

Deploy an FTDv Gateway in AWS Using MCD

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Background Information](#)

[Configure](#)

[Enable Cisco Multicloud Defense on the SCC Tenant](#)

[Onboard an AWS Account \(CSP Account\)](#)

[Create a Service VPC](#)

[Start the FTDv Gateway Wizard](#)

[Configure Gateway Properties](#)

[Configure Advanced Settings \(Optional\)](#)

[Review and Deploy](#)

[Verify](#)

[Troubleshoot](#)

[Summary](#)

[Related Information](#)

Introduction

This document describes how to onboard your AWS account to Cisco Multicloud Defense (MCD) and deploy FTDv gateways by using the Cisco MCD controller.

Prerequisites

- A cloud-delivered Firewall Management Center (cdFMC) provisioned for the SCC tenant.
- An AWS EC2 Key Pair available in the region targeted for deployment.
- An AWS account with sufficient IAM permissions to deploy a CloudFormation stack.
- An active Cisco Multicloud Defense subscription/entitlement on the SCC tenant, along with the applicable FTDv license types and performance tier entitlements.
- SCC administrative access with rights to manage Platform Subscriptions and Multicloud Defense infrastructure.
- AWS Console access with permissions to create and monitor CloudFormation stacks and EC2 resources.

Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco Security Cloud Control (SCC) navigation
- Basic AWS networking concepts (VPC, CIDR, Transit Gateway, Availability Zones)
- AWS CloudFormation stack deployment and review

Components Used

- Cisco Security Cloud Control (SCC)
- Cisco Multicloud Defense (MCD)
- Cisco Secure Firewall Threat Defense Virtual (FTDv)
- Cloud-delivered Firewall Management Center (cdFMC)
- Amazon Web Services (AWS) – CloudFormation, EC2, VPC, Transit Gateway

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

This document covers a first-time MCD deployment into a single AWS account and region using a Transit Gateway (TGW) network type. AWS Cloud WAN network types and ingress gateway deployments are outside the scope of this document, as ingress gateways are not currently supported by MCD.



Note: Ingress gateways are not currently supported by Multicloud Defense. Only Egress/East-West gateway deployments are covered in this document.

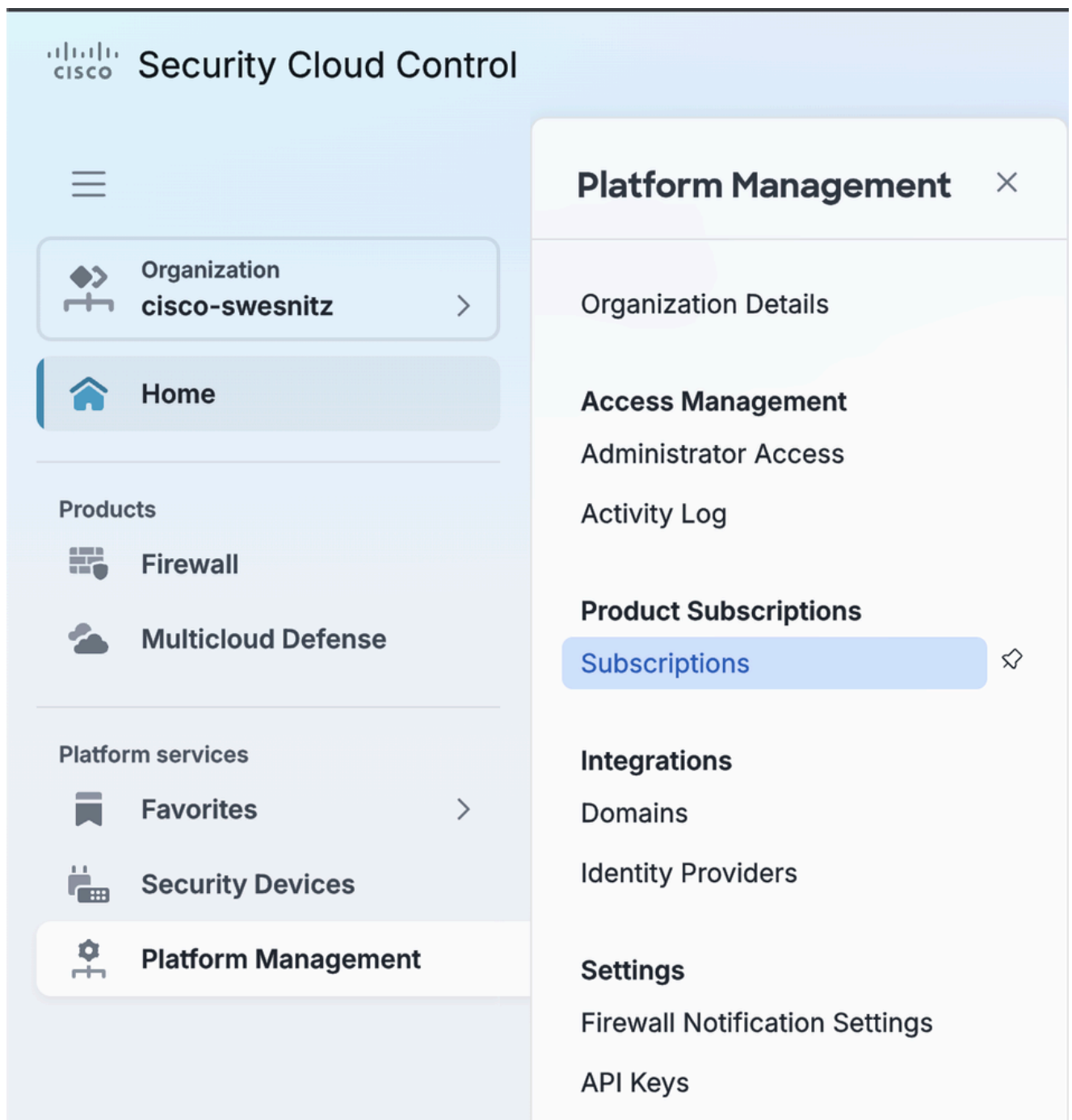


Note: If the initial cdFMC registration attempt fails or times out, this is expected behavior. Allow additional time for the cluster to retry registration automatically before troubleshooting further.

Configure

Enable Cisco Multicloud Defense on the SCC Tenant

1. In the **Cisco Security Cloud Control (SCC)** console, navigate to **Home > Platform Management > Subscriptions**.



2. Enable the **Multicloud Defense** subscription for the tenant.

Services 4 available 3 enabled

^ Some services come enabled as core capabilities on the SCC platform, while additional services are available to be enabled as needed.

Service Name	Region	Status
Cisco Multicloud Defense	United States	✓ Enabled
Cisco Security Services Exchange	North America	✓ Enabled
Cisco Mesh Policy Engine	—	<button>Enable</button>
Cisco Security Cloud Control Firewall Management	North America	✓ Enabled

Onboard an AWS Account (CSP Account)

This step connects an AWS account to the Multicloud Defense Controller so MCD can deploy and manage resources on its behalf. This example uses AWS as the Cloud Service Provider (CSP).

1. From the **SCC left navigation** pane, select **Multicloud Defense**.



Security Cloud Control



Organization
cisco-swesnitz



Home

Products



Firewall



Multicloud Defense

Platform services



Favorites



Security Devices



Platform Management



Security Cloud Control



Infrastructure



. This opens a new browser tab and launches an AWS CloudFormation stack that deploys the

IAM roles and resources required for MCD to integrate with the AWS account.

6. In the **AWS Console**, confirm the CloudFormation stack completes successfully.



Stacks (6)				Filter status	View nested
Search by stack name				Active	☒
Stack name	Status	Created time	Description		
cisco-mcd-resources	CREATE_COMPLETE	2026-07-21 13:08:44 UTC-0400	Create 3 IAM Roles mcd-gateway-role that is assigned to Multicloud Defense gateway instances. mcd-controller-role is a cross account IAM role used by the Multicloud Defense Controller to manage the customer's AWS account (create gateway instances etc). mcd-inventory-role that enables posting of CloudTrail updates to the Multicloud Defense Controller. Create S3 bucket and enable CloudTrail to go this bucket. Enable Event notification on the S3 bucket to notify the Multicloud Defense Controller		

7. Open the **Outputs** tab of the CloudFormation stack. These values are required in the next step. ■

8. In the MCD **Add Account** form, enter these values:

AWS Account Number: The AccountNumber output from the CloudFormation stack.

AWS Account Name: A friendly, identifiable name for this AWS account within MCD.

Controller IAM Role: The MCDControllerRoleArn output from the CloudFormation stack.

Inventory Monitor Role: The MCDInventoryRoleArn output from the CloudFormation stack.

AWS Account Number * ⓘ

AWS Account Name * ⓘ

Description ⓘ

Description (optional)

External ID ⓘ

Regenerate

Edit ⓘ

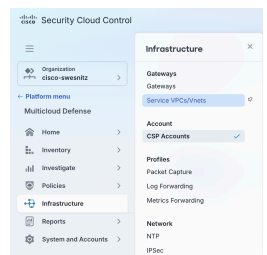
Controller IAM Role * ⓘ

Inventory Monitor Role * ⓘ

9. Save the **account**. The AWS account is onboarded to MCD.

Create a Service VPC

The Service VPC hosts the networking infrastructure (subnets, route tables, Transit Gateway) used by the FTDv gateway.



1. Navigate to **Multicloud Defense > Infrastructure > Service VPCs/VNets**.

A screenshot of the 'Service VPCs/VNets' configuration page. The page has a light blue header with the title 'Service VPCs/VNets'. Below the header, there are two tabs: 'Quick Filters' (selected) and 'Advanced'. Under the 'Quick Filters' tab, there is a search bar labeled 'Name' with a dropdown arrow. At the bottom of the page, there are two buttons: 'Create' (a solid blue button) and 'Actions' (a button with a dropdown arrow).

2. Select **Create**.
3. Configure the VPC settings:
 - Name:** A unique, easily identifiable name for the VPC.
 - CSP Account:** The AWS account integrated in Step 2.
 - Region:** The AWS region where the FTDv cluster is launched.
 - CIDR Block:** A CIDR range dedicated to this MCD deployment (must not overlap with existing VPCs).
 - Availability Zones:** At least one AZ; two are recommended for redundancy.
 - Network Type:** Select **Transit Gateway (TGW)**. CloudWAN is a separate network type used specifically for AWS Cloud WAN deployments and is out of scope for this document.
 - Transit Gateway:** Select **create_new**, with a unique name for the new Transit Gateway.
 - NAT Gateway** (optional): Enables all egress traffic to route through a NAT Gateway. Not enabled in this example; NAT Gateway configuration is out of scope for this document.

Create Service VPC

Name * ⓘ

mcd_test_vpc-swesnitz

CSP Account * ⓘ

AWS-CXLABS-RTP-FW

Region * ⓘ

US East (Ohio) us-east-2

CIDR Block * ⓘ

10.4.0.0/16

Availability Zones * ⓘ



us-east-2b



us-east-2c



us-east-2a

Network Type *

TGW

Transit Gateway * ⓘ

create_new

Transit Gateway Name * ⓘ

mcd_test_vpc-swesnitz-tgw



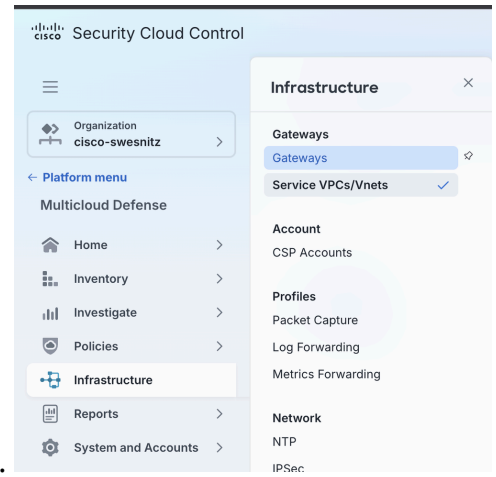
Auto accept shared attachments ⓘ



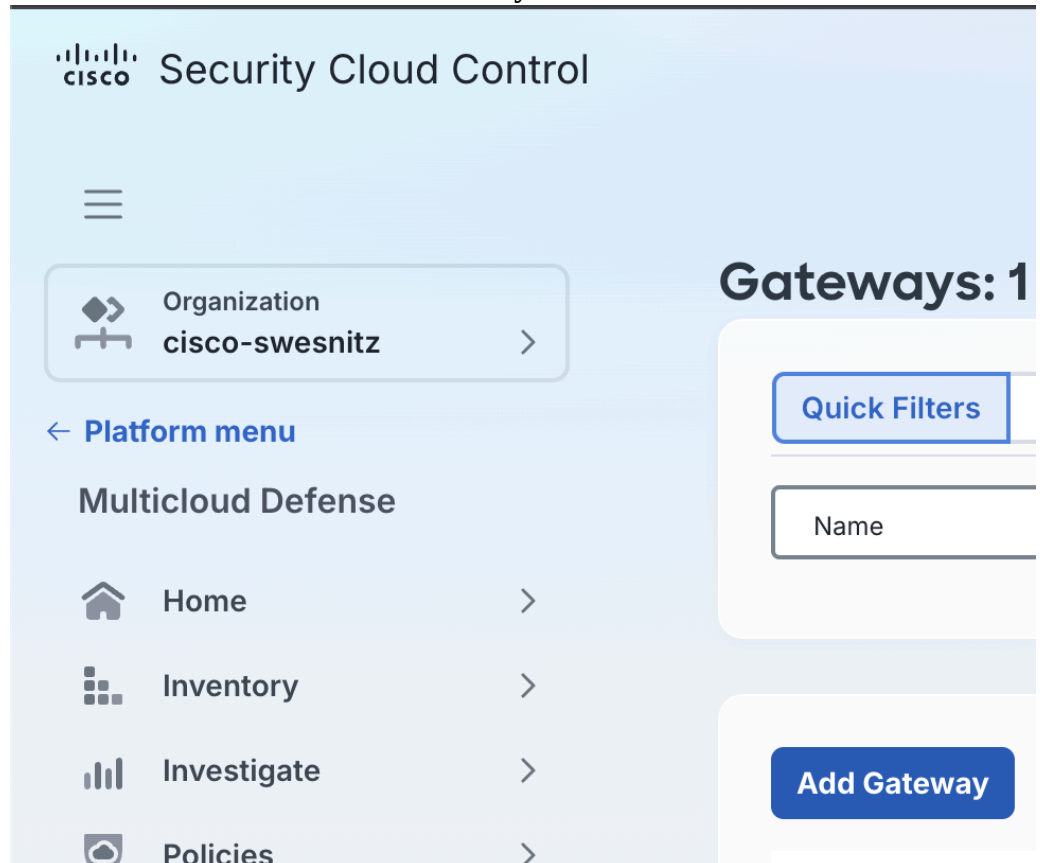
Use NAT Gateway ⓘ

4. Select **Save**.

Start the FTDv Gateway Wizard



1. Navigate to **Multicloud Defense > Infrastructure > Gateways**.



2. Select **Add Gateway**.
3. Configure the initial settings:
 - Accounts:** The CSP account integrated in Step 2.
 - Gateway Type:** Select **FTDv Gateway**.
 - Name:** The display name for this cluster in MCD.
 - Instance Type:** The instance size matching the required throughput and performance needs. This example uses the minimum supported type, C5_XLARGE.
 - Minimum/Maximum Instances:** The desired scaling range. Minimum is 1 instance; maximum is 10.
 - HealthCheck Port:** Default is 65534; change only if a different port has been specified for the MCD load balancer. If changed, the port must be allowed in any datapath security groups associated with the FTDv instances.

Create Gateway

Gateway Information

Gateway Details

Advanced Settings

Review

Properties

Accounts * ⓘ
AWS-CXLABS-RTP-FW

Gateway Type *
FTDv Gateway

Name * ⓘ
mcd-lab-cluster

Description
Optional

Instance Type * ⓘ
4 Virtual CPU | AWS_C5_XLARGE

Minimum Instances * ⓘ
1

Maximum Instances * ⓘ
3

HealthCheck Port * ⓘ
65534

Cancel

Next

4. Select **Next**.

Configure Gateway Properties

Properties: Select **Egress/East-West**. Ingress gateways are not currently supported.

FTDv Version: The software version best suited to the environment.

Policy Ruleset: The access control policy (ACP) to apply to this FTDv cluster.

Password: A password for the FTDv instances.

License Model: The desired licensing model.

Performance Tier: The tier appropriate for the expected device throughput.

License Types: The license types purchased for this deployment.

Region: The region where these FTDv instances are deployed.

VPC/VNet ID: The Service VPC created in Step 3.

Key Pair: An existing AWS Key Pair.

Gateway IAM Role: The role containing gateway in its name, corresponding to the MCDFirewallRoleName value from the CloudFormation stack in Step 2. Selecting this role automatically populates the associated Security Groups.

EBS Encryption: AWS-managed encryption is selected by default. Amazon EBS automatically and transparently encrypts block storage volumes, data in transit, and snapshots.

1. Select Next.

Create Gateway

1

2

3

Gateway InformationGateway DetailsAdvanced Settings

Properties

Security ⓘ

Egress X East West X

FTDv Version *

10.0.0

Policy Ruleset ⓘ

Default Access Control Policy X

FTDv

Admin Password

..... Show

License Model ⓘ

Smart Licensing Multicloud Defense Pay As You Go

Performance Tier ⓘ

FTDv30

License Types ⓘ

Base X

Location

Region *

US East (Ohio) us-east-2

VPC/VNet ⓘ

vpc-0cebc0628f15f7f76 | mcd_test_vpc-swesnitz

Key Pair ⓘ

swesnitz_keypair

Gateway IAM Role ⓘ

ciscomcd-swesnitz-gateway-role

Mgmt. Security Group ⓘ

Password Requirements:

- Must be between 12 and 72 characters long
- Use lowercase and uppercase characters, and numbers
- At least one special character (excluding \ and -)
- No more than 2 repeating or sequential characters

Mgmt. Security Group * ⓘ

sg-03931c93a84997b5d | mcd_test_vpc-swesni... ⓘ ↻

Datapath Security Group 1 * ⓘ

sg-0f5f5b6c316f00167 | mcd_test_vpc-swesnitz... ⓘ ↻

Datapath Security Group 2 * ⓘ

sg-0e6c2dd50947c2c80 | mcd_test_vpc-swesni... ⓘ ↻

EBS Encryption * ⓘ

AWS managed encryption ▼

Instance Details

You can only modify availability zones for gateways deployed in edge mode for GCP, Azure, and OCI environments

Availability Zone ⓘ	Mgmt. Subnet ⓘ	Datapath Subnet 1	Datapath Subnet 2
us-east-2a ⓘ ▼	subnet-0da851c36011e1f35 ... ⓘ ▼	subnet-07abbe3e632e4bb6 ... ⓘ ▼	subnet-04cb07e100352efce ... ⓘ ▼
us-east-2b ⓘ ▼	subnet-0ca2534481246f7c7 ... ⓘ ▼	subnet-08ff302671bc4af9b ... ⓘ ▼	subnet-0254dc31950566c37 ... ⓘ ▼

Cancel

Configure Advanced Settings (Optional)

Advanced Settings allow configuration of options such as disabling public IP addresses for the FTDv instances. Advanced settings are not configured in this example.

Review and Deploy

1. Review all **configured settings** for accuracy.

Create Gateway

Gateway Information Gateway Details Advanced Settings Review

Gateway Information ⓘ Edit

Name mcd-lab-cluster

Gateway Type FTDv Gateway

Min Instances 1

Max Instances 3

HealthCheckPort 65534

Policy Ruleset ID Default Access Control Policy

Property Egress, East West

Instance Type AWS_C5_XLARGE

FTDv Version 10.0.0

Gateway Details ⓘ Edit

License Model Smart Licensing

Performance Tier FTDv30

License Type Base

Region us-east-2

VPC/VNet ID vpc-0c6bc0628f15f7776 | mcd_test_vpc-swesnitz

Key Pair swesnitz_keypair

IAM Role for Firewall arn:aws:iam::421931305595:role/ciscomcd-swesnitz-gateway-role

Mgmt. Security Group sg-03931c93a84997b5d

Datapath Security Group 1 sg-0f5f5b6c316f00167

Datapath Security Group 2 sg-0e6c2dd50947c2c80

EBS Encryption AWS EBS encryption key

Instance Details

Availability Zone	Mgmt. Subnet	Datapath Subnet 1	Datapath Subnet 2
us-east-2a	subnet-0da851c36011e1f35	subnet-07abbe3e632e4bb6	subnet-04cb07e100352efce
us-east-2b	subnet-0ca2534481246f7c7	subnet-08ff302671bc4af9b	subnet-0254dc31950566c37

Resources Info ⓘ

Cancel Back Finish

2. Select **Finish** to begin deployment.



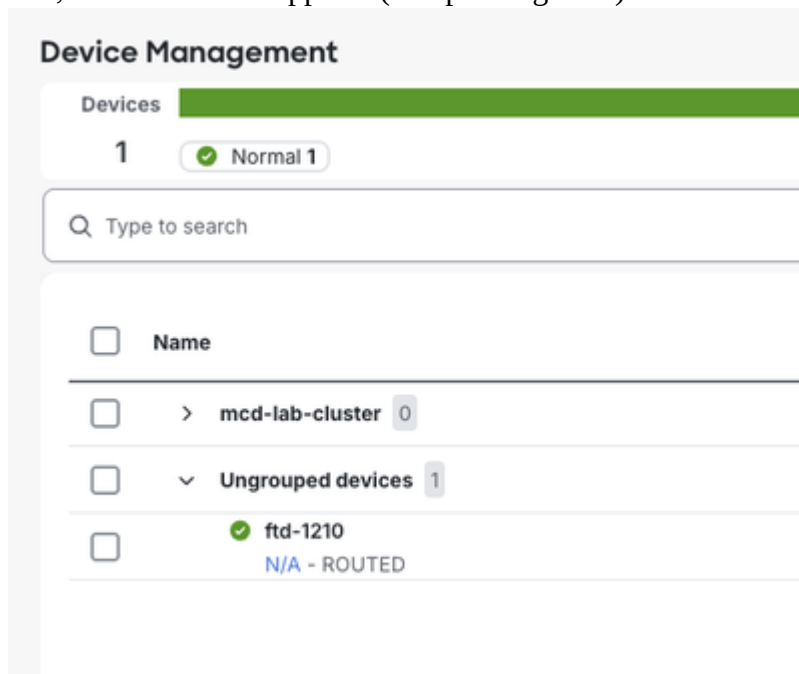
Note: Deployment can take up to 30 minutes. During this time, MCD provisions and clusters the specified number of FTDv instances and registers them with cdFMC.

Verify

Use this section in order to confirm that your configuration works properly.

Deployment and registration success can be confirmed from several locations:

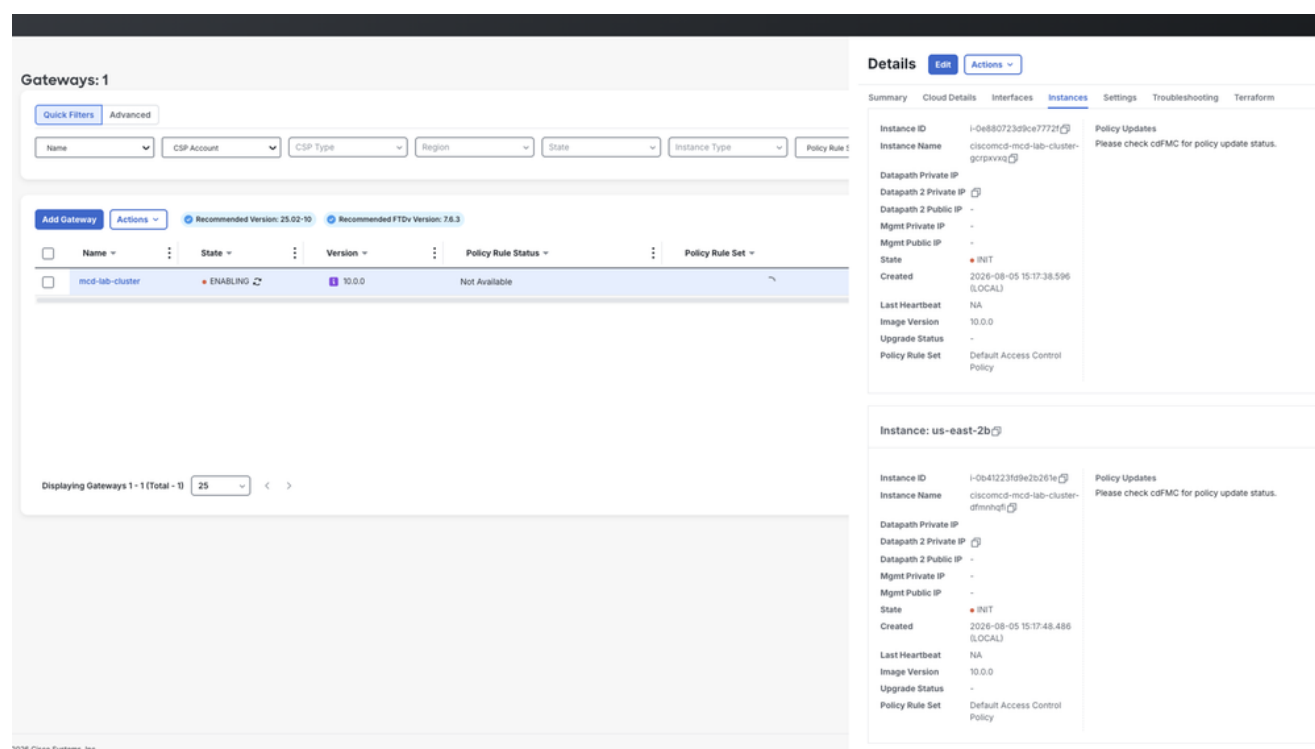
- **cdFMC:** Immediately after selecting Finish, the new cluster appears (in a pending state) in cdFMC



under **Devices > Device Management**.

- **MCD Gateway Details:** Selecting the gateway name opens a details panel showing launch progress.

Select the specified **name** then click the **Instances** tab.



- **AWS EC2 Console:** Individual instance status can be monitored directly in **EC2 > Instances**.

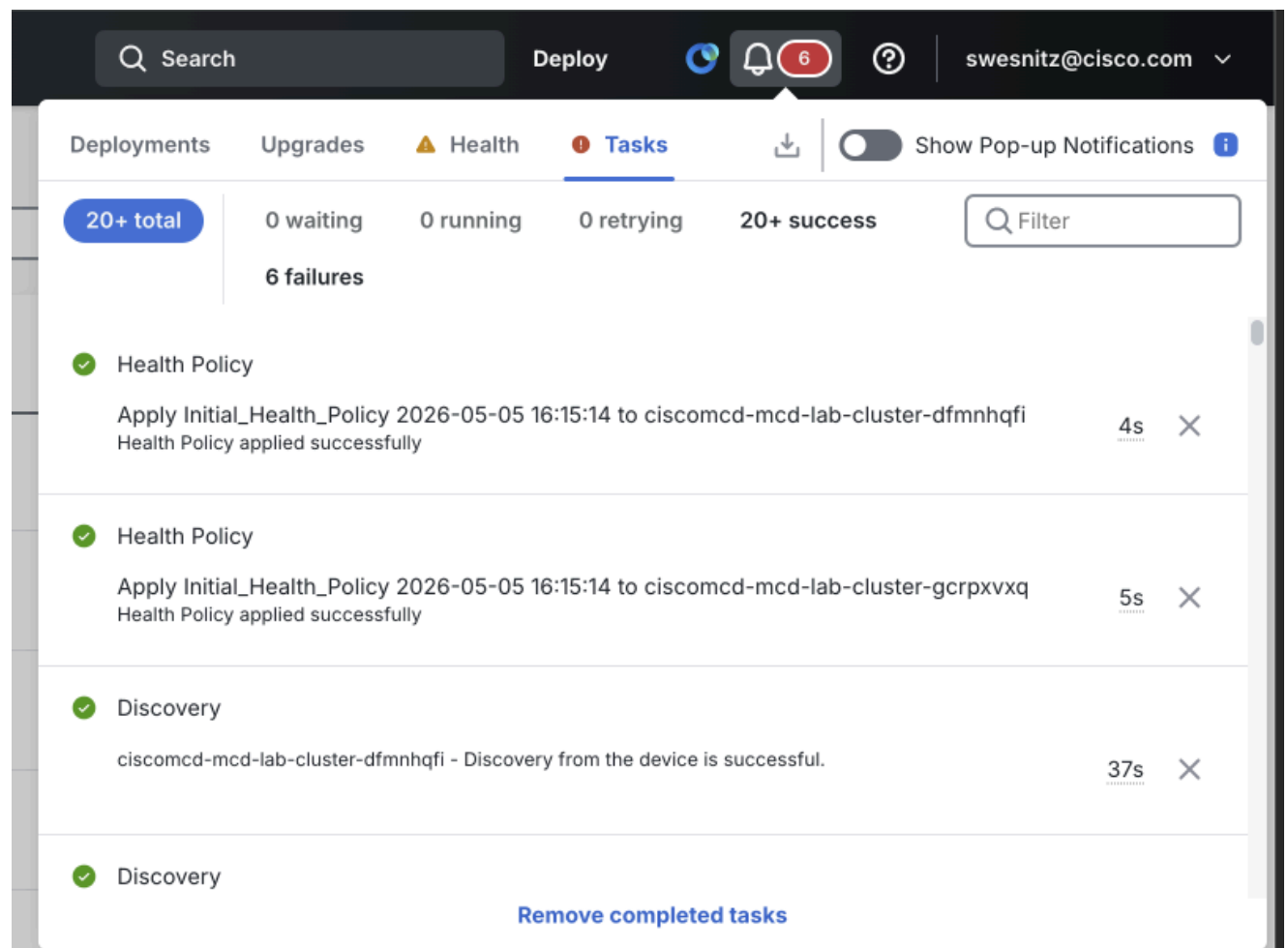


- **cdFMC Tasks Tab:** Registration progress is tracked here:

Registration continuing:

 Register Registration ciscomcd-mcd-lab-cluster-dfmnhqfi: Established secure connection	2m 52s
 Register Registration ciscomcd-mcd-lab-cluster-gcrpxvxq: Established secure connection	47s

Registration success:



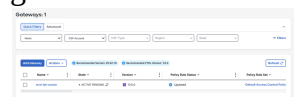
The screenshot shows the Cisco FMC interface with the **Tasks** tab selected. The top navigation bar includes a search bar, a **Deploy** button, a notification bell with a red badge showing '6', and a user profile for **swesnitz@cisco.com**. The **Tasks** tab is active, displaying a summary of task status: **20+ total**, **0 waiting**, **0 running**, **0 retrying**, **20+ success**, and **6 failures**. A **Filter** input field is available. The task list shows three successful tasks:

- Health Policy**: Apply Initial_Health_Policy 2026-05-05 16:15:14 to ciscomcd-mcd-lab-cluster-dfmnhqfi. Health Policy applied successfully. Duration: 4s.
- Health Policy**: Apply Initial_Health_Policy 2026-05-05 16:15:14 to ciscomcd-mcd-lab-cluster-gcrpxvxq. Health Policy applied successfully. Duration: 5s.
- Discovery**: ciscomcd-mcd-lab-cluster-dfmnhqfi - Discovery from the device is successful. Duration: 37s.

A link to **Remove completed tasks** is visible at the bottom of the task list.

- **Final State:** After successful registration, the gateway shows an Active - Pending status before

transitioning to fully **Active**, confirming the cluster is deployed and operational.



Troubleshoot

This section provides information you can use in order to troubleshoot your configuration.

- **Initial registration attempt fails or times out in the cdFMC Tasks tab** – Expected behavior on the first registration attempt. Allow additional time for the cluster to retry registration automatically before further troubleshooting.
- **CloudFormation stack fails to complete** – Verify the AWS IAM user/role deploying the stack has sufficient permissions, and review the **Events** tab for the specific failure reason.
- **Gateway IAM Role or Security Groups do not populate in the Gateway wizard** – Confirm the CloudFormation stack in Step 2 completed successfully and that the correct CSP Account and Region were selected.

Summary

Completing this procedure results in:

- Multicloud Defense enabled on the SCC tenant.
- AWS account onboarded via CloudFormation.
- Service VPC created with a Transit Gateway.
- Clustered FTDv gateway deployed and registered to cdFMC.

The FTDv gateway is active and ready for policy configuration and traffic inspection.

Related Information

- [Firewall Threat Defense Virtual](#)
- [Connect AWS Account to Multicloud Defense Controller from the Multicloud Defense Dashboard](#)
- [Create a Service VPC or VNet](#)
- [Create an FTDv Gateway](#)
- [Technical Support & Documentation - Cisco Systems](#)