

Deploy an FTDv Gateway in Azure Using MCD

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Configure](#)

[Register an Application](#)

[Create a Custom Role](#)

[Assign the Custom Role](#)

[Connect the Azure Account to MCD](#)

[Create a VNet](#)

[Create the Azure MCD FTDv Gateway](#)

[Verify](#)

[Related Information](#)

Introduction

This document describes how to configure the Microsoft Azure prerequisites and deploy a Firewall Threat Defense Virtual (FTDv) Gateway through MCD.

Prerequisites

- An Azure subscription that is acquired and registered, and associated with Microsoft Entra ID. Confirm this in the list of **App Registrations** in the Azure portal.
- A custom role created for the Azure subscription that grants Multicloud Defense (MCD) access to the specific resources and actions that are otherwise blocked.
- A subscription to the Azure Event Grid, so that MCD can receive real-time updates from the Azure subscription.
- The Azure subscription connected to the Multicloud Defense Controller from the MCD dashboard.
- The Cisco Marketplace Terms accepted in Azure, if this is the first time that the Azure account is onboarded to MCD.
- (Optional) A user-assigned managed identity configured, if you require Key Vault or Blob Storage access.
- A new Service VNet. VNets that were created before FTDv gateway support was introduced cannot be used for an FTDv gateway deployment.
- An active subscription to Cloud-Delivered Firewall Management Center (cdFMC), which manages the access control policy for the FTDv device.
- At least one FTDv license purchased through your Cisco seller or partner.

Requirements

Cisco recommends that you have knowledge of these topics:

- Navigation of the Microsoft Azure portal
- Microsoft Entra ID (Azure AD) application registration and role-based access control (RBAC)
- Cisco Multicloud Defense (MCD)
- Cisco Secure Firewall Threat Defense Virtual (FTDv)

Components Used

This document is not restricted to specific software and hardware versions.

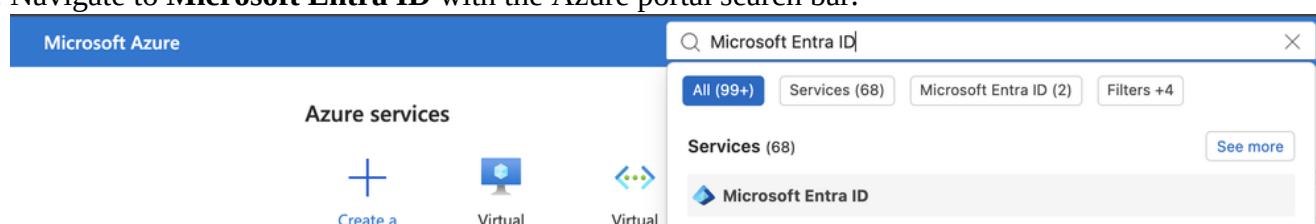
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Configure

Use these procedures in order to prepare Microsoft Azure, connect your Azure account to MCD, and deploy an FTDv Gateway.

Register an Application

1. Navigate to **Microsoft Entra ID** with the Azure portal search bar.



2. Click **Add**, then select **App registration**.

Home

cxsecurity | Overview ...

Overview

 Preview features

 Diagnose and solve problems

> Manage

> Monitoring

> Troubleshooting + Support

+ Add ▾



Manage tenants



What's new

User >

Group

Enterprise application

App registration

[App, integrated experier](#)

Properties

Recom

Basic information

Name cxsecurity

Tenant ID af42bac0-52aa-429f-92

Primary domain cxsecurity.onmicrosoft.

3. On the **Register an application** form, enter these values:

- **Name:** An easily identifiable name for the application.
- **Supported account types:** Select the option that best suits your environment. This document uses Single tenant only.

Home > cxsecurity | Overview

Register an application ...

* Name

The user-facing display name for this application (this can be changed later).

Multicloud Defense Controller ✓

Supported account types

Choose the account types that can use this application or access this API

Single tenant only - cxsecurity ▾

Single tenant only - cxsecurity

Multiple Entra ID tenants

Any Entra ID Tenant + Personal Microsoft accounts

Personal accounts only

Communicating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

[Help me choose](#)

Select a platform ▾

e.g. <https://example.com/auth>

Register an app you're working on here. Integrate gallery apps and other apps from outside your organization by adding from [Enterprise applications](#).

4. For **Redirect URI (optional)**, choose the **option** appropriate for your environment. This document does not configure a redirect URI.

Redirect URI (optional)

We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Select a platform ▾

e.g. https://example.com/auth

Public client/native (mobile & desktop)

Web

Single-page application (SPA)

Integrate gallery apps and other apps from outside your organization by adding from [Enterprise applications](#).

5. Click **Register**.

6. After you register the application, the overview page appears. Copy and save the **Application (client) ID** and the **Directory (tenant) ID** to a notepad.

Home > cxsecurity | Overview

Multicloud Defense Controller

Search

Overview

Quickstart

Integration assistant

Diagnose and solve problems

Manage

Support + Troubleshooting

Essentials

Display name	: Multicloud Defense Controller	Client credentials	: Add a certificate or secret
Application (client) ID	: e5e0d63d-6f62-4ff9-aaed-2eabd850cf72	Redirect URIs	: Add a Redirect URI
Object ID	: ec1746e4-bd16-4a00-aa7d-3b8e7e52496a	Application ID URI	: Add an Application ID URI
Directory (tenant) ID	: af42bac0-52aa-429f-92db-925819967d17	Managed application in...	: Multicloud Defense Controller
Supported account types	: My organization only	State	: Activated

Welcome to the new and improved App registrations. Looking to learn how it's changed from App registrations (Legacy)? [Learn more](#)

Azure Active Directory Authentication Library (ADAL) and Azure AD Graph no longer receive new feature updates. We continue to provide technical support and security updates. Applications should be upgraded to Microsoft Authentication Library (MSAL) and Microsoft Graph. [Learn more](#)

Get Started Documentation

7. From the **left navigation** of the application page, navigate to **Manage > Certificates & secrets**.



Multicloud Defense Controller



Deactivate



Delete



Endpoints



Overview



Quickstart



Integration assistant



Diagnose and solve problems



Manage



Branding & properties



Authentication (Preview)



Certificates & secrets



Token configuration



API permissions



Expose an API



App roles



Owners



Roles and administrators



Manifest

> Support + Troubleshooting

^ Essentials

Display name : [Multicloud Defense Controller](#)

Application (client) ID : e5e0d63d-6f62-4ff

Object ID : ec1746e4-bd16-4a

Directory (tenant) ID : af42bac0-52aa-429

Supported account types : [My organization or personal Microsoft account](#)



Welcome to the new and improved App registrations page



Azure Active Directory Authentication Library (MSAL) and Microsoft Graph. [Learn more](#)

Get Started

Documentation

The Microsoft

8. Click **New client secret**.



Multicloud Defense Controller | Certificates & secrets

Got feedback?

Overview

Quickstart

Integration assistant

Diagnose and solve problems

Manage

Branding & properties

Authentication (Preview)

Certificates & secrets

Token configuration

API permissions

Expose an API

App roles

Owners

Roles and administrators

Manifest

> Support + Troubleshooting

Credentials enable confidential applications to identify themselves to the authentication service when receiving to scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credent

Application registration certificates, secrets and federated credentials can be found in the tabs below.

Certificates (0)

Client secrets (0)

Federated credentials (0)

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as

New client secret

New client secret

Expires

Value ⓘ

No client secrets have been created for this application.

9. On the **Add a client secret** page, enter these values, then click **Add**:

- **Description:** An appropriate description for the client secret.
- **Expires:** From the drop-down menu, choose the option that best suits your environment.



Note: You must create a new secret when the current secret expires.

Copilot swesnitz@cisco.com
CXSECURITY (CXSECURITY.ONMI...

Add a client secret

Description

swesnitz-mcd-secret

Expires

Recommended: 180 days (6 months)

10. Copy and save both the **Value** and the **Secret ID** to a notepad.



Warning: You can view the secret value only at the time of creation.

Application registration certificates, secrets and federated credentials can be found in the tabs below.

Certificates (0) **Client secrets (1)** Federated credentials (0)

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

+ New client secret

Client secret values cannot be viewed, except for immediately after creation. Be sure to save the secret when created before leaving the page.

Description	Expires	Value ⓘ	Secret ID
swesnitz-mcd-secret	3/14/2027	[REDACTED]	[REDACTED]



Tip: The client secret is listed in the Value column.

Create a Custom Role

1. Navigate to **Subscriptions** with the Azure portal search bar.

Microsoft Azure

Home > cx-tac-rtp-fw-azure (cxsecurity) | Access control (IAM)

Create a custom role ...

Search: sub

All (99+) Services (19) Resources (30) Filters +4

Services (19) See more

Subscriptions

2. Click your **subscription**.

Home > Subscriptions

Subscriptions Compare the different Azure subscription types Forecast my cost for next billing period

cxsecurity (cxsecurity.onmicrosoft.com)

+ Add Manage Policies View Requests View eligible subscriptions Export to CSV Analyze

Global administrators can manage all subscriptions in this list by updating their policy setting [here](#).

Showing subscriptions in cxsecurity directory. Don't see a subscription? [Switch directories](#)

Search for any field...

Subscriptions : **Filtered (1 of 1)** My role == all Status == all Add filter

☐ Subscription name ↑↓	Subscription ID ↑↓	My role ↑↓	Current cost
☐ cx-tac-rtp-fw-azure (cxsecurity)	560f3235-2739-42bf-947e-e6ee1cc2b999	Specified access	\$1,418.01

3. Click **Access control (IAM)**.

Microsoft Azure

Search resources, services, and docs (G+)

Home > Subscriptions

Subscriptions

cxsecurity (cxsecurity.onmicrosoft.com)

+ Add Manage Policies ...

Global administrators can manage all subscriptions in this list by updating their policy setting [here](#).

Showing subscriptions in cxsecurity directory. Don't see a subscription? [Switch directories](#)

Search for any field...

Subscriptions

My role

Status

Admin

cx-tac-rtp-fw-azure (cxsecurity)

Subscription

Search

Cancel subscription Rename Change directory

Change service administrator functionality is no longer supported

Essentials

Subscription ID : 560f3235-2739-42bf-947e-e6ee1cc2b

Directory : cxsecurity (cxsecurity.onmicrosoft.com)

My role : Specified access

Offer : Enterprise Agreement

Offer ID : MS-AZR-0017P

Parent management group : Americas

4. Click **Add**, then select **Add custom role** from the drop-down menu.

azure (cxsecurity)

cx-tac-rtp-fw-azure (cxsecurity) | Access control (IAM)

Subscription

Search

+ Add Download role assignments Edit

Overview

Activity log

Access control (IAM)

Tags

Add role assignment

Add custom role

Add custom role

users have elevated access in your tenant root scope that is not inherited. [View role assignments](#)

5. Enter these values:

- **Custom role name:** An easily identifiable name for the custom role.
- **Description:** A description for the role.
- **Baseline permissions:** Click the **Start from scratch** radio button, if it is not already selected.

Microsoft Azure

Search resources, services, and docs (G+)

Home > Subscriptions > cx-tac-rtp-fw-azure (cxsecurity) | Access control (IAM)

Create a custom role

Basics Permissions Assignable scopes JSON Review + create

To create a custom role for Azure resources, fill out some basic information. [Learn more](#)

Custom role name * Multicloud Defense-controller-role

Description mcd azure test swesnitz

Baseline permissions ☐ Clone a role ☒ Start from scratch ☐ Start from JSON



Note: The JSON that you provide, not the Permissions tab, assigns permissions to the custom

role.

6. Click **JSON**.

7. Click **Edit**.

8. Paste this **code block** within the square brackets for **actions**:

```
"Microsoft.ApiManagement/service/*",
"Microsoft.Compute/disks/*",
"Microsoft.Compute/images/read",
"Microsoft.Compute/sshPublicKeys/read",
"Microsoft.Compute/virtualMachines/*",
"Microsoft.ManagedIdentity/userAssignedIdentities/read",
"Microsoft.ManagedIdentity/userAssignedIdentities/assign/action",
"Microsoft.Network/loadBalancers/*",
"Microsoft.Network/natGateways/*",
"Microsoft.Network/networkInterfaces/*",
"Microsoft.Network/networkSecurityGroups/*",
"Microsoft.Network/publicIPAddresses/*",
"Microsoft.Network/routeTables/*",
"Microsoft.Network/virtualNetworks/*",
"Microsoft.Network/virtualNetworks/subnets/*",
"Microsoft.Resources/subscriptions/resourcegroups/*",
"Microsoft.Storage/storageAccounts/blobServices/*",
"Microsoft.Storage/storageAccounts/listkeys/action",
"Microsoft.Network/networkWatchers/*",
"Microsoft.Network/applicationSecurityGroups/*",
"Microsoft.Compute/diskEncryptionSets/read",
"Microsoft.Insights/Metrics/Read",
"Microsoft.Network/locations/serviceTagDetails/read",
"Microsoft.Network/locations/serviceTags/read",
"Microsoft.CognitiveServices/*/read",
"Microsoft.CognitiveServices/accounts/listkeys/action",
"Microsoft.Network/virtualHubs/*",
"Microsoft.Network/virtualHubs/hubRouteTables/*",
"Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/agreements/*",
"Microsoft.Authorization/roleAssignments/read",
"Microsoft.Authorization/roleDefinitions/read"
```

Create a custom role ...

 If you change tabs and have unsaved edits, those changes will be discarded.

Basics Permissions Assignable scopes **JSON** Review + create

Here is your custom role in JSON format. [Learn more](#)

Download



Discard changes

Save

```

1  {
2      "properties": {
3          "roleName": "Multicloud Defense-controller-role",
4          "description": "mcd azure test swesnitz",
5          "assignableScopes": [
6              "/subscriptions/560f3235-2739-42bf-947e-e6ee1cc2b999"
7          ],
8          "permissions": [
9              {
10                 "actions": [],
11                 "notActions": [],
12                 "dataActions": [],
13                 "notDataActions": []
14             }
15         ]
16     }
17 }
```



Note: Verify the correct spacing and tabs for the JSON code block.

This is an example of the completed role definition:

```

{
  "id": "/subscriptions/redacted/providers/Microsoft.Authorization/roleDefinitions/redacted",
  "properties": {
    "roleName": "Multicloud Defense-controller-role",
    "description": "mcd azure test swesnitz",
    "assignableScopes": [
      "/subscriptions/redacted"
    ],
    "permissions": [
      {
        "actions": [
          "Microsoft.ApiManagement/service/*",
          "Microsoft.Compute/disks/*",
          "Microsoft.Compute/images/read",
          "Microsoft.Compute/sshPublicKeys/read",
          "Microsoft.Compute/virtualMachines/*",
          "Microsoft.ManagedIdentity/userAssignedIdentities/read",
          "Microsoft.ManagedIdentity/userAssignedIdentities/assign/action",
          "Microsoft.Network/loadBalancers/*",
          "Microsoft.Network/natGateways/*",
          "Microsoft.Network/networkInterfaces/*",
          "Microsoft.Network/networkSecurityGroups/*",
          "Microsoft.Network/publicIPAddresses/*",
          "Microsoft.Network/routeTables/*",

```

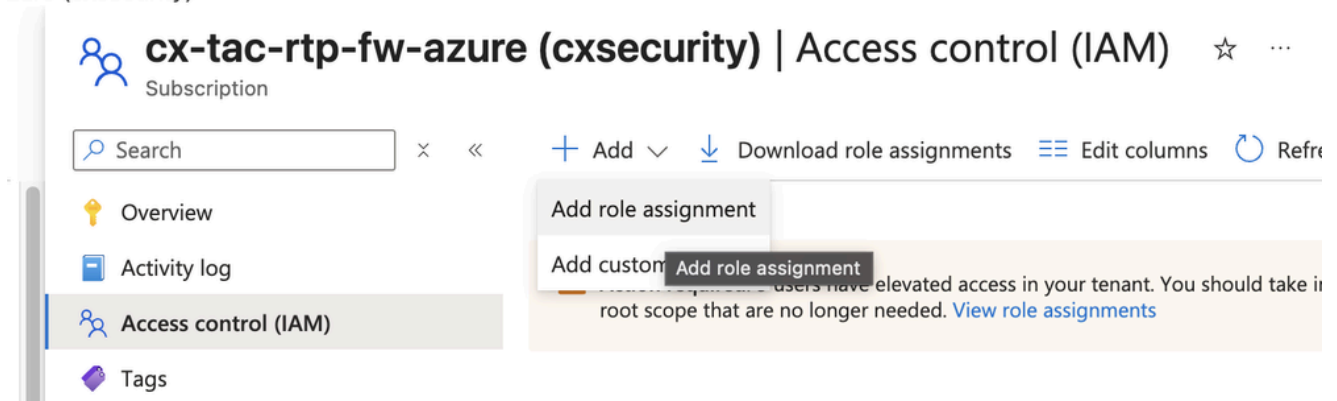
```

"Microsoft.Network/virtualNetworks/*",
"Microsoft.Network/virtualNetworks/subnets/*",
"Microsoft.Resources/subscriptions/resourcegroups/*",
"Microsoft.Storage/storageAccounts/blobServices/*",
"Microsoft.Storage/storageAccounts/listkeys/action",
"Microsoft.Network/networkWatchers/*",
"Microsoft.Network/applicationSecurityGroups/*",
"Microsoft.Compute/diskEncryptionSets/read",
"Microsoft.Insights/Metrics/Read",
"Microsoft.Network/locations/serviceTagDetails/read",
"Microsoft.Network/locations/serviceTags/read",
"Microsoft.CognitiveServices/*/read",
...

```

Assign the Custom Role

1. From the subscription **Access control (IAM)** page, click **Add role assignment**.



2. Search for the **role** that you created in the **Create a Custom Role** section.

Home > Subscriptions > cx-tac-rtp-fw-azure (cxsecurity) | Access control (IAM)

Add role assignment

Role Members Conditions Assignment type Review + assign

A role definition is a collection of permissions. You can use the built-in roles or you can create your own custom roles. [Learn more](#)



Copilot can help pick a role

Job function roles Privileged administrator roles

Grant access to Azure resources based on job function, such as the ability to create virtual machines.

Search: mcd Type: All Category: All

Name ↑↓

Description ↑↓

Multicloud Defense-controller-role

mcd azure test swesnitz

Showing 1 - 1 of 1 results.

3. Click **Next** and leave **Assign access to** set to **User, group, or service principal**.

Add role assignment

Role **Members** Conditions Assignment type Review + assign

Selected role Multicloud Defense-controller-role

Assign access to ☒ User, group, or service principal
☐ Managed identity

Members [+ Select members](#)

Name	Object ID	Type
------	-----------	------

No members selected

Description

Optional

4. Click **Select members**.

Add role assignment

Role **Members** Conditions Assignment type Review + assign

Selected role Multicloud Defense-controller-role

Assign access to ☒ User, group, or service principal
☐ Managed identity

Members [+ Select members](#)

Name	Object ID	Type
------	-----------	------

No members selected

Description

Optional

5. Add the **role** that you created in the **Create a Custom Role** section.

Select members



 Multi 



Multicloud - Azure - RTP
Application



Multicloud Defense Controller
Application

Selected members:



Multicloud Defense Controller
Application



6. Click **Next**, then copy the **subscription ID**.

Add role assignment

Role Members Conditions Assignment type Review + assign

 If you changed your role or member selection, your assignment type might have changed. Please review the assignment before submitting.

Role	Multicloud Defense-controller-role		
Scope	/subscriptions/560f3235-2739-42bf-947e-e6ee1cc2b999		
Members	Name	Object ID	Type
	Multicloud Defense Controller	309bad3d-eb32-4c16-b2bb-0289b3d491f6	App
Description	No description		
Assignment type	Active		
Assignment duration	Permanent		

7. Click **Review + assign**.

Add role assignment ...

Role Members Conditions Assignment type Review + assign

 If you changed your role or member selection, your assignment type might have changed. Please review the assignment before submitting.

Role	Multicloud Defense-controller-role	
Scope	/subscriptions/560f3235-2739-42bf-947e-e6ee1cc2b999	
Members	Name	Object ID
	Multicloud Defense Controller	309bad3d-eb32-4c16-b2bb-0289b3d491f6
Description	No description	
Assignment type	Active	
Assignment duration	Permanent	

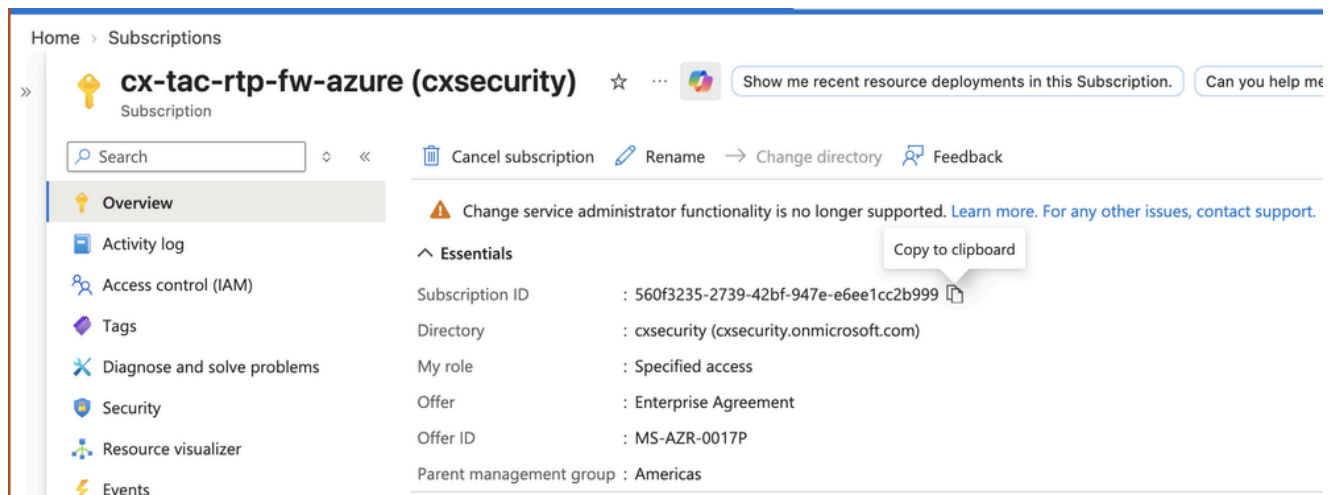
Review + assign

Review + assign

Previous

Next

8. The overview page for the subscription appears. From the left-hand menu, navigate to **Overview** and copy the **subscription ID**.



This completes the Azure prerequisites to add the Azure Account to MCD. These procedures describe the integration and deployment through MCD.

Connect the Azure Account to MCD

1. Navigate to **SCC > Multicloud Defense**.



Security Cloud Control



Organization
cisco-swesnitz



Ho



Home

Products



Firewall



Multicloud Defense

Platform services



Favorites



Security Devices



Platform Management



2. From the main dashboard, click **Add Account** in the **Cloud Accounts** pane.

Dashboard

Cloud Accounts

Discover X

1

Cloud Accounts

1

aws

0

A

0

0

Add Account

View More

3. Click the **Azure** icon.

Select Your Cloud Account

Please select Account Type you want to set up









Close

Back

4. On the **Connect Your Azure Account** page, enter these values:
- **Azure Account Name:** The name of the Azure account from the MCD perspective.
 - **Directory ID:** The directory ID that you saved in the Register an Application section.
 - **Subscription ID:** The subscription ID that you saved in the Assign the Custom Role section.
 - **Application ID:** The application ID that you saved in the Register an Application section.
 - **Client Secret:** The Value that you saved in the Register an Application section.

Connect Your AZURE Account

Prepare your cloud account for integration with Cisco Multicloud Defense Controller with following steps:



- 1 Open up [Azure Cloud Shell](#) in bash mode.
- 2 Download and execute Cisco Multicloud Defense onboarding script in the bash shell. This script creates an App Registration for Cisco Multicloud Defense Controller.
Click [here](#) to see the privilege for the App created.

[Copy](#)

```
bash <( curl -Ls https://raw.githubusercontent.com/valtix-security/cli-azure-setup/master/azure-setup.  
sh ) -w "https://prod1-webhook.mcd.us.cdo.cisco.com:8093/webhook/ciscoswesnitz-US_htztw/azure"
```

Azure Account Name * ⓘ

Description ⓘ

Directory ID * ⓘ

Subscription ID * ⓘ

Application ID * ⓘ

Client Secret * ⓘ

[Show](#)

Cancel

Back

Next

5. MCD discovers and displays the Azure assets. Click **Next**.

Discovering Assets

Doing our magic to discover all of your assets. Please give us a minute...

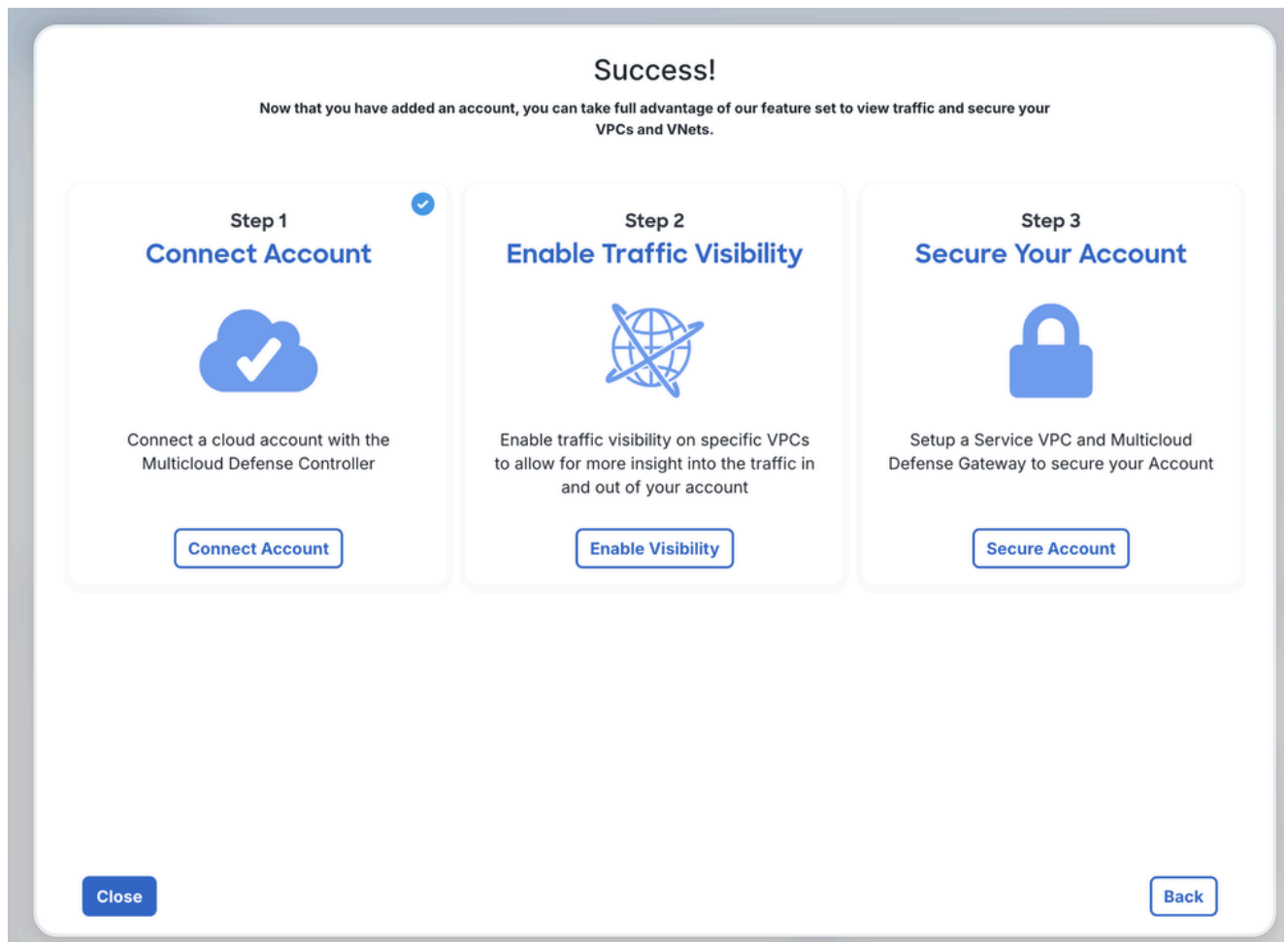
1 Cloud Accounts	63 Regions	- Network ACL	- Network ACL Rules
- Application Security Groups (Azure)	- AI Inventory	- VPCs/VNets	- Subnets
- Security Groups	- Load Balancers	- Instances	- Network Interfaces
- Tags	- Route Tables	- Applications	- Certificates

Cancel

Back

Next

6. Click **Close**.



7. You can now view the onboarded account from **Infrastructure > CSP Accounts**.



Organization
cisco-swesnitz >

< Platform menu

Multicloud Defense



Home >



Inventory >



Investigate >



Policies >



Infrastructure



Reports >



System and Accounts >

Platform services



Favorites >



Security Devices



Platform Management >

Infrastructure ×

Gateways

Gateways

Service VPCs/Vnets

Account

CSP Accounts ✓

Profiles

Packet Capture

Log Forwarding

Metrics Forwarding

Network

NTP

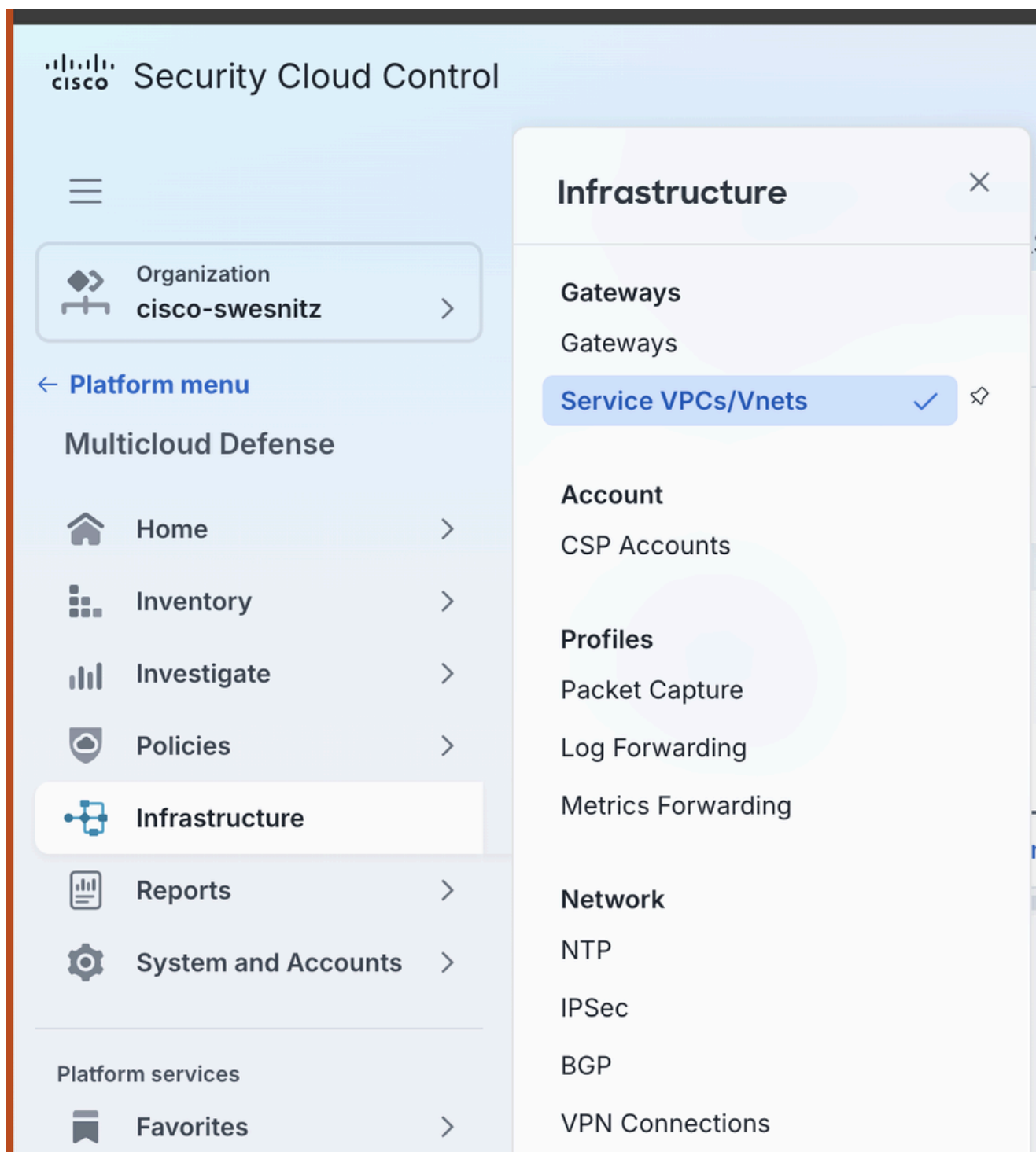
IPSec

BGP

VPN Connections

Create a VNet

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



2. Click **Create**.

Service VPCs/VNets: 1

Quick Filters
Advanced

Name ▼

All Accounts ▼

CSP Type

Create
Actions ▼

☐	Name ▼	ID ▼	Account ▼
☐	mcd_test_vpc-swesnitz	1	AWS-CXLABS-RTP-FW

3. Enter these values:

- **Name:** An easily identifiable name for the VNet that this procedure creates for the FTDv Gateway.
- **CSP Account:** The name that you assigned in the Connect the Azure Account to MCD section.
- **Region:** The region where the FTDv Gateway is deployed.
- **CIDR Block:** A unique IP block for the transit gateway associated with the VNet.
- **Availability Zones:** Select at least two availability zones for resiliency.
- **Resource Group:** Select + **Create Resource Group** from the drop-down menu.
- **Resource Group Name:** A name for the resource group.
- **Resource Group Region:** The region that aligns with the region that you selected for Region.

Click **Save**.

Create Service VPC



Name * ⓘ

mcd_azure_vnet



CSP Account * ⓘ

cx-tac-rtp-fw-azure



Region * ⓘ

East US eastus



CIDR Block * ⓘ

10.4.0.0/16



Availability Zones * ⓘ



1



2



3

Resource Group *

+ Create Resource Group



Resource Group Name *

mcd_swesnitz



Resource Group Region *

East US eastus



Use NAT Gateway ⓘ

vWAN Attachment



Enable vWAN Attachment

Cancel

Save

4. A success message appears.



Success

Service VPC/VNet created successfully.

OK

Confirm creation of the VNet from the Azure side, navigate to **Network foundation > Virtual networks overview > Virtual Networks**.

Home > Network foundation

Network foundation | Virtual Network overview

Preview

Search

Overview

Virtual network

Virtual Network overview

Virtual networks

NAT gateways

Public IP addresses

Network interfaces

Network security groups

Application security groups

Virtual network

Network foundation

Service to provision private networks. Build an isolated, secure environment to run virtual machines (VMs) and applications.

Enhanced security through isolated, secure environments.

Flexible, scalable without physical changes.

Secure connectivity across Azure regions

Learn more

CreateView resources

Connectivity

Home > Network foundation

Network foundation | Virtual networks

Preview

Search

Overview

Virtual network

Virtual Network overview

Virtual networks

NAT gateways

Public IP addresses

Network interfaces

Create

Manage view

Refresh

Export to CSV

Open query

mcd

Subscription equals all

Resource Group equals all

Name ↑

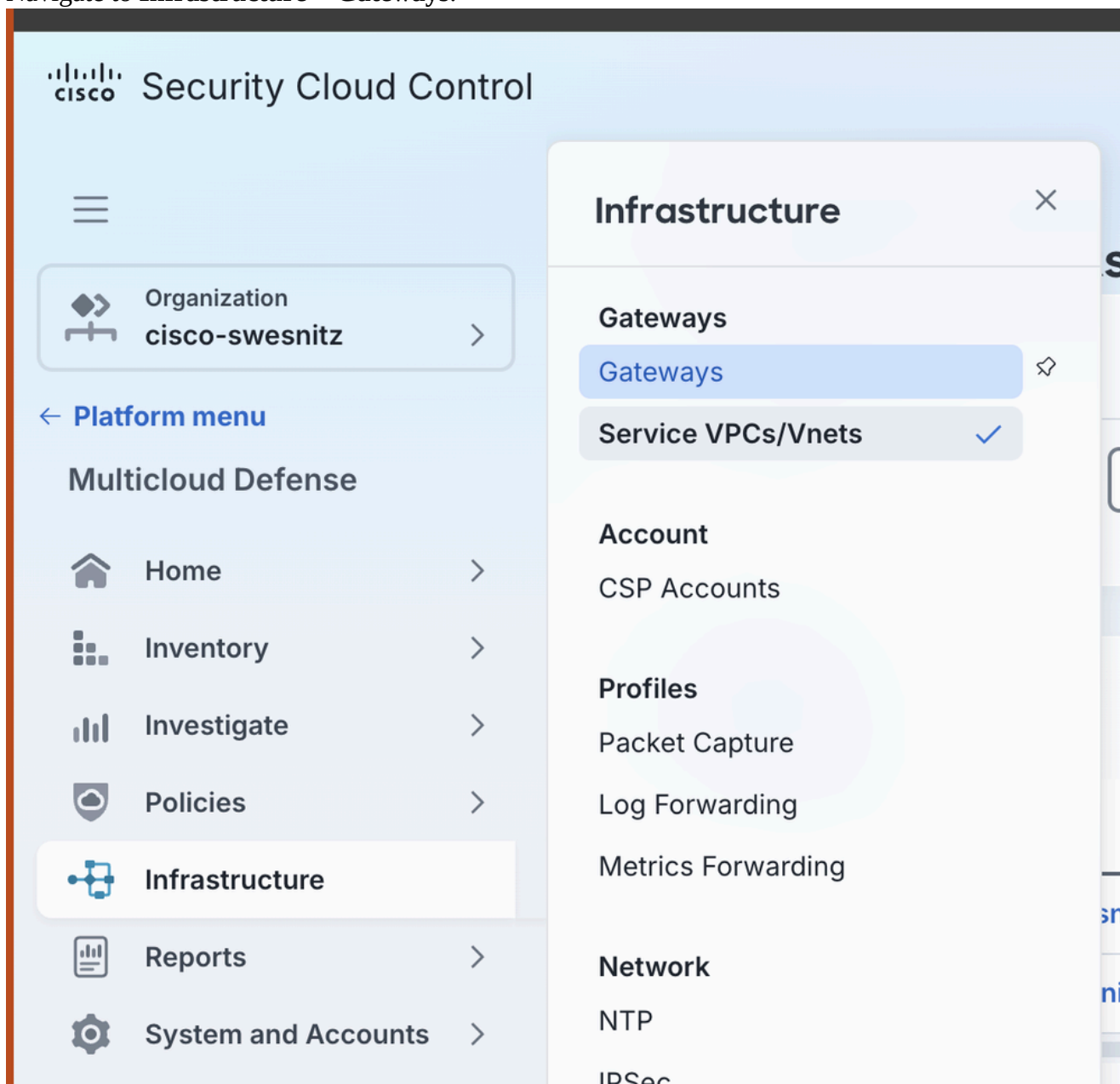
mcd_test_vnet-swesnitz

The VNet transitions to an Active state once it is created.

CreateActions							Refresh
☐	Name	ID	Account	CSP Type	Region	State	
☐	mcd_test_vnet-swesnitz	2	cx-tac-rtp-fw-azure	AZURE	eastus	ACTIVE	

Create the Azure MCD FTDv Gateway

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



2. Click **Add Gateway**.

The screenshot shows the Cisco Security Cloud Control web interface. On the left is a navigation sidebar with a 'Platform menu' containing 'Multicloud Defense' and 'Infrastructure' (highlighted). The main content area is titled 'Gateways: 1' and includes a 'Quick Filters' section with 'Name' and 'CSP Account' dropdowns. Below this is a table with columns for 'Name' and 'State'. A table row is partially visible with the name 'med lab cluster' and state 'ACTIVE'.

3. Enter these values:

- **Accounts:** From the drop-down menu, select the Azure account that you linked in the **Connect the Azure Account to MCD** section.
- **Gateway Type:** Select **FTDv Gateway**.
- **Name:** An easily identifiable name for the FTDv Gateway.
- **Instance Type:** The instance type appropriate for your environment.
- **Minimum Instances:** Select at least one instance from the drop-down menu.
- **Maximum Instances:** The desired number of maximum FTDv instances for your environment. The maximum allowed is 10.
- **HealthCheck Port:** The default is 65534. This document does not alter this value.

Create Gateway

×

Gateway Information

Gateway Details

Advanced Settings

Review

Properties

Accounts * ⓘ

cx-tac-rtp-fw-azure

×

▼

Gateway Type *

FTDv Gateway

×

▼

Name * ⓘ

mcd-azure-lab

×

Description

Optional

Instance Type * ⓘ

8 Virtual CPU | AZURE_D8S_V5

×

▼

Minimum Instances * ⓘ

1

▼

Maximum Instances * ⓘ

3

▼

HealthCheck Port * ⓘ

65534

×

Cancel

Next



Note: The HealthCheck Port is the port number that the Multicloud Defense load balancer uses to check the health of the instances. The datapath security groups assigned to the instances must allow traffic on this port.

4. Enter these values:

- **Properties:** Select **Egress** or **East-West**.
- **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 VNet that you created in the Create a VNet section.

Create Gateway

Security * ⓘ

East West X v

FTDv Version *

10.0.0 X v

Policy Ruleset * ⓘ

Default Access Control Policy X v

FTDv

Admin Password

..... X Show

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

License Model ⓘ

Smart Licensing

Multicloud Defense

Performance Tier * ⓘ

FTDv20 v

License Types * ⓘ

Base X v

Location

Region *

East US eastus X v

VPC/VNet ID * ⓘ

mcd_test_vnet-swesnitz | mcd_test_vnet-swesnitz X v

Key Selection

Cancel

Back

Next

5. Create a public key pair. Refer to [Create an SSH key pair on Windows](#) for guidance.

```

Your Cloud Shell session will be ephemeral so no files or system changes will
shelby [ ~ ]$ ssh-keygen -m PEM -t rsa -b 2048
Generating public/private rsa key pair.
Enter file in which to save the key (/home/shelby/.ssh/id_rsa):
Created directory '/home/shelby/.ssh'.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/shelby/.ssh/id_rsa
Your public key has been saved in /home/shelby/.ssh/id_rsa.pub
The key fingerprint is:

```

6. Enter the values for **SSH Public Key** and **Resource Groups**.

Create Gateway

×

Key Selection

SSH Public Key

SSH Key Pair

SSH Public key *

ssh-rsa
AAAAAB3NzaC1yc2EAAAADAQABAAQChvSlgyD
Kk+X6zGCgM3AxV3iPcxZIF7QtWB7WiagDgo+IRKcH
cPNUofBzsgvIOSuP1mYf6LZQp6Xdhk/9UG6Cq6R0O
LYvmuK/DY2LcDm/P0CFeww/cKCMtpG6Qgy8IK/M

Resource Groups *

mcd_swesnitz | eastus

⊗

↺

User Assigned Identity ID ⓘ

Enter User Assigned Identity ID

Mgmt. Security Group * ⓘ

mcd_test_vnet-swesnitz-mgmt-sg | mcd_swesnitz

⊗

↺

Datapath Security Group 1 * ⓘ

mcd_test_vnet-swesnitz-datapath-sg | mcd_sw...

⊗

↺

Datapath Security Group 2 *

mcd_test_vnet-swesnitz-second-datapath-sg | ...

⊗

↺

Disk Encryption * ⓘ

Azure 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

1

⊗

mcd test vnet-

⊗

mcd test vne-

⊗

mcd test vne-

⊗

Cancel

Back

Next

7. Disable the **public IP**, then click **Next**.

Create Gateway

✓

✓

3

4

Gateway InformationGateway DetailsAdvanced SettingsReview

Public IP

☒ Disable Public IP

8. Review all the values that you specified.

Create Gateway

Gateway Information

Edit

Name

mcd-azure-lab

Gateway Type

FTDv Gateway

Min Instances

1

Max Instances

3

HealthCheckPort

65534

Policy Ruleset ID

Default Access Control Policy

Property

East West

Instance Type

AZURE_D8S_V5

FTDv Version

10.0.0

Gateway Details

Edit

License Model

Smart Licensing

Performance Tier

FTDv20

License Type

Base

Region

eastus

VPC/VNet ID

mcd_test_vnet-swesnitz | mcd_test_vnet-swesnitz

SSH Public Key

ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQChvSlgyDr

Resource Groups

mcd_swesnitz

Mgmt. Security Group

mcd_test_vnet-swesnitz-mgmt-sg

Datapath Security Group 1

mcd_test_vnet-swesnitz-datapath-sg

Datapath Security Group 2

mcd_test_vnet-swesnitz-second-datapath-sg

Cancel

Back

Finish

9. After you review the values and the resources finish loading, click **Finish**.

Create Gateway

Performance Tier

FTDv20

License Type

Base

Region

eastus

VPC/VNet ID

mcd_test_vnet-swesnitz | mcd_test_vnet-swesnitz

SSH Public Key

ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQChvSlgyDr

Resource Groups

mcd_swesnitz

Mgmt. Security Group

mcd_test_vnet-swesnitz-mgmt-sg

Datapath Security Group 1

mcd_test_vnet-swesnitz-datapath-sg

Datapath Security Group 2

mcd_test_vnet-swesnitz-second-datapath-sg

EBS Encryption

AZURE EBS encryption key

Instance Details

Availability Zone	Mgmt. Subnet	Datapath Subnet 1	Datapath Subnet 2
1	mcd_test_vnet-swesnitz-mgmt-1	mcd_test_vnet-swesnitz-datapath-1	mcd_test_vnet-swesnitz-second-datapath-1
2	mcd_test_vnet-swesnitz-mgmt-2	mcd_test_vnet-swesnitz-datapath-2	mcd_test_vnet-swesnitz-second-datapath-2

Recommendations

loading...

Resources Info

loading...

Advanced Settings

Edit

Disable Public IP

enabled

Cancel

Back

Finish

Dashboard view once resources have loaded.

Instance Details

Availability Zone	Mgmt. Subnet	Datapath Subnet 1	Datapath Subnet 2
1	mcd_azure_vnet-mgmt-1	mcd_azure_vnet-datapath-1	mcd_azure_vnet-second-datapath-1
2	mcd_azure_vnet-mgmt-2	mcd_azure_vnet-datapath-2	mcd_azure_vnet-second-datapath-2

Resources Info



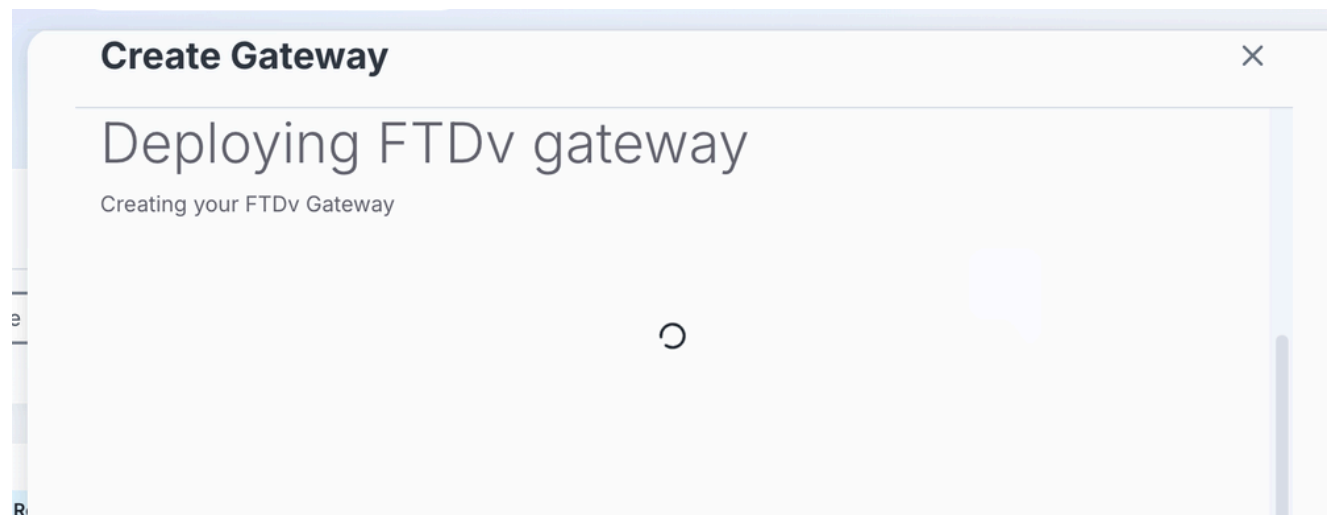
Resource	Limit	In Use	Min Usage for Gateway	Max Usage for Gateway	Recommendation
Private IPs in Subnets	254	0	1	3	
Elastic IPs	1000	51	1	3	
Load Balancers	1000	8	1	1	
Instances	25000	31	2	6	
Virtual CPUs	350	0	16	48	

Advanced Settings

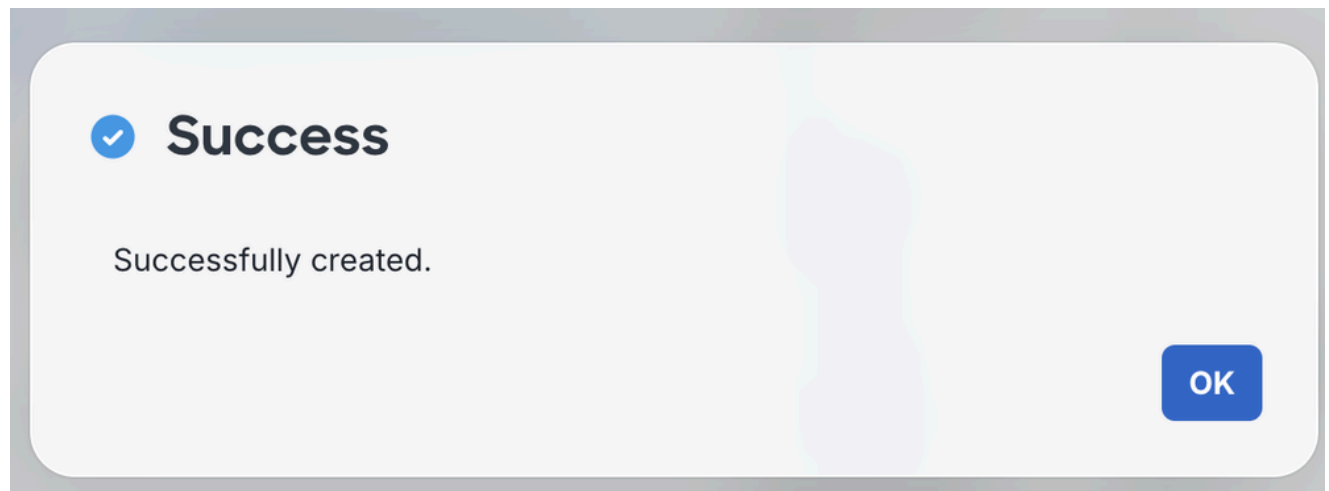
[Edit](#)**Disable Public IP**

enabled

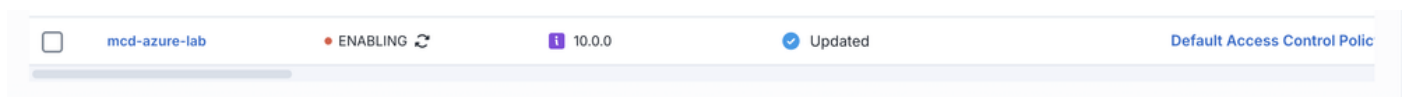
Dashboard view of gateway deploying.



10. After the gateway begins creation, a success message appears. Click **OK**.



From the MCD dashboard, the status displays **ENABLING**.



Monitor the status from the **Summary** and **Instances** tabs.

Details

Edit

Actions

×

Summary

Cloud Details

Interfaces

Instances

Settings

Troubleshooting

Terraform

Name

mcd-azure-lab

State

ENABLING

Description

Instance Type

AZURE_D8S_V5

Type

FTDv Gateway

Min/Max Instances

1 / 3

Mode

HUB

Security Type

East West

Policy Rule Set

Default Access Control Policy

FTDv Version

10.0.0

License Model

Smart Licensing

Performance Tier

FTDv20

License Types

Base

Date Created (Local)

2026-09-15 16:22:37.053

Last Modified (Local)

2026-09-15 16:23:32.156

Verify

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

- Under **Compute > Virtual machines** in Azure, monitor the FTDv instances. The status changes from **Creating** to **Running**.

Home > Compute infrastructure

Compute infrastructure | Virtual machines

Identify VMs with network connectivity issues

Analyze alerts across virtual machines

Get workload templates for VMs

Search

Virtual machines

Get started

Overview

All resources

Infrastructure

Virtual machines

Virtual Machine Scale Set (VMSS)

Compute Fleet

Arc Machines

Create

Reservations

Manage view

Refresh

Export to CSV

Open query

Assign tags

Start

Restart

Stop

Delete

Services

Group by no

mcd

Subscription equals all

Type equals all

Resource Group equals all

Location equals all

Add filter

Name	Subscription	Resource Group	Location	Status	Operating syst...	Size	Public IP address	Disks	Update status
ciscocomd-mcd-azure-lab-nrbcgf	cx-tac-rtg-fw-a...	MCD_SWESNITZ	East US	Creating	Linux	Standard_D8s_v5	-	1	Enable periodic ...
ciscocomd-mcd-azure-lab-psprom	cx-tac-rtg-fw-a...	MCD_SWESNITZ	East US	Creating	Linux	Standard_D8s_v5	-	1	Enable periodic ...

- Confirm the gateway status from the MCD dashboard.

Summary

Cloud Details

Interfaces

Instances

Settings

Troubleshooting

Terraform

Availability Zone	Number of Instances
1	1
2	1

AVAILABILITY ZONES DETAILS

Refresh

Instance: 1

Instance Actions

Instance ID

/subscriptions/560f3235-2739-42bf-947e-e6ee1cc2b999/resourceGroups/mcd_swesnitz/providers/Microsoft.Compute/virtualMachines/ciscomcd-mcd-azure-lab-psprorne

Instance Name

ciscomcd-mcd-azure-lab-psprorne

Datapath Private IP

Datapath 2 Private IP

Datapath 2 Public IP

-

Mgmt Private IP

-

Mgmt Public IP

-

State

● INIT

Created

2026-09-15 16:26:05.711 (LOCAL)

Last Heartbeat

NA

Image Version

10.0.0

Policy Updates

Please check cdFMC for policy update status.

Related Information

- [Create a Service VPC or VNet](#)
- [FTDv Integration Procedure](#)
- [Configure Gateway Prerequisites](#)
- [Multicloud Defense for Azure Overview](#)
- [Create and use an SSH public-private key pair for Linux VMs in Azure](#)
- [Technical Support & Documentation - Cisco Systems](#)