

MCD를 사용하여 Azure에서 FTDv 클러스터 배포

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[구성](#)

[애플리케이션 등록](#)

[사용자 지정 역할 만들기](#)

[사용자 지정 역할 할당](#)

[Azure 계정을 MCD에 연결](#)

[VNet 만들기](#)

[Azure MCD FTDv 게이트웨이 만들기](#)

[다음을 확인합니다.](#)

[관련 정보](#)

소개

이 문서에서는 Microsoft Azure 필수 구성 요소를 구성하고 MCD를 통해 FTDv(Firewall Threat Defense Virtual) 게이트웨이를 배포하는 방법을 설명합니다.

사전 요구 사항

- 획득 및 등록되고 Microsoft Entra ID와 연결된 Azure 구독입니다. Azure 포털의 앱 등록 목록에서 이를 확인합니다.
- MCD(Multicloud Defense) 액세스 권한을 특정 리소스 및 차단된 작업에 부여하는 Azure 구독에 대해 만든 사용자 지정 역할입니다.
- MCD가 Azure 구독에서 실시간 업데이트를 받을 수 있도록 Azure Event Grid에 대한 구독입니다.
- MCD 대시보드에서 Multicloud Defense Controller에 연결된 Azure 구독입니다.
- Azure 계정이 MCD에 온보딩되는 것이 처음인 경우 Azure에서 수락된 Cisco Marketplace 약관입니다.
- (선택 사항) 사용자가 할당한 관리되는 ID를 구성합니다(Key Vault 또는 Blob Storage 액세스가 필요한 경우).
- 새로운 서비스 VNet. FTDv 게이트웨이 지원을 도입하기 전에 생성된 VNet은 FTDv 게이트웨이 구축에 사용할 수 없습니다.

- FTDv 디바이스에 대한 액세스 제어 정책을 관리하는 cdFMC(Cloud-Delivered Firewall Management Center)에 대한 활성 서브스크립션.
- Cisco 판매자 또는 파트너를 통해 구매한 하나 이상의 FTDv 라이선스

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Microsoft Azure 포털 탐색
- Microsoft Azure AD(Enterprise ID) 응용 프로그램 등록 및 RBAC(역할 기반 액세스 제어)
- Cisco MCD(Multicloud Defense)
- Cisco FTDv(Secure Firewall Threat Defense Virtual)

사용되는 구성 요소

이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다.

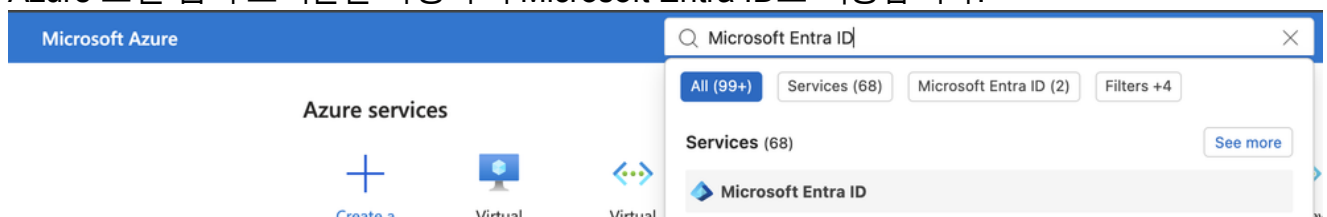
이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

구성

Microsoft Azure를 준비하고 Azure 계정을 MCD에 연결하고 FTDv 게이트웨이를 배포하려면 다음 절차를 사용합니다.

애플리케이션 등록

1. Azure 포털 검색 표시줄을 사용하여 Microsoft Entra ID로 이동합니다.



2. Add(추가)를 클릭한 다음 App registration(앱 등록)을 선택합니다.

×

«

+ Add ▾

⚙ Manage tenants

📄 What's new

Overview

Preview features

Diagnose and solve problems

> Manage

> Monitoring

> Troubleshooting + Support

User >

Group

Enterprise application

App registration

Properties

Recom

Basic information

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

3. 응용 프로그램 등록 양식에서 다음 값을 입력합니다.

- 이름: 응용 프로그램의 쉽게 식별할 수 있는 이름입니다.
- 지원되는 계정 유형: 환경에 가장 적합한 옵션을 선택합니다. 이 문서에서는 단일 테넌트만 사용합니다.

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

nticating 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. Redirect URI(리디렉션 URI)(선택 사항)에서 사용자 환경에 적합한 옵션을 선택합니다. 이 문서에서는 리디렉션 URI를 구성하지 않습니다.

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

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

5. Register(등록)를 클릭합니다.
6. 응용 프로그램을 등록하면 개요 페이지가 나타납니다. 애플리케이션(클라이언트) ID와 디렉토리(테넌트) ID를 복사하여 메모장에 저장합니다.

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:

Property	Value	Action
Display name	Multicloud Defense Controller	
Application (client) ID	e5e0d63d-6f62-4ff9-aaed-2eabd850cf72	Add a certificate or secret
Object ID	ec1746e4-bd16-4a00-aa7d-3b8e7e52496a	Add a Redirect URI
Directory (tenant) ID	a442bac0-52aa-429f-92db-925819967d17	Add an Application ID URI
Supported account types	My organization only	Managed application in L...
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. 애플리케이션 페이지의 왼쪽 탐색에서 Manage(관리) > Certificates & secrets(인증서 및 비밀)로 이동합니다.



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. New client secret을 클릭합니다.



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. 클라이언트 암호 추가 페이지에서 다음 값을 입력한 다음 추가를 클릭합니다.

- 설명: 클라이언트 암호에 대한 적절한 설명입니다.
- 만료: 드롭다운 메뉴에서 환경에 가장 적합한 옵션을 선택합니다.



참고: 현재 암호가 만료되면 새 암호를 만들어야 합니다.

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

Add a client secret

Description

Expires

Recommended: 180 days (6 months)

10. Value(값)와 Secret ID(비밀 ID)를 모두 메모장에 복사하여 저장합니다.



경고: 비밀값은 작성 시에만 볼 수 있습니다.

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		



팁: 클라이언트 암호는 값 열에 나열됩니다.

사용자 지정 역할 만들기

1. Azure 포털 검색 표시줄을 사용하여 구독으로 이동합니다.

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. 구독을 클릭합니다.

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. IAM(액세스 제어)을 클릭합니다.

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

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Security

Resource visualizer

Events

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. Add(추가)를 클릭한 다음 드롭다운 메뉴에서 Add custom role(사용자 지정 역할 추가)을 선택합니다.

azure (cxsecurity)

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

Subscription

Search

+ Add Add role assignment Download role assignments Edit

Overview

Activity log

Access control (IAM)

Tags

Add custom role

Add custom role

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

5. 다음 값을 입력합니다.

- 사용자 지정 역할 이름: 사용자 지정 역할의 쉽게 식별할 수 있는 이름입니다.
- 설명: 역할에 대한 설명입니다.
- 기본 사용 권한: 아직 선택하지 않은 경우 Start from scratch(처음부터 시작) 라디오 버튼을 클릭합니다.

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 * ① Multicloud Defense-controller-role ✓

Description mcd azure test swesnitz

Baseline permissions ① ☐ Clone a role ☒ Start from scratch ☐ Start from JSON



참고: Permissions 탭이 아닌 사용자가 제공하는 JSON은 사용자 지정 역할에 권한을 할당합니다.

6. JSON을 클릭합니다.
7. Edit를 클릭합니다.
8. 작업을 위해 이 코드 블록을 대괄호 안에 붙여넣습니다.

```
"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 }
```



참고: JSON 코드 블록에 대한 올바른 간격과 탭을 확인합니다.

다음은 완료된 역할 정의의 예입니다.

```

{
  "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/*",

```

```

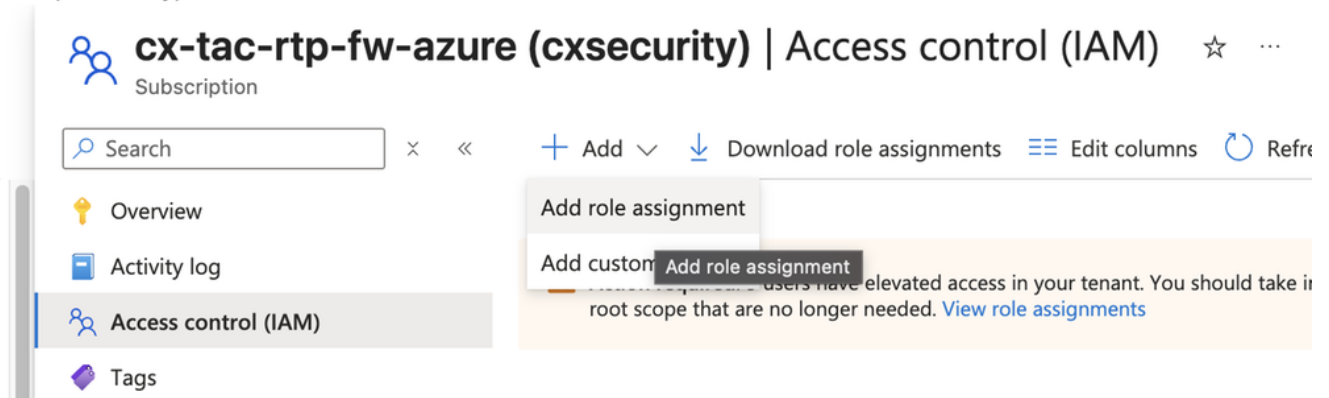
"Microsoft.Network/routeTables/*",
"Microsoft.Network/virtualNetworks/*",
"Microsoft.Network/virtualNetworks/subnets/*",
"Microsoft.Resources/subscriptions/resourcegroups/*",
"Microsoft.Storage/storageAccounts/blobServices/*",
"Microsoft.Storage/storageAccounts/listkeys/action",
"Microsoft.Network/networkWatchers/*",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

```

사용자 지정 역할 할당

1. IAM(Subscription Access Control) 페이지에서 역할 할당 추가를 클릭합니다.

zure (cxsecurity)



2. Create a Custom Role 섹션에서 생성한 역할을 검색합니다.

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.

Type: All Category: All

Name ↑↓	Description ↑↓
Multicloud Defense-controller-role	mcd azure test swesnitz

Showing 1 - 1 of 1 results.

3. Next(다음)를 클릭하고 Assign access to set to User, group, or service principal(액세스 권한

할당을 사용자, 그룹 또는 서비스 보안 주체로 설정합니다.)를 클릭합니다.

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

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. 멤버 선택을 클릭합니다.

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

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. 사용자 지정 역할 만들기 섹션에서 생성한 역할을 추가합니다.

Select members



 Multi 



Multicloud - Azure - RTP
Application



Multicloud Defense Controller
Application

Selected members:



Multicloud Defense Controller
Application



6. Next(다음)를 클릭한 다음 서브스크립션 ID를 복사합니다.

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. Review(검토) + assign(할당)을 클릭합니다.

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	

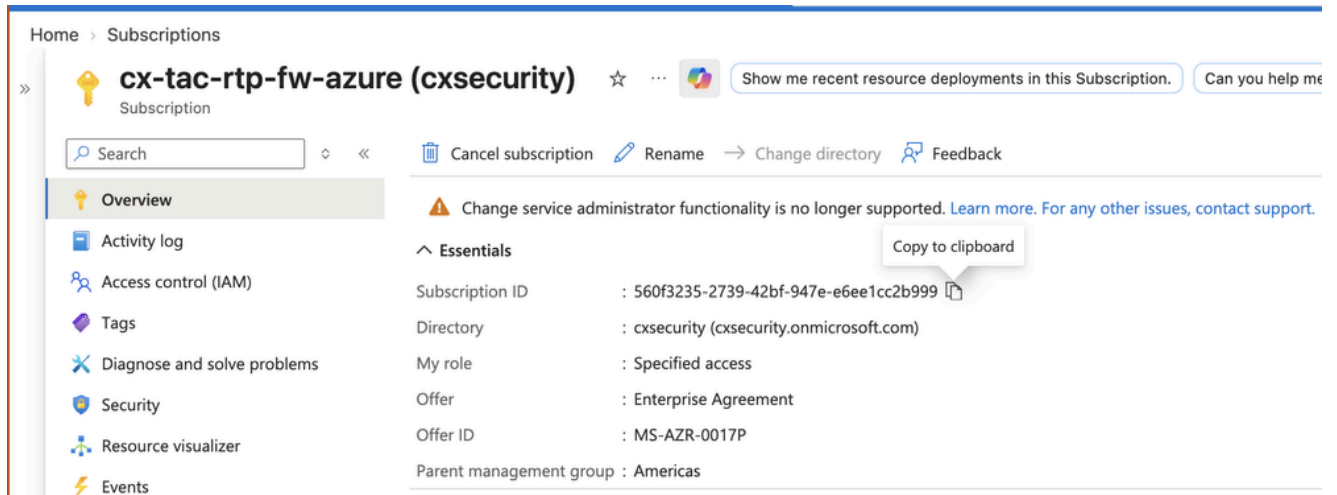
Review + assign

Review + assign

Previous

Next

- 등록에 대한 개요 페이지가 나타납니다. 왼쪽 메뉴에서 Overview(개요)로 이동하고 서브스크립션 ID를 복사합니다.



이렇게 하면 Azure 계정을 MCD에 추가하기 위한 Azure 필수 구성 요소가 완료됩니다. 이 절차에서는 MCD를 통한 통합 및 구축에 대해 설명합니다.

Azure 계정을 MCD에 연결

1. SCC > Multicloud Defense로 이동합니다.



Security Cloud Control



Organization
cisco-swesnitz



Ho



Home

Products



Firewall



Multicloud Defense

Platform services



Favorites



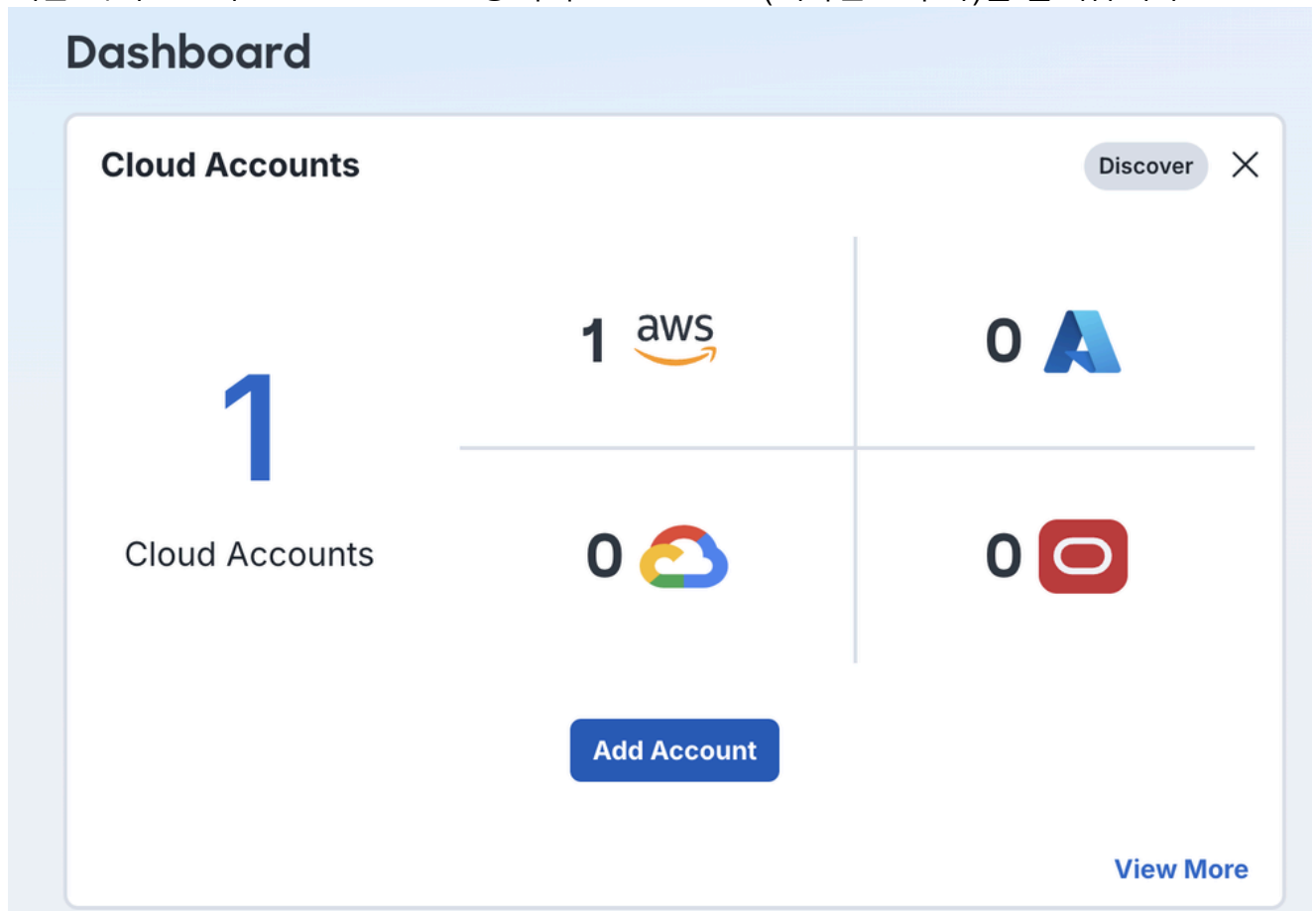
Security Devices



Platform Management



2. 기본 대시보드의 Cloud Accounts 창에서 Add Account(어카운트 추가)를 클릭합니다.



3. Azure 아이콘을 클릭합니다.

Select Your Cloud Account

Please select Account Type you want to set up









Close

Back

4. Azure 계정 연결 페이지에서 다음 값을 입력합니다.

- Azure 계정 이름: MCD 관점에서 Azure 계정의 이름입니다.
- 디렉터리 ID: Register an Application(애플리케이션 등록) 섹션에 저장한 디렉터리 ID.
- 구독 ID: Assign the Custom Role(맞춤형 역할 할당) 섹션에서 저장한 서브스크립션 ID.
- 애플리케이션 ID: Register an Application(애플리케이션 등록) 섹션에 저장한 애플리케이션 ID.
- 클라이언트 암호: Register an Application(애플리케이션 등록) 섹션에 저장한 값입니다.

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 * ⓘ

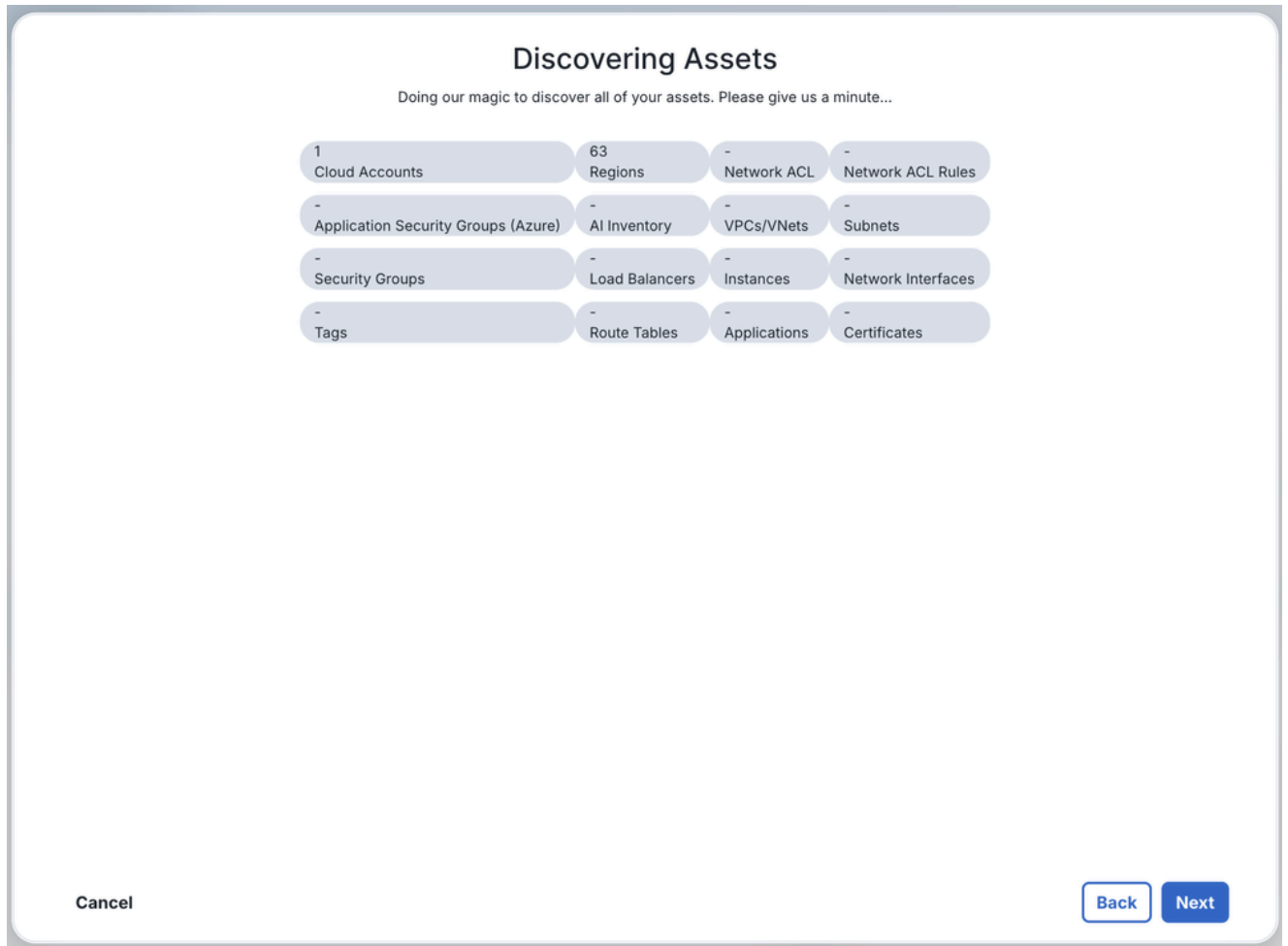
[Show](#)

Cancel

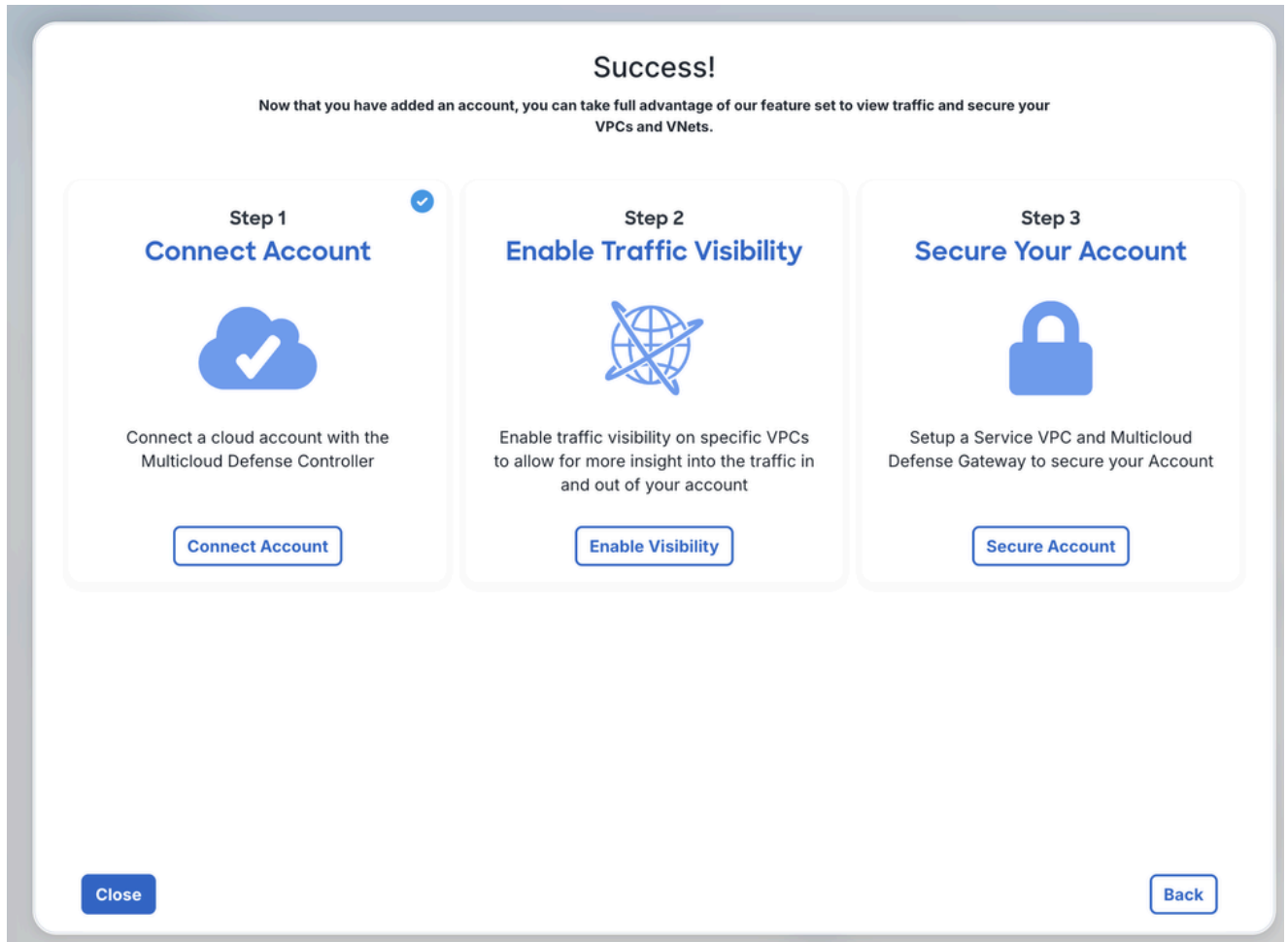
Back

Next

5. MCD는 Azure 자산을 검색하여 표시합니다. Next(다음)를 클릭합니다.



6. Close(닫기)를 클릭합니다.



7. 이제 Infrastructure(인프라) > CSP Accounts(CSP 계정)에서 온보딩된 계정을 볼 수 있습니다.



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

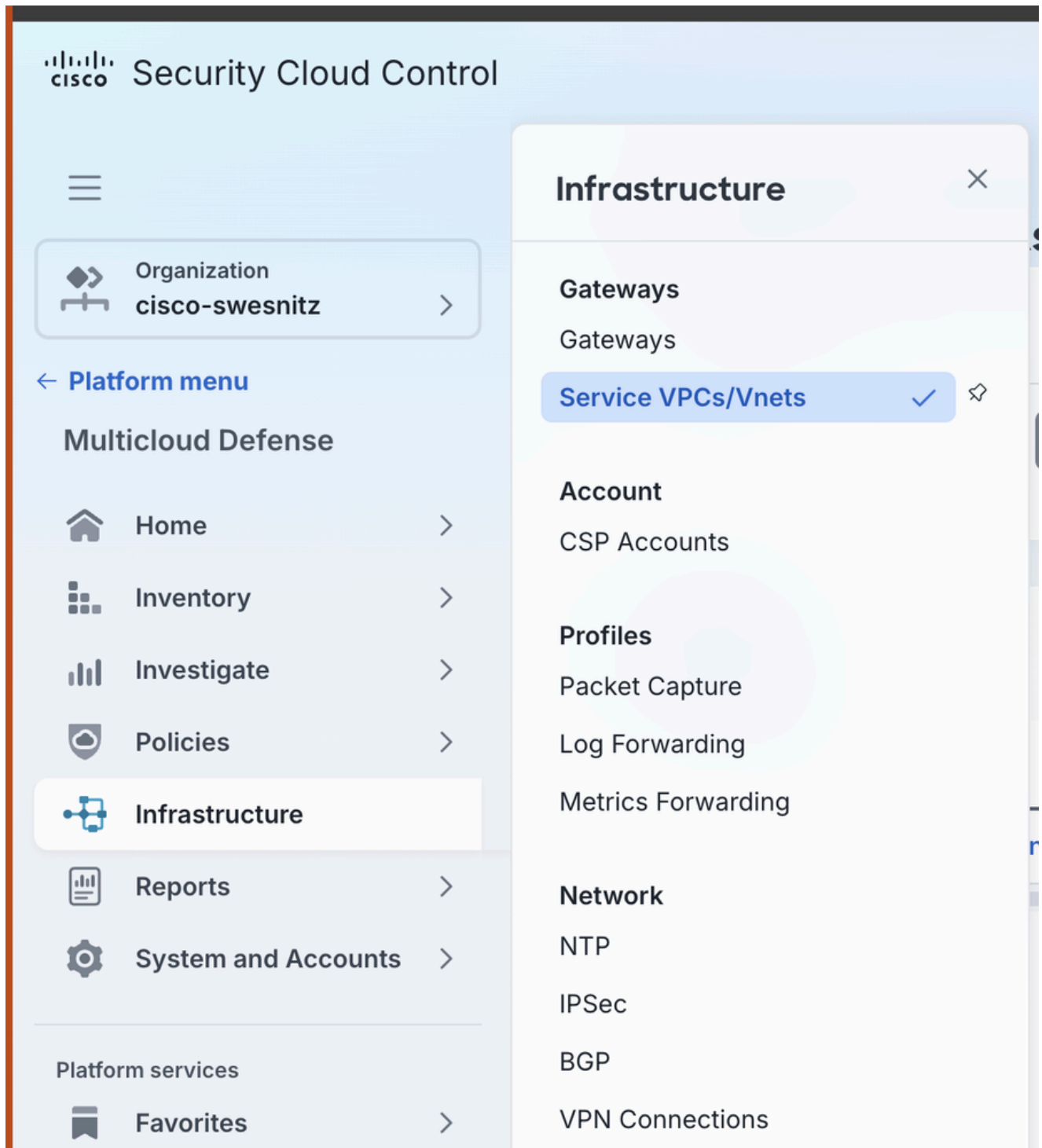
NTP

IPSec

BGP

VPN Connections

1. Infrastructure(인프라) > Service VPCs/VNets(서비스 VPC/VNets)로 이동합니다.



2. Create(생성)를 클릭합니다.

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. 다음 값을 입력합니다.

- 이름: 이 절차에서 FTDv 게이트웨이에 대해 생성하는 VNet의 쉽게 식별할 수 있는 이름입니다.
- CSP 계정: Connect the Azure Account to MCD(Azure 계정을 MCD에 연결) 섹션에서 할당한 이름입니다.
- 지역: FTDv 게이트웨이가 구축된 지역입니다.
- CIDR 블록: VNet과 연결된 트랜짓 게이트웨이의 고유 IP 블록입니다.
- 가용 영역: 복원력을 위해 2개 이상의 가용 영역을 선택하십시오.
- 리소스 그룹: 드롭다운 메뉴에서 + 리소스 그룹 생성을 선택합니다.
- 리소스 그룹 이름: 리소스 그룹의 이름입니다.
- 자원 그룹 지역: 영역에 대해 선택한 영역과 정렬되는 지역입니다.

저장을 클릭합니다.

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. 성공 메시지가 나타납니다.

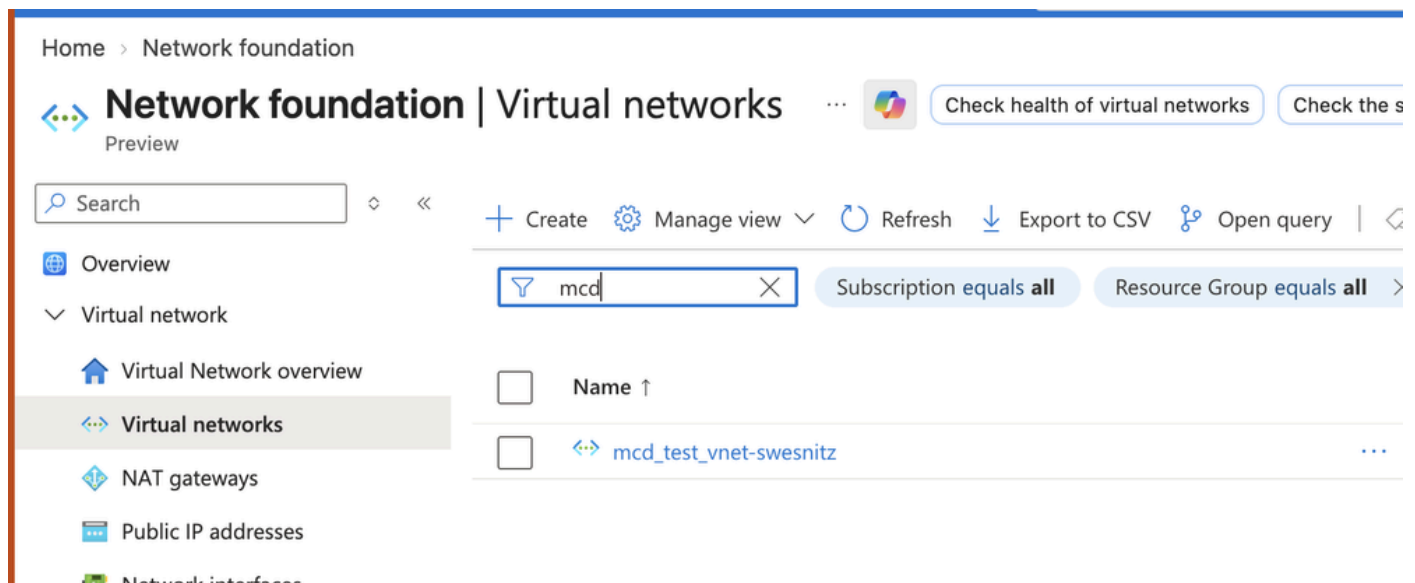
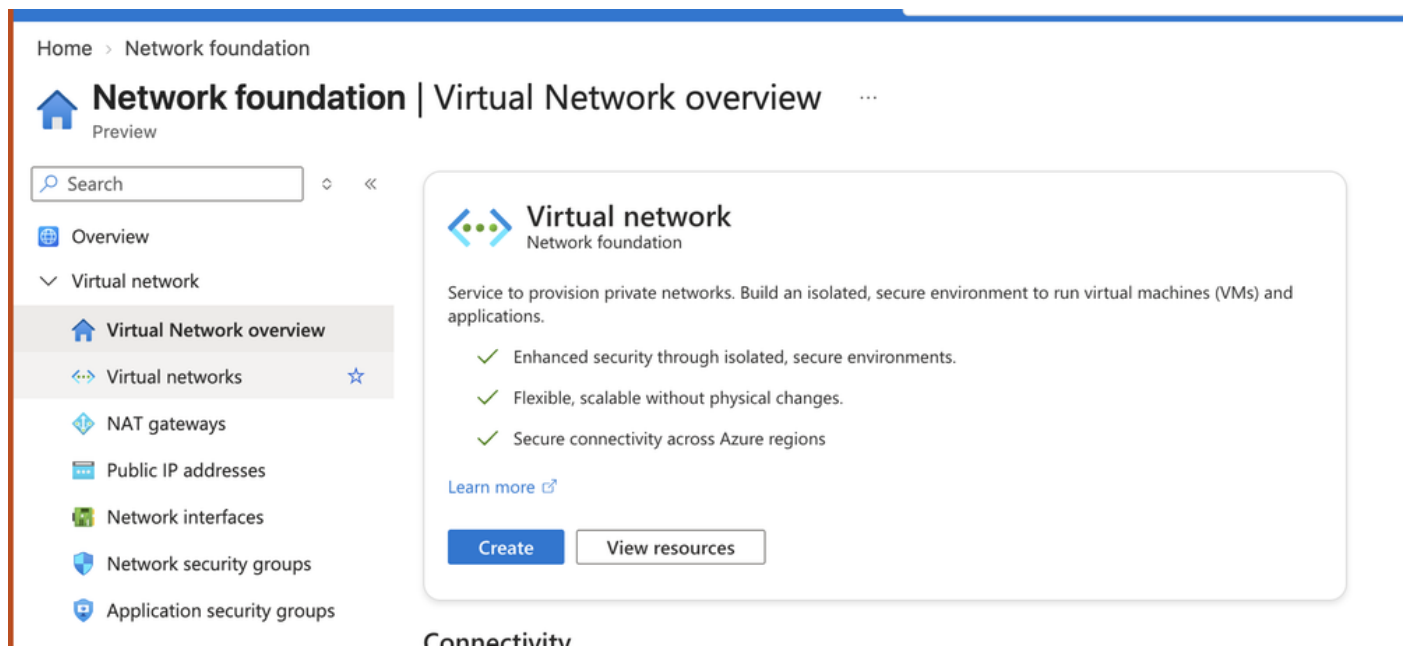


Success

Service VPC/VNet created successfully.

OK

Azure 측에서 VNet 생성을 확인하고 Network foundation > Virtual networks overview > Virtual Networks로 이동합니다.

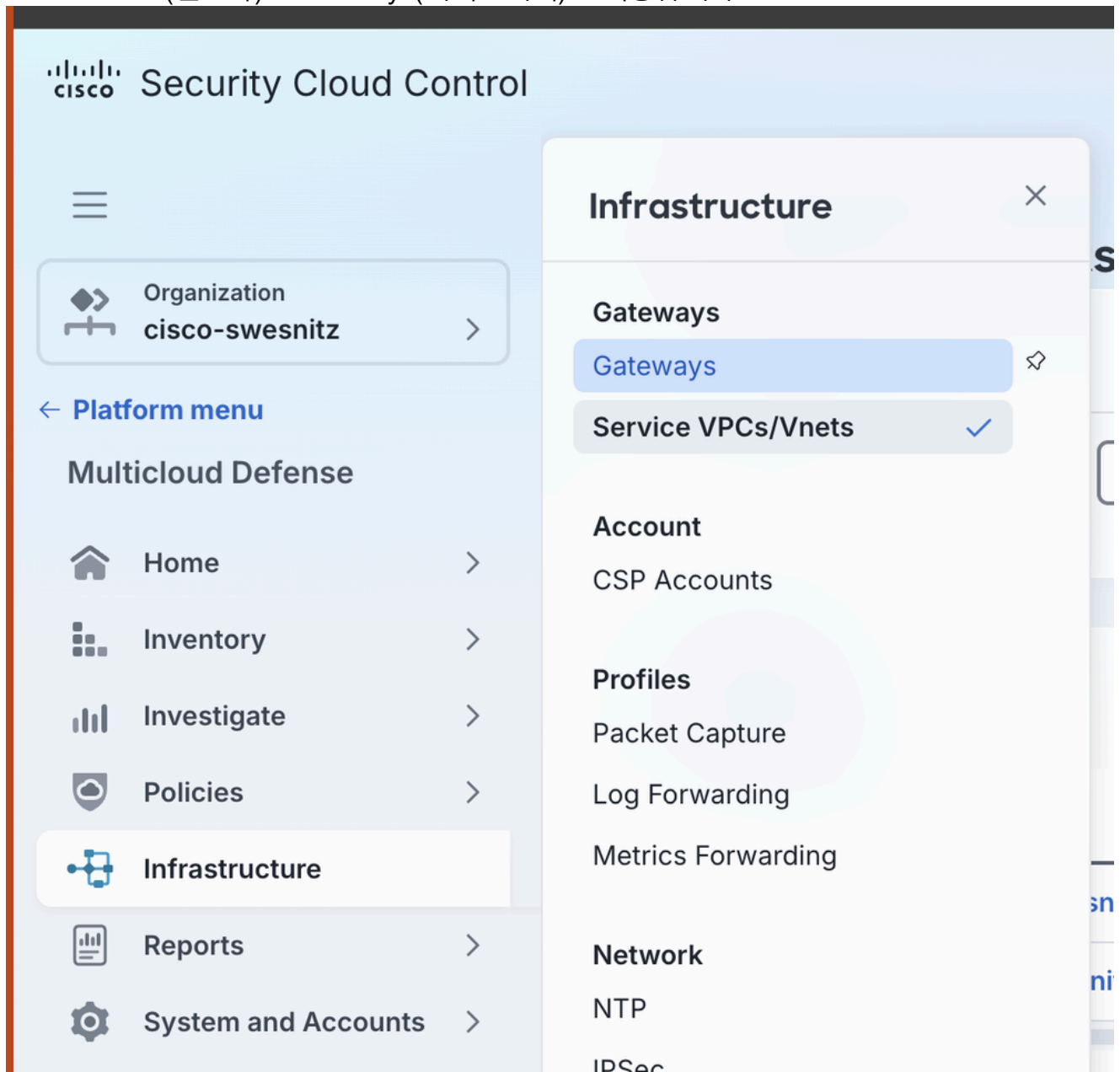


VNet는 일단 생성되면 Active 상태로 전환됩니다.

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

Azure MCD FTDv 게이트웨이 만들기

1. Infrastructure(인프라) > Gateways(게이트웨이)로 이동합니다.



2. Add Gateway(게이트웨이 추가)를 클릭합니다.

The screenshot displays the Cisco Security Cloud Control interface. On the left, the 'Organization' is set to 'cisco-swesnitz'. The 'Platform menu' includes 'Multicloud Defense' and various navigation options. The main section, titled 'Gateways: 1', features 'Quick Filters' and 'Advanced' tabs. Below these are input fields for 'Name' and 'CSP Account'. A table lists gateways, with the first entry being 'med lab cluster' in an 'ACTIVE' state.

3. 다음 값을 입력합니다.

- 어카운트: 드롭다운 메뉴에서 Azure 계정을 MCD에 연결 섹션에서 연결한 Azure 계정을 선택합니다.
- 게이트웨이 유형: FTDv Gateway를 선택합니다.
- 이름: FTDv 게이트웨이에 대해 쉽게 식별할 수 있는 이름입니다.
- 인스턴스 유형: 환경에 적합한 인스턴스 유형입니다.
- 최소 인스턴스: 드롭다운 메뉴에서 인스턴스를 하나 이상 선택합니다.
- 최대 인스턴스: 환경에 대해 원하는 최대 FTDv 인스턴스 수입니다. 최대 허용 값은 10입니다.
- 상태 확인 포트: 기본값은 65534입니다. 이 문서는 이 값을 변경하지 않습니다.

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



참고: HealthCheck Port는 Multicloud Defense 로드 밸런서가 인스턴스 상태를 확인하는 데 사용하는 포트 번호입니다. 인스턴스에 할당된 데이터 경로 보안 그룹은 이 포트에서 트래픽을 허용해야 합니다.

4. 다음 값을 입력합니다.

- 속성: Egress 또는 East-West를 선택합니다.
- FTDv 버전: 환경에 가장 적합한 소프트웨어 버전.
- 정책 규칙 세트: 이 FTDv 클러스터에 적용할 ACP(액세스 제어 정책).
- 암호: FTDv 인스턴스에 대한 비밀번호입니다.

- 라이선스 모델: 원하는 라이선싱 모델.
- 성능 계층: 예상 디바이스 처리량에 적합한 계층입니다.
- 라이선스 유형: 이 구축에 대해 구매한 라이선스 유형.
- 지역: 이러한 FTDv 인스턴스가 구축되는 지역입니다.
- VPC/VNet ID: Create a VNet(VNet 생성) 섹션에서 생성한 서비스 VNet.

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. 공개 키 쌍을 만듭니다. 지침은 [Windows에서 SSH 키 쌍 생성](#)을 참조하십시오.

```

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. SSH 공개 키 및 리소스 그룹에 대한 값을 입력합니다.

Create Gateway

SSH Public Key

SSH Key Pair

SSH Public key *

ssh-rsa
AAAAAB3NzaC1yc2EAAAADAQABAAQChvSlgyD
Kk+X6zGCgM3AxV3iPcxZIF7QtWB7WiagDgo+IRKcH
cPNUofBzsgyIOSuP1mYf6LZQp6Xdhk/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. 공용 IP를 비활성화한 다음 Next(다음)를 클릭합니다.

Create Gateway

✓

✓

3

4

Gateway Information

Gateway Details

Advanced Settings

Review

Public IP

Disable Public IP

8. 지정한 모든 값을 검토합니다.

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. 값과 리소스 로드 완료를 검토한 후 완료를 누릅니다.

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

리소스가 로드되면 대시보드 보기

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



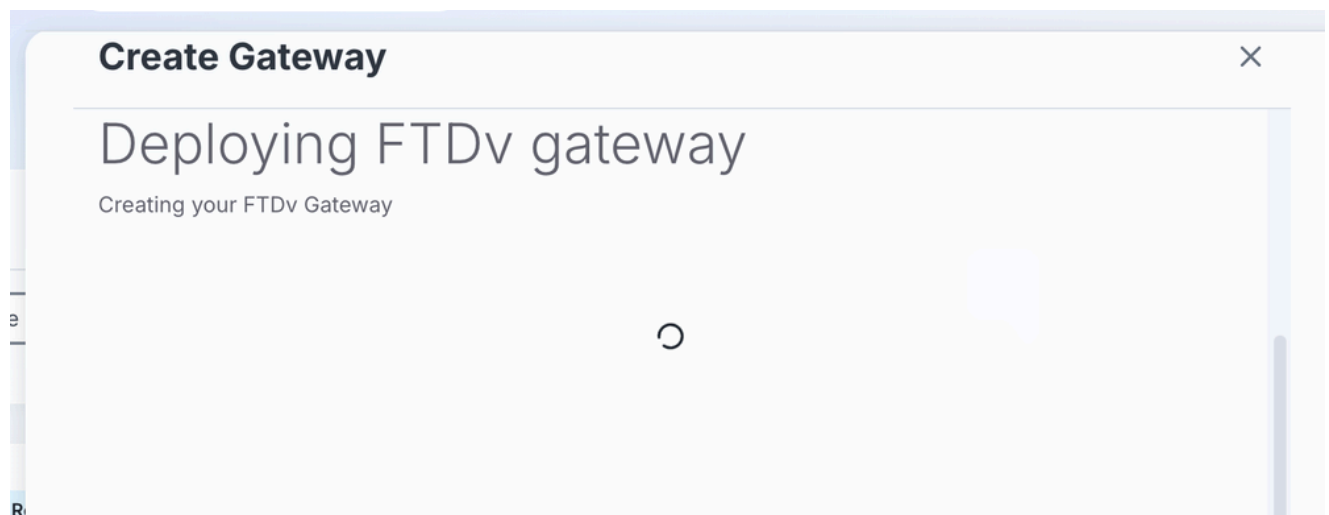
Resource	Limit	In Use	Min Usage for Gateway	Max Usage for Gateway	Recommendation
Private IPs in Subnets	254	0	1	3	
Elastic IPs	1000	51	1	3	
Load Balancers	1000	8	1	1	
Instances	25000	31	2	6	
Virtual CPUs	350	0	16	48	

Advanced Settings

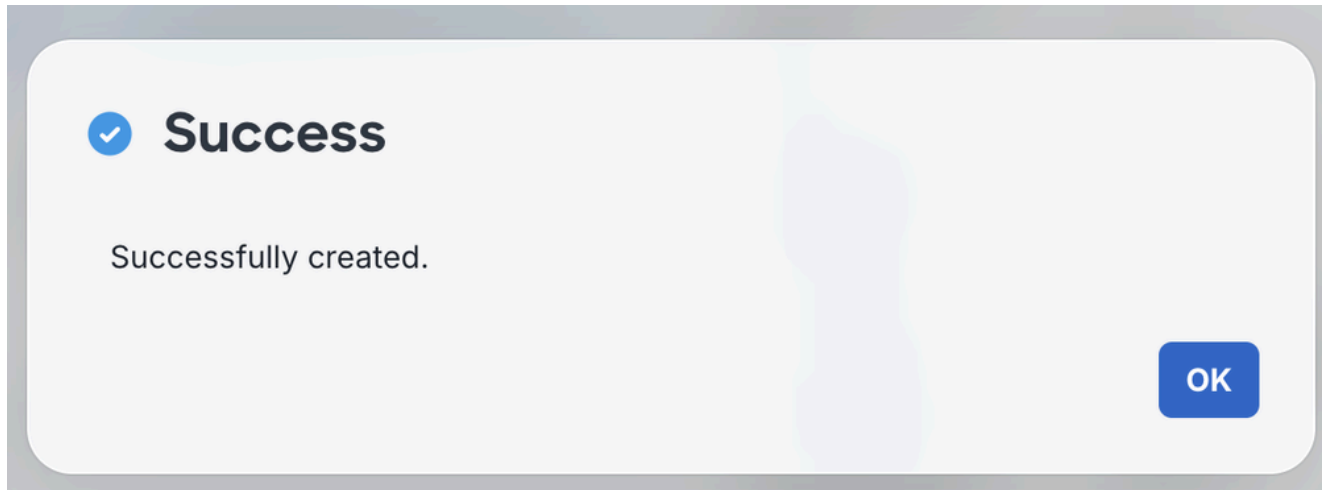
[Edit](#)**Disable Public IP**

enabled

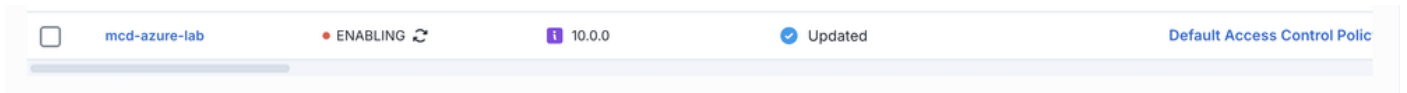
게이트웨이 구축의 대시보드 보기



10. 게이트웨이가 생성을 시작하면 성공 메시지가 나타납니다. OK(확인)를 클릭합니다.



MCD 대시보드에서 상태가 ENABLING(활성화)으로 표시됩니다.



Summary 및 Instances 탭에서 상태를 모니터링합니다.

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

다음을 확인합니다.

구성이 올바르게 작동하는지 확인하려면 이 섹션을 활용하십시오.

- Azure의 Compute(컴퓨팅) > Virtual machines(가상 머신)에서 FTDv 인스턴스를 모니터링합니다. 상태가 Creating(생성)에서 Running(실행 중)으로 변경됩니다.

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
☐	ciscomcd-mcd-azure-lab-nrbcg	cx-tac-rtg-fw-a...	MCD_SWESNITZ	East US	Creating	Linux	Standard_D8s_v5	-	1	Enable periodic ...
☐	ciscomcd-mcd-azure-lab-psprom	cx-tac-rtg-fw-a...	MCD_SWESNITZ	East US	Creating	Linux	Standard_D8s_v5	-	1	Enable periodic ...

- MCD 대시보드에서 게이트웨이 상태를 확인합니다.

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.

관련 정보

- [서비스 VPC 또는 VNet 생성](#)
- [FTDv 통합 절차](#)
- [게이트웨이 사전 요구 사항 구성](#)
- [Azure용 멀티 클라우드 방어 개요](#)
- [Azure에서 Linux VM용 SSH 공개-개인 키 쌍 만들기 및 사용](#)
- [기술 지원 및 문서 - Cisco Systems](#)

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.