



Managing Site-to-Site Virtual Private Network in CDO

- [Introduction to Site-to-Site Virtual Private Network, on page 1](#)
- [Site-to-Site VPN Configuration for On-Prem Management Center-Managed Secure Firewall Threat Defense, on page 2](#)
- [Prerequisites for Configuring Site-to-Site VPN for On-Prem Management Center-managed Threat Defense, on page 3](#)
- [Create a Site-to-Site VPN Between On-Prem Firewall Management Center-Managed Threat Defense and ASA, on page 3](#)
- [Create a Site-to-Site VPN Between On-Prem Firewall Management Center-Managed Threat Defense Devices, on page 5](#)
- [Create a Site-to-Site VPN Between On-Prem Firewall Management Center-Managed Threat Defense and Cloud-delivered Firewall Management Center-Managed Threat Defense, on page 6](#)
- [Create a Site-to-Site VPN Between On-Prem Firewall Management Center-Managed Threat Defense and Extranet, on page 8](#)
- [Create a Site-to-Site VPN Between On-Prem Management Center-Managed Threat Defense and Multicloud Defense Gateway, on page 10](#)
- [Discover Existing Site-to-Site VPN Tunnels from On-Prem Management Center, on page 12](#)
- [About Global IKE Policies, on page 12](#)
- [About IPsec Proposals, on page 13](#)
- [Encryption and Hash Algorithms Used in VPN, on page 13](#)

Introduction to Site-to-Site Virtual Private Network

A site-to-site VPN tunnel connects networks in different geographic locations. 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.

This connection enables secure communication between the two sites, protecting the data being exchanged from unauthorized access.

VPN Topology

To create a new site-to-site VPN topology, you must provide a unique name, choose the IKE version that is used for IPsec IKEv1 or IKEv2, or both and authentication method. When configured, you deploy the topology to the devices from the on-prem management center.

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

For authentication of VPN connections, configure a pre-shared key in the topology on each device. Pre-shared keys allow a secret key, which is used during the IKE authentication phase, to be shared between two peers.

VPN Encryption Domain

CDO supports only route-based encryption for creating site-to-site VPN for on-prem management center-managed threat defense devices.

Route-Based: The encryption domain is set to encrypt only specific IP ranges for both source and destination. It creates a virtual IPsec interface, and whatever traffic enters that interface is encrypted and decrypted. ASA supports route-based VPN with the use of Virtual Tunnel Interfaces (VTIs).

Site-to-Site VPN Configuration for On-Prem Management Center-Managed Secure Firewall Threat Defense

You can connect two sites securely by configuring a site-to-site VPN tunnel between an on-prem management center-managed threat defense device on a site and another device on a different site that comply with all relevant standards.

CDO supports the following configuration:

Site A	Site B
On-Prem Management Center-managed threat defense	CDO-managed ASA
On-Prem Management Center-managed threat defense	On-Prem Management Center-managed threat defense Note Threat Defense devices that are managed by two different or the same on-prem management center
On-Prem Management Center-managed threat defense	cloud-delivered Firewall Management Center managed threat defense
On-Prem Management Center-managed threat defense	Extranet device

Site A	Site B
On-Prem Management Center-managed threat defense	Multicloud Defense Gateway

Prerequisites for Configuring Site-to-Site VPN for On-Prem Management Center-managed Threat Defense

- Make sure that the on-prem management center has been successfully added to the CDO platform, and the threat defense devices are running version 7.2.x or later.

Enable the **Discover & Manage Network Objects** on CDO to discover objects from your on-prem management center, which you can share, manage, and use to set consistent object definitions across other platforms managed by CDO. See [Discover and Manage On-Prem Firewall Management Center Network Objects](#).


- The virtual tunnel interface (VTI) used by the tunnel must already exist on the on-prem management center-managed threat defense devices. CDO does not provide the functionality to create interfaces on these devices, instead it only displays pre-existing interfaces. Therefore, to create new VTIs, you need to configure them from the on-prem management center before creating a tunnel in CDO.
- The on-prem management center must have a preconfigured access list and a policy-based routing to enable traffic routing and tunnel operation.

**Note**

Not applicable to site-to-site VPN between on-prem management center-managed threat defense and Extranet.

Create a Site-to-Site VPN Between On-Prem Firewall Management Center-Managed Threat Defense and ASA

Step 1 In the navigation pane, choose **VPN > Site-to-Site VPN**.

Step 2 Click the create tunnel () button on the top-right corner and click **Site-to-Site VPN** with the **FMC Managed Device / ASA** label.

Step 3 In the **Configuration Name** field, enter a name for the site-to-site VPN configuration you create.

Step 4 Click the **Route Based** radio button.

Step 5 In the **Peer Devices** area, provide the following information:

- a) **Peer 1:** From the **Device** drop-down list, choose a threat defense managed by an on-prem management center. The device type is **FMC FTD**.
- b) **Peer 2:** From the **Device** drop-down list, select an ASA device. The device type is **ASA**.

- c) **VPN Access Interface:** Choose the virtual tunnel interfaces of both peers. The peer 2 (ASA) connects peer 1 (on-prem management center-managed threat defense through the VPN access interface of peer 1. Similarly, peer 1 (on-prem management center-managed threat defense) connects peer 2 (ASA) through the VPN access interface of peer 2.

Note CDO does not provide the functionality to create virtual tunnel interfaces for the on-prem management center-managed threat defense devices, instead it only displays pre-existing interfaces of the on-prem management center. Therefore, you must configure them from the on-prem management center before creating a tunnel in CDO.

- d) **LAN Interfaces:** Choose the LAN interfaces of both peers that control the LAN subnets. You can select multiple interfaces.

The networks attached to the selected LAN interfaces will be added to the routing policy access list. The traffic matching the routing policy access list will be encrypted/decrypted by the VPN tunnel.

- e) **Routing:** Click **Add Network** and choose protected networks from each peer to create a site-to-site tunnel between them.
- f) Click **Next**.

Step 6

In the **Tunnel Details** area, the **VTI Address** specifies the addresses for the new Virtual Tunnel Interfaces on the peers. CDO provides a sample address which you can change if it causes conflict. You can assign any unused IP address that is currently not used on this device.

Step 7

In the **IKE Settings** area, choose the IKE version for the Internet Key Exchange (IKE) negotiations and specify the privacy configurations. For more information on the IKE policies, see [About Global IKE Policies](#).

Based on your configuration, CDO suggests the IKE settings. You can either continue with the recommended IKE configuration settings or configure a new one.

Note Enabling both IKE versions is not allowed for route-based VPN.

- a) Enable any one IKE version that you want.
By default, the **IKEV Version 2** protocol is enabled.
- b) To configure IKE Version 2, enable **IKE Version 2** and click **Add IKEv2 Policies** to select the policies you want. The IKEv2 policies must be selected for both peers.

CDO generates a default **Pre-Shared Key** for peer 1. This is a secret key string that is configured on the peers. IKE uses this key during the authentication phase. It is used to verify each other when establishing a tunnel between the peers.

- c) To configure IKE Version 1, enable **IKE Version 1** and click **Add IKEv1 Policies** to select the policies you want. The IKEv1 policies must be selected for both peers.

CDO generates a default **Pre-shared Key** which can be modified.

- d) Click **Next**.


Step 8

In the **IPSec Settings** area, provide the following information:

- a) Click **Add IKE IPSec Proposals** to select the IKE IPSec configuration. The proposals are available depending on the selection that is made in the **IKE Settings** step. The IKEv2 IPSec proposals policies must be selected for both peers. For more information, see [About IPSec Proposals](#).
- b) (Optional) Choose the **Diffie-Hellman Group for Perfect Forward Secrecy**. For more information, see [Encryption and Hash Algorithms Used in VPN, on page 13](#)
- c) Click **Next**.

- Step 9** In the **Finish** area, read the configuration and continue further only if you're satisfied with your configuration.
- By default, the **Deploy changes to ASA immediately** check box is checked to deploy the configurations immediately to the ASA device after clicking **Submit**.
- If you want to review and deploy the configurations manually later, then uncheck this check box.
- Step 10** Click **Submit**.
- The configurations are automatically pushed from CDO to on-prem management center.
- Step 11** Perform the following steps to deploy the configuration manually to an on-prem management center-managed threat defense device.
- a) Login to the on-prem management center and choose **Devices > VPN > Site To Site**. You can see the same VPN topology that was configured in CDO.
 - b) Deploy these changes to your threat defense. See [Configuration Deployment](#) in the *Cisco Secure Firewall Management Center Device Configuration Guide* for more information.
-

Create a Site-to-Site VPN Between On-Prem Firewall Management Center-Managed Threat Defense Devices

- Step 1** In the navigation pane, choose **VPN > Site-to-Site VPN**.
- Step 2** Click the create tunnel () button on the top-right corner and click **Site-to-Site VPN** with the **FMC Managed Device / ASA** label.
- Step 3** In the **Configuration Name** field, enter a name for the site-to-site VPN configuration you create.
- Step 4** Click the **Route Based** radio button.
- Step 5** In the **Peer Devices** area, provide the following information:
- a) **Device**: From the **Device** drop-down list for **Peer 1**, choose on-prem management center-managed threat defense device and then click **Select**. The device type is **FMC FTD**. Repeat this step for **Peer 2**.
 - b) **VPN Access Interface**: Choose the virtual tunnel interfaces of both peers. The devices use the selected interfaces for their connection with each other.
- Note** CDO does not provide the functionality to create virtual tunnel interfaces for the on-prem management center-managed threat defense devices, instead it only displays pre-existing interfaces of the on-prem management center. Therefore, you must configure them from the on-prem management center before creating a tunnel in CDO.
- c) **LAN Interfaces**: Choose the LAN interfaces of both peers that control the LAN subnets. You can select multiple interfaces.
- The networks attached to the selected LAN interfaces will be added to the routing policy access list. The traffic matching the routing policy access list will be encrypted/decrypted by the VPN tunnel.
- d) **Routing**: Click **Add Network** and choose protected networks from each peer to create a site-to-site tunnel between them.

- e) Click **Next**.

Step 6

In the **IKE Settings** area, 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 [About Global IKE Policies](#).

Based on the configuration made by the user, CDO suggests the IKE settings. You can either continue with the recommended IKE configuration settings or define a new one.

Note Enabling both IKE versions is not allowed for route-based VPN.

- a) Enable any one IKE version that you want.

By default, the **IKEV Version 2** is enabled.

Note Enabling both IKE versions is not allowed for route-based VPN.

- b) To configure IKE Version 2, enable **IKE Version 2** and click **Add IKEv2 Policies** to select the policies you want. The IKEv2 policies must be selected for both peers.

CDO generates a default **Pre-Shared Key** for peer 1. This is a secret key string that is configured on the peers. IKE uses this key during the authentication phase. It is used to verify each other when establishing a tunnel between the peers.

- c) To configure IKE Version 1, enable **IKE Version 1** and click **Add IKEv1 Policies** to select the policies you want. The IKEv1 policies must be selected for both peers.

CDO generates a default **Pre-shared Key** which can be modified.

- d) Click **Next**.

Step 7

In the **IPSec Settings** area, provide the following information:

- a) Click **Add IKE IPSec Proposals** to select the IKE IPSec configuration. The proposals are available depending on the selection that is made in the **IKE Settings** step. The IKEv2 IPSec proposals policies must be selected for both peers. For more information, see [About IPSec Proposals](#).
- b) (Optional) Choose the **Diffie-Hellman Group for Perfect Forward Secrecy**. For more information, see [Encryption and Hash Algorithms Used in VPN, on page 13](#)
- c) Click **Next**.

Step 8

In the **Finish** area, read the configuration and continue further only if you're satisfied with your configuration.

Step 9

Click **Submit**.

The configurations are automatically pushed from CDO to on-prem management center.

Step 10


Perform the following steps to deploy configurations manually to an on-prem management center-managed threat defense device.

- a) Login to the on-prem management center and choose **Devices > VPN > Site To Site**. You can see the same VPN topology that was configured in CDO.
- b) Deploy these changes to your threat defense. See [Configuration Deployment](#) in the *Cisco Secure Firewall Management Center Device Configuration Guide* for more information.

Create a Site-to-Site VPN Between On-Prem Firewall Management Center-Managed Threat Defense and

Cloud-delivered Firewall Management Center-Managed Threat Defense

Step 1 In the navigation pane, choose **VPN** > **Site-to-Site VPN**.

Step 2 Click the create tunnel () icon on the top-right corner and click **Site-to-Site VPN** with the **FMC Managed Device / ASA** label.

Step 3 In the **Configuration Name** field, enter a name for the site-to-site VPN configuration you create.

Step 4 Click the **Route Based** radio button.

Step 5 In the **Peer Devices** area, provide the following information:

- a) **Peer 1:** From the **Device** drop-down list, choose an on-prem management center-managed threat defense device. The device type is **FMC FTD**.
- b) **Peer 2:** From the **Device** drop-down list, choose a cloud-delivered Firewall Management Center-managed threat defense device. The device type is **FTD**.
- c) **VPN Access Interface:** Choose the virtual tunnel interfaces of both peers. The peer 2 (cloud-delivered Firewall Management Center-managed threat defense) connects peer 1 (on-prem management center for threat defense) through the VPN access interface of peer 1. Similarly, peer 1 (on-prem management center-managed threat defense) connects peer 2 (cloud-delivered Firewall Management Center-managed threat defense) through the VPN access interface of peer 2.

Note CDO does not provide the functionality to create virtual tunnel interfaces for the on-prem management center-managed threat defense devices, instead it only displays pre-existing interfaces of the on-prem management center. Therefore, you must configure them from the on-prem management center before creating a tunnel in CDO.

- d) **LAN Interfaces:** Choose the LAN interfaces of both peers that control the LAN subnets. You can select multiple interfaces.

The networks attached to the selected LAN interfaces will be added to the routing policy access list. The traffic matching the routing policy access list will be encrypted/decrypted by the VPN tunnel.

- e) **Routing:** Click **Add Network** and choose protected networks from each peer to create a site-to-site tunnel between them.
- f) Click **Next**.

Step 6 In the **IKE Settings** area, 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 [About Global IKE Policies](#).

Based on the configuration made by the user, CDO suggests the IKE settings. You can either continue with the recommended IKE configuration settings or define a new one.

Note Enabling both IKE versions is not allowed for route-based VPN.

- a) Enable any one IKE version that you want.

By default, the **IKEV Version 2** is enabled.

Note Enabling both IKE versions is not allowed for route-based VPN.

- b) To configure IKE Version 2, enable **IKE Version 2** and click **Add IKEv2 Policies** to select the policies you want. The IKEv2 policies must be selected for both peers.

CDO generates a default **Pre-Shared Key** for peer 1. This is a secret key string that is configured on the peers. IKE uses this key during the authentication phase. It is used to verify each other when establishing a tunnel between the peers.

- c) To configure IKE Version 1, enable **IKE Version 1** and click **Add IKEv1 Policies** to select the policies you want. The IKEv1 policies must be selected for both peers.

CDO generates a default **Pre-shared Key** which can be modified.

- d) Click **Next**.

Step 7

In the **IPSec Settings** area, provide the following information:

- a) Click **Add IKE IPSec Proposals** to select the IKE IPSec configuration. The proposals are available depending on the selection that is made in the **IKE Settings** step. The IKEv2 IPSec proposals policies must be selected for both peers. For more information, see [About IPsec Proposals](#).
- b) (Optional) Choose the **Diffie-Hellman Group for Perfect Forward Secrecy**. For more information, see [Encryption and Hash Algorithms Used in VPN, on page 13](#)
- c) Click **Next**.

Step 8

In the **Finish** area, read the configuration and continue further only if you're satisfied with your configuration.

Step 9

Click **Submit**.

Step 10

Perform the following steps to deploy the configuration to a cloud-delivered Firewall Management Center-managed threat defense device:

- a) Choose **Tools & Services > Firewall Management Center**.
- b) Ensure the check box corresponding to **Cloud-Delivered FMC** is checked and in the **Actions** pane on the right, click **Deployment**.
- c) Select the device participating in the site-to-site VPN configuration and click **Deploy**.
- d) Choose **Devices > VPN > Site To Site**. You can see the same VPN topology that was configured in CDO.

Step 11

Perform the following steps to deploy the configuration to an on-prem management center-managed threat defense device.


- a) Login to the on-prem management center and choose **Devices > VPN > Site To Site**. You can see the same VPN topology that was configured in CDO.
- b) Deploy these changes to your threat defense. See [Configuration Deployment](#) in the *Cisco Secure Firewall Management Center Device Configuration Guide* for more information.

Create a Site-to-Site VPN Between On-Prem Firewall Management Center-Managed Threat Defense and Extranet

You can configure a site-to-site VPN tunnel between the on-prem management center-managed threat defense device onboarded to CDO and an extranet device. The extranet can be non-Cisco devices or Cisco devices that CDO does not manage.

Before you begin

The site-to-site VPN tunnel configurations must be applied manually to the extranet devices.

-
- Step 1** In the navigation pane, choose **VPN > Site-to-Site VPN**.
- Step 2** Click the create tunnel () button on the top-right corner and click **Site-to-Site VPN** with **FMC Managed Device / ASA** label.
- Step 3** In the **Configuration Name** field, enter a name for the site-to-site VPN configuration you create.
- Step 4** Click the **Route Based** radio button.
- Step 5** In the **Peer Devices** area, provide the following information:
- Peer 1:** From the **Device** drop-down list, choose an on-prem management center-managed threat defense device and then click **Select**. The device type is **FMC FTD**.
 - Peer 2:** Enable **Extranet** and enter an IP address for the static interface.
 - VPN Access Interface:** Choose the virtual tunnel interface of peer 1. The extranet device uses the selected interface to connect with on-prem management center-managed threat defense.
- Note** CDO does not provide the functionality to create virtual tunnel interfaces for the on-prem management center-managed threat defense devices, instead it only displays pre-existing interfaces of the on-prem management center. Therefore, you must configure them from the on-prem management center before creating a tunnel in CDO.
- d) Click **Next**.
- Step 6** In the **IKE Settings** area, 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 [About Global IKE Policies](#).
- Based on the configuration made by the user, CDO suggests the IKE settings. You can either continue with the recommended IKE configuration settings or define a new one.
- Note** Enabling both IKE versions is not allowed for route-based VPN.
- Enable any one IKE version that you want.
By default, the **IKEV Version 2** is enabled.
 - To configure IKE Version 2, enable **IKE Version 2** and click **Add IKEv2 Policies** to select the policies you want.
CDO generates a default **Pre-Shared Key** for peer 1. This is a secret key string that is configured on the peers. IKE uses this key during the authentication phase. It is used to verify each other when establishing a tunnel between the peers.
 - To configure IKE Version 1, enable **IKE Version 1** and click **Add IKEv1 Policies** to select the policies you want.
CDO generates a default **Pre-shared Key** which can be modified.
 - Click **Next**.
- Step 7** In the **IPSec Settings** area, perform the following:
- Click **Add IKE IPSec Proposals** to select the IKE IPSec configuration. The proposals are available depending on the selection that is made in the **IKE Settings** step. For more information, see [About IPSec Proposals](#).
 - (Optional) Choose the **Diffie-Hellman Group for Perfect Forward Secrecy**. For more information, see [Encryption and Hash Algorithms Used in VPN, on page 13](#)
 - Click **Next**.

- Step 8** In the **Finish** area, read the configuration and continue further only if you're satisfied with your configuration.
- Step 9** Click **Submit**.
- The configurations are pushed automatically to the on-prem management center after clicking **Submit**.
- Step 10** Perform the following steps to deploy the configuration to an on-prem management center-managed threat defense device.
- Login to the on-prem management center and choose **Devices > VPN > Site To Site**. You can see the same VPN topology that was configured in CDO.
 - Deploy these changes to your threat defense. See [Configuration Deployment](#) in the *Cisco Secure Firewall Management Center Device Configuration Guide* for more information.

Create a Site-to-Site VPN Between On-Prem Management Center-Managed Threat Defense and Multicloud Defense Gateway


You can create site-to-site IPsec connections between an on-prem management center-managed threat defense and a Multicloud Defense Gateway that complies with all relevant standards. After the VPN connection is established, the hosts behind the firewall can connect to the hosts behind the gateway through the secure VPN tunnel.

Multicloud Defense currently supports Amazon Web Services (AWS), Azure, Google Cloud Platform (GCP), and Oracle OCI cloud accounts.

Before you begin

Ensure that the following prerequisites are met:

- The on-prem management center-managed threat defense device must not have any pending changes.
- The Multicloud Defense Gateway must be in the **Active** state.
- The Multicloud Defense Gateway must be VPN enabled. See [Enable VPN within the gateway](#).
- Read the [Prerequisites for Configuring Site-to-Site VPN for On-Prem Management Center-managed Threat Defense](#) for more information.
- Read the [Multicloud Defense Gateway prerequisites and limitations](#) for more information.

- Step 1** In the left pane, choose **VPN > Site-to-Site VPN**.
- Step 2** Click the create tunnel () icon on the top right corner and click **Site-to-Site VPN** with Multicloud Defense label.
- Step 3** In the **Peer Devices** section, provide the following information:
- Configuration Name:** Enter a name for the site-to-site VPN configuration.
 - Peer 1:** From the **Device 1** drop-down list, click **FMC FTD** tab and choose an on-prem management center-managed threat defense.

- c) **Peer 2:** From the **Device 2** drop-down list, click **Multicloud Defense** tab and choose a Multicloud Defense Gateway.
- d) **VPN Access Interface:** Choose the virtual tunnel interface (VTI) of peer 1 (on-prem management center-managed threat defense). The peer 2 (Multicloud Defense Gateway) uses the selected virtual access interface to connect with peer 1 (on-prem management center-managed threat defense).

Note CDO does not provide the functionality to create virtual tunnel interfaces for the on-prem management center-managed threat defense devices, instead it only displays pre-existing interfaces of the on-prem management center. Therefore, you must configure them from the on-prem management center before creating a tunnel in CDO.

- e) **Public IP (optional):**
- f) **Routing:** Click **Add Network** and choose protected networks from peer 1 to create a site-to-site tunnel between peers.

Step 4 In the **Tunnel Details** section, provide the following information:

- a) **Virtual Interface Tunnel IP:** : CDO assigns an IP address to the virtual tunnel interface of on-prem management center-managed threat defense, which cannot be changed. You must enter an IP address for the Multicloud Defense Gateway's virtual tunnel interface.
- b) **Autonomous System Number:** Enter the autonomous system numbers to uniquely identify the networks the peers manage.
- c) Select a threat defense managed using an on-prem management center.
- d) Click **Next**.

Step 5 In the **IKE Settings** section, click **Add IKEv2 Policies** to select the policies you want.

CDO generates a default **Pre-Shared Key** for peer 1. This is a secret key string that is configured on the peers. IKE uses this key during the authentication phase. It is used to verify each other when establishing a tunnel between the peers.

For more information on the IKE policies, see [About Global IKE Policies](#)

Step 6 Click **Next**.

Step 7 In the **IPSec Settings** section, click **Add IKE IPSec Proposals** to select the IKE IPSec configuration. The proposals are available depending on the selection that is made in the **IKE Settings** step.

For more information, see [About IPsec Proposals](#).

Step 8 Click **Next**.

Step 9 In the **Finish** section, read the configuration and continue further only if you're satisfied with your configuration.

Step 10 Click **Submit**.

The configurations are pushed automatically to the on-prem management center after clicking **Submit**.

What to do next

Ensure you manually deploy these changes to your threat defense devices on your on-prem management center. See [Configuration Deployment](#) in the *Cisco Secure Firewall Management Center Device Configuration Guide* for more information.

Discover Existing Site-to-Site VPN Tunnels from On-Prem Management Center

When you onboard the on-prem management center to CDO, the existing site-to-site VPN policies on the threat defense devices will be imported into CDO. If the site-to-site VPN policies are created for an on-prem management center that has already been onboarded, you must click **Check for Changes** to import the policies. After importing, these policies can be managed through CDO and deployed manually from the on-prem management center.

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.

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.

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.

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.

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 curves 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.