

Onboard a Secure Firewall Threat Defense to the Cloud-Delivered Firewall Management Center

Read the following information for onboarding prerequisties and procedures.

- Onboarding methods, on page 1
- Maximum Firewall Threat Defense devices supported in Cloud-Delivered Firewall Management Center, on page 2
- Requirements: Prerequisites to onboard a device to Cloud-Delivered Firewall Management Center, on page 3
- Onboard a device with a CLI registration key, on page 4
- Onboard a Firewall Threat Defense Device to Cloud-Delivered Firewall Management Center using Zero-Touch Provisioning, on page 6
- Onboard a Firewall Threat Defense Device to On-Prem Firewall Management Center using Zero-Touch Provisioning, on page 8
- Onboard Firewall Threat Defense Devices using Device Templates to Cloud-Delivered Firewall Management Center using Zero-Touch Provisioning, on page 10
- Cloud deployment, on page 12
- Onboard a Secure Firewall Threat Defense Cluster, on page 30
- Onboard a chassis, on page 33
- Delete Devices from Cloud-Delivered Firewall Management Center, on page 35
- Enable Cloud-Delivered Firewall Management Center , on page 35
- Troubleshooting, on page 36

Onboarding methods

Onboarding is a device management process that

- connects Firewall Threat Defense devices to Cloud-Delivered Firewall Management Center for centralized management
- supports multiple methods including registration key and Zero-Touch Provisioning, and
- enables policy configuration and device monitoring through the management platform.

Onboarding requirements and compatibility

Review these use cases and supported software versions that are compatible with Cloud-Delivered Firewall Management Center management.

Note You must ensure that the Firewall Threat Defense device ports have external and outbound access for the Cloud-Delivered Firewall Management Center to onboard them. There is no requirement for an on-premises or cloud-based Security Device Controller (SDC) for this operation. For more information, see Network Requirements.

To send Firewall Threat Defense Syslog events to the Cisco cloud, you can set up the Secure Event Connector (SEC). For more information, see Installing Secure Event Connectors.

Firewall Threat Defense devices currently managed by Cloud-Delivered Firewall Management Center

These scenarios occur when you either move or migrate a device to the Cloud-Delivered Firewall Management Center:

- If you delete a device from an On-Premises Firewall Management Center or Secure Firewall Threat Defense Firewall Device Manager to onboard to the Cloud-Delivered Firewall Management Center, the change of managers wipes any policies configured through the On-Premises Firewall Management Center.
- If you **migrate** a device from an On-Premises Firewall Management Center to the Cloud-Delivered Firewall Management Center, the device retains the majority of your previously configured policies.

Note If you do not know if your device is already managed by an alternative manager, use the **show managers** command in the device's CLI.

Onboarding methods

Cloud-Delivered Firewall Management Center supports these onboarding methods:

- Registration Key - Onboard a device with a registration key. The initial device setup wizard is complete on the device.
- Zero-Touch Provisioning - Onboard a new factory-shipped device with its serial number. Note that this method only supports Firepower 1000, Firepower 2100, or Secure Firewall 3100 devices.
- Zero-Touch Provisioning using a device template - Onboard new factory-shipped devices using serial numbers and a device template. Note that this method only supports Firepower 1000, Firepower 2100, Secure Firewall 1200 or Secure Firewall 3100 devices.

Maximum Firewall Threat Defense devices supported in Cloud-Delivered Firewall Management Center

Cloud-Delivered Firewall Management Center supports up to 2,000 Firewall Threat Defense devices per deployment. This total can include a combination of standalone devices, devices in high-availability pairs, and devices that are cluster nodes.

The Cloud-Delivered Firewall Management Center can manage Firewall Threat Defense Version 7.2.0 and later.

Note The maximum number of supported Secure Firewall Threat Defense devices in Cloud-Delivered Firewall Management Center includes devices that are deployed for analytics on Firewall Management Center and onboarded to Cloud-Delivered Firewall Management Center for management. These devices count toward the platform device capacity limit and must be included in your capacity planning to ensure proper sizing and performance.

Requirements: Prerequisites to onboard a device to Cloud-Delivered Firewall Management Center

Onboard limitations and requirements

Be aware of the following limitations when onboarding a device to the Cloud-Delivered Firewall Management Center:

- Devices **must** be running version 7.2 and later.
- You can migrate an HA pair that is managed by an On-Premises Firewall Management Center by following the Migrate FTD to Cloud-Delivered Firewall Management Center process. Confirm both peers are in a healthy state prior to migrating.
- Devices managed locally by Firewall Device Manager can be onboarded using the serial number.
- Firewall Threat Defense devices can be onboarded to Cloud-Delivered Firewall Management Center using zero-touch provisioning if they are new (just unboxed) or have undergone a factory reset.
- If the device is managed by an On-Premises Firewall Management Center, you can either onboard the device to Cloud-Delivered Firewall Management Center or migrate the device. Migrating retains any existing policies and objects, whereas onboarding the device removes most policies and all objects. See Migrate FTD to Cloud-Delivered Firewall Management Center for more information.
- If your device is currently managed by a Firewall Device Manager, unregister all your smart licenses before you onboard the device. Even if you switch device management, the Cisco Smart Software Manager will retain the smart licenses.
- If you have previously onboarded a device that was managed by a Firewall Device Manager and deleted the device from Security Cloud Control with the intention of re-onboarding for cloud management, you **must** register the Firewall Device Manager to the Security Services Exchange cloud after deleting the device. See the "Access Security Services Exchange" chapter in the *Firepower and Cisco SecureX Threat Response Integration Guide.*

Tip Onboarding a device to the Cloud-Delivered Firewall Management Center removes any policies and most objects configured through the previous manager. If your device is currently managed by an On-Premises Firewall Management Center, it is possible to migrate the device and retain your policies and objects. See Migrate FTD to Cloud-Delivered Firewall Management Center for more information.

Network requirements

Before you onboard a device, ensure the following ports have external and outbound access. Confirm the following ports on the device are allowed. If communication ports are blocked behind a firewall, onboarding the device may fail.

Note You cannot configure these ports in the Security Cloud Control UI. You must enable these ports through the device's SSH.

Table 1: Device port requirements

Port	Protocol / Feature	Details
443/tcp	HTTPS	Send and receive data from the internet.
443	HTTPS	Communicate with the AMP cloud (public or private)
8305/tcp	Appliance communications	Securely communicate between appliances in a deployment.

Management and data interfaces

Make sure your device is correctly configured with either a management or data interface.

To configure a management or data interface on your device, see Complete the initial configuration of a Secure Firewall Threat Defense device using the CLI.

Onboard a device with a CLI registration key

This task enables you to onboard a Firewall Threat Defense device to Cloud-Delivered Firewall Management Center using a CLI registration key method, allowing for remote management and policy deployment to the device.

Use this procedure to onboard a device for Cloud-Delivered Firewall Management Center with a CLI registration key.

Note If your device is currently managed by an On-Premises Firewall Management Center, onboarding the device will fail. You can either delete the device from the On-Premises Firewall Management Center and onboard as a fresh, new device with no policies or objects, or you can migrate the device and retain the existing policies and objects. See Migrate FTD to Cloud-Delivered Firewall Managmenet Center for more information.

Important You can create a Security Cloud Control-managed, standalone logical Firewall Threat Defense device using the Secure Firewall chassis manager or the FXOS CLI.

Before you begin

Before you onboard a device, be sure to complete these tasks:

- Cloud-Delivered Firewall Management Center is enabled for your tenant.
- Confirm the device's CLI configuration is successfully completed. See Complete the initial configuration of a Secure Firewall Threat Defense device using the CLI for more information.
- Review the prerequesites and limitations before you onboard the device. See "Prerequisites to Onboard a Device to Cloud-Delivered Firewall Management Center" in Managing Firewall Threat Defense with Cloud-Delivered Firewall Management Center in Security Cloud Control for more information.
- The device can be configured for either local management with Secure Firewall Device Manager or remote management with Cloud-Delivered Firewall Management Center.
- Device must be running version 7.2.0 and later.
- You have reset the device's SSH password as part of the bootstrap process. If you have you not reset the SSH password, Security Cloud Control recommends using the Onboard a Firewall Threat Defense Device to Cloud-Delivered Firewall Management Center using Zero-Touch Provisioning, on page 6 method.

Follow these steps to onboard a device with a CLI registration key:

Procedure

Step 1 In the left pane, click **Security Devices**.

Step 2 Click **Onboard device or service** ( ) icon.

Step 3 Click the **FTD** tile.

Step 4 Under **Management Mode**, select **FTD**.

By selecting **FTD** under **Management Mode**, you will not be able to manage the device using the previous management platform. All existing policy configurations except for interface configurations will be reset. You must re-configure policies after you onboard the device.

Step 5 Select **Use CLI Registration Key** as the onboarding method.

Step 6 Enter the device name in the **Device Name** field and click **Next**.

Step 7 In the **Policy Assignment** step, use the drop-down menu to select an access control policy to deploy once the device is onboarded.

If you have no policies configured, select the **Default Access Control Policy**.

Step 8 Specify whether the device you are onboarding is a physical or virtual device.

If you are onboarding a virtual device, you must select the device's performance tier from the drop-down menu.

Step 9 Select the subscription licenses you want to apply to the device and click **Next**.

Step 10 Security Cloud Control generates a command with the registration key. Connect to the device you are onboarding using SSH, log in as "admin" or a user with equivalent admin privileges and paste the entire registration key as is into the device's CLI.

Note: For Firepower 1000, Firepower 2100, ISA 3000, and Firewall Threat Defense Virtual devices, open an SSH connection to the device and log in as **admin**. Copy the entire registration command and paste it into the device's CLI interface at the prompt. In the CLI, enter **Y** to complete the registration. If your device was previously managed by Firewall Device Manager, enter **Yes** to confirm the submission.

Step 11 Click **Next** in the Security Cloud Control onboarding wizard.

Step 12 (Optional) Add labels to your device to help sort and filter the **Security Devices** page.

Enter a label and select the blue plus button. Labels are applied to the device after it's onboarded to Security Cloud Control.

Once the device is synchronized, select the device you just onboarded from the **Security Devices** page and select any of the options listed under the **Device Management** pane located to the right. We strongly recommend these actions:

- If you did not already, create a custom access control policy to customize the security for your environment. See Access Control Overview in *Managing Firewall Threat Defense with Cloud-Delivered Firewall Management Center in Security Cloud Control* for more information.
- Enable Cisco Security Analytics and Logging (SAL) to view events in the Security Cloud Control dashboard **or** register the device to an Secure Firewall Management Center for security analytics. See Cisco Security Analytics and Logging in *Managing Firewall Threat Defense with Cloud-Delivered Firewall Management Center in Security Cloud Control* for more information.

The device is successfully onboarded to Cloud-Delivered Firewall Management Center and appears in the Security Devices page. The selected access control policy is deployed to the device, and any configured labels are applied for device management and filtering.

Onboard a Firewall Threat Defense Device to Cloud-Delivered Firewall Management Center using Zero-Touch Provisioning

This task enables you to onboard a Firewall Threat Defense device to Cloud-Delivered Firewall Management Center using Zero-Touch Provisioning for automated device registration and configuration.

Only the Firepower 1000, Firepower 2100, Secure Firewall 1200, and Secure Firewall 3100 devices can be onboarded with the zero-touch provisioning method.

Before you begin

Confirm that the following is completed before onboarding:

- You have a Security Cloud Control tenant. If you do not, see Request a Security Cloud Control Tenant for more information.
- Cloud-Delivered Firewall Management Center is enabled for your tenant.
- The device is freshly installed but has never been logged into by either the device CLI, a Firewall Management Center, or the Firewall Device Manager.
- The device is running version 7.2 or later.
- The device's outside or management interface should be able to access the Security Services Exchange domain registration.us.sse.itd.cisco.com.

Procedure

Step 1 In the left pane, click **Security Devices**.

Step 2 Click **Onboard device or service** ( ) icon.

Step 3 Click the **FTD** tile.

Step 4 Under **Management Mode**, select **FTD**.

By selecting **FTD** under **Management Mode**, you will not be able to manage the device using the previous management platform. All existing policy configurations except for interface configurations will be reset. You must re-configure policies after you onboard the device.

Step 5 Click the **Use Serial Number** tile.

Step 6 Select Cloud-Delivered Firewall Management Center from the drop-down list. Click **Next**.

For information on onboarding a threat defense device to On-Prem Firewall Management Center, see Onboard a Threat Defense Device to On-Prem Firewall Management Center using Zero-Touch Provisioning.

Step 7 Enter the **Device Serial Number** and the **Device Name**. Select **Next**.

Step 8 Choose an option depending on whether the device is logged into and configured for a manager:

- If your device is brand new and has never been configured for a manager, click **Yes, this new device has never been logged into or configured for a manager**.
- If your device has been previously registered for a manager or is **still** registered to a manager, click **No, this device has been logged into and configured for a manager**.

Step 9 Click **Next**.

Step 10 In the **Policy Assignment** step, use the drop-down menu to select an access control policy to deploy once the device is onboarded.

If you have no policies configured, select the **Default Access Control Policy**.

Step 11 Select the subscription licenses you want to apply to the device and click **Next**.

Step 12 Once the device is synchronized, select the device you just onboarded from the **Security Devices** page and select any of the options listed under the **Device Management** pane located to the right. We strongly recommend these actions:

- If you did not already, create a custom access control policy to customize the security for your environment.

  For more information, see Access Control Overview.

- You can enable Cisco Security Analytics and Logging to view events in the Security Cloud Control dashboard, or register the device to a Secure Firewall Management Center for security analytics.

  For more information, see Cisco Security Analytics and Logging.

The Firewall Threat Defense device is successfully onboarded to Cloud-Delivered Firewall Management Center and appears in the Security Devices list with synchronized status.

Onboard a Firewall Threat Defense Device to On-Prem Firewall Management Center using Zero-Touch Provisioning

This task allows you to onboard a Firewall Threat Defense device to an on-premises Firewall Management Center using Zero-Touch Provisioning, enabling centralized security management.

Only the Firepower 1000, Firepower 2100, Secure Firewall 1200, and Secure Firewall 3100 devices can be onboarded to On-Premises Firewall Management Center using the zero-touch provisioning method.

Before you begin

Confirm the following is completed prior to onboarding:

- You have a Security Cloud Control tenant. If you do not, see Request a Security Cloud Control Tenant for more information.
- Before onboarding any new devices, ensure an on-prem FMC is fully set up, configured, and recognized as a management center within your Security Cloud Control tenant.
- The device is freshly installed and has never been logged into through the device CLI, a Firewall Management Center, or the Firewall Device Manager.
- The device is running version 7.2 or later. .

Procedure

Step 1 In the left pane, click **Security Devices**.

Step 2 Click **Onboard device or service** () icon.

Step 3 Click the **FTD** tile.

Step 4 Under **Management Mode**, select **FTD**.

By selecting **FTD** under **Management Mode**, you will not be able to manage the device using the previous management platform. All existing policy configurations except for interface configurations will be reset. You must re-configure policies after you onboard the device.

Step 5 Click **Use Serial Number**.

Step 6 Select an available on-prem FMC from the drop-down list. Click **Next**.



Note

- On-prem FMCs running version 7.4 or later and onboarded with Cisco Security Cloud are displayed in the drop-down.
- Provide the **Public IP address** or **FQDN** value of the selected on-prem FMC unless
  - The FTD is publicly reachable
  - The FTD is running a version earlier than 7.4
  - The connection is being made through the data interface

For information on onboarding a threat defense device to a Cloud-Delivered Firewall Management Center, see Onboard a Threat Defense Device to Cloud-delivered Firewall Management Center using Zero-Touch Provisioning.

Step 7 Enter the **Device Serial Number** and the **Device Name**. Click **Next**.

Step 8 Choose an option depending on whether the device is logged into and configured for a manager:

- If your device is brand new and has never been configured for a manager, click **Yes, this new device has never been logged into or configured for a manager**.
- If your device has been previously registered for a manager or is **still** registered to a manager, click **No, this device has been logged into and configured for a manager**.

Step 9 Click **Next**.

Step 10 In the **Policy Assignment** step, use the drop-down menu to select an access control policy to deploy once the device is onboarded.

If you have no policies configured, select the **Default Access Control Policy**.

Step 11 Select the subscription licenses you want to apply to the device and click **Next**.

Step 12 Once the device is synchronized, select the device you just onboarded from the **Security Devices** page and select any of the options listed under the **Device Management** pane located to the right. We strongly recommend these actions:

- If you did not already, create a custom access control policy to customize the security for your environment.

  For more information, see Access Control Overview.
- You can enable Cisco Security Analytics and Logging to view events in the Security Cloud Control dashboard, or register the device to a Secure Firewall Management Center for security analytics.

  For more information, see Cisco Security Analytics and Logging.

The Firewall Threat Defense device is successfully onboarded to the on-premises Firewall Management Center and appears in your Security Devices page for centralized management and monitoring.

Onboard Firewall Threat Defense Devices using Device Templates to Cloud-Delivered Firewall Management Center using Zero-Touch Provisioning

This task enables you to efficiently onboard multiple Firewall Threat Defense devices to Security Cloud Control using Zero-Touch Provisioning, device templates, and CSV files with serial numbers, template variables, object overrides, and licensing information.

Only the Firepower 1000, Firepower 2100, Secure Firewall 1200, Secure Firewall 200, and Secure Firewall 3100 devices can be onboarded with the zero-touch provisioning method.

Before you begin

Confirm that the following is completed before onboarding:

- You have a Security Cloud Control tenant. If you do not, see Request a Security Cloud Control Tenant for more information.
- Cloud-Delivered Firewall Management Center is enabled for your tenant.
- The device is freshly installed but has never been logged into by either the device CLI, a Firewall Management Center, or the Firewall Device Manager.
- The device is running version 7.4 or later.

Procedure

Step 1 In the left pane, click **Security Devices**.

Step 2 Click **Onboard device or service** ( ) icon.

Step 3 Click the **FTD** tile.

Step 4 Under **Management Mode**, select **FTD**.

By selecting **FTD** under **Management Mode**, you will not be able to manage the device using the previous management platform. All existing policy configurations except for interface configurations will be reset. You must re-configure policies after you onboard the device.

Step 5 Click the **Bulk Onboard using CSV File** tile.

Step 6 In the **Template Assignment** field, select a template from the drop-down list. The access control policy associated with the template and the supported device models for the selected template are then displayed. Click **Next**.

Step 7 In the **Upload CSV File** field, **Drag & drop** your CSV template file or **Click** to select the CSV template file that you want to upload.

You can download a **CSV Sample Template File** to have a look at the required header details that have to be used in the template. The CSV template file must be less than 2 MB in size. The filename must satisfy the following criteria:

- Can have a maximum of 64 characters.
- Only alphanumeric characters and special characters such as dash (-), period (.), and underscore (_) are allowed.
- Must not contain any spaces.

A properly formatted .CSV file has the following fields:

- Mandatory fields
  - Display Name - Name of the device. Type: string. Example: test1
  - Serial Number - Serial number of the device. Type: string, Example: JADX345670EG
- Optional fields
  - Device Group - Name of the device group, Type: string, Example: testgroup
  - Admin Password - Password for admin access, Type: string, Example: E28@2OiUrhx
- Variables - Use the following format: $<*varName*>. Sample variable: $LAN-Devices-IPv4Address - IPv4 address of the LAN device. Type: string. Example: 1.2.3.4.
- Network object overrides - Use the following format:<*objType*>:<*objName*>. Sample network object override: Network:LAN-Devices-Network - IP address of the network of LAN devices. Type: string. Example: 1.2.3.4.

A sample CSV template file containing configuration for two devices is as given below.

DisplayName	SerialNumber	AdminPassword	$WANLinkIP	Host:gateway
Branch A FTD	JADX345410AB	C15c05n0rt#	10.20.30.1	10.2.3.1
Branch B FTD	JADX345670CE	Admin123!	10.20.30.5	10.2.3.1

Step 8 Click **Next**.

Step 9 A statement mentioning that the devices are being onboarded is displayed. You can check the onboarding status of the devices in the **Security Devices** window.

Once the device is synchronized, select the device you just onboarded from the **Security Devices** page and select any of the options listed under the **Device Management** pane located to the right. We strongly recommend these actions:

- If you did not already, create a custom access control policy to customize the security for your environment. See Access Control Overview in *Managing Firewall Threat Defense with Cloud-Delivered Firewall Management Center in Security Cloud Control* for more information.
- Enable Cisco Security Analytics and Logging (SAL) to view events in the Security Cloud Control dashboard **or** register the device to an Secure Firewall Management Center for security analytics. See

Cisco Security Analytics and Logging in *Managing Firewall Threat Defense with Cloud-Delivered Firewall Management Center in Security Cloud Control* for more information.

The devices are successfully onboarded to Security Cloud Control using Zero-Touch Provisioning. You can view the onboarding status and manage the devices from the Security Devices window.

Cloud deployment

A cloud deployment is a deployment approach that

- streamlines the configuration of Cisco Secure Firewall Threat Defense Virtual and Multicloud Defense across multiple cloud platforms,
- enables selection and launch of optimal enforcement points for scalable network security, and
- ensures high performance within complex multicloud environments.

Cloud deployment capabilities and enforcement points

Cloud deployment helps you deploy cloud-based enforcement points based on your intended outcomes and use cases. This provides the most cost-effective, scalable, and fully featured security for your multicloud needs.

With cloud deployment, you can:

- deploy faster with a guided, intuitive interface,
- select and launch the right enforcement point for your use case, and
- scale automatically to match demand and sustain performance.

Available enforcement points:

- Cisco Secure Firewall Threat Defense Virtual (FTDv): recommended for TLS Decrypt, IDS/IPS, Antivirus, Geo IP, or Malicious IP.
- Multicloud Defense: recommended for Proxy, WAF – L7 DOS, DLP, or Two-Core Enforcement.

Supported cloud service providers are:

- AWS
- Azure
- Google Cloud Platform (GCP)
- Oracle Cloud Infrastructure (OCI): Supported in this release by Multicloud Defense gateway only

Configure FTDv enforcement point

Enable critical security features such as IDS/IPS, TLS decryption, and malware protection for cloud workloads across AWS, Azure, and GCP.

Cloud Deployment helps you deploy cloud-based enforcement points based on your intended outcomes and use cases. If you select TLS Decrypt, IDS/IPS, Antivirus, Geo IP, or Malicious IP, Cloud Deployment uses the Cisco Secure Firewall Threat Defense Virtual (FTDv) gateway for deployment.

Follow these steps to configure your FTDv enforcement point:

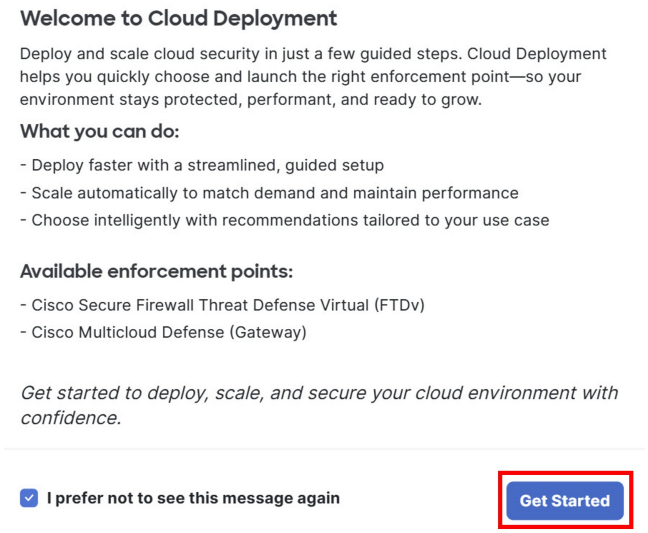
Before you begin

- Ensure you have access credentials and administrative permissions on your AWS, Azure, or GCP account.
- Prepare any required network settings, such as VPC/VNet information, security groups, and key pairs.
- Identify which security features you will enable (e.g., IDS/IPS, TLS decryption, Antivirus).

Procedure

Step 1 Choose **Security Devices** > **Cloud Deployment** .

Step 2 Click **Get Started** .



Step 3 On the **Account & Enforcement Type** tab, enter these details.

Field	Description
Account	Select an account from the drop-down list: AWS, Azure, or Google Cloud Platform (GCP).
Region	Select the region this gateway will be deployed into.

Select the type of Traffic Flow	Select the type of traffic flow (at least one must be selected): Ingress: Traffic entering from external destination Egress: Traffic leaving a network to external destination East-West: Traffic communicated across workloads with the network
Select your architectural requirements	Select TLS Decrypt, IDS/IPS, Antivirus, Geo IP, or Malicious IP to deploy through the FTDv gateway. Select Proxy, WAF – L7 DOS, DLP, or Two-Core Enforcement to deploy through Multicloud Defense gateway. Note that if you select Two-Core Enforcement, Antivirus is unavailable as it is not supported.

Step 4 Click **Next** .

Step 5 On the **Configure Enforcement Point** tab, enter these details.

Firepower Threat Defense Virtual Enforcement Information	
Name	Enter a unique name for this enforcement point; the name can be up to 53 characters long and must be alphanumeric and include an underscore or a hyphen.
Description	(Optional) Enter a description for this enforcement point.

If you selected AWS account earlier, enter these details:

VPC/VNet	You can select an existing Service VPC/VNet from the drop-down list or click **+ Create SVPC** to create a new one. After creation and activation, the wizard auto-populates the related network fields. This step can take up to three to four minutes.
Mgmt. Security Group	Select the security group to associate with the management interface.
Datapath Security Group 1	Select the security group to associate with datapath 1 interface.
Datapath Security Group 2	Select the security group to associate with datapath 2 interface.
Availability Zone	(Optional) Select the specific availability zone within a cloud region where a particular FTDv gateway instance is deployed. Click **+ Add Availability Zone** to add a new availability zone.

Management Subnet	(Optional) Select the subnet for the management interface in the selected availability zone.
Datapath Subnet 1	(Optional) Select the subnet for the primary datapath interface in the selected availability zone.
Datapath Subnet 2	(Optional) Select the subnet for the secondary datapath interface.
Cisco Secure Firewall Threat Defense Virtual	
License Model	Select the licensing model for the deployment: **Smart Licensing** , **Gateway Hours** , or **Pay As You Go**
Smart Licensing/Gateway Hours/Pay As You Go	
Software Version	Select the FTDv release to deploy.
Admin Password	Enter the Admin password. It must be between 12 and 72 characters in length and include uppercase and lowercase letters, numeric digits, and special characters, excluding the backslash (\) and hyphen (-) characters. The password cannot contain more than two identical or sequential characters in a row (such as 'aaa' or '123').
Policy Ruleset	Select the FMC policy to attach to the FTDv deployment.
Performance Tier	(Smart Licensing only) Expand the drop-down menu and select the appropriate performance tier for your device. FTDv50 is selected by default.
License Types	(Smart Licensing only) Expand the drop-down menu and select the appropriate license type that you have purchased or will purchase in the future. The **Base** license is auto-selected. For more information about different licensing types, refer to Licensing . If you want to enable malware defense features, you must also have the THREAT license active. The THREAT license is required to support the MALWARE license functionalities.
Gateway Configuration	
Instance Type	Select the VM size used for the gateway instances.
Minimum Instances	(Optional) Enter the minimum number of instances that you plan to deploy. This must be at least 1.
Maximum Instances	(Optional) Enter the maximum number instances that you plan to deploy. This is the maximum number that is used for auto-scaling in each availability zone. This number must be greater than or equal to minimum instances.

Health Check Port	(Optional) Enter the port number that the load balancer uses to check instance health. Datapath security groups assigned to the instance(s) must allow traffic on this port. The default port is 65534, and the valid range is from 1 to 65535.
Cloud Configuration	
Key Pair	Select the key pair that is associated with the cloud account you selected earlier. You must select an existing key pair from the chosen region.
EBS Encryption	Select the appropriate EBS encryption for your AWS account.
Advanced Settings	
Disable Public IP	Check the **Disable Public IP** check box. Disabling this setting reduces the exposure of your network to external threats. Private IP addresses help protect against unauthorized access, potential attacks, and provide better control over internal traffic. This setting applies only when using NAT-based service and only for data interfaces.

If you selected Azure account earlier, enter these details:

VPC/VNet	You can select an existing Service VPC/VNet from the drop-down list or click **+ Create SVPC** to create a new one. After creation and activation, the wizard auto-populates the related network fields. This step can take up to three to four minutes.
Resource Group	Select the resource group that owns the deployment resources.
Mgmt. Security Group	Select the security group to associate with the management interface.
Datapath Security Group 1	Select the security group to associate with datapath 1 interface.
Datapath Security Group 2	Select the security group to associate with datapath 2 interface.
Availability Zone	(Optional) Select the specific availability zone within a cloud region where a particular FTDv gateway instance is deployed. Click **+ Add Availability Zone** to add a new availability zone.
Management Subnet	(Optional) Select the subnet for the management interface in the selected availability zone.
Datapath Subnet 1	(Optional) Select the subnet for the primary datapath interface in the selected availability zone.

Datapath Subnet 2	(Optional) Select the subnet for the secondary datapath interface.
Cisco Secure Firewall Threat Defense Virtual	
License Model	Select the licensing model for the deployment: **Smart Licensing** or **Gateway Hours**
Smart Licensing/Gateway Hours	
Software Version	Select the FTDv release to deploy.
Admin Password	Enter the Admin password. It must be between 12 and 72 characters in length and include uppercase and lowercase letters, numeric digits, and special characters, excluding the backslash (\) and hyphen (-) characters. The password cannot contain more than two identical or sequential characters in a row (such as 'aaa' or '123').
Policy Ruleset	Select the FMC policy to attach to the FTDv deployment.
Performance Tier	(Smart Licensing only) Expand the drop-down menu and select the appropriate performance tier for your device. FTDv50 is selected by default.
License Types	(Smart Licensing only) Expand the drop-down menu and select the appropriate license type that you have purchased or will purchase in the future. The **Base** license is auto-selected. For more information about different licensing types, refer to Licensing . If you want to enable malware defense features, you must also have the THREAT license active. The THREAT license is required to support the MALWARE license functionalities.
Gateway Configuration	
Instance Type	Select the VM size used for the gateway instances.
Minimum Instances	(Optional) Enter the minimum number of instances that you plan to deploy. This must be at least 1.
Maximum Instances	(Optional) Enter the maximum number instances that you plan to deploy. This is the maximum number that is used for auto-scaling in each availability zone. This number must be greater than or equal to minimum instances.
Health Check Port	(Optional) Enter the port number that the load balancer uses to check instance health. Datapath security groups assigned to the instance(s) must allow traffic on this port. The default port is 65534, and the valid range is from 1 to 65535.
Azure Configuration	

Key Selection	You can either provide an **SSH Public Key** directly or select an existing **SSH Key Pair** from the drop-down list.
Disk Encryption	Select either a provider-managed encryption key or a customer-managed key (CMK). If using a CMK, provide the **Disk Encryption Set ID** .
Advanced Settings	
Disable Public IP	Check the **Disable Public IP** check box. Disabling this setting reduces the exposure of your network to external threats. Private IP addresses help protect against unauthorized access, potential attacks, and provide better control over internal traffic. This setting applies only when using NAT-based service and only for data interfaces.

If you selected GCP account earlier, enter these details:

GCP Configuration	
Datapath VPC	You can select an existing Service VPC/VNet from the drop-down list or click **+ Create SVPC** to create a new one. After creation and activation, the wizard auto-populates the related network fields. This step can take up to three to four minutes.
Datapath Network Tag 1	Select the network tag used for datapath firewall rules.
Datapath Network Tag 2	This is the second datapath tag used for dual-interface FTDv layouts. This identifies a separate management VPC.
Management VPC	Select the management VPC from the drop-down list.
Management Network Tag	Select the network tag used for management firewall rules from the drop-down list.
SSH Public Key	(Optional) Paste the SSH public key.
Disk Encryption	Select either a provider-managed encryption key or a customer-managed key (CMK). If using a CMK, provide the **Cloud KMS key resource name** .
Availability Zone	(Optional) Select the specific availability zone within a cloud region where a particular FTDv gateway instance is deployed. Click **+ Add Availability Zone** to add a new availability zone.
Management Subnet	(Optional) Select the subnet for the management interface in the selected availability zone.
Datapath Subnet 1	(Optional) Select the subnet for the primary datapath interface in the selected availability zone.

Datapath Subnet 2	(Optional) Select the subnet for the secondary datapath interface.
Cisco Secure Firewall Threat Defense Virtual	
License Model	Select the licensing model for the deployment: **Smart Licensing** or **Gateway Hours**
Smart Licensing/Gateway Hours	
Software Version	Select the FTDv release to deploy.
Admin Password	Enter the Admin password. It must be between 12 and 72 characters in length and include uppercase and lowercase letters, numeric digits, and special characters, excluding the backslash (\) and hyphen (-) characters. The password cannot contain more than two identical or sequential characters in a row (such as 'aaa' or '123').
Policy Ruleset	Select the FMC policy to attach to the FTDv deployment.
Performance Tier	(Smart Licensing only) Expand the drop-down menu and select the appropriate performance tier for your device. FTDv50 is selected by default.
License Types	(Smart Licensing only) Expand the drop-down menu and select the appropriate license type that you have purchased or will purchase in the future. The **Base** license is auto-selected. For more information about different licensing types, refer to Licensing . If you want to enable malware defense features, you must also have the THREAT license active. The THREAT license is required to support the MALWARE license functionalities.
Gateway Configuration	
Instance Type	Select the VM size used for the gateway instances.
Minimum Instances	(Optional) Enter the minimum number of instances that you plan to deploy. This must be at least 1.
Maximum Instances	(Optional) Enter the maximum number instances that you plan to deploy. This is the maximum number that is used for auto-scaling in each availability zone. This number must be greater than or equal to minimum instances.
Health Check Port	(Optional) Enter the port number that the load balancer uses to check instance health. Datapath security groups assigned to the instance(s) must allow traffic on this port. The default port is 65534, and the valid range is from 1 to 65535.
Advanced Settings	

Disable Public IP	Check the **Disable Public IP** check box. Disabling this setting reduces the exposure of your network to external threats. Private IP addresses help protect against unauthorized access, potential attacks, and provide better control over internal traffic. This setting applies only when using NAT-based service and only for data interfaces.

Step 6 Click **Next** . If you want to modify the settings, click **Back**

Step 7 On the **Review & Deploy** tab, review your configuration and deploy the enforcement point. If you encounter an error, return to the **Configure Enforcement Points** tab to correct it.

Step 8 Click **Deploy** .

Multicloud Defense deploys the gateway.

You must attach at least one ruleset to the gateway before you secure a spoke VPC/VNet. For more information about rule sets, refer to Rule Sets and Rule Set Groups .

The Cisco Secure Firewall Threat Defense Virtual (FTDv) enforcement point is deployed in your cloud environment, protecting workloads with the specified security features

Configure Multicloud Defense enforcement point

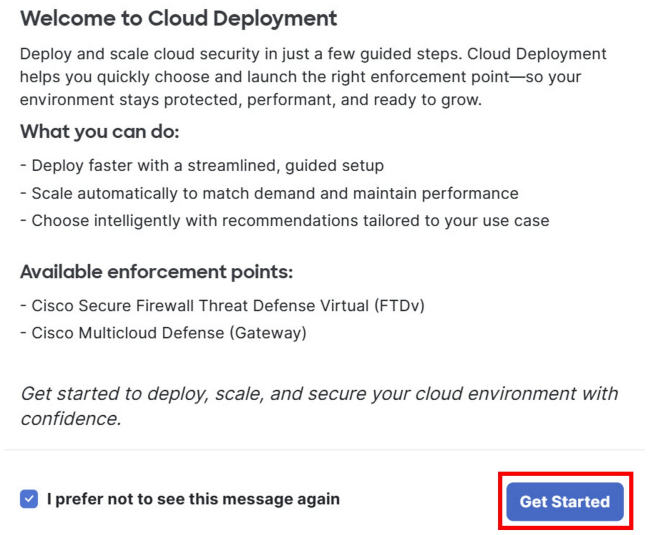
Cloud Deployment helps you deploy cloud-based enforcement points based on your intended outcomes and use cases. If you select Proxy, WAF – L7 DOS, DLP, or Two-Core Enforcement, Cloud Deployment uses the Multicloud Defense gateway for deployment.

Follow these steps to configure Multicloud Defense enforcement point:

Procedure

Step 1 Choose **Security Devices** > **Cloud Deployment** .

Step 2 Click **Get Started** .



Step 3 On the **Account & Enforcement Type** tab, enter these details.

Field	Description
Account	Select an account from the drop-down list: AWS, Azure, Google Cloud Platform (GCP), or Oracle Cloud Infrastructure (OCI).
Region	Select the region this gateway will be deployed into.
Select the type of Traffic Flow	Select the type of traffic flow (at least one must be selected): Ingress: Traffic entering from an external destination Egress: Traffic leaving a network to external destination East-West: Traffic communicated across workloads with the network
Select your architectural requirements	Select TLS Decrypt, IDS/IPS, Antivirus, Geo IP, or Malicious IP if you want to deploy these features through the FTDv gateway. Select Proxy, WAF – L7 DOS, DLP, or Two-Core Enforcement if you want to deploy through the Multicloud Defense gateway. Note that if you select Two-Core Enforcement, Antivirus is unavailable as it is not supported.

Step 4 Click **Next** .

Step 5 On the **Configure Enforcement Point** tab, enter these details.

Multicloud Defense Gateway Enforcement Information

Name	Enter a unique name for this enforcement point; the name can be up to 53 characters long and must be alphanumeric and include an underscore or a hyphen.
Description	(Optional) Enter a description for this enforcement point.

If you selected AWS account earlier, enter these details:

Multicloud Defense Gateway Enforcement Information	
Deployment	Click **Centralized** or **Distributed** to select the deployment type. **Centralized** allows you to select only a Service VPC. **Distributed** allows you to select only a regular VPC/VNet. If you select a Service VPC, the deployment operates in Hub mode. If you select a regular VPC or VNet, the deployment operates in Edge mode.
VPC/VNet	You can select an existing Service VPC/VNet from the drop-down list or click **+ Create SVPC** to create a new one. You cannot create a new Service VPC/VNet if you selected **Distributed** earlier. After you create and activate the service, the wizard automatically fills in the related network fields. This step can take up to 3 to 4 minutes.
Mgmt. Security Group	Select the security group to associate with the management interface.
Datapath Security Group	Select the security group to associate with the datapath interface.
Availability Zone	(Optional) Select the specific availability zone within a cloud region where a particular Multicloud Defense gateway instance is deployed. Click **+ Add Availability Zone** to add a new availability zone.
Management Subnet	(Optional) Select the subnet for the management interface in the selected availability zone.
Datapath Subnet	(Optional) Select the subnet for the primary datapath interface in the selected availability zone.
Gateway Configuration	
Instance Type	Select the VM size used for the gateway instances from the drop-down list.
Minimum Instances	(Optional) Enter the minimum number of instances you plan to deploy. This must be at least one.

Maximum Instances	(Optional) Enter the maximum number of instances you plan to deploy. This is the maximum number that is used for autoscaling in each availability zone. This number must be greater than or equal to minimum instances.
Health Check Port	Enter the port number used by Multicloud Defense load balancer to check the health of the instances. Datapath security groups assigned to the instance(s) must allow traffic on this port. The default port is 65534, and the valid range is from 1 to 65535.
Gateway Image Group	Select the logical grouping of available gateway images from the drop-down list.
Gateway Image	Select the exact gateway image/version to deploy from the drop-down list.
Policy Ruleset	Select the Multicloud Defense policy ruleset to attach to the gateway.
Cloud Configuration	
Key Pair	Select the key pair associated with the cloud account you selected in the previous screen.
Gateway IAM Role	Select the IAM role that allows the gateway to perform READ and WRITE operations on your AWS account. Multicloud Defense creates this role for you when you save and deploy the gateway.
EBS Encryption	Select the appropriate EBS encryption for your specific AWS account.
Multicloud Defense Profiles	
Packet Capture Profile	(Optional) Select the packet capture profile for threat and flow PCAPs.
Log Forwarding Profile	(Optional) Select the log forwarding profile used to forward Events/Logs to a security information and event management (SIEM) system.
Metrics Profile	(Optional) Select the metrics profile.
NTP Profile	(Optional) Select the Network Time Protocol (NTP) for time synchronization.
Advanced Settings	
Use Global Accelerator	(Ingress only) Associate the gateway with an AWS Global Accelerator listener so that traffic uses your accelerator.
Disable Public IP	By default, the Multicloud Defense gateway enables the use of the public IP of the router available. If you do not want this enabled, check the **Disable Public IP** check box. This reduces the exposure of your network to external threats.

Use Internal Load Balancer	To reduce the exposure of your network to external threats, you can use an internal load balancer instead of a public one for the gateway front end (Ingress only). While the Multicloud Defense gateway enables a public router IP by default, you can opt for a private configuration by checking the **Disable Public IP** check box.

If you selected Azure account earlier, enter these details:

Multicloud Defense Gateway Enforcement Information	
Deployment	Click **Centralized** or **Distributed** to select the deployment type. **Centralized** allows the selection of only a Service VPC. **Distributed** allows the selection of only a regular VPC/VNet. If you select a Service VPC, the deployment operates in Hub mode. If you select a regular VPC or VNet, the deployment operates in Edge mode.
VPC/VNet	You can select an existing Service VPC/VNet from the drop-down list or click **+ Create SVPC** to create a new one. You cannot create a new Service VPC/VNet if you selected **Distributed** earlier. After you create and activate the service, the wizard automatically fills in the related network fields. This step can take up to 3 to 4 minutes.
Resource Group	Select the resource group that owns the deployment resources.
Mgmt. Security Group	Select the security group to associate with the management interface.
Datapath Security Group 1	Select the security group to associate with the datapath interface.
Availability Zone	(Optional) Select the specific availability zone within a cloud region where a particular Multicloud Defense gateway instance is deployed. Click **+ Add Availability Zone** to add a new availability zone.
Management Subnet	(Optional) Select the subnet for the management interface in the selected availability zone.
Datapath Subnet	(Optional) Select the subnet for the primary datapath interface in the selected availability zone.
Gateway Configuration	

Instance Type	Select the VM size used for the gateway instances.
Minimum Instances	(Optional) Enter the minimum number of instances you plan to deploy. This must be at least one.
Maximum Instances	(Optional) Enter the maximum number of instances you plan to deploy. This is the maximum number that is used for autoscaling in each availability zone. This number must be greater than or equal to minimum instances.
Health Check Port	Enter the port number that the load balancer uses to check instance health. Datapath security groups assigned to the instance(s) must allow traffic on this port. The default port is 65534, and the valid range is from 1 to 65535.
Gateway Image Group	Select the logical grouping of available gateway images from the drop-down list.
Gateway Image	Select the exact gateway image/version to deploy from the drop-down list.
Policy Ruleset	Select the Multicloud Defense policy ruleset to attach to the gateway.
Azure Configuration	
Key Selection	You can either provide an **SSH Public Key** directly or select an existing **SSH Key Pair** from the drop-down list.
Username	The default SSH username is centos.
User Assigned Identity ID	(Optional) Used for accessing Key Vault or writing PCAP files to Blob Storage.
Disk Encryption	(Optional) Select the disk encryption type from the drop-down list
Multicloud Defense Profiles	
Packet Capture Profile	(Optional) Select the packet capture profile for threat and flow PCAPs.
Log Forwarding Profile	(Optional) Select the log forwarding profile used to forward Events/Logs to a security information and event management (SIEM) system.
Metrics Profile	(Optional) Select the metrics profile.
NTP Profile	(Optional) Select the Network Time Protocol (NTP) for time synchronization.
Advanced Settings	
Management DNS Server	(Optional) Enter the IP address of a DNS server reachable by the gateway for management traffic.

Attach Additional Load Balancer	(Optional) Click **+ Add** to associate Azure Load Balancers with this gateway for advanced traffic distribution. Select the **Azure LB Name** from the drop-down list and enter the **Backend Pool Name** and **Resource Group** .
Disable Public IP	By default, the Multicloud Defense gateway enables the use of the public IP of the router available. If you do not want this enabled, check the **Disable Public IP** check box. This reduces the exposure of your network to external threats.
Use Internal Load Balancer	To reduce the exposure of your network to external threats, you can use an internal load balancer instead of a public one for the gateway front end (Ingress only). While the Multicloud Defense gateway enables a public router IP by default, you can opt for a private configuration by checking the **Disable Public IP** check box.

If you selected GCP account earlier, enter these details:

Deployment	Click **Centralized** or **Distributed** to select the deployment type. **Centralized** allows the selection of only a Service VPC. **Distributed** allows the selection of only a regular VPC/VNet. If you select a Service VPC, the deployment operates in Hub mode. If you select a regular VPC or VNet, the deployment operates in Edge mode.
GCP Configuration	
Service Account Email	Enter the service account email attached to gateway instances.
Datapath VPC	You can select an existing Service VPC/VNet from the drop-down list or click **+ Create SVPC** to create a new one. After you create and activate the service, the wizard automatically fills in the related network fields. This step can take up to 3 to 4 minutes.
Datapath Network Tag	Select the network tag used for datapath firewall rules.
Management VPC	Select the management VPC from the drop-down list.
Management Network Tag	Select the network tag used for management firewall rules from the drop-down list.
Username	The default SSH username is centos.
SSH Public Key	(Optional) Paste the SSH public key.

Disk Encryption	(Optional) Select the disk encryption type from the drop-down list
Network Details	
Availability Zone	(Optional) Select the specific availability zone within a cloud region where a particular Multicloud Defense gateway instance is deployed. Click **+ Add Availability Zone** to add a new availability zone.
Management Subnet	(Optional) Select the subnet for the management interface in the selected availability zone.
Datapath Subnet	(Optional) Select the subnet for datapath interface in the selected availability zone.
Gateway Configuration	
Instance Type	Select the VM size used for the gateway instances.
Minimum Instances	(Optional) Enter the minimum number of instances you plan to deploy. This must be at least one.
Maximum Instances	(Optional) Enter the maximum number of instances you plan to deploy. This is the maximum number that is used for autoscaling in each availability zone. This number must be greater than or equal to minimum instances.
Health Check Port	Enter the port number that the load balancer uses to check instance health. Datapath security groups assigned to the instance(s) must allow traffic on this port. The default port is 65534, and the valid range is from 1 to 65535.
Gateway Image Group	Select the logical grouping of available gateway images from the drop-down list.
Gateway Image	Select the exact gateway image/version to deploy from the drop-down list.
Policy Ruleset	Select the Multicloud Defense policy ruleset to attach to the gateway.
Multicloud Defense Profiles	
Packet Capture Profile	(Optional) Select the packet capture profile for threat and flow PCAPs.
Log Forwarding Profile	(Optional) Select the log forwarding profile used to forward Events/Logs to a security information and event management (SIEM) system.
Metrics Profile	(Optional) Select the metrics profile.
NTP Profile	(Optional) Select the Network Time Protocol (NTP) for time synchronization.
Advanced Settings	

Disable Public IP	By default, the Multicloud Defense gateway enables the use of the public IP of the router available. If you do not want this enabled, check the **Disable Public IP** check box. This reduces the exposure of your network to external threats.
GCP LB Protocol UDP	Check this check box to enable UDP on the gateway's GCP load balancer configuration.

If you selected Oracle Cloud Infrastructure (OCI) account earlier, enter these details:

Multicloud Defense Gateway Enforcement Information	
Deployment	Click **Centralized** or **Distributed** to select the deployment type. **Centralized** allows the selection of only a Service VPC. **Distributed** allows the selection of only a regular VPC/VNet. If you select a Service VPC, the deployment operates in Hub mode. If you select a regular VPC or VNet, the deployment operates in Edge mode.
VPC/VNet	You can select an existing Service VPC/VNet from the drop-down list or click **+ Create SVPC** to create a new one. You cannot create a new Service VPC/VNet if you selected **Distributed** earlier. After you create and activate the service, the wizard automatically fills in the related network fields. This step can take up to 3 to 4 minutes.
Mgmt. Security Group	(Optional) Select the security group to associate with the management interface.
Datapath Security Group	(Optional) Select the security group to associate with the datapath interface.
Availability Zone	(Optional) Select the specific availability zone within a cloud region where a particular Multicloud Defense gateway instance is deployed. Click **+ Add Availability Zone** to add a new availability zone.
Management Subnet	(Optional) Select the subnet for the management interface in the selected availability zone.
Datapath Subnet	(Optional) Select the subnet for the primary datapath interface in the selected availability zone.
Gateway Configuration	

Instance Type	Select the VM size used for the gateway instances from the drop-down list.
Minimum Instances	(Optional) Enter the minimum number of instances you plan to deploy. This must be at least one.
Maximum Instances	(Optional) Enter the maximum number of instances you plan to deploy. This is the maximum number that is used for autoscaling in each availability zone. This number must be greater than or equal to minimum instances.
Health Check Port	Enter the port number used by Multicloud Defense load balancer to check the health of the instances. Datapath security groups assigned to the instance(s) must allow traffic on this port. The default port is 65534, and the valid range is from 1 to 65535.
Gateway Image Group	Select the logical grouping of available gateway images from the drop-down list.
Gateway Image	Select the exact gateway image/version to deploy from the drop-down list.
Policy Ruleset	Select the Multicloud Defense policy ruleset to attach to the gateway.
OCI Configuration	
Compartment	OCI Compartment where Multicloud Defense gateway will be deployed.
SSH Public Key	Paste the SSH public key.
Multicloud Defense Profiles	
Packet Capture Profile	Select the packet capture profile for threat and flow PCAPs.
Log Forwarding Profile	Select the log forwarding profile used to forward Events/Logs to a security information and event management (SIEM) system.
Metrics Profile	Select the metrics profile.
NTP Profile	Select the Network Time Protocol (NTP) for time synchronization.
Advanced Settings	
Internal Load Balancer	To reduce the exposure of your network to external threats, you can use an internal load balancer instead of a public one for the gateway front end (Ingress only). While the Multicloud Defense gateway enables a public router IP by default, you can opt for a private configuration by selecting the **Disable Public IP** check box.
User ID	Enable User ID on the gateway if your account supports it.
Management DNS Server	Enter the IP address of a DNS server reachable by the gateway for management traffic.

Public IP	By default, the Multicloud Defense gateway enables the use of the public IP of the router available. If you do not want this enabled, check the **Disable Public IP** check box. This reduces the exposure of your network to external threats.

Step 6 Click **Next** . If you want to modify the settings, click **Back** .

Step 7 On the **Review & Deploy** tab, review your configuration and deploy the enforcement point. If you encounter an error, return to the **Configure Enforcement Points** tab to correct it.

Step 8 Click **Deploy** .

Multicloud Defense deploys the gateway.

You must attach at least one ruleset to the gateway before you secure a spoke VPC/VNet. For more information about rule sets, refer to Rule Sets and Rule Set Groups .

Onboard a Secure Firewall Threat Defense Cluster

This task enables you to register a Secure Firewall Threat Defense cluster with Cloud-Delivered Firewall Management Center for centralized management and policy enforcement.

The following table provides information about device models that support cluster onboarding and creation on the Cloud-Delivered Firewall Management Center:

Secure Firewall Threat Defense Platforms	Minimum Secure Firewall Threat Defense Version for Cluster Management	Support cluster creation from Cloud-Delivered Firewall Management Center?
VMware, KVM	7.2.1	Yes
AWS, GCP	7.2.1	No
Azure	7.3	No
Secure Firewall 3100	7.2.1	Yes
Firepower 4100	7.2.x	No
Secure Firewall 4200	7.4	Yes
Firepower 9300	7.2.x	No

Note When you onboard a Secure Firewall Threat Defense cluster to Cloud-Delivered Firewall Management Center, you register only the cluster CONTROL NODE. After the CONTROL NODE registers, Cloud-Delivered Firewall Management Center discovers the DATA nodes in the cluster.

Before you begin

Review these limitations:

- Firepower 4100 and Firepower 9300 devices must be clustered through the device's Firewall Chassis Manager.
- Secure Firewall 3100 devices, Secure Firewall 4200 devices, KVM, and VMware environments must be clustered through the Cloud-Delivered Firewall Management Center UI.
- Azure, AWS, and GCP environment clusters must be created through their own environment and onboarded to Cloud-Delivered Firewall Management Center.
- Verify that the Secure Firewall Threat Defense virtual devices are successfully configured as a cluster before you register the cluster with Cloud-Delivered Firewall Management Center.

  For example, in the Secure Firewall Threat Defense CLI, enter the `show cluster info` command. Confirm that the output shows the cluster as `On`, one unit in `CONTROL_NODE` state, and the remaining units in `DATA_NODE` state.

```
> show cluster info
Cluster mAZ-ngfw-cl: On
    Interface mode: individual
Cluster Member Limit : 16
    This is "74-a" in state DATA_NODE
        ID        : 2
        Version   : 9.22(1)1
        Serial No.: 9AUVQ3DSF66
        CCL IP    : 1.1.1.74
        CCL MAC   : 02e2.778f.d3ed
        Module    : NGFWv
        Resource  : 4 cores / 7680 MB RAM
        Last join : 07:28:26 UTC Sep 25 2024
        Last leave: 07:28:11 UTC Sep 25 2024
Other members in the cluster:
    Unit "135-b" in state CONTROL_NODE
        ID        : 0
        Version   : 9.22(1)1
        Serial No.: 9A6W0A51KGK
        CCL IP    : 1.1.2.135
        CCL MAC   : 1294.34ae.4ce9
        Module    : NGFWv
        Resource  : 4 cores / 7680 MB RAM
        Last join : 09:45:52 UTC Sep 24 2024
        Last leave: N/A
    Unit "183-c" in state DATA_NODE
        ID        : 1
        Version   : 9.22(1)1
        Serial No.: 9A1S400HL8F
        CCL IP    : 1.1.3.183
        CCL MAC   : 0aff.e889.f193
        Module    : NGFWv
        Resource  : 4 cores / 7680 MB RAM
        Last join : 07:29:29 UTC Sep 25 2024
        Last leave: 07:28:11 UTC Sep 25 2024
>
```

Follow these steps to onboard a Secure Firewall Threat Defense cluster:

Procedure

Step 1 In the left pane, click **Security Devices**.

Step 2 Click **Onboard device or service** ( ) icon.

Step 3 Click the **FTD** tile.

Step 4 Under **Management Mode**, select **FTD**.

By selecting **FTD** under **Management Mode**, you will not be able to manage the device using the previous management platform. All existing policy configurations except for interface configurations will be reset. You must re-configure policies after you onboard the device.

Step 5 Select **Use CLI Registration Key**.

Step 6 Enter the device name in the **Device Name** field and click **Next**.

Step 7 In the **Policy Assignment** step, use the drop-down menu to select an access control policy to deploy once the device is onboarded.

If you have no policies configured, select the **Default Access Control Policy**.

Step 8 Specify whether the device you are onboarding is a physical or virtual device.

If you are onboarding a virtual device, you must select the device's performance tier from the drop-down menu.

Step 9 Select the subscription licenses you want to apply to the device and click **Next**.

Step 10 Security Cloud Control generates a command with the registration key. Paste the entire registration key into the device's CLI without making changes.

Step 11 (Optional) Add labels to your device to help sort and filter the **Security Devices** page.

Enter a label and select the blue plus button. Labels are applied to the device after it's onboarded to Security Cloud Control.

Once the device is synchronized, select the device you just onboarded from the **Security Devices** page and select any of the options listed under the **Device Management** pane located to the right. We strongly recommend these actions:

- If you did not already, create a custom access control policy to customize the security for your environment. See Access Control Overview in *Managing Firewall Threat Defense with Cloud-Delivered Firewall Management Center in Security Cloud Control* for more information.
- Enable Cisco Security Analytics and Logging (SAL) to view events in the Security Cloud Control dashboard **or** register the device to an Secure Firewall Management Center for security analytics. See Cisco Security Analytics and Logging in *Managing Firewall Threat Defense with Cloud-Delivered Firewall Management Center in Security Cloud Control* for more information.

Onboard a chassis

This task allows you to add a Firepower 4100/9300 or Secure Firewall 3100/4200 chassis to the Cloud-Delivered Firewall Management Center for centralized management and health monitoring.

You can add a Firepower 4100/9300 chassis to the Cloud-Delivered Firewall Management Center. The management center and the chassis share a separate management connection using the chassis MGMT interface. The Cloud-Delivered Firewall Management Center offers chassis-level health alerts. For configuration, you still need to use the Firewall Chassis Manager or FXOS CLI.

Security Cloud Control does not record the processes on the **Workflow** page when you onboard a chassis or provision a multi-instance Firewall Management CenterFirewall Threat Defense device from the Cloud-Delivered Firewall Management Center chassis manager page.

Note For the Secure Firewall 3100/4200, you need to first convert to multi-instance mode. See Onboard the multi-instance chassis using the CLI.

Procedure

Step 1 Connect to the chassis FXOS CLI, either using the console port or SSH.

Step 2 In the left pane, click **Security Devices**.

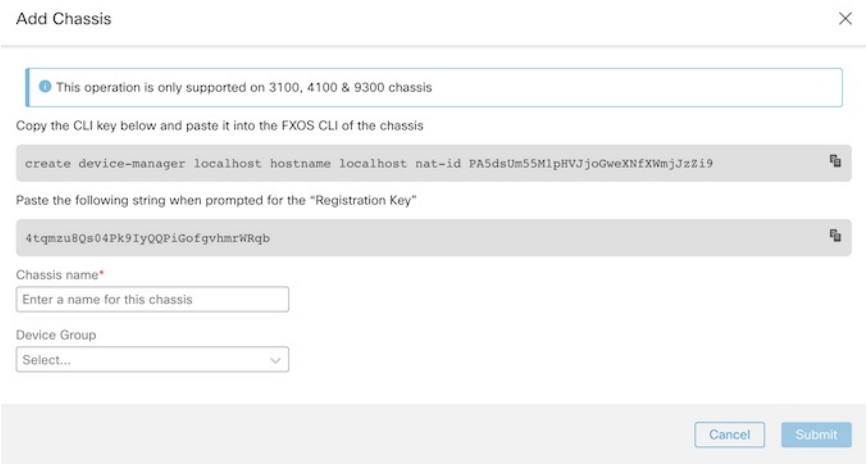
Step 3 Click **Onboard device or service** ( ) icon.

Step 4 Click the **FTD Chassis** tile to open the **Add Chassis** dialog box.

Figure 1: FTD chassis tile



Figure 2: Add chassis



Step 5 Click **Copy** ( ) to copy the top generated command, then paste it at the FXOS CLI of your chassis.

Step 6 When prompted for the Registration Key at the FXOS CLI, click **Copy** ( ) on the **Add Chassis** dialog box for the generated registration key and paste it at the FXOS CLI.

You can disconnect from the FXOS CLI at this point.

Step 7 In the Cloud-Delivered Firewall Management Center **Chassis Name** field, enter a name for the chassis as you want it to display in the Cloud-Delivered Firewall Management Center.

Step 8 (Optional) Add the chassis to a **Device Group**.

Step 9 Click **Submit**.

The chassis is added to the **Device** > **Device Management** page.

The chassis is successfully onboarded and appears on the Device Management page where you can monitor its health and manage its configuration through the Cloud-Delivered Firewall Management Center.

Delete Devices from Cloud-Delivered Firewall Management Center

This task removes devices from Cloud-Delivered Firewall Management Center management by deleting them from the Security Cloud Control dashboard.

Though devices may be registered to Cloud-Delivered Firewall Management Center, Security Cloud Control still manages device enrollment. You must delete the device from the Security Cloud Control dashboard to remove a device from Cloud-Delivered Firewall Management Center.



Note Security Cloud Control does not synchronize the deletion of devices that are associated with an AWS VPC environment. You must delete a device direclty from the AWS VPC UI. See AWS documentation for more information.

Procedure

Step 1 Log into Security Cloud Control and click **Security Devices**.

Step 2 Locate the device you want to delete by using the filters or search bar. Select it so the device row is highlighted. If your device is part of a high availability pair, locate and select the active device.

Step 3 In the Device Actions pane located to the right, click **Remove**.

Step 4 When prompted, select **OK** to confirm the removal of the selected device. Click **Cancel** to keep the device onboarded.

The device is removed from Cloud-Delivered Firewall Management Center and no longer appears in the Security Devices list.

Enable Cloud-Delivered Firewall Management Center

Enable Cloud-Delivered Firewall Management Center to manage your Secure Firewall Threat Defense devices through Security Cloud Control.

If you want to manage your Secure Firewall Threat Defense devices, you can enable the Cloud-Delivered Firewall Management Center on your tenant. You need to have an admin or a super admin user role to perform this task.

Procedure

From the Security Cloud Control menu, click **Administration** > **Integrations** > **Firewall Management Center** and click **Enable Cloud-Delivered FMC**.

Security Cloud Control starts provisioning a Cloud-Delivered Firewall Management Center instance in the background; it typically takes 15 to 30 minutes for this to be complete. You can track the provisioning progress on the **Status** column of **Cloud-Delivered FMC**.

After the provisioning is complete, the status changes to **Active**. In addition, you get a **Cloud-Delivered Firewall Management Center is Ready** notification on the Security Cloud Control notifications panel and on the applications on which you have configured incoming webhooks. See Notification Settings for more information.

Note After you receive the **Cloud-Delivered Firewall Management Center is Ready** notification, ensure that you log out of and log in back to your tenant once, to see the **Cloud-Delivered FMC** right pane options, such as **Actions**, **Management**, and **System**.

What to do next:

a. Register Cloud-Delivered Firewall Management Center with Cisco Smart Software Manager (CSSM) to activate smart license. For detailed steps, refer to Register the Cloud-Delivered Firewall Management Center with the Smart Software Manager.

b. Onboard your Firewall Threat Defense devices to the Cloud-Delivered Firewall Management Center and manage them.

After the provisioning is complete, the status changes to **Active** and you receive readiness notifications. You can then proceed to register with the Smart Software Manager and onboard your devices.

Troubleshooting

Troubleshooting is a diagnostic process that identifies and resolves onboarding issues between Firewall Threat Defense devices and management systems.

Troubleshooting scenarios

Use these scenarios to troubleshoot any onboarding issues.

Troubleshoot Cloud-Delivered Firewall Management Center Connectivity with TCP

This task helps diagnose and resolve connectivity issues between the Cloud-Delivered Firewall Management Center and a Firewall Threat Defense device using TCP port 8305.

Use this procedure to troubleshoot connectivity between the Cloud-Delivered Firewall Management Center and a Firewall Threat Defense device with TCP port 8305.

Procedure

Step 1 Log into Security Cloud Control.

Step 2 Navigate to **Tools & Services** in the left panel and select **Firewall Management Center** to open the **Services** page. Choose **Cloud-Delivered FMC** and locate the Cloud-Delivered Firewall Management Center's FQDN in the top righthand corner.

Step 3 Make sure the Firewall Threat Defense device's state in Security Cloud Control is currently **Onboarding**. Cloud-Delivered Firewall Management Center will not respond if the device is not in an onboarding state. If onboarding has failed, click **Retry Onboarding**.

Step 4 Log into the Firewall Threat Defense device with SSH.

Step 5 Enter into Expert mode with the following command:

```
> expert
admin@devicename:~$
```

Step 6 Execute a TCP handshake:

```
admin@devicename:~$ nc -v xxxxxx.cdo.cisco.com 8305
Connection to xxxxxx.cdo.cisco.com 8305 port [tcp/*] succeeded!
^C (CTRL-C to exit netcat)
admin@devicename:~$.
```

If there is still no response from the Cloud-Delivered Firewall Management Center, then there is a chance that outbound port TCP 8305 may be blocked upstream from your Firewall Threat Defense device and that network path will need to be assured before your Firewall Threat Defense will be able to connect to Cloud-Delivered Firewall Management Center.

You have successfully tested the TCP connectivity between the Cloud-Delivered Firewall Management Center and the Firewall Threat Defense device. If the connection succeeded, the devices can communicate properly on TCP port 8305. If the connection failed, network path issues need to be resolved before the devices can connect.

Troubleshoot Firewall Threat Defense Device Connectivity

Test connectivity to identify potential L1-L3 networking issues or DNS resolution problems that may affect device management operations.

Test connectivity to the Internet from the management-plane of the Firewall Threat Defense device:

Procedure

Step 1 Log into the Firewall Threat Defense device with SSH.

Step 2 Ping one or both of the following:

```
ping system 208.67.222.222
```

```
ping system cisco.com
```

If either of these tests fail, there is likely an L1-L3 issue and you will need to check your management networking configuration (**show network**) and/or a DNS issue.

Successful ping results confirm Internet connectivity from the management-plane. Failed ping tests indicate networking or DNS configuration issues that require further investigation.

Troubleshoot device connectivity loss after Cloud-Delivered Firewall Management Center update

This task helps restore management connectivity between your threat defense device and the Cloud-Delivered Firewall Management Center after the management center receives a new dynamic IP address during an update.

A Cloud-Delivered Firewall Management Center is assigned a dynamic IP address when it is added to a Security Cloud Control tenant. When the management center is updated, the management center receives a new dynamic IP address.

If you have a firewall inspecting the outbound traffic from your threat defense device to the Cloud-Delivered Firewall Management Center, your firewall rules must allow the threat defense traffic to flow to the FQDN and port of the management center rather than its IP address, or the management center will not be able to manage your threat defense device.

Procedure

Step 1 Change your existing IP-based firewall rule to use FQDN-based rules for both required ports.

For example, if your network traffic rule allowing management traffic from your threat defense device to the Cloud-Delivered Firewall Management Center looks like this:

```
allow all traffic <my-threat-defense-IP-src> to 200.165.200.225
```

where 200.165.200.225 is the management address of the Cloud-Delivered Firewall Management Center, change the one allow rule to these two allow rules as both ports 443 and 8305 need to be open:

```
allow all traffic <my-threat-defense-IP-src > to <my-cdfFMC-FQDN>:443
```

```
allow all traffic <my-threat-defense-IP-src > to <my-cdfFMC-FQDN>:8305
```

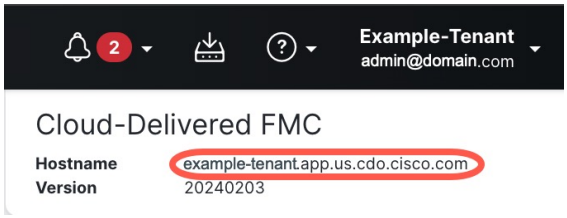
See "Network Requirements" in Prerequisites to Onboard a Device to Cloud-delivered Firewall Management Center for more port information.

Step 2 Find the domain name of your Cloud-Delivered Firewall Management Center.

a) Log in to Security Cloud Control.
b) In the left pane, click **Administration** > **Integrations** > **Firewall Management Center**
c) Select **Cloud-Delivered FMC** in the FMC table.

In the top-right corner of the screen, you will see the Hostname of the management center. This is the FQDN.

Figure 3: Cloud-delivered FMC FQDN



Your threat defense device can now maintain management connectivity with the Cloud-Delivered Firewall Management Center using FQDN-based firewall rules, even when the management center's IP address changes during updates.

Troubleshoot Onboarding a Device to the Cloud-Delivered Firewall Management Center Using the CLI Registration Key

Error: device remains in pending setup state after onboarding

This task resolves device registration failures that occur when the configuration manager command is not executed within 3 minutes after onboarding.

When a device fails to register, the device's connectivity status is displayed as **Pending Setup**. In the panel located to the right, Security Cloud Control displays a **Registration Failed** message as well as a **Retry Onboarding** button to immediately allow you to reattempt onboarding the device.

If you fail to execute the `configuration manager` command in the device CLI within 3 mins after onboarding it to Security Cloud Control, the device's registration attempt expires and results in a registrationg failure.

Procedure

Step 1 Log into Security Cloud Control and navigate to the **Security Devices** page. Locate the device that failed to register.

Step 2 In the panel located to the right, locate the **Registration Failed** window. Beside the device's CLI registration key, click **Copy**. This actions copies the CLI key to a local clipboard.

Step 3 Open an SSH connection to the device and log in as `admin`.

Step 4 Paste the CLI registration key into the device's CLI interface. In the CLI, enter **Y** to complete the registration. If your device was previously managed by Firewall Device Manager, enter **Yes** to confirm the submission.

The device registration completes successfully and the device status changes from Pending Setup to an active connectivity status.

Troubleshoot Onboarding a Device to Cloud-Delivered Firewall Management Center Using the Serial Number

Device is offline or unreachable

If the device is unreachable during the onboarding process, or at any point post-onboarding, Security Cloud Control displays an **Unreachable** connectivity status. The device will not be able to fully onboard to Security Cloud Control until the device is able to connect.

These scenarios might be the cause:

- The device is cabled incorrectly.
- Your network may require a static IP address for the device.
- Your network uses custom DNS, or there is external DNS blocking the network.
- If your device is associated with the European region (https://defenseorchestrator.eu/), you may need to enable PPPoE authentication.For other domains, review the domain requirements.
- The device may be blocked by a firewall, or is incorrectly blocking a port for connectivity. Review the device #unique_22 unique_22_Connect_42_cdfmc_network and confirm the correct outgoing ports are enabled.

Error: Serial Number Already Claimed

The Device was Purchased From an External Vendor

If the device was purchased from an external vendor and fails to onboard with a **Serial Number Already Claimed** error, it's possible the device is still associated to the vendor's tenant. Use the following steps to claim the device and its serial number:

1. Delete the device from your Security Cloud Control tenant.
2. Install the FXOS image on the device. For more information, see the "Reimage Procedures" chapter of the Cisco FXOS Troubleshooting Guide for the Firepower 1000/21000 and Secure Firewall 3100 Firepower Threat Defense guide.
3. Connect a laptop to the device's console port.
4. Connect to the FXOS CLI and log in as **admin**.
5. In the FXOS CLI, connect to **local-mgmt** with the `firepower # connect local-mgmt` command.
6. Execute the `firepower(local-mgmt) # cloud deregister` command to deregister the device from the cloud tenancy.
7. Once the device is successfully unregistered, the CLI interface returns a success message. An example of the message:

```
Example: firepower(local-mgmt) # cloud deregister Release Image Detected RESULT=success
 MESSAGE=SUCCESS 10, X-Flow-Id: 2b3c9e8b-76c3-4764-91e4-cfd9828e73f9
```

Note If the device was never registered to another Security Cloud Control tenant, the message above states `RESULT=success MESSAGE=DEVICE_NOT_FOUND.`

8. Onboard the device to your Security Cloud Control tenant with its serial number. See Onboard a Firewall Threat Defense Device to Cloud-Delivered Firewall Management Center using Zero-Touch Provisioning, on page 6 for more information.

The Device is Claimed By a Security Cloud Control Tenant in Another Region

The device may have been previously managed by another Security Cloud Control instance in a different region and is still registered to that tenant.

If you **do** have access to the tenant the device is currently registered to, use the following procedure:

1. Delete the device from the incorrect Security Cloud Control tenant.
2. Log into the device's Firewall Device Manager UI.
3. Navigate to **System Settings** > **Cloud Services**.
4. Click **Cloud Services** and select **Unregister Cloud Services** from the drop-down list.
5. Confirm the action and click **Unregister**. This action generates a warning to indicate that the device has been removed from Security Cloud Control. This is expected behavior.
6. Log into Security Cloud Control tenant in the correct region and onboard the device. See Onboard a Firewall Threat Defense Device to Cloud-Delivered Firewall Management Center using Zero-Touch Provisioning, on page 6 for more information.
7. Navigate to **System Settings** > **Cloud Services**.
8. Click **Cloud Services** and select **Unregister Cloud Services** from the drop-down list.
9. Select the **Auto-enroll with Tenancy from Security Cloud Control** and click **Register**. The device maps to the new tenant that belongs to the new region and Security Cloud Control onboards the device.

If you **do not** have access to the tenant, use the procedure below:

1. Connect to the FXOS CLI from the console port and log in as **admin**. For information on how to log into the FXOS CLI, see Accessing the FXOS CLI.
2. In the FXOS CLI, connect to **local-mgmt** with the `firepower # connect local-mgmt` command.
3. Execute the `firepower(local-mgmt) # cloud deregister` command to deregister the device from the cloud tenancy.
4. Once the device is successfully unregistered, the CLI interface returns a success message. An example of the message:

```
Example: firepower(local-mgmt) # cloud deregister Release Image Detected RESULT=success
 MESSAGE=SUCCESS 10, X-Flow-Id: 2b3c9e8b-76c3-4764-91e4-cfd9828e73f9
```

Note If the device was never registered to another Security Cloud Control tenant, the message above states `RESULT=success MESSAGE=DEVICE_NOT_FOUND`.

5. In your Security Cloud Control tenant in the correct domain, onboard the device. See Onboard a Firewall Threat Defense Device to Cloud-Delivered Firewall Management Center using Zero-Touch Provisioning, on page 6 for more information.
6. In the device's Firewall Device Manager UI, navigate to **System Settings** > **Cloud Services**.
7. Select the **Auto-enroll with Tenancy from Security Cloud Control** and click **Register**. The device maps to the new tenant that belongs to the new region and Security Cloud Control onboards the device.

Resolve claim error

Resolve claim errors that result from entering incorrect serial numbers during device onboarding.

If you enter the wrong serial number when onboarding a device, Security Cloud Control generates a **Claim Error** status.

Note Confirm that the device is claimed in the correct region within Security Cloud Control.

Follow these steps to resolve claim error issues:

Procedure

Step 1 Log into Security Cloud Control and navigate to the **Security Devices** page. Locate the device with the error.

Step 2 Select the device so it is highlighted and **Remove** the device from Security Cloud Control.

Step 3 Confirm the following:

- The device is online and can reach the internet.
- The device has not already been onboarded to your Security Cloud Control instance or claimed by a Security Cloud Control tenant in another region.

Step 4 Locate the device's serial number. You can use one of the following methods:

- For the 1000, 2100 and 3100 series model, locate the serial number on the physical device.
- Open an SSH connection to the device and issue the **show serial-number** command.

Step 5 In Security Cloud Control, onboard the device with the correct serial number. See Onboard a Firewall Threat Defense Device to Cloud-Delivered Firewall Management Center using Zero-Touch Provisioning, on page 6 for more information.

The device is successfully onboarded with the correct serial number and the claim error is resolved.

Error: failed to claim

This task helps resolve device onboarding failures when you see an **Error: Failed to Claim** connectivity status or error message after attempting to onboard a device.

If you see an **Error: Failed to Claim** connectivity status or error message after attempting to onboard a device, the following might be the cause:

- The Security Services Exchange platform may have temporary issues that result in no connectivity.
- The Security Cloud Control server may be down.

Follow these steps to resolve this issue:

Procedure

Step 1 Log into Security Cloud Control and navigate to the **Security Devices** page. Locate the device that failed to register.

Step 2 Select the device so it is highlighted and **Remove** the device from your Security Cloud Control tenant.

Step 3 Wait at least 10 minutes before attempting to onboard the device back to your Security Cloud Control tenant. See Onboard a Firewall Threat Defense Device to Cloud-Delivered Firewall Management Center using Zero-Touch Provisioning, on page 6 for more information.

If you are still unable to claim the device, review the device's workflow to see is there is an error message. If there is,Export the Workflow and open a support case to further troubleshoot the issue.

The device should successfully onboard to your Security Cloud Control tenant without the claim failure error.

Resolve provisional error for device onboarding

Resolve UnProvisioned connectivity status that occurs when onboarding devices to Security Cloud Control due to password configuration mismatches or other provisional errors.

Devices can generate an UnProvisioned connectivity status during onboarding for various reasons, including password configuration mismatches between the device state and the onboarding wizard selections. This task provides multiple resolution approaches based on different scenarios.

Procedure

Step 1 Determine which scenario applies to your device.

Table 2: Device password configuration scenarios

If...	Then...
You did not change the default password and selected **No, this device has been logged into and configured for a manager** during onboarding	Proceed to step 2 to change the device password

If...	Then...
You did change the default password and selected **Is this a new device that has never been logged into or configured before?** during onboarding	Proceed to step 3 to confirm and proceed with onboarding
Neither scenario applies or the issue persists	Proceed to step 4 to try alternative resolution methods

Step 2 If the device password has not been changed, change the device password.

a. Log into Security Cloud Control and navigate to the **Security Devices** page.

b. Locate and select the device with the **UnProvisioned** connectivity status so it is highlighted.

c. In the pane located to the right, locate the **Change Password** window.

d. Click **Change Password** and enter a new password for your device. This overwrites the default password.

It may take a few minutes for the device to onboard and fully synchronize to Security Cloud Control.

Step 3 If the device password has already been changed, confirm and proceed with onboarding.

a. Log into Security Cloud Control and navigate to the **Security Devices** page.

b. Locate and select the device with the **UnProvisioned** connectivity status so it is highlighted.

c. In the pane located to the right, locate the **Confirm and Proceed** window.

d. Click **Confirm and Proceed**. This action ignores the password that was provided in the onboarding wizard and reinstates the default password for the device. Security Cloud Control then continues to onboard the device.

Step 4 If other provisional error scenarios occur, try alternative resolution methods.

If you confirm the password selection in the onboarding wizard is accurate for the state of the device, consider these options:

- Select the device so it is highlighted. In the window located on the right pane of the screen, click **Retry** to force Security Cloud Control to re-onboard the device with existing provisional parameters.
- Delete the device from the **Security Devices** page and attempt to re-onboard the device.
- In the device's Firewall Device Manager UI, navigate to **System Settings** > **Cloud Services**. Select the **Auto-enroll with Tenancy from** Security Cloud Control and click **Register**.

If you are still unable to claim the device, review the device's workflow to see is there is an error message. If there is, Export the Workflow and open a support case to further troubleshoot the issue.

The device successfully onboards to Security Cloud Control and displays a normal connectivity status instead of UnProvisioned.