

使用MCD在Azure中部署FTDv網關

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[設定](#)

[註冊應用程式](#)

[建立自定義角色](#)

[分配自定義角色](#)

[將Azure帳戶連線到MCD](#)

[建立VNet](#)

[建立Azure MCD FTDv網關](#)

[驗證](#)

[相關資訊](#)

簡介

本文檔介紹如何配置Microsoft Azure先決條件和通過MCD部署防火牆威脅防禦虛擬(FTDv)網關。

必要條件

- 已獲取並註冊並與Microsoft Entra ID關聯的Azure訂閱。在Azure門戶中的應用註冊列表中確認此項。
- 為Azure訂閱建立的自定義角色，該角色授予多雲防禦(MCD)對特定資源和操作的訪問許可權，否則這些資源和操作將被阻止。
- 對Azure事件網格的訂閱，以便MCD可以從Azure訂閱接收即時更新。
- Azure訂閱從MCD儀表板連線到多雲防禦控制器。
- Azure中接受的思科應用商店條款（如果這是Azure帳戶首次登入MCD）。
- （可選）配置使用者分配的託管身份（如果您需要金鑰保管庫或Blob儲存訪問）。
- 新的服務VNet。在引入FTDv閘道支援之前建立的VNet無法用於FTDv閘道部署。
- 對雲交付的防火牆管理中心(cdFMC)的活動訂閱，該中心管理FTDv裝置的訪問控制策略。
- 通過思科銷售商或合作夥伴購買的至少一個FTDv許可證。

需求

思科建議您瞭解以下主題：

- Microsoft Azure門戶的導航
- Microsoft Entra ID(Azure AD)應用程式註冊和基於角色的訪問控制(RBAC)
- Cisco Multicloud Defense(MCD)
- 思科安全防火牆威脅防禦虛擬(FTDv)

採用元件

本文件所述內容不限於特定軟體和硬體版本。

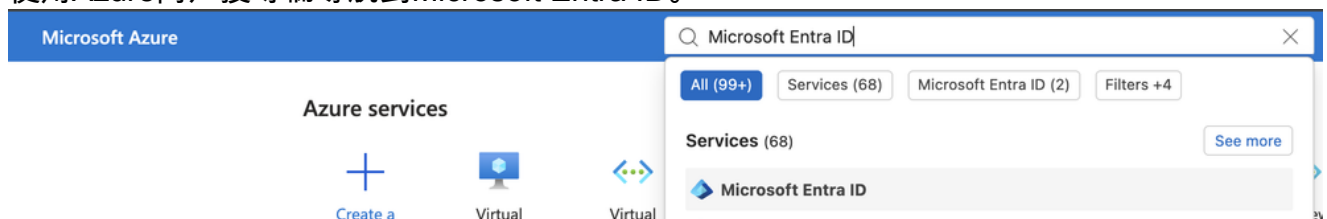
本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

設定

使用這些過程準備Microsoft Azure、將Azure帳戶連線到MCD以及部署FTDv網關。

註冊應用程式

1. 使用Azure門戶搜尋欄導航到Microsoft Entra ID。



2. 按一下Add，然後選擇App registration。

Home

cxsecurity | Overview ...

×

«

+ Add ▾

 Manage tenants

 What's new

 Overview

 Preview features

 Diagnose and solve problems

> Manage

> Monitoring

> Troubleshooting + Support

Basic information

Name	cxsecurity
Tenant ID	af42bac0-52aa-429f-92
Primary domain	cxsecurity.onmicrosoft.com
...	...

3. 在「註冊應用程式」表單上，輸入以下值：

- 名稱:應用程式的易於識別的名稱。
- 支援的帳戶型別:選擇最適合您環境的選項。此文檔僅使用單租戶。

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

indicating 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>

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

4. 針對重新導向URI（可選），選擇適用於您的環境的選項。本文檔未配置重定向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

Public client/native (mobile & desktop)
Web
Single-page application (SPA)

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

5. 按一下「Register」。
6. 註冊應用程式後，將顯示概述頁面。將應用程式(客戶端)ID和目錄(租戶)ID複製並保存到記事本。

The screenshot shows the 'Overview' page for 'Multicloud Defense Controller' in the Azure portal. The left sidebar contains navigation links: Overview, Quickstart, Integration assistant, Diagnose and solve problems, Manage, and Support + Troubleshooting. The main content area is titled 'Essentials' and displays the following information:

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 L...	: Multicloud Defense Controller
Supported account types	: My organization only	State	: ✔ Activated

Below the essentials section, there are two informational messages:

- 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](#)

At the bottom, there are links for 'Get Started' and 'Documentation'.

7. 在應用程式頁面的左導航欄中，導航至管理>證書和密碼。



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. 按一下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. 在Add a client secret頁面上，輸入以下值，然後按一下Add:

- 說明:客戶端密碼的正確描述。
- 到期:從下拉選單中，選擇最適合您環境的選項。



附註：當前金鑰到期時，必須建立新金鑰。

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

Add a client secret

Description

swesnitz-mcd-secret

Expires

Recommended: 180 days (6 months)

10. 將Value和Secret ID複製並儲存到記事本。



警告：您只能在建立時檢視加密值。

i 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]



提示：客戶端密碼列在Value列中。

建立自定義角色

1. 使用Azure門戶搜尋欄導航到Subscriptions。

Microsoft Azure

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

Create a custom role ...

Search: subj

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

Services (19) See more

Subscriptions

2. 按一下您的訂閱。

Home > Subscriptions

Subscriptions

cxsecurity (cxsecurity.onmicrosoft.com)

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

+ 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](#).

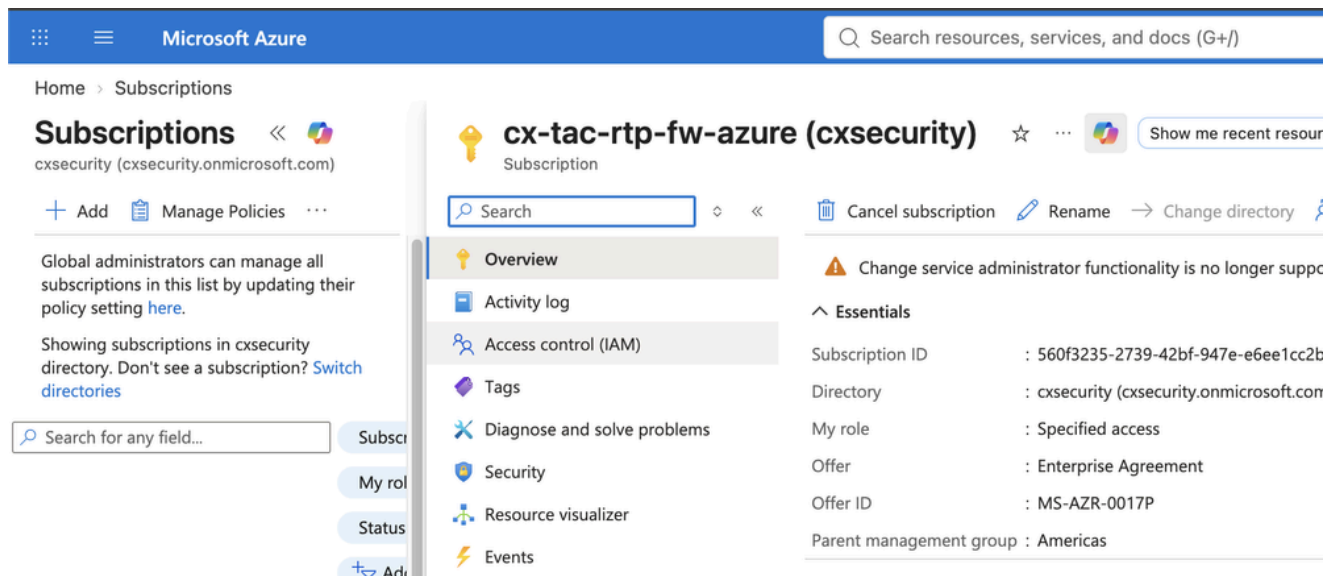
Showing subscriptions in cxsecurity directory. Don't see a subscription? [Switch directories](#)

Search for any field...

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

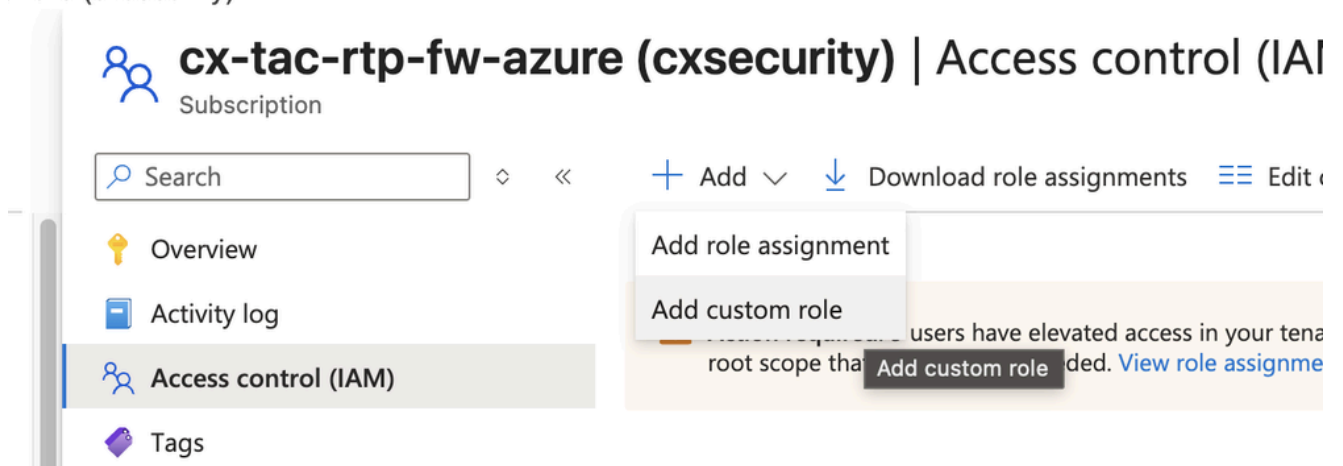
☐ Subscription name ↑↓	Subscription ID ↑↓	My role ↑↓	Current cost
☐ cx-tac-rtp-fw-azure (cxsecurity)	560f3235-2739-42bf-947e-e6ee1cc2b999	Specified access	\$1,418.01

3. 按一下「Access control(IAM)」。



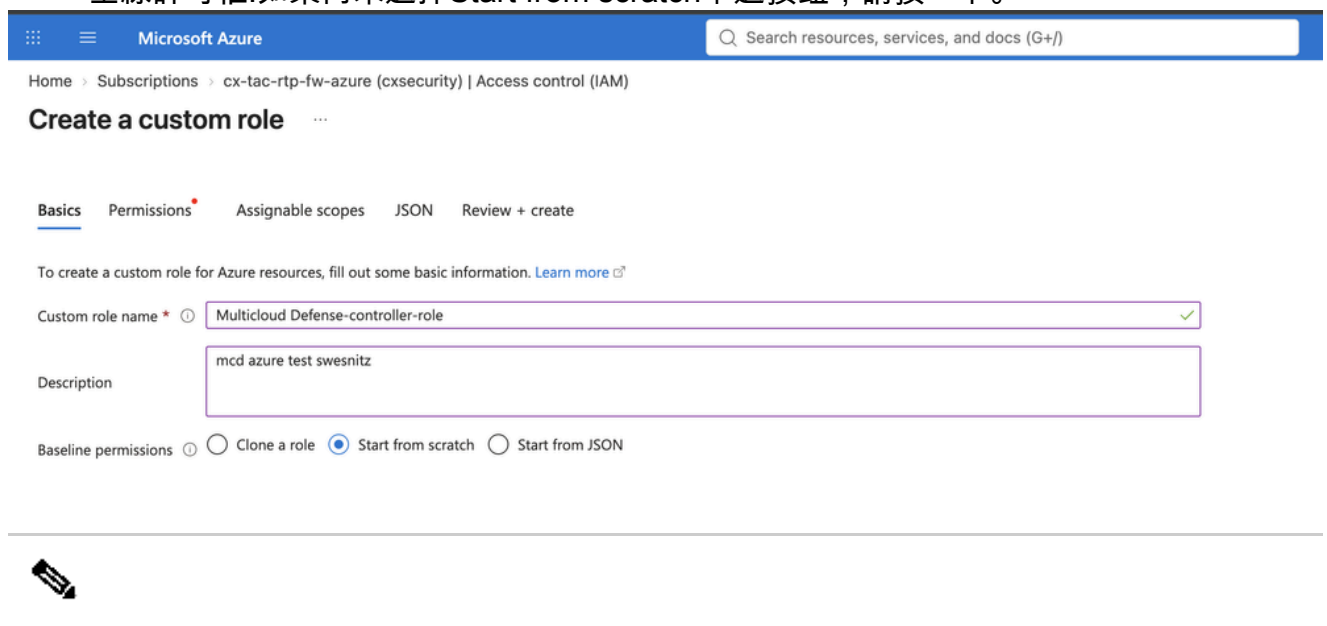
4. 按一下Add，然後從下拉選單中選擇Add custom role。

azure (cxsecurity)



5. 輸入以下值：

- 自定義角色名稱:自定義角色的易識別名稱。
- 說明:角色的說明。
- 基線許可權:如果尚未選擇Start from scratch單選按鈕，請按一下。



附註：您提供的JSON (而不是「許可權」頁籤) 為自定義角色分配許可權。

6. 按一下JSON。
7. 按一下「Edit」。
8. 將此代碼塊貼上到方括弧中，以便執行以下操作:

```
"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 }
```



附註：驗證JSON代碼塊的間距和頁籤是否正確。

以下是已完成的角色定義的示例：

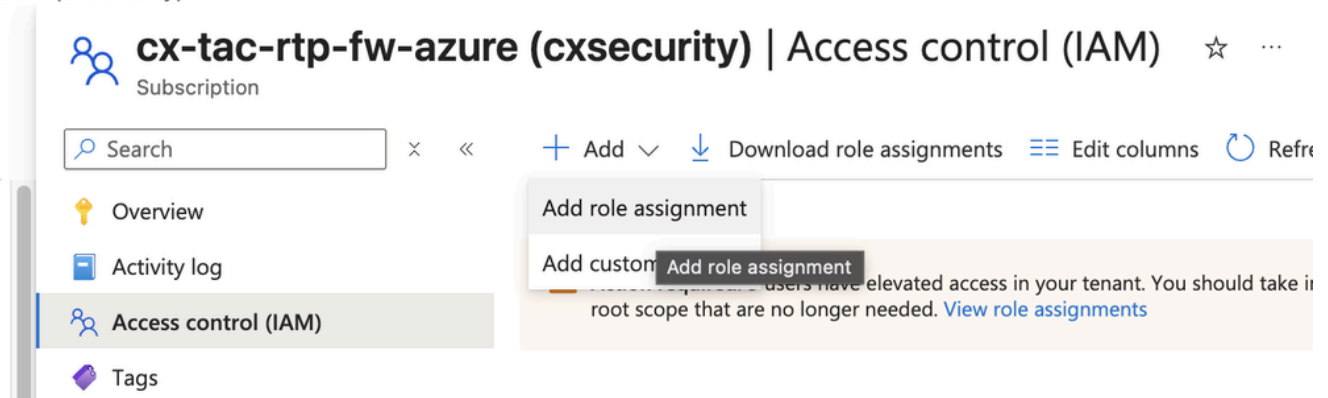
```
{
  "id": "/subscriptions/redacted/providers/Microsoft.Authorization/roleDefinitions/redacted",
  "properties": {
    "roleName": "Multicloud Defense-controller-role",
    "description": "mcd azure test swesnitz",
    "assignableScopes": [
      "/subscriptions/redacted"
    ],
    "permissions": [
      {
        "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",
...
```

分配自定義角色

1. 在訂閱訪問控制(IAM)頁面中，按一下Add role assignment。

zure (cxsecurity)



2. 搜尋您在建立自定義角色部分建立的角色。

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. 按一下下一步，將Assign access設定為User、group或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

4. 按一下「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

5. 新增在建立自定義角色部分建立的角色。

Select members



 Multi 



Multicloud - Azure - RTP
Application



Multicloud Defense Controller
Application

Selected members:



Multicloud Defense Controller
Application



6. 按一下下一步，然後複製訂閱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. 按一下「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	

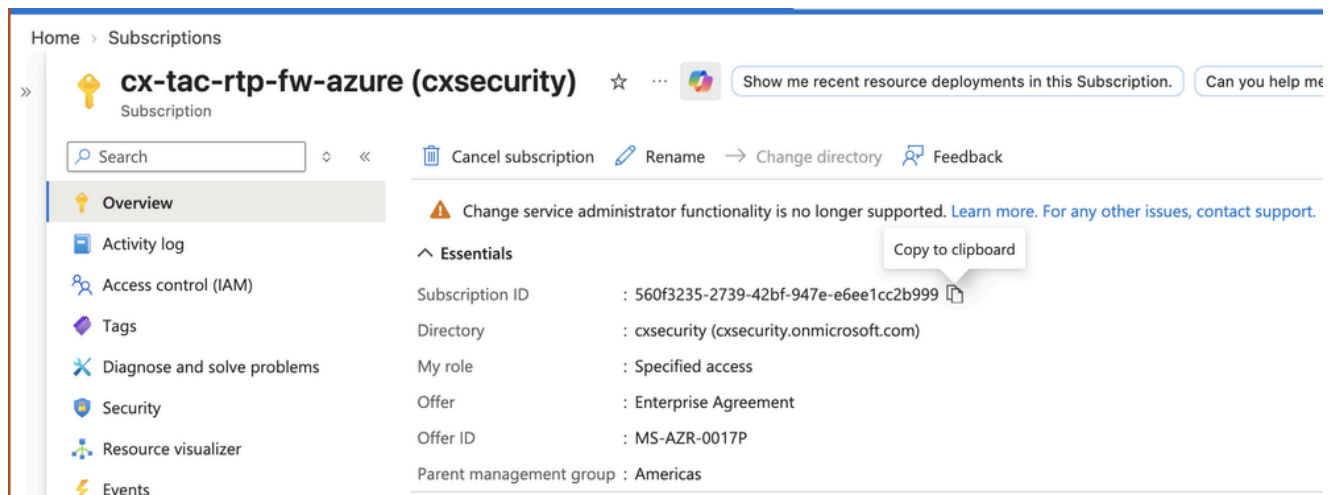
Review + assign

Review + assign

Previous

Next

8. 系統將顯示預訂的概述頁面。從左側選單中，導航到Overview並複製Subscription ID。



這將完成Azure先決條件以將Azure帳戶新增到MCD。這些過程描述了通過MCD的整合和部署。

將Azure帳戶連線到MCD

1. 導覽至SCC > Multicloud Defense。



Security Cloud Control



Organization
cisco-swesnitz



Home

Products



Firewall



Multicloud Defense

Platform services



Favorites



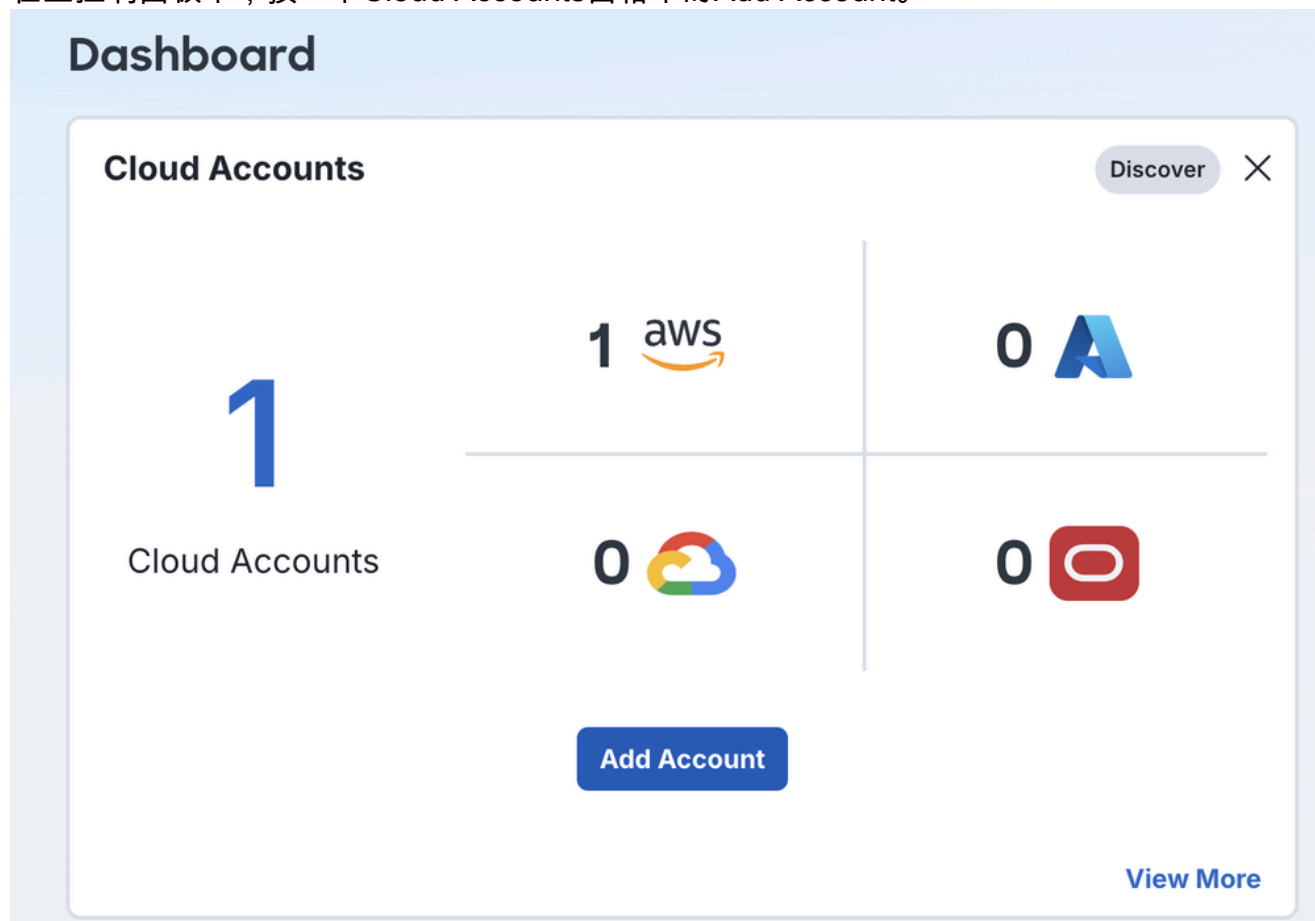
Security Devices



Platform Management



2. 在主控制面板中，按一下Cloud Accounts窗格中的Add Account。



3. 按一下Azure圖標。

Select Your Cloud Account

Please select Account Type you want to set up









Close

Back

4. 在「連線Azure帳戶」頁上，輸入以下值：

- Azure帳戶名稱:從MCD視角來看Azure帳戶的名稱。
- 目錄ID:在「註冊應用程式」部分中儲存的目錄ID。
- 訂閱ID:在「分配自定義角色」部分中儲存的訂閱ID。
- 應用程式ID:您在「註冊應用程式」部分中儲存的應用程式ID。
- 客戶端密碼：在「註冊應用程式」部分中儲存的值。

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發現並顯示Azure資產。按「Next」（下一步）。



6. 按一下「Close」。

Success!

Now that you have added an account, you can take full advantage of our feature set to view traffic and secure your VPCs and VNETs.

Step 1

Connect Account



Connect a cloud account with the Multicloud Defense Controller

Connect Account

Step 2

Enable Traffic Visibility



Enable traffic visibility on specific VPCs to allow for more insight into the traffic in and out of your account

Enable Visibility

Step 3

Secure Your Account



Setup a Service VPC and Multicloud Defense Gateway to secure your Account

Secure Account

Close

Back

7. 現在，您可以從基礎設施> CSP帳戶檢視已註冊帳戶。



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

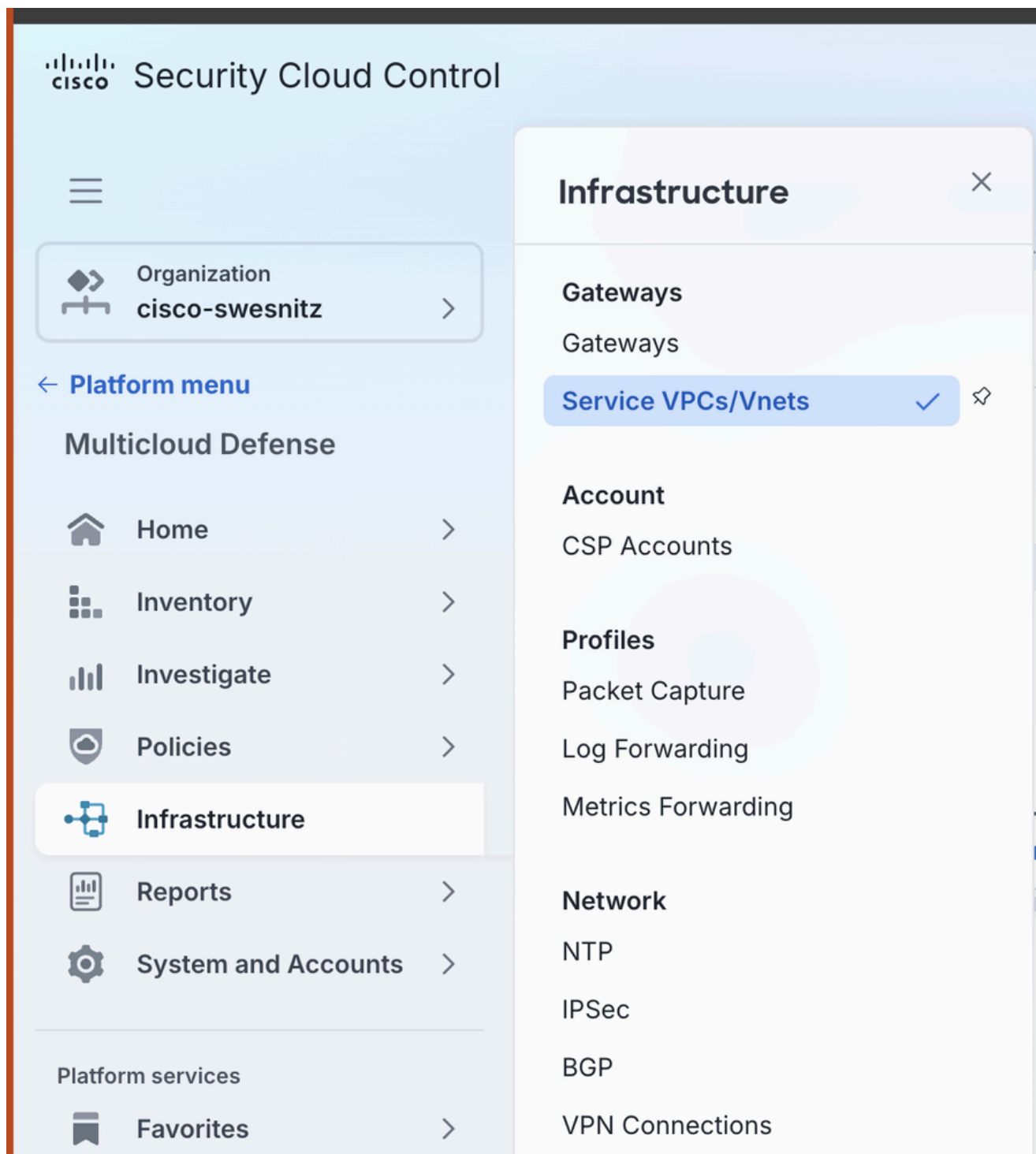
IPSec

BGP

VPN Connections

建立VNet

1. 導航到Infrastructure > Service VPCs/VNets。



2. 按一下「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. 輸入以下值：

- 名稱:此過程為FTDv網關建立的VNet的易於識別的名稱。
- CSP帳戶:在「將Azure帳戶連線到MCD」部分中分配的名稱。
- 地區:部署FTDv閘道的區域。
- CIDR塊:與VNet關聯的傳輸網關的唯一IP塊。
- 可用區:至少選擇兩個可用區域以實現恢復能力。
- 資源組:從下拉選單中選擇+建立資源組。
- 資源組名稱:資源組的名稱。
- 資源組區域:與為「區域」選擇的區域對齊的區域。

按一下「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. 系統將顯示成功消息。



Success

Service VPC/VNet created successfully.

OK

確認從Azure端建立VNet，導航到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](#)

[Create](#) [View resources](#)

Connectivity

Home > Network foundation

Network foundation | Virtual networks

Preview

Search

[+ Create](#) [Manage view](#) [Refresh](#) [Export to CSV](#) [Open query](#)

Subscription equals all Resource Group equals all

☐ Name ↑

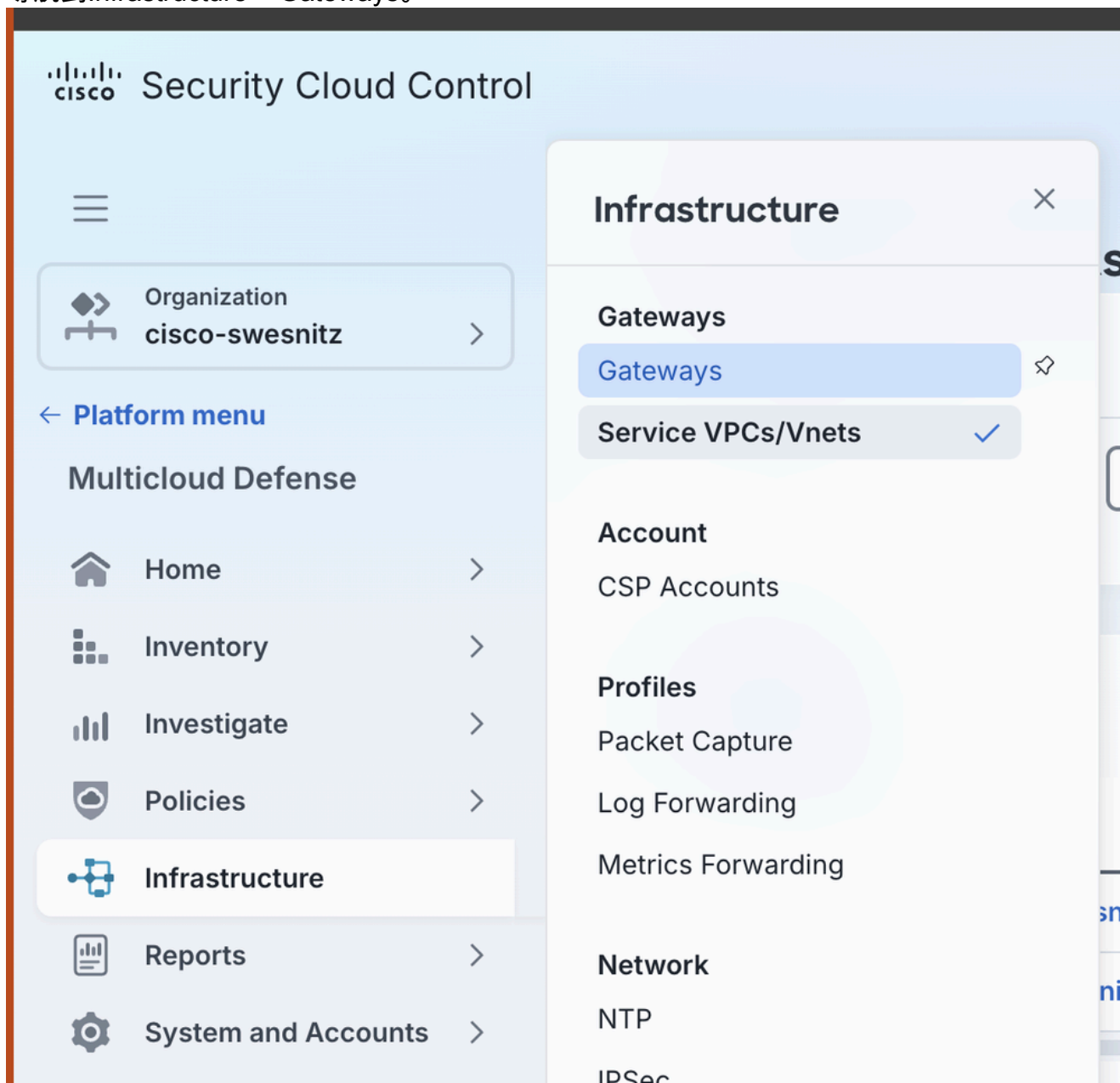
☐ mcd_test_vnet-swesnitz

一旦建立VNet，它就會轉變為「活動」狀態。

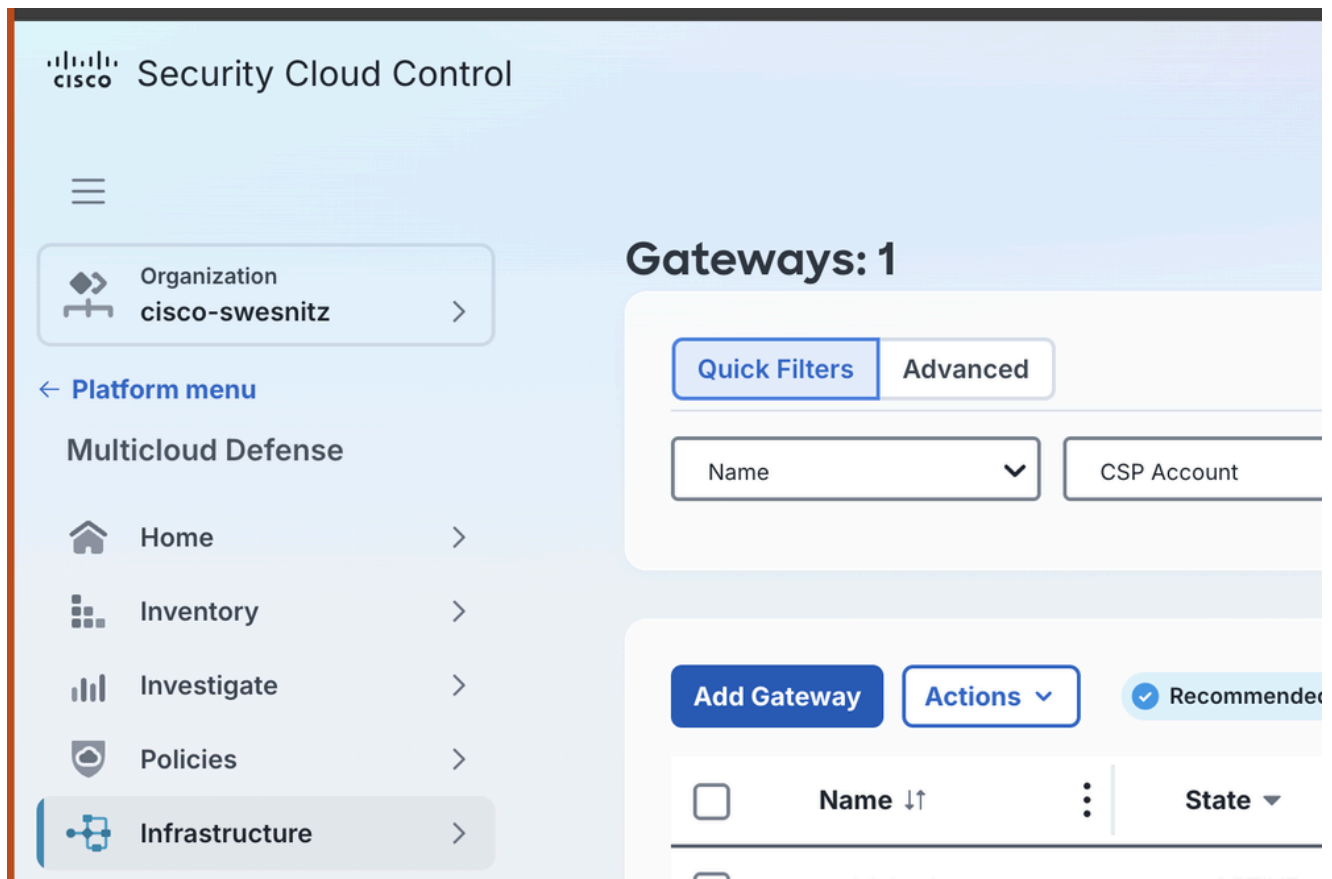
Create Actions Refresh						
☐	Name	ID	Account	CSP Type	Region	State
☐	mcd_test_vnet-swesnitz	2	cx-tac-rtp-fw-azure	AZURE	eastus	ACTIVE

建立Azure MCD FTDv網關

1. 導航到Infrastructure > Gateways。



2. 按一下「Add Gateway」。



3. 輸入以下值：

- 帳戶:從下拉選單中，選擇在「將Azure帳戶連線到MCD」部分中連結的Azure帳戶。
- 網關型別:選擇FTDv Gateway。
- 名稱:FTDv閘道的易於識別名稱。
- 例項型別:適合您環境的例項型別。
- 最小例項:從下拉選單中選擇至少一個例項。
- 最大例項數:環境所需的最大FTDv例項數。允許的最大值為10。
- HealthCheck埠:預設值為65534。本文檔不更改此值。

Create Gateway

Gateway InformationGateway DetailsAdvanced SettingsReview

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

CancelNext

附註：HealthCheck Port是多雲防禦負載平衡器用於檢查例項健康狀況的埠號。分配給例項的資料路徑安全組必須允許此埠上的流量。

4. 輸入以下值：

- 屬性:選擇Egress或East-West。
- FTDv版本:最適合該環境的軟體版本。
- 策略規則集:要應用到此FTDv群集的訪問控制策略(ACP)。
- 密碼:FTDv例項的密碼。
- 許可證型號：所需的許可模式。

- 效能層:適用於預期裝置吞吐量的層。
- 許可證型別:為此部署購買的許可證型別。
- 地區:部署這些FTDv例項的區域。
- VPC/VNet ID:在建立VNet部分建立的服務VNet。

Create Gateway

Security ⓘ

East West X

FTDv Version *

10.0.0 X

Policy Ruleset * ⓘ

Default Access Control Policy X

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

License Types * ⓘ

Base X

Location

Region *

East US eastus X

VPC/VNet ID * ⓘ

mcd_test_vnet-swesnitz | mcd_test_vnet-swesnitz X

Key Selection

Cancel Back Next

5. 建立公鑰對。請參閱[在Windows上建立SSH金鑰對](#)以獲取指導。

```

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. 輸入SSH公鑰和資源組的值。

Create Gateway

×

Key Selection

SSH Public Key

SSH Key Pair

SSH Public key *

ssh-rsa
AAAAAB3NzaC1yc2EAAAADAQABAAQChvSlgyD
Kk+X6zGCgM3AxV3iPcxZIF7QtWB7WiagDgo+IRKcH
cPNUofBzsgyIOSuP1mYf6LZQp6Xdhk/9UG6Cq6R0O
LYvmuK/DY2LcDm/P0CFeww/cKCMToG6Qgy8IK/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. 停用公共IP，然後按一下Next。

Create Gateway

✓

✓

3

4

Gateway Information

Gateway Details

Advanced Settings

Review

Public IP

Disable Public IP

8. 複查您指定的所有值。

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. 檢視這些值和資源完成載入後，按一下完成。

Create Gateway

Performance Tier

License Type

Region

VPC/VNet ID

SSH Public Key

Resource Groups

Mgmt. Security Group

Datapath Security Group 1

Datapath Security Group 2

EBS Encryption

FTDv20

Base

eastus

mcd_test_vnet-swesnitz | mcd_test_vnet-swesnitz

ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQChvSlgyDr

mcd_swesnitz

mcd_test_vnet-swesnitz-mgmt-sg

mcd_test_vnet-swesnitz-datapath-sg

mcd_test_vnet-swesnitz-second-datapath-sg

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

載入資源後儀表板檢視。

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



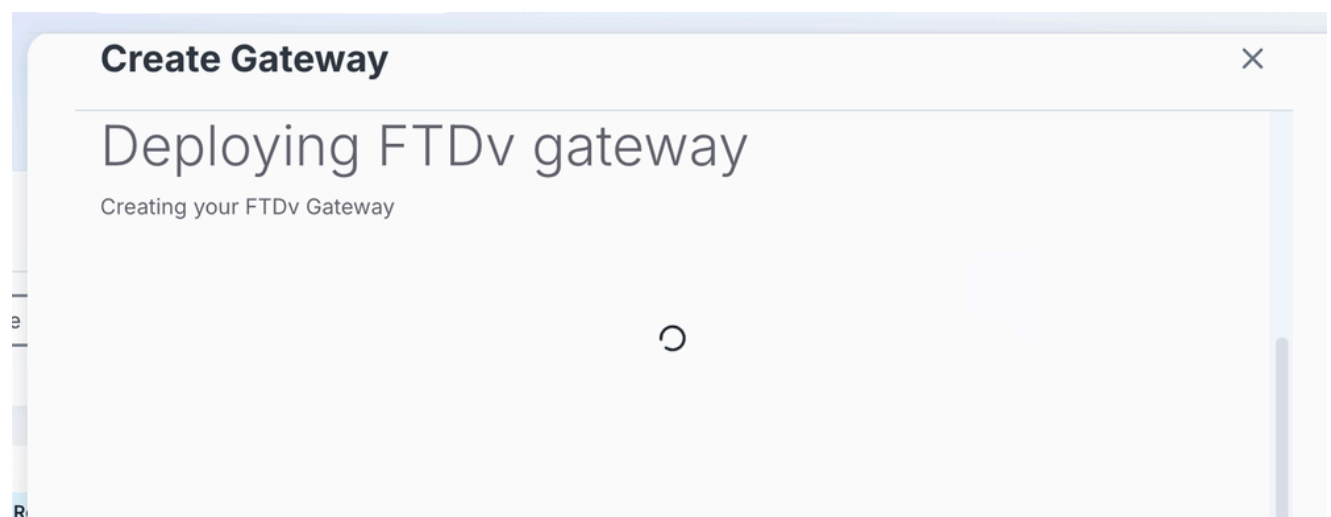
Resource	Limit	In Use	Min Usage for Gateway	Max Usage for Gateway	Recommendation
Private IPs in Subnets	254	0	1	3	
Elastic IPs	1000	51	1	3	
Load Balancers	1000	8	1	1	
Instances	25000	31	2	6	
Virtual CPUs	350	0	16	48	

Advanced Settings

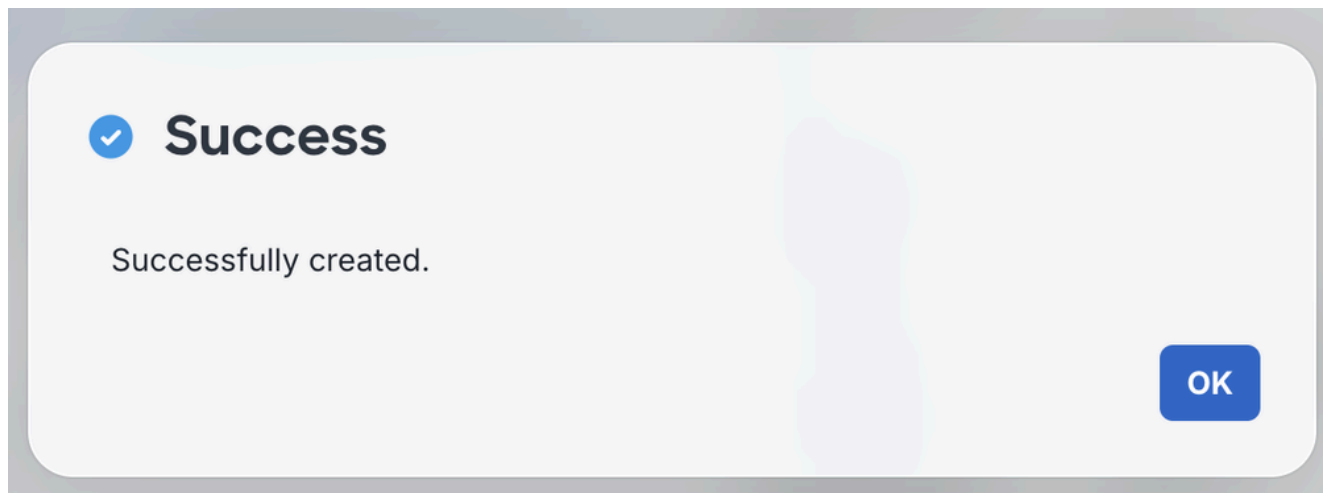
[Edit](#)**Disable Public IP**

enabled

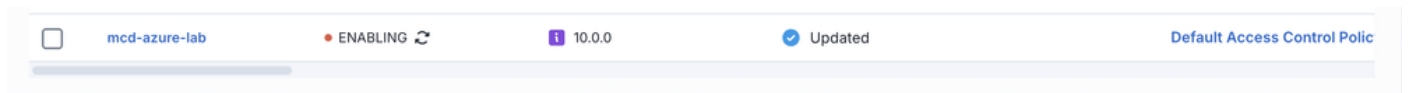
網關部署的儀表板檢視。



10. 網關開始建立後，將出現一條成功消息。按一下「OK」（確定）。



在MCD控制面板中，狀態顯示啟用。



從Summary和Instances頁籤監控狀態。

Details

EditActions

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

驗證

使用本節內容，確認您的組態是否正常運作。

- 在Azure中的計算>虛擬機器下，監視FTDv例項。狀態從Creating更改為Running。

Home > Compute infrastructure

Compute infrastructure | Virtual machines

Identify VMs with network connectivity issuesAnalyze alerts across virtual machinesGet workload templates for VMs

SearchVirtual machinesGet 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

ciscomcd-mcd-azure-lab-nrbcgf

cx-tac-rtip-fw-a...

MCD_SWESNITZ

East US

Creating

Linux

Standard_D8s_v5

-

1

Enable periodic ...

ciscomcd-mcd-azure-lab-pprom

cx-tac-rtip-fw-a...

MCD_SWESNITZ

East US

Creating

Linux

Standard_D8s_v5

-

1

Enable periodic ...

- 從MCD控制面板確認網關狀態。

SummaryCloud DetailsInterfacesInstancesSettingsTroubleshootingTerraform

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.

相關資訊

- [建立服務VPC或VNet](#)
- [FTDv整合程式](#)
- [配置網關先決條件](#)
- [Azure多雲防禦概述](#)
- [為Azure中的Linux虛擬機器建立並使用SSH公鑰 — 私鑰對](#)
- [技術支援與文件 - Cisco Systems](#)

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。