffic matching criteria using any combination of the following tabs:

- **Source/Destination**—The security zones (interfaces) through which the traffic passes, the IP addresses or the country or continent (geographical location) for the IP address, or the TCP ports used in the traffic. The default is any zone, address, geographical location, and TCP port. See Source/Destination Criteria for SSL Decryption Rules.
- **URL**—The URL category of a web request. The default is that the URL category and reputation are not considered for matching purposes. See URL Criteria for SSL Decryption Rules
- **Application**—The application, or a filter that defines applications by type, category, tag, risk, or business relevance. The default is any encrypted application. See Application Criteria for SSL Decryption Rules .
- **Users**—The user or user group. Your identity policies determine whether user and group information is available for traffic matching. You must configure identity policies to use this criteria. See User Criteria for SSL Decryption Rules.
- **Advanced**—The characteristics derived from the certificates used in the connection, such as SSL/TLS version and certificate status. See Advanced Criteria for SSL Decryption Rules.

To modify a condition, you click the blue plus button  within that condition, select the desired object or element, and click **Select** in the popup dialog box. If the criterion requires an object, you can click **Create New Object** if the object you require does not exist. Click the x for an object or element to remove it from the policy.

When adding conditions to SSL decryption rules, consider the following tips:

- You can configure multiple conditions per rule. Traffic must match all the conditions in the rule for the rule to apply to traffic. For example, you can use a single rule to decrypt traffic based on URL category.
- For each condition in a rule, you can add up to 50 criteria. Traffic that matches any of a condition's criteria satisfies the condition. For example, you can use a single rule to apply application control for up to 50

applications or application filters. Thus, there is an OR relationship among the items in a single condition, but an AND relationship between condition types (for example, between source/destination and application).

- Matching URL category requires the URL license.

Step 11 (Optional.) Configure logging for the rule.

You must enable logging for traffic that matches the rule to be included in dashboard data or Event Viewer. Select from these options:

- **No logging**—Do not generate any events.
- **Send Connection Events To**—If you want to send a copy of the events to an external syslog server, select the server object that defines the syslog server. If the required object does not already exist, click **Create** and create it. (To disable logging to a syslog server, select Any from the server list.)
- **At End of Connection**—Generate an event at the conclusion of the connection. Because event storage on the device is limited, sending events to an external syslog server can provide more long term storage and enhance your event analysis.

If you have a subscription to Cisco Security Analytics and Logging, specify or create a syslog server object using a Secure Event Connector's IP address and port. See Cisco Security Analytics and Logging for more information.

Step 12 Click **Save**.

Step 13 (Optional) For any rule that you created, you can select it and add a comment about it in the Add Comments field. To learn more about rule comments see, Adding Comments to Rules in Policies and Rulesets.

Step 14 Preview and Deploy Configuration Changes for All Devices now the changes you made, or wait and deploy multiple changes at once.

Source/Destination Criteria for SSL Decryption Rules

The Source/Destination criteria of an SSL decryption rule define the security zones (interfaces) through which the traffic passes, the IP addresses or the country or continent (geographical location) for the IP address, or the TCP ports used in the traffic. The default is any zone, address, geographical location, and any TCP port. TCP is the only protocol matched to SSL decryption rules.

To modify a condition, you click the blue button  within that condition, select the desired object or element, and click **Select**. If the criterion requires an object, you can click **Create New Object** if the object you require does not exist. Click the **x** for an object or element to remove it from the policy.

Source Zones, Destination Zones

The security zone objects that define the interfaces through which the traffic passes. You can define one, both, or neither criteria: any criteria not specified applies to traffic on any interface.

- To match traffic leaving the device from an interface in the zone, add that zone to the Destination Zones.
- To match traffic entering the device from an interface in the zone, add that zone to the Source Zones.
- If you add both source and destination zone conditions to a rule, matching traffic must originate from one of the specified source zones and egress through one of the destination zones.

Use this criteria when the rule should apply based on where the traffic enters or exits the device. For example, if you want to ensure that all traffic going from outside hosts to inside hosts gets decrypted, you would select your outside zone as the Source Zones and your inside zone as the Destination Zones.

Source Networks, Destination Networks

The network objects or geographical locations that define the network addresses or locations of the traffic.

- To match traffic from an IP address or geographical location, configure the Source Networks.
- To match traffic to an IP address or geographical location, configure the Destination Networks.

If you add both source and destination network conditions to a rule, matching traffic must originate from one of the specified IP addresses and be destined for one of the destination IP addresses.

When you add this criteria, you select from the following menu options:

- **Network**—Select the network objects or groups that define the source or destination IP addresses for the traffic you want to control.

Note For Decrypt Known-Key rules, select an object with the IP address of the destination server that uses the certificate and key you uploaded.

- **Country/Continent**—Select the geographical location to control traffic based on its source or destination country or continent. Selecting a continent selects all countries within the continent.
- **Custom Geolocation**-You can also select a geolocation object that you created to define the location. Using geographical location, you could easily restrict access to a particular country without needing to know all of the potential IP addresses used there.

Source Ports, Destination Ports/Protocols

The port objects that define the protocols used in the traffic. You can specify TCP protocol and ports only for SSL decryption rules.

- To match traffic from a TCP port, configure the Source Ports.
- To match traffic to a TCP port, configure the Destination Ports/Protocols.

To match traffic both originating from specific TCP ports and destined for specific TCP ports, configure both. For example, you could target traffic from port TCP/80 to port TCP/8080.

Step 10

Application Criteria for SSL Decryption Rules

The Application criteria of an SSL decryption rule defines the application used in an IP connection, or a filter that defines applications by type, category, tag, risk, or business relevance. The default is any application that has the SSL Protocol tag. You cannot match SSL decryption rules to any non-encrypted application.

Although you can specify individual applications in the rule, application filters simplify policy creation and administration. For example, you could create an SSL decryption rule that decrypts or blocks all high risk, low business relevance applications. If a user attempts to use one of those applications, the session is decrypted or blocked.

In addition, Cisco frequently updates and adds additional application detectors via system and vulnerability database (VDB) updates. Thus, a rule for high risk applications can automatically apply to new applications without you having to update the rule manually.

You can specify applications and filters directly in the rule, or create application filter objects that define those characteristics. The specifications are equivalent, although using objects can make it easier to stay within the 50-items-per-criteria system limit if you are creating a complex rule.

To modify the application and filters list, you click the  button within the condition, select the desired applications or application filter objects, and click Select in the popup dialog box and then click Save. Click the x for an application, filter, or object to remove it from the policy. Click the Save As Filter link to save the combined criteria that is not already an object as a new application filter object.

For more information about the application criteria and how to configure advanced filters and select applications, see Configuring Application Filter Objects.

Consider the following tips when using application criteria in SSL decryption rules:

- The system can identify unencrypted applications that become encrypted using StartTLS. This includes such applications as SMTPS, POPS, FTPS, TelnetS, and IMAPS. In addition, it can identify certain encrypted applications based on the Server Name Indication in the TLS ClientHello message, or the server certificate subject distinguished name value.
- The system can identify the application only after the server certificate exchange. If traffic exchanged during the SSL handshake matches all other conditions in an SSL rule containing an application condition but the identification is not complete, the SSL policy allows the packet to pass. This behavior allows the handshake to complete so that applications can be identified. After the system completes its identification, the system applies the SSL rule action to the remaining session traffic that matches its application condition.

Step 10

URL Criteria for SSL Decryption Rules

The URL criteria of an SSL decryption rule defines the category to which the URL in a web request belongs. You can also specify the relative reputation of sites to decrypt, block, or allow without decryption. The default is to not match connections based on URL categories.

For example, you could block all encrypted Gaming sites, or decrypt all high risk Social Networking sites. If a user attempts to browse to any URL with that category and reputation combination, the session is blocked or decrypted.

To add URL criteria to an SSL decryption rule:

Procedure

Step 1 Click the URL tab to add a URL category to an SSL Decryption rule.

Step 2 Search for and select the URL categories you want to block.

Step 3 By default, the traffic from URLs in the categories you pick will be decrypted by the SSL decryption rule no matter their security reputation. However, you can fine-tune the URL category or all the URL categories in your rule to exclude some sites from decryption based on reputation.

- To fine-tune the reputation of a single category in the URL:

a. Click the URL category after you selected it.

b. Uncheck **Any Reputation**.

c. Slide the green slider to the right to choose the URL reputation settings you want to exclude from the rule and click **Save**.

   The reputations that the slider covers are excluded from the effect of the rule. For example, if you slide the green slider to Benign Sites, Well Known Sites and Benign Sites are excluded from the effects of the SSL Decryption rule for the category you chose. URLs deemed to be Sights with Security Risks, Suspicious Sites, and High Risk Sites will still be affected by the rule for that URL category.

- To fine-tune the reputation of all the URL categories you added to the rule:

  a. After you have selected all the categories you want to include in the SSL Decryption rule, click **Apply Reputation to Selected Categories**.

  b. Uncheck **Any Reputation**.

  c. Slide the green slider to the right to choose the URL reputation settings you want to exclude from the rule and click **Save**.

     The reputations that the slider covers are excluded from the effect of the rule. For example, if you slide the green slider to Benign Sites, Well Known Sites and Benign Sites are excluded from the effects of the SSL Decryption rule for all the categories you chose. URLs deemed to be Sights with Security Risks, Suspicious Sites, and High Risk Sites will still be affected by the rule for all the URL categories.

Step 4 Click **Select**.

Step 5 Click **Save**.

Step 10

User Criteria for SSL Decryption Rules

The User criteria of an SSL decryption rule defines the user or user group for an IP connection. You must configure identity policies and the associated directory server to include user or user group criteria in a rule.

Your identity policies determine whether user identity is collected for a particular connection. If identity is established, the IP address of the host is associated with the identified user. Thus, traffic whose source IP address is mapped to a user is considered to be from that user. IP packets themselves do not include user identity information, so this IP-address-to-user mapping is the best approximation available.

Because you can add a maximum of 50 users or groups to a rule, selecting groups usually makes more sense than selecting individual users. For example, you could create a rule that decrypts traffic to the Engineering group that comes from the outside network, and create a separate rule that does not decrypt outgoing traffic from that group. Then, to make the rule apply to new engineers, you only need to add the engineer to the Engineering group in the directory server.

To modify the users list, you click the + button within the condition and select the desired user groups and click Select.

Step 10

Advanced Criteria for SSL Decryption Rules

The Advanced traffic matching criteria relate to characteristics derived from the certificates used in the connection. You can configure any or all of the following options.

Certificate Properties

Traffic matches the certificate properties option of the rule if it matches any of the selected properties. You can configure the following:

- **Certificate Status**: Whether the certificate is Valid or Invalid. Select Any (the default) if you do not care about certificate status. A certificate is considered valid if all of the following conditions are met, otherwise it is invalid:
  - The policy trusts the CA that issued the certificate.
  - The certificate's signature can be properly validated against the certificate's content.
  - The issuer CA certificate is stored in the policy's list of trusted CA certificates.
  - None of the policy's trusted CAs revoked the certificate.
  - The current date is between the certificate Valid From and Valid To dates.
- **Self-Signed**: Whether the server certificate contains the same subject and issuer distinguished name. Select one of the following:
- Self-Signing—The server certificate is self-signed.
  - CA-Signing—The server certificate is signed by a Certificate Authority. That is, the issuer and subject are not the same.
  - Any—Do not consider whether the certificate is self-signed as a match criteria.

Supported Version

The SSL/TLS version to match. The rule applies to traffic that uses the any of the selected versions only. The default is all versions. Select from: SSLv3.0, TLSv1.0, TLSv1.1, TLSv1.2.

For example, if you wanted to permit TLSv1.2 connections only, you could create a block rule for the non-TLSv1.2 versions. Traffic that uses any version not listed, such as SSL v2.0, is handled by the default action for the SSL decryption policy.

Step 10

Configure Certificates for Known Key and Re-Sign Decryption

If you implement decryption, either by re-signing or using known keys, you need to identify the certificates that the SSL decryption rules can use. Ensure that all certificates are valid and unexpired.

Especially for known-key decryption, you need to ensure that the system has the current certificate and key for each destination server whose connections you are decrypting. With a decrypt known key rule, you use the actual certificate and key from the destination server for decryption. Thus, you must ensure that the FDM-managed device has the current certificate and key at all times, or decryption will be unsuccessful.

Upload a new internal certificate and key whenever you change the certificate or key on the destination server in a known key rule. Upload them as an internal certificate (not an internal CA certificate). You can upload

the certificate during the following procedure, or upload the certificate to the **Objects** page by clicking the  button and selecting **FTD > Certificate**.

Procedure

Step 1 In the navigation pane, click **Inventory**.

Step 2 Click the **Devices** tab to locate the device or the **Templates** tab to locate the model device.

Step 3 Click the **FTD** tab and select the device for which you want to create the SSL policy and click **Policy** in the Management pane at the right.

Step 4 Click **SSL Decryption** in the policy bar.

Step 5 Click the certificate button 

in the SSL decryption policy policy bar.

Step 6 In the SSL Decryption Configuration dialog, click the **Select Decrypt Re-Sign Certificate** menu and select or create the internal CA certificate to use for rules that implement decryption with re-signed certificates. You can use the pre-defined **NGFW-Default-InternalCA** certificate, or one that you created or uploaded.

If you have not already installed the certificate in client browsers, click the download button  to obtain a copy. See the documentation for each browser for information on how to install the certificate. Also see the **Downloading the CA Certificate for Decrypt Re-Sign Rules** section of the Security Policies chapter of the Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager for the version your device is running

Step 7 For each rule that decrypts using a known key, upload the internal certificate and key for the destination server.

Step 8 Click  under **Decrypt Known-Key Certificates**.

Step 9 Select the internal identity certificate, or click **Create New Internal Certificate** to upload it now.

Step 10 Click **Save**.

Step 11 Preview and Deploy Configuration Changes for All Devices now the changes you made, or wait and deploy multiple changes at once.

Downloading the CA Certificate for Decrypt Re-Sign Rules

If you decide to decrypt traffic, users must have the internal CA certificate that is used in the encryption process defined as a Trusted Root Certificate Authority in their applications that use TLS/SSL. Typically if you generate a certificate, or sometimes even if you import one, the certificate is not already defined as trusted in these applications. By default in most web browsers, when users send HTTPS requests, they will see a warning message from the client application informing them that there is a problem with the web site's security certificate. Usually, the error message says that the web site's security certificate was not issued by a trusted certificate authority or the web site was certified by an unknown authority, but the warning might also suggest there is a possible man-in-the-middle attack in progress. Some other client applications do not show this warning message to users nor allow users to accept the unrecognized certificate.

You have the following options for providing users with the required certificate:

Inform users to accept the root certificate

You can inform the users in your organization what the new policies are at the company and tell them to accept the root certificate supplied by the organization as a trusted source. Users should accept the certificate

and save it in the Trusted Root Certificate Authority storage area so that they are not prompted again the next time they access the site.

Note The user needs to accept and trust the CA certificate that created the replacement certificate. If they instead simply trust the replacement server certificate, they will continue to see warnings for each different HTTPS site that they visit.

Add the root certificate to client devices

You can add the root certificate to all client devices on the network as a trusted root certificate authority. This way, the client applications automatically accept transactions with the root certificate.

You can either make the certificate available to users by E-mailing it or placing it on a shared site, or you could incorporate the certificate into your corporate workstation image and use your application update facilities to distribute it automatically to users.

The following procedure explains how to download the internal CA certificate and install it on Windows clients.

Procedure

The process differs depending on the operating system and type of browser. For example, you can use the following process for Internet Explorer and Chrome running on Windows. (For Firefox, install through the **Tools** > **Options** > **Advanced** page.)

Messages should indicate that the import was successful. You might see an intermediate dialog box warning you that Windows could not validate the certificate if you generated a self-signed certificate rather than obtaining one from a well-known third-party Certificate Authority.

You can now close out the Certificate and Internet Options dialog boxes.

Procedure

Step 1 Download the certificate from Firepower Device Manager.

a) In the navigation pane, click **Inventory**.
b) Click the **Devices** tab to locate the device or the **Templates** tab to locate the model device.
c) Click the **FTD** tab and select the device on which the certificate is stored.
d) Click **Policy** in the Management pane at the right.
e) Click **SSL Decryption** in the policy bar.
f) Click the SSL decryption configuration button 

in the SSL decryption policy policy bar.
g) Click the Download button 
h) Select a download location, optionally change the file name (but not the extension), and click Save.
i) You can now cancel out of the SSL Decryption Settings dialog box.

Step 2 Install the certificate in the Trusted Root Certificate Authority storage area in web browsers on client systems, or make it available for clients to install themselves. This procedure will be different for different browsers and operating systems.

Warning

CA Certificates Configured Through FDM-Managed Devices

Cisco Defense Orchestrator can manage multiple devices but is limited the in additional information that is saved when the device configuration is saved, which may incur some issues when handling internal CA certificates. CDO **does not** save the cert or key information of CA certificates that are configured through the FDM-managed console; if you attempt to use a CA certificate that was configured in an FDM-managed device and apply it to an SSL policy that is deployed to a secondary device, CDO creates a local copy of the CA certificate but does not and cannot copy the key information. As a result, neither CDO or the secondary device have the key information and the CA certificate cannot be successfully deployed. This also means that the download link for the local copy of the CA certificate is unavailable.

We strongly recommend configuring a separate CA certificate for any additional devices through an FDM-managed device, or creating CA certificates through the CDO UI.

Rulesets

About Rulesets

A ruleset is a collection of access control rules that can be shared with multiple FDM-managed devices. Any changes made to the rules of a ruleset affect the other managed devices that use this ruleset. An FDM-managed device can have device-specific (local) and shared (rulesets) rules. You can also create rulesets from existing rules in an FDM-managed device.

Important The "Rulesets" feature is currently available FDM-managed devices version 6.5 or later and later. Also note that rulesets do not support devices enabled for Snort 3.

The following limitations apply:

- You cannot attach rulesets to Snort 3-enabled devices.
- You cannot create a ruleset from an existing device that has Snort 3 installed.
- You cannot associate a custom IPS policy with a ruleset.

Copy or Move Rules associated with Rulesets

It's possible to copy or move access control rules within a ruleset or across different rulesets. Also, you're allowed to copy or move rules between local and rulesets. See Copy FDM-Managed Access Control Rules and Move FDM-Managed Access Control Rules for more information.

Auto-Detect Existing Rulesets

When you onboard a device, Cisco Defense Orchestrator auto-detects existing rulesets on them and tries to match them with the rules on the device. On a successful match, CDO automatically attaches the rulesets to the newly onboarded device. However, if there are multiple ruleset matches for the same set of rules on the device, none of them are attached, and you have to assign them manually.

Configure Rulesets for a Device

Use the sections below to create and deploy a ruleset:

Procedure

Step 1 Configure Rulesets for a Device.

a) Create a new ruleset and assign rules to it.
b) Assign objects to the rules.
c) Set the priority of the ruleset.
d) Change the order of the rules if required.

Step 2 Configure Rulesets for a Device.

a) Attach multiple devices to a ruleset.
b) Review and deploy the ruleset to the devices.

Create or Edit a Ruleset

You can create a ruleset and add new access control rules to it.

Use the following procedure to create a ruleset for multiple FDM-managed devices:

Procedure

Step 1 In the navigation pane, click **Policies > FTD Rulesets**.

Step 2 Click the plus  button to create a new ruleset.

Note To edit an existing ruleset, select the ruleset and click the edit icon .

Step 3 Enter a name for the ruleset and then click **Create**.

Step 4 Create access control rules to add them to the ruleset. See Configure the FDM Access Control Policy for instructions.

Note Access Control rules in the rulesets don't support criteria for Users criteria.

Step 5 In the upper right corner of the window, select the ruleset's priority 

. The priority can be set when the device is not attached to the ruleset. This selection affects all of the rules included in this ruleset and how it is handled on the devices:

- **Top**- The ruleset is processed before all other rules on the device. Rules are ordered at the top of the rule list and are processed first. No other ruleset can precede the rules in this policy. You can only have one top ruleset per device.
- **Bottom**- The ruleset is processed after all other rules on the device. Other than the policy's default action, no other ruleset can succeed rules in this policy. You can only have one bottom ruleset per device. By default, the priority is set to **Bottom**.

The **Local Rules** displays all the device-specific rules of the device.

Note The priority cannot be changed when a ruleset is attached to a device. You have to detach the device and change the priority.

Step 6 Click **Save**. You can create as many rules as you want.

Step 7 (Optional) For any rule that you created, you can select it and add a comment about it in the Add Comments field. To learn more about rule comments see, Adding Comments to Rules in Policies and Rulesets.

Note

- You can change the order of rules in a ruleset even if you have devices attached to the ruleset. Use the following procedure to change the priority of the ruleset:
  a. In the navigation pane, click **Policies** > **Rulesets** and select the ruleset you want to modify.
  b. Select a rule that you want to move.
  c. Hover the cursor inside the rule row and use the **Move Up** or **Move Down** arrow to move the rule to the desired order.
- CDO allows you to override objects associated with the rules of a ruleset. When you add a new object to a rule, you can override it only after you attach a device to the ruleset and save the changes.

Deploy a Ruleset to Multiple FDM-Managed Devices or Templates

You must attach a ruleset to a device or template for the rules to be enforced. After reviewing the changes, you can deploy the configuration on the device. When you apply a template to a new FDM-managed device, the ruleset included in the template is pushed to the device.

For more information, see Rulesets with FDM-Managed Templates.

Before you begin, consider the following information:

- You can only attach a ruleset to FDM-managed devices that are already onboarded to Cisco Defense Orchestrator.
- A device can have only **one** bottom or top ruleset.
- After you attach or remove a device from a ruleset, the changes are staged in CDO but not deployed, and the device becomes **Not Synced** with CDO. Deploy the changes to the device by clicking the icon from the top right corner of the screen.
- After you attach a device, the new rules associated with rulesets don't overwrite existing rules associated with the device.

You can associate rulesets with devices in two ways:

- Add devices to a Ruleset from the Ruleset page.
- Add Rulesets to a device from the Device Policy page.

Add Devices to a Ruleset from the Ruleset page

Procedure

Step 1 In the navigation pane, click **Policies > FTD Rulesets**.

Step 2 Select the ruleset you want to assign to FDM-managed devices and in the **Actions** pane, click **Edit**.

Step 3 On the top right corner, click the **Device** button 

appearing beside **Ruleset for**.

Step 4 Select from the list of eligible FDM-managed devices.

Step 5 In the gear icon, select one of the following actions for the system to perform when it determines duplicate names between the rules in the ruleset and the device-specific rules:

- **Fail on conflicting rules** (default option): CDO doesn't add the ruleset to the device. You need to manually rename the duplicate rules and then add the ruleset.
- **Rename conflicting rules**: CDO renames the conflicting rules present on the device (Local Rules).

Step 6 Click **Save**. The **Attached Ruleset to Devices** wizard is closed.

Step 7 Click **Save** in the upper right corner to save the changes made to the ruleset. Saving the ruleset stages the changes to CDO.

Note Each time you modify a ruleset, you must click **Save**. By doing this operation, all changes are staged to CDO. You have to deploy the changes manually.

Step 8 Click **Confirm**. Saving the ruleset stages the changes to CDO.

Step 9 Preview and Deploy Configuration Changes for All Devices the changes you made, or wait and deploy multiple changes at once. If you Discard Configuration Changes the staged ruleset changes on a device, see Impact of Discarding Staged Ruleset Changes for information.

Add Rulesets to a Device from the Device Policy page

Procedure

Step 1 In the navigation pane, click **Inventory**.

Step 2 Click the **Devices** tab to locate the device or the **Templates** tab to locate the model device.

Step 3 Click the **FTD** tab and select the device you want from the list.

Step 4 In the **Management** pane on the right, click **Policy**.

Step 5 Click the  button appearing in the upper right corner of the window.

Step 6 Select the rulesets that you want.

Step 7 In the gear icon, select one of the following actions for the system to perform when it determines duplicate names between the rules in the ruleset and the device-specific rules:

- **Fail on conflicting rules** (default option): CDO doesn't add the ruleset to the device. You need to manually rename the duplicate rules and then add the ruleset.

- **Rename conflicting rules**: CDO renames the conflicting rules present on the device (Local Rules).

Note If there are no conflicting rules on the selected device, CDO attaches the ruleset to the device without any changes.

Step 8 Click **Attach Ruleset**. The ruleset gets added to the device based on the priority of the ruleset.

Step 9 Preview and Deploy Configuration Changes for All Devices the changes you made, or wait and deploy multiple changes at once. If you Discard Configuration Changes the staged ruleset changes on a device, see Impact of Discarding Staged Ruleset Changes for information.

Related Information:

- Rulesets
- Rulesets with FDM-Managed Templates
- Detach FDM-Managed Devices from a Selected Ruleset
- Delete Rules and Rulesets
- Impact of Out-of-Band Changes on Rulesets
- View Rules and Rulesets
- Change Log Entries after Creating Rulesets
- Create Rulesets from Existing Device Rules

Rulesets with FDM-Managed Templates

Cisco Defense Orchestrator allows you to assign the rulesets to FDM-managed templates.

- When you create a template from an FDM-managed device with rulesets, CDO adds the template automatically to the rulesets that were present on the source device. You can manage the template from rulesets.
- When you apply a template with rulesets to a target FDM-managed device, CDO adds the target device automatically to the rulesets, thereby manage the target device from rulesets.
- When a template with rulesets is applied to a target FDM-managed device which already has different rulesets, CDO removes the existing rulesets from the target device and adds new rulesets associated with the template.

See Deploy a Ruleset to Multiple FDM-Managed Devices or Templates for more information.

Related Information:

- Rulesets
- Configure Rulesets for a Device
- Create Rulesets from Existing Device Rules
- Impact of Out-of-Band Changes on Rulesets
- View Rules and Rulesets

- Change Log Entries after Creating Rulesets
- Detach FDM-Managed Devices from a Selected Ruleset
- Delete Rules and Rulesets

Create Rulesets from Existing Device Rules

You're allowed to create rulesets by selecting existing rules in the FDM-managed device.

Use the following procedure to create a ruleset from existing device rules:

Procedure

Step 1 In the navigation pane, click **Inventory**.

Step 2 Click the **Devices** tab to locate the device or the **Templates** tab to locate the model device.

Step 3 Click the **FTD** tab and select the device that you want from the list.

Step 4 In the **Management** pane on the right, click **Policy**. The existing rules of the device appear.

Step 5 Perform the following based on your requirement:

a) To create **Top** rules, select consecutive rules starting from the first rule at the top.

b) To create **Bottom** rules, select consecutive rules that include the last rule at the bottom.

Step 6 In the **Actions** pane on the right, click **Create Ruleset**.

Note Your selection must include the first or last rule for the **Create Ruleset** link to be clickable.

Step 7 Specify a name in the **Ruleset Name** field and click **Create**. The corresponding ruleset is created in the device.

You can continue creating ruleset using the remaining rules in the device.

Impact of Out-of-Band Changes on Rulesets

When you add new rules or make changes to the existing rules using the FDM-managed device, and you have enabled conflict detection in Cisco Defense Orchestrator for your FDM-managed device, CDO detects the out-of-band change and the device's configuration status shows **Conflict Detected**. Resolve Configuration Conflicts.

If you accept the device changes, CDO overwrites the last know configuration with the new changes made on the device. The following changes take place:

- Rulesets that are impacted by the changes lose their relationship with devices.
- Rules associated with these rulesets are converted to local rules.

If you reject the device changes, CDO rejects the new changes and replaces configuration on the device with the last synced configuration in CDO.

Related Information:

- Rulesets
- Configure Rulesets for a Device

- Create Rulesets from Existing Device Rules
- Impact of Discarding Staged Ruleset Changes
- View Rules and Rulesets
- Change Log Entries after Creating Rulesets
- Detach FDM-Managed Devices from a Selected Ruleset
- Delete Rules and Rulesets

Impact of Discarding Staged Ruleset Changes

When you add new rules to a ruleset or make changes to the existing rules associated with the ruleset using CDO, it saves the changes you make to its own copy of the configuration file. Those changes are considered "pending" on CDO until they are "deployed" to the device.

If you Discard Configuration Changes the pending ruleset changes on the device, CDO **completely overwrites** its local copy of a device's configuration with the configuration stored on the device.

The following changes occur on the rulesets and the associated devices:

- Rulesets that are impacted by the changes lose their relationship with devices.
- Rules associated with these rulesets are converted to local rules.
- CDO discards the new staged changes and retains the configuration present on the device.

Related Information:

- Rulesets
- Configure Rulesets for a Device
- Create Rulesets from Existing Device Rules
- Impact of Out-of-Band Changes on Rulesets
- View Rules and Rulesets
- Change Log Entries after Creating Rulesets
- Detach FDM-Managed Devices from a Selected Ruleset
- Delete Rules and Rulesets

View Rules and Rulesets

View Rules from Device Policy Page

The FDM-managed device policy page shows individual (local) and shared rules (associated with rulesets).

Use the following procedure to view the FDM-managed device ruleset from the policy page:

Procedure

Step 1 In the navigation pane, click **Inventory**.

Step 2 Click the **Devices** tab to locate the device or the **Templates** tab to locate the model device.

Step 3 Click the **FTD** tab and select the device that you want.

Step 4 In the **Management** pane on the right, click **Policy**. You see the following rules based on the configuration you have made:

- **Top Rules**: Shows the mandatory shared rules which will be processed before all other rules on the device.
- **Local Rules**: Shows device-specific rules which will be processed after mandatory rules on the device.
- **Bottom**: Shows the default shared rules which will be processed after all other rules on the device.

Note You can edit the ruleset by going to the corresponding ruleset page.

a) On the top right corner of the ruleset header, click **Go to ruleset**  .
b) Make the required changes to the rules and click **Save**. The new changes are updated on all devices associated with the ruleset.

View Rulesets

The **Rulesets** page shows all rulesets available in your tenant. It also provides information about devices associated with the rulesets.

Use the following procedure to view all rulesets from the Rulesets page:

Procedure

Step 1 In the navigation pane, click **Policies** > **Rulesets**. The rules available in your tenant are displayed.

Step 2 Click a ruleset to view its details. The **Devices** column shows the number of FDM-managed devices attached to each ruleset.

Step 3 In the **Management** pane, click **Workflows**. This page shows all the actions that you performed on the device. You can click **Diagram** to view a pictorial representation of the workflow.

Search Rulesets

You can use the **Filter by Device** filter to select the devices for viewing the rulesets assigned to them.

Procedure

Step 1 In the navigation pane, click **Policies** > **Rulesets**.

Step 2 Click the filter icon and click **Filter by Device**.

Step 3 Select one or more devices from the list and click **OK**.

You can see the rulesets based on the devices you have selected.

View Jobs Associated with Rulesets

The **Jobs** page records actions when you apply ruleset to FDM-managed devices or remove them from FDM-managed devices. It also determines if the action was successful or failed.

Procedure

Step 1 In the navigation pane, click **Policies** > **Rulesets**.

Step 2 Click a ruleset to view its details.

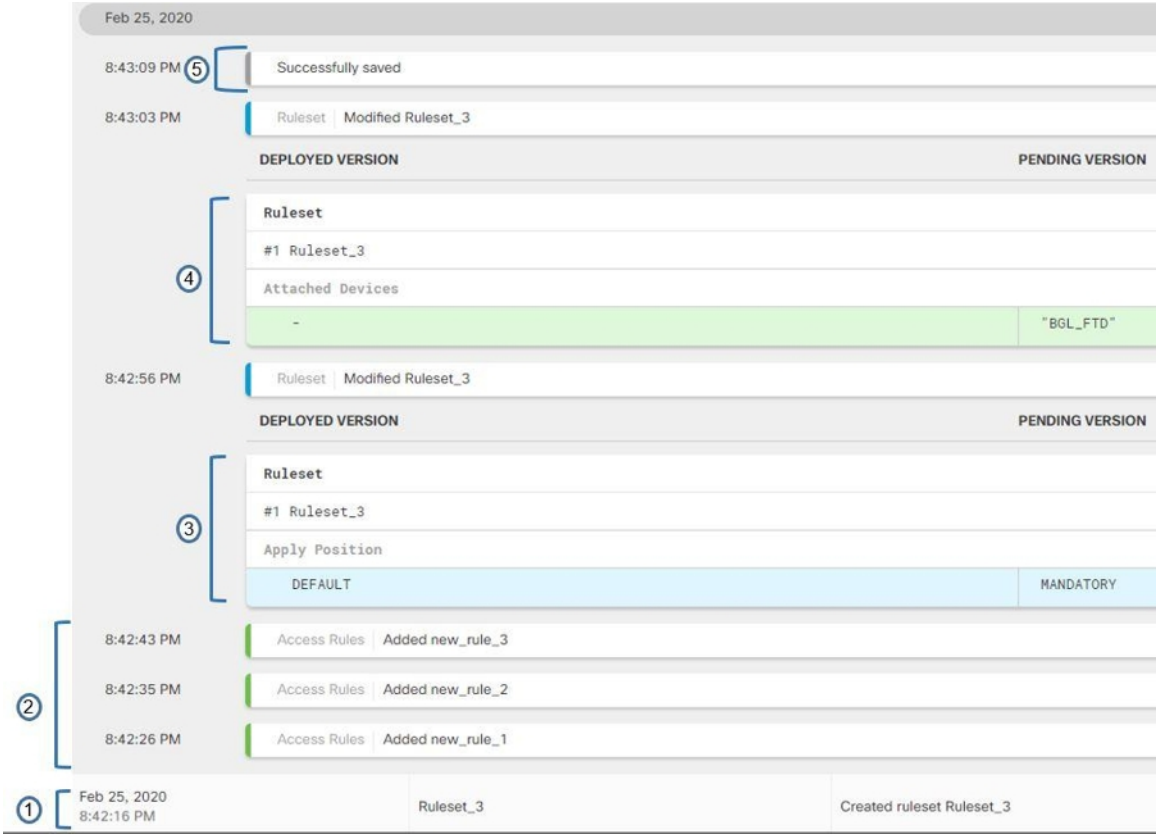
Step 3 In the **Management** pane, click **Jobs**. This page shows actions that you performed on the ruleset.

Change Log Entries after Creating Rulesets

When CDO detects a change on the ruleset, it creates a change log entry for every action performed on the ruleset.

Clicking the blue Diff link in the change log entry row displays a side-by-side comparison of the changes in the context of the running configuration file.

In the following example, the change log shows entries for a new ruleset with three rules added to the ruleset. It also shows information about setting the ruleset's priority and the FDM-managed device attached to the ruleset.



Number in Illustration	Explanation
1	The new ruleset "Ruleset_3" is created at 11:03:18 A.M on Feb 25, 2020.
2	The new access rules "new_rule_1", "new_rule_3", and "new_rule_3" are created in the ruleset.
3	The ruleset's priority is set to "Mandatory".
4	The ruleset is attached to the "BGL_FTD" device.
5	The ruleset changes are saved.

Detach FDM-Managed Devices from a Selected Ruleset

Use the following procedure to detach devices from a ruleset:

Procedure

Step 1 In the navigation pane, click **Policies** > **Rulesets**.

Step 2 Select the ruleset you want to edit and click the **Edit** link in the **Actions** pane.

Step 3 On the top right corner, click the **Device** button appearing beside **Ruleset for**.

Step 4 Uncheck the devices that are currently attached to the ruleset, or click **Clear** to remove all devices at once.

Step 5 Click **Save**.

Step 6 Click **Save** in the upper right window to save the ruleset. Saving the policy stages the changes to CDO.

Step 7 Preview and Deploy Configuration Changes for All Devices the changes you made, or wait and deploy multiple changes at once.

Related Information:

- Rulesets
- Configure Rulesets for a Device
- Create Rulesets from Existing Device Rules
- Impact of Out-of-Band Changes on Rulesets
- View Rules and Rulesets
- Change Log Entries after Creating Rulesets
- Delete Rules and Rulesets

Delete Rules and Rulesets

Delete Rules from a Ruleset

You can delete a rule that you no longer need in the ruleset.

Use the following procedure to delete rules:

Procedure

Step 1 In the navigation pane, click **Policies** > **Rulesets** and select a ruleset.

Step 2 Click **Edit** in the **Actions** pane.

Step 3 Select a rule that you want to delete and then click **Remove** under **Actions**.

Step 4 Click **OK** to confirm the deletion.

Step 5 Click **Save** in the upper right corner to save the changes made to the ruleset. Saving the ruleset stages the changes to CDO.

Step 6 Preview and Deploy Configuration Changes for All Devices your changes now or wait and deploy multiple changes at one time.

Delete a Ruleset

You can delete a ruleset only after detaching all devices associated with it. See Delete Rules and Rulesets.

Use the following procedure to delete a ruleset:

Procedure

Step 1 In the navigation pane, click **Policies** > **Rulesets** and select the ruleset you want to delete.

Step 2 Click **Remove** inside the ruleset row.

Step 3 Click **Confirm** to delete the ruleset permanently.

Step 4 Preview and Deploy Configuration Changes for All Devices your changes now or wait and deploy multiple changes at one time.

- Rulesets
- Configure Rulesets for a Device
- Detach FDM-Managed Devices from a Selected Ruleset

Remove a Ruleset From a Selected FDM-Managed Device

There are two ways of removing a ruleset from a selected FDM-managed device, but their behaviors are slightly different.

- Delete a Ruleset From a Selected FDM-Managed Device: This feature deletes a Ruleset and its associated shared rules from a selected FDM-managed device.
- Disassociate a Ruleset From a Selected FDM-Managed Device: This feature doesn't remove the shared rules. Instead, it converts the shared rules to local rules.

Delete a Ruleset From a Selected FDM-Managed Device

You can delete a ruleset and its associated shared rules from a selected FDM-managed device. The ruleset can also be Detach FDM-Managed Devices from a Selected Ruleset from the ruleset page.

Procedure

Step 1 In the navigation pane, click **Inventory**.

Step 2 Click the **Devices** tab to locate the device or the **Templates** tab to locate the model device.

Step 3 Click the **FTD** tab and select the device that you want from the list.

Step 4 Click the delete icon appearing on the top right corner of a ruleset.

Step 5 Click **Confirm**.

Step 6 Preview and Deploy Configuration Changes for All Devices the changes you made, or wait and deploy multiple changes at once.

Disassociate a Ruleset From a Selected FDM-Managed Device

If you want to add a new device-specific rule to a ruleset in an FDM-managed device, you need to dissociate that ruleset from the FDM-managed device, which converts its associated shared rules to local rules. Then, you can add the rules that you want to local rules.

Procedure

Step 1 In the navigation pane, click **Inventory**.

Step 2 Click the **Devices** tab to locate the device or the **Templates** tab to locate the model device.

Step 3 Click the **FTD** tab and select the device that you want from the list.

Step 4 In the **Management** pane on the right, click **Policy**.

Step 5 Click the icon appearing on the top right corner of a ruleset.

Step 6 Click **Confirm**.

Step 7 Preview and Deploy Configuration Changes for All Devices the changes you made, or wait and deploy multiple changes at once.

Adding Comments to Rules in Policies and Rulesets

You can add comments to rules in FDM-managed device policies and rules in rulesets to document some characteristic of a rule. Rule comments are are only visible on Cisco Defense Orchestrator; they are never written to the FDM-managed device nor are they visible in FDM.

Comments are added to rules after they are created and saved in CDO. As rule comments are only a feature of CDO, creating, changing, or deleting a rule comment does not change the configuration status of the device in CDO to "Not Synced". You will not need to write changes from CDO to the FDM-managed device to save a rule comment.

Comments associated with rules in an FDM-managed device policy can be viewed and edited on the device's policy page. Comments associated with rules in an FDM-managed device ruleset can be viewed and edited on the rulesets page. When a ruleset is used in a policy, any comments associated with any of the rules in the ruleset are displayed in the comments area of the policy. The comments are read-only.

When you search for a string in policies, rulesets, or the change log, CDO will search the comments associated with a rule for that string along with the other attributes and values of a rule.

When a comment for a rule is added or edited, that action is recorded in the Change log. Because rule comments are only recorded and maintained in CDO, they are labeled (CDO-only change) in the change log.

Caution If there is an out of band change to an FDM-managed device's configuration and CDO reads that configuration into its database, the comments associated with any rules will be wiped out.

Adding a Comment to a Rule

Procedure

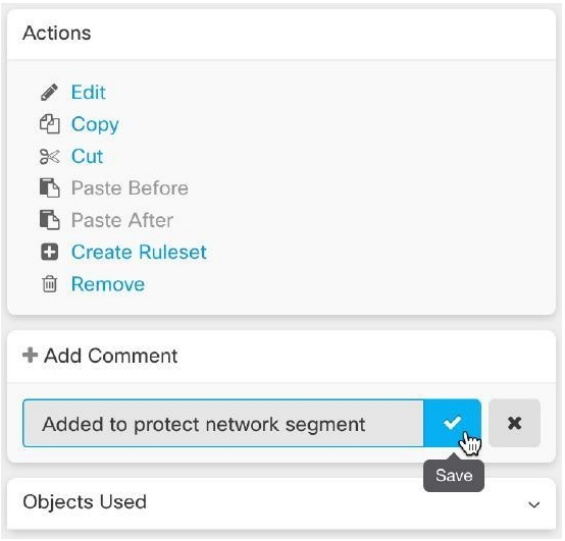
Step 1 Open the policy or ruleset that contains the rule you want to comment on.

Step 2 Select the rule.

Step 3 Click **Add Comment** in the Add Comment area for the rule.

Step 4 Add a comment in the text box.

Step 5 Click **Save**.



Editing Comments about Rules in Policies and Rulesets

Editing a comment on a rule in a policy

Use this procedure to edit a comment on a rule in an FDM-managed device policy.

Procedure

Step 1 From the CDO menu bar, select **Policies > FTD/Meraki/AWS Policies**.

Step 2 Select the FDM-managed device policy with the Local Rule you are going to add a comment to. You are not able to add a comment to a rule in a ruleset within a policy.

Step 3 In the Comment pane, click the edit icon .

Step 4 Edit the comment and click save. You will see the comment change reflected in the Comment area immediately.

Editing a comment on a rule in a ruleset

In order to see a change to a comment on a rule in a ruleset, reflected on the policy page, you have to make changes to the comment and the rule in a specific order.

Procedure

Step 1 From the CDO navigation panel, select **Policies > FTD Rulesets**.

Step 2 Select the ruleset with the rule you want to add a comment to.

Step 3 In the Actions pane, click **Edit**.

Step 4 Select the rule.

Step 5 In the Comment pane, click the edit icon .

Step 6 Edit the comment and click save. You will see the comment change reflected in the Comment area of the ruleset page immediately.

Step 7 Select the rule you are going to change and in the Actions pane, click **Edit**.

Step 8 Edit the rule and click the blue check button to save the change.

Step 9 At the top of the ruleset page, click **Save** to save the ruleset. The new comment for the rule in the ruleset will now be reflected on a policy page.

Step 10 To see the comment change in a policy page:

a) From the CDO menu bar, select **Policies > FTD/Meraki/AWS Policies**.
b) Select an FDM-managed device policy that contains the ruleset you just edited.
c) Select the rule with the comment you just edited. You should see your new comment in the Comment pane.

Network Address Translation

Each computer and device within an IP network is assigned a unique IP address that identifies the host. Because of a shortage of public IPv4 addresses, most of these IP addresses are private and not routable anywhere outside of the private company network. RFC 1918 defines the private IP addresses you can use internally that should not be advertised:

- 10.0.0.0 through 10.255.255.255
- 172.16.0.0 through 172.31.255.255
- 192.168.0.0 through 192.168.255.255

One of the main functions of Network Address Translation (NAT) is to enable private IP networks to connect to the Internet. NAT replaces a private IP address with a public IP address, translating the private addresses in the internal private network into legal, routable addresses that can be used on the public Internet. In this way, NAT conserves public addresses because it can be configured to advertise at a minimum only one public address for the entire network to the outside world.

Other functions of NAT include:

- Security-Keeping internal IP addresses hidden discourages direct attacks.
- IP routing solutions-Overlapping IP addresses are not a problem when you use NAT.
- Flexibility-You can change internal IP addressing schemes without affecting the public addresses available externally; for example, for a server accessible to the Internet, you can maintain a fixed IP address for Internet use, but internally, you can change the server address.
- Translating between IPv4 and IPv6 (Routed mode only)-If you want to connect an IPv6 network to an IPv4 network, NAT lets you translate between the two types of addresses.

You can use Cisco Defense Orchestrator to create NAT rules for many different use cases. Use the NAT rule wizard or these topics to create different NAT rules:

Order of Processing NAT Rules

Network Object NAT and twice NAT rules are stored in a single table that is divided into three sections. Section 1 rules are applied first, then section 2, and finally section 3, until a match is found. For example, if a match is found in section 1, sections 2 and 3 are not evaluated. The following table shows the order of rules within each section.

Table 5: NAT Rule Table

Table Section	Rule Type	Order of Rules within the Section
Section 1	Twice NAT (ASA) Manual NAT (FTD)	Applied on a first match basis, in the order they appear in the configuration. Because the first match is applied, you must ensure that specific rules come before more general rules, or the specific rules might not be applied as desired. By default, twice NAT rules are added to section 1.
Section 2	Network Object NAT (ASA) Auto NAT (FTD)	If a match in section 1 is not found, section 2 rules are applied in the following order: **1.** Static rules. **2.** Dynamic rules. **Within each rule type, the following ordering guidelines are used:** **1.** Quantity of real IP addressesâ€”From smallest to largest. For example, an object with one address will be assessed before an object with 10 addresses. **2.** For quantities that are the same, then the IP address number is used, from lowest to highest. For example, 10.1.1.0 is assessed before 11.1.1.0. **3.** If the same IP address is used, then the name of the network object is used, in alphabetical order. For example, object "Arlington" is assessed before object "Detroit."
Section 3	Twice NAT (ASA) Manual NAT (FTD)	If a match is still not found, section 3 rules are applied on a first match basis, in the order they appear in the configuration. This section should contain your most general rules. You must also ensure that any specific rules in this section come before general rules that would otherwise apply.

For section 2 rules, for example, you have the following IP addresses defined within network objects:

- 192.168.1.0/24 (static)

- 192.168.1.0/24 (dynamic)
- 10.1.1.0/24 (static)
- 192.168.1.1/32 (static)
- 172.16.1.0/24 (dynamic) (object Detroit)
- 172.16.1.0/24 (dynamic) (object Arlington)

The resultant ordering would be:

- 192.168.1.1/32 (static)
- 10.1.1.0/24 (static)
- 192.168.1.0/24 (static)
- 172.16.1.0/24 (dynamic) (object Arlington)
- 172.16.1.0/24 (dynamic) (object Detroit)
- 192.168.1.0/24 (dynamic)

Network Address Translation Wizard

The Network Address Translation (NAT) wizard helps you create NAT rules on your devices for these types of access:

- **Enable Internet Access for Internal Users**. You may use this NAT rule to allow users on an internal network to reach the internet.
- **Expose an Internal Server to the Internet**. You may use this NAT rule to allow people outside your network to reach an internal web or email server.

Prerequisites to "Enable Internet Access for Internal Users"

Before you create your NAT rule, gather this information:

- The interface that is closest to your users; this is usually called the "inside" interface.
- The interface closest to your Internet connection; this is usually called the "outside" interface.
- If you want to allow only specific users to reach the internet, you need the subnet addresses for those users.

Prerequisites to "Expose an Internal Server to the Internet"

Before you create your NAT rule, gather this information:

- The interface that is closest to your users; this is usually called the "inside" interface.
- The interface closest to your Internet connection; this is usually called the "outside" interface.
- The IP address of the server inside your network that you would like to translate to an internet-facing IP address.

- The public IP address you want the server to use.

What to do Next

See Create a NAT Rule by using the NAT Wizard, on page 182.

Create a NAT Rule by using the NAT Wizard

Before you begin

See Network Address Translation Wizard, on page 181 for the prerequisites needed to create NAT rules using the NAT wizard.

Procedure

Step 1 In the CDO navigation bar, click **Inventory**.

Step 2 Click the **Devices** tab to locate the device or the **Templates** tab to locate the model device.

Step 3 Click the appropriate device type tab.

Step 4 Use the filter and search fields to find the device for which you want to create the NAT rule.

Step 5 In the **Management** area of the details panel, click **NAT** NAT.

Step 6 Click + > **NAT Wizard**.

Step 7 Respond to the NAT Wizard questions and follow the on-screen instructions.

- The NAT Wizard creates rules with Network Objects. Either select an existing object from the drop-down menu, or create a new object with the create button + Create... .
- Before you can save the NAT rule, all IP addresses need to be defined as network objects.

Step 8 Preview and Deploy Configuration Changes for All Devices now the changes you made, or wait and deploy multiple changes at once.

Common Use Cases for NAT

Twice NAT and Manual NAT

Here are some common tasks that can be achieved using "Network Object NAT", also known as "Auto NAT":

- Enable a Server on the Inside Network to Reach the Internet Using a Public IP address, on page 183
- Enable Users on the Inside Network to Access the Internet Using the Outside Interface's Public IP Address, on page 184
- Make a Server on the Inside Network Available on a Specific Port of a Public IP Address, on page 185
- Translate a Range of Private IP Addresses to a Range of Public IP Addresses, on page 188

Network Object NAT and Auto NAT

Here is a common task that can be achieved using "Twice NAT", also know as "Manual NAT":

- Prevent a Range of IP Addresses from Being Translated When Traversing the Outside Interface, on page 189

Enable a Server on the Inside Network to Reach the Internet Using a Public IP address

Use Case

Use this NAT strategy when you have a server with a private IP address that needs to be accessed from the internet and you have enough public IP addresses to NAT one public IP address to the private IP address. If you have a limited number of public IP addresses, see Make a Server on the Inside Network Available on a Specific Port of a Public IP Address (that solution may be more suitable).

Strategy

Your server has a static, private IP address, and users outside your network have to be able to reach your server. Create a network object NAT rule that translates the static private IP address to a static public IP address. After that, create an access policy that allows traffic from that public IP address to reach the private IP address. Finally, deploy these changes to your device.

Before you begin

Before you begin, create two network objects. Name one object *servername*_inside and the other object *servername*_outside. The *servername*_inside network object should contain the private IP address of your server. The *servername*_outside network object should contain the public IP address of your server. See Create Network Objects for instructions.

Procedure

Step 1 In the CDO navigation bar, click **Inventory**.

Step 2 Click the **Devices** tab to locate the device or the **Templates** tab to locate the model device.

Step 3 Click the appropriate device type tab.

Step 4 Select the device you want to create the NAT rule for.

Step 5 Click **NAT** in the **Management** pane at the right.

Step 6 Click  > **Network Object NAT.**

Step 7 In section 1, **Type**, select **Static.** Click **Continue**.

Step 8 In section 2, **Interfaces**, choose **inside** for the source interface and **outside** for the destination interface. Click **Continue**.

Step 9 In section 3, **Packets**, perform these actions:

a. Expand the Original Address menu, click **Choose**, and select the **servername_inside** object.

b. Expand the Translated Address menu, click **Choose**, and select the **servername_outside** object.

Step 10 Skip section 4, **Advanced**.

Step 11 For an FDM-managed device, in section 5, **Name**, give the NAT rule a name.

Step 12 Click **Save**.

Step 13 For ASA, deploy a Network Policy rule or for FDM-managed device, deploy an access control policy rule to allow the traffic to flow from *servername*_inside to *servername*_outside.

Step 14 Preview and Deploy Configuration Changes for All Devices now the changes you made, or wait and deploy multiple changes at once.

Enable Users on the Inside Network to Access the Internet Using the Outside Interface's Public IP Address

Use Case

Allow users and computers in your private network to connect to the internet by sharing the public address of your outside interface.

Strategy

Create a port address translation (PAT) rule that allows all the users on your private network to share the outside interface public IP address of your device.

After the private address is mapped to the public address and port number, the device records that mapping. When incoming traffic bound for that public IP address and port is received, the device sends it back to the private IP address that requested it.

Procedure

Step 1 In the CDO navigation bar, click **Inventory**.

Step 2 Click the **Devices** tab to locate the device or the **Templates** tab to locate the model device.

Step 3 Click the appropriate device type tab.

Step 4 Select the device you want to create the NAT rule for.

Step 5 Click **NAT** in the **Management** pane at the right.

Step 6 Click  **Network Object NAT.**

Step 7 In section 1, **Type**, select **Dynamic.** Click **Continue**.

Step 8 In section 2, **Interfaces**, choose **any** for the source interface and **outside** for the destination interface. Click **Continue**.

Step 9 In section 3, **Packets**, perform these actions :

a. Expand the Original Address menu, click **Choose** and select the **any-ipv4** or **any-ipv6** object depending on your network configuration.

b. Expand the Translated Address menu, and select **interface** from the available list. Interface indicates to use the public address of the outside interface.

Step 10 For an FDM-managed device, in section 5, **Name**, enter a name for the NAT rule.

Step 11 Click **Save**.

Step 12 Preview and Deploy Configuration Changes for All Devices now the changes you made, or wait and deploy multiple changes at once.

Entries in the ASA's Saved Configuration File

Here are the entries that are created and appear in an ASA's saved configuration file as a result of this procedure.

Note This does not apply to FDM-managed devices.

Objects created by this procedure:

```
object network any_network
subnet 0.0.0.0 0.0.0.0
```

NAT rules created by this procedure:

```
object network any_network
nat (any,outside) dynamic interface
```

Make a Server on the Inside Network Available on a Specific Port of a Public IP Address

Use Case

If you only have one public IP address, or a very limited number, you can create a network object NAT rule that translates inbound traffic, bound for a static IP address and port, to an internal address. We have provided procedures for specific cases, but you can use them as a model for other supported applications.

Prerequisites

Before you begin, create three separate network objects, one each for an FTP, HTTP, and SMTP server. For the sake of the following procedures, we call these objects **ftp-server-object**, **http-server-object**, and **smtp-server-object**. See Create Network Objects for instructions.

NAT Incoming FTP Traffic to an FTP Server

Procedure

Step 1 In the CDO navigation bar, click **Inventory**.

Step 2 Click the **Devices** tab to locate the device or the **Templates** tab to locate the model device.

Step 3 Click the appropriate device type tab.

Step 4 Select the device you want to create the NAT rule for.

Step 5 Click **NAT** in the **Management** pane at the right.

Step 6 Click  > **Network Object NAT.**

Step 7 In section 1, **Type**, select **Static.** Click **Continue**.

Step 8 In section 2, **Interfaces**, choose **inside** for the source interface and **outside** for the destination interface. Click **Continue**.

Step 9 In section 3, **Packets**, perform these actions:

- Expand the Original Address menu, click **Choose**, and select the **ftp**-server-object.
- Expand the Translated Address menu, click **Choose**, and select the **Interface**.

- Check **Use Port Translation**.
- Select **tcp**, **ftp, ftp.**

Step 10 Skip section 4, **Advanced**.

Step 11 For an FDM-managed device, in section 5, **Name**, give the NAT rule a name.

Step 12 Click **Save**. The new rule is created in Order of Processing NAT Rules of the NAT table.

Step 13 Preview and Deploy Configuration Changes for All Devices now the changes you made, or wait and deploy multiple changes at once.

NAT Incoming HTTP Traffic to an HTTP Server

If you only have one public IP address, or a very limited number, you can create a network object NAT rule that translates inbound traffic, bound for a static IP address and port, to an internal address. We have provided procedures for specific cases, but you can use them as a model for other supported applications.

Before you begin

Before you begin, create a network object for the http server. For the sake of this procedure, we will call the object, **http-object**. See Create Network Objects for instructions.

Procedure

Step 1 In the CDO navigation bar, click **Inventory**.

Step 2 Click the **Devices** tab to locate the device or the **Templates** tab to locate the model device.

Step 3 Click the appropriate device type tab.

Step 4 Select the device you want to create the NAT rule for.

Step 5 Click **NAT** in the **Management** pane at the right.

Step 6 Click  > **Network Object NAT.**

Step 7 In section 1, **Type**, select **Static.** Click **Continue**.

Step 8 In section 2, **Interfaces**, choose **inside** for the source interface and **outside** for the destination interface. Click **Continue**.

Step 9 In section 3, **Packets**, perform these actions:

- Expand the Original Address menu, click **Choose**, and select the **http**-object.
- Expand the Translated Address menu, click **Choose**, and select the **Interface**.
- Check **Use Port Translation**.
- Select **tcp**, **http**, http.

Step 10 Skip section 4, **Advanced**.

Step 11 For an FDM-managed device, in section 5, **Name**, give the NAT rule a name.

Step 12 Click **Save**. The new rule is created in Order of Processing NAT Rules of the NAT table.

Step 13 Preview and Deploy Configuration Changes for All Devices now the changes you made, or wait and deploy multiple changes at once.

NAT Incoming SMTP Traffic to an SMTP Server

If you only have one public IP address, or a very limited number, you can create a network object NAT rule that translates inbound traffic, bound for a static IP address and port, to an internal address. We have provided procedures for specific cases, but you can use them as a model for other supported applications.

Before you begin

Before you begin, create a network object for the smtp server. For the sake of this procedure, we will call the object, **smtp-object**. See Create Network Objects for instructions.

Procedure

Step 1 In the CDO navigation bar, click **Inventory**.

Step 2 Click the **Devices** tab to locate the device or the **Templates** tab to locate the model device.

Step 3 Click the appropriate device type tab.

Step 4 Select the device you want to create the NAT rule for.

Step 5 Click **NAT** in the **Management** pane at the right.

Step 6 Click + > **Network Object NAT.**

Step 7 In section 1, **Type**, select **Static.** Click **Continue**.

Step 8 In section 2, **Interfaces**, choose **inside** for the source interface and **outside** for the destination interface. Click **Continue**.

Step 9 In section 3, **Packets**, perform these actions:

- Expand the Original Address menu, click **Choose**, and select the smtp-server-object.
- Expand the Translated Address menu, click **Choose**, and select the **Interface**.
- Check **Use Port Translation**.
- Select **tcp**, **smtp**, **smtp.**

Step 10 Skip section 4, **Advanced**.

Step 11 For an FDM-managed device, in section 5, **Name**, give the NAT rule a name.

Step 12 Click **Save**. The new rule is created in Order of Processing NAT Rules of the NAT table.

Step 13 Preview and Deploy Configuration Changes for All Devices now the changes you made, or wait and deploy multiple changes at once.

Translate a Range of Private IP Addresses to a Range of Public IP Addresses

Use Case

Use this approach if you have a group of specific device types, or user types, that need to have their IP addresses translated to a specific range so that the receiving devices (the devices on the other end of the transaction) allow the traffic in.

Translate a Pool of Inside Addresses to a Pool of Outside Addresses

Before you begin

Create a network object for the pool of private IP addresses you want to translate and create a network object for the pool of public addresses you want to translate those private IP addresses into.

Note For the ASA FTD, the network group that defines the pool of "translated address" cannot be a network object that defines a subnet.

When creating these address pools, use Create or Edit a Firepower Network Object or Network Group for instructions.

For the sake of the following procedure, we named the pool of private addresses, **inside_pool** and name the pool of public addresses, **outside_pool.**

Procedure

Step 1 In the CDO navigation bar, click **Inventory**.

Step 2 Click the **Devices** tab to locate the device or the **Templates** tab to locate the model device.

Step 3 Click the appropriate device type tab.

Step 4 Select the device you want to create the NAT rule for.

Step 5 Click **NAT** in the **Management** pane at the right.

Step 6 Click + > **Network Object NAT**.

Step 7 In section 1, **Type**, select **Dynamic** and click **Continue**.

Step 8 In section 2, **Interfaces**, set the source interface to **inside** and the destination interface to **outside**. Click **Continue**.

Step 9 In section 3, **Packets**, perform these tasks:

- For the Original Address, click **Choose** and then select the **inside_pool** network object (or network group) you made in the prerequisites section above.

- For the Translated Address, click **Choose** and then select the **outside_pool** network object (or network group) you made in the prerequisites section above.

Step 10 Skip section 4, **Advanced**.

Step 11 For an FDM-managed device, in section 5, **Name**, give the NAT rule a name.

Step 12 Click **Save**.

Step 13 Preview and Deploy Configuration Changes for All Devices now the changes you made, or wait and deploy multiple changes at once.

Prevent a Range of IP Addresses from Being Translated When Traversing the Outside Interface

Use Case

Use this Twice NAT use case to enable site-to-site VPN.

Strategy

You are translating a pool of IP addresses to itself so that the IP addresses in one location on the network arrives unchanged in another.

Create a Twice NAT Rule

Before you begin

Create a network object or network group that defines the pool of IP addresses you are going to translate to itself. For the ASA, the range of addresses can be defined by a network object that uses an IP address range, a network object that defines a subnet, or a network group object that includes all the addresses in the range. For the FTD, the range of addresses can be defined by a network object that defines a subnet or a network group object that includes all the addresses in the range.

When creating the network objects or network groups, use Create or Edit a Firepower Network Object or Network Group for instructions.

For the sake of the following procedure, we are going call the network object or network group, Site-to-Site-PC-Pool.

Procedure

Step 1 In the CDO navigation bar, click **Inventory**.

Step 2 Click the **Devices** tab to locate the device or the **Templates** tab to locate the model device.

Step 3 Click the appropriate device type tab.

Step 4 Select the device you want to create the NAT rule for.

Step 5 Click **NAT** in the **Management** pane at the right.

Step 6 Click  > **Twice NAT.**.

Step 7 In section 1, **Type**, select **Static.** Click **Continue**.

Step 8 In section 2, **Interfaces**, choose **inside** for the source interface and **outside** for the destination interface. Click **Continue**.

Step 9 In section 3, **Packets**, make these changes:

- Expand the Original Address menu, click **Choose**, and select the Site-to-Site-PC-Pool object you created in the prerequisites section.
- Expand the Translated Address menu, click **Choose**, and select the Site-to-Site-PC-Pool object you created in the prerequisites section.

Step 10 Skip section 4, **Advanced**.

Step 11 For an FDM-managed device, in section 5, **Name**, give the NAT rule a name.

Step 12 Click **Save**.

Step 13 For an ASA, create a crypto map. See CLI Book 3: Cisco ASA Series VPN CLI Configuration Guide and review the chapter on LAN-to-LAN IPsec VPNs for more information on creating a crypto map.

Step 14 Preview and Deploy Configuration Changes for All Devices now the changes you made, or wait and deploy multiple changes at once.

Manage Virtual Private Network Management in CDO

A virtual private network (VPN) connection establishes a secure tunnel between endpoints over a public network such as the Internet.

This section applies to Remote Access and Site-to-site VPNs on FDM-managed device. It describes the Internet Protocol Security (IPsec) standards to build site-to-site VPNs connection on FTD. It also describes the SSL standards that are used to build and remote access VPN connections on FTD.

CDO supports the following types of VPN connections:

- Introduction to Site-to-Site Virtual Private Network, on page 190
- Introduction to Remote Access Virtual Private Network

For additional information about Virtual Private Networks, refer to the Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager.

Introduction to Site-to-Site Virtual Private Network

A site-to-site VPN tunnel 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 Internet Key Exchange version 2 (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.

VPN Topology

To create a new site-to-site VPN topology you must provide a unique name, specify a topology type, choose the IKE version that is used for IPsec IKEv1 or IKEv2, or both and authentication method. Once configured, you deploy the topology to FTD.

IPsec and IKE Protocols

In CDO, 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.

Authentication VPN Tunnels

For authentication of VPN connections, configure a pre-shared key in the topology on each device. Pre-shared keys allow a secret key, used during the IKE authentication phase, to be shared between two peers.

Virtual Tunnel Interface (VTI)

CDO does not currently support the management, monitoring, or use of Virtual Tunnel Interface (VTI) tunnels on FTD. Devices with configured VTI tunnels can be onboarded to CDO but it ignores the VTI interfaces. If a security zone or static route references a VTI, CDO reads the security zone and static route without the VTI reference.

About Extranet Devices

You can add non-Cisco or unmanaged Cisco devices to a VPN topology as "Extranet" devices with either static or dynamic IP addresses.

- Non-Cisco Device: You can’t use CDO to create and deploy configurations to non-Cisco devices.
- Unmanaged Cisco Device: Cisco device not managed by your organization, such as spokes in networks managed by other organizations within your company, or a connection to a service provider or partner's network.

Related Information:

- Configure Site-to-Site VPN for an FDM-Managed Device, on page 191
- Monitor FDM-Managed Device Site-to-Site Virtual Private Networks

Configure Site-to-Site VPN for an FDM-Managed Device

Cisco Defense Orchestrator (CDO) supports these aspects of site-to-site VPN functionality on FDM-managed devices:

- Both IPsec IKEv1 & IKEv2 protocols are supported.
- Automatic or manual pre-shared keys for authentication.
- IPv4 and IPv6. All combinations of inside and outside are supported.
- IPsec IKEv2 site-to-site VPN topologies provide configuration settings to comply with Security Certifications.

- Static and dynamic interfaces.
- Support for the dynamic IP address for the extranet device as an endpoint.

Configure Site-to-Site VPN Connections with Dynamicall Addressed Peers

CDO allows you to create a site-to-site VPN connection between peers when one of the peers' VPN interface IP address is not known or when the interface obtains its address from a DHCP server. Any dynamic peer whose preshared key, IKE settings, and IPsec configurations match with another peer can establish a site-to-site VPN connection.

Consider two peers, A and B. The static peer is a device whose IP address of its VPN interface is fixed and a dynamic peer is a device whose IP address of the VPN interface is not known or has a temporary IP address.

The following use cases describe different scenarios for establishing a secure site-to-site VPN connection with dynamically-addressed peers:

- A is a static peer, and B is a dynamic peer or conversely.
- A is a static peer, and B is a dynamic peer with a resolved IP address from the DHCP server or conversely. You can select **Bind VPN to the assigned IP** to establish the VPN connection between the IP address of the static peer and the DHCP assigned IP address of the dynamic peer.
- A and B are dynamic with resolved IP addresses from the DHCP server. In such a case, you must select **Bind VPN to the assigned IP** for at least one peer to establish the VPN connection between the IP address of the static peer and the DHCP assigned IP address of the dynamic peer.
- A is a dynamic peer, and B is an extranet device with a static or dynamic IP address.
- A is a dynamic peer with a resolved IP address from the DHCP server, and B is an Extranet device with a static or dynamic IP address. You can select **Bind VPN to the assigned IP** to establish the VPN connection between the IP address of the static peer and the DHCP assigned IP address of the dynamic peer.

Important If you select **Bind VPN to the assigned IP**, the VPN binds statically to the DHCP assigned IP address. However, this dynamic interface can receive many new IP addresses after the peer restarts. Although the VPN tunnel updates the new IP address, the other peer is not updated with the new configuration. You must deploy the site-to-site configuration again for out-of-band changes on the other peer.

Note If the IP address of the interface is changed by using a local manager like firewall device manager, the **Configuration Status** of that peer in CDO shows "Conflict Detected". When you Resolve Configuration Conflicts, the **Configuration Status** of the other peer changes to the "Not Synced" state. You must deploy the CDO configuration to the device which is in "Not Synced" state.

Typically, the dynamic peer must be the one that initiates the connection as the other peer would not know the IP address of the dynamic peer. When the remote peer attempts to establish the connection, the other peer validates the connection using the preshared key, IKE settings, and IPsec configurations.

Because the VPN connection is established only after the remote peer initiates the connection, any outbound traffic that matches access control rules that allow traffic in the VPN tunnel will be dropped until that connection

is established. This ensures that data does not leave your network without the appropriate encryption and VPN protection.

Note A site-to-site VPN connection cannot be configured in the following scenarios:

- If both peers have DHCP assigned IP addresses.
  - **Workaround**: You can configure a site-to-site VPN, if one of the peers has a resolved IP address from the DHCP server. In such a case, you must select **Bind VPN to the assigned IP** to configure site-to-site VPN.
- If a device has more than one dynamic peer connection.
  - **Workaround**: You can configure a site-to-site VPN by performing the following steps:
    - Consider three devices A, B, and C.
    - Configure site-to-site VPN connection between A (static peer) and B (dynamic peer).
    - Configure site-to-site VPN connection between A and C (dynamic peer) by creating an Extranet device. Assign the static VPN interface IP address of A to the Extranet device and establish a connection with C.

FDM-Managed Device Site-to-Site VPN Guidelines and Limitations

- CDO does not support a crypto-acl to design the interesting traffic for S2S VPN. It only supports protected networks.
- CDO does not currently support the management, monitoring, or use of Virtual Tunnel Interface (VTI) tunnels on ASA or FDM-managed devices. Devices with configured VTI tunnels can be onboarded to CDO but it ignores the VTI interfaces. If a security zone or static route references a VTI, CDO reads the security zone and static route without the VTI reference. CDO support for VTI tunnels is coming soon.
- Whenever IKE ports 500/4500 are in use or when there are some PAT translations that are active, the site-to-site VPN cannot be configured on the same ports as it fails to start the service on those ports.
- Transport mode is not supported only tunnel mode. IPsec tunnel mode encrypts the entire original IP datagram which becomes the payload in a new IP packet. Use tunnel mode when the firewall is protecting traffic to and from hosts positioned behind a firewall. Tunnel mode is the normal way regular IPsec is implemented between two firewalls (or other security gateways) that are connected over an untrusted network, such as the Internet.
- For this release, only PTP topology is supported, containing one or more VPN tunnels. Point-to-point (PTP) deployments establish a VPN tunnel between two endpoints.

Related Information:

- Create a Site-To-Site VPN
- Edit an Existing CDO Site-To-Site VPN
- Encryption and Hash Algorithms Used in VPN

- Exempt Site-to-Site VPN Traffic from NAT

Encryption and Hash Algorithms Used in VPN

Because a VPN tunnel typically traverses a public network, most likely the Internet, you need to encrypt the connection to protect the traffic. You define the encryption and other security techniques to apply using IKE policies and IPsec proposals.

If your device license allows you to apply strong encryption, there is a wide range of encryption and hash algorithms, and Diffie-Hellman groups, from which to choose. However, as a general rule, the stronger the encryption that you apply to the tunnel, the worse the system performance. Find a balance between security and performance that provides sufficient protection without compromising efficiency.

We cannot provide specific guidance on which options to choose. If you operate within a larger corporation or other organization, there might already be defined standards that you need to meet. If not, take the time to research the options.

The following topics explain the available options:

Deciding Which Encryption Algorithm to Use

When determining which encryption algorithms to use for the IKE policy or IPsec proposal, your choice is limited to algorithms supported by the devices in the VPN.

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 IKEv1, you can select a single option only.

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. In IKEv1 IPsec proposals, the algorithm name is prefixed with ESP.

If your device license qualifies for strong encryption, you can choose from the following encryption algorithms. If you are not qualified for strong encryption, you can select DES only.

- AES-GCM - (IKEv2 only.) Advanced Encryption Standard in Galois/Counter Mode is a block cipher mode of operation providing confidentiality and data-origin authentication and provides greater security than AES. AES-GCM offers three different key strengths: 128-, 192-, and 256-bit keys. A longer key provides higher security but a reduction in performance. GCM is a mode of AES that is required to support NSA Suite B. NSA Suite B is a set of cryptographic algorithms that devices must support to meet federal standards for cryptographic strength.
- AES-GMAC - (IKEv2 IPsec proposals only.) Advanced Encryption Standard Galois Message Authentication Code is a block cipher mode of operation providing only data-origin authentication. It is a variant of AES-GCM that allows data authentication without encrypting the data. AES-GMAC offers three different key strengths: 128-, 192-, and 256-bit keys.
- AES - Advanced Encryption Standard is a symmetric cipher algorithm that provides greater security than DES and is computationally more efficient than 3DES. AES offers three different key strengths: 128-, 192-, and 256-bit keys. A longer key provides higher security but a reduction in performance.
- DES - Data Encryption Standard, which encrypts using 56-bit keys, is a symmetric secret-key block algorithm. If your license account does not meet the requirements for export controls, this is your only option. It is faster than 3DES and uses fewer system resources, but it is also less secure. If you do not need strong data confidentiality, and if system resources or speed is a concern, choose DES.

- 3DES - Triple DES, which encrypts three times using 56-bit keys, is more secure than DES because it processes each block of data three times with a different key. However, it uses more system resources and is slower than DES.
- NULL - A null encryption algorithm provides authentication without encryption. This is typically used for testing purposes only.

Deciding Which Hash Algorithms to Use

In IKE policies, the hash algorithm creates a message digest, which is used to ensure message integrity. In IKEv2, the hash algorithm is separated into two options, one for the integrity algorithm, and one for the pseudo-random function (PRF).

In IPsec proposals, the hash algorithm is used by the Encapsulating Security Protocol (ESP) for authentication. In IKEv2 IPsec Proposals, this is called the integrity hash. In IKEv1 IPsec proposals, the algorithm name is prefixed with ESP-, and there is also an -HMAC suffix (which stands for "hash method authentication code").

For IKEv2, you can configure multiple hash algorithms. The system orders the settings from the most secure to the least secure and negotiates with the peer using that order. For IKEv1, you can select a single option only.

You can choose from the following hash algorithms:

- SHA (Secure Hash Algorithm) - Standard SHA (SHA-1) produces a 160-bit digest. SHA is more resistant to brute-force attacks than MD5. However, it is also more resource-intensive than MD5. For implementations that require the highest level of security, use the SHA hash algorithm.
- The following SHA-2 options, which are even more secure, are available for IKEv2 configurations. Choose one of these if you want to implement the NSA Suite B cryptography specification.
  - SHA-256 - Specifies the Secure Hash Algorithm SHA-2 with the 256-bit digest.
  - SHA-384 - Specifies the Secure Hash Algorithm SHA-2 with the 384-bit digest.
  - SHA-512 - Specifies the Secure Hash Algorithm SHA-2 with the 512-bit digest.
- MD5 (Message Digest 5) - Produces a 128-bit digest. MD5 uses less processing time for overall faster performance than SHA, but it is considered to be weaker than SHA.
- Null or None (NULL, ESP-NONE) - (IPsec Proposals only.) A null Hash Algorithm; this is typically used for testing purposes only. However, you should choose the null integrity algorithm if you select one of the AES-GCM/GMAC options as the encryption algorithm. Even if you choose a non-null option, the integrity hash is ignored for these encryption standards.

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 different size modules. A larger modulus provides higher security but requires more processing time. You must have a matching modulus group on both peers.

If you select AES encryption, to support the large key sizes required by AES, you should use Diffie-Hellman (DH) Group 5 or higher. IKEv1 policies do not support all of the groups listed below.

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.

For IKEv2, you can configure multiple groups. The system orders the settings from the most secure to the least secure and negotiates with the peer using that order. For IKEv1, you can select a single option only.

- 2 - Diffie-Hellman Group 2: 1024-bit modular exponential (MODP) group. This option is no longer considered good protection.
- 5 - Diffie-Hellman Group 5: 1536-bit MODP group. Formerly considered good protection for 128-bit keys, this option is no longer considered good protection.
- 14 - Diffie-Hellman Group 14: 2048-bit modular exponential (MODP) group. Considered good protection for 192-bit keys.
- 19 - Diffie-Hellman Group 19: National Institute of Standards and Technology (NIST) 256-bit elliptic curve modulo a prime (ECP) group.
- 20 - Diffie-Hellman Group 20: NIST 384-bit ECP group.
- 21 - Diffie-Hellman Group 21: NIST 521-bit ECP group.
- 24 - Diffie-Hellman Group 24: 2048-bit MODP group with 256-bit prime order subgroup. This option is no longer recommended.

Deciding Which Authentication Method to Use

You can use the following methods to authenticate the peers in a site-to-site VPN connection..

Preshared Keys

Preshared keys are secret key strings configured on each peer in the connection. These keys are used by IKE during the authentication phase. For IKEv1, you must configure the same preshared key on each peer. For IKEv2, you can configure unique keys on each peer.

Preshared keys do not scale well compared to certificates. If you need to configure a large number of site-to-site VPN connections, use the certificate method instead of the preshared key method.

Create a Site-To-Site VPN

You can create a site-to-site VPN by following one of the two methods: simple configuration and advanced configuration. In a simple configuration, the default configuration is used for establishing the site-to-site VPN connection. You can modify the configuration in the **Advanced** mode.

Each site-to-site VPN topology can include extranet devices that you do not manage in CDO. An Extranet device can be any device (Cisco or third-party), which is not managed by CDO.

For this release, only PTP topology is supported, containing one tunnel per site-to-site connection. Point-to-point (PTP) deployments establish a VPN tunnel between two endpoints.

Related information:

- Create a Site-To-Site VPN using the Simple Configuration, on page 197
- Create a Site-To-Site VPN using the Advanced Configuration, on page 197
- Configure Networking for Protected Traffic Between the Site-To-Site Peers, on page 199

Create a Site-To-Site VPN using the Simple Configuration

Procedure

Step 1 In the navigation pane, choose **VPN** > **Site-to-Site VPN**.

Step 2 Click the blue plus button to create a VPN Tunnel.

Note Alternatively, you can create the Site-to-Site VPN connection from the **Inventory** page.

a. On the navigation bar, click **Inventory**.

b. Select two FDM-managed devices that you want to configure. If you select an extranet device, specify the extranet device's IP address.

c. In the right-page, under **Device Actions,** click **Create Site-to-Site VPN**.

Step 3 Enter a unique topology **Configuration Name**. We recommend naming your topology to indicate that it is an FDM-managed device VPN, and its topology type.

Step 4 Choose the endpoint devices for this VPN deployment from Devices.

Step 5 If you choose an extranet device in **Peer 2**, select **Static,** and specify an IP address or select **Dynamic** for extranet devices with DHCP assigned IP. The **IP Address** displays the IP address for static interface or **DHCP Assigned** for the dynamic interface.

Step 6 Choose the **VPN Access Interface** for the for the endpoint devices.

Note If one or both endpoint devices have dynamic IP addresses, see Configure Site-to-Site VPN Connections with Dynamicall Addressed Peers for additional instructions.

Step 7 Click the blue plus button to add the **Protected Networks** for the participating devices.

Step 8 (Optional) Select **NAT Exempt** to exempt the VPN traffic from NAT policies on the local VPN access interface. It must be configured manually for individual peers. If you do not want NAT rules to apply to the local network, select the interface that hosts the local network. This option works only if the local network resides behind a single routed interface (not a bridge group member). If the local network is behind more than one routed interface or one or more bridge group members, you must manually create the NAT exempt rules. For information on manually creating the required rules, see Exempt Site-to-Site VPN Traffic from NAT .

Step 9 Click **Create VPN**, and then click **Finish**.

Step 10 Perform the additional mandatory configuration. See Configure Networking for Protected Traffic Between the Site-To-Site Peers.

The Site-To-Site VPN is configured.

Create a Site-To-Site VPN using the Advanced Configuration

Procedure

Step 1 On the navigation bar, choose **VPN**.

Step 2 Click the blue plus button to create a VPN Tunnel.

Step 3 In the **Peer Devices** section, specify the following device configurations:

a. Enter a unique topology **Configuration Name**. We recommend naming your topology to indicate that it is an FDM-managed devicee VPN, and its topology type.

b. Choose the endpoint devices for this VPN deployment from Devices.

c. If you choose an extranet device, select **Static** and specify an IP address or select **Dynamic** for extranet devices with DHCP assigned IP. The **IP Address** displays the IP address for static interface or **DHCP Assigned** for the dynamic interface.

d. Choose the **VPN Access Interface** for the endpoint devices.

Note If one or both endpoint devices have dynamic IP addresses, see Configure Site-to-Site VPN Connections with Dynamicall Addressed Peers for additional instructions.

Step 4 Click the blue plus button to add the **Protected Networks** for the participating devices.

Step 5 Click **Advanced**.

Step 6 In the **IKE Settings** section, choose the IKE versions to use during Internet Key Exchange (IKE) negotiations and specify the privacy configurations: For more information on the IKE policies, see the About Global IKE Policies.

Note IKE policies are global to a device and apply to all VPN tunnels associated with it. Therefore, adding or deleting policies affect all VPN tunnels in which this device is participating.

a. Select either or both options as appropriate.

Note By default, **IKEV Version 2** is enabled and the **IKEV2 POLICIES**.

b. Click the blue plus button and select the IKEv2 policies.

Click **Create New IKEv2 Policy** to create new IKEv2 policies. Alternatively, you can go to the CDO navigation bar and click **Objects > FDM Objects**, then click > **IKEv2 Policy**. For more information about creating new IKEv2 policies, see the Configuring IKEv2 Policies. To delete an existing IKEv2 Policy, hover-over the selected policy and click the **x** icon.

c. Click **IKE Version 1** to enable it.

d. Click the blue plus button and select the IKEv1 policies. Click **Create New IKEv1 Policy** to create new IKEv1 policies. Alternatively, you can go to the CDO navigation bar and click **Objects > FDM Objects** , then click **> IKEv1 Policy**. For more information about creating new IKEv1 policies, see the Configuring IKEv1 Policies. To delete an existing IKEv1 Policy, hover-over the selected policy and click the **x** icon.

e. Enter the **Pre-Shared Key** for the participating devices. Preshared keys are secret key strings configured on each peer in the connection. These keys are used by IKE during the authentication phase.

- (IKEv2) **Peer 1 Pre-shared Key**, **Peer 2 Pre-shared Key**: For IKEv2, you can configure unique keys on each peer. Enter the **Pre-shared Key**. You can click the **Show Override** button and enter

the appropriate pre-shared for the peer. The key can be 1-127, alphanumeric characters. The following table describes the purpose of the pre-shared key for both peers.

	Local Pre-shared Key	Remote Peer Pre-shared Key
Peer 1	Peer 1 Pre-shared Key	Peer 2 Pre-shared Key
Peer 2	Peer 2 Pre-shared Key	Peer 1 Pre-shared Key

- (IKEv1) **Pre-shared Key**: For IKEv1, you must configure the same preshared key on each peer. The key can be 1-127, alphanumeric characters. In this scenario, Peer 1 and Peer 2 use the same pre-shared key to encrypt and decrypt data.

f. Click **Next**.

Step 7 In the **IPSec Settings** section, specify the IPSec configurations. The corresponding IKEV proposals are available depending on the selection that is made in the **IKE Settings** step.

For more information on the IPSec settings, see the About IPsec Proposals.

a. Click the blue plus button and select the IKEv2 proposals. To delete an existing IKEv2 Proposal, hover-over the selected proposal and click the **x** icon.

Note Click Create New IKEv2 Proposal to create new IKEv2 proposals. Alternatively, you can go to the CDO navigation bar and click **Objects > FDM Objects**, then click > **IKEv2 IPSec Proposal**.

For more information about creating new IKEv2 policies, see the Configuring IPSec Proposals for IKEv2.

b. Choose the **Diffie-Hellman Group for Perfect Forward Secrecy**. For more information, see Deciding Which Diffie-Hellman Modulus Group to Use.

c. Click **Create VPN**.

d. Read the configuration and then click **Finish** if you're satisfied.

e. Perform the additional mandatory configuration. See Configure Networking for Protected Traffic Between the Site-To-Site Peers.

Configure Networking for Protected Traffic Between the Site-To-Site Peers

After completing the configuring of the Site-To-Site connection, make sure that you perform the following configuration for VPN to function on all targeted devices.

Procedure

Step 1 Configure AC policies:

Configure AC policies for permitting bidirectional traffic between the protected networks behind both peers. These policies help the packets to traverse to the intended destination without being dropped.

Note You must create AC policies for incoming and outgoing traffic on both peers.

a. In the Cisco Defense Orchestrator navigation bar at the left, click **Policies** and select the option that you want.

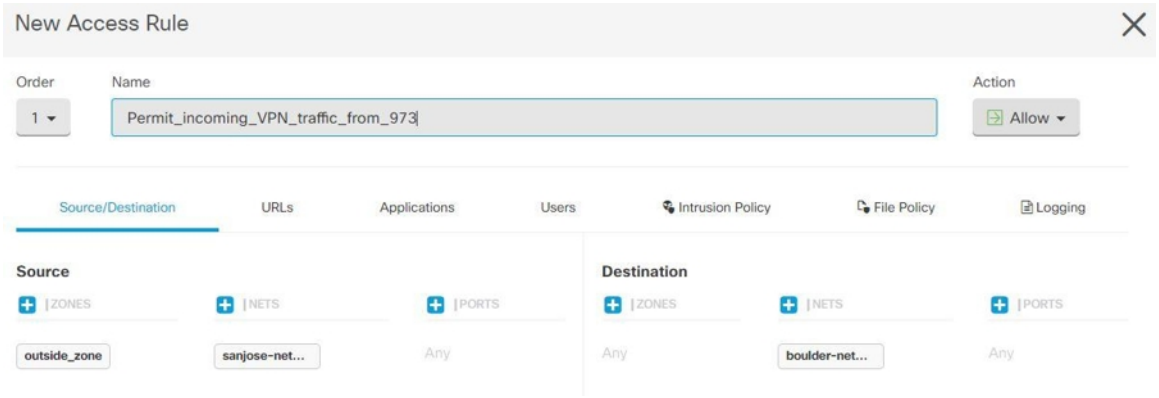
b. Create policies for incoming and outgoing traffic on both peers. For more information on AC policy creation, see Configure the FDM Access Control Policy.

The following example shows steps for creating AC policies on both peers.

Consider two FDM-managed devices 'FTD_BGL_972' and 'FTD_BGL_973' with Site-To-Site VPN connection between two protected networks 'boulder-network' and 'sanjose-network' respectively.

Creating the AC policy for permitting incoming traffic:

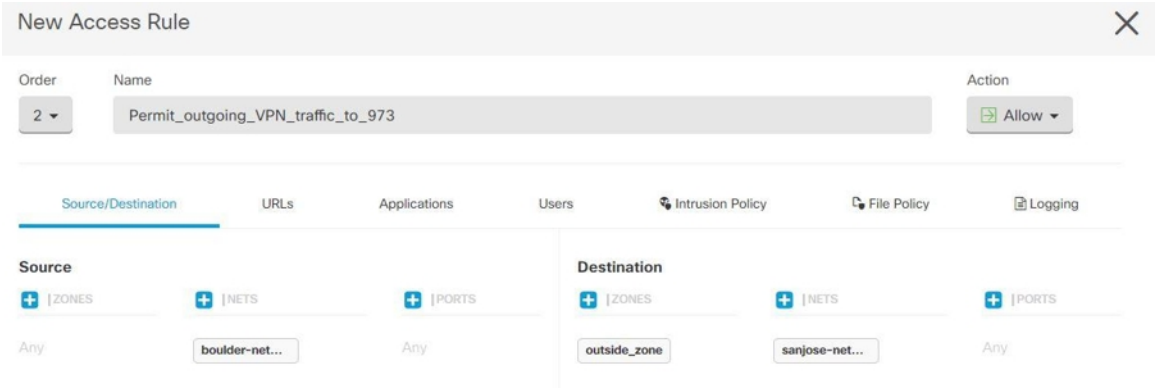
The policy 'Permit_incoming_VPN_traffic_from_973' is created on the 'FTD_BGL_972' device for allowing incoming traffic from the peer ('FTD_BGL_973').



- **Source Zone**: Set the zone of the peer device from which the network traffic originates. In this example, the traffic is originating from FTD_BGL_973 and reaching FTD_BGL_972.
- **Source Network**: Set the protected network of the peer device from which the network traffic originates. In this example, traffic is originating from 'sanjose-network' which is the protected network behind the peer device (FTD_BGL_973).
- **Destination Network**: Set the protected network of the device on which the network traffic arrives. In this example, traffic is arriving at 'boulder-network' which is the protected network behind the peer device (FTD_BGL_972). **Note**: The remaining fields can have the default value ("Any").
- Set **Action** to **Allow** for allowing the traffic subject to the intrusion and other inspection settings in the policy.

Creating the AC policy for permitting outgoing traffic:

The policy 'Permit_outgoing_VPN_traffic_to_973' is created on the 'FTD_BGL_972' device for permitting outgoing traffic to the peer ('FTD_BGL_973').



- **Source Network**: Set the protected network of the peer device from which the network traffic originates. In this example, traffic is originating from 'boulder-network' which is the protected network behind the peer device (FTD_BGL_972).
- **Destination Zone**: Set the zone of the peer device on which the network traffic arrives. In this example, the traffic is arriving from FTD_BGL_972 and reaching FTD_BGL_973.
- **Destination Network**: Set the protected network of the peer on which the network traffic arrives. In this example, traffic is arriving on 'sanjose-network' which is the protected network behind the peer device (FTD_BGL_972). **Note**: The remaining fields can have the default value ("Any").
- Set **Action** to **Allow** for allowing the traffic subject to the intrusion and other inspection settings in the policy.

After creating AC policies on one device, you must create similar policies on its peer.

Step 2 If NAT is configured on either of the peer devices, you need to configure the NAT exempt rules manually. See Exempt Site-to-Site VPN Traffic from NAT .

Step 3 Configure routing for receiving the return VPN traffic on each peer. For more information, see Configure Static and Default Routes for FDM-Managed Devices.

a. **Gateway**-Select the network object that identifies the IP address for the gateway to the destination network. Traffic is sent to this address.

b. **Interface**-Select the interface through which you want to send traffic. In this example, the traffic is sent through 'outside' interface.

c. **Destination Networks**-Select one or network objects, that identify the destination network. In this example, the destination is 'sanjose-network' which is behind peer (FTD_BGL_973).

After configuring routing settings on one device, you must configure similar settings on its peer.

Edit an Existing CDO Site-To-Site VPN

The advanced configuration wizard is used by default to modify an existing site-to-site VPN configuration.

Procedure

Step 1 On the navigation bar, choose **VPN** > **Site-to-Site VPN**.

Step 2 Select the desired site-to-site VPN tunnel that you want to edit.

Step 3 In the **Actions** pane, click **Edit**.

Note Alternatively, you can perform the following to edit the configuration:

a. Open the VPN page and click **Global View** button in the filter panel (for more information, see Search and Filter Site-to-Site VPN Tunnels).

The illustration of all site-to-site VPN tunnels available across all devices appears.

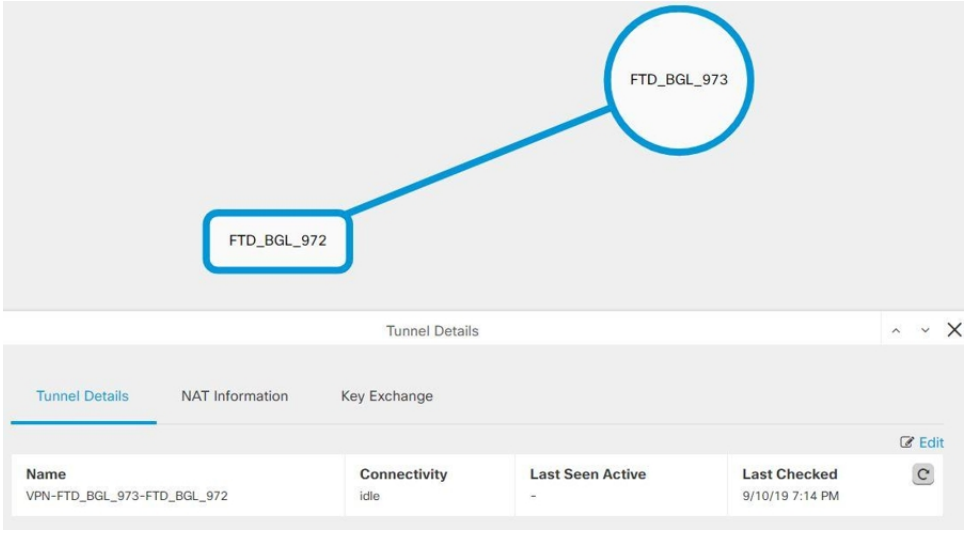
To edit the configuration, one of the peers must be FDM-managed device.

b. Select a device by clicking the box.

c. Click **View details** to view its peers.

d. Click the peer device to view the tunnel details.

You can view the tunnel details, NAT information, and key exchange information pertaining to the device.



e. Click **Edit** in **Tunnel Details**.

Step 4 In the **Peer Devices** section, you can modify the following device configurations: Configuration Name, VPN Access Interface, and Protected Networks.

Note You cannot change the participating devices.

Step 5 In the **IKE Settings** section, you can modify the following IKEv2 policies configurations:

a. Click the blue plus button for the respective device and select new IKEv2 policies. To delete an existing IKEv2 Policy, hover-over the selected policy and click the **x** icon.

b. Modify the **Pre-Shared Key** for the participating devices. If the pre-shared keys are different for endpoint devices, click the blue settings button and enter the appropriate pre-shared keys for the devices.

c. Click **Next**.

Step 6 In the **IPSec Settings** section, you can modify the following IPSec configurations:

a. Click the blue plus button to select new IKEv2 proposals. To delete an existing IKEv2 Proposal, hover-over the selected proposal and click the **x** icon.

b. Choose the **Diffie-Hellman Group for Perfect Forward Secrecy**.

c. Click **Edit VPN**, and then **Finish**.

The Point to point VPN is modified and updated with all the changes you have made.

Delete a CDO Site-To-Site VPN Tunnel

Procedure

Step 1 On the navigation bar, choose **VPN**> **ASA/FDM Site-to-Site VPN**.

Step 2 Select the desired site-to-site VPN tunnel that you want to delete.

Step 3 In the **Actions** pane, click **Delete**.

The selected site-to-site VPN tunnel is deleted.

Exempt Site-to-Site VPN Traffic from NAT

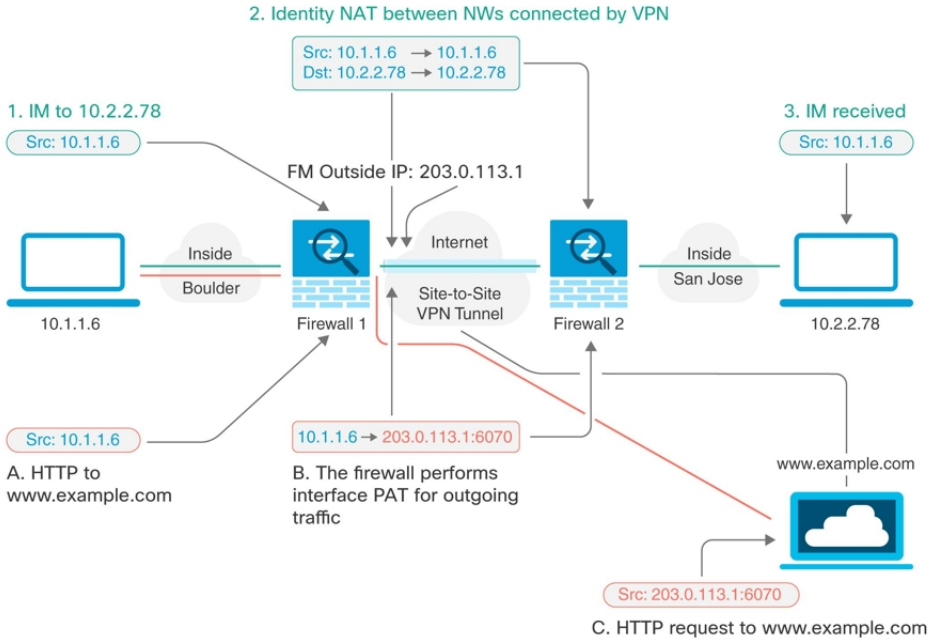
When you have a site-to-site VPN connection defined on an interface, and you also have NAT rules for that interface, you can optionally exempt the traffic on the VPN from the NAT rules. You might want to do this if the remote end of the VPN connection can handle your internal addresses.

When you create the VPN connection, you can select the **NAT Exempt** option to create the rules automatically. However, this works only if your local protected network is connected through a single routed interface (not a bridge group member). If instead, the local networks in the connection reside behind two or more routed interfaces or one or more bridge group members, you need to configure the NAT exempt rules manually.

To exempt VPN traffic from NAT rules, you create an identity manual NAT rule for the local traffic when the destination is the remote network. Then, apply NAT to the traffic when the destination is anything else (for example, the Internet). If you have more than one interface for the local network, create rules for each interface. Also, consider the following suggestions:

- If there is more than one local network in the connection, create a network object group to hold the objects that define the networks.
- If you are including both IPv4 and IPv6 networks in the VPN, create separate identity NAT rules for each.

Consider the following example, which shows a site-to-site tunnel connecting the Boulder and San Jose offices. For traffic that you want to go to the Internet (for example from 10.1.1.6 in Boulder to www.example.com), you need a public IP address provided by NAT to access the Internet. The below example uses interface Port Address Translation (PAT) rules. However, for traffic that you want to go over the VPN tunnel (for example from 10.1.1.6 in Boulder to 10.2.2.78 in San Jose), you do not want to perform NAT; you need to exempt that traffic by creating an identity NAT rule. Identity NAT translates an address to the same address.



The following example explains the configuration for Firewall1 (Boulder). The example assumes that the inside interface is a bridge group, so you need to write the rules for each member interface. The process is the same if you have a single or multiple routed inside interfaces.

Note This example assumes IPv4 only. If the VPN also includes IPv6 networks, create parallel rules for IPv6. Note that you cannot implement IPv6 interface PAT, so you need to create a host object with a unique IPv6 address to use for PAT.

Procedure

Step 1 Create objects to define the various networks.

a. In the CDO navigation bar at the left, click **Objects > FDM Objects**.

b. Click the blue plus button to create an object.

c. Click **FTD** > **Network**.

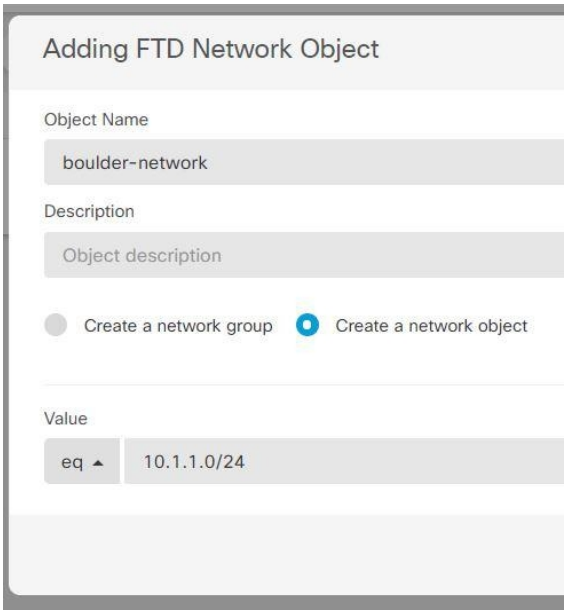
d. Identify the Boulder inside network.

e. Enter an object name (for example, boulder-network).

f. Select **Create a network object**.

g. In the Value section:

- Select **eq** and enter a single IP address or a subnet address expressed in CIDR notation.
- Select **range** and enter an IP address range. For example, enter the network address as 10.1.1.0/24.



h. Click **Add**.

i. Click the blue plus button to create an object.

j. Define the inside San Jose network.

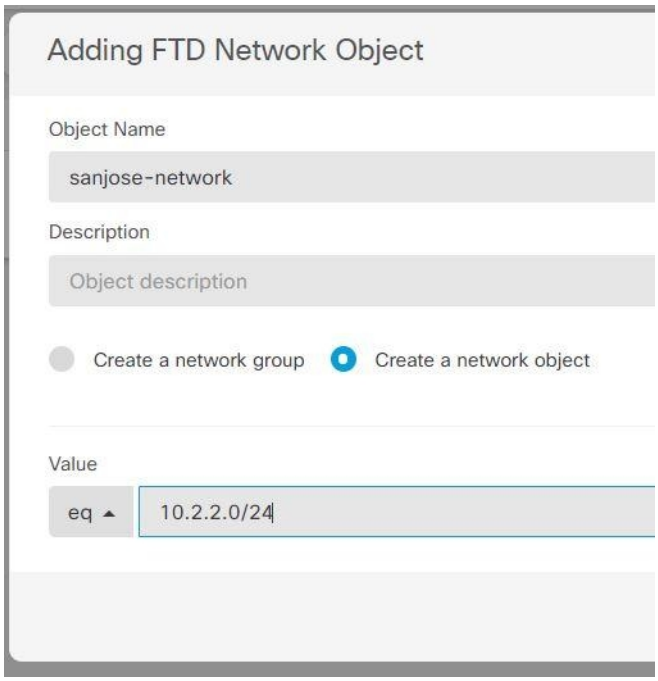
k. Enter the object name (for example, san-jose).

l. Select **Create a network object**.

m. In the Value section:

- Select **eq** and enter a single IP address or a subnet address expressed in CIDR notation.

- Select **range** and enter an IP address range. For example, enter the network address as 10.1.1.0/24.



n. Click **Add**.

Step 2 Configure manual identity NAT for the Boulder network when going over the VPN to San Jose on Firewall1 (Boulder).

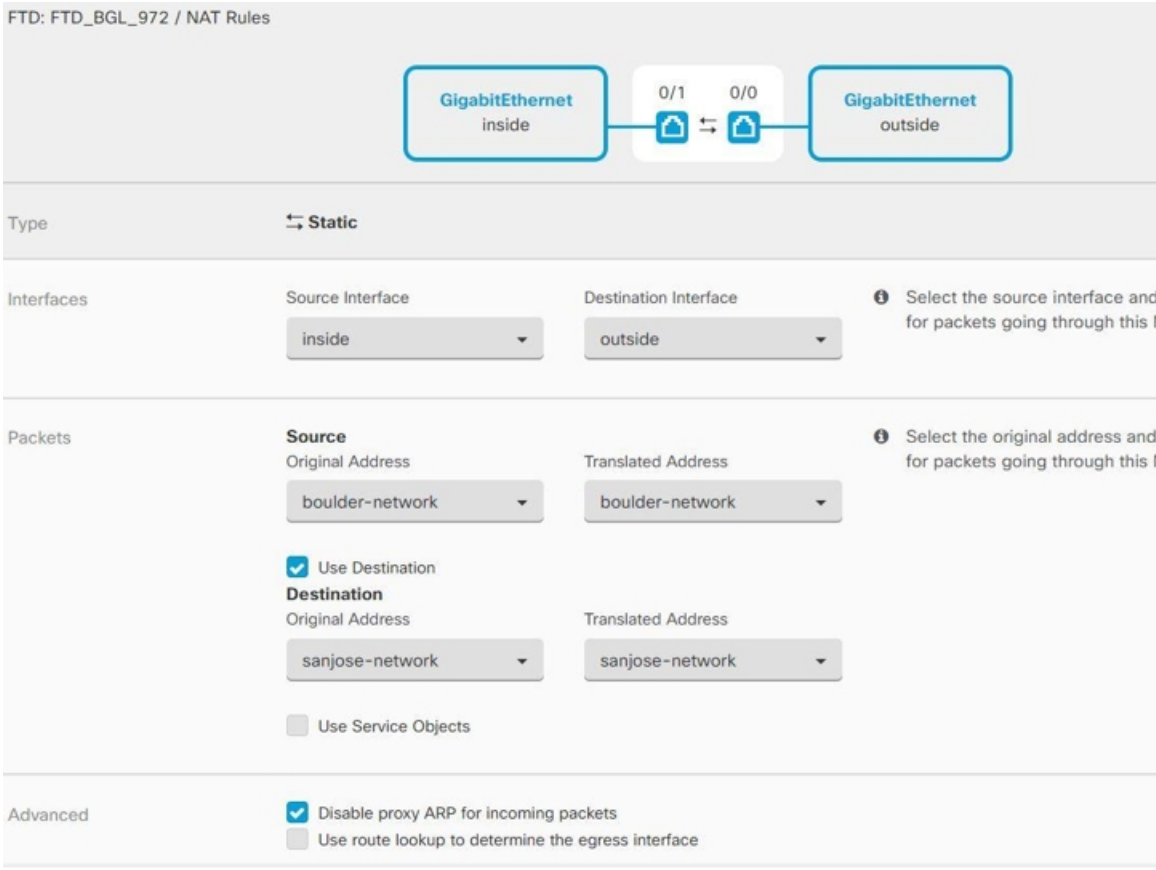
a. In the CDO navigation bar, click **Inventory**.

b. Use the filter to find the device for which you want to create the NAT rule.

c. In the Management area of the details panel, click **NAT** NAT.

d. Click + > **Twice NAT**.

- In section 1, select **Static.** Click **Continue**.
- In section 2, select **Source Interface** = **inside** and **Destination Interface** = **outside.** Click **Continue**.
- In section 3, select **Source Original Address** = 'boulder-network' and **Source Translated Address** = 'boulder-network'.
- Select **Use Destination**.
- Select **Destination Original Address** = 'sanjose-network' and **Source Translated Address** = 'sanjose-network'. **Note**: Because you do not want to translate the destination address, you need to configure identity NAT for it by specifying the same address for the original and translated destination addresses. Leave all of the port fields blank. This rule configures identity NAT for both source and destination.



- Select **Disable proxy ARP for incoming packets**.
- Click **Save**.
- Repeat the process to create equivalent rules for each of the other inside interfaces.

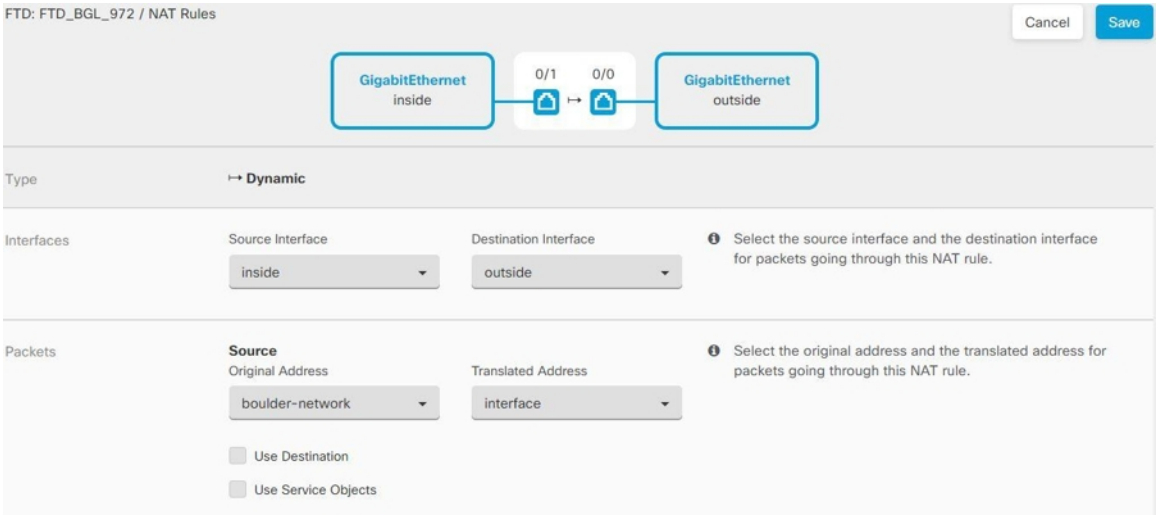
Step 3 Configure manual dynamic interface PAT when going to the Internet for the inside Boulder network on Firewall1 (Boulder). **Note**: There might already be dynamic interface PAT rules for the inside interfaces, covering any IPv4 traffic, as these are created by default during initial configuration. However, the configuration is shown here for completeness. Before completing these steps, check whether a rule already exists that covers the inside interface and network, and skip this step if it does.

a. Click + > **Twice NAT**.

b. In section 1, select **Dynamic.** Click **Continue**.

c. In section 2, select **Source Interface** = **inside** and **Destination Interface** = **outside.** Click **Continue**.

d. In section 3, select **Source Original Address** = 'boulder-network' and **Source Translated Address** = 'interface'.



e. Click **Save**.

f. Repeat the process to create equivalent rules for each of the other inside interfaces.

Step 4 Deploy configuration changes to CDO. For more information, see Deploy Configuration Changes from CDO to FDM-Managed Device.

Step 5 If you are also managing Firewall2 (San Jose), you can configure similar rules for that device.

- The manual identity NAT rule would be for 'sanjose-network' when the destination is boulder-network. Create new interface objects for the Firewall2 inside and outside networks.
- The manual dynamic interface PAT rule would be for 'sanjose-network' when the destination is "any."

About Global IKE Policies

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

The IKE negotiation comprises two phases. Phase 1 negotiates a security association between two IKE peers, which enables the peers to communicate securely in Phase 2. During Phase 2 negotiation, IKE establishes SAs for other applications, such as IPsec. Both phases use proposals when they negotiate a connection. An IKE proposal is a set of algorithms that two peers use to secure the negotiation between them. IKE negotiation begins by each peer agreeing on a common (shared) IKE policy. This policy states which security parameters are used to protect subsequent IKE negotiations.

IKE policy objects define the IKE proposals for these negotiations. The objects that you enable are the ones used when the peers negotiate a VPN connection: you cannot specify different IKE policies per connection. The relative priority of each object determines which of these policies are tried first, with the lower number being a higher priority. The connection is not established if the negotiation fails to find a policy that both peers can support.

To define the global IKE policy, you select which objects to enable for each IKE version. If the pre-defined objects do not satisfy your requirements, create new policies to enforce your security policy.

The following procedure explains how to configure the global policy through the Objects page. You can also enable, disable, and create policies when editing a VPN connection by clicking Edit for the IKE Policy settings.

The following topics explain how to configure IKE policies for each version:

- Configuring IKEv1 Policies
- Configuring IKEv2 Policies

Managing IKEv1 Policies

About IKEv1 Policy

Internet Key Exchange (IKE) version 1 policy objects contain the parameters required for IKEv1 policies when defining VPN connections. IKE is a key management protocol that facilitates the management of IPsec-based communications. It is used to authenticate IPsec peers, negotiate and distribute IPsec encryption keys, and automatically establish IPsec security associations (SAs).

There are several pre-defined IKEv1 policies. If any suit your needs, simply enable them by clicking the State toggle. You can also create new policies to implement other combinations of security settings. You cannot edit or delete system-defined objects.

Related Topics

Create an IKEv1 Policy, on page 209

Create an IKEv1 Policy

Internet Key Exchange (IKE) version 1 policy objects contain the parameters required for IKEv1 policies when defining VPN connections. IKE is a key management protocol that facilitates the management of IPsec-based communications. It is used to authenticate IPsec peers, negotiate and distribute IPsec encryption keys, and automatically establish IPsec security associations (SAs).

There are several pre-defined IKEv1 policies. If any suit your needs, simply enable them by clicking the State toggle. You can also create new policies to implement other combinations of security settings. You cannot edit or delete system-defined objects.

The following procedure explains how you can create and edit objects directly through the Objects page. You can also create an IKEv1 policy while editing the IKE settings in a Site-to-Site VPN connection by clicking the **Create New IKEv1 Policy** link shown in the object list.

Procedure

Step 1 In the CDO navigation bar on the left, click **Objects > FDM Objects**.

Step 2 Do one of these things:

- Click the blue plus button  and select **FDM** > **IKEv1 Policy** to create a new IKEv1 policy.
- In the object page, select the IKEv1 policy you want to edit and click **Edit** in the Actions pane at the right.

Step 3 Enter an **object name**, up to 128 characters.

Step 4 Configure the IKEv1 properties.

- **Priority** - The relative priority of the IKE policy, from 1 to 65,535. The priority determines the order of the IKE policy 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 highest priority policy, it tries to use the parameters defined in the next lowest priority. The lower the number, the higher the priority.
- **Encryption** - The encryption algorithm used to establish the Phase 1 security association (SA) for protecting Phase 2 negotiations. For an explanation of the options, see Deciding Which Encryption Algorithm to Use.
- **Diffie-Hellman Group** - The Diffie-Hellman group to use for deriving a shared secret between the two IPsec peers without transmitting it to each other. A larger modulus provides higher security but requires more processing time. The two peers must have a matching modulus group. For an explanation of the options, see Deciding Which Diffie-Hellman Modulus Group to Use.
- **Lifetime** - The lifetime of the security association (SA), in seconds, from 120 to 2147483647 or blank. 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 set up more quickly than with shorter lifetimes. The default is 86400. To specify an unlimited lifetime, enter no value (leave the field blank).
- **Authentication** - The method of authentication to use between the two peers. For more information, see Deciding Which Authentication Method to Use.
  - **Preshared Key** - Use the preshared key that is defined on each device. These keys allow for a secret key to be shared between two peers and to be used by IKE during the authentication phase. If the peer is not configured with the same preshared key, the IKE SA cannot be established.
  - **Certificate** - Use the device identity certificates for the peers to identify each other. You must obtain these certificates by enrolling each peer in a Certificate Authority. You must also upload the trusted CA root and intermediate CA certificates used to sign the identity certificates in each peer. The peers can be enrolled in the same or a different CA. You cannot use self-signed certificates for either peer.
- **Hash** - The hash algorithm for creating a message digest, which is used to ensure message integrity. For an explanation of the options, see Deciding Which Diffie-Hellman Modulus Group to Use.

Step 5 Click **Add**.

Managing IKEv2 Policies

About IKEv2 Policy

Internet Key Exchange (IKE) version 2 policy objects contain the parameters required for IKEv2 policies when defining VPN connections. IKE is a key management protocol that facilitates the management of IPsec-based communications. It is used to authenticate IPsec peers, negotiate and distribute IPsec encryption keys, and automatically establish IPsec security associations (SAs).

There are several pre-defined IKEv2 policies. If any suit your needs, simply enable them by clicking the State toggle. You can also create new policies to implement other combinations of security settings. You cannot edit or delete system-defined objects.

Related Topics

Create an IKEv2 Policy, on page 211

Create an IKEv2 Policy

Internet Key Exchange (IKE) version 2 policy objects contain the parameters required for IKEv2 policies when defining VPN connections. IKE is a key management protocol that facilitates the management of IPsec-based communications. It is used to authenticate IPsec peers, negotiate and distribute IPsec encryption keys, and automatically establish IPsec security associations (SAs).

There are several pre-defined IKEv2 policies. If any suit your needs, simply enable them by clicking the State toggle. You can also create new policies to implement other combinations of security settings. You cannot edit or delete system-defined objects.

The following procedure explains how you can create and edit objects directly through the Objects page. You can also create an IKEv2 policy while editing the IKE settings in a Site-to-Site VPN connection by clicking the **Create New IKEv2 Policy** link shown in the object list.

Procedure

Step 1 In the CDO navigation bar on the left, click **Objects > FDM Objects**.

Step 2 Do one of these things:

- Click the blue plus button  and select **FDM** > **IKEv2 Policy** to create a new IKEv2 policy.
- In the object page, select the IKEv2 policy you want to edit and click **Edit** in the Actions pane at the right.

Step 3 Enter an **object name**, up to 128 characters.

Step 4 Configure the IKEv2 properties.

- **Priority** - The relative priority of the IKE policy, from 1 to 65,535. The priority determines the order of the IKE policy 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 highest priority policy, it tries to use the parameters defined in the next lowest priority. The lower the number, the higher the priority.
- **State** - Whether the IKE policy is enabled or disabled. Click the toggle to change the state. Only enabled policies are used during IKE negotiations.
- **Encryption** - The encryption algorithm used to establish the Phase 1 security association (SA) for protecting Phase 2 negotiations. Select all algorithms that you want to allow, although you cannot include both mixed-mode (AES-GCM) and normal mode options in the same policy. (Normal mode requires that you select an integrity hash, whereas mixed-mode prohibits a separate integrity hash selection.) The system negotiates with the peer, starting from the strongest to the weakest algorithm until a match is agreed upon. For an explanation of the options, see Deciding Which Encryption Algorithm to Use.
- **Diffie-Hellman Group** - The Diffie-Hellman group to use for deriving a shared secret between the two IPsec peers without transmitting it to each other. A larger modulus provides higher security but requires

more processing time. The two peers must have a matching modulus group. Select all the algorithms that you want to allow. The system negotiates with the peer, starting from the strongest to the weakest group until a match is agreed upon. For an explanation of the options, see Deciding Which Diffie-Hellman Modulus Group to Use.

- **Integrity Hash** - The integrity portion of the hash algorithm for creating a message digest, which is used to ensure message integrity. Select all the algorithms that you want to allow. The system negotiates with the peer, starting from the strongest to the weakest algorithm until a match is agreed upon. The integrity hash is not used with the AES-GCM encryption options. For an explanation of the options, see Deciding Which Hash Algorithms to Use.
- **Pseudo-Random Function (PRF) Hash** - The pseudo-random function (PRF) portion of the hash algorithm, which is used as the algorithm to derive keying material and hashing operations required for the IKEv2 tunnel encryption. In IKEv1, the Integrity and PRF algorithms are not separated, but in IKEv2, you can specify different algorithms for these elements. Select all the algorithms that you want to allow. The system negotiates with the peer, starting from the strongest to the weakest algorithm until a match is agreed upon. For an explanation of the options, see Deciding Which Hash Algorithms to Use.
- **Lifetime** - The lifetime of the security association (SA), in seconds, from 120 to 2147483647 or blank. 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 set up more quickly than with shorter lifetimes. The default is 86400. To specify an unlimited lifetime, enter no value (leave the field blank).

Step 5 Click **Add**.

About IPsec Proposals

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 called a transform set. During the IPsec security association (SA) negotiation, peers search for a transform set that is the same at both peers.

There are separate IPsec proposal objects based on the IKE version, IKEv1, or IKEv2:

- When you create an IKEv1 IPsec proposal, you select the mode in which IPsec operates, and define the required encryption and authentication types. You can select single options for the algorithms. If you want to support multiple combinations in a VPN, create and select multiple IKEv1 IPsec Proposal objects.
- When you create an IKEv2 IPsec proposal, you can select all of the encryption and hash algorithms allowed in a VPN. The system orders the settings from the most secure to the least secure and negotiates with the peer until a match is found. This allows you to potentially send a single proposal to convey all the allowed combinations instead of the need to send each allowed combination individually as with IKEv1.

The Encapsulating Security Protocol (ESP) is used for both IKEv1 and IKEv2 IPsec proposals. It provides authentication, encryption, and antireplay services. ESP is IP protocol type 50.

Note We recommend using both encryption and authentication on IPsec tunnels.

The following topics explain how to configure IPsec proposals for each IKE version:

- Create and Edit IKEv1 IPsec Proposal Object
- Create and Edit IKEv2 IPsec Proposal Object

Managing an IKEv1 IPsec Proposal Object

IPsec Proposal objects configure the IPsec proposal used during IKE Phase 2 negotiations. The IPsec proposal defines the combination of security protocols and algorithms that secure traffic in an IPsec tunnel. There are separate objects for IKEv1 and IKEv2. Currently, Cisco Defense Orchestrator (CDO) supports IKEv1 IPsec proposal objects.

The Encapsulating Security Protocol (ESP) is used for both IKEv1 and IKEv2 IPsec proposals. It provides authentication, encryption, and anti-replay services. ESP is IP protocol type 50.

Note We recommend using both encryption and authentication on IPsec tunnels.

Related Topics

Create an IKEv1 IPsec Proposal Object, on page 213

Create an IKEv1 IPsec Proposal Object

IPsec Proposal objects configure the IPsec proposal used during IKE Phase 2 negotiations. The IPsec proposal defines the combination of security protocols and algorithms that secure traffic in an IPsec tunnel. There are separate objects for IKEv1 and IKEv2. Currently, Cisco Defense Orchestrator (CDO) supports IKEv1 IPsec proposal objects.

The Encapsulating Security Protocol (ESP) is used for both IKEv1 and IKEv2 IPsec proposals. It provides authentication, encryption, and anti-replay services. ESP is IP protocol type 50.

Note We recommend using both encryption and authentication on IPsec tunnels.

There are several pre-defined IKEv1 IPsec proposals. You can also create new proposals to implement other combinations of security settings. You cannot edit or delete system-defined objects.

The following procedure explains how you can create and edit objects directly through the Objects page. You can also create IKEv1 IPsec Proposals objects while editing the IKEv1 IPsec settings in a Site-to-Site VPN connection by clicking the **Create New IKEv1 Proposal** link shown in the object list.

Procedure

Step 1 In the CDO navigation bar on the left, click **Objects > FDM Objects**.

Step 2 Do one of these things:

- Click the blue plus button  and select **FDM** > **IKEv1 IPsec Proposal** to create the new object.
- In the object page, select the IPsec proposal you want to edit and click **Edit** in the Actions pane at the right.

Step 3 Enter an **object name** for the new object.

Step 4 Select the Mode in which the IKEv1 IPsec Proposal object operates.

- **Tunnel mode** encapsulates the entire IP packet. The IPSec header is added between the original IP header and a new IP header. This is the default. Use tunnel mode when the firewall is protecting traffic to and from hosts positioned behind the firewall. Tunnel mode is the normal way regular IPSec is implemented between two firewalls (or other security gateways) that are connected over an untrusted network, such as the Internet.
- **Transport mode** encapsulates only the upper-layer protocols of an IP packet. The IPSec header is inserted between the IP header and the upper-layer protocol header (such as TCP). Transport mode requires that both the source and destination hosts support IPSec, and can only be used when the destination peer of the tunnel is the final destination of the IP packet. Transport mode is generally used only when protecting a Layer 2 or Layer 3 tunneling protocol such as GRE, L2TP, and DLSW.

Step 5 Select the **ESP Encryption** (Encapsulating Security Protocol encryption) algorithm for this proposal. For an explanation of the options, see Deciding Which Encryption Algorithm to Use.

Step 6 Select the **ESP Hash** or integrity algorithm to use for authentication. For an explanation of the options, see Deciding Which Hash Algorithms to Use.

Step 7 Click **Add**.

Managing an IKEv2 IPsec Proposal Object

IPsec Proposal objects configure the IPsec proposal used during IKE Phase 2 negotiations. The IPsec proposal defines the combination of security protocols and algorithms that secure traffic in an IPsec tunnel.

When you create an IKEv2 IPsec proposal, you can select all of the encryption and hash algorithms allowed in a VPN. The system orders the settings from the most secure to the least secure and negotiates with the peer until a match is found. This allows you to potentially send a single proposal to convey all the allowed combinations instead of the need to send each allowed combination individually as with IKEv1.

Related Topics

Create or Edit an IKEv2 IPsec Proposal Object, on page 214

Create or Edit an IKEv2 IPsec Proposal Object

There are several pre-defined IKEv2 IPsec proposals. You can also create new proposals to implement other combinations of security settings. You cannot edit or delete system-defined objects.

The following procedure explains how you can create and edit objects directly through the Objects page. You can also create IKEv2 IPsec Proposals objects while editing the IKEv2 IPsec settings in a VPN connection by clicking the Create New IPsec Proposal link shown in the object list.

Procedure

Step 1 In the CDO navigation bar on the left, click **Objects** > **FDM Objects**.

Step 2 Do one of these things:

- Click the blue plus button  and select **FDM** > **IKEv2 IPsec Proposal** to create the new object.
- In the object page, select the IPsec proposal you want to edit and click **Edit** in the Actions pane at the right.

Step 3 Enter an **object name** for the new object.

Step 4 Configure the IKE2 IPsec proposal objects:

- **Encryption** - The Encapsulating Security Protocol (ESP) encryption algorithm for this proposal. Select all the algorithms that you want to allow. The system negotiates with the peer, starting from the strongest to the weakest algorithm until a match is agreed upon. For an explanation of the options, see Deciding Which Encryption Algorithm to Use.
- **Integrity Hash** - The hash or integrity algorithm to use for authentication. Select all the algorithms that you want to allow. The system negotiates with the peer, starting from the strongest to the weakest algorithm until a match is agreed upon. For an explanation of the options, see Deciding Which Hash Algorithms to Use.

Step 5 Click **Add**.

Monitor FDM-Managed Device Site-to-Site Virtual Private Networks

CDO allows you to monitor, modify, and delete existing or newly created site-to-site VPN configurations on onboarded FDM-managed devices.

Check Site-to-Site VPN Tunnel Connectivity

Use the **Check Connectivity** button to trigger a real-time connectivity check against the tunnel to identify whether the tunnel is currently Search and Filter Site-to-Site VPN Tunnels. Unless you click the on-demand connectivity check button, a check across all tunnels, available across all onboarded devices, occurs once an hour.

Note

- CDO runs this connectivity check command on the FTD to determine if a tunnel is active or idle:

  ```
  show vpn-sessiondb l2l sort ipaddress
  ```

- Model ASA device(s) tunnels will always show as **Idle**.

To check tunnel connectivity from the VPN page:

Procedure

Step 1 From the main navigation bar, click VPN > ASA/FDM Site-to-Site VPN.

Step 2 Search and Filter Site-to-Site VPN Tunnels the list of tunnels for your site-to-site VPN tunnel and select it.

Step 3 In the Actions pane at the right, click **Check Connectivity**.

Identify VPN Issues

CDO can identify VPN issues on FTD. (This feature is not yet available for AWS VPC site-to-site VPN tunnels.) This article describes:

- Find VPN Tunnels with Missing Peers
- Find VPN Peers with Encryption Key Issues
- Find Incomplete or Misconfigured Access Lists Defined for a Tunnel
- Find Issues in Tunnel Configuration

Resolve Tunnel Configuration Issues, on page 218

Find VPN Tunnels with Missing Peers

The "Missing IP Peer" condition is more likely to occur on ASA devices than FDM-managed devices.

Procedure

Step 1 In the CDO navigation pane, click **VPN** > **ASA/FDM Site-to-Site VPN** to open the VPN page.

Step 2 Select **Table View**.

Step 3 Open the Filter panel by clicking the filter icon .

Step 4 Check **Detected Issues**.

Step 5 Select each device reporting an issue and look in the Peers pane at the right. One peer name will be listed. CDO reports the other peer name as, "[Missing peer IP.]"

Find VPN Peers with Encryption Key Issues

Use this approach to locate VPN Peers with encryption key issues such as:

- IKEv1 or IKEv2 keys are invalid, missing, or mismatched
- Obsolete or low encryption tunnels

Procedure

Step 1 In the CDO navigation bar, click **VPN** > **ASA/FDM Site-to-Site VPN** to open the VPN page.

Step 2 Select **Table View**.

Step 3 Open the Filter panel by clicking the filter icon.

Step 4 Select each device reporting an issue and look in the Peers pane at the right. The peer information will show you both peers.

Step 5 Click on **View Peers** for one of the devices.

Step 6 Double-click the device reporting the issue in the Diagram View.

Step 7 Click **Key Exchange** in the Tunnel Details panel at the bottom. You will be able to view both devices and diagnose the key issue from that point.

Find Incomplete or Misconfigured Access Lists Defined for a Tunnel

The "incomplete or misconfigured access-list" condition could only occur on ASA devices.

Procedure

Step 1 In the CDO navigation bar, click **VPN** > **ASA/FDM Site-to-Site VPN** to open the VPN page.

Step 2 Select **Table View**.

Step 3 Open the Filter panel by clicking the filter icon.

Step 4 Select each device reporting an issue and look in the Peers pane at the right. The peer information shows you both peers.

Step 5 Click on **View Peers** for one of the devices.

Step 6 Double-click the device reporting the issue in the Diagram View.

Step 7 Click **Tunnel Details** in the Tunnel Details panel at the bottom. You will see the message, "Network Policy: Incomplete"

Find Issues in Tunnel Configuration

The tunnel configuration error can occur in the following scenarios:

- When the IP address of a site-to-site VPN interface changes, the "Peer IP Address Value has changed".
- When the IKE value of a VPN tunnel doesn't match the other VPN tunnel, the "IKE value Mismatch" message appears.

Procedure

Step 1 In the CDO navigation bar, click **VPN** > **ASA/FDM Site-to-Site VPN** to open the VPN page.

Step 2 Select **Table View**.

Step 3 Open the Filter panel by clicking the filter icon.

Step 4 In the **Tunnel Issues**, click **Detected Issues** to view the VPN configuration reporting errors. You can view the configuration reporting issues.

Step 5 Select the VPN configuration reporting issues.

Step 6 In the **Peers** pane on the right, the ⚠ icon appears for the peer having the issue. Hover over the ⚠ icon to see the issue and resolution.

Next Step: Resolve Tunnel Configuration Issues.

Resolve Tunnel Configuration Issues

This procedure attempts to resolve these tunnel configuration issues:

- When the IP address of a site-to-site VPN interface changes, the "Peer IP Address Value has changed".
- When the IKE value of a VPN tunnel doesn't match the other VPN tunnel, the "IKE value Mismatch" message appears.

See Find Issues in Tunnel Configuration for more information.

Procedure

Step 1 In the CDO navigation bar, click **Inventory**.

Step 2 Click the **Devices** tab.

Step 3 Click the appropriate device type tab and select the device associated with the VPN configuration reporting an issue.

Step 4 Resolve the Conflict Detected Status.

Step 5 In the CDO navigation pane, click **VPN** > **ASA/FDM Site-to-Site VPN** to open the VPN page.

Step 6 Select the VPN configuration reporting this issue.

Step 7 In the **Actions** pane, click the **Edit** icon.

Step 8 Click **Next** in each step until you click the **Finish** button in step 4.

Step 9 Preview and Deploy Configuration Changes for All Devices, on page 337.

Search and Filter Site-to-Site VPN Tunnels

Use the filter sidebar in combination with the search field to focus your search of VPN tunnels presented in the VPN tunnel diagram.

Procedure

Step 1 From the main navigation bar, navigate **VPN > ASA/FDM Site-to-Site VPN**.

Step 2 Click the filter icon to open the filter pane.

Step 3 Use these filters to refine your search:

- **Filter by Device**-Click **Filter by Device**, select the device type tab, and check the devices you want to find by filtering.
- **Tunnel Issues**-Whether or not we have detected either side of the tunnel has issues. Some examples of a device having issues may be but not limited to is: missing associated interface or peer IP address or

access list, IKEv1 proposal mismatches, etc. (Detecting tunnel issues is not yet available for AWS VPC VPN tunnels.)

- **Devices/Services**-Filter by type of device.
- **Status**–Tunnel status can be active or idle.
  - **Active**-There is an open session where network packets are traversing the VPN tunnel or a successful session was established and hasn't been timed-out yet. Active can assist to indicate that tunnel is active and relevant.
  - **Idle**-CDO was unable to discover an open session for this tunnel, the tunnel may either be not in use or there is an issue with this tunnel.
- **Onboarded** - Devices could be managed by CDO or not managed (unmanaged) by CDO.
  - **Managed** – Filter by devices that CDO manages.
  - **Unmanaged** – Filter by devices that CDO does not manage.
- **Device Types** - Whether or not either side of the tunnel is a live (connected device) or model device.

Step 4 You can also search the filtered results by device name or IP address by entering that information in the search bar. The search is case-insensitive.

Onboard an Unmanaged Site-to-Site VPN Peer

CDO will discover a site-to-site VPN tunnel when one of the peers is onboarded. If the second peer is not managed by CDO, you can filter the list of VPN tunnels to find the unmanaged device and onboard it:

Procedure

Step 1 In the main navigation bar, select **VPN** > **ASA/FDM Site-to-Site VPN** to open the VPN page.

Step 2 Select **Table View**.

Step 3 Open the filter panel by clicking .

Step 4 Check **Unmanaged**.

Step 5 Select a tunnel from the table from the results.

Step 6 In the **Peers** pane on the right, click **Onboard Device** and follow the instructions on the screen.

Related Information:

- Onboard Devices and Services
- Onboard a Threat Defense Device

View IKE Object Details of Site-To-Site VPN Tunnels

You can view the details of the IKE objects configured on the peers/devices of the selected tunnel. These details appear in a tree structure in a hierarchy based on the priority of the IKE policy object.

Note Extranet devices don't show the IKE Objects details.

Procedure

Step 1 In the CDO navigation bar on the left, click **VPN > ASA/FDM Site-to-Site VPN**.

Step 2 In the **VPN Tunnels** page, click the name of the VPN tunnel that connects the peers.

Step 3 Under **Relationships** on the right, expand the object that you want to see its details.

View Last Successful Site-to-Site VPN Tunnel Establishment Date

Procedure

Step 1 View Site-to-Site VPN Tunnel Information.

Step 2 Click the **Tunnel Details** pane.

Step 3 View the **Last Seen Active** field.

View Site-to-Site VPN Tunnel Information

The site-to-site VPN table view is a complete listing of all site-to-site VPN tunnels available across all devices onboarded to CDO. A tunnel only exists once in this list. Clicking on a tunnel listed in the table provides an option in the right side bar to navigate directly to a tunnel's peers for further investigation.

In cases where CDO does not manage both sides of a tunnel, you can click Onboard an Unmanaged Site-to-Site VPN Peer to open the main onboarding page an onboard the unmanaged peer. In cases where CDO manages both side of a tunnel, the Peer 2 column contains the name of the managed device. However, in the case of an AWS VPC, the Peer 2 column contains the IP address of the VPN gateway.

To view site-to-site VPN connections in the table view:

Procedure

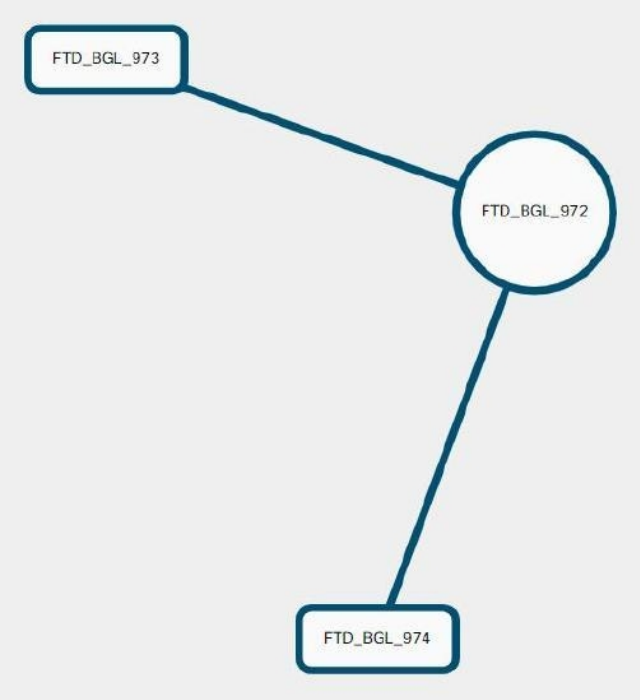
Step 1 From the main navigation bar, click **VPN > ASA/FDM Site-to-Site VPN.**

Step 2 Click the **Table view** button.

Step 3 Use Search and Filter Site-to-Site VPN Tunnels to find a specific tunnel, or zoom into the Global View graphic to find the VPN gateway and its peers that you are looking for.

Site-to-Site VPN Global View

This is an example fo the global view. In the illustration, 'FTD_BGL_972' has a site-to-site connection with FTD_BGL_973 and FTD_BGL_974 devices.



Procedure

Step 1 From the main navigation bar, click **VPN > ASA/FDM Site-to-Site VPN.**

Step 2 Click the **Global view** button.

Step 3 Use Search and Filter Site-to-Site VPN Tunnels to find a specific tunnel, or zoom into the Global View graphic to find the VPN gateway and its peers that you are looking for.

Step 4 Select one of the peers represented in the Global View.

Step 5 Click **View Details**.

Step 6 Click the other end of the VPN tunnel and CDO displays Tunnel Details, NAT Information, and Key Exchange information for that connection:

- **Tunnel Details**-Displays the name and connectivity information about the tunnel. Clicking the Refresh icon updates the connectivity information for the tunnels.
- **Tunnel Details specific to AWS connections**-Tunnel details for AWS site-to-site connections are slightly different than for other connections. For each connection from the AWS VPC to your VPN gateway, AWS creates two VPN tunnels. This is for high availability.
  - The name of the tunnel represents the name of the VPC your VPN gateway is connected to. The IP address named in the tunnel is the IP address that your VPN gateway knows as the VPC.
  - If the CDO Connectivity status shows "active," the AWS tunnel state is "Up." If the CDO Connectivity state is "inactive," the AWS tunnel state is "Down."

- **NAT Information**-Displays the type of NAT rule being used, original and translated packet information, and provides links to the NAT table to view the NAT rule for that tunnel. (Not yet available for AWS VPC site-to-site VPN.)
- **Key Exchange**-Displays the cryptographic keys in use by the tunnel and key-exchange issues. (Not yet available for AWS VPC site-to-site VPN.)

Site-to-Site VPN Tunnels Pane

The Tunnels pane displays a list of all the tunnels associated with a particular VPN gateway. For site-to-site VPN connections between your VPN gateway and an AWS VPC, the tunnels pane shows all the tunnels from your VPN gateway to the VPC. Since each site-to-site VPN connection between your VPN gateway and an AWS VPC has two tunnels, you will see double the number of tunnels you normally would for other devices.

VPN Gateway Details

Displays the number of peers connected to the VPN gateway and the IP address of the VPN gateway. This is only visible in the VPN Tunnels page.

View Peer

After you select a site-to-site VPN peer pair, the peers pane lists the two devices in the pair and allows you to click **View Peer** for one of the devices. By clicking **View Peer**, you see any other site-to-site peer that device is associated with. This is visible in the Table view and in the Global view.

Introduction to Remote Access Virtual Private Network

Remote Access irtual Private Network (RA VPN) capability enables users to connect to your network from a location outside the physical office premises. This means that they can use a computer or a supported iOS/Android device that is connected to the internet and access your network resources securely. This feature is particularly useful for mobile workers who need to connect from their home network or a public Wi-Fi network while ensuring that their data remains safe and protected.

Related Information:

-
- Configuring Remote Access VPN for an FDM-Managed Device

Introduction to Remote Access Virtual Private Network

Remote Access irtual Private Network (RA VPN) capability enables users to connect to your network from a location outside the physical office premises. This means that they can use a computer or a supported iOS/Android device that is connected to the internet and access your network resources securely. This feature is particularly useful for mobile workers who need to connect from their home network or a public Wi-Fi network while ensuring that their data remains safe and protected.

Related Information:

-
- Configuring Remote Access VPN for an FDM-Managed Device

Configuring Remote Access VPN for an FDM-Managed Device

CDO provides an intuitive user interface for configuring a new Remote Access Virtual Private Network (RA VPN). It also allows you to quickly and easily configure RA VPN connection for multiple FDM-managed devices that are on board in CDO. AnyConnect is the only client that is supported on endpoint devices for an RA VPN connectivity to FDM-managed devices.

When the AnyConnect client negotiates an SSL VPN connection with the FDM-managed device, it connects using Transport Layer Security (TLS) or Datagram Transport Layer Security (DTLS). DTLS avoids latency and bandwidth problems associated with some SSL connections and improves the performance of real-time applications that are sensitive to packet delays. The client and the FDM-managed device negotiate the TLS/DTLS version to use. DTLS is used if the client supports it.

CDO supports the following aspects of RA VPN functionality on FDM-managed devices:

- SSL client-based remote access
- IPv4 and IPv6 addressing
- Shared RA VPN configuration across multiple FDM-managed devices

Important If an onboarded FDM-managed device (running on software version 6.7 or later) contains RA VPN configuration with SAML server as the authentication source, CDO doesn't populate the AAA details in the connection profile as it doesn't manage SAML server objects in the current release. Thus you can't manage such RA VPN configuration from CDO. However, CDO reads the RA VPN connection profile and associated trusted CA certificate and SAML server objects.

Related Information:

- Control User Permissions and Attributes Using RADIUS and Group Policies, on page 224
- End-to-End Remote Access VPN Configuration Process for an FDM-Managed Device, on page 237
  - Download AnyConnect Client Software Packages, on page 239
  - Upload AnyConnect Software Packages to an FDM-Managed Device Running Version 6.4.0, on page 239
  - Upload AnyConnect Software Packages to an FDM-Managed Device Running Version 6.5 or Later, on page 242
  - Upload RA VPN AnyConnect Client Profile, on page 270
  - Configure Identity Sources for FDM-Managed Device, on page 245
    - Create or Edit an Active Directory Realm Object, on page 248
    - Create or Edit a RADIUS Server Object or Group, on page 250
  - Create New RA VPN Group Policies, on page 253
  - Create an RA VPN Configuration, on page 259
  - Configure an RA VPN Connection Profile, on page 262
  - Allow Traffic Through the Remote Access VPN, on page 267

Split Tunneling for RA VPN Users (Hair Pinning)

This article describes the split tunneling for RA VPN.

Typically, in remote access VPN, you might want the VPN users to access the Internet through your device. However, you can allow your VPN users to access an outside network while they are connected to an RA VPN. This technique is called split tunneling or hair pinning. The split tunnel allows VPN connectivity to a remote network across a secure tunnel, and it also allows connectivity to a network outside the VPN tunnel. Split tunneling reduces the network load on the FDM-managed devices and increases the bandwidth on the outside interface.

To configure a split-tunnel list, you must create a Standard Access List or Extended Access List. Follow the instructions explained in the **How to Provide Internet Access on the Outside Interface for Remote Access VPN Users (Hair Pinning)** section of Virtual Private Networks (VPN) chapter of the Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager for the version your device is running.

Control User Permissions and Attributes Using RADIUS and Group Policies

This article provides information on applying attributes to RA VPN connections from an external RADIUS server or a group policy.

You can apply user authorization attributes (also called user entitlements or permissions) to RA VPN connections from an external RADIUS server or from a group policy defined on the FDM-managed device. If the FDM-managed device receives attributes from the external AAA server that conflict with those configured on the group policy, then attributes from the AAA server always take precedence.

The FDM-managed device applies attributes in the following order:

Procedure

Step 1 User attributes defined on the external AAA server - The server returns these attributes after successful user authentication or authorization.

Step 2 Group policy configured on the FDM-managed device - If a RADIUS server returns the value of the RADIUS CLASS attribute IETF-Class-25 (OU= group-policy) for the user, the FDM-managed device places the user

in the group policy of the same name and enforces any attributes in the group policy that are not returned by the server.

Step 3 Group policy assigned by the connection profile - The connection profile has the preliminary settings for the connection and includes a default group policy applied to the user before authentication. All users connecting to the FDM-managed device initially belong to this group, which provides any attributes that are missing from the user attributes returned by the AAA server, or the group policy assigned to the user.

FDM-managed devices support RADIUS attributes with vendor ID 3076. If the RADIUS server you use does not have these attributes defined, you must manually define them. To define an attribute, use the attribute name or number, type, value, and vendor code (3076).

The following topics explain the supported attributes based on whether the values are defined in the RADIUS server, or whether they are values the system sends to the RADIUS server.

Attributes Sent to the RADIUS Server

RADIUS attributes 146 and 150 are sent from the FDM-managed device to the RADIUS server for authentication and authorization requests. All the following attributes are sent from the FDM-managed device to the RADIUS server for accounting start, interim-update, and stop requests.

Table 6: Attributes Secure Firewall Threat Defense Sends to RADIUS

Attribute	Attribute	Syntax, Type	Single or Multi-valued	Description or Value
Client Type	150	Integer	Single	The type of client this is connecting to the VPN: 2= AnyConnect Client SSL VPN
Session Type	151	Integer	Single	The type of connection: 1 = AnyConnect Client SSL VPN
Tunnel Group Name	146	String	Single	The name of the connection profile that was used for establishing the session, as defined on the FDM-managed device. The name can be 1 - 253 characters.

Attributes Received from the RADIUS Server

The following user authorization attributes are sent to the FDM-managed device from the RADIUS server.

Attribute	Attribute Number	Syntax, Type	Single or Multi-valued	Description or Value
Access-List-Inbound	86	String	Single	Both Access-List attributes take the name of an ACL that is configured on the FDM-managed device. Create these ACLs in firewall device manager using the Smart CLI Extended Access List object type (Log in to firewall device manager and select **Device** > **Advanced Configuration** > **Smart CLI** > **Objects**). These ACLs control traffic flow in the inbound (traffic entering the FDM-managed device) or outbound (traffic leaving the FDM-managed device) direction.
Access-List-Outbound	87	String	Single	
Address-Pools	217	String	Single	The name of a network object defined on the FDM-managed device that identifies a subnet, which will be used as the address pool for clients connecting to the RA VPN. Define the network object on the **Objects** page.
Banner1	15	String	Single	The banner to display when the user logs in.
Banner2	36	String	Single	The second part of the banner to display when the user logs in. Banner2 is appended to Banner1.

Attribute	Attribute Number	Syntax, Type	Single or Multi-valued	Description or Value
Group-Policy	25	String	Single	The group policy to use in the connection. You must create the group policy on the RA VPN **Group Policy** page. You can use one of the following formats: • *group policy name* • OU=*group policy name* • OU=*group policy name*;
Simultaneous-Logins	2	Integer	Single	The number of separate simultaneous connections the user can establish, 0 - 2147483647.
VLAN	140	Integer	Single	The VLAN on which to confine the user's connection, 0 - 4094. You must also configure this VLAN on a subinterface on the FDM-managed device.

Two-Factor Authentication

You can configure two-factor authentication for the RA VPN. With two-factor authentication, the user must supply a username and static password, plus an additional item such as a Duo passcode. Two-factor authentication differs from using a second authentication source in that two-factor is configured on a single authentication source, with the relationship to the Duo server tied to the primary authentication source. The exception is Duo LDAP, where you configure the Duo LDAP server as the secondary authentication source.

- Duo Two-Factor Authentication Using RADIUS, on page 227
- Duo Two-Factor Authentication using LDAP, on page 232

Duo Two-Factor Authentication Using RADIUS

You can configure the Duo RADIUS server as the primary authentication source. This approach uses the Duo RADIUS Authentication Proxy.

For the detailed steps to configure Duo, please see https://duo.com/docs/cisco-firepower.

You would then configure Duo to forward authentication requests directed to the proxy server to use another RADIUS server, or a Microsoft Active Directory(AD) server, as the first authentication factor, and the Duo Cloud Service as the second factor.

When using this approach, the user must authenticate using a username that is configured on both the Duo Authentication Proxy and the associated RADIUS/AD server, and the password for the username configured in the RADIUS/AD server, followed by one of the following Duo codes:

Duo-passcode. For example, my-password,12345.

push. For example, *my-password*,**push**. Use **push** to tell Duo to send a push authentication to the Duo Mobile app, which the user must have already installed and registered.

sms. For example, *my-password*,**sms**. Use sms to tell Duo to send an SMS message with a new batch of passcodes to the user's mobile device. The user's authentication attempt will fail when using sms. The user must then re-authenticate and enter the new passcode as the secondary factor.

phone. For example, *my-password*,**phone**. Use phone to tell Duo to perform phone callback authentication.

If the username and password are authenticated, the Duo Authentication Proxy contacts the Duo Cloud Service, which validates that the request is from a valid configured proxy device and then pushes a temporary passcode to the mobile device of the user as directed. When the user accepts this passcode, the session is marked authenticated by Duo and the RA VPN is established.

For a detailed explanation, see How to Configure Two-Factor Authentication using Duo RADIUS, on page 228

How to Configure Two-Factor Authentication using Duo RADIUS

You can configure the Duo RADIUS server as the primary authentication source. This approach uses the Duo RADIUS Authentication Proxy.

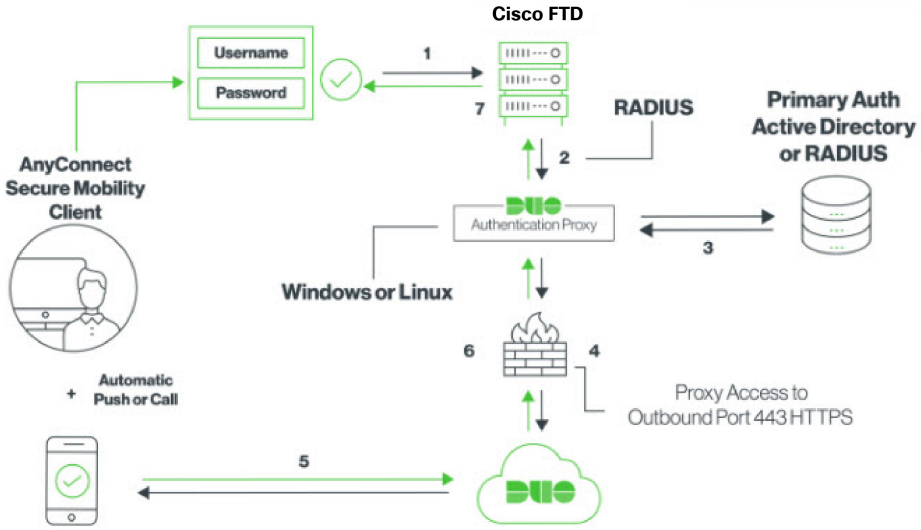
You would then configure Duo to forward authentication requests directed to the proxy server to use another RADIUS server, or an AD server, as the first authentication factor, and the Duo Cloud Service as the second factor.

The following topics explain the configuration in more detail:

- System Flow for Duo RADIUS Secondary Authentication, on page 228
- Configure Device for Duo RADIUS Using CDO, on page 230

System Flow for Duo RADIUS Secondary Authentication

Following is an explanation of the system



flow:

1. The user makes a remote access VPN connection to the FDM-managed device and provides username associated with RADIUS/AD server, the password for the username configured in the RADIUS/AD server, followed by one of the DUO codes, Duo-password, push, SMS, or phone. For more information, Duo Two-Factor Authentication Using RADIUS, on page 227
2. FDM-managed device sends the authentication request to the Duo Authentication proxy.
3. Duo Authentication proxy authenticates this primary authentication attempt with the primary authentication server, which might be Active Directory or RADIUS.
4. If the credentials are authenticated, the Duo Authentication Proxy connection is established to Duo Security over TCP port 443.
5. Duo then authenticates the user separately through push notification, text message with a passcode, or a telephone call. The user must complete this authentication successfully.
6. Duo authentication proxy receives the authentication response.
7. If the secondary authentication was successful, the FDM-managed device establishes a remote access VPN connection with the user's AnyConnect client.

Configure Duo RADIUS Secondary Authentication

Duo Authentication proxy authenticates this primary authentication attempt with the primary authentication server, which might be Active Directory or RADIUS.

Create a Duo Account

Create a Duo account and obtain the integration key, secret key, and API hostname.

Following is an overview of the process. For details, please see the Duo web site,

Procedure

Step 1 Sign up for a Duo account.

Step 2 Log in to the Duo Admin Panel and navigate to **Applications**.

Step 3 Click **Protect an Application** and locate **Cisco Firepower Threat Defense VPN** in the applications list.

Step 4 Click **Protect this Application** to get your integration key, secret key, and API hostname. You'll need this information when configuring the proxy. For help, see the *Duo Getting Started* guide, https://duo.com/docs/getting-started.

Step 5 Install and configure the Duo Authentication Proxy. For instructions, see the "Install the Duo Authentication Proxy" section in https://duo.com/docs/cisco-firepower.

Step 6 Start the Authentication Proxy. For instructions, see the "Start the Proxy" section in https://duo.com/docs/cisco-firepower.

For enrolling new users in Duo, see https://duo.com/docs/enrolling-users.

Configure Device for Duo RADIUS Using CDO

Procedure

Step 1 Configure FTD Radius Server Object.

a) In the CDO navigation bar on the left, click **Objects > FDM Objects**.

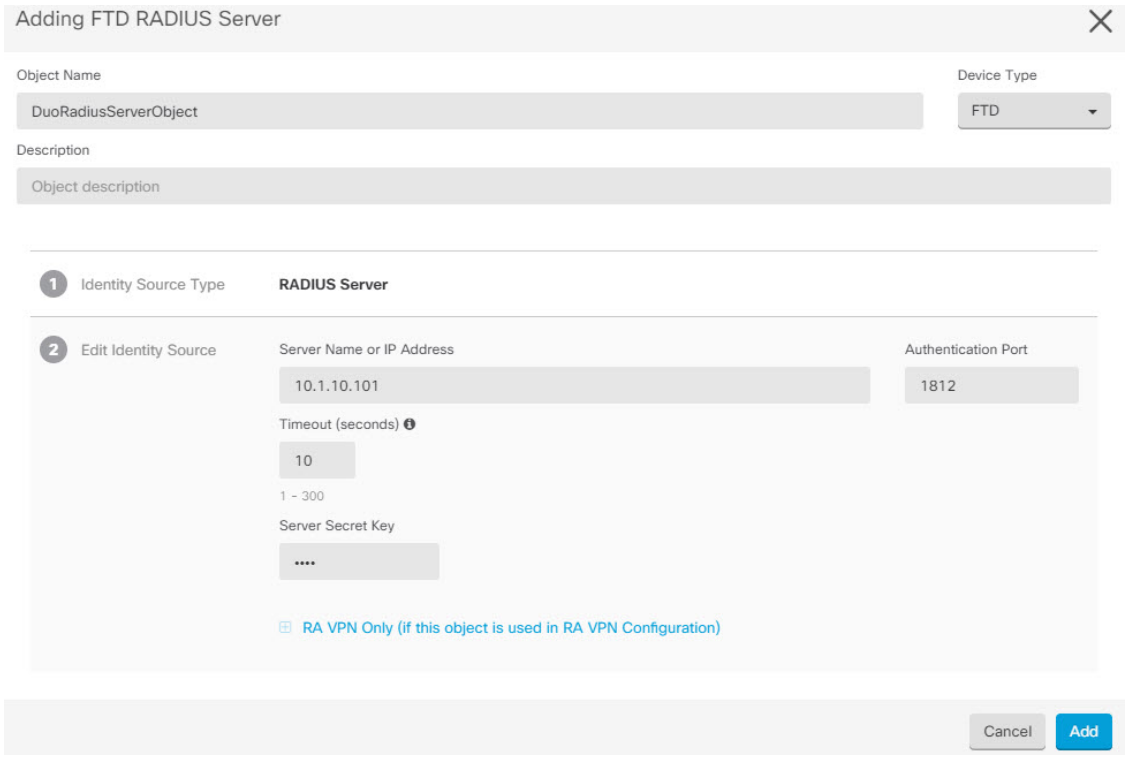
b) Click  > **RA VPN Objects (ASA & FTD)** > **Identity Source**.

c) Provide a name and set the **Device Type** as **FTD**.

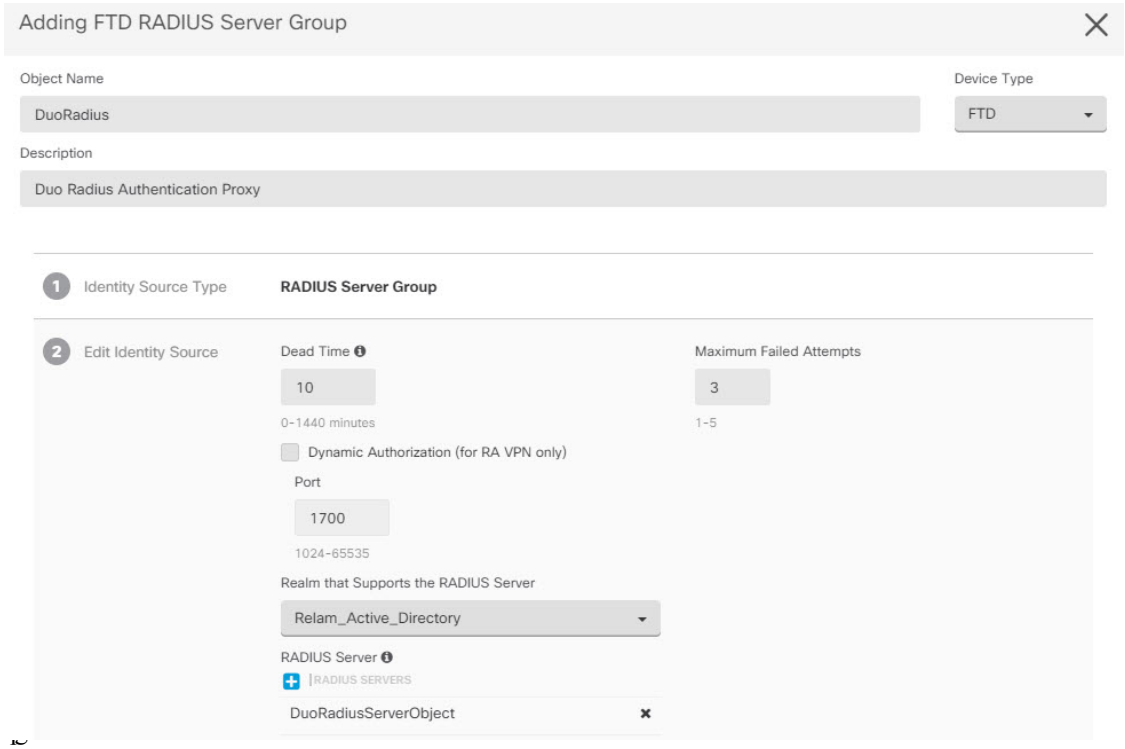
d) Select **Radius Server Group** and click **Continue**. For details, see step 6 in Create a RADIUS Server Group, on page 251.

e) In the **Radius Server** section, click the **Add** button and click **Create New Radius Server**. See Create a RADIUS Server Object, on page 250

In the **Server Name or IP Address** field, enter your Duo Authentication Proxy server's fully-qualified hostname or IP address.

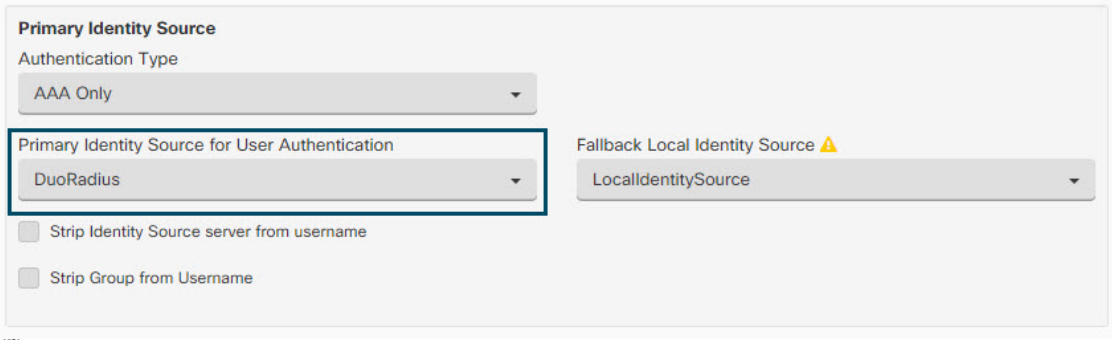


f) Once you have added the Duo RADIUS server to the group, click **Add** to create the new Duo RADIUS server



Step 2 Change the Remote Access VPN Authentication Method to Duo RADIUS.

a) In the CDO navigation menu, click **VPN** > **Remote Access VPN Configuration**.
b) Expand the VPN configuration and click on the connection profile to which you want to add Duo.
c) In the **Actions** pane on the right, click **Edit**.
d) Select the **Authentication Type** can be **AAA** or **AAA and Client Certificate**.
e) In the **Primary Identity Source for User Authentication** list, select the server group you created



f) You typically do not need to select an "Authorization Server" or "Accounting Server".
g) Click **Continue**.
h) In the **Summary and Instructions** step, click **Done** to save the configuration.

Step 3 Preview and Deploy Configuration Changes for All Devices now the changes you made, or wait and deploy multiple changes at once.

Duo Two-Factor Authentication using LDAP

You can use the Duo LDAP server as the secondary authentication source along with a Microsoft Active Directory (AD) or RADIUS server as the primary source. With Duo LDAP, the secondary authentication validates the primary authentication with a Duo passcode, push notification, or phone call.

Note The Duo two-factor authentication feature is available in CDO for devices running Firepower Threat version 6.5 or later.

The FDM-managed device communicates with Duo LDAP using LDAPS over port TCP/636.

When using this approach, the user must authenticate using a username that is configured on both the AD/RADIUS server and the Duo LDAP server. When prompted to log in by AnyConnect, the user provides the AD/RADIUS password in the primary Password field, and for the Secondary Password, provides one of the following to authenticate with Duo. For more details, see the "Second Password for Factor Selection" section in https://guide.duo.com/anyconnect.

- *Duo passcode*—Authenticate using a passcode, either generated with Duo Mobile, sent via SMS, generated by your hardware token, or provided by an administrator. For example, 1234567.
- **push**—Push a login request to your phone, if you have installed and activated the Duo Mobile app. Review the request and tap **Approve** to log in.
- **phone**—Authenticate using a phone callback.
- **sms**—Request a Duo passcode in a text message. The login attempt will fail. Log in again using the new passcode.

For a detailed explanation, see How to Configure Two-Factor Authentication using Duo LDAP, on page 233.

How to Configure Two-Factor Authentication using Duo LDAP

You can use the Duo LDAP server as the secondary authentication source along with a Microsoft Active Directory (AD) or RADIUS server as the primary source. With Duo LDAP, the secondary authentication validates the primary authentication with a Duo passcode, push notification, or phone call..

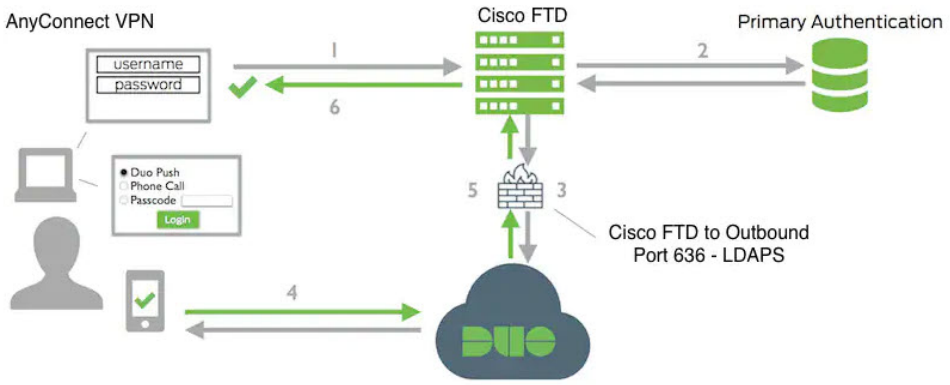
The following topics explain the configuration in more detail:

- System Flow for Duo LDAP Secondary Authentication, on page 233
- Configure Duo LDAP Secondary Authentication, on page 233

System Flow for Duo LDAP Secondary Authentication

The following graphic shows how threat defense and Duo work together to provide two-factor authentication using LDAP.

Following is an explanation of the system flow:



1. The user makes a remote access VPN connection to the FDM-managed device and provides username and password.
2. FDM-managed device authenticates this primary authentication attempt with the primary authentication server, which might be Active Directory or RADIUS.
3. If the primary authentication works, FDM-managed device sends a request for secondary authentication to the Duo LDAP server.
4. Duo then authenticates the user separately, through push notification, text message with a passcode, or a telephone call. The user must complete this authentication successfully.
5. Duo responds to the FDM-managed device to indicate whether the user authenticated successfully.
6. If the secondary authentication was successful, the FDM-managed device establishes a remote access VPN connection with the user's AnyConnect client.

Configure Duo LDAP Secondary Authentication

The following procedure explains the end-to-end process of configuring two-factor authentication, using Duo LDAP as the secondary authentication source, for remote access VPN. You must have an account with Duo, and obtain some information from Duo, to complete this configuration.

Create a Duo Account

Create a Duo account and obtain the integration key, secret key, and API hostname.

Following is an overview of the process. For details, please see the Duo web site,

Procedure

Step 1 Sign up for a Duo account.

Step 2 Log in to the Duo Admin Panel and navigate to **Applications**.

Step 3 Click **Protect an Application** and locate **Cisco Firepower Threat Defense VPN** in the applications list.

Step 4 Click **Protect this Application** to get your **Integration key**, **Secret key**, and **API hostname**. For help, see the *Duo Getting Started* guide, https://duo.com/docs/getting-started.

For enrolling new users in Duo, see https://duo.com/docs/enrolling-users.

Upload a Trusted CA Certificate to an FDM-Managed Device

The FDM-managed device must have the trusted CA certificate needed to validate the connection to the Duo LDAP server. You can go directly to https://www.digicert.com/digicert-root-certificates.htm and download either **DigiCertSHA2HighAssuranceServerCA** or **DigiCert High Assurance EV Root CA** and upload it using Firewall Device Manager (FDM).

Procedure

Step 1 Access the firewall device manager page of the FDM-managed device, choose **Objects** > **Certificates**.

Step 2 Click **+** > **Add Trusted CA Certificate**.

Step 3 Enter a name for the certificate, for example, DigiCert_High_Assurance_EV_Root_CA. (Spaces are not allowed.)

Step 4 Click **Upload Certificate** and select the file that you downloaded.

Step 5 Click **OK**.

Step 6 Onboard the device to Cisco Defense Orchestrator if you haven't onboarded it already.

Step 7 Read All Device Configurations.

Configure FTD for Duo LDAP in CDO

Procedure

Step 1 Create a Duo LDAP identity source object for the Duo LDAP server.

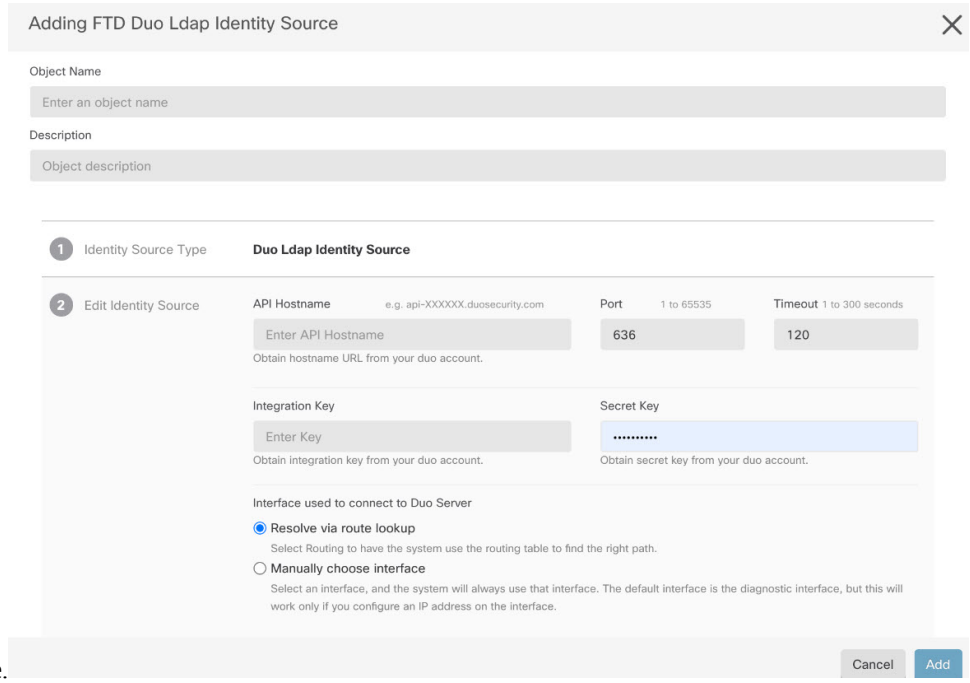
a) In the CDO navigation bar on the left, click **Objects > FDM Objects**.

b) Click the  to create an object > **RA VPN Objects (ASA & FTD)** > **Identity Source**.

c) Enter a name for the object, for example, Duo-LDAP-server.

d) Select the **Device Type** as **FTD**.

e) Click **Duo Ldap Identity Source** and click



Continue.

f) In the **Edit Identity Source** area, provide the following details:

- **API Hostname**: Enter the API Hostname that you obtained from your Duo account. The hostname should look like the following, with the X's replaced with your unique value: API-XXXXXXXX.DUOSECURITY.COM. Uppercase is not required.
- **Port**: Enter the TCP port to use for LDAPS. This should be 636 unless you have been told by Duo to use a different port. Note that you must ensure that your access control list allows traffic to the Duo LDAP server through this port.
- **Timeout**: Enter the timeout, in seconds, to connect to the Duo server. The value can be 1-300 seconds. The default is 120. To use the default, either enter 120 or delete the attribute line.
- **Integration Key**: Enter the integration key that you obtained from your Duo account.
- **Secret Key**: Enter the secret key that you obtained from your Duo account. This key will subsequently be masked.
- **Interface used to connect to Duo Server**: Select the interface that is used for connecting to Duo Server.
  - **Resolve via route lookup**: Select this option to use the routing table to find the right path. For creating a routing table, see Routing.
  - **Manually choose interface**: Select this option and choose one of the interfaces from the list. The default interface is the diagnostic interface, but this will work only if you configure an IP address on the interface. Note: Ensure that the selected interface is present on the same device you want to connect to Duo Server.
  - Click **Add**.

Step 2 (optional) Use the AnyConnect Profile Editor to create a profile that specifies 60 seconds or more for authentication timeout.

You need to give users extra time to obtain the Duo passcode and complete the secondary authentication. We recommend at least 60 seconds. The following procedure explains how to configure the authentication timeout only and then upload the profile to FDM-managed device. If you want to change other settings, you can do so now.

a) If you have not already done so, download and install the AnyConnect profile editor package. You can find this in the Cisco Software center (software.cisco.com) in the folder for your AnyConnect version. The base path at the time of this writing is **Downloads Home** > **Security** > **VPN and Endpoint Security Clients** > **Cisco VPN Clients** > **AnyConnect Secure Mobility Client**.
b) Open the AnyConnect **VPN Profile Editor**.
c) Select **Preferences (Part 2)** in the table of contents, scroll to the end of the page, and change **Authentication Timeout** to 60 (or more). The following image is from the AnyConnect 4.7 VPN Profile Editor; previous or subsequent versions might be different.
d) Choose **File** > **Save**, and save the profile XML file to your workstation with an appropriate name, for example, duo-ldap-profile.xml.
e) You can now close the **VPN Profile Editor** application.
f) In CDO, Upload RA VPN AnyConnect Client Profile.

Step 3 Create a group policy and select the AnyConnect profile in the policy.

The group policy that you assign to a user controls many aspects of the connection. The following procedure explains how to assign the profile XML file to the group. For more information, see Create New RA VPN Group Policies.

a) In the CDO navigation bar on the left, click **Objects > FDM Objects**.
b) To edit an existing group policy, use the **RA VPN Group Policy** filter to view only the existing group policies and modify the policy that you want and save it.
c) To create a new group policy, click **RA VPN Objects (ASA & FTD)** > **RA VPN Group Policy**.
d) On the **General** page, configure the following properties:
   - **Name** — For a new profile, enter a name. For example, Duo-LDAP-group.
   - **AnyConnect Client Profiles** — Select the AnyConnect client profile object that you created.
e) Click **Add** to save the object.
f) Click **VPN** > **Remote Access VPN Configuration**.
g) Click the remote access VPN configuration that you want to update.
h) In the **Actions** pane on the right, click **Group Policies**.
i) Click **+** to select the group policies that you want to associate with the VPN configuration.
j) Click **Save** to save the group policy.

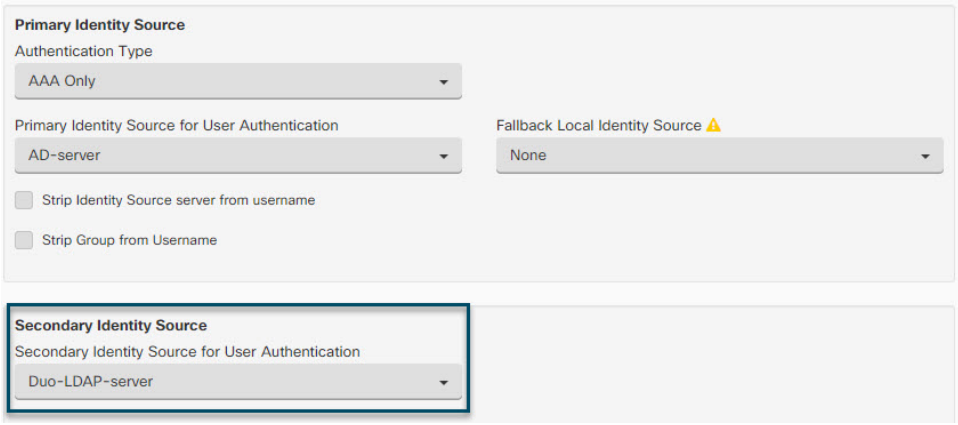
Step 4 Create or edit the remote access VPN connection profile to use for Duo-LDAP secondary authentication.

The following procedure just mentions the key changes to enable Duo-LDAP as the secondary authentication source and apply the AnyConnect client profile. For new connection profiles, you must configure the rest of the required fields. For this procedure, we assume you are editing an existing connection profile, and you simply must change these two settings.

a) On the CDO navigation page, click **VPN** > **Remote Access VPN Configuration**.
b) Expand the remote access VPN configuration and click the connection profile that you want to update.
c) In the **Actions** pane on the right, click **Edit**.

d) Under **Primary Identity Source**, configure the following:

- **Authentication Type** — Choose either AAA Only or AAA and Client Certificate. You cannot configure two-factor authentication unless you use AAA.
- **Primary Identity Source for User Authentication** — Select your primary Active Directory or RADIUS server. Note that you can select a Duo-LDAP identity source as the primary source. However, Duo-LDAP provides authentication services only, not identity services, so if you use it as a primary authentication source, you will not see usernames associated with RA VPN connections in any dashboards, and you will not be able to write access control rules for these users. (You can configure fallback to the local identity source if you want to.)
- **Secondary Identity Source** — Select the Duo-LDAP identity source.



Note If username in **Primary Identity Source** and **Secondary Identity Source** are the same, we recommend enabling **Use Primary username for Secondary login** in the **Advanced** options in the Connection Profile. Configuring this way allows the end-user to use a single username for both primary and secondary identity sources.

e) Click **Continue**.

f) On the **Group Policy** page, select the group policy that you created or

g) Click **Continue**.

h) Click **Done** to save your changes to the connection profile.

Step 5 Preview and Deploy Configuration Changes for All Devices, on page 337.

End-to-End Remote Access VPN Configuration Process for an FDM-Managed Device

This section provides the end-to-end procedure for configuring Remote Access Virtual Private Network (RA VPN) on an FDM-managed device onboarded to CDO.

To enable remote access VPN for your clients, you need to configure several separate items. The following procedure provides the end-to-end process.

Procedure

Step 1 Enable two licenses.

- When you register the device, you must do so with a Smart Software Manager account that is enabled for export-controlled features. The license must meet export control requirements before you can configure remote access VPN. You also cannot configure the feature using the evaluation license. Your purchase of an FDM-managed device automatically includes an license. The license covers all features not covered by the optional licenses. It is a perpetual license. The device must be registered to Secure Firewall device manager. See the **Registering the Device** section in the Licensing the System chapter of the Cisco Secure Firewall Threat Defense Configuration Guide for the version your device is running.
- A license. For details, see Licensing Requirements for Remote Access VPN.
  - To enable the license, see the **Enabling or Disabling Optional Licenses** section in the Licensing the System chapter of the Secure Firewall Threat Defense Configuration Guide for the version your device is running.

Step 2 Configure Certificates.

Certificates are required to authenticate SSL connections between the clients and the device. You can use the pre-defined DefaultInternalCertificate for the VPN or create your own.

If you use an encrypted connection for the directory realm used for authentication, you must upload a trusted CA certificate. For more information on certificates and how to upload them, see Configuring Certificates.

Step 3 Configure the identity source used for authenticating remote users.

You can use the following sources to authenticate users attempting to connect to your network using RA VPN. Additionally, you can use client certificates for authentication, either alone or in conjunction with an identity source.

- Active Directory identity realm: As a primary authentication source. The user accounts are defined in your Active Directory (AD) server. See Configuring AD Identity Realms. See Create or Edit an Active Directory Realm Object.
- RADIUS server group: As a primary or secondary authentication source, and for authorization and accounting. See Create or Edit a RADIUS Server Object or Group.
- Local Identity Source (the local user database): As a primary or fallback source. You can define users directly on the device and not use an external server. If you use the local database as a fallback source, ensure that you define the same usernames/passwords as the ones described in the external server.

  Note You can create user accounts directly on the FDM-managed device only from Secure Firewall device manager. See Configure Local Users.

Step 4 (Optional.) Create New RA VPN Group Policies.

The group policy defines user-related attributes. You can configure group policies to provide differential access to resources based on group membership. Alternatively, use the default policy for all connections.

Step 5 Create an RA VPN Configuration.

Step 6 Configure an RA VPN Connection Profile.

Step 7 Preview and Deploy Configuration Changes for All Devices.

Step 8 Allow Traffic Through the Remote Access VPN.

Step 9 (Optional.) Enable the identity policy and configure a rule for passive authentication. If you enable passive user authentication, users who logged in through the remote access VPN will be shown in the dashboards, and they will also be available as traffic-matching criteria in policies. If you do not enable passive authentication, RA VPN users will be available only if they match an active authentication policy. You must enable the identity policy to get any username information in the dashboards or for traffic matching. See Configure Identity Policies.

Important If you change the Remote Access VPN configuration by using a local manager like Secure Firewall device manager, the **Configuration Status** of that device in CDO shows "Conflict Detected". See Out-of-Band Changes on Devices. You can Resolve Configuration Conflicts on this FDM-managed device.

What to do next

Once the RA VPN configuration is downloaded to the FDM-managed devices, the users can connect to your network from a remote location using a computer or other supported iOS or Android device connected to the Internet. You can monitor live AnyConnect Remote Access Virtual Private Network (RA VPN) sessions from all onboarded RA VPN head-ends in your tenant. See Monitor Remote Access Virtual Private Network Sessions.

Download AnyConnect Client Software Packages

Before configuring a remote access VPN, you must download the AnyConnect software packages from https://software.cisco.com/download/home/283000185 to your workstation. Ensure that you download the "AnyConnect Headend Deployment Package" for your desired operating systems. Later, you can upload these packages to FDM-managed devices when defining the VPN.

Always download the latest AnyConnect version, to ensure that you have the latest features, bug fixes, and security patches. Regularly update the packages on the device.

Note You can upload one AnyConnect package per Operating System (OS): Windows, Mac, and Linux. You cannot upload multiple versions for a given OS type.

Upload AnyConnect Software Packages to an FDM-Managed Device Running Version 6.4.0

You can upload the AnyConnect software packages to the FDM-managed devices version 6.4.0 using firewall device manager API explorer. A minimum of one AnyConnect software package must be present on the device to create an RA VPN connection.

Important The procedure applies only to firewall device manager Version 6.4. If you are using firewall device manager Version 6.5 or later, use the Cisco Defense Orchestrator interface to Upload AnyConnect Software Packages to an FDM-Managed Device Running Version 6.5 or Later.

Use the following procedure to upload the AnyConnect package to firewall device manager Version 6.4.0:

Procedure

Step 1 Download the AnyConnect packages from https://software.cisco.com/download/home/283000185.

- Make sure you accept the EULA and have K9 (encrypted image) privileges.
- Select the "AnyConnect Headend Deployment Package" package for your operating system. The package name will be similar to, "anyconnect-win-4.7.04056-webdeploy-k9.pkg. There are separate headend Webs Deploy packages for Windows, macOS, and Linux.

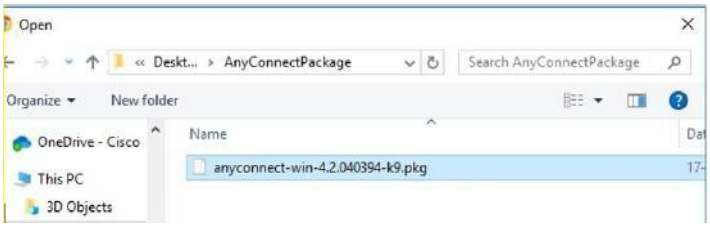
Step 2 Using a browser, open the home page of the system. For example, https://ftd.example.com.

Step 3 Log into Firewall Device Manager.

Step 4 Edit the URL to point to /#/api-explorer, for example, https://ftd.example.com/#/api-explorer.

Step 5 Scroll down and click **Upload** > **/action/uploaddiskfile.**

Step 6 In **fileToUpload** field**,** click **Choose File** and select the required AnyConnect package. You can upload the packages one at a time.



Step 7 Click **Open**.

Step 8 Scroll down and click **TRY IT OUT!.** Wait until the package uploads completely. In the **Response Body**, the API response appears in the following format.

{ "version": null, "name": "691f47e1-90c7-11e9-a361-79e2452f0c57.pkg",

"fileName": "691f47e1-90c7-11e9-a361-79e2452f0c57.pkg",

"id": "691f47e1-90c7-11e9-a361-79e2452f0c57.pkg",

"type": "fileuploadstatus",

"links": {

"self":

https://ftd.example.com:972/api/fdm/...90d111e9-a361- cf32937ce0df.pkg

} }

Record the **fileName** of the package from the response as you must enter the same string when performing the POST operation. In this example, the fileName is **691f47e1-90c7-11e9-a361-79e2452f0c57.pkg**.

Step 9 Scroll up near the top of Threat Defense REST API page and click **AnyConnectPackageFile** > **POST /object/anyconnectpackagefiles**. Perform a POST operation to the API providing the temp staged diskFilename and the OS type of the package file in the payload. This action creates the AnyConnect package file.

Step 10 In the **body** field, enter the package details in the following format only:

{ "platformType": "WINDOWS",

"diskFileName": "691f47e1-90c7-11e9-a361-79e2452f0c57.pkg",

"type": "anyconnectpackagefile",

"name": "AnyConnectWindowsBGL" }

a. In the **platformType** field, enter the OS platform as WINDOWS, MACOS, or LINUX.

b. In the **diskFileName** field, enter the **fileName** that you have recorded after uploading disk file.

c. In the **name** field, enter a name that you want for the package.

d. Click **TRY IT OUT!**.

In the **Response Body** field, the API response appears in the following format after a successful POST operation.

{ "version": "ni7xeneslft3p",
"name": "AnyConnectWindowsBGL",
"description": null,
"diskFileName": "41d592e3-90ca-11e9-a361-6d05320a165d.pkg",
"md5Checksum": "9bbe53dcf92e515d3ce5423048212488",
"platformType": "WINDOWS",
"id": "c9c9dfe3-9cd8-11e9-a361-23534f081c43",
"type": "anyconnectpackagefile",
"links": { "self":
"https:/>/ftd.example.com:972...1-cf32937ce0df"
}
}

The AnyConnect package is created on firewall device manager.

Step 11 Click **AnyConnectPackageFile** > **GET /object/anyconnectpackagefiles** > **TRY IT OUT!.**

The **Response Body** shows all AnyConnect package files.

A sample response is shown below.

{
"items": [
{
"version": "la4nwceqk2sg4",
"name": "AnyConnectWindowsBGL",
"description": null,
"diskFileName": "82f1e362-9cd8-11e9-a361-9758ba07962d.pkg",
"md5Checksum": "9bbe53dcf92e515d3ce5423048212488",
"platformType": "WINDOWS",
"id": "c9c9dfe3-9cd8-11e9-a361-23534f081c43",
"type": "anyconnectpackagefile",
"links": {
"self":
"https://ftd.example.com:972...1-23534f081c43"
}

```
}
],
```

Step 12 Upload other AnyConnect packages for each OS type. Repeat steps from 4 to 10.

Step 13 Edit the URL to point to the web page, for example, https://ftd.example.com

Step 14 Click the **Deploy Changes** icon in the upper right of the web page. The icon is highlighted with a dot when there are undeployed changes.

Step 15 If you are satisfied with the changes, you can click **Deploy Now** to start the job immediately. The window will show that the deployment is in progress. You can close the window or wait for the deployment to complete.

Note To delete a package from the FDM-managed device, click **AnyConnectPackageFile** > **Delete**. In the **objID** field, type the package id and click **TRY IT OUT!**.

To complete a VPN connection, your users must install the AnyConnect client software on their workstation. For more information, see How Users Can Install the AnyConnect Client Software on FDM-Managed Device, on page 272.

Upload AnyConnect Software Packages to an FDM-Managed Device Running Version 6.5 or Later

If you're using an FDM-managed device, running version 6.5 or later, for configuring RA VPN, you can use the RA VPN wizard in Cisco Defense Orchestrator to upload AnyConnect software packages to the device. In the RA VPN wizard, you must provide the URL of the remote HTTP or HTTPS server where the AnyConnect packages are preloaded.

Note You can upload the AnyConnect package using the Upload AnyConnect Software Packages to an FDM-Managed Device Running Version 6.4.0 as well.

Upload an AnyConnect Package from CDO Repository

The remote access VPN Configuration wizard presents AnyConnect packages per operating system from the CDO repository, which you can select and upload to device. Make sure that the device has access to the internet and proper DNS configuration.

Note If the desired package is unavailable in the presented list or the device has no access to the internet, you can upload the package using the server where the AnyConnect packages are preloaded.

Procedure

Step 1 Click on the field that corresponds to an operating system and select an AnyConnect package.

Step 2 Click  to upload the package. If the checksum doesn't match, the AnyConnect package upload fails. You can see the device's workflow tab for more details about the failure.

Before you Begin

Make sure that you download the "AnyConnect Headend Deployment Package" for your desired operating systems. Always download the latest AnyConnect version, to ensure that you have the latest features, bug fixes, and security patches. Regularly update the packages on the device.

Note You can upload one AnyConnect package per Operating System (OS): Windows, Mac, and Linux. You cannot upload multiple versions for a given OS type.

Procedure

Step 1 Download the AnyConnect packages from https://software.cisco.com/download/home/283000185.

- Make sure you accept the EULA and have K9 (encrypted image) privileges.
- Select the "AnyConnect Headend Deployment Package" package for your operating system. The package name will be similar to "anyconnect-win-4.7.04056-webdeploy-k9.pkg." There are separate headend packages for Windows, macOS, and Linux.

Step 2 Upload the AnyConnect packages to a remote HTTP or HTTPS server. Ensure that there is a network route from the FDM-managed device to the HTTP or HTTPS server.

Note If you are uploading the AnyConnect package to an HTTPS server, ensure that the following steps are performed:

- Upload the trusted CA certificate of that server on the FDM-managed device from firewall device manager. To upload the certificate, see the "Uploading Trusted CA Certificates" section in the "Certificates" chapter of Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager, Version X.Y.
- Install the trusted CA certificate on the HTTPS server.

Step 3 The remote server's URL must be a direct link without prompting for authentication. If the URL is pre-authenticated, the file can be downloaded by specifying the RA VPN wizard's URL.

Step 4 If the remote server IP address is NATed, you have to provide the NATed public IP address of the remote server location.

Upload new AnyConnect Packages

Use the following procedure to upload new AnyConnect packages to an FDM-managed device running Version 6.5.0:

Procedure

Step 1 Create an RA VPN Configuration.

Step 2 In the **AnyConnect Package Detected**, you can upload separate packages for Windows, Mac, and Linux endpoints.

Step 3 In the corresponding platform field, specify the server's paths where the AnyConnect packages compatible for Windows, Mac, and Linux are pre-uploaded. Examples of server paths: 'http://<ip_address>:port_number/<folder_name>/anyconnect-win-4.8.01090-webdeploy-k9.pkg', 'https://<ip_address>:port_number/<folder_name>/anyconnect-linux64-4.7.03052-webdeploy-k9.pkg'.

Step 4 Click to upload the package. CDO validates if the path is reachable, and the specified filename is a valid package. When the validation is successful, the names of the AnyConnect packages appear. As you add more FDM-managed devices to the RA VPN configuration, you can upload the AnyConnect packages to them.

Step 5 Click **OK**. The AnyConnect packages are added to the RA VPN configuration.

Step 6 Continue to Create an RA VPN Configuration from step 6 onwards.

What to do next

To complete a VPN connection, your users must install the AnyConnect client software on their workstation. For more information, see How Users Can Install the AnyConnect Client Software on FDM-Managed Device.

Replace an Existing AnyConnect Package

If the AnyConnect packages are already present on the devices, you can see them in the RA VPN wizard. You can see all the available AnyConnect packages for an operating system in a drop-down list. You can select an existing package from the list and replace it with a new one but can't add a new package to the list.

Note If you want to replace an existing package with a new one, ensure that the new AnyConnect package is uploaded already to a server on the network that the FDM-managed device can reach.

Procedure

Step 1 In the CDO navigation bar at the left, click **VPN** > **Remote Access VPN**.

Step 2 Select the RA VPN configuration to be modified, and under **Actions**, click **Edit**.

Step 3 In **AnyConnect Packages Detected**, click icon appearing beside the existing AnyConnect package. If there are multiple versions of AnyConnect package for an operating system, select the package you want to replace from the list and click **Edit**. The existing package disappears from the corresponding field.

Step 4 Specify the server's path where the new AnyConnect package is preloaded and click to upload the package.

Step 5 Click **OK**. The new AnyConnect package is added to the RA VPN configuration.

Step 6 Continue to Create an RA VPN Configuration from step 6 onwards.

Delete the AnyConnect Package

Procedure

Step 1 In the CDO navigation bar at the left, click **VPN** > **Remote Access VPN**.

Step 2 Select the RA VPN configuration to be modified, and under **Actions**, click **Edit**.

Step 3 In **AnyConnect Packages Detected**, click icon appearing beside the AnyConnect package that you want to delete. If there are multiple versions of AnyConnect package for an operating system, select the package you want to delete from the list. The existing package disappears from the corresponding field.

Note Click **Cancel** to stop the delete operation and retain the existing package,

Step 4 Click **OK**. The device's **Configuration Status** is in 'Not Synced' state.

Note If you want to undo the delete action at this stage, go to **Inventory** page and click **Discard Changes** to retain the existing AnyConnect package.

Step 5 Preview and Deploy Configuration Changes for All Devices.

Configure Identity Sources for FDM-Managed Device

Identity Sources, such as Microsoft AD realms and RADIUS Servers, are AAA servers and databases that define user accounts for the people in your organization. You can use this information in a variety of ways, such as providing the user identity associated with an IP address, or authenticating remote access VPN connections or access to Cisco Defense Orchestrator.

Click **Objects > FDM Objects**, then click and choose **> RA VPN Objects (ASA & FTD)** > **Identity Source** to create your sources. You would then use these objects when you configure the services that require an identity source. You can apply appropriate filters to search existing sources and manage them.

Active Directory Realms

Active Directory provides user account and authentication information. When you deploy a configuration that includes an AD realm to an FDM-managed device, CDO fetches users and groups from the AD server.

You can use this source for the following purposes:

- Remote Access VPN, as a primary identity source. You can use AD in conjunction with a RADIUS server.
- Identity policy, for active authentication and as the user identity source used with passive authentication.
- Identity rule, for active authentication for a user.

You can create access control rules with user identities. See How to Implement an Identity Policy for more information.

CDO requests an updated list of user groups once every 24 hours. Because you can add a maximum of 50 users or groups to a rule, selecting groups usually makes more sense than selecting individual users. For example, you could create a rule allowing the Engineering group access to a development network, and create a subsequent rule that denies all other access to the network. Then, to make the rule apply to new engineers, you only need to add the engineer to the Engineering group in the directory server.

Active Directory Realms In CDO

You configure the AD realm when you create an AD Identity object. The identity source objects wizard assists in determining how to connect to the AD server and where the AD server is located in the network.

Note If you create an AD realm in CDO, CDO remembers the AD password when you create affiliate identity source objects and when you add those objects to an identity rule.

Active Directory Realms In FDM

You can point to AD realm objects that were created in FDM from the CDO objects wizard. Note that CDO does **not** read the AD password for AD realm objects that are created in FDM. You must manually enter the correct AD password in CDO.

To configure an AD realm in firewall device managers, see the **Configuring AD Identity Realms** section of the Reusable Objects chapters of the Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager for the version your device is running.

Supported Directory Servers

You can use AD on Windows Server 2008 and 2012.

Note the following about your server configuration:

- If you want to perform user control on user groups or on users within groups, you must configure user groups on the directory server. The system cannot perform user group control if the server organizes the users in a basic object hierarchy.
- The directory server must use the field names listed in the following table in order for the system to retrieve user metadata from the servers for that field:

Metadata	Active Directory Field
LDAP user name	samaccountname
First name	givename
Last Name	sn
email address	mail userprincipalname (if mail has no value)
Department	department distinguishedname (if department has no value)
Telephone number	telephonenumber

Determining the Directory Base DN

When you configure directory properties, you need to specify the common base Distinguished Name (DN) for users and groups. The base is defined in your directory server and differs from network to network. You must enter the correct bases for identity policies to work. If the base is wrong, the system cannot determine user or group names, and thus identity-based policies will be inoperable.

Note To get the correct bases, consult the administrator who is responsible for the directory servers.

For an active directory, you can determine the correct bases by logging into the AD server as a domain administrator, and using the **dsquery** command at a command prompt as follows to determine the bases:

User search base

Enter the **dsquery user** command with known username (partial or complete) to determine the base distinguished name. For example, the following command uses the partial name "John*" to return information for all users that start with "John."

C:\Users\Administrator>dsquery user -name "John*"

"CN=John Doe,CN=Users,DC=csc-lab,DC=example,DC=com"

The base DN would be "DC=csc-lab,DC=example,DC=com."

Group search base

Enter the **dsquery group** command with a known group name to determine the base DN. For example, the following command uses the group name Employees to return the distinguished name:

C:\>dsquery group -name "Employees"

"CN=Employees,CN=Users,DC=csc-lab,DC=example,DC=com"

The group base DN would be "DC=csc-lab,DC=example,DC=com."

You can also use the ADSI Edit program to browse the AD structure (**Start** > **Run** > **adsiedit.msc**). In ADSI Edit, right click any object, such as an organizational unit (OU), group, or user, and choose **Properties** to view the distinguished name. You can then copy the string of DC values as the base.

To verify that you have the correct base:

Procedure

Step 1 Click the **Test Connection** button in the directory properties to verify connectivity. Resolve any problems, and save the directory properties.

Step 2 Commit changes to the device.

Step 3 Create an access rule, select the **Users** tab, and try to add known user and group names from the directory. You should see auto-complete suggestions as you type for matching users and groups in the realm that contains the directory. If these suggestions appear in a drop-down list, then the system was able to query the directory successfully. If you see no suggestions, and you are certain the string you typed should appear in a user or group name, you need to correct the corresponding search base.

What to do next

See Create or Edit an Active Directory Realm Object for more information.

RADIUS Servers and Groups

You can use RADIUS servers to authenticate and authorize administration users.

When you configure a feature to use RADIUS servers, you select a RADIUS group instead of individual servers. A RADIUS group is a collection of RADIUS servers that are copies of each other. If a group has more than one server, they form a chain of backup servers to provide redundancy in case one server becomes unavailable. But even if you have only one server, you must create a one-member group to configure RADIUS support for a feature.

You can use this source for the following purposes:

- Remote Access VPN, as an identity source for authentication, and for authorization and accounting. You can use AD in conjunction with a RADIUS server.
- Identity policy, as a passive identity source to collect user identity from remote access VPN logins.

See Create or Edit a RADIUS Server Object or Group for more information.

Related Information:

- Create or Edit an Active Directory Realm Object
- Create or Edit a RADIUS Server Object or Group
- Configure Identity Policies

Create or Edit an Active Directory Realm Object

About Active Directory Realm Objects

When you create or edit an identity source object such as an AD realm object, Cisco Defense Orchestrator sends the configuration request to the FDM-managed devices through the SDC. The FDM-managed device then communicates with the configured AD realm.

Note that CDO does not read the Directory Password for AD realms that are configured through the firewall device manager console. If you use an AD realm object that was originally created in firewall device manager, you must manually enter the Directory Password.

Create an FTD Active Directory Realm Object

Use the following procedure to create an object:

Procedure

Step 1 In the CDO navigation bar on the left, click **Objects > FDM Objects**.

Step 2 Click  , then click **RA VPN Objects (ASA & FTD)** > **Identity Source**.

Step 3 Enter an **Object Name** for the object.

Step 4 Select the **Device Type** is as **FTD**.

Step 5 In the first part of the wizard, select **Active Directory Realm** as the **Identity Source Type**. Click **Continue**.

Step 6 Configure the basic realm properties.

- **Directory Username, Directory Password** - The distinguished username and password for a user with appropriate rights to the user information you want to retrieve. For AD, the user does not need elevated privileges. You can specify any user in the domain. The username must be fully qualified; for example, Administrator@example.com (not simply Administrator).

Note The system generates ldap-login-dn and ldap-login-password from this information. For example, Administrator@example.com is translated as cn=administrator,cn=users,dc=example,dc=com. Note that cn=users is always part of this translation, so you must configure the user you specify here under the common name "users" folder.

- **Base Distinguished Name** - The directory tree for searching or querying user and group information, that is, the common parent for users and groups. For example, cn=users,dc=example,dc=com.
- **AD Primary Domain** - The fully qualified AD domain name that the device should join. For example, example.com.

Step 7 Configure the directory server properties.

- **Hostname/IP Address** - The hostname or IP address of the directory server. If you use an encrypted connection to the server, you must enter the fully-qualified domain name, not the IP address.
- **Port** - The port number used for communications with the server. The default is 389. Use port 636 if you select LDAPS as the encryption method.
- **Encryption** - To use an encrypted connection for downloading user and group information, select the desired method,**STARTTLS** or **LDAPS**. The default is **None**, which means that user and group information is downloaded in clear text.
  - **STARTTLS** negotiates the encryption method and uses the strongest method supported by the directory server. Use port 389. This option is not supported if you use the realm for remote access VPN.
  - **LDAPS** requires LDAP over SSL. Use port 636.
- **Trusted CA Certificate** - If you select an encryption method, upload a Certificate Authority (CA) certificate to enable a trusted connection between the system and the directory server. If you are using a certificate to authenticate, the name of the server in the certificate must match the server Hostname / IP Address. For example, if you use 10.10.10.250 as the IP address but ad.example.com in the certificate, the connection fails.

Step 8 (Optional) Use the **Test** button to validate the configuration.

Step 9 (Optional) Click **Add another configuration** to add multiple AD servers to the AD realm. The AD servers need to be duplicates of each other and support the same AD domain. Therefore, the basic realm properties such as **Directory name**, **Directory Password**, and **Base Distinguished Name** must be the same across all AD servers associated with that AD realm.

Step 10 Click **Add**.

Step 11 Preview and Deploy Configuration Changes for All Devices now the changes you made, or wait and deploy multiple changes at once.

Edit an FTD Active Directory Realm Object

Note that you cannot change the Identity Source Type when editing an Identity source object. You must create a new object with the correct type.

Procedure

Step 1 In the CDO navigation bar on the left, click **Objects > FDM Objects**.

Step 2 Locate the object you want to edit by using object filters and search field.

Step 3 Select the object you want to edit.

Step 4 Click the edit icon in the **Actions** pane of the details panel.

Step 5 Edit the values in the dialog box in the same fashion that you created in the procedures above. Expand the configuration bar listed below to edit or test the hostname/IP address or encryption information.

Step 6 Click **Save**.

Step 7 CDO displays the policies that will be affected by the change. Click **Confirm** to finalize the change to the object and any policy affected by it.

Step 8 Preview and Deploy Configuration Changes for All Devices now the changes you made, or wait and deploy multiple changes at once.

Related Information:

- Create or Edit a RADIUS Server Object or Group
- Configure Identity Policies
- Configure Identity Rules
- Configure Identity Policy Settings

Create or Edit a RADIUS Server Object or Group

About RADIUS Server Objects or Groups

When you create or edit an identity source object such as a RADIUS server object or a group of RADIUS server objects, CDO sends the configuration request to the FDM-managed devices through the SDC. The FDM-managed device then communicates with the configured AD realm.

Create a RADIUS Server Object

RADIUS servers provide AAA (authentication, authorization, and accounting) services.

Use the following procedure to create an object:

Procedure

Step 1 In the CDO navigation bar on the left, click **Objects > FDM Objects**.

Step 2 Click , then click **RA VPN Objects (ASA & FTD)** > **Identity Source**.

Step 3 Enter an **Object name** for the object.

Step 4 For the **Device Type**, select **FTD**.

Step 5 For the **Identity Source** type, select **RADIUS Server**. Click **Continue**.

Step 6 Edit the Identity Source configuration with the following properties:

- **Server Name or IP Address** - The fully-qualified host name (FQDN) or IP address of the server.
- **Authentication Port** (Optional) - The port on which RADIUS authentication and authorization are performed. The default is 1812.
- **Timeout** - The length of time, 1-300 seconds, that the system waits for a response from the server before sending the request to the next server. The default is 10 seconds.
- Enter the **Server Secret Key**(Optional) - The shared secret that is used to encrypt data between the Firepower Threat Defense device and the RADIUS server. The key is a case-sensitive, alphanumeric string of up to 64 characters, with no spaces. The key must start with an alphanumeric character or an underscore, and it can contain the special characters: $ & - _ . + @. The string must match the one configured on the RADIUS server. If you do not configure a secret key, the connection is not encrypted.

Step 7 If you have Cisco Identity Services Engine (ISE) already configured for your network and are using the server for remote access VPN Change of Authorization configuration, click the **RA VPN Only** link and configure the following:

- **Redirect ACL** - Select the extended Access Control List (ACL) to use for the RA VPN redirect ACL. If you do not have an extended ACL you must create the required extended ACL object from a Smart CLI template in the FDM-managed device console. See the **Configuring Smart CLI Objects** section of the Advanced Configuration chapter of the Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager for the version your device is running. The purpose of the redirect ACL is to send initial traffic to ISE to assess the client posture. The ACL should send HTTPS traffic to ISE, but not traffic that is already destined for ISE, or traffic that is directed to a DNS server for name resolution. See the **Configure Change of Authorization** section of the Virtual Private Networks (VPN) chapter of the Cisco Firepower Threat Defense Configuration Guide for Firepower Device Managerfor the version your device is running.
- **Diagnostic Interface** -Enabling this option allows the system to always use the "Diagnostic" interface to communicate with the server. If you leave this disabled, CDO will default to using the routing table to determine the which interface to use.

Step 8 Click **Add**.

Step 9 Preview and Deploy Configuration Changes for All Devices now the changes you made, or wait and deploy multiple changes at once.

Create a RADIUS Server Group

A RADIUS server group contains one or more RADIUS server objects. The servers within a group must be copies of each other. These servers form a chain of backup servers, so that if the first server is unavailable, the system can try the next server in the list.

Use the following procedure to create an object group:

Procedure

Step 1 In the CDO navigation bar on the left, click **Objects > FDM Objects**.

Step 2 Click  , then click **FTD** > **Identity Source**.

Step 3 Enter an **Object name** for the object.

Step 4 Select the **Device Type** as **FTD**.

Step 5 Select **RADIUS Server Group** as the Identity Source Type. Click **Continue**.

Step 6 Edit the Identity Source configuration with the following properties:

- **Dead Time** - Failed servers are reactivated only after all servers have failed. The dead time is how long to wait after the last server fails before reactivating all servers.
- **Maximum Failed Attempts** - The number of failed requests (that is, requests that do not get a response) sent to a RADIUS server in the group before trying the next server. When the maximum number of failed attempts is exceeded, the system marks the server as Failed. For a given feature, if you configured a fallback method using the local database, and all the servers in the group fail to respond, then the group is considered to be unresponsive, and the fallback method is tried. The server group remains marked as unresponsive for the duration of the dead time, so that additional AAA requests within that period do not attempt to contact the server group, and the fallback method is used immediately.
- **Dynamic Authorization/Port** (Optional) - If you enable RADIUS dynamic authorization or change of authorization (CoA) services for this RADIUS server group, the group will be registered for CoA notification and listen on the specified port for CoA policy updates from Cisco Identity Services Engine (ISE). Enable dynamic authorization only if you are using this server group in a remote access VPN in conjunction with ISE.

Step 7 Select an AD realm that supported the RADIUS server from the drop-down menu. If you have not already created an AD realm, click **Create** from inside the drop-down menu.

Step 8 Click the **Add** button  to add existing RADIUS server objects. Optionally, you can create a new RADIUS server object from this window is necessary.

Note Add these objects in priority, as the first server in the list is used until it is unresponsive. FDM-managed device then defaults to the next server in the list.

Step 9 Preview and Deploy Configuration Changes for All Devices now the changes you made, or wait and deploy multiple changes at once.

Edit a Radius Server Object or Group

Use the following procedure to edit a Radius server object or Radius server group:

Procedure

Step 1 In the CDO navigation bar on the left, click **Objects > FDM Objects**.

Step 2 Locate the object you want to edit by using object filters and search field.

Step 3 Select the object you want to edit.

Step 4 Click the edit icon  in the **Actions** pane of the details panel.

Step 5 Edit the values in the dialog box in the same fashion that you created them in the procedures above. To edit or test the hostname/IP address or encryption information, expand the configuration bar.

Step 6 Click **Save**.

Step 7 CDO displays the policies that will be affected by the change. Click **Confirm** to finalize the change to the object and any policy affected by it.

Step 8 Preview and Deploy Configuration Changes for All Devices now the changes you made, or wait and deploy multiple changes at once.

Create New RA VPN Group Policies

A group policy is a set of user-oriented attribute/value pairs for remote access VPN connections. The connection profile uses a group policy that sets terms for user connections after the tunnel is established. Group policies let you apply whole sets of attributes to a user or a group of users, rather than having to specify each attribute individually for each user.

The system includes a default group policy named "DfltGrpPolicy". You can create additional group policies to provide the services you require.

Note You cannot add inconsistent group policy objects to RA VPN configuration. Resolve all inconsistencies before adding the group policy to the RA VPN Configuration.

Procedure

Step 1 In the Cisco Defense Orchestrator navigation bar on the left, click **Objects > FDM Objects**.

Step 2 Click the blue plus button.

Step 3 Click **RA VPN Objects (ASA & FTD)** > **RA VPN Group Policy**.

Step 4 Enter a name for the group policy. The name can be up to 64 characters and spaces are allowed.

Step 5 In the **Device Type** drop-down, select **FTD**.

Step 6 Do any of the following:

- Click the required tabs and configure the attributes on the page:
  - RA VPN Group Policy Attributes
  - AnyConnect Client Profiles, on page 254
  - Session Setting Attributes, on page 255
  - Address Assignment Attributes, on page 255
  - Split Tunneling Attributes, on page 256
  - AnyConnect Attributes, on page 257
  - Traffic Filters Attributes, on page 258
  - Windows Browser Proxy Attributes, on page 258

Step 7 Click **Save** to create the group policy.

RA VPN Group Policy Attributes

The general attributes of a group policy define the name of the group and some other basic settings. The Name attribute is the only required attribute.

- **DNS Server**: Select the DNS server group that defines the DNS servers clients should use for domain name resolution when connected to the VPN. If the group you need is not yet defined, click **Create DNS Group** and create it now.
- **Banner**: The banner text, or welcome message, to present to users at login. The default is no banner. The length can be up to 496 characters. The AnyConnect client supports partial HTML. To ensure that the banner displays properly to remote users, use the
 tag to indicate line breaks.
- **Default Domain**: The default domain name for users in the RA VPN. For example, example.com. This domain is added to hostnames that are not fully-qualified, for example, serverA instead of serverA.example.com.
- **AnyConnect Client Profiles**: Click + and select the AnyConnect Client Profiles to use for this group. See Upload RA VPN AnyConnect Client Profile. If you configure a fully-qualified domain name for the outside interface (in the connection profile), a default profile will be created for you. Alternatively, you can upload your client profile. Create these profiles using the Standalone AnyConnect Profile Editor, which you can download and install from software.cisco.com. If you do not select a client profile, the AnyConnect client uses default values for all options. The items in this list are AnyConnect Client Profile objects rather than the profiles themselves. You can create (and upload) new profiles by clicking **Create New AnyConnect Client Profile** in the drop-down list.

AnyConnect Client Profiles

This feature is supported on firewall device manager running software version 6.7 or later versions.

Cisco AnyConnect VPN client offers enhanced security through various built-in modules. These modules provide services such as web security, network visibility into endpoint flows, and off-network roaming protection. Each client module includes a client profile that includes a group of custom configurations as per your requirement.

You can select the AnyConnect VPN profile object and AnyConnect modules to be downloaded to clients when the VPN user downloads the VPN AnyConnect client software.

1. Choose or create an AnyConnect VPN profile object. See Upload RA VPN AnyConnect Client Profile, on page 270. Except for DART and Start Before Login modules, the AnyConnect VPN profile object must be selected.
2. Click **Add Any Connect Client Module**.

   The following AnyConnect modules are optional and you can configure these modules to be downloaded with VPN AnyConnect client software:

   - **AMP Enabler** — Deploys advanced malware protection (AMP) for endpoints.
   - **DART** — Captures a snapshot of system logs and other diagnostic information and creates a .zip file on your desktop so you can conveniently send troubleshooting information to Cisco TAC.
   - **Feedback** — Provides information about the features and modules customers have enabled and used.
   - **ISE Posture** — Uses the OPSWAT library to perform posture checks to assess an endpoint's compliance.

- **Network Access Manager** — Provides 802.1X (Layer 2) and device authentication to access both wired and wireless networks.
- **Network Visibility** — Enhances the enterprise administrator's ability to do capacity and service planning, auditing, compliance, and security analytics.
- **Start Before Login** — Forces the user to connect to the enterprise infrastructure over a VPN connection before logging on to Windows by starting AnyConnect before the Windows login dialog box appears.
- **Umbrella Roaming Security** — Provides DNS-layer security when no VPN is active.
- **Web Security** — Analyzes the elements of a web page, allows acceptable content, and blocks malicious or unacceptable content based on a defined security policy.

3. In the **Client Module** list, select an **AnyConnect module**.
4. In the **Profile** list, choose or create a profile object containing an AnyConnect Client Profile.
5. Select **Enable Module Download** to enable endpoints to download the client module along with the profile. If not selected, the endpoints can download only the client profile.

Session Setting Attributes

The session settings of a group policy control how long users can connect through the VPN and how many separate connections they can establish.

- **Maximum Connection Time**: The maximum length of time, in minutes, that users can stay connected to the VPN without logging out and reconnecting, from 1- 4473924 or blank. The default is unlimited (blank), but the idle timeout still applies.
- **Connection Time Alert Interval**: If you specify a maximum connection time, the alert interval defines the amount of time before the maximum time is reached to display a warning to the user about the upcoming automatic disconnect. The user can choose to end the connection and reconnect to restart the timer. The default is 1 minute. You can specify 1 to 30 minutes.
- **Idle Time**: The length of time, in minutes, that the VPN connection can be idle before it is automatically closed, from 1-35791394. If there is no communication activity on the connection for this consecutive number of minutes, the system stops the connection. The default is 30 minutes.
- **Idle Time Alert Interval**: The amount of time before the idle time is reached to display a warning to the user about the upcoming automatic disconnect due to an idle session. Any activity resets the timer. The default is 1 minute. You can specify 1 to 30 minutes.
- **Simultaneous Login Per User**: The maximum number of simultaneous connections allowed for a user. The default is 3. You can specify 1 to 2147483647 connections. Allowing many simultaneous connections might compromise security and affect performance.

Address Assignment Attributes

The address assignment attributes of a group policy define the IP address pool for the group. The pool defined here overrides the pool defined in any connection profile that uses this group. Leave these settings blank if you want to use the pool defined in the connection profile.

- **IPv4 Address Pool, IPv6 Address Pool**: These options define the address pools for the remote endpoints. Clients are assigned an address from these pools based on the IP version they use to make the VPN connection. Select a network object that defines a subnet for each IP type you want to support. Leave the list empty if you do not want to support that IP version. For example, you could define an IPv4 pool as 10.100.10.0/24. The address pool cannot be on the same subnet as the IP address for the outside interface. You can specify a list of up to six address pools to use for local address allocation. The order in which you specify the pools is significant. The system allocates addresses from these pools in the order in which the pools appear.
- **DHCP Scope**: If you configure DHCP servers for the address pool in the connection profile, the DHCP scope identifies the subnets to use for the pool for this group. The DHCP server must also have addresses in the same pool identified by the scope. The scope allows you to select a subset of the address pools defined in the DHCP server to use for this specific group. If you do not define a network scope, the DHCP server assigns IP addresses in the order of the address pools configured. It goes through the pools until it identifies an unassigned address. To specify a scope, select the network object that contains the network number host address. Click **Create New Network** if the object does not yet exist. For example, to tell the DHCP server to use addresses from the 192.168.5.0/24 subnet pool, select a network object that specifies 192.168.5.0 as a host address. You can use DHCP for IPv4 addressing only.

Split Tunneling Attributes

The split tunneling attributes of a group policy define how the system should handle traffic meant for the internal network vs. externally-directed traffic. Split tunneling directs some network traffic through the VPN tunnel (encrypted) and the remaining network traffic outside the VPN tunnel (unencrypted or in clear text).

- **IPv4 Split Tunneling**, **IPv6 Split Tunneling**: You can specify different options based on whether the traffic uses IPv4 or IPv6 addresses, but the options for each are the same. If you want to enable split tunneling, specify one of the options that require you to select network objects.
  - **Allow all traffic over tunnel**: Do no split tunneling. Once the user makes an RA VPN connection, all the user's traffic goes through the protected tunnel. This is the default. It is also considered the most secure option.
  - **Allow specified traffic over the tunnel**: Select the network objects that define destination network and host addresses. Any traffic to these destinations goes through the protected tunnel. The client routes traffic to any other destination to connections outside the tunnel (such as a local Wi-Fi or network connection).
  - **Exclude networks specified below**: Select the network objects that define destination network or host addresses. The client routes any traffic to these destinations to connections outside the tunnel. Traffic to any other destination goes through the tunnel.
- **Split DNS** - You can configure the system to send some DNS requests through the secure connection while allowing the client to send other DNS requests to the DNS servers configured on the client. You can configure the following DNS behavior:
  - **Send DNS Request as per split tunnel policy**: With this option, DNS requests are handled the same way as the split tunnel options are defined. If you enable split tunneling, DNS requests are sent based on the destination addresses. If you do not enable split tunneling, all DNS requests go over the protected connection.
  - **Always send DNS requests over tunnel**: Select this option if you enable split tunneling, but you want all DNS requests sent through the protected connection to the DNS servers defined for the group.

- **Send only specified domains over tunnel**: Select this option if you want your protected DNS servers to resolve addresses for certain domains only. Then, specify those domains, separating domain names with commas. For example, example.com, example1.com. Use this option if you want your internal DNS servers to resolve names for internal domains, while external DNS servers handle all other Internet traffic.

AnyConnect Attributes

The AnyConnect attributes of a group policy define some SSL and connection settings used by the AnyConnect client for a remote access VPN connection.

- **SSL Settings**
  - **Enable Datagram Transport Layer Security (DTLS)**: Whether to allow the AnyConnect client to use two simultaneous tunnels: an SSL tunnel and a DTLS tunnel. Using DTLS avoids latency and bandwidth problems associated with some SSL connections and improves the performance of real-time applications that are sensitive to packet delays. If you do not enable DTLS, AnyConnect client users establishing SSL VPN connections connect with an SSL tunnel only.
  - **DTLS Compression**: Whether to compress Datagram Transport Layer Security (DTLS) connections for this group using LZS. DTLS Compression is disabled by default.
  - **SSL Compression**: Whether to enable data compression, and if so, the method of data compression to use, **Deflate**, or **LZS**. SSL Compression is **Disabled** by default. Data compression speeds up transmission rates but also increases the memory requirement and CPU usage for each user session. Therefore, SSL compression decreases the overall throughput of the device.
  - **SSL Rekey Method**, **SSL Rekey Interval**: The client can rekey the VPN connection, renegotiating the crypto keys and initialization vectors, to increase the security of the connection. Disable rekeying by selecting **None**. To enable rekey, select **New Tunnel** to create a new tunnel each time. (The **Existing Tunnel** option results in the same action as **New Tunnel**.) If you enable rekeying, also set the rekey interval, which is 4 minutes by default. You can set the interval to 4-10080 minutes (1 week).

- **Connection Settings**
  - **Ignore the DF (Don't Fragment) bit**: Whether to ignore the Don't Fragment (DF) bit in packets that need fragmentation. Select this option to allow the forced fragmentation of packets that have the DF bit set, so that these packets can pass through the tunnel.
  - **Client Bypass Protocol** - Allows you to configure how the secure gateway manages IPv4 traffic (when it is expecting only IPv6 traffic), or how it manages IPv6 traffic (when it is expecting only IPv4 traffic).

    When the AnyConnect client makes a VPN connection to the headend, the headend assigns it an IPv4, IPv6, or both an IPv4 and IPv6 address. If the headend assigns the AnyConnect connection only an IPv4 address or only an IPv6 address, you can configure the Client Bypass Protocol to drop network traffic for which the headend did not assign an IP address (default, disabled, not checked), or allow that traffic to bypass the headend and be sent from the client unencrypted or "in the clear" (enabled, checked).

    For example, assume that the secure gateway assigns only an IPv4 address to an AnyConnect connection and the endpoint is dual-stacked. When the endpoint attempts to reach an IPv6 address,

if Client Bypass Protocol is disabled, the IPv6 traffic is dropped; however, if Client Bypass Protocol is enabled, the IPv6 traffic is sent from the client in the clear.

- **MTU**: The maximum transmission unit (MTU) size for SSL VPN connections established by the Cisco AnyConnect VPN Client. The default is 1406 bytes. The range is 576 to 1462 bytes.
  - **Keepalive Messages Between AnyConnect and VPN Gateway**: Whether to exchange keepalive messages between peers to demonstrate that they are available to send and receive data in the tunnel. Keepalive messages transmit at set intervals. The default interval is 20 seconds, and the valid range is 15 to 600 seconds.
  - **DPD on Gateway Side Interval**, **DPD on Client Side Interval**: Enable Dead Peer Detection (DPD) to ensure that the VPN gateway or VPN client quickly detects when the peer is no longer responding. You can separately enable gateway or client DPD. The default interval is 30 seconds for sending DPD messages. The interval can be 5-3600 seconds.

Traffic Filters Attributes

The traffic filter attributes of a group policy define restrictions you want to place on users assigned to the group. You can use these attributes instead of creating access control policy rules to restrict RA VPN users to specific resources, based on host or subnet address and protocol, or VLAN. By default, RA VPN users are not restricted by the group policy from accessing any destination on your protected network.

- **Access List Filter**: Restrict access using an extended access control list (ACL). Select the Smart CLI Extended ACL object. The extended ACL lets you filter based on source address, a destination address, and protocol (such as IP or TCP). ACLs are evaluated on a top-down, first-match basis, so ensure that you place specific rules before more general rules. There is an implicit "deny any" at the end of the ACL, so if you intend to deny access to a few subnets while allowing all other access, ensure that you include a "permit any" rule at the end of the ACL. Because you cannot create network objects while editing an extended ACL Smart CLI object, you should create the ACL before editing the group policy. Otherwise, you might need to simply create the object, then go back later to create the network objects and then all the access control entries that you need. To create the ACL, log in to firewall device manager, go to **Device** > **Advanced Configuration** > **Smart CLI** > **Objects**, create an object, and select **Extended Access List** as the object type.
- **Restrict VPN to VLAN**: Also called "VLAN mapping," this attribute specifies the egress VLAN interface for sessions to which this group policy applies. The system forwards all traffic from this group to the selected VLAN. Use this attribute to assign a VLAN to the group policy to simplify access control. Assigning a value to this attribute is an alternative to using an ACL to filter traffic on a session. Ensure that you specify a VLAN number that is defined on a subinterface on the device. Values range from 1 to 4094.

Windows Browser Proxy Attributes

The Windows browser proxy attributes of a group policy determine how, and whether, a proxy defined on the user's browser operates.

You can select one of the following values for **Browser Proxy During VPN Session**:

- **No change in endpoint settings**: Allow the user to configure (or not configure) a browser proxy for HTTP and use the proxy if it is configured.

- **Disable browser proxy**: Do not use the proxy defined for the browser, if any. No browser connections will go through the proxy.
- **Auto detect settings**: Enable the use of automatic proxy server detection in the browser for the client device.
- **Use custom settings**: Define a proxy that should be used by all client devices for HTTP traffic. Configure the following settings:
  - **Proxy Server IP or Hostname**, **Port**: The IP address, or hostname, of the proxy server, and the port used for proxy connections by the proxy server. The host and port combined cannot exceed 100 characters.
  - **Browser Proxy Exemption List**: Connections to the hosts/ports in the exemption list do not go through the proxy. Add all the host/port values for destinations that should not use the proxy. For example, www.example.com port 80. Click **Add proxy exemption** to add items to the list. Click the trash can icon to delete items. The entire proxy exception list, combining all addresses and ports, cannot be longer than 255 characters.

Create an RA VPN Configuration

CDO allows you to add one or more FDM-managed devices to the RA VPN configuration wizard and configure the VPN interfaces, access control, and NAT exemption settings associated with the devices. Therefore, each RA VPN configuration can have connection profiles and group policies shared across multiple FDM-managed devices that are associated with the RA VPN configuration. Further, you can enhance the configuration by creating connection profiles and group policies.

You can either onboard an FDM-managed device that has already been configured with RA VPN settings or a new device without RA VPN settings. When you onboard an FDM-managed device that already has RA VPN settings, CDO automatically creates a "Default RA VPN Configuration" and associates the FDM-managed device with this configuration. Also, this default configuration can contain all the connection profile objects that are defined on the device.

Important

- You are not allowed to add ASA and FDM-managed device in the same Remote Access VPN Configuration.
- An FDM-managed device can't have more than one RA VPN Configuration.

Prerequisites

Before adding the FDM-managed devices to RA VPN configuration, the following prerequisites must be met:

- Make sure that the FDM-managed devices have the following:
  - A valid license. For more information, see Licensing Requirements for Remote Access VPN.
  - For FDM Version 6.4.0, ensure that a minimum of one AnyConnect software package pre-uploaded to the device. For more information, see Upgrade AnyConnect Package on an FDM-Managed Device Running Version 6.4.0.
  - For FDM Version 6.5.0 and later, you can upload AnyConnect package using CDO. For more information, see Upload AnyConnect Software Packages to an FDM-Managed Device Running Version 6.5 or Later.

- There are no configuration deployments pending.

- FDM changes are synchronized to CDO.
  1. In the CDO navigation bar at the left, click **Inventory** and search for one or more FDM-managed devices to be synchronized.
  2. Select one or more devices and then click **Check for changes**. CDO communicates with one or more FDM-managed devices to synchronize the changes.

- RA VPN configuration group policy objects are consistent.
  - Ensure that all inconsistent group policy objects are resolved as they cannot be added to the RA VPN configuration. Either address the issue or remove inconsistent group policy objects from the **Objects** page. For more information see, Resolve Duplicate Object Issues and Resolve Inconsistent Object Issues.

- RA VPN group policies of the FDM-managed device match RA VPN configuration group policies.

Procedure

Procedure

Step 1 In the Cisco Defense Orchestrator navigation bar at the left, click **VPN** > **Remote Access VPN Configuration**.

Step 2 Click the blue plus button to create a new RA VPN configuration.

Step 3 Enter a name for the Remote Access VPN configuration.

Step 4 Click the blue plus button to add FDM-managed devices to the configuration. You can add the device details and configure network traffic-related permissions that are associated with the device.

a. Provide the following device details:

- **Device**: Select an FDM-managed device that you want to add and click **Select**.

  Important You are not allowed to add ASA and FDM-managed device in the same Remote Access VPN Configuration.

- **Certificate of Device Identity**: Select the internal certificate used for establishing the identity of the device. This establishes the device identity for AnyConnect clients when they make a connection to the device. Clients must accept this certificate to complete a secure VPN connection. If you do not already have a certificate, click **Create New Internal Certificate** in the drop-down list. See Generating Self-Signed Internal and Internal CA Certificates.

- **Outside Interface**: The interface to which users connect when making the remote access VPN connection. Although this is normally the outside (internet-facing) interface, choose whichever interface is between the device and the end-users you are supporting with this connection profile. To create a new subinterface, see Configure Firepower VLAN Subinterfaces and 802.1Q Trunking.

- **Fully Qualified Domain Name or IP for the Outside Interface**: The name of the interface, for example, ravpn.example.com or the IP address must be provided. If you specify a name, the system can create a client profile for you. **Note**: You are responsible for ensuring that the DNS servers used

in the VPN and by clients can resolve this name to the outside interface's IP address. Add the FQDN to the relevant DNS servers.

b. Click **Continue** to configure the traffic permissions.

- **Bypass Access Control policy for decrypted traffic (sysopt permit-vpn)**: Decrypted traffic is subjected to Access Control Policy inspection by default. Enabling this option bypasses the decrypted traffic option bypasses the access control policy inspection, but the VPN Filter ACL and the authorization ACL downloaded from the AAA server are still applied to VPN traffic. Note that if you select this option, the system configures the sysopt connection permit-vpn command, which is a global setting. This will also impact the behavior of site-to-site VPN connections. If you do not select this option, it might be possible for external users to spoof IP addresses in your remote access VPN address pool, and thus gain access to your network. This can happen because you will need to create access control rules that allow your address pool to have access to internal resources. If you use access control rules, consider using user specifications to control access, rather than source IP address alone. The downside of selecting this option is that the VPN traffic will not be inspected, which means that intrusion and file protection, URL filtering, or other advanced features will not be applied to the traffic. This also means that no connection events will be generated for the traffic, and thus statistical dashboards will not reflect VPN connections.
- **NAT Exempt**: Enable NAT Exempt to exempt traffic to and from the remote access VPN endpoints from NAT translation. If you do not exempt VPN traffic from NAT, ensure that the existing NAT rules for the outside and inside interfaces do not apply to the RA VPN pool of addresses. NAT exempt rules are manual static identity NAT rules for a given source/destination interface and network combination, but they are not reflected in the NAT policy, they are hidden. If you enable NAT Exempt, you must also configure the following.
  - **Inside Interfaces**: Select the interfaces for the internal networks remote users will be accessing. NAT rules are created for these interfaces.
  - **Inside Networks**: Select the network objects that represent internal networks remote users will be accessing. The networks list must contain the same IP types as the address pools you are supporting.

Step 5 Click **OK**.

- If you have onboarded an firewall device manager Version 6.4.0 device, the **AnyConnect Packages Detected** shows the AnyConnect packages available in the device.
- If you have onboarded an firewall device manager Version 6.5.0 or later device, you must add the AnyConnect packages from the server where the AnyConnect packages are pre-uploaded. See Upload AnyConnect Software Packages to an FDM-Managed Device Running Version 6.5 or Later for instructions.

Step 6 Click **OK**. The device is added to the configuration.

What to do next

Note Select a configuration and under **Actions**, click the appropriate action:

- **Group Policies** to add or remove group policies.
  - Click + to select the required group policies. To create a new RA VPN group policy, see Create New RA VPN Group Policies.
- **Remove** to delete the selected RA VPN configuration.

Modify RA VPN Configuration

You can modify the name and the device details of an existing RA VPN configuration.

Procedure

Select the configuration to be modified and under **Actions**, click **Edit**.

- Modify the name if required.
- Click the blue plus  button to add a new device
- Click to perform the following on the FDM-managed device.
  - Click **Edit** to modify the existing RA VPN configuration.
  - Click **Remove** to remove the FDM-managed device from the RA VPN configuration. All connection profiles and RA VPN settings associated with that device except the group policies are deleted. You can remove the group policies explicitly from the objects page. **Note**: You cannot remove the FDM-managed device if that is the only device using the configuration. Alternatively, you can remove the RA VPN configuration.

You can also search for remote access VPN configuration by typing the name of the configuration or device.

Related Information:

- Configure an RA VPN Connection Profile.
- Preview and Deploy Configuration Changes for All Devices.
- Allow Traffic Through the Remote Access VPN.

Configure an RA VPN Connection Profile

An RA VPN connection profile defines the characteristics that allow external users to create a VPN connection to the system using the AnyConnect client. Each profile defines the AAA servers and certificates used for authenticating users, the address pool for assigning users IP addresses, and the group policies that define various user-oriented attributes.

You can create multiple profiles within the RA VPN configuration if you need to provide variable services to different user groups, or if you have various authentication sources. For example, if your organization merges with a different organization that uses different authentication servers, you can create a profile for the new group that uses those authentication servers.

An RA VPN connection profile allows your users to connect to your inside networks when they are on external networks, such as their home network. Create separate profiles to accommodate different authentication methods.

Before you begin

Before configuring the remote access (RA) VPN connection:

- The outside interface, the one that terminates remote access VPN connections, cannot also have a management access list that allows HTTPS connections. Delete any HTTPS rules from the outside interface before configuring RA VPN. See the "Configuring the Management Access List" section in the "System Settings" chapter of Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager, Version X.Y.
- Create an RA VPN configuration. See Create an RA VPN Configuration.

Procedure

Procedure

Step 1 On the CDO navigation pane, click **VPN** > **Remote Access VPN Configuration**. You can click a VPN configuration to view the summary information on how many connection profiles and group policies are currently configured.

Step 2 Click the connection profile and under **Actions** in the sidebar at the right, click **Add Connection Profile**.

Step 3 Configure the basic connection attributes.

- **Connection Profile Name**: The name for this connection, up to 50 characters without spaces. For example, MainOffice.

  Note The name you enter here is what users will see in the connection list in the AnyConnect client. Choose a name that will make sense to your users.

- **Group Alias, Group URL**: Aliases contain alternate names or URLs for a specific connection profile. VPN users can choose an alias name in the AnyConnect client in the list of connections when they connect to the FDM-managed device. The connection profile name is automatically added as a group alias. You can also configure the list of group URLs, which your endpoints can select while initiating the Remote Access VPN connection. If users connect using the group URL, the system will automatically use the connection profile that matches the URL. This URL would be used by clients who do not yet have the AnyConnect client installed. Add as many group aliases and URLs as required. These aliases and URLs must be unique across all connection profiles defined on the device. Group URLs must start with **https://**.
- For example, you might have the alias Contractor and the group URLhttps://ravpn.example.com/contractor. Once the AnyConnect client is installed, the user would simply select the group alias in the AnyConnect VPN drop-down list of connections.

Step 4 Configure the primary and optionally, secondary identity sources. These options determine how remote users authenticate to the device to enable the remote access VPN connection. The simplest approach is to use AAA only and then select an AD realm or use the LocalIdentitySource. You can use the following approaches for **Authentication Type**:

- **AAA Only**: Authenticate and authorize users based on username and password. For details, see Configure AAA for a Connection Profile.

- **Client Certificate Only**: Authenticate users based on client device identity certificate. For details, see Configure Certificate Authentication for a Connection Profile.
- **AAA and ClientCertificate**: Use both username/password and client device identity certificate.

Step 5 Configure the address pool for clients. The address pool defines the IP addresses that the system can assign to remote clients when they establish a VPN connection. For more information, see Configure Client Address Pool Assignment.

Step 6 Click **Continue**.

Step 7 Select the **Group Policy** to use for this profile from the list and click **Select**. The group policy sets terms for user connections after the tunnel is established. The system includes a default group policy named DfltGrpPolicy. You can create additional group policies to provide the services you require.

Note If the group policy you need does not yet exist, create the group policy on the **Objects** page and then associate the policy to the RA VPN configuration. For detailed information about group policies, see Create New RA VPN Group Policies.

Step 8 Click **Continue**.

Step 9 Review the summary. First, verify that the summary is correct. You can see what end-users need to do to initially install the AnyConnect software and test that they can complete a VPN connection. Click  to copy the instructions to the clipboard, and then distribute them to your users.

Step 10 Click **Done**.

What to do next

Ensure that traffic is allowed in the VPN tunnel, as explained in Allow Traffic Through the Remote Access VPN.

Configure AAA for a Connection Profile

Authentication, Authorization, and Accounting (AAA) servers use username and password to determine if a user is allowed access to the remote access VPN. If you use RADIUS servers, you can distinguish authorization levels among authenticated users, to provide differential access to protected resources. You can also use RADIUS accounting services to keep track of usage.

When configuring AAA, you must configure a primary identity source. Secondary and fallback sources are optional. Use a secondary source if you want to implement dual authentication, for example, using RSA tokens or DUO.

Primary Identity Source Options

- **Primary Identity Source for User Authentication**: The primary identity source used for authenticating remote users. End users must be defined in this source or the optional fallback source to complete a VPN connection. Select one of the following:
  - An Active Directory (AD) identity realm. If the realm you need does not yet exist, click **Create New Identity Realm**.
  - A RADIUS server group.

    - LocalIdentitySource (the local user database): You can define users directly on the device and not use an external server.

- **Fallback Local Identity Source**: If the primary source is an external server, you can select the LocalIdentitySource as a fallback in case the primary server is unavailable. If you use the local database as a fallback source, ensure that you define the same local usernames/passwords as the ones defined in the external server.
- **Strip options**: A realm is an administrative domain. Enabling the following options allows the authentication to be based on the username alone. You can enable any combination of these options. However, you must select both check boxes if your server cannot parse delimiters.
    - **Strip Identity Source Server from Username**: Whether to remove the identity source name from the username before passing the username on to the AAA server. For example, if you select this option and the user enters domain\username as the username, the domain is stripped off from the username and sent to AAA server for authentication. By default, this option is unchecked.
    - **Strip Group from Username**: Whether to remove the group name from the username before passing the username on to the AAA server. This option applies to names given in the username@domain format; the option strips the domain and @ sign. By default, this option is unchecked.

Secondary Identity Source

- **Secondary Identity Source for User Authorization**: The optional second identity source. If the user successfully authenticates with the primary source, the user is prompted to authenticate with the secondary source. You can select an AD realm, RADIUS server group, or the local identity source.
- **Advanced options**: Click the **Advanced** link and configure the following options:
    - **Fallback Local Identity Source for Secondary**: If the secondary source is an external server, you can select the LocalIdentitySource as a fallback in case the secondary server is unavailable. If you use the local database as a fallback source, ensure that you define the same local usernames/passwords as the ones defined in the secondary external server.
    - **Use Primary Username for Secondary Login**: By default, when using a secondary identity source, the system will prompt for both username and password for the secondary source. If you select this option, the system prompts for the secondary password only and uses the same username for the secondary source that was authenticated against the primary identity source. Select this option if you configure the same usernames in both the primary and secondary identity sources.
        - **Username for Session Server**: After successful authentication, the username is shown in events and statistical dashboards, is used for determining matches for a user- or group-based SSL decryption and access control rules and is used for accounting. Because you are using two authentication sources, you need to tell the system whether to use the Primary or Secondary username as the user identity. By default, the primary name is used.
        - **Password Type**: How to obtain the password for the secondary server. The default is **Prompt**, which means the user is asked to enter the password. Select **Primary Identity Source Password** to automatically use the password entered when the user authenticated to the primary server. Select **Common Password** to use the same password for every user, then enter that password in the **Common Password** field.
    - **Authorization Server**: The RADIUS server group that has been configured to authorize remote access, VPN users. After authentication is complete, authorization controls the services and commands

available to each authenticated user. Authorization works by assembling a set of attributes that describe what the user is authorized to perform, their actual capabilities, and restrictions. Were you not to use authorization, authentication alone would provide the same access to all authenticated users. For information on configuring RADIUS for authorization, see Control User Permissions and Attributes Using RADIUS and Group Policies. Note that if the system obtains authorization attributes from the RADIUS server that overlap those defined in the group policy, the RADIUS attributes override the group policy attributes.

- **Accounting Server**: (Optional.) The RADIUS server group to use to account for the remote access VPN session. Accounting tracks the services users are accessing as well as the number of network resources they are consuming. The FDM-managed device reports user activity to the RADIUS server. Accounting information includes when sessions start and stop, usernames, the number of bytes that pass through the device for each session, the service used, and the duration of each session. You can then analyze the data for network management, client billing, or auditing. You can use accounting alone or together with authentication and authorization.

Configure Certificate Authentication for a Connection Profile

Note This section is not applicable for **Authentication Type** as **AAA Only**.

You can use certificates installed on the client device to authenticate remote access VPN connections.

When using client certificates, you can still configure a secondary identity source, fallback source, and authorization and accounting servers. These are AAA options; for details, see Configure an RA VPN Connection Profile.

Following are the certificate-specific attributes. You can configure these attributes separately for primary and secondary identity sources. Configuring a secondary source is optional.

- **Username from Certificate**: Select one of the following:
  - **Map Specific Field**: Use the certificate elements in the order of **Primary Field** and **Secondary Field**. The defaults are CN (Common Name) and OU (Organizational Unit). Select the options that work for your organization. The fields are combined to provide the username, and this is the name used in events, dashboards, and for matching purposes in SSL decryption and access control rules.
  - **Use entire DN (distinguished name) as username**: The system automatically derives the username from the DN fields. •
- **Advanced options** (not applicable for **Authentication Type** as **Client Certificate Only**): Click the **Advanced** link and configure the following options:
  - **Prefill username from certificate on user login window**: Whether to fill in the username field with the retrieved username when prompting the user to authenticate.
  - **Hide username in login window**: If you select the **Prefill** option, you can hide the username, which means the user cannot edit the username in the password prompt.

Configure Client Address Pool Assignment

There must be a way for the system to provide an IP address to endpoints that connect to the remote access VPN. The AAA server can provide these addresses, a DHCP server, an IP address pool configured in the group policy, or an IP address pool configured in the connection profile. The system tries these resources in that order and stops when it obtains an available address, which it then assigns to the client. Thus, you can configure multiple options to create a failsafe in case of an unusual number of concurrent connections.

Use one or more of the following methods to configure the address pool for a connection profile.

- **IPv4 Address Pool** and **IPv4 Address Pool**: First, create up to six network objects that specify subnets. You can configure separate pools for IPv4 and IPv6. Then, select these objects in the **IPv4 Address Pool** and **IPv6 Address Pool** options, either in the group policy or in the connection profile. You do not need to configure both IPv4 and IPv6, configure the addressing scheme you want to support. You also do not need to configure the pool in both the group policy and the connection profile. The group policy overrides the connection profile settings, so if you configure the pools in the group policy, leave the options empty in the connection profile. Note that the pools are used in the order in which you list them.
- **DHCP Servers**: First, configure a DHCP server with one or more IPv4 address ranges for the RA VPN (you cannot configure IPv6 pools using DHCP). Then, create a host network object with the IP address of the DHCP server. You can then select this object in the **DHCP Servers** attribute of the connection profile. You can configure more than one DHCP server. If the DHCP server has multiple address pools, you can use the **DHCP Scope** attribute in the group policy that you attach to the connection profile to select which pool to use. Create a host network object with the network address of the pool. For example, if the DHCP pool contains 192.168.15.0/24 and 192.168.16.0/24, setting the DHCP scope to 192.168.16.0 will ensure that an address from the 192.168.16.0/24 subnet will be selected.

Allow Traffic Through the Remote Access VPN

You can use one of the following techniques to enable traffic flow in the remote access VPN tunnel.

- Configure the **sysopt connection permit-vpn** command, which exempts traffic that matches the VPN connection from the access control policy. The default for this command is **no sysopt connection permit-vpn**, which means VPN traffic must also be allowed by the access control policy. This is the more secure method to allow traffic in the VPN because external users cannot spoof IP addresses in the remote access VPN address pool. The downside is that the VPN traffic will not be inspected, which means that intrusion and file protection, URL filtering, or other advanced features will not be applied to the traffic. This also means that no connection events will be generated for the traffic, and thus statistical dashboards will not reflect VPN connections. To configure this command, select the **Bypass Access Control policy for decrypted traffic** option in your RA VPN Configuration. See Create an RA VPN Configuration.
- Create access control rules to allow connections from the remote access VPN address pool. This method ensures that VPN traffic is inspected, and advanced services can be applied to the connections. The downside is that it opens the possibility for external users to spoof IP addresses and thus gain access to your internal network. See Configure the FDM Access Control Policy.

Upgrade AnyConnect Package on an FDM-Managed Device Running Version 6.4.0

You can use Cisco Defense Orchestrator to upgrade the AnyConnect package available on an FDM-managed device so that it can be distributed to RA VPN users.

The following are the major steps that are involved in upgrading the AnyConnect package:

Procedure

Step 1 Use firewall device manager to remove the AnyConnect package and upload a later version of the package. Use one of these methods to accomplish this task.

- Remove the old package and upload the new package from the firewall device manager UI.
- Remove the old package and upload the new package from the firewall device manager API explorer.

Step 2 Deploy firewall device manager changes to device.

Step 3 Read the new configuration information into CDO.

Step 4 Verify the new package in the RA VPN connection profile.

Prerequisites

- A minimum of one RA VPN configuration with connection profile is already deployed to FDM-managed device.
- Download the AnyConnect package that you want from https://software.cisco.com/download/home/283000185. Cisco recommends upgrading to the latest available package.

Upload your desired AnyConnect Package to Secure Firewall Threat Defense using Firewall Device Manager

Procedure

Step 1 Using a browser, open the home page of the system. For example, https://ftd.example.com.

Step 2 Log into Firewall Device Manager.

Step 3 Click **View Configuration** in the **Device** > **Remote Access VPN** group. The group shows summary information on how many connection profiles and group policies are currently configured.

Step 4 Click the view ( ) button (**View** configuration button.) to open a summary of the connection profile and connection instructions.

Note You can edit any one of the connection profiles to upload the AnyConnect package to the FDM-managed device.

Step 5 Click the **Edit** button to make changes.

Step 6 Click **Next** until the **Global Settings** screen appears. The **AnyConnect Package** shows AnyConnect packages available on the FDM-managed device.

Step 7 Click 'X' button to remove the AnyConnect package which you want to replace.

Step 8 Click **Upload Package** and then click the OS that you want for uploading the compatible package.

Step 9 Select the package and click **Open**. You can see the package being uploaded on the Firewall device manager UI.

Step 10 Click **Finish**. The configuration is saved.

Note Alternatively, you can use the Firewall device manager API explorer to remove and upload a new AnyConnect package.

a. Edit the URL to point to /#/api-explorer, for example, https://ftd.example.com/#/api-explorer.

b. Delete a package from the FDM-managed device, click **AnyConnectPackageFile** > **Delete**. In the **objID** field, type the package id and click **TRY IT OUT!**.

c. Upload a new package by performing the steps that are described in the Upload AnyConnect Software Packages to an FDM-Managed Device Running Version 6.4.0 section.

Step 11 Click the **Deploy Changes** icon in the upper right of the web page. The icon is highlighted with a dot when there are undeployed changes.

Step 12 If you are satisfied with the changes, you can click **Deploy Now** to start the job immediately. The window shows that the deployment is in progress. You can close the window, or wait for the deployment to complete.

Verify the new package is referenced in the RA VPN connection profile

Procedure

Step 1 In the CDO navigation bar at the left, click **Inventory**.

Step 2 Click the **Devices** tab.

Step 3 Click the **FTD** tab and select the FDM-managed device which has the upgraded AnyConnect package. This device would be reporting conflict.

Step 4 Accept the Out-of-band changes to overwrite the configuration **and any pending changes stored on CDO** with the device's running configuration. For more information, see Resolve the Conflict Detected Status

Step 5 View the new AnyConnect package by performing the following:

- Click **VPN** > **Remote Access VPN**.
- Click the RA VPN configuration that is associated with this FDM-managed device.

- Click **Edit** under **Actions**. The new package is displayed under **Devices**.

Upload RA VPN AnyConnect Client Profile

The Remote Access VPN AnyConnect Client Profile is a group of configuration parameters stored in a file. There are different AnyConnect client profiles containing configuration settings for the core client VPN functionality and for the optional client modules Network Access Manager, AMP Enabler, ISE posture, Network Visibility, Customer Feedback Experience profiles, Umbrella roaming security, and Web Security.

CDO allows uploading of these profiles as objects which can be used in the group policy later.

- **AnyConnect VPN Profile** — AnyConnect client profiles are downloaded to clients along with the VPN AnyConnect client software. These profiles define many client-related options, such as auto-connect on startup and auto-reconnect, and whether the end-user can change the option from the AnyConnect client preferences and advanced settings. CDO supports the XML file format.
- **AMP Enabler Service Profile** — The profile is used for the AnyConnect AMP Enabler. The AMP Enabler and this profile are pushed to the endpoints from FDM-managed device when a remote access VPN user connects to the VPN. CDO supports XML and ASP file formats.
- **Feedback Profile** — You can add a Customer Experience Feedback profile and select this type to receive information about the features and modules customers have enabled and used. CDO supports the FSP file format.
- **ISE Posture Profile** — Choose this option if you add a profile file for the AnyConnect ISE Posture module. CDO supports XML and ISP file formats.
- **Network Access Manager Service Profile** — Configure and add the NAM profile file using the Network Access Manager profile editor. CDO supports XML and NSP file formats.
- **Network Visibility Service Profile** — Profile file for AnyConnect Network Visibility module. You can create the profile using the NVM profile editor. CDO supports XML and NVMSP file formats.
- **Umbrella Roaming Security Profile** — You must select this file type if you deploy the Umbrella Roaming Security module. CDO supports XML and JSON file formats.
- **Web Security Service Profile** — Select this file type when you add a profile file for the Web security module. CDO supports XML, WSO, and WSP file formats.

Before you begin

Use the suitable GUI-based AnyConnect profile editors to create the profiles you need. You can download the profile editors from Cisco Software Download Center in the AnyConnect Secure Mobility Client category and install the AnyConnect "Profile Editor - Windows / Standalone installer (MSI)." The profile editor installer contains stand-alone versions of the profile editors. The installation file is for Windows only and has the file name anyconnect-profileeditor-win-<version>-k9.msi, where <version> is the AnyConnect version. For example, anyconnect-profileeditor-win-4.3.04027-k9.msi. You must also install Java JRE 1.6 (or higher) before installing the profile editor.

Except for the Umbrella Roaming Security profile editor, this package contains all the profile editors required for creating the modules. For detailed information, see the *AnyConnect Profile Editor* chapter in the appropriate release of the Cisco AnyConnect Secure Mobility Client Administrator Guide for details. Download the Umbrella Roaming Security profile separately from the Umbrella dashboard. For detailed information, see

the "Download the AnyConnect Roaming Security Profile from the Umbrella Dashboard" section of the "Umbrella Roaming Security" chapter in the Cisco Umbrella User Guide.

Procedure

Step 1 In the CDO navigation bar at the left, click **Objects** > **FDM Objects**.

Step 2 Click the blue plus button.

Step 3 Click **RA VPN Objects (ASA & FDM)** > **AnyConnect Client Profile**.

Step 4 In the **Object Name** field, enter a name for the AnyConnect client profile.

Step 5 Click **Browse** and select the file you created using the Profile Editor.

Step 6 Click **Open** to upload the profile.

Step 7 Click **Add** to add the object.

Related information:

- Associate the client modules with the AnyConnect VPN profile in the RA VPN group policies window. See Create New RA VPN Group Policies.

Note The client module association is supported by all ASA versions and FDM running software version 6.7 or later.

Guidelines and Limitations of Remote Access VPN for FDM-Managed Device

Keep the following guidelines and limitations in mind when configuring RA VPN.

- AnyConnect packages must be pre-loaded to FDM-Managed devices running Version 6.4.0 using firewall device manager.

Note Upload AnyConnect package separately to the FDM-Managed device running Version 6.5.0 using the Remote Access VPN Configuration wizard in Cisco Defense Orchestrator.

- Before configuring RA VPN from CDO:
  - Register the license for the FDM-managed devices from firewall device manager.
  - Enable the license from firewall device manager with export-control.
- CDO does not support the Extended Access List object. Configure the object using the Smart CLI in firewall device manager and then use in VPN filter and Change of Authorization (CoA) redirect ACL.
- The template you create from an FDM-managed device will not contain the RA VPN configuration.
- Device-specific overrides are required for IP pool objects and RADIUS identity sources.

- You cannot configure both firewall device manager access (HTTPS access in the management access-list) and AnyConnect remote access SSL VPN on the same interface for the same TCP port. For example, if you configure remote access SSL VPN on the outside interface, you cannot also open the outside interface for HTTPS connections on port 443. Because you cannot configure the port used by these features in firewall device manager, you cannot configure both features on the same interface.
- If you configure two-factor authentication using RADIUS and RSA tokens, the default authentication timeout of 12 seconds is too quick to allow successful authentication in most cases. Increase the authentication timeout value by creating a custom AnyConnect client profile and applying it to the RA VPN connection profile, as described in Upload RA VPN AnyConnect Client Profile, on page 270. We recommend an authentication timeout of at least 60 seconds so that users have enough time to authenticate and then paste the RSA token and for the round-trip verification of the token.

How Users Can Install the AnyConnect Client Software on FDM-Managed Device

Use firewall device manager APIs to upload the AnyConnect Client Software package to FDM-managed device to distribute to your users. See Upload AnyConnect Software Packages to an FDM-Managed Device Running Version 6.4.0.

To complete a VPN connection, your users must install the AnyConnect client software. You can use your existing software distribution methods to install the software directly. Or, you can have users install the AnyConnect client directly from the FDM-managed device.

Note Users must have Administrator rights on their workstations to install the software.

If you decide to have users initially install the software from the FDM-managed device, inform users to perform the following steps:

Note Android and iOS users should download AnyConnect from the appropriate App Store.

Procedure

Step 1 Using a web browser, open **https://***ravpn-address*, where *ravpn-address* is the IP address or hostname of the outside interface on which you are allowing VPN connections. You identify this interface when you configure the remote access VPN. The system prompts the user to log in.

Step 2 Log into the site. Users are authenticated using the directory server configured for the remote access VPN. Log in must be successful to continue. If the login is successful, the system determines if the user already has the required version of the AnyConnect client. If the AnyConnect client is absent from the user's computer or is down-level, the system automatically starts installing the AnyConnect software. When the installation is finished, AnyConnect completes the remote access VPN connection.

Distribute new AnyConnect Client Software version

You can distribute the new version of AnyConnect client software to your users by uploading them to FDM-managed device without removing the old version. Once the AnyConnect client is uploaded successfully, you can remove the old version.

The AnyConnect client detects the new version on the next VPN connection the user makes. The system will automatically prompt the user to download and install the updated client software. This automation simplifies software distribution for you and your clients.

The following figure shows an example of an FDM-managed device with two versions of AnyConnect client software (**AnyConnectWindows_3.2_BGL** and **AnyConnectWindows_4.2_BGL**) for Windows OS.

Upload RA VPN AnyConnect Client Profile

The Remote Access VPN AnyConnect Client Profile is a group of configuration parameters stored in a file. There are different AnyConnect client profiles containing configuration settings for the core client VPN functionality and for the optional client modules Network Access Manager, AMP Enabler, ISE posture, Network Visibility, Customer Feedback Experience profiles, Umbrella roaming security, and Web Security.

CDO allows uploading of these profiles as objects which can be used in the group policy later.

- **AnyConnect VPN Profile** — AnyConnect client profiles are downloaded to clients along with the VPN AnyConnect client software. These profiles define many client-related options, such as auto-connect on startup and auto-reconnect, and whether the end-user can change the option from the AnyConnect client preferences and advanced settings. CDO supports the XML file format.
- **AMP Enabler Service Profile** — The profile is used for the AnyConnect AMP Enabler. The AMP Enabler and this profile are pushed to the endpoints from FDM-managed device when a remote access VPN user connects to the VPN. CDO supports XML and ASP file formats.
- **Feedback Profile** — You can add a Customer Experience Feedback profile and select this type to receive information about the features and modules customers have enabled and used. CDO supports the FSP file format.
- **ISE Posture Profile** — Choose this option if you add a profile file for the AnyConnect ISE Posture module. CDO supports XML and ISP file formats.
- **Network Access Manager Service Profile** — Configure and add the NAM profile file using the Network Access Manager profile editor. CDO supports XML and NSP file formats.
- **Network Visibility Service Profile** — Profile file for AnyConnect Network Visibility module. You can create the profile using the NVM profile editor. CDO supports XML and NVMSP file formats.
- **Umbrella Roaming Security Profile** — You must select this file type if you deploy the Umbrella Roaming Security module. CDO supports XML and JSON file formats.

- **Web Security Service Profile** — Select this file type when you add a profile file for the Web security module. CDO supports XML, WSO, and WSP file formats.

Before you begin

Use the suitable GUI-based AnyConnect profile editors to create the profiles you need. You can download the profile editors from Cisco Software Download Center in the AnyConnect Secure Mobility Client category and install the AnyConnect "Profile Editor - Windows / Standalone installer (MSI)." The profile editor installer contains stand-alone versions of the profile editors. The installation file is for Windows only and has the file name anyconnect-profileeditor-win-<version>-k9.msi, where <version> is the AnyConnect version. For example, anyconnect-profileeditor-win-4.3.04027-k9.msi. You must also install Java JRE 1.6 (or higher) before installing the profile editor.

Except for the Umbrella Roaming Security profile editor, this package contains all the profile editors required for creating the modules. For detailed information, see the *AnyConnect Profile Editor* chapter in the appropriate release of the Cisco AnyConnect Secure Mobility Client Administrator Guide for details. Download the Umbrella Roaming Security profile separately from the Umbrella dashboard. For detailed information, see the "Download the AnyConnect Roaming Security Profile from the Umbrella Dashboard" section of the "Umbrella Roaming Security" chapter in the Cisco Umbrella User Guide.

Procedure

Step 1 In the CDO navigation bar at the left, click **Objects > FDM Objects**.

Step 2 Click the blue plus  button.

Step 3 Click **RA VPN Objects (ASA & FDM)** > **AnyConnect Client Profile**.

Step 4 In the **Object Name** field, enter a name for the AnyConnect client profile.

Step 5 Click **Browse** and select the file you created using the Profile Editor.

Step 6 Click **Open** to upload the profile.

Step 7 Click **Add** to add the object.

Related information:

- Associate the client modules with the AnyConnect VPN profile in the RA VPN group policies window. See Create New RA VPN Group Policies.

Note The client module association is supported by all ASA versions and FDM running software version 6.7 or later.

Licensing Requirements for Remote Access VPN

Enable (register) the license for the FDM-managed devices from firewall device manager to configure RA VPN connection. When you register the device, you must do so with a Smart Software Manager (SSM) account that is enabled for export-controlled features. You also cannot configure the feature using the evaluation license.

Also, you must purchase and enable a license; it can be any of the following: . These licenses are treated the same for FDM-managed devices, although they are designed to allow different feature sets when used with ASA Software-based headends.

For more information about enabling license from firewall device manager, see the **Licensing Requirements for Remote Access VPN** section of the Remote Access VPN chapter of the Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager for the version your device is running.

For more information, see the *Cisco AnyConnect Ordering Guide*. There are also other data sheets available on http://www.cisco.com/c/en/us/product...t-listing.html.

To view the license status, perform the following:

Procedure

Step 1 In the Cisco Defense Orchestrator navigation bar on the left, click **Inventory**.

Step 2 Click the **Devices** device.

Step 3 Click the **FTD** tab and select a device that you want.

Step 4 In the **Device Actions** pane on the right, click **Manage Licenses**. If the license is valid, the **Status** shows **Enabled**.

Maximum Concurrent VPN Sessions By Device Model

There is a maximum limit to the number of concurrent remote access VPN sessions allowed on a device based on the device model. This limit is designed, so that system performance does not degrade to unacceptable levels. Use these limits for capacity planning.

Device Model	Maximum Concurrent Remote Access VPN Sessions
Firepower 2110	1,500
Firepower 2120	3,500
Firepower 2130	7,500
Firepower 2140	10,000
Firepower Threat Defense Virtual	250

RADIUS Change of Authorization

The RADIUS Change of Authorization (CoA) feature provides a mechanism to change the attributes of authentication, authorization, and accounting (AAA) session after it is authenticated. A key challenge for RA VPNs is to secure the internal network against compromised endpoints and to secure the endpoint itself when it is affected by viruses or malware, by remediating the attack on the endpoint. There is a need to secure the endpoint and the internal network in all phases, that is, before, during, and after the RA VPN session. The RADIUS CoA feature helps in achieving this goal.

If you use Cisco Identity Services Engine (ISE) RADIUS servers, you can configure Change of Authorization policy enforcement. When a policy changes for a user or user group in AAA, ISE sends CoA messages to the FDM-managed device to reinitialize authentication and apply the new policy. An Inline Posture Enforcement Point (IPEP) is not required to apply access control lists (ACLs) for each VPN session established with the FDM-managed device.

Related Information:

- Configure Change of Authorization on the FDM-Managed Device

Configure Change of Authorization on the FDM-Managed Device

Most of the Change of Authorization policy is configured in the ISE server. However, you must configure the FDM-managed device to connect to ISE correctly.

Before you begin

If you use hostnames in any object, ensure that you configure DNS servers for use with the data interfaces, as explained in **Configuring DNS for Data and Management Interfaces** section of the System Settings chapter of the Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager for the version your device is running.You typically need to configure DNS anyway to have a fully-functional system.

Procedure

Procedure

Step 1 Log in to the firewall device manager for your FDM-managed device.

Step 2 Configure the extended access control list (ACL) for redirecting initial connections to ISE. The purpose of the redirect ACL is to send initial traffic to ISE so that ISE can assess the client posture. The ACL should send HTTPS traffic to ISE, but not traffic that is already destined for ISE, or traffic that is directed to a DNS server for name resolution. A sample redirect ACL might look like the following:

access-list redirect extended deny ip any host <ISE server IP>

access-list redirect extended deny ip any host <DNS server IP>

access-list redirect extended deny icmp any any

access-list redirect extended permit tcp any any eq www

However, note that ACLs have an implicit "deny any any" as the last access control entry (ACE). In this example, the last ACE, which matches TCP port www (that is, port 80), will not match any traffic that matches the first 3 ACEs, so those are redundant. You could simply create an ACL with the last ACE and get the same results. Note that in a redirect ACL, the permit and deny actions simply determine which traffic matches the ACL, with permit matching and deny not matching. No traffic is actually dropped, denied traffic is simply not redirected to ISE. To create the redirect ACL, you need to configure a Smart CLI object.

a. Choose **Device** > **Advanced Configuration** > **Smart CLI** > **Objects**.

b. Click **+** to create a new object.

c. Enter a name for the ACL. For example, **redirect**.

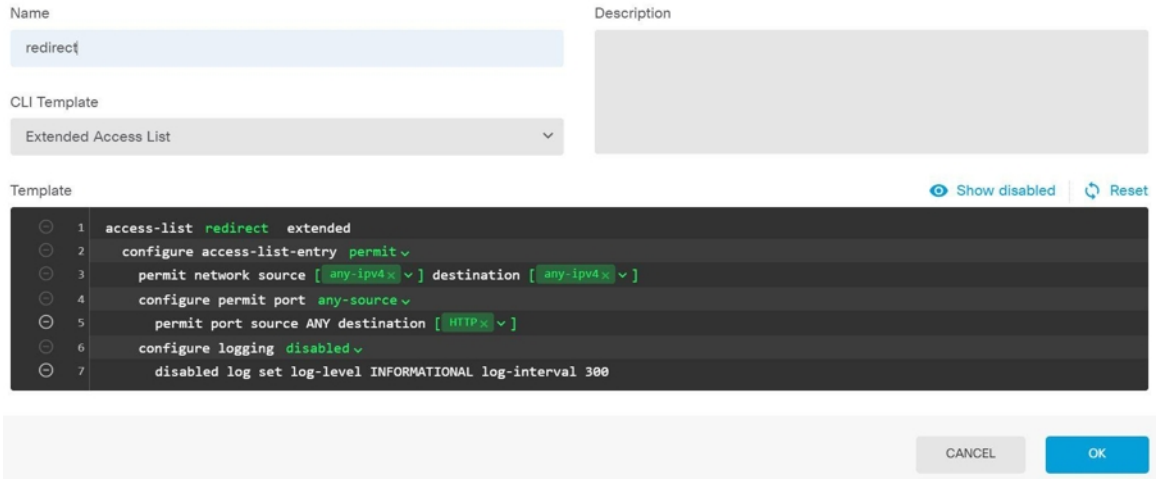
d. For **CLI Template**, select **Extended Access List**.

e. Configure the following in the **Template** body:

- configure access-list-entry action = permit
- source-network = any-ipv4
- destination-network = any-ipv4
- configure permit port = any-source

- destination-port = HTTP
- configure logging = disabled

The ACE should look like the following:



f. Click **OK**.

This ACL will be configured the next time you deploy changes. You do not need to use the object in any other policy to force deployment.

Note This ACL applies to IPv4 only. If you also want to support IPv6, simply add a second ACE with all the same attributes, except select any-ipv6 for the source and destination networks. You can also add the other ACEs to ensure traffic to the ISE or DNS server is not redirected. You will first need to create host network objects to hold the IP addresses of those servers.

Step 3 Configure a RADIUS server group for dynamic authorization.

Perform the below steps by following the instructions provided in the Create or Edit a RADIUS Server Object or Group section.

a. Create a RADIUS Server Object

b. Create a RADIUS Server Group

Step 4 Create a connection profile that uses this RADIUS server group. See Configure an RA VPN Connection Profile. Use **AAA Authentication** (either only or with certificates), and select the server group in the **Primary Identity Source for User Authentication**, **Authorization**, and **Accounting** options.

Verify Remote Access VPN Configuration of FDM-Managed Device

After you configure the remote access VPN and deploy the configuration to the device, verify that you can make remote connections.

Procedure

Step 1 From an external network, establish a VPN connection using the AnyConnect client. Using a web browser, open **https://***ravpn-address*, where *ravpn-address* is the IP address or hostname of the outside interface on which you are allowing VPN connections. If necessary, install the client software and complete the connection. See How Users Can Install the AnyConnect Client Software on FDM-Managed Device. If you configured group URLs, also try those URLs.

Step 2 In the **Inventory** page, select the device you want to verify and click **Command Line Interface** under **Device Actions**.

Step 3 Use the **show vpn-sessiondb** command to view summary information about current VPN sessions.

Step 4 The statistics should show your active AnyConnect Client session, and information on cumulative sessions, the peak concurrent number of sessions, and inactive sessions. Following is sample output from the command.

```
> show vpn-sessiondb
--------------------------------------------------------------------------------
VPN Session Summary
--------------------------------------------------------------------------------
                            Active : Cumulative : Peak Concur : Inactive
                           ------------------------------------------------
AnyConnect Client           :      1 :         49 :           3 :        0
  SSL/TLS/DTLS              :      1 :         49 :           3 :        0
Clientless VPN              :      0 :          1 :           1
  Browser                   :      0 :          1 :           1
--------------------------------------------------------------------------------


  Total Active and Inactive    :      1             Total Cumulative :     50
  Device Total VPN Capacity    :  10000
  Device Load                  :     0%
  --------------------------------------------------------------------------------

  --------------------------------------------------------------------------------
  Tunnels Summary
  --------------------------------------------------------------------------------
                               Active : Cumulative : Peak Concurrent
                              ----------------------------------------------
  Clientless                  :      0 :          1 :               1
  AnyConnect-Parent           :      1 :         49 :               3
  SSL-Tunnel                  :      1 :         46 :               3
  DTLS-Tunnel                 :      1 :         46 :               3
  --------------------------------------------------------------------------------
  Totals                      :      3 :        142
  --------------------------------------------------------------------------------

  --------------------------------------------------------------------------------
  IPv6 Usage Summary
  --------------------------------------------------------------------------------
                               Active : Cumulative : Peak Concurrent
                              ----------------------------------------------
  AnyConnect SSL/TLS/DTLS     :        :            :
    Tunneled IPv6             :      1 :         20 :           2
  --------------------------------------------------------------------------------
```

Step 5 Use the **show vpn-sessiondb anyconnect** command to view detailed information about current AnyConnect VPN sessions. Detailed information includes encryption used, bytes transmitted and received, and other statistics. If you use your VPN connection, you should see the bytes transmitted/received numbers change as you re-issue this command.

```
> show vpn-sessiondb anyconnect

Session Type: AnyConnect

Username     : User1                  Index        : 4820
Assigned IP  : 172.18.0.1             Public IP    : 192.168.2.20
Assigned IPv6: 2009::1
Protocol     : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License      : AnyConnect Premium
Encryption   : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-256 DTLS-Tunnel: (1)AES256
Hashing      : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA384  DTLS-Tunnel: (1)SHA1
Bytes Tx     : 27731                  Bytes Rx     : 14427
Group Policy : MyRaVpn|Policy         Tunnel Group : MyRaVpn
Login Time   : 21:58:10 UTC Mon Apr 10 2017
Duration     : 0h:51m:13s
Inactivity   : 0h:00m:00s
VLAN Mapping : N/A                    VLAN         : none
Audt Sess ID : c0a800fd012d400058ebfff2
Security Grp : none                   Tunnel Zone : 0
```

View Remote Access VPN Configuration Details of FDM-Managed Device

Procedure

Step 1 In the CDO navigation bar at the left, click **VPN** > **Remote Access VPN Configuration**.

Step 2 Click on a VPN configuration object present.

The group shows summary information on how many connection profiles and group policies are currently configured.

- Expand the RA VPN configuration to view all connection profiles associated with them.
  - Click the add + button to add a new connection profile.
  - Click the view button ( ) to open a summary of the connection profile and connection instructions. Under **Actions**, you can click **Edit** to modify the changes.
- You can click one of the following options under **Actions** to perform additional tasks:
  - Click **Group Policies** to assign/add group policies.
  - Click a configuration object or connection profile that you no longer need and click **Remove** to delete.

Monitor Remote Access Virtual Private Network Sessions

Remote access Virtual Private Network provides secure connections for remote users, such as mobile users or telecommuters. Monitoring these connections provides important indicators of connection and user session performance at a glance. Cisco Defense Orchestrator (CDO) remote access VPN monitoring capabilities enable you to determine quickly whether remote access VPN problems exist and where they exist. You can then apply this knowledge and use your network management tools to reduce or eliminate problems for your network and users. You can also disconnect remote access VPN sessions as needed.

The Remote Access Virtual Private Monitoring page provides the following information:

- A list of active and historical sessions for up to a year.
- Shows intuitive graphical visuals to provide at-a-glance views from all active VPN headends managed by CDO.
- The live session screen shows the most used operating system and VPN connection profile in the CDO tenant. It also shows the average session duration and data uploaded and downloaded.
- Filtering capabilities to narrow your search based on criteria such as device type, device names, session length, and the amount of data transmitted and received.

Related Information:

- Monitor Live AnyConnect Remote Access VPN Sessions, on page 280
- Monitor Historical AnyConnect Remote Access VPN Sessions, on page 282
- Search and Filter Remote Access VPN Sessions
- Customize the Remote Access VPN Monitoring View
- Export Remote Access VPN Sessions to a CSV File
- Disconnect Remote Access VPN Sessions on FDM-Managed Device

Monitor Live AnyConnect Remote Access VPN Sessions

You can monitor real-time data from active AnyConnect remote access VPN sessions on the devices. This data is automatically refreshed every 10 minutes. If you want to retrieve the latest list of sessions at any point, you click the reload icon appearing on the right corner of the screen.

Before you begin

- Onboard the remote access VPN head-ends to CDO.
- Ensure that the connectivity status of the devices you want to monitor live data is "Online" on the **Inventory** page.

Procedure

Step 1 In the CDO navigation pane, click **VPN** > **Remote Access VPN Monitoring**.

Alternatively, you can click **View Active Remote Access VPN Sessions**on the CDO home page or navigate to **VPN** > **Remote Access VPN** and click the icon on the top-right corner of the screen.

Step 2 Click **RA VPN**.

Step 3 Click **Live**.

You can Search and Filter Remote Access VPN Sessions to narrow down your search based on criteria such as device type, session length, and upload and download data range.

Note The **Data TX** and **Data RX** information are not available for FTD.

View Live Remote Access VPN Data

The live data is presented both in the dashboard and tabular form.

Dashboard View

You have to click the **Show Charts View** icon appearing at the top right corner of the screen to see the dashboard.

The dashboard provides at-a-glance views from all active VPN headends managed by CDO.

- **Breakdown (All Devices)**: Shows a total number of live sessions. It also shows a pie chart that is divided into four arc lengths. It illustrates the percentage of VPN sessions of the top three devices with the highest number of sessions. The remaining arc length represents the aggregate of other devices.
- Shows most used operating system and connection profile in the CDO tenant.
- Shows average session duration and data uploaded and downloaded.
- **Active Sessions by Country**: Shows an interactive heat map of the location of the users connected to your RA VPN headends.
  - Countries from which users have connected are shown in progressively darker shades of blue, depending on the relative proportion of the sessions established from that country — the darker the blue color means more sessions are established from that country.
  - The legend at the bottom of the map provides a scale that indicates the correlation between the number of sessions in a country and the shade of blue used to color the country.
  - Hover the mouse pointer on the map to see the country's name and the total number of active user sessions established from that country.
  - Hover the mouse pointer on the table to see the country's location and the total number of active user sessions on the map.

Tabular View

Click the **Show Tabular View** icon on the top right corner of the screen to view the data in tabular format.

The tabular form provides a complete list of VPN users connected presently.

- The **Location** column shows the location of all the users connected to the VPN headends by geolocating their public IP addresses. Click a row to view the user details. On clicking the location link in the left pane, the location of the user is shown on the Google map.

Important CDO applies a standard filter to the live data and represents them on the dashboard. You can apply new filters only when tabular data is shown, since the custom filters are not supported in the visual dashboard view. Click **Clear** to remove all filters you have applied. You cannot remove the standard filter.

You can use Search and Filter Remote Access VPN Sessions functionalities to narrow down your search based on criteria such as device type, session length, and upload and download data range. Note that a maximum of 10,000 results can be displayed at once.

A green dot with an **Active** label in the status column indicates an active VPN user's session.

Monitor Historical AnyConnect Remote Access VPN Sessions

You can monitor the historical data from AnyConnect Remote Access VPN sessions recorded over the last three months.

Before you begin

- Onboard the RA VPN head-ends to CDO.

Procedure

Step 1 In the CDO navigation pane, click **VPN** > **Remote Access VPN Monitoring**.

Alternatively, you can click **View Active Remote Access VPN Sessions** on the CDO home page or navigate to **VPN** > **Remote Access VPN** and click the icon in the top-right corner.

Step 2 Click **RA VPN**.

Step 3 Click **Historical**.

CDO displays the historical data from the Remote Access VPN sessions recorded over the last three months.

You can use Search and Filter Remote Access VPN Sessions functionalities to narrow down your search based on criteria such as device type, session length, and upload and download data range.

The **Data TX** and **Data RX** information are not available for FTD.

View Historical Remote Access VPN Data

The historical data is presented both in the dashboard and tabular form.

Dashboard View

You have to click the **Show Charts View** icon appearing at the top right corner of the screen to see the dashboard. You will see the dashboard view along with the tabular view.

The dashboard provides at-a-glance views from all active VPN headends managed by CDO. It provides a bar graph showing the VPN sessions recorded for all devices in the last 24 hours, 7 days, and 30 days. You can select the duration from the drop-down. You can hover over on individual bars to see the date and the total number of sessions on that day.

Tabular View

You have to click the **Show Tabular View** icon appearing at the top right corner of the screen to see only the tabular view. The tabular form provides a complete list of VPN users connected over the last three months.

The **Location** column shows the location of all the users connected to the VPN headends by geolocating their public IP addresses. Click a row to view the user details. On clicking the location link in the left pane, the location of the user is shown on the Google map.

Important CDO applies a standard filter to the historical data and represents them on the dashboard. You can apply new filters only when tabular data is shown, since the dashboard is not supported for custom filters. Clearing the newly applied filters relaunches the dashboard (On the screen, click **Clear** to remove manually applied filters). You cannot remove the standard filter.

You can use Search and Filter Remote Access VPN Sessions functionalities to narrow down your search based on criteria such as session date and time range, session length, and upload and download data range. Note that a maximum of 10,000 results can be displayed at once.

A green dot with an **Active** label in the status column indicates an active VPN user's session.

Search and Filter Remote Access VPN Sessions

Search

Use the search bar functionality to find remote access VPN sessions. Start typing device name, IP address, or serial number in the search bar, and remote access VPN sessions that fit the search criteria will be displayed. Search is not case-sensitive.

Filter

Use the filter sidebar to find remote access VPN sessions based on criteria such as session time range, session length, and upload and download data range. The filter functionality is available to both live and historical views.

- **Filter by Devices**: Select one or all devices from the **All Types** tab to view sessions from selected devices. The window also categorizes the devices based on their type and displays them under the corresponding tabs.
- **Sessions Time Range** (Applicable only for historical data): View historical sessions from a specified date and time range. Note that you can view data recorded over the last three months.
- **Sessions Length**: View sessions based on a specified session's duration length. Set the time unit (hours, minutes, or seconds) and specify the minimum and maximum duration length by moving the slider. You can also specify the length in the provided fields.
- **Upload (TX)**: View sessions based on a specified amount of data uploaded or transferred to the secured network. Set the unit (GB, MB, or KB) and select the range by moving the slider accordingly. You can also specify the values in the available fields.
- **Download (RX)**: View sessions based on a specified amount of data downloaded or received from the secured network. Set the unit (GB, MB, or KB) and select the range by moving the slider accordingly. You can also specify the values in the available fields.

Customize the Remote Access VPN Monitoring View

You can modify the remote access VPN monitoring view in both live and historical modes to only include column headers that apply to the view you want. Click the column filter icon located to the right of the columns and select or deselect the columns you want.

CDO remembers your selection the next time you sign in to CDO.

Export Remote Access VPN Sessions to a CSV File

You can export the remote access VPN sessions of one or more devices to a comma-separated value (.csv) file. You can open the .csv file in a spreadsheet application such as Microsoft Excel to sort and filter the items on your list. This information helps you to analyze the remote access VPN sessions. Every time you export the sessions, CDO creates a new .csv file, where the file created has a date and time in its name.

CDO can export a maximum of 100,000 active sessions to the CSV file. If the total number of sessions from all devices exceeds the maximum limit, you can use the **View By Device** filter and generate reports for individual devices.

Procedure

Step 1 In the CDO navigation pane, click **VPN** > **Remote Access VPN Monitoring**.

Step 2 In the **View By Devices** area, select one of the following:

- **All Devices** to export active sessions from all devices listed below it.
- Click on a device that you want to export sessions of that device.

Step 3 Click the icon on the top right corner. CDO exports the rules you see on the screen to a .csv file.

Step 4 Open the .csv file in a spreadsheet application to sort and filter the results.

Disconnect Remote Access VPN Sessions on FDM-Managed Device

Currently, it is not possible to terminate remote access VPN sessions on an FDM-managed device using the Cisco Defense Orchestrator interface. Instead, you can connect to the Threat Defense CLI using SSH and disconnect the desired user. You can perform this task on an online FDM-managed device onboarded to CDO.

Procedure

Step 1 Log on to Firewall device manager and use the device CLI as explained in the **Logging Into the Command Line Interface (CLI)** section of the "Getting Started" chapter of the Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager for the version your device is running.

Step 2 Execute the `vpn-sessionsdb logoff {name}` command and replace **name** with the user name. This command terminates all sessions for the username that you specify.

Templates

Templates provide the means to develop a preferred and general use version of device configuration files:

- Templates are created from an existing base configuration file.
- They support value parameters for easy customization of expected values, including IP addresses and port numbers.
- They are exportable, with parameter substitution, for use across multiple devices.

Related Information

- FDM-Managed Device Templates, on page 285
  - Configure an FDM Template, on page 286
  - Apply Template to an FDM-Managed Device, on page 290

FDM-Managed Device Templates

About FDM-Managed Device Templates

Cisco Defense Orchestrator allows you to create a FDM-managed device template of an onboarded FDM-managed device's configuration. When you are creating the template, select the parts (objects, policies, settings, interfaces, and NAT) that you want to include in your FDM-managed device template. You can then modify that template and use it to configure other FDM-managed devices you manage. FDM-managed device templates are a way to promote policy consistency between your FDM-managed devices.

When creating the FDM-managed device template, you can opt to either create a complete or custom template:

- A complete template includes all parts of the FDM-managed device configuration and applies everything on other FDM-managed devices.
- A custom template includes only one or more parts of the FDM-managed device configuration that you select and applies only that part and its associated entities on other FDM-managed devices.

Important The FDM-managed device template will not include certificate, Radius, AD, and RA VPN Objects.

How You Could Use FDM-Managed Device Templates

Here are some ways that you could use FDM-managed device templates:

- Configure one FDM-managed device by applying another FDM-managed device's configuration template to it. The template you apply may represent a "best practice" configuration that you want to use on all your FDM-managed devices.
- Use the template as a method to make the device configuration changes and simulate them in a lab environment to test its functionality before applying those changes to a live FDM-managed device.

- Parameterize the attributes of the interfaces and sub-interfaces when creating a template. You can change the parameterized values of interfaces and subinterfaces at the time of applying the template.

What You Will See in the Change Log

When you apply a template to a device, you overwrite the entire configuration of that device. The CDO change log records every change that gets made as a result. So, change log entries will be very long after applying a template to a device.

Related Information:

- Configure an FDM Template
- Apply an FDM Template

Configure an FDM Template

Prerequisites

Before you create a FDM-managed device template, onboard to Cisco Defense Orchestrator the FDM-managed device from which you will create the template. You can only create an FDM-managed device template from an onboarded FDM-managed device.

We **strongly** recommend using templates to configure brand new FDM-managed devices being added to your environment.

Note When you create a template from an FDM-managed device, the RA VPN objects are not included in the template.

Create an FDM Template

When creating a template, if you select all parts, the template will include every aspect of that device's configuration; it's management IP address, interface configurations, policy information, and so on.

If you select some of the parts, the custom template includes the following entities.

Template Parts	Parts included in Custom Template
Access Rules	Includes access control rules and any related entities for those rules. For example, objects and interfaces (with sub-interfaces).
NAT Rules	Includes NAT rules and any related entities required for those NAT rules. For example, objects and interfaces (with sub-interfaces).
Settings	Includes system settings and any related entities required for those settings. For example, objects and interfaces (with sub-interfaces).
Interfaces	Includes interfaces and sub-interfaces.

Template Parts	Parts included in Custom Template
Objects	Includes objects and any related entities required for those objects. For example, interfaces and sub-interfaces.

Use this procedure to create an FDM-managed device template:

Procedure

Step 1 In the Cisco Defense Orchestrator navigation bar, click **Inventory**.

Step 2 Click the **Devices** tab.

Step 3 Click the **FTD** tab and select the device that you want from the list.

Step 4 Use the filter or search field to find the FDM-managed device from which you want to create the template.

Step 5 In the **Device Actions** pane on the right, click **Create Template**. The **Name Template** provides the count of each part on the device. It also shows the count of sub-interfaces, if any.

Step 6 Select the parts that you want to include in the template.

Step 7 Enter a name for your template.

Step 8 Click **Create Template**.

Step 9 In the **Parameterize Template** area, you can perform the following:

- To parameterize an interface, hover (until you see curly braces) and click a cell corresponding to that interface.
- To parameterize a sub-interface, expand the interface that has a sub-interface, and hover (until you see curly braces) and click a cell corresponding to that sub-interface.

You can parameterize the following attributes to enable per-device customization.

- **Logical Name**
- **State**
- **IP Address/Netmask**

Note These attributes only support one value per parameter.

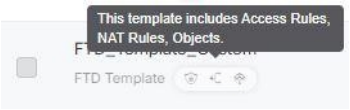
Step 10 Click **Continue**.

Step 11 Review the template and any parameterizations. Click **Done** to create the template.

The **Inventory** page now displays the FDM-managed device template you just created.

Note After creating a template, in the **Inventory** pane, CDO displays the corresponding template part icons to show the parts included in that template. This information also appears in the **Device Details** pane when you click the device or when you hover over the mouse pointer on the icon.

The following picture shows an example of a part icon to show that the template includes "access rules", "NAT rules", and "objects".



Edit an FDM-Managed Device Template

Edit the template parameters with the following procedure:

Procedure

Step 1 In the Cisco Defense Orchestrator navigation bar, click **Inventory**.

Step 2 Click the **Templates** tab.

Step 3 Click the **FTD** tab.

Step 4 Use the Model/Template filter to find the template you want to modify.

Step 5 In the **Device Actions** pane on the right, click **Edit Parameters**.

Step 6 (Optional) make any changes to the parameters by directly editing the text box.

Step 7 Click **Save**.

You can edit the rest of the FDM-managed device template just as you would the configuration of a live FDM-managed device. You can edit your FDM-managed device template with the following configurations:

- FDM-Managed Device Settings
- Manage Virtual Private Network Management in CDO
- Create an RA VPN Configuration
- FDM Policy Configuration
- Promote policy and configuration consistency

Delete an FDM Template

You delete an FDM-managed device template just as you would remove an FDM-managed device from Cisco Defense Orchestrator:

Procedure

Step 1 In the CDO navigation bar, click **Inventory**.

Step 2 Click the **Templates** tab.

Step 3 Click the **FTD** tab.

Step 4 Use the filter and search fields to find the FDM-managed device template you want to delete.

Step 5 In the **Device Actions** pane, click **Remove** .

Step 6 Read the warning message and click **OK** to delete the template.

Related Information:

- FDM-Managed Device Templates
- Apply an FDM Template

Apply an FDM Template

Before applying a template, you can identify its contents by navigating to the **Inventory** page and filter for **Model/Template**. Cisco Defense Orchestrator displays the corresponding template part icons to show the parts included in that template. This information also appears in the **Device Details** pane when you click the device or when you hover over the mouse pointer on the icon.

You can parameterize the following attributes to enable per-device customization, which means you can apply device-specific values at the time of applying the template:

When applying the FDM-managed device template, you can change the parameterized values of interfaces and subinterfaces configured when creating the template.

Apply a Complete Template

Applying a complete FDM-managed device template to create a new FDM-managed device overwrites entirely any existing configuration on the FDM-managed device, including any staged changes that have not yet been deployed from CDO to the device. Anything on the device that was not included in the template will be lost.

Apply a Custom Template

Applying a custom FDM-managed device template to other FDM-managed devices will retain or remove the existing configuration based on the template part. The following table provides the changes that occur after applying the custom template on other FDM-managed devices.

Template Parts	After Applying Custom Template
Access Rules	• New access control rules present in the custom template overwrites any existing access control rules on the device. • New objects and interfaces (with sub-interfaces), if any, in the custom template are applied to the device without deleting any existing objects and interfaces.
NAT Rules	• New NAT rules present in the custom template overwrites any existing NAT rules on the device. • New objects and interfaces (with sub-interfaces), if any, in the custom template are applied to the device without deleting any existing objects and interfaces.
Settings	• New system settings from the custom template are applied to the device without deleting any existing system settings. • New objects and interfaces (with sub-interfaces), if any, in the custom template are applied to the device without deleting any existing objects and interfaces.

Template Parts	After Applying Custom Template
Interfaces	• New interfaces and sub-interfaces from the custom template are applied to the device without deleting any existing interfaces and sub-interfaces. • CDO does not allow applying a template to a device where more interfaces are defined in the template than there are interfaces on the device.
Objects	• New objects from the custom template are applied to the device without deleting any existing objects. • New interfaces and sub-interfaces, if any, in the custom template are applied to the device without deleting any existing interfaces and sub-interfaces.

Prerequisites

The following conditions must be met prior to applying a template:

- When using a template, be sure that any changes you have made to the template have been committed and that the template is in the "Synced" state on the **Inventory** page.
- When using an FDM-managed device as a template, be sure that any changes on CDO you intended to deploy to the device have been deployed and that there are no changes from the firewall device manager console that have not been deployed. The device must show a Synced state on the **Inventory** page.

Applying the template to a device is a three-step process.

1. Apply a Complete Template
2. Review Device and Networking Settings
3. Deploy Changes to the Device

Apply Template to an FDM-Managed Device

Important Before you deploy the changes to the device, continue to the next procedure:

Review Device and Networking Settings

You can use change request tracking to apply a tracking label to your changes before you apply the template. Use the following procedure to apply an FDM-managed device template:

Procedure

Step 1 (Optional) Before you begin, make a template of your FDM-managed device before you apply another template to it. This gives you a configuration backup you can reference when you need to reapply device and networking settings.

Step 2 In the CDO navigation bar, click **Inventory**.

Step 3 Click the **Templates** tab.

Step 4 Click the **FTD** tab.

Step 5 Use the filter and search field to find the FDM-managed device or template to which you are going to apply the template.

Note If you change the name of the template at this point, you are applying a full device configuration or template to *DeviceName*. Deploying this change to *DeviceName* will overwrite the entire configuration running on that device.

Step 6 In the device **Actions** pane on the right, click **Apply Template**.

Step 7 Click **Select Template** and select the desired template and click **Continue**.

Step 8 You can configure the following and click **Continue** appearing on each screen.

a. **Map Interfaces**: Confirm or change the mapping of interfaces between the template and the device. Note that you cannot have more than one template interface mapped to a single device interface; if the interface configuration is not supported, you cannot continue and apply the template.

Note CDO does not allow applying a template to a device where more interfaces are defined in the template than there are interfaces on the device.

b. **Fill Parameters**: Customize the interface or sub-interface parameter values for the device that you are applying the template to.

c. **Review**: Review the template configuration and click **Apply Template** when you are ready to overwrite the existing device configuration with the configuration in the template.

Step 9 Click Preview and Deploy Configuration Changes for All Devices now the changes you made, or wait and deploy multiple changes at once.

Review Device and Networking Settings

When creating an FDM-managed device template, Cisco Defense Orchestrator copies the entire device configuration into the template. So, things like the management IP address of the original device are contained in the template. Review these device and network settings before you apply the template to a device:

Procedure

Step 1 Review these FDM-managed device settings to ensure that they reflect the correct information for the new FDM-managed device:

- FDM-Managed Device Settings
- Management Interface
- Hostname

Step 2 Review the Configure the FDM Access Control Policy to ensure that rules reference the new FDM-managed device's IP addresses where appropriate.

Step 3 Review inside_zone and outside_zone security objects to ensure they reference the correct IP address for the new FDM-managed device.

Step 4 Review NAT policies to ensure they reference the correct IP addresses for the new FDM-managed device.

Step 5 Review Interface configurations to ensure that they reflect the correct configuration for the new FDM-managed device.

Deploy Changes to the Device

Preview and Deploy Configuration Changes for All Devices now the changes you made, or wait and deploy multiple changes at once.

Related Information:

- FDM-Managed Device Templates
- Configure an FDM Template

Migrating an ASA Configuration to an FDM-Managed Device Template

Attention Secure Firewall device manager (FDM) support and functionality is only available upon request. If you do not already have Firewall device manager support enabled on your tenant you cannot manage or deploy to FDM-managed devices. Send a request to the support team to enable this platform.

Cisco Defense Orchestrator helps you migrate your ASA to an FDM-managed device. CDO provides a wizard to help you migrate these elements of the ASA's running configuration to an FDM-managed device template:

- Access Control Rules (ACLs)
- Interfaces
- Network Address Translation (NAT) rules
- Network objects and network group objects
- Routes
- Service objects and service group objects
- Site-to-site VPN

Once these elements of the ASA running configuration have been migrated to an FDM-managed device template, you can then apply the FDM template to a new FDM-managed device that is managed by CDO. The FDM-managed device adopts the configurations defined in the template, and so, the FDM-managed device is now configured with some aspects of the ASA's running configuration.

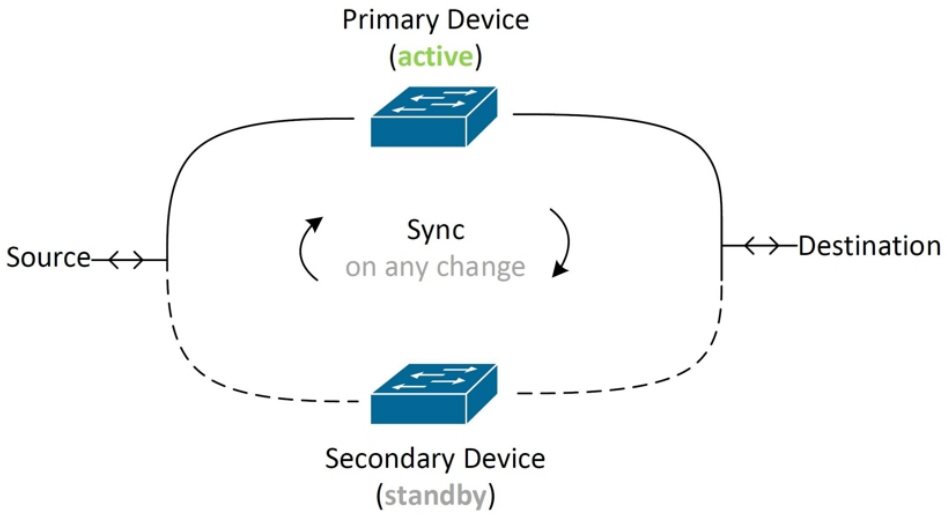
Other elements of the ASA running configuration are not migrated using this process. Those other elements are represented in the FDM-managed device template by empty values. When the template is applied to an FDM-managed device, we apply values we migrated to the new FDM-managed device and ignore the empty values. Whatever other default values the new FDM-managed device has, it retains. Those other elements of the ASA running configuration that we did not migrate, will need to be recreated on the FDM-managed device outside the migration process.

See Migrating an ASA to an FDM-Managed Device Using Cisco Defense Orchestrator for a full explanation of the process of migrating an ASA to an FDM-managed device using CDO.

FDM-Managed High Availability

About High Availability

A high availability (HA), or failover configuration, joins two devices into a primary/secondary setup so that if the primary device fails, the secondary automatically takes over. Configuring high availability, also called failover, requires two identical FDM-managed devices connected to each other through a dedicated failover link and, optionally, a state link. The health of the active unit (hardware, interfaces, software, and environmental status) is monitored to determine if specific failover conditions are met. If those conditions are met, failover occurs. This helps keep your network operation in case of a device failure or during a maintenance period when the devices are upgrading. See the related articles below for more information.



The units form an active/standby pair, where the primary unit is the active unit and passes traffic. The secondary (standby) unit does not actively pass traffic, but synchronizes configuration and other state information from the active unit. The two units communicate over the failover link to determine the operating status of each unit.

Note When you opt to accept changes from or deploy to an FDM-managed HA pair, you are communicating with the active device of the HA pair. This means that configurations and backups are pulled from the active device only.

Certificate and High Availability Pairs

When you apply a certificate to an FDM-managed HA pair, CDO only applies the certificate to the active device; only upon deploying the active device is the configuration, and the certificate, synchronized with the standby device. If you apply a new certificate to the active device through FDM-managed, the active device and standby device may have two different certificates. This may cause issues in failover or failover history, among other possible issues. The two devices must have the same certificate to function successfully. If you

must change the certificate through FDM-managed, then you must deploy changes and synchronize the certificate within the HA pair.

Related Information:

- Failover and Stateful Link for FDM-Managed High Availability
- FDM-Managed High Availability Pair Requirements
- Create an FDM-Managed High Availability Pair
- FDM-Managed Devices in High Availability Page
- Break an FDM-Managed High Availability Pairing
- FDM-Managed High Availability Failover History
- Refresh the FDM-Managed High Availability Status
- Force a Failover on an FDM-Managed High Availability Pair
- Upgrade an FDM-Managed High Availability Pair
- About Device Configuration Changes
- Read Configuration Changes from FDM-Managed Device to CDO
- Deploy Configuration Changes from CDO to FDM-Managed Device

FDM-Managed High Availability Pair Requirements

High Availability Requirements

There are several requirements you must establish before you create a high availability (HA) pair.

Physical and Virtual Device Requirements for HA

The following hardware requirements must be met:

- The devices must be the same hardware model.
- The devices must have the same modules installed. For example, if one has an optional network module, then you must install the same network module in the other device.
- The devices must have the same type and number of interfaces.
- To create an HA pair in Cisco Defense Orchestrator, both devices must have management interfaces configured. If the devices have data interfaces configured, you must create the HA pair through the FDM-managed UI, and then onboard the pair to CDO.

Note You **cannot** use an FDM-managed template in an HA pair.

Software Requirements for HA

The following software requirements must be met for both physical and virtual FDM-managed devices:

- You have two standalone FDM-managed devices onboarded in the Defense Orchestrator.
- The devices must run the exact same software version, which means the same major (first), minor (second), and maintenance (third) numbers. You can find the version inside the Device Details window on the **Inventory** page, or you can use the show version command in the CLI.

Note Devices with different versions are allowed to join, but the configuration is not imported into the standby unit and failover is not functional until you upgrade the units to the same software version.

- Both devices must be in local manager mode, that is, configured using FDM. If you can log into FDM on both devices, they are in local manager mode. You can also use the show managers command in the CLI to verify.
- You must complete the initial setup wizard for each device before onboarding to CDO.
- Each device must have its own management IP address. The configuration for the management interface is not synchronized between the devices.
- The devices must have the same NTP configuration.
- You cannot configure any interface to obtain its address using DHCP. That is, all interfaces must have static IP addresses.

  Note: If you change any interface configurations, you must deploy the changes to the device before establishing HA.
- Both devices must be **synced**. If you have pending changes or conflicts detected, see Resolve Configuration Conflicts and Resolve Configuration Conflicts for more information.

Note When you opt to accept changes from or deploy to an FDM-managed HA pair, you are communicating with the active device of the HA pair. This means that configurations and backups are pulled from the active device only.

Smart License Requirements for HA

The following license requirements must be met for both physical and virtual FDM-managed devices:

- Both devices in an HA pair must have either a registered license, or an evaluation license. If the devices are registered, they can be registered to different Cisco Smart Software Manager accounts, but the accounts must have the same state for the export-controlled functionality setting, either both enabled or both disabled. However, it does not matter if you have enabled different optional licenses on the devices.
- Both devices within the HA pair must have the same licenses during operation. It is possible to be in compliance on one device, but out of compliance on the other if there are insufficient licenses. If your Smart Licenses account does not include enough purchased entitlements, your account becomes Out-of-Compliance (even though one of the devices may be compliant) until you purchase the correct number of licenses.

Note that if the device is in evaluation mode, you must ensure that the registration status for CDO is the same on the devices. You must also ensure that your selection for participation in the Cisco Success Network is the same. For registered devices, the settings can be different on the units, but whatever is configured on the primary (active) device will either register or unregister the secondary. An agreement to participate in the Cisco Success Network on the primary implies an agreement for the secondary.

If you register the devices to accounts that have different settings for export controlled features, or try to create an HA pair with one unit registered and the other in evaluation mode, the HA join might fail. If you configure an IPsec encryption key with inconsistent settings for export controlled features, both devices will become active after you activate HA. This will impact routing on the supported network segments, and you will have to manually break HA on the secondary unit to recover.

Cloud Services Configuration for HA

Both of the devices within an HA pair must have **Send Events to the Cisco Cloud** enabled. This feature is available in the FDM UI. Navigate to **System Settings** and click **Cloud Services** to enable this feature. Without this option enabled, the HA pair cannot form in CDO and an event description error occurs. See the **Configuring Cloud Services** chapter of the Firepower Device Manager Configuration Guide of the version you are running for more information.

Create an FDM-Managed High Availability Pair

Before you create an FDM-managed HA pair in Defense Orchestrator, you must first onboard two standalone FDM-managed devices that meet the requirements described in FDM-Managed High Availability Pair Requirements.

Note To create an HA pair in CDO, both devices must have management interfaces configured. If the devices have data interfaces configure, you must create the HA pair through the FDM console, and then onboard the pair to CDO.

Once you create an FDM-managed HA pair, the primary device is **active** and the secondary device is **standby** by default. All configuration changes or deployments are made through the primary device and the secondary device remains in standby mode until the primary unit becomes unavailable.

Note that when you opt to accept configuration changes from or deploy to an FDM-managed HA pair, you are communicating with the active device of the HA pair. Any changes made to the primary device are transferred over the link between the primary and the secondary device. CDO deploys to and accepts changes only from the primary device; thusly, the **Inventory** page displays a single entry for the pair. Once the deploy occurs, the primary device synchronized any configuration changes to the secondary device.

Simi liar to how CDO communicates with only the active device, when you schedule or opt to back up an FDM-managed HA pair, only the active device is eligible to back up.

Note If the HA devices experience an issue during the creation process or the HA pair does not result with a healthy status, you must manually break the HA configuration before you attempt to create the pair again.

Procedure

Create an HA pair from two standalone FDM-managed devices with the following procedure:

Procedure

Step 1 In the navigation bar, click **Inventory**.

Step 2 Click the **Devices** tab to locate your device.

Step 3 Click the **FTD**tab and select the device you want to establish as the primary device.

Note CDO does not support creating an HA pair with devices configured with DHCP.

Step 4 In the Management pane, click **High Availability**.

Step 5 Locate the area for the secondary device and click **Select Device**, then choose a device from the list of eligible devices.

Step 6 Configure the Failover link.

a. Click **Physical Interface**and select an interface from the drop-down menu.

b. Select the appropriate **IP Type**.

c. Enter the **Primary IP** address.

d. Enter the **Secondary IP** address.

e. Enter the **Netmask**. By default, this value is 24.

f. If applicable, enter a valid **IPSec Encryption Key**.

Step 7 Configure the Stateful link. If you want to use the same configuration as the failover link, check the **The same as Failover Link** checkbox. If you want to use a different configuration, use the following procedure:

a. Click **Physical Interface** and select an interface from the drop-down menu. Note that both the primary and secondary device **must** have the same number of physical interfaces.

b. Select the appropriate **IP Type**.

c. Enter the **Primary IP** address.

d. Enter the **Secondary IP** address.

e. Enter the **Netmask**. By default, this value is 24.

Step 8 Click **Create** in the upper right corner of the screen to finish the wizard. CDO immediately redirects you to the High Availability Status page. From this page you can monitor the status of the HA creation. Note that once the HA pair is created, the **Inventory** page displays the pair as a single row.

Step 9 Preview and Deploy Configuration Changes for All Devices the changes you made now, or wait and deploy multiple changes at once.

FDM-Managed Devices in High Availability Page

The FDM-managed in High Availability (HA) management page is a multi-purpose page for FDM-managed devices. This page is only available for devices that are already configured as an HA pair. You can onboard an FDM-managed HA pair or you can create an FDM-managed HA pair from two standalone FDM-managed devices.

If you select a standalone FDM-managed device from the **Inventory** page, this page acts as a wizard for creating an HA pair. At this time, you must have two FDM-managed devices onboarded to Cisco Defense Orchestrator to create a pair. To create an FDM-managed HA pair in CDO, see Create an FDM-Managed High Availability Pair.

If you select an FDM-managed HA pair from the **Inventory** page, this page acts as an overview page. From here you can view the HA configuration and the failover history, as well as actionable items such as force a failover, edit the failover criteria, and remove the HA link.

High Availability Management Page

To see the High Availability page, use the following procedure:

Procedure

Step 1 In the navigation bar, click **Inventory**.

Step 2 Click the **Devices** tab to locate your device.

Step 3 Click the **FTD**tab and select a standlalone FDM-managed device **or** the active FDM-managed device of the FDM-managed HA pair.

Step 4 In the **Management** pane, click **High Availability**.

Related Information:

- FDM-Managed High Availability Failover History
- Edit High Availability Failover Criteria
- Force a Failover on an FDM-Managed High Availability Pair
- Break an FDM-Managed High Availability Pairing
- Refresh the FDM-Managed High Availability Status

Edit High Availability Failover Criteria

You can edit the failover criteria after the FDM-managed HA pair is created.

Procedure

Step 1 In the navigation bar, click **Inventory**.

Step 2 Click the **Devices** tab to locate your device.

Step 3 Click the **FTD** tab and select the active device of the FDM-managed HA pair.

Step 4 In the Management pane, click **High Availability**.

Step 5 In the Failover Criteria window click **Edit**.

Step 6 Make any necessary changes and click **Save**.

Step 7 Preview and Deploy Configuration Changes for All Devices the changes now you made to the active device, or wait and deploy multiple changes at once.

Break an FDM-Managed High Availability Pairing

When you break HA, the configured interfaces on the standby device are automatically disabled. The devices may experience a disruption in traffic during this process. After the HA pair is successfully removed you will be redirected from the status page to the High Availability page where you will have the option to create another HA pair with the same primary device.

Note You cannot deploy to either of the devices until the HA pair is successfully removed.

Break HA with Management Interfaces

When you break HA for a pair that is configure with management interfaces, the break may take 10 minutes or longer to complete and both devices go offline during this process. When the HA configuration is successfully removed, CDO displays both units as standalone devices in the **Services & Devices** page.

Break HA with Data Interfaces

When you break HA for a pair that is configured with data interfaces, the break may take 20 minutes or more to complete and both of the devices go offline. you must manually reconnect the active device after the HA configuration is removed.

The standby device retains the HA configuration, though, and will become unreachable since it has the same configuration as the active device. You must manually reconfigure the IP interfaces outside of CDO, and then re-onboard the device as a standalone.

Break High Availability

Use the following procedure to remove the HA pairing of two FDM-managed devices:

Procedure

Step 1 In the navigation bar, click **Inventory** and select the active device of the FDM-managed HA pair.

Step 2 Click the **Devices** tab to locate your device.

Step 3 Click the **FTD** tab.

Step 4 In the Management pane, click **High Availability**.

Step 5 Click **Break High Availability**.

Step 6 CDO removes the HA configuration and both devices are displayed as standalone devices in the **Inventory** page.

Step 7 Deploy Configuration Changes from CDO to FDM-Managed Device to deploy the new configuration to both devices.

Step 8 Preview and Deploy Configuration Changes for All Devices the changes you made to the active device now, or wait and deploy multiple changes at once.

Break Out-of-Band High Availability

If you break an FDM-managed HA pair using the FDM interface, the configuration status of the HA pair in Cisco Defense Orchestrator changes to **Conflict Detected.** After you break HA, you must deploy the changes to the primary device through FDM-managed and then Resolve Configuration Conflicts state in CDO.

After the device is back in the Synced state, you can deploy configuration changes made in CDO to the device.

We do **not** recommend reverting changes from CDO after breaking HA using the FDM-managed interface.

Related Information:

- FDM-Managed High Availability Failover History
- Refresh the FDM-Managed High Availability Status
- Force a Failover on an FDM-Managed High Availability Pair
- About Device Configuration Changes

Force a Failover on an FDM-Managed High Availability Pair

Switch the active and standby devices within an FDM-managed HA pair by forcing a failover. Note that if you recently applied a new certificate to the active device and have **not** deployed changes, the standby device retains the original certificate and failover will fail. The active and standby devices must have the same certificate applied. Use the following procedure to manually force a failover:

Procedure

Step 1 In the navigation bar, click **Inventory**.

Step 2 Click the **Devices** tab to locate your device.

Step 3 Click the **FTD** tab.

Step 4 Select the active device of the FDM-managed HA pair.

Step 5 In the Management pane, click **High Availability**.

Step 6 Click the options icon  .

Step 7 Click **Switch Mode**. The active device is now on standby, and the standby device is now active.

Related Information:

- Break an FDM-Managed High Availability Pairing
- FDM-Managed High Availability Failover History
- Refresh the FDM-Managed High Availability Status

- Force a Failover on an FDM-Managed High Availability Pair

FDM-Managed High Availability Failover History

Procedure

Step 1 In the navigation bar, click **Inventory**.

Step 2 Click the **Devices** tab to locate your device.

Step 3 Click the **FTD** tab.

Step 4 Select the active device of the FDM-managed HA pair.

Step 5 In the Management pane, click **High Availability**.

Step 6 Click **Failover History**. CDO generates a window that details the failover history for both the primary and secondary device since the HA pair was formed.

Note Failover history is also displayed in the pair's change log, available from the **Inventory** page.

Related Information:

- Break an FDM-Managed High Availability Pairing
- FDM-Managed High Availability Failover History
- Refresh the FDM-Managed High Availability Status
- Force a Failover on an FDM-Managed High Availability Pair

Refresh the FDM-Managed High Availability Status

Procedure

Step 1 In the navigation bar, click **Inventory**.

Step 2 Click the **Devices** tab to locate your device.

Step 3 Click the **FTD** tab and select the FDM-managed device or the FDM-managed HA pair.

Step 4 In the **Management** pane, click **High Availability**.

Step 5 Click the options icon .

Step 6 Click **Get Latest Status**. CDO requests a health status from the primary device.

Related Information:

- Break an FDM-Managed High Availability Pairing
- FDM-Managed High Availability Failover History
- Refresh the FDM-Managed High Availability Status
- Force a Failover on an FDM-Managed High Availability Pair

Failover and Stateful Link for FDM-Managed High Availability

Failover Link and (Optional) Stateful Link

The failover link is a dedicated connection between the two units. The stateful failover link is also a dedicated connection, but you can either use the one failover link as a combined failover/state link, or you can create a separate, dedicated state link. If you use just the failover link, the stateful information also goes over that link: you do not lose stateful failover capability. By default, the communications on the failover and stateful failover links are plain text (unencrypted). You can encrypt the communications for enhanced security by configuring an IPsec encryption key.

You can use any unused data physical interfaces as the failover link and optional dedicated state link. However, you cannot select an interface that is currently configured with a name, or one that has subinterfaces. The failover and stateful failover link interfaces are not configured as normal networking interfaces. They exist for failover communication only, and you cannot use them for through traffic or management access. Because the configuration is synchronized between the devices, you must select the same port number for each end of a link. For example, GigabitEthernet1/3 on both devices for the failover link.

Note The FDM-managed device does not support sharing interfaces between user data and the failover link.

Failover Link

The two units in a failover pair constantly communicate over a failover link to determine the operating status of each unit and to synchronize configuration changes. The following information is shared over the link:

- The unit state (active or standby)
- Hello messages (keep-alives)
- Network link status
- MAC address exchange
- Configuration replication and synchronization

You can use an unused data interface (physical, redundant, or EtherChannel) as the failover link; however, you cannot specify an interface that is currently configured with a name. Do **not** use a subinterface as the failover link.

The failover link interface is not configured as a normal networking interface; it exists for failover communication only. This interface can only be used for the failover link (and also for the state link).

Stateful Link

The active unit uses the state link to pass connection state information to the standby device. This means that the standby unit can maintain certain types of connections without impacting the user. This information helps the standby unit maintain existing connections when a failover occurs.

You can use a dedicated data interface (physical, redundant, or EtherChannel) for the state link. For an EtherChannel used as the state link, to prevent out-of-order packets, only one interface in the EtherChannel is used. If that interface fails, then the next interface in the EtherChannel is used.

Using a single link for both the failover and stateful failover links is the best way to conserve interfaces. However, you must consider a dedicated interface for the state link and failover link, if you have a large configuration and a high traffic network. We recommend that the bandwidth of the stateful failover link should match the largest bandwidth of the data interfaces on the device.

FDM-Managed Device Settings

Configure an FDM-Managed Device's System Settings

Use this procedure to configure settings on a single FDM-managed device:

Procedure

Step 1 Open the **Inventory** page.

Step 2 Click the **Devices** tab to locate your device.

Step 3 Click the **FTD** tab and select the FDM-managed device you want to configure the settings. To narrow down your search results and easily find the FDM-managed devices, you can make use of the filter button.

Step 4 In the **Management** pane at the right, click **Settings**.

Step 5 Click the **System Settings** tab.

Step 6 Edit any of these device settings:

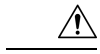
- Configure Management Access
- Configure Logging Settings
- Configure DHCP Servers
- Configure DNS Server
- Hostname
- Configure NTP Server
- Configure URL Filtering
- Cloud Services
- Enabling or Disabling Web Analytics

Configure Management Access

By default, you can reach the device's management address from any IP address. System access is protected by username and password only. However, you can configure an access list to allow connections from specific IP addresses or subnets only to provide another level of protection.

You can also open data interfaces to allow an FDM-managed device or SSH connections to the CLI. You can then manage the device without using the management address. For example, you could allow management

access to the outside interface, so that you can configure the device remotely. The username and password protects against unwanted connections. By default, HTTPS management access to data interfaces is enabled on the inside interface, but it's disabled on the outside interface. For device models that have a default "inside" bridge group, this means that you can make FDM-managed device connections through any data interface within the bridge group to the bridge group IP address (default is 192.168.1.1). You can open a management connection only on the interface through which you enter the device.



Caution If you constrain access to specific addresses, you can easily lock yourself out of the system. If you delete access for the IP address that you are currently using, and there's no entry for "any" address, you'll lose access to the system when you deploy the policy. Be mindful of this when configuring the access list.

Create Rules for Management Interfaces

Use the following procedure to create rules for managment interfaces:

Procedure

Step 1 Click **New Access** in the Management Interface section.

- **Protocol**. Select whether the rule is for HTTPS (port 443) or SSH (port 22).
- **Allowed Networks**. Select the network object that defines the IPv4 or IPv6 network or host that should be able to access the system. To specify "any" address, select **any-ipv4** (0.0.0.0/0) and **any-ipv6**(::/0).

Step 2 Click **Save**.

Create Rules for Data Interfaces

Use the following procedure to create rules for data interfaces:

Procedure

Step 1 Click **New Access** in the Data Interface section.

- **Interface**. Select the interface on which you want to allow management access.
- **Protocol**. Select whether the rule is for HTTPS (port 443), SSH (port 22), or both. You cannot configure HTTPS rules for the outside interface if it's used in a remote access VPN connection profile.
- **Allowed Networks**. Select the network object that defines the IPv4 or IPv6 network or host that should be able to access the system. To specify "any" address, select **any-ipv4** (0.0.0.0/0) and **any-ipv6** (::/0).

Step 2 Click **Save**.

Step 3 Preview and Deploy Configuration Changes for All Devices the changes you made now, or wait and deploy multiple changes at once.

Configure Logging Settings

This procedure describes how to enable logging of diagnostic (data) messages, file and malware events, intrusion events, and console events. Connection events are not logged as a result of these settings; they are logged if connection logging is configured on access rules, security intelligence policies, or SSL decryption rules.

Procedure

Step 1 Configure an FDM-Managed Device's System Settings.

Step 2 On the System Settings page click **Logging** in the settings menu.

Step 3 **Data logging**. Slide the **Data Logging** slider to **On** to capture diagnostic logging syslog messages. Click the plus button  to specify the syslog server object that represents the syslog server that you want to send the events to. (You can also create a syslog server object at this point.) Additionally, select the minimum level of Message Severity Levels you want to log.

This will send data logging events for any type of syslog message, with your minimum chosen severity level, to the syslog server.

Note Cisco Defense Orchestrator doesn't currently support creating a Custom Logging Filter for Data Logging. For finer control of which messages you send to the syslog server, we recommend you define this setting in an FDM-managed device. To do so, log on to an FDM-managed device, and navigate **System Settings > Logging Settings**.

Tip Do not enable data logging if you are a Cisco Security Analytics and Logging customer *unless* you forward the data logging events to a syslog server other than the Secure Event Connector. Data events (diagnostic events) are not traffic events. Sending the data events to a different syslog server removes the burden on the SEC from analyzing and filtering them out.

Step 4 **File/Malware Log Settings**. Slide the slider to **On** to capture file and malware events. Specify the syslog server object that represents the syslog server that you want to send the events to. You can also create a syslog server object at this point if you have not already.

File and malware events are generated at the same severity level. The minimum level of Message Severity Levels you select will be assigned to all file and malware events.

File and malware events are reported when a file or malware policy in any access control rule has been triggered. This is not the same as a connection event. Note that the syslog settings for file and malware events are relevant only if you apply file or malware policies, which require the and Malware licenses.

For Cisco Security Analytics and Logging subscribers:

- If you send events to the Cisco cloud through a Secure Event Connector (SEC), specify an SEC as your syslog server. You will then be able to see these events alongside file policy and malware policy connection events.
- If you send events directly to the Cisco cloud without an SEC, you do not need to enable this setting. File and malware events are sent if the access control rule is configured to send connection events.

Step 5 **Intrusion Logging**. Send intrusion events to a syslog server by specifying the syslog server object that represents the syslog server you want to send events to. You can also create a syslog server object at this point if you have not already.

Intrusion events are reported when an intrusion policy in any access control rule has been triggered. This is not the same as a connection event. Note that the syslog settings for intrusion events are relevant only if you apply intrusion policies, which require the license.

For Cisco Security Analytics and Logging subscribers:

- If you send events to the Cisco cloud through a Secure Event Connector (SEC), specify an SEC as your syslog server. You will then be able to see these events alongside file policy and malware policy connection events.
- If you send events directly to the Cisco cloud without an SEC, you do not need to enable this setting. Intrusion events are sent to the Cisco cloud if the access control rule is configured to send connection events.

Step 6 **Console Filter**. Slide the slider to **On** to send data logging (diagnostic logging) events to a console rather than to a syslog server. Additionally, select the minimum level of event severity you want to log. This will send a data logging event for any type of syslog message, with your chosen severity level.

You will see these messages when you log into the CLI on the console port of your FDM-managed device. You can also see these logs in an SSH session to other FDM-managed device interfaces (including the management interface) by using the **show console-output** command. In addition, you can see these messages in real time in the diagnostic CLI by entering **system support diagnostic-cli** from the main CLI.

Step 7 Click **Save**.

Step 8 Preview and Deploy Configuration Changes for All Devices the changes you made now, or wait and deploy multiple changes at once.

Message Severity Levels

The following table lists the syslog message severity levels.

Level Number	Severity Level	Description
0	**emergencies**	System is unusable.
1	**alert**	Immediate action is needed.
2	**critical**	Critical conditions.
3	**error**	Error conditions.
4	**warning**	Warning conditions.
5	**notification**	Normal but significant conditions.
6	**informational**	Informational messages only.
7	**debugging**	Debugging messages only.

Level Number	Severity Level	Description
Note	FDM-managed device does not generate syslog messages with a severity level of zero (emergencies).	

Configure DHCP Servers

A Dynamic Host Configuration Protocol (DHCP) server provides network configuration parameters, such as IP addresses, to DHCP clients. You can configure a DHCP server on an interface to provide configuration parameters to DHCP clients on the attached network.

An IPv4 DHCP client uses a broadcast rather than a multicast address to reach the server. The DHCP client listens for messages on UDP port 68. The DHCP server listens for messages on UDP port 67. The DHCP server does not support BOOTP requests.

DHCP clients must be on the same network as the interface on which the server is enabled. There cannot be an intervening router between the server and client, although there can be a switch.

Caution Do not configure a DHCP server on a network that already has a DHCP server operating on it. The two servers will conflict with each other, and the results will be unpredictable.

Procedure

Step 1 The section has two areas. Initially, the Configuration section shows the global parameters. The DHCP Servers area shows the interfaces on which you have configured a server, whether the server is enabled, and the address pool for the server.

Step 2 In the **Configuration** section, configure auto configuration and global settings.

DHCP auto configuration enables the DHCP server to provide DHCP clients with DNS server, domain name, and WINS server information obtained from a DHCP client that's running on the specified interface. Typically, you would use auto configuration if you're obtaining an address using DHCP on the outside interface, but you could choose any interface that obtains its address through DHCP. If you cannot use auto configuration, you can manually define the required options.

a. Click the **Enable Auto Configuration** slider to On if you want to use auto configuration, and in the **From Interface** pull-down, select the interface that's obtaining its address through DHCP.

b. If you do not enable auto configuration, or if you want to override any of the automatically configured settings, configure the following global options. These settings are sent to DHCP clients on all interfaces that host DHCP server.

1. **Primary WINS IP Address**, **Secondary WINS IP Address**. The addresses of the Windows Internet Name Service (WINS) servers that clients should use for NetBIOS name resolution.

2. **Primary DNS IP Address**, **Secondary DNS IP Address**. The addresses of the Domain Name System (DNS) servers that clients should use for domain name resolution. Click **Apply Umbrella Settings** if you want to populate the DNS IP address fields with Cisco Umbrella DNS servers. Clicking the button loads the appropriate IP addresses into the fields.

c. Click **Save**.

Step 3 In the DHCP Servers section, either edit an existing server, or click **New DHCP Server** to add and configure a new server.

a. Configure the server properties:

1. **Enable DHCP Server**. Whether to enable the server. You can configure a server but keep it disabled until you are ready to use it.
2. **Interface**. Select the interface on which you will provide DHCP addresses to clients. The interface must have a static IP address; you cannot be using DHCP to obtain the interface address if you want to run a DHCP server on the interface. For bridge groups, you configure the DHCP server on the Bridge Virtual Interface (BVI), not the member interfaces, and the server operates on all member interfaces. You cannot configure DHCP server on the Diagnostic interface, configure it on the Management interface instead, on the **Device** > **System Settings > Management Interface** page.
3. **Address Pool**. Add the single IP address or an IP address range of a DHCP server. The range of IP addresses from lowest to highest that the server is allowed to provide to clients that request an address. The range of IP addresses must be on the same subnet as the selected interface and cannot include: the IP address of the interface itself, the broadcast address, or the subnet network address. Specify the start and end address for the pool, separated by a hyphen. For example, 10.100.10.12-10.100.10.250.

b. Click **OK**.

Step 4 Click **Save**.

Step 5 Preview and Deploy Configuration Changes for All Devices the changes you made now, or wait and deploy multiple changes at once.

Configure DNS Server

A Domain Name System (DNS) server is used to resolve hostnames to IP addresses. DNS servers are used by the management interface.

Procedure

Step 1 In **Primary, Secondary, Tertiary DNS IP Address**, enter the IP addresses of up to three DNS servers in order of preference. The primary DNS server is used unless it cannot be contacted, in which case the secondary is tried, and finally the tertiary. Click **Apply Umbrella Settings** if you want to populate the DNS IP address fields with Cisco Umbrella DNS servers. Clicking the button loads the appropriate IP addresses into the fields.

Step 2 In **Domain Search Name**, enter the domain name for your network; for example, example.com. This domain gets appended to hostnames that are not fully qualified; for example, serverA becomes serverA.example.com.

Step 3 Click **Save**.

Step 4 Preview and Deploy Configuration Changes for All Devices the changes you made now, or wait and deploy multiple changes at once.

Management Interface

The management interface is a virtual interface attached to the physical management port. The physical port is named the Diagnostic interface, which you can configure on the Interfaces page with the other physical ports. On virtual FDM-managed devices, this duality is maintained even though both interfaces are virtual.

The management interface has two uses:

- You can open web and SSH connections to the IP address and configure the device through the interface.
- The system obtains smart licensing and database updates through this IP address.

If you use the CLI setup wizard, you configure the management address and gateway for the device during initial system configuration. If you use the FDM-managed setup wizard, the management address and gateway remain the defaults.

If necessary, you can change these addresses through an FDM-managed device. You can also change the management address and gateway in the CLI using the **configure network ipv4 manual** and **configure network ipv6 manual** commands.

You can define static addresses, or obtain an address through DHCP if another device on the management network is acting as a DHCP server. By default, the management address is static, and a DHCP server runs on the port (except for Virtual FDM-Managed Device, which does not have a DHCP server). Thus, you can plug a device directly into the management port and get a DHCP address for your workstation. This makes it easy to connect to and configure the device.

Caution If you change the address to which you are currently connected, you will lose access to the FDM-managed device (or the CLI) when you save the changes, as they are applied immediately. You will need to reconnect to the device. Ensure that the new address is valid and available on the management network.

Procedure

Step 1 Configure the management IP address, network mask or IPv6 prefix, and gateway (if necessary) for IPv4, IPv6, or both. You must configure at least one set of properties. Leave one set blank to disable that addressing method.

Step 2 Select **Type** > **DHCP** to obtain the address and gateway through DHCP or IPv6 auto configuration. However, you cannot use DHCP if you are using the data interfaces as the gateway. In this case, you must use a static address.

Step 3 Click **Save**.

Step 4 Preview and Deploy Configuration Changes for All Devices the changes you made now, or wait and deploy multiple changes at once.

Hostname

You can change the device hostname.

Procedure

Step 1 In the **Firewall Hostname** field, enter a new hostname for the device.

Step 2 Click **Save**.

Step 3 Preview and Deploy Configuration Changes for All Devices the changes you made now, or wait and deploy multiple changes at once.

Configure NTP Server

Configure Network Time Protocol (NTP) servers to set the time on the system.

Procedure

Step 1 Select whether you want to use your own (manual) or Cisco's time servers.

- **New NTP Server**. Enter the fully qualified domain name or IP address of the NTP server you want to use. For example, ntp1.example.com or 10.100.10.10.
- **Use Default**.

Step 2 Click **Save.**

Step 3 Preview and Deploy Configuration Changes for All Devices the changes you made now, or wait and deploy multiple changes at once.

Configure URL Filtering

The system obtains the URL category and reputation database from Cisco Collective Security Intelligence (CSI). These preferences control database updates and how the system handles URLs with unknown category or reputation. You must enable the URL Filtering license to set these preferences.

Caution You can configure URL Filtering Preferences if you do not have a URL Smart License, but you need the smart license to deploy. You will be blocked from deploying until you add a URL Smart License.

Procedure

Step 1 Enable the applicable options:

- Click the **Enable Automatic Updates** slider On to automatically check for and download updated URL data, which includes category and reputation information. After you deploy, the FDM-managed device checks for updates every 30 minutes.

- Click the **Query Cisco CSI for Unknown URLs** slider to ON to check the Cisco CSI for updated information on URLs that do not have category and reputation data in the local URL filtering database.
- **URL Time to Live** is only in effect if you enable the **Query Cisco CSI for Unknown URLs** option. This determines how long to cache the category and reputation lookup values for a given URL. When the time to live expires, the next attempted access of the URL results in a fresh category/reputation lookup. A shorter time results in more accurate URL filtering, a longer time results in better performance for unknown URLs. The default selection is **Never**.

Step 2 Click **Save**.

Step 3 Preview and Deploy Configuration Changes for All Devices the changes you made now, or wait and deploy multiple changes at once.

Cloud Services

Use the Cloud Services page to manage cloud-based services.

Note Connecting to the Cisco Success Network and configuring which events are sent to the Cisco cloud are features that can be configured on FDM-managed devices running software versions 6.6 and higher.

Connecting to the Cisco Success Network

By enabling Cisco Success Network, you are providing usage information and statistics to Cisco that are essential for Cisco to provide you with technical support. This information also allows Cisco to improve the product and to make you aware of unused available features so that you can maximize the value of the product in your network.

When you enable the connection, your device establishes a secure connection to the Cisco Cloud so that your device can participate in additional service offerings from Cisco such as technical support services, cloud management and monitoring services. Your device will establish and maintain this secure connection at all times.

Before you begin

To enable Cisco Success Network the device must be enrolled with the cloud using an FDM-managed device. To enroll the device either register the device with Cisco Smart Software Manager (on the Smart Licensing page) or enroll with Cisco Defense Orchestrator by entering a registration key.

Attention If you enable Cisco Success Network on the active unit in a high availability group, you are also enabling the connection on the standby unit.

Procedure

Step 1 Click the **Cloud Services** tab.

Step 2 Click the **Enabled** slider for the Cisco Success Network feature to change the setting as appropriate.

Step 3 Click **Save**.

Step 4 Preview and Deploy Configuration Changes for All Devices the changes you made now, or wait and deploy multiple changes at once.

Sending Events to the Cisco Cloud

You can send events to the Cisco cloud server. From there, various Cisco cloud services can access the events. You can then use these cloud applications, such as Cisco Threat Response, to analyze the events and to evaluate threats that the device might have encountered.

Before you begin

You must register the device with the Cisco Smart Software Manager before you can enable this service.

You can connect to the Cisco Threat Response at https://visibility.amp.cisco.com/ in the US region, https://visibility.amp.cisco.com/ in the EU region. You can watch videos about the use and benefits of the application on YouTube at http://cs.co/CTRvideos. For more information about using Cisco Threat Response with FTD, see *Firepower and CTR Integration Guide*, which you can find at https://www.cisco.com/c/en/us/support/security/defense-center/products-installation-and-configuration-guides-list.html.

Procedure

Step 1 Click the **Cloud Services** tab.

Step 2 Click the **Enabled** slider for the **Send Events to the Cisco Cloud** option to change the setting as appropriate.

Step 3 When you are enabling the service, you are prompted to select the events to send to the cloud.

- **File/Malware** - For any file policies, you have applied in any access control rule.
- **Intrusion Events** - For any intrusion policies, you have applied in any access control rule.
- **Connection Events** - For access control rules where you have enabled logging. When you select this option, you can also elect to send All Connection Events, or only send the High Priority connection events. High-priority connection events are those related to connections that trigger intrusion, file, or malware events, or that match Security Intelligence blocking policies.

Step 4 Click **Save**.

Step 5 Preview and Deploy Configuration Changes for All Devices the changes you made now, or wait and deploy multiple changes at once.

Enabling or Disabling Web Analytics

Enabling web analytics provides anonymous product usage information to Cisco based on page hits. The information includes pages viewed, the time spent on a page, browser versions, product version, device hostname, and so forth. This information can help Cisco determine feature usage patterns and help Cisco improve the product. All usage data is anonymous and no sensitive data is transmitted. You can use CDO to configure this feature on all versions of FDM-managed device.

Web analytics is enabled by default.

Procedure

Step 1 Click the **Web Analytics** tab.

Step 2 Click the **Enable** slider for the **Web Analytics** feature to change the setting as appropriate.

Step 3 Click **Save**.

Step 4 Preview and Deploy Configuration Changes for All Devices the changes you made now, or wait and deploy multiple changes at once.

CDO Command Line Interface

CDO provides users with a command line interface (CLI) for managing , FDM-managed threat defense devices. Users can send commands to a single device or to multiple devices simultaneously.

Related Information:

- For FTD CLI documentation, see Cisco Firepower Threat Defense Command Reference. Note that FDM-managed devices have limited CLI functionality. These devices only have the following commands: `show, ping, traceroute, packet-tracer, failover, and shutdown.`

Using the Command Line Interface

Procedure

Step 1 Open the **Inventory** page.

Step 2 Click the **Devices** button abobve the Inventory table.

Step 3 Use the device tabs and filter button to find the device you want to manage using the command line interface (CLI).

Step 4 Select the device.

Step 5 In the **Device Actions** pane, click **>_Command Line Interface.**

Step 6 Click the **Command Line Interface** tab.

Step 7 Enter your command, or commands, in the command pane and click **Send.** The device's response to the command(s) are displayed below in the "response pane."

Note If there are limitations on the commands you can run, those limitations are listed above the command pane.

Related Topics

Entering Commands in the Command Line Interface, on page 314

Entering Commands in the Command Line Interface

A single command can be entered on a single line or several commands can be entered sequentially on several lines and CDO will execute them in order. The following ASA example sends a batch of commands which creates three network objects and a network object group that contains those network objects.

Entering FDM-managed device Commands: The CLI console uses the base Threat Defense CLI. You cannot enter the diagnostic CLI, expert mode, or FXOS CLI (on models that use FXOS) using the CLI console. Use SSH if you need to enter those other CLI modes.

Work with Command History

After you send a CLI command, CDO records that command in the history pane on the **Command Line Interface** page. You can rerun the commands saved in the history pane or use the commands as a template:

Procedure

Step 1 On the **Inventory** page, select the device you want to configure.

Step 2 Click the **Devices** tab to locate the device.

Step 3 Click the appropriate device type tab.

Step 4 Click **>_Command Line Interface**.

Step 5 Click the clock icon to expand the history pane if it is not already expanded.

Step 6 Select the command in the history pane that you want to modify or resend.

Step 7 Reuse the command as it is or edit it in the command pane and click **Send**. CDO displays the results of the command in the response pane.

Note CDO displays the `Done!` message in the response pane in two circumstances:

- After a command has executed successfully.
- When the command has no results to return. For example, you may issue a show command with a regular expression searching for a configuration entry. If there is no configuration entry that meets the criteria of the regular expression, CDO returns `Done!`.

Bulk Command Line Interface

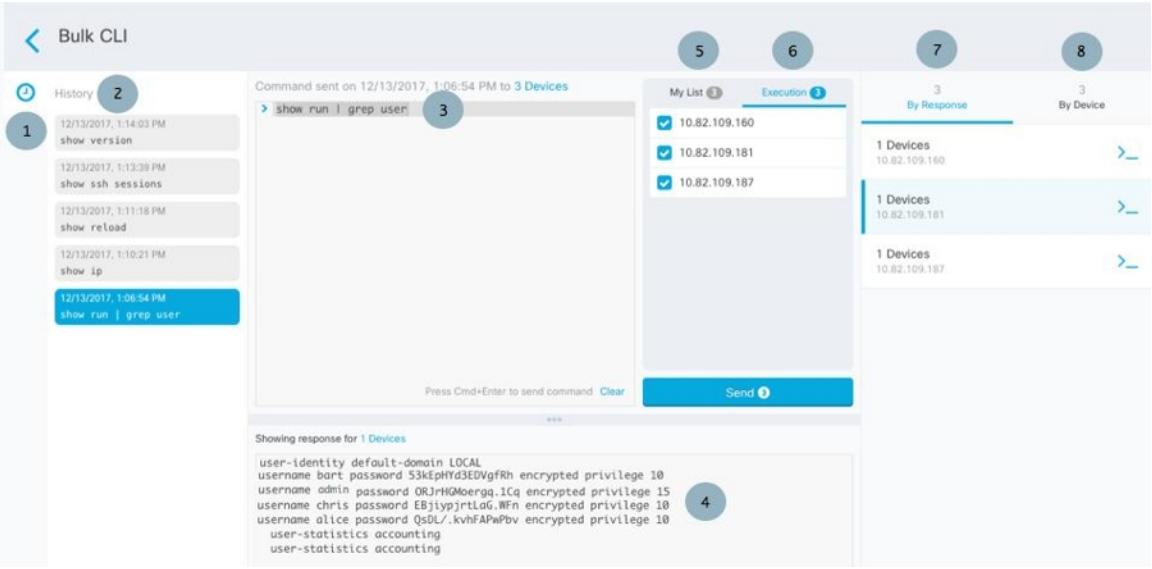
CDO offers users the ability to manage Secure Firewall ASA, FDM-managed Threat Defense, SSH, and Cisco IOS devices using a command-line interface (CLI). Users can send commands to a single device or to multiple devices of the same kind simultaneously. This section describes sending CLI commands to multiple devices at once.

Related Information:

- For FDM-managed device documentation, CDO supports only the base FTD CLI. These devices only have the following commands: `show, ping, traceroute, packet-tracer, failover, and shutdown`.

  For Threat Defense CLI documentation, see Cisco Firepower Threat Defense Command Reference.

Bulk CLI Interface



Note CDO displays the **Done!** message in two circumstances:

- After a command has executed successfully without errors.
- When the command has no results to return. For example, you may issue a show command with a regular expression searching for a certain configuration entry. If there is no configuration entry that meets the criteria of the regular expression, CDO returns **Done!**.

Number	Description
1	Click the clock to expand or collapse the command history pane.
2	Command history. After you send a command, CDO records the command in this history pane so you can return to it, select it, and run it again.

Number	Description
3	Command pane. Enter your commands at the prompt in this pane.
4	Response pane. CDO displays the device's response to your command as well as CDO messages. If the response was the same for more than one device, the response pane displays the message "Showing Responses for X devices." Click X devices and CDO displays all the devices that returned the same response to the command. **Note** CDO displays the **Done!** message in two circumstances: • After a command has executed successfully without errors. • When the command has no results to return. For example, you may issue a show command with a regular expression searching for a certain configuration entry. If there is no configuration entry that meets the criteria of the regular expression, CDO returns **Done!**.
5	**My List** tab displays the devices you chose from the **Inventory** table and allows you to include or exclude devices you want to send a command to.
6	The **Execution** tab, highlighted in the figure above, displays the devices in the command that is selected in the history pane. In this example, the show run | grep user command is selected in the history pane and the Execution tab shows that it was sent to 10.82.109.160, 10.82.109.181, and 10.82.10.9.187.
7	Clicking the **By Response** tab shows you the list of responses generated by the command. Identical responses are grouped together in one row. When you select a row in the By Response tab, CDO displays the response to that command in the response pane.
8	Clicking the **By Device** tab displays individual responses from each device. Clicking one of the devices in the list allows you to see the response to the command from a specific device.

Send Commands in Bulk

Procedure

Step 1 In the navigation bar, click **Inventory**.

Step 2 Click the **Devices** tab to locate the devices.

Step 3 Select the appropriate device tab and use the filter button to find the devices you want to configure using the command line interface.

Step 4 Select the devices.

Step 5 in the **Device Actions** pane, click **>_Command Line Interface**.

Step 6 You can check or uncheck devices you want to send the commands to in the **My List** field.

Step 7 Enter your commands in the command pane and click **Send**. The command output is displayed in the response pane, the command is logged in the Change Log, and the command CDO records your command in the History pane in the Bulk CLI window.

Work with Bulk Command History

After you send a bulk CLI command, CDO records that command in the Bulk CLI Interface history page. You can rerun the commands saved in the history pane or use the commands as a template. The commands in the history pane are associated with the original devices on which they were run.

Procedure

Step 1 In the navigation bar, click **Inventory**.

Step 2 Click the **Devices** tab to locate devices.

Step 3 Click the appropriate device type tab and click the filter icon to find the devies you want to configure.

Step 4 Select the devices.

Step 5 Click **Command Line Interface**.

Step 6 **Select** the command in the History pane that you want to modify or resend. Note that the command you pick is associated with specific devices and not necessarily the ones you chose in the first step.

Step 7 Look at the My List tab to make sure the command you intend to send will be sent to the devices you expect.

Step 8 Edit the command in the command pane and click **Send**. CDO displays the results of the command in the response pane.

Work with Bulk Command Filters

After you run a bulk CLI command you can use the **By Response** filter and the **By Device** filter to continue to configure the devices.

By Response Filter

After running a bulk command, CDO populates the **By Response** tab with a list of responses returned by the devices that were sent the command. Devices with identical responses are consolidated in a single row. Clicking a row in the **By Response** tab displays the response from the device(s) in the response pane. If the response pane shows a response for more than one device, it displays the message "Showing Responses for X devices." Click **X devices** and CDO displays all the devices that returned the same response to the command.

To send a command to the list of devices associated with a command response, follow this procedure:

Procedure

Step 1 Click the command symbol in a row in the **By Response** tab.

Step 2 Review the command in the command pane and click **Send** to resend the command or click **Clear** to clear the command pane and enter a new command to send to the devices and then click **Send**.

Step 3 Review the responses you receive from your command.

Step 4 If you are confident that the running configuration file on the devices you chose reflects your change, type `write memory` in the command pane and click **Send**. This saves your running configuration to the startup configuration.

By Device Filter

After running a bulk command, CDO populates the the Execution tab and the By Device tab with the list of devices that were sent the command. Clicking a row in the By Device tab displays the response for each device.

To run a command on that same list of devices, follow this procedure:

Procedure

Step 1 Click the **By Device** tab.

Step 2 Click **>_Execute a command on these devices**.

Step 3 Click **Clear** to clear the command pane and enter a new command.

Step 4 In the My List pane, specify the list of devices you want to send the command to by checking or unchecking individual devices in the list.

Step 5 Click **Send**. The response to the command is displayed in the response pane. If the response pane shows a response for more than one device, it displays the message "Showing Responses for X devices." Click X devices and CDO displays all the devices that returned the same response to the command.

Step 6 If you are confident that the running configuration file on the devices you chose reflects your change, type `write memory` in the command pane and click **Send**.

Command Line Interface Macros

A CLI macro is a fully-formed CLI command ready to use, or a template of a CLI command you can modify before you run it. All macros can be run on one or more FTD devices simultaneously.

Use CLI macros that resemble templates to run the same commands on multiple devices at the same time. CLI macros promote consistency in your device configurations and management. Use fully-formed CLI macros to get information about your devices. There are different CLI macros that are immediately available for you to use on your FTD devices.

You can create CLI macros for monitoring tasks that you perform frequently. See Create a CLI Macro from a New Command for more information.

CLI macros are system-defined or user-defined. System-defined macros are provided by CDO and can not be edited or deleted. User-defined macros are created by you and can be edited or deleted.

Note You can only create macros for a device once it has been onboarded to CDO.

Using the ASA as an example, if you want to find a particular user on one of your ASAs, you could run this command:

```
show running-config | grep username
```

When you run the command, you would replace *username* with the username of the user you are searching for. To make a macro out of this command, use the same command and put curly braces around *username.*

```
> show running-config | grep {{username}}
```

You can name your parameters anything you want. You can also create the same macro with this parameter name:

```
> show running-config | grep {{username_of_local_user_stored_on_asa}}
```

The parameter name can be descriptive and must use alphanumeric characters and underlines. The command syntax, in this case the

```
show running-config | grep
```

part of the command, must use proper CLI syntax for the device you are sending the command to.

Create a CLI Macro from a New Command

Procedure

Step 1 Before you create a CLI macro, test the command in CDO's Command Line Interface to make sure the command syntax is correct and it returns reliable results.

Note

- For FDM-managed devices, CDO supports only the commands that can be run in FDM's CLI console: `show`, `ping`, `traceroute`, `packet-tracer`, `failover`, `reboot`, and `shutdown`. See Cisco Firepower Threat Defense Command Reference for a full description of the syntax of those commands.

Step 2 In the navigation bar, click **Inventory**.

Step 3 Click the **Devices** tab to locate the device.

Step 4 Click the appropriate device type tab and select an online and synced device.

Step 5 Click **>_Command Line Interface.**

Step 6 Click the CLI macro favorites star to see what macros already exist.

Step 7 Click the the plus button .

Step 8 Give the macro a unique name. Provide a description and notes for the CLI macro if you wish.

Step 9 Enter the full command in the **Command** field.

Step 10 Replace the parts of the command that you would want to modify, when you run the command, with a parameter name surrounded by curly braces.

Step 11 Click **Create**. The macro you create is available for use on all the devices of that type, not just the one you initially specified.

To run the command see, Run a CLI Macro.

Create a CLI Macro from CLI History or from an Existing CLI Macro

In this procedure, you are going to create a user-defined macro from a command you have already run, another user-defined macro, or from a system-defined macro.

Procedure

Step 1 In the navigation bar, click **Inventory**.

Note If you want to create a user-defined macro from CLI history, select the device on which you ran the command. CLI macros are shared across devices on the same account but not CLI history.

Step 2 Click the **Devices** tab.

Step 3 Click the appropriate device type tab and select an online and synced device.

Step 4 Click **>_Command Line Interface.**

Step 5 Find the command you want to make a CLI macro from and select it. Use one of these methods:

- Click the clock to view the commands you have run on that device. Select the one you want to turn into a macro and the command appears in the command pane.
- Click the CLI macro favorites star to see what macros already exist. Select the user-defined or system-defined CLI macro you want to change. The command appears in the command pane.

Step 6 With the command in the command pane, click the CLI macro gold star . The command is now the basis for a new CLI macro.

Step 7 Give the macro a unique name. Provide a description and notes for the CLI macro if you wish.

Step 8 Review the command in the Command field and make the changes you want.

Step 9 Replace the parts of the command that you would want to modify, when you run the command, with a parameter name surrounded by curly braces.

Step 10 Click **Create**. The macro you create is available for use on all the devices of that type, not just the one you initially specified.

To run the command see, Run a CLI Macro.

Run a CLI Macro

Procedure

Step 1 In the navigation bar, click **Inventory**.

Step 2 Click the **Devices** tab.

Step 3 Click the appropriate device type tab and select one or more devices.

Step 4 Click **>_Command Line Interface.**

Step 5 In the command panel, click the star ★.

Step 6 Select a CLI macro from the command panel.

Step 7 Run the macro one of two ways:

- If the macro has no parameters to define, click **Send**. The response to the command appears in the response pane. You're done.
- If the macro contains parameters, such as the Configure DNS macro below, click **>_ View Parameters.**

Step 8 In the Parameters pane, fill in the values for the parameters in the Parameters fields.

Step 9 Click **Send**. After CDO has successfully, sent the command and updated the device's configuration, you receive the message, Done!

- For an FTD, the device's active configuration is updated.

Step 10 After you send the command you may see the message, "Some commands may have made changes to the running config" along with two links.

- Clicking **Write to Disk** saves the changes made by this command, and any other change that in the running config, to the device's startup config.
- Clicking **Dismiss**, dismisses the message.

Edit a CLI Macro

You can edit user-defined CLI macros but not system-defined macros. Editing a CLI macro changes it for all your FTD devices. Macros are not specific to a particular device.

Procedure

Step 1 In the navigation bar, click **Inventory**.
Step 2 Click the **Devices** tab.
Step 3 Click the appropriate device type tab.
Step 4 Select your device.
Step 5 Click **Command Line Interface**.
Step 6 Select the user-defined macro you want to edit.
Step 7 Click the edit icon in the macro label.
Step 8 Edit the CLI macro in the Edit Macro dialog box.
Step 9 Click **Save**.

See Run a CLI Macro for instructions on how to run the CLI macro.

Delete a CLI Macro

You can delete user-defined CLI macros but not system-defined macros. Deleting a CLI macro deletes it for all your devices. Macros are not specific to a particular device.

Procedure

Step 1 In the navigation bar, click **Inventory**.
Step 2 Click the **Devices** tab.
Step 3 Click the appropriate device type tab.
Step 4 Select your device.
Step 5 Click >_**Command Line Interface**.

Step 6 Select the user-defined CLI macro you want to delete.

Step 7 Click the trash can icon in the CLI macro label.

Step 8 Confirm you want to remove the CLI macro.

Command Line Interface Documentation

CDO partially supports the command line interface of the FDM-managed device. We provide a terminal-like interface within CDO for users to send commands to single devices and multiple devices simultaneously in command-and-response form. For commands that are not supported in CDO, access the device with a device GUI terminal, such as PuTTy or an SSH Client, and see the CLI documentation for more commands.

Export CDO CLI Command Results

You can export the results of CLI commands issued to a standalone device, or several devices, to a comma separated value (.csv) file so you can filter and sort the information in it however you like. You can export the CLI results of a single device, or many devices at once. The exported information contains the following:

- Device
- Date
- User
- Command
- Output

Export CLI Command Results

You can export the results of commands you have just executed in the command window to a .csv file:

Procedure

Step 1 In the navigation bar, click**Inventory**.

Step 2 Click the **Devices** tab.

Step 3 Click the appropriate device type tab.

Step 4 Select the device or devices so they are highlighted.

Step 5 In the **Device Actions** pane for the device, click >_**Command Line Interface**.

Step 6 In the command line interface pane, enter a command and click **Send** to issue it to the device.

Step 7 To the right of the window of entered commands, click the export icon .

Step 8 Give the .csv file a descriptive name and save the file to your local file system. When reading the command output on the .csv file, expand all the cells to see all the results of the command.

Export the Results of CLI Macros

You can export the results of macros that have been executed in the command window. Use the following procedure to export to a .csv file, the results of CLI macros executed on one or multiple devices:

Procedure

Step 1 Open the **Inventory** page.

Step 2 Click the **Devices** tab.

Step 3 Click the appropriate device type tab.

Step 4 Select the device or devices so they are highlighted.

Step 5 In the **Device Actions** pane for the device, click >_**Command Line Interface**.

Step 6 In the left pane of the CLI window, select the CLI macro favorites star .

Step 7 Click on the macro command you want to export. Fill in any appropriate parameters and click **Send**.

Step 8 To the right of the window of entered commands, click the export icon .

Step 9 Give the .csv file a descriptive name and save the file to your local file system. When reading the command output on the .csv file, expand all the cells to see all the results of the command.

Export the CLI Command History

Use the following procedure to export the CLI history of one or multiple devices to a .csv file:

Procedure

Step 1 In the navigation pane, click **Inventory**.

Step 2 Click the **Devices** tab.

Step 3 Click the appropriate device type tab.

Step 4 Select the device or devices so they are highlighted.

Step 5 In the Device Actions pane for the device, click >_**Command Line Interface**.

Step 6 Click the **Clock** icon to expand the history pane if it is not already expanded.

Step 7 To the right of the window of entered commands, click the export icon .

Step 8 Give the .csv file a descriptive name and save the file to your local file system. When reading the command output on the .csv file, expand all the cells to see all the results of the command.

Related Information:

- CDO Command Line Interface, on page 313
- Create a CLI Macro from a New Command
- Delete a CLI Macro

- Edit a CLI Macro
- Run a CLI Macro
- Command Line Interface Documentation
- Bulk Command Line Interface

Export the CLI Macro List

You can only export macros that have been executed ed in the command window. Use the following procedure to export the CLI macros of one or multiple devices to a .csv file:

Procedure

Step 1 In the navigation pane, click **Inventory**.

Step 2 Click the **Devices** tab.

Step 3 Click the appropriate device type tab.

Step 4 Select the device or devices so they are highlighted.

Step 5 In the Device Actions pane for the device, click **>_Command Line Interface**.

Step 6 In the left pane of the CLI window, select the CLI macro favorites star .

Step 7 Click on the macro command you want to export. Fill in any appropriate parameters and click **Send**.

Step 8 To the right of the window of entered commands, click the export icon .

Step 9 Give the .csv file a descriptive name and save the file to your local file system.

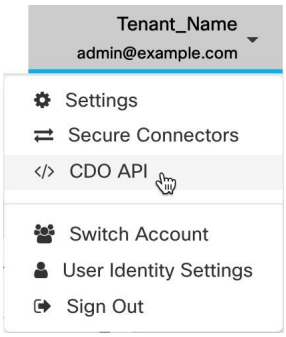
CDO Public API

CDO has published its public API and provided you with documentation, examples, and a playground to try things out. The goal of our public API is to provide you with a simple and effective way to perform a lot of what you would normally be able to do in the CDO UI, but in code.

To use this API, you will need to know GraphQL. Their official guide (https://graphql.org/learn/) provides a thorough, light read.

To find the full schema documentation, go to the GraphQL Playground, and click the docs tab on the right side of the page.

You can launch the CDO Public API by selecting it from the user menu.



Create a REST API Macro

Using the API Tool

CDO provides the API Tool interface to execute the FDM-managed device REpresentational State Transfer (REST) Application Programming (API) requests for performing advanced actions on an FDM-managed device. The REST API uses JavaScript Object Notation (JSON) format to represent objects.

The interface provides system-defined or user-defined API macros. System-defined macros are provided by CDO and can not be edited or deleted. User-defined macros are created by you and can be edited or deleted. You can use all the resource groups supported in the Secure Firewall device manager API Explorer.

Note CDO supports only API endpoints that return JSON.

Assumption

It is assumed that you have a general knowledge of programming and a specific understanding of REST APIs and JSON. If you are new to these technologies, please first read a general guide on REST APIs.

Supported Documents

- You can refer to the Cisco Firepower Threat Defense REST API Guide for detailed information.
- You can also find reference information and examples online at Cisco DevNet Site.

Supported HTTP Methods

You can use the following HTTP methods only.

Important A user with the Read-Only role can perform only the GET operation.

Attribute	Description
GET	To read data from the device.

Attribute	Description
POST	To create new objects for a type of resource. For example, use POST to create a new network object.
PUT	To change the attributes of an existing resource. When using PUT, you must include the entire JSON object. You cannot selectively update individual attributes within an object. For example, use PUT to modify the address contained within an existing network object.
DELETE	To remove a resource that you, or another user, created. For example, use DELETE to remove a network object that you no longer use.

Related Information:

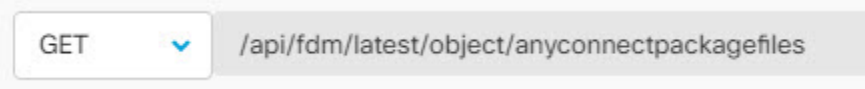
- How to Enter a Secure Firewall Threat Defense REST API Request
- About FTD REST API Macros
  - Create a REST API Macro
  - Run a REST API Macro
  - Edit a REST API Macro
  - Delete a REST API Macro

How to Enter a Secure Firewall Threat Defense REST API Request

You can select an FDM-managed device and specify a single command or execute commands that need additional parameters.

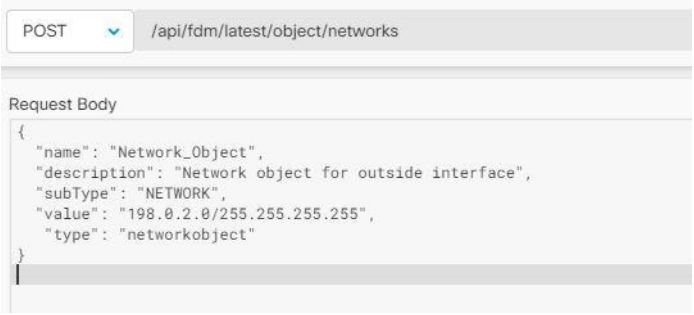
If you want to determine the syntax of a REST API request, log on to the device's API Explorer page, such as https://ftd.example.com/#/api-explorer, and click the required resource groups to see the syntax of the command to be executed. For example, https://10.10.5.84/#/api-explorer.

The following figure shows an example of a single REST API request in Cisco Defense Orchestrator:



The following figure shows an example of a REST API request that needs additional parameters. You need manually specify the data in the **Request Body**. If you want to determine the syntax of a command, log on to the device's API Explorer page.

Note The device must be in the synced state to execute the POST request.



Procedure

Step 1 In the navigation bar, click **Inventory**.

Step 2 Click the **Devices** tab to locate your device.

Step 3 Click the **FTD** tab.

Step 4 Select an FDM-managed device you want to manage using the REST API, and in **Device Actions** on the right, click **API Tool**.

Step 5 Select the request method from the drop-down and type**/api/fdm/latest/**and then the command that you want to execute. If you are executing a POST or PUT command, enter the request body.

Step 6 Click **Send**. The **Response Body** shows the response of the executed command.

Important The POST request usually makes changes to the staged configuration on the device. Click **Commit Changes in FDM** to send the changes to the FDM-managed device.

Related Information:

- Using the API Tool, on page 326
- About FTD REST API Macros
  - Create a REST API Macro
  - Run a REST API Macro
  - Edit a REST API Macro
  - Delete a REST API Macro

About FTD REST API Macros

A REST API macro is a fully-formed REST API command ready to use, or a template of a REST API command you can modify before you run it. All REST API macros can be run on one or more FDM-managed devices simultaneously.

Use REST API macros that resemble templates to run the same commands on multiple devices at the same time. REST API macros promote consistency in your device configurations and management. Use fully-formed REST API macros to get information about your devices. There are different REST API macros that are immediately available for you to use on your FDM-managed devices.

You can create REST API macros for tasks that you perform frequently. See Create a REST API Macro for more information.

REST API macros are system-defined or user-defined. System-defined macros are provided by CDO and can not be edited or deleted. User-defined macros are created by you and can be edited or deleted.

Note You can only create macros for a device once it has been onboarded to CDO.

Related Information:

- Create a REST API Macro
- Run a REST API Macro
- Edit a REST API Macro
- Delete a REST API Macro

Create a REST API Macro

Create a REST API Macro from a New Command

Procedure

Step 1 Before you create a REST API macro, test the command in CDO's REST API Interface to make sure the command syntax is correct and it returns reliable results.

Note You can only create macros for a device once it has been onboarded to CDO.

Step 2 Select an FDM-managed device you want to manage using the REST API, and in **Device Actions** on the right, click **API Tool**.

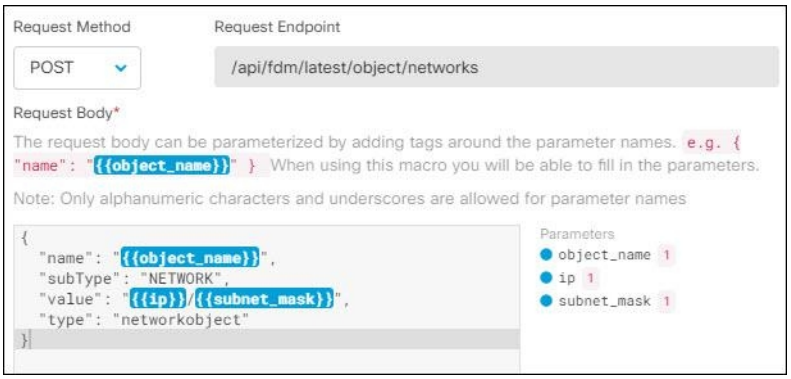
Step 3 Click the REST API macro favorites star to see what macros already exist.

Step 4 Click the plus button.

Step 5 Give the macro a unique name. Provide a description and notes for the REST API macro if you wish.

Step 6 Select a **Request Method** and enter the endpoint URL in the **Request Endpoint** field. See Cisco Firepower Threat Defense REST API Guide for detailed information.

Step 7 Replace the parts of the command that you would want to modify, when you run the command, with a parameter name surrounded by curly braces.



Step 8 Click **OK**. The macro you create is available for use on all the devices of that type, not just the one you initially specified.

To run the command see, Run a REST API Macro.

Create a REST API Macro from History or from an Existing REST API Macro

In this procedure, you are going to create a user-defined REST API macro from a command you have already executed, another user-defined macro, or from a system-defined macro.

Procedure

Step 1 Select an FDM-managed device you want to manage using the REST API, and in **Device Actions** on the right, click **API Tool**.

Note If you want to create a user-defined macro from REST API history, select the device on which you ran the command. REST API macros are shared across devices on the same account but not REST API history.

Step 2 Find the command you want to make an API macro from and select it. Use one of these methods:

- Click the clock to view the commands you have run on that device. Double-click to select the one you want to turn into a macro and the command appears in the command pane.
- Click the API macro favorites star to see what macros already exist. Select the user-defined or system-defined API macro you want to change. The command appears in the command pane.

Step 3 With the command in the command pane, click the API macro gold star . The command is now the basis for a new API macro.

Step 4 Give the macro a unique name. Provide a description and notes for the API macro if you wish.

Step 5 Review the command in the Command field and make the changes you want.

Step 6 Replace the parts of the command that you would want to modify, when you run the command, with a parameter name surrounded by curly braces.

Step 7 Click **Create**. The macro you create is available for use on all the devices of that type, not just the one you initially specified.

To run the command see, Run a REST API Macro.

Related Information:

About FTD REST API Macros

Run a REST API Macro

Procedure

Step 1 In the navigation bar, click **Inventory**.

Step 2 Click the **Devices** tab to locate your device.

Step 3 Click the **FTD** tab.

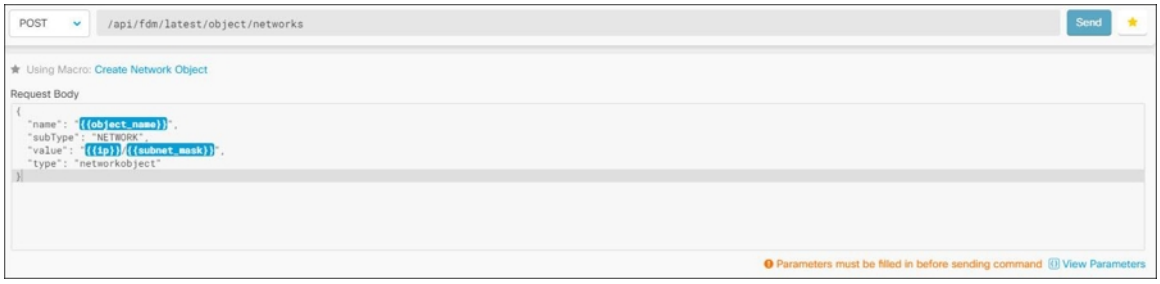
Step 4 Click **API Tool** in the **Device Actions** pane on the right.

Step 5 In the command panel, click the star to view the REST API macros.

Step 6 Select a REST API macro from the command panel.

Step 7 Run the macro one of two ways:

- If the macro has no parameters to define, click **Send**. The response to the command appears in the response pane. You're done.
- If the macro contains parameters, such as the Create Network Object macro below, click **View Parameters.**



Step 8 In the **Parameters** pane, fill in the values for the parameters in the Parameters fields.

Step 9 Click **Send**.

Note The FDM-managed device's active configuration is updated.

Related Information:

About FTD REST API Macros

Edit a REST API Macro

You can edit user-defined REST API macros but not system-defined macros. Editing a REST API macro changes it for all your FDM-managed devices. Macros are not specific to a particular device.

Procedure

Step 1 In the navigation bar, click **Inventory**.

Step 2 Click the **Devices** tab to locate your device.

Step 3 Click the **FTD** tab.

Step 4 Select an FDM-managed device you want to manage using the REST API, and in **Device Actions** on the right, click **API Tool**.

Step 5 Select the user-defined macro you want to edit.

Step 6 Click the edit icon in the macro label.

Step 7 Edit the REST API macro in the Edit Macro dialog box.

Step 8 Click **Save**.

See Run a REST API Macro for instructions on how to run the REST API macro.

Related Information:

About FTD REST API Macros

Delete a REST API Macro

You can delete user-defined REST API macros but not system-defined macros. Deleting a REST API macro deletes it for all your devices. Macros are not specific to a particular device.

Procedure

Step 1 In the navigation bar, click **Inventory**.

Step 2 Click the **Devices** tab to locate your device.

Step 3 Click the **FTD** tab.

Step 4 Select a device and in **Device Actions** on the right, click **API Tool**.

Step 5 Select the user-defined REST API macro you want to delete.

Step 6 Click the trash can icon in the REST API macro label.

Step 7 Confirm you want to remove the REST API macro.

Related Infomration:

About FTD REST API Macros

About Device Configuration Changes

In order to manage a device, CDO must have its own copy of the device's configuration stored in its local database. When CDO "reads" a configuration from a device it manages, it takes a copy of the device's configuration and saves it. The first time CDO reads and saves a copy of a device's configuration is when the device is onboarded. These choices describe reading a configuration for different purposes:

- **Discard Changes**: This action is available when a device's configuration status is "Not Synced." In the Not Synced state, there are changes to the device's configuration pending on CDO. This option allows you to undo all pending changes. The pending changes are deleted and CDO overwrites its copy of the configuration with copy of the configuration stored on the device.
- **Check for Changes**: This action is available if the device's configuration status is Synced. Clicking Checking for Changes directs CDO to compare its copy of the device's configuration with the copy of the configuration stored on the device. If there is a difference, CDO immediately overwrites its copy of the device's configuration with the copy stored on the device.
- **Review Conflict** and **Accept Without Review**: If you have enabled Conflict Detection on a device, CDO checks for configuration changes made on the device every 10 minutes. If the copy of the configuration stored on the device has changed, CDO notifies you by displaying the "Conflict Detected" configuration status.
  - **Review Conflict**: Click Review Conflict allows you to review changes made directly on a device and accept or reject them.
  - **Accept Without Review**: This action overwrites CDO's copy of a device's configuration with the latest copy of the configuration stored on the device. CDO does not prompt you to confirm the differences in the two copies of the configuration before taking the overwriting action.

Read All: This is a bulk operation. You can select more than one device, in any state, and click **Read All** to overwrite all the devices' configurations stored on CDO with the configurations stored on the devices.

- **Deploy Changes**: As you make changes to a device's configuration, CDO saves the changes you make to its own copy of the configuration. Those changes are "pending" on CDO until they are deployed to the device. When there are changes to a device's configuration that have not been deployed to the device, the device is in the Not Synced configuration state.

  Pending configuration changes have no effect on the network traffic running through the device. Only after CDO deploys the changes to the device do they have an effect. When CDO deploys changes to the device's configuration, it only overwrites those elements of the configuration that were changed. It does not overwrite the entire configuration file stored on the device. Deployments can be initiated for a single device or on more than one device simultaneously.
- **Discard All** is an option that is only available after you click **Preview and Deploy...**. After clicking Preview and Deploy, CDO shows you a preview of the pending changes in CDO. Clicking **Discard All** deletes all pending changes from CDO and does not deploy anything to the selected device(s). Unlike "Discard Changes" above, deleting the pending changes is the end of the operation.

Note You can schedule deployments or recurring deployments. See Schedule an Automatic Deployment, on page 341 for more information.

Read All Device Configurations

If a configuration change is made to a device outside of Cisco Defense Orchestrator (CDO), the device's configuration stored on CDO and the device's local copy of its configuration are no longer the same. You many want to overwrite CDO's copy of the device's configuration with the configuration stored on the device to make the configurations the same again. You can perform this task on many devices simultaneously using the **Read All** link.

See About Device Configuration Changes for more information about how CDO manages the two copies of the device's configuration.

Here are three configuration statuses where clicking **Read All** will overwrite CDO's copy of the device's configuration with the device's copy of the configuration.

- **Conflict Detected**-If conflict detection is enabled, CDO polls the devices it manages every 10 minutes for changes made to their configurations. If CDO finds that the configuration on the device has changed, CDO displays a "Conflict detected" configuration status for the device.
- **Synced**-If the device is in a synced state, and you click **Read All**, CDO immediately checks the devices to determine if there have been any changes made to its configurations directly. After clicking **Read All**, CDO confirms your intent to overwrite its copy of the device's configuration and then CDO performs the overwrite.
- **Not Synced**-If the device is in the Not Synced state, and you click **Read All**, CDO warns you that there are pending changes made to to the device's configuration using CDO and that proceeding with the Read All operation will delete those changes and then overwrite CDO's copy of the configuration with the configuration on the device. This Read All functions like Discard Configuration Changes.

Procedure

Step 1 In the navigation bar, click **Inventory**.

Step 2 Click the **Devices** tab.

Step 3 Click the appropriate device type tab.

Step 4 (Optional) Create a change request label to identify the results of this bulk action easily in the Change Log.

Step 5 Select the devices whose configurations you want to save CDO. Notice that CDO only provides command buttons for actions that can be applied to all the selected devices.

Step 6 Click **Read All**.

Step 7 CDO warns you if there are configuration changes staged on CDO, for any of the devices you selected, and asks if you want to continue with the bulk reading configurations action. Click **Read All** to continue.

Step 8 Look at the notifications tab for the progress of the Read All configurations operation. If you want more information about how individual actions in the bulk operation succeeded or failed, click the blue Review link and you will be directed to the Jobs page.

Step 9 If you created and activated a change request label, remember to clear it so that you don't inadvertently associate other configuration changes with this event.

Related Information

- About Device Configuration Changes
- Discard Configuration Changes
- Check for Configuration Changes

Read Configuration Changes from FDM-Managed Device to CDO

Why Does Cisco Defense Orchestrator Read FDM-managed device Configurations?

In order to manage an FDM-managed device, CDO must have its own stored copy of the FDM-managed device's configuration. When CDO reads a configuration from an FDM-managed device, it takes a copy of the FDM-managed device's deployed configuration and saves it to its own database. The first time CDO reads and saves a copy of the device's configuration file is when the device is onboarded. See About Device Configuration Changes for more information.

Pending and Deployed Changes

Configuration changes made to the FDM-managed device directly through the Firepower Device Manager (FDM) or its CLI are referred to as staged changes on the FDM-managed device until they are deployed. A staged, or pending, change can be edited or deleted without having any affect on traffic running through the FDM-managed device. Once the pending changes are deployed, however, they are enforced by the FDM-managed device and affect traffic running through the device.

Conflict Detected

If you enable Conflict Detection on the device, CDO checks for configuration changes every 10 minutes. If the copy of the configuration stored on the device has changed, CDO notifies you by displaying the "Conflict Detected" configuration status. If you do **not** have Conflict Detection enabled, or a change has been made to the device's configuration within the 10 minute interval between automatic polling, clicking **Check for Changes** prompts CDO to immediately compare the copy of the configuration on the device with the copy of the configuration stored on CDO. You can choose to **Review Conflict** to examine the differences between the device configuration and the configuration saved to CDO, then select **Discard Changes** to remove the staged changes and revert to the saved configuration or confirm the changes. You can also choose to **Accept without Review**; this option takes the configuration and overwrites what is currently saved to CDO.

Discard Changes Procedure

To discard configuration changes from the FDM-managed device, follow this procedure:

Procedure

Step 1 In the navigation bar, click **Inventory**.

Step 2 Click the **Devices** tab.

Step 3 Click the appopriate device type tab.

Step 4 Select the device whose configuration is set to Conflict Detected and gives you the link to Revert Pending Changes. The message explains that you can click the link to revert pending changes or you can log on to the device using the local manager FDM and deploy the changes first. You can use filters to find the device in a conflict state.

Caution Clicking the Revert Pending Changes link deletes pending changes on FDM-managed device immediately. You are not given an opportunity to review the changes first.

Step 5 Review the changes on FDM before clicking Revert Pending Changes:

a. Open a browser window and enter https://<*IP_address_of_the_FTD*>.

b. Look for the deployment icon in FDM. It will have an orange circle indicating that there are changes ready to deploy  .

c. Click the icon and review the pending changes:

- If the changes can be deleted, return to CDO and click "Revert Pending Changes." At this point, the configuration on the FDM-managed device and the copy of the configuration on CDO should be the same. You are done.
- If you want to deploy the changes to the device, click **Deploy Now**. Now the deployed configuration on the FDM-managed device and the configuration on stored on CDO are different. You can then return to CDO and Check for Configuration Changes. CDO identifies identifies that there has been a change on the FDM-managed device, and gives you an opportunity to review the conflict. See Conflict Detection to resolve that state.

If Reverting Pending Changes Fails

Changes to the system databases and security feeds can't be reverted by CDO. CDO recognizes that there are pending changes, attempts to revert them and then fails. To determine if the revert failure is due to pending database updates or security feed updates, log into the device's FDM console. It will have an orange circle indicating that there are changes ready to deploy  . Click the deploy button to review the pending changes and deploy them or discard them as is appropriate.

Review Conflict Procedure

To review configuration changes from the FDM-managed device, follow this procedure:

Procedure

Step 1 In the navigation bar, click **Inventory**.

Step 2 Click the **Devices** tab.

Step 3 Click the appropriate device type tab.

Step 4 Select the device whose configuration is marked Conflict Detected and gives you a link to **Review Conflict** in the Conflict Detected pane on the right.

Step 5 Click **Review Conflict.**

Step 6 Compare the two configurations presented to you.

Step 7 Take one of these actions:

- Click **Accept** to overwrite the last known configuration on CDO with the one found on the device. **Note**: The entire configuration stored on CDO will be completely overwritten by the configuration found on the device.
- Click **Reject** to reject the changes made on the device and replace them with the last known configuration on CDO.
- Click **Cancel** to stop the action.

Note You can prompt CDO to immediately check a device for an out-of-band change by clicking Check for Configuration Changes while the device is in the Synced state.

Accept Without Review Procedure

To accept configuration changes from the FDM-managed device without reviewing, follow this procedure:

Procedure

Step 1 In the navigation bar, click **Inventory**.

Step 2 Click the **Devices** tab.

Step 3 Click the appopriate device type tab.

Step 4 Select the device whose configuration is marked Conflict Detected and gives you a link to **Accept Without Review** in the Conflict Detected pane on the right.

Step 5 Click **Accept Without Review**. CDO accepts and overwrites the current configuration.

Related Information:

- About Device Configuration Changes
- Conflict Detection
- Discarding Changes

Preview and Deploy Configuration Changes for All Devices

CDO informs you when you have made a configuration change to a device on your tenant, but you have not deployed that change, by displaying an orange dot on the Deploy icon

. The devices affected by these changes show the status "Not Synced" in the Devices and **Services** page. By clicking **Deploy**, you can review which devices have pending changes and deploy the changes to those devices.

Note For every new FDM or FTD network object or group that you create and make changes to, CDO creates an entry in this page for all on-prem management centers that are managed by CDO.

This deployment method is available for all supported devices.

You can use this deployment method for single configuration changes or wait and deploy multiple changes at once.

Procedure

Step 1 In the top right corner of the screen, click the **Deploy** icon  **.**

Step 2 Select the devices with changes you want to deploy. If a device has a yellow caution triangle, you can not deploy changes to that device. Hover your mouse over the yellow caution triangle to find out why you can't deploy changes to that device.

Step 3 (Optional) If you want to see more information about a pending change, click the **View Detailed Changelog** link to open the change log associated with that change. Click the **Deploy** icon to return to the **Devices with Pending Changes** page.

Step 4 (Optional) Create a change request to track your changes without leaving the **Devices with Pending Changes** page.

Step 5 Click **Deploy Now** to deploy the changes immediately to the devices you selected. You'll see the progress in the Active jobs indicator in the Jobs tray.

Step 6 (Optional) After the deployment has finished, click **Jobs** in the CDO navigation bar. You will see a recent "Deploy Changes" job showing the results of the deployment.

Step 7 If you created a change request label, and you have no more configuration changes to associate with it, clear it.

What to do next

- About Scheduled Automatic Deployments
- Deploy Configuration Changes from CDO to FDM-Managed Device, on page 339
- Change Log Entries after Deploying to FDM-Managed Device

Deploy Configuration Changes from CDO to FDM-Managed Device

Why Does CDO Deploy Changes to an FDM-Managed Device?

As you manage and make changes to a device's configuration with CDO, CDO saves the changes you make to its own copy of the configuration file. Those changes are considered staged on CDO until they are deployed to the device. Staged configuration changes have no effect on the network traffic running through the device. Only after CDO deploys the changes to the device do they have an affect on the traffic running through the device. When CDO deploys changes to the device's configuration, it only overwrites those elements of the configuration that were changed. It does not not overwrite the entire configuration file stored on the device.

Like CDO, FDM-managed device has the concept of pending changes and deployed changes. Pending changes on FDM-managed device are the equivalent of staged changes on CDO. A pending change can be edited or deleted without having any affect on traffic running through the FDM-managed device. Once the pending changes are deployed, however, they are enforced by the FDM-managed device and affect traffic running through the device.

Because of FDM-managed devices two step process for editing configuration files, CDO deploys changes to an FDM-managed device slightly differently than it does to other devices it manages. CDO first deploys the changes to FDM-managed device and the changes are in the pending state. Then, CDO deploys the changes on the devices and they become live. Now that the changes have been deployed, they are enforced and affect traffic running through the FDM-managed device. This applies to both standalone and high availability (HA) devices.

Deployments can be initiated for a single device or on more than one device simultaneously. You can schedule individual deployments or recurring deployments for a single device.

Two things will prevent CDO from deploying changes to an FDM-managed device:

- If there are staged changes on the FDM-managed device. See Conflict Detection for more information on how to resolve this state.
- CDO does not deploy changes if there are changes in the process of being deployed to the FDM-managed device.

Scheduling Automatic Deployments

You can also configure your tenant to schedule deployments to a single device with pending changesAbout Scheduled Automatic Deployments.

Deploy Changes to a device

Procedure

Step 1 After you make a configuration change for a device using CDO and save it, that change is saved in CDO instance of the device's configuration.

Step 2 In the navigation bar, click **Inventory**.

Step 3 Click the **Devices** tab.

Step 4 Click the appropriate device type tab. You should see that the configuration status of the device you made changes to is now "Not synced."

Step 5 Deploy the changes using one of these methods:

- Select the device and in the Not Synced pane on the right, click **Preview and Deploy.** On the Pending Changes screen, review the changes. If you are satisfied with the pending version, click **Deploy Now**. After the changes are deployed successfully, you can view the change log to confirm what just happened.
- Click the **Deploy** icon at the top-right of the screen. See Preview and Deploy Configuration Changes for All Devices, on page 337 for more information.

Cancelling Changes

If, when deploying a change from CDO to a device, you click **Cancel**, the changes you made are not deployed to the device. The process is canceled. The changes you made are still pending on CDO and can be edited further before you finally deploy them to FDM-managed device.

Discarding Changes

If, when previewing changes, you click **Discard all**, the changes you made, and any other changes any other user made but did not deploy to the device, are deleted. CDO reverts its pending configuration to the last read or deployed configuration before any changes were made.

Bulk Deploy Device Configurations

If you have made changes to multiple devices, for instance by editing a shared object, you can apply those change to all of the affected devices at once:

Procedure

Step 1 In the navigation pane, click **Inventory**.

Step 2 Click the **Devices** tab.

Step 3 Click the appropriate device type tab.

Step 4 Select all of the devices for which you have made configuration changes on CDO. These devices should show "Not Synced" status.

Step 5 Deploy the changes using one of these methods:

- Click the button at the top-right of the screen to view the **Devices with Pending Changes** window. This gives you a chance to review the pending changes on the devices you selected before you deploy them. Click **Deploy Now** to deploy the changes.

Note If you see a yellow warning triangle next to a device on the **Devices with Pending Changes** screen, you cannot deploy a change to that device. Hover your mouse over the warning triangle for information about why changes cannot be deployed to that device.

- Click **Deploy All** on the details pane. Review any warnings and click **OK**. The bulk deployment starts immediately without a review of the changes.

Step 6 (Optional) Click the Jobs icon  in the navigation bar to view the results of the bulk deploy.

Related Information:

- Schedule an Automatic Deployment, on page 341

About Scheduled Automatic Deployments

Using CDO, you can make configuration changes to one or more of the devices it manages and then schedule the changes to be deployed to those devices at a time that is convenient for you.

You can only schedule deployments if you Enable the Option to Schedule Automatic Deployments in the **Tenant Settings** tab of the Settings page. Once this option is enabled, you can create, edit, or delete scheduled deployments. A scheduled deployment deploys all the staged changes saved on CDO at the date and time set. You can also view and delete scheduled deployments from the Jobs page.

If there were changes made directly to the device that have not been About Device Configuration Changes to CDO, the scheduled deployment will be skipped until that conflict is resolved. The Jobs page will list any instance where a scheduled deployment fails. If **Enable the Option to Schedule Automatic Deployments** is turned off, all scheduled deployments are deleted.

Caution If you schedule a new deployment for multiple devices, and some of those devices already have deployments scheduled, the new scheduled deployment overwrites the existing scheduled deployments.

Note When you create a scheduled deployment, the schedule is created in your local time, not in the time zone of the device. Scheduled deployments *do not* automatically adjust for daylight savings time.

Schedule an Automatic Deployment

The deployment schedule can be a single event or a recurring event. You may find recurring automatic deployments a convenient way to line up recurring deployments with your maintenance window. Follow this procedure to schedule a one-time or a recurring deployment for a single device:

Note If you schedule a deployment for a device that has an existing deployment scheduled, the new scheduled deployment overwrites the existing deployment.

Procedure

Step 1 In the navigation bar, click **Inventory**.

Step 2 Click the **Devices** tab.

Step 3 Click the appropriate device type tab.

Step 4 Select one ore more devices.

Step 5 In the Device Details pane, locate the Scheduled Deployments tab and click **Schedule**.

Step 6 Select when the deployment should occur.

- For a one-time deployment, click the **Once on** option to select a date and time from the calendar.
- For a recurring deployment, click the **Every** option. You can choose either a daily or once a week deployment. Select the **Day** and **Time** the deployment should occur.

Step 7 Click **Save**.

Edit a Scheduled Deployment

Follow this procedure to edit a scheduled deployment:

Procedure

Step 1 In the navigation bar, click **Inventory**.

Step 2 Click the **Devices** tab.

Step 3 Click the appropriate device type tab.

Step 4 Select one or more devices.

Step 5 In the **Device Details** pane, locate the Scheduled Deployments tab and click **Edit** .

Step 6 Edit the recurrence, date, or time of a scheduled deployment.

Step 7 Click **Save**.

Delete a Scheduled Deployment

Follow this procedure to delete a scheduled deployment:

Note If you schedule a deployment for multiple devices, and then change or delete the schedule for some of the devices, the original scheduled deployment for the remaining devices will be preserved.

Procedure

Step 1 In the navigation bar, click**Inventory**.
Step 2 Click the **Devices** tab.
Step 3 Click the appropriate device type tab.
Step 4 Select one or more devices.
Step 5 In the **Device Details** pane, locate the Scheduled Deployments tab and click **Delete** .

What to do next

- About Device Configuration Changes
- Read All Device Configurations, on page 334
- Deploy Configuration Changes from CDO to FDM-Managed Device, on page 339
- Preview and Deploy Configuration Changes for All Devices, on page 337

Check for Configuration Changes

Check for Changes to determine if the device's configuration has been changed directly on the device and it is no longer the same as the copy of the configuration stored on CDO. You will see the this option when the device is in the "Synced" state.

To check changes:

Procedure

Step 1 In the navigation bar, click **Inventory**.
Step 2 Click the **Devices** tab.
Step 3 Click the appropriate device type tab.
Step 4 Select the device, whose configuration you suspect may have been changed directly on the device.
Step 5 Click **Check for Changes** in the Synced pane on the right.
Step 6 The behavior that follows is slightly different depending on the device:

- For FTD device if there has been a change to the device's configuration, you will receive the message:

  ```
  Reading the policy from the device. If there are active deployments on the device,
  reading will start after they are finished.
  ```

  - Click **OK** to continue. The configuration on the device will overwrite the stored configuration on CDO.
  - Click **Cancel** to cancel the action.

- For device:

a. Compare the two configurations presented to you. Click **Continue**. The configuration labeled **Last Known Device Configuration** is the configuration stored on CDO. The configuration labeled **Found on Device** is the configuration saved on the ASA.

b. Select either:

   1. **Reject** the out-of-band changes to keep the "Last Known Device Configuration."
   2. **Accept** the out-of-band changes to overwrite the device's configuration stored in CDO with the configuration found on the device.

c. Click **Continue**.

Discard Configuration Changes

Click **Discard Changes** when you want to "undo" all the *undeployed* configuration changes you made to a device's configuration using CDO. When you click **Discard Changes**, CDO *completely overwrites* its local copy of a device's configuration with the configuration stored on the device.

When you click **Discard Changes**, your device's configuration status is in a **Not Synced** state. After you discard your changes, the copy of the configuration on CDO will be the same as the copy of the configuration on the device and the configuration status in CDO will return to Synced.

To discard, or "undo," all of your undeployed configuration changes for a device:

Procedure

Step 1 In the navigation bar, click **Inventory**.

Step 2 Click the **Devices** tab.

Step 3 Click the appropriate device type tab.

Step 4 Select the device you have been making configuration changes to.

Step 5 Click **Discard Changes** in the **Not Synced** pane on the right.

- For FDM-managed devices-CDO warns you that "Pending changes on CDO will be discarded and the CDO configuration for this device will be replaced with the configuration currently running on the device." Click **Continue** to discard your changes.
- For Meraki devices-CDO deletes the change immediately.
- For AWS devices-CDO displays what you are about to delete. Click **Accept** or **Cancel**.

Out-of-Band Changes on Devices

Out-of-band changes refer to changes made directly on the device without using CDO. These changes may be made using the device's command-line interface over an SSH connection or by using a local manager like the Adaptive Security Device Manager (ASDM) for the ASA, the FDM for the FDM-managed device, or for an On-Prem Firewall Management Center on the On-Prem Firewall Management Center user interface. An out-of-band change causes a conflict between the device's configuration stored on CDO and the configuration stored on the device itself.

Detecting Out-of-Band Changes on Devices

If Conflict Detection is enabled for an ASA, or an FDM-managed device, a Cisco IOS device, or an On-Prem Firewall Management Center, CDO checks the device every 10 minutes searching for any new changes made directly to the device's configuration outside of CDO.

If CDO finds that there are changes to the device's configuration that are not stored on CDO, it changes the **Configuration Status** of that device to the "Conflict Detected" state.

When Defense Orchestrator detects a conflict, one of two conditions is likely:

- There have been configuration changes made to the device directly that have not been saved to CDO's database.
- In the case of an FDM-managed device, there may be "pending" configuration changes on the FDM-managed device that have not been deployed.
- In the case of an On-Prem Firewall Management Center, there may be changes made, for instance, to objects outside CDO, which are pending to be synchronized with CDO or changes made in CDO which are pending to be deployed to the On-Prem Firewall Management Center.

Synchronizing Configurations Between Defense Orchestrator and Device

About Configuration Conflicts

On the **Inventory** page, you may see devices or services have the status "Synced," "Not Synced," or "Conflict Detected." To know the status of an On-Prem Firewall Management Center that you manage using CDO, navigate **Tools & Services** > **Firewall Management Center**.

- When a device is **Synced**, the configuration on Cisco Defense Orchestrator (CDO) and the configuration stored locally on the device are the same.
- When a device is **Not Synced**, the configuration stored in CDO was changed and it is now different that the configuration stored locally on the device. Deploying your changes from CDO to the device changes the configuration on the device to match CDO's version.
- Changes made to devices outside of CDO are called **out-of-band changes**. When out-of-band changes are made, you'll see the device state change to "Conflict Detected," if conflict detection is enabled for the device. Accepting the out-of-band changes, changes the configuration on CDO to match the configuration on the device.

Conflict Detection

When conflict detection is enabled, Cisco Defense Orchestrator (CDO) polls the device for the default interval to to determine if a change has been made to the device's configuration outside of CDO. If CDO detects that a change was made, it changes the configuration status for the device to **Conflict Detected**. Changes made to a device outside of CDO are called "out-of-band" changes.

In the case of an On-Prem Firewall Management Center that is managed by CDO, if there are changes that are staged and the device is in **Not Synced** state, CDO stops polling the device to check for changes. When there are changes made outside CDO which are pending to be synchronized with CDO and changes made in CDO which are pending to be deployed to the on-prem management center, CDO declares the on-prem management center to be in the **Conflict Detected** state.

Once this option is enabled, you can configure how often conflicts or OOB changes are detected per device. See Schedule Polling for Device Changes, on page 349 for more information.

Enable Conflict Detection

Enabling conflict detection alerts you to instances where changes have been made to a device outside of Defense Orchestrator.

Procedure

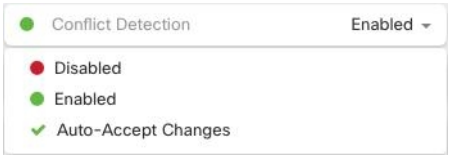
Step 1 In the navigation bar, click **Inventory**.

Step 2 Click the **Devices** tab.

Step 3 Select the appropriate device type tab.

Step 4 Select the device or devices for which you want to enable conflict detection.

Step 5 In the **Conflict Detection** box at the right of the device table, select **Enabled** from the list.



Automatically Accept Out-of-Band Changes from your Device

You can configure Cisco Defense Orchestrator (CDO) to automatically accept any change made directly to a managed device by enabling auto-accept changes. Changes made directly to a device without using CDO are referred to as out-of-band changes. An out-of-band change creates a *conflict* between the device's configuration stored on CDO and the configuration stored on the device itself.

The auto-accept changes feature is an enhancement to conflict detection. If you have auto-accept changes enabled on your device, CDO checks for changes every 10 minutes to determine if there have been any

out-of-band changes made to the device's configuration. If there have been configuration changes, CDO automatically updates its local version of the device's configuration without prompting you.

CDO will ***not*** automatically accept a configuration change if there are configuration changes made on CDO that have not yet been deployed to the device. Follow the prompts on the screen to determine your next action.

To use auto-accept changes, you first enable the tenant to display the auto-accept option in the Conflict Detection menu on the **Inventory** page; then, you enable auto-accept changes for individual devices.

If you want CDO to detect out-of-band changes but give you the option to accept or reject them manually, enable Conflict Detection, on page 346 instead.

Configure Auto-Accept Changes

Procedure

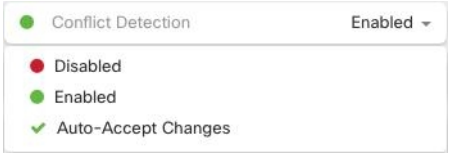
Step 1 Log in to CDO using an account with Admin or Super Admin privileges.

Step 2 From the CDO menu, navigate to **Settings** > **General Settings**

Step 3 In the **Tenant Settings** area, click the toggle to "**Enable the option to auto-accept device changes**." This enables the Auto-Accept Changes menu option to appear in the Conflict Detection menu on the **Inventory** page.

Step 4 Open the **Inventory** page and select the device for which you want to automatically accept out-of-band changes.

Step 5 In the **Conflict Detection** menu, select **Auto-Accept Changes** in the drop-down menu.



Disabling Auto-Accept Changes for All Devices on the Tenant

Procedure

Step 1 Log-in to CDO using an account with Admin or Super Admin privileges.

Step 2 From the CDO menu, navigate **Settings** > **General Settings**

Step 3 In the **Tenant Settings** area, disable the "**Enable the option to auto-accept device changes**" by sliding the toggle to the left so it shows a grey X. This disables Auto-Accept Changes option in the Conflict Detection menu and disables the feature for every device on your tenant.

Note Disabling "Auto-Accept" will require you to review each device conflict before you can accept it into CDO. This includes devices previously configured to auto-accept changes.

Resolve Configuration Conflicts

This section provides information about resolving configuration conflicts that occur on the device.

Resolve the Not Synced Status

Use the following procedure to resolve a device with a "Not Synced" Configuration Status:

Procedure

Step 1 In the navigation bar, click **Inventory**.

Note For an On-Prem Firewall Management Center, navigate **Tools & Services** > **Firewall Management Center** and select the FMC that is in **Not Synced** state and continue from Step 5.

Step 2 Click the **Devices** tab to locate the device or the **Templates** tab to locate the model device.

Step 3 Click the appropriate device type tab.

Step 4 Select the device reported as Not Synced.

Step 5 In the **Not synced** panel to the right, select either of the following:

- **Preview and Deploy...** -If you want to push the configuration change from CDO to the device, Preview and Deploy Configuration Changes for All Devices the changes you made now, or wait and deploy multiple changes at once.
- **Discard Changes** -If you do **not** want to push the configuration change from CDO to the device, or you want to "undo" the configuration changes you started making on CDO. This option overwrites the configuration stored in CDO with the running configuration stored on the device.

Resolve the Conflict Detected Status

CDO allows you to enable or disable conflict detection on each live device. If Conflict Detection, on page 346 is enabled and there was a change made to the device's configuration without using CDO, the device's configuration status will show **Conflict Detected**.

To resolve a "Conflict Detected" status, follow this procedure:

Procedure

Step 1 In the navigation bar, click **Inventory**.

Note For an On-Prem Firewall Management Center, navigate **Tools & Services** > **Firewall Management Center** and select the FMC that is in **Conflict Detected** state and continue from Step 4.

Step 2 Click the **Devices** tab to locate your device.

Step 3 Click the appropriate device type tab.

Step 4 Select the device reporting the conflict and click **Review Conflict** in the details pane on the right.

Step 5 In the **Device Sync** page, compare the two configurations by reviewing the highlighted differences.

- The panel labeled "Last Known Device Configuration" is the device configuration stored on CDO.
- The panel labeled "Found on Device" is the configuration stored in the running configuration on the ASA.

Step 6 Resolve the conflict by selecting one of the following:

- **Accept Device changes**: This will overwrite the configuration **and any pending changes stored on CDO** with the device's running configuration.

  Note As CDO does not support deploying changes to the Cisco IOS devices outside of the command line interface, your only choice for a Cisco IOS device will be to select **Accept Without Review** when resolving the conflict.

- **Reject Device Changes**: This will overwrite the configuration stored on the device with the configuration stored on CDO.

Note All configuration changes, rejected or accepted, are recorded in the change log.

Schedule Polling for Device Changes

If you have Conflict Detection, on page 346 enabled, or if you **Enable the option to auto-accept device changes** from the Settings page, CDO polls the device for the default interval to determine if a change has been made to the device's configuration outside of CDO. You can customize how often CDO polls for changes per device. These changes can be applied to more than one device.

If there is no selection configured for a device, the interval is automatically configured for "tenant default".

Note Customizing the interval per device from the **Inventory** page overrides the polling interval selected as the Default Conflict Detection Interval from the **General Settings** page.

After you enable **Conflict Detection** from the **Inventory** page or **Enable the option to auto-accept device changes** from the Settings page, use the following procedure to schedule how often you want CDO to poll your devices:

Procedure

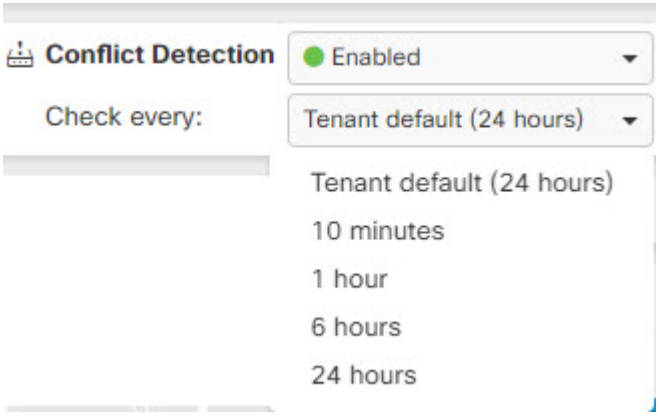
Step 1 In the navigation bar, click **Inventory**.

Step 2 Click the **Devices** tab to locate your device.

Step 3 Click the appropriate device type tab.

Step 4 Select the device or devices for which you want to enable conflict detection.

Step 5 In the same area as **Conflict Detection**, click the drop-down menu for **Check every** and select the desired polling interval:



Schedule a Security Database Update

This section provides information about scheduling a security database update on the device.

Create a Scheduled Security Database Update

Use the following procedure to create a scheduled task to check and update the security databases for an FDM-managed device:

Procedure

Step 1 In the navigation bar, click **Inventory**.

Step 2 Click the **Devices** tab to locate your device.

Step 3 Click the **FTD** tab.

Step 4 Select a device.

Step 5 In the **Actions** pane, locate the **Security Database Updates** section and click the**add +** button.

Note If there is an existing scheduled task for the selected device, click the edit icon to create a new task. Creating a new task will overwrite the existing one.

Step 6 Configure the scheduled task with the following:

- **Frequency** . Choose for the update to occur daily, weekly, or monthly.
- **Time**. Choose the time of day. Note that the time displayed is UTC.
- **Select Days.** Choose which day(s) of the week you want the update to occur.

Step 7 Click **Save**.

The device's Configuration Status will change to "Updating Databases".

Edit a Scheduled Security Database Update

Use the following procedure to edit an existing scheduled task to check and update the security databases for an FDM-managed device.

Procedure

Step 1 In the navigation bar, click **Inventory**.

Step 2 Click the **Devices** tab to locate your device.

Step 3 Click the **FTD** tab.

Step 4 Select a device.

Step 5 In the **Actions** pane, locate the **Security Database Updates** section and click the edit icon .

Step 6 Edit the scheduled task with the following:

- **Frequency** . Choose for the update to occur daily, weekly, or monthly.
- **Time**. Choose the time of day. Note that the time displayed is UTC.
- **Select Days.** Choose which day(s) of the week you want the update to occur.

Step 7 Click **Save**.

Step 8 The device's Configuration Status will change to "Updating Databases".

Update FDM-Managed Device Security Databases

By updating the security databases on an FDM-managed device, you are updating the following: SRUs (intrusion rules), security intelligence (SI), vulnerability databases (VDB), and geolocation databases. If you opt into updating the security databases through the Cisco Defense Orchestrator UI, note that **all** of the mentioned databases are updated; you cannot select which databases you want to update.

Please note that security database updates cannot be reverted.

Note When you update the security databases, some packets may be dropped or pass uninspected. We recommend you schedule your security database updates during a maintenance window.

Update FDM-Managed Device Security Database While Onboarding

When you onboard an FDM-managed device to CDO, part of the onboarding process allows you to **Enable scheduled recurring updates for databases**. This option is checked by default. When enabled, CDO immediately checks for and applies any security updates as well as automatically schedules the device to check for additional updates. You are able to modify the date and time of the scheduled task after the device is onboarded.

We recommend enabling the automatic scheduler during the onboarding process to regularly check for and apply security database updates. This way your device will always be up to date. To update the security databases while onboarding your FDM-managed device, see Onboard an FDM-Managed Device with a Registration Key.

Note If you onboard your device with the registration key method, the device must **not** be registered with a smart license. We recommend registering an license. As an alternative method, you can onboard your device using the device's username, password, and IP address.

Update FDM-Managed Device Security Database After Onboarding

After an FDM-managed device is onboarded to CDO, you can configure a device to check for security database updates by scheduling an update. You can modify this scheduled task at any time by selecting the device the update is scheduled for. See Schedule a Security Database Update for more information.

Workflows

Device licenses

Cisco Defense Orchestrator cannot update the security databases if there is no license. We recommend that your FDM-managed device has at least an license.

If you are onboarding a device that has no license, this does not inhibit CDO from onboarding the device. Instead, the device will experience a **Connectivity** status of "insufficient licenses". To resolve this issue, you must apply the correct licenses through the FDM-managed device UI.

Note If you onboard an FDM-managed device and opt in to schedule future security database updates and the device does **not** have a registered license, CDO still creates the scheduled task but does not trigger the task until the appropriate licenses have been applied and the device is successfully synchronized.

Security database updates are pending in FDM

If you update the security databases through the FDM-managed device UI, and you have **conflict detection** enabled on your device, CDO detects the pending update as a conflict.

Note If you onboard your FDM-managed device and opt to schedule the updates, CDO automatically updates the security databases as well as any other pending changes to the stored configuration during the next deploy. **does not have to be a configuration deploy**

Device has OOB changes, or staged changes, during a security database update

If you schedule a security database update for an FDM-managed device that has out of band (OOB) changes, or staged changes that have not been deployed, CDO only checks and updates the security databases. CDO does **not** deploy OOB or staged changes.

Device already has a scheduled task to update the security databases

Each device can only have one scheduled task. If the device already has a scheduled task to update the security databases, creating a new one overwrites it. This applies to tasks that are created in either CDO or an FDM-managed device.

No security database updates available

If there are no updates available, CDO does not deploy anything to the device.

Security database updates for FDM-managed High Availability (HA) pair

Security database updates are applied only to the primary device of an HA pair.

Related Information:

- Onboard an FDM-Managed Device with a Registration Key
- Onboard an FDM-Managed Device Using Username, Password, and IP Address
- Schedule a Security Database Update