

MCDを使用してAzureにFTDv Gatewayをデプロイする

内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[設定](#)

[アプリケーションの登録](#)

[カスタムロールの作成](#)

[カスタムロールの割り当て](#)

[AzureアカウントをMCDに接続する](#)

[VNetの作成](#)

[Azure MCD FTDv Gatewayの作成](#)

[確認](#)

[関連情報](#)

概要

このドキュメントでは、Microsoft Azureの前提条件を設定し、MCDを介してFirewall Threat Defense Virtual(FTDv)ゲートウェイを展開する方法について説明します。

前提条件

- 取得および登録され、Microsoft Entra IDに関連付けられているAzureサブスクリプション。Azureポータルアプリ登録の一覧でこれを確認します。
- Azureサブスクリプション用に作成されたカスタムロールで、マルチクラウド防御(MCD)に対して、ブロックされている特定のリソースとアクションへのアクセスを許可します。
- MCDがAzureサブスクリプションからリアルタイムの更新を受信できるように、Azure Event Gridのサブスクリプション。
- Azureサブスクリプションは、MCDダッシュボードからマルチクラウド防衛コントローラーに接続されました。
- Azureアカウントが初めてMCDにオンボーディングされる場合、Azureで受け入れられるCisco Marketplace規約。
- (オプション) Key VaultまたはBLOBストレージアクセスが必要な場合は、ユーザーに割り

当てられた管理対象IDが構成されます。

- 新しいサービスVNetFTDvゲートウェイのサポートが導入される前に作成されたVNetは、FTDvゲートウェイの導入には使用できません。
- Cloud-Delivered Firewall Management Center(cdFMC)のアクティブなサブスクリプション。FTDvデバイスのアクセスコントロールポリシーを管理します。
- シスコの販売担当者またはパートナーを通じて購入した1つ以上のFTDvライセンス。

要件

次の項目に関する知識があることが推奨されます。

- Microsoft Azureポータルナビゲーション
- Microsoft Entra ID (Azure AD)アプリケーションの登録とロールベースアクセスコントロール(RBAC)
- Ciscoマルチクラウド防御(MCD)
- Cisco Secure Firewall Threat Defense Virtual(FTDv)

使用するコンポーネント

本書の内容は、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

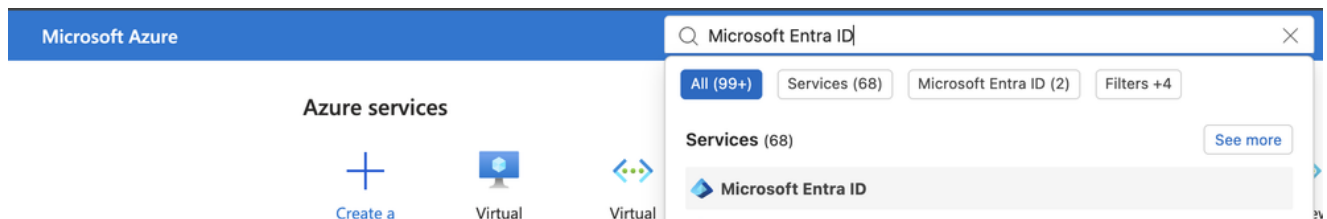
このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

設定

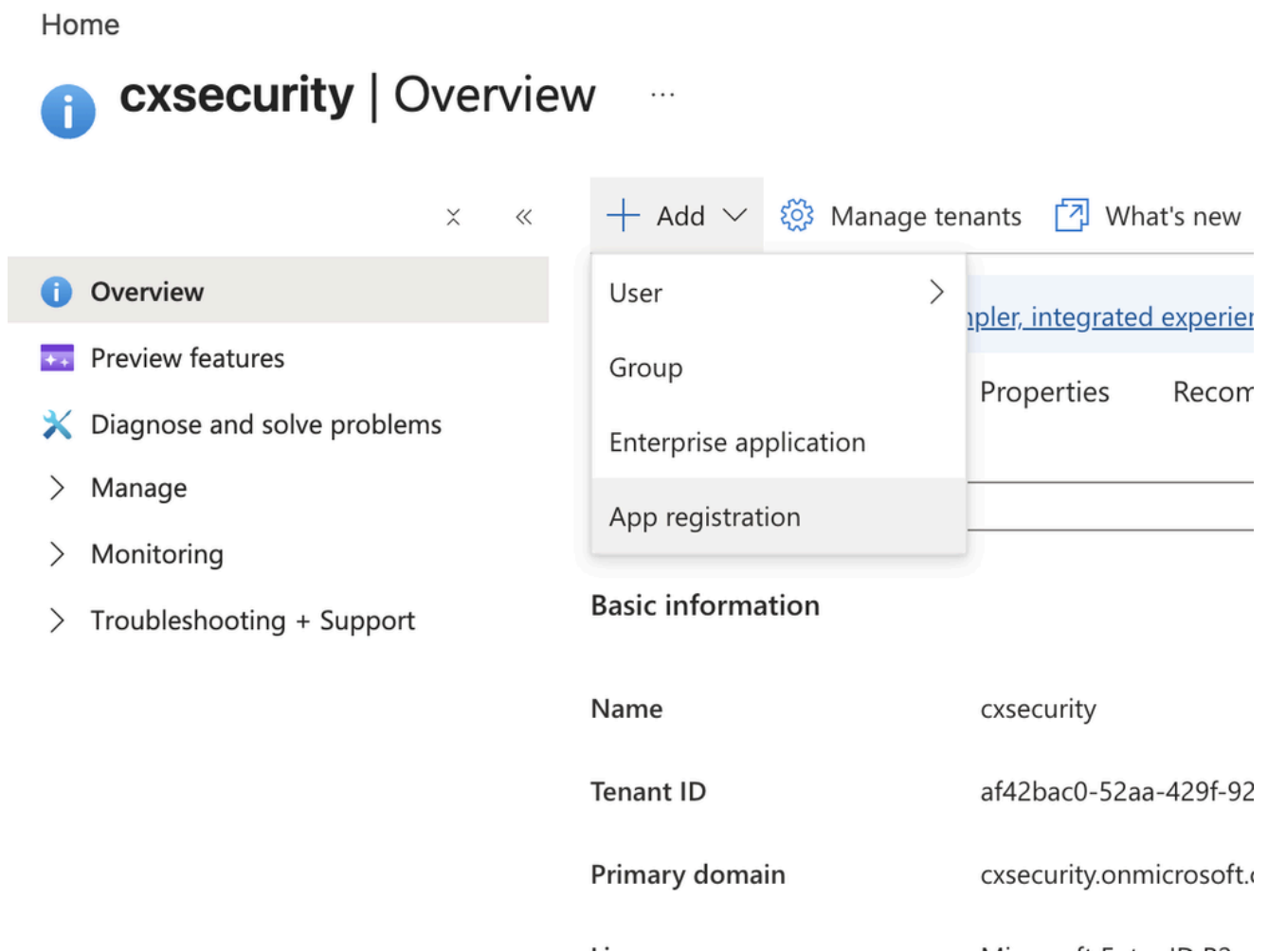
Microsoft Azureを準備し、AzureアカウントをMCDに接続して、FTDv Gatewayをデプロイするには、次の手順を使用します。

アプリケーションの登録

1. Azureポータルの検索バーでMicrosoft Entra IDに移動します。



2. Addをクリックし、App registrationを選択します。



3. Register an applicationフォームで、次の値を入力します。

- Name : アプリケーションの識別しやすい名前。
- サポートされているアカウントの種類 : 環境に最適なオプションを選択します。このドキュメントでは、シングルテナントのみを使用します。

Register an application ...

* Name

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

Supported account types

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

[Help me choose](#)

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

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 (オプション) には、ご使用の環境に適したオプションを選択します。このドキュメントでは、リダイレクトURIは設定しません。

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.

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

5. [Register] をクリックします。
6. アプリケーションを登録すると、概要ページが表示されます。アプリケーション (クライアント) IDとディレクトリ (テナント) IDをコピーしてメモ帳に保存します。

Multicloud Defense Controller ...

[Deactivate](#) [Delete](#) [Endpoints](#)

Overview

[Quickstart](#)[Integration assistant](#)[Diagnose and solve problems](#)[Manage](#)[Support + Troubleshooting](#)

Essentials

Display name : [Multicloud Defense Controller](#)

Application (client) ID : e5e0d63d-6f62-4f99-aaed-2eabd850cf72

Object ID : ec1746e4-bd16-4a00-aa7d-3b8e7e52496a

Directory (tenant) ID : af42bac0-52aa-429f-92db-925819967d17

Supported account types : [My organization only](#)

Client credentials : [Add a certificate or secret](#)

Redirect URIs : [Add a Redirect URI](#)

Application ID URI : [Add an Application ID URI](#)

Managed application in : [Multicloud Defense Controller](#)

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. アプリケーションページの左側のナビゲーションから、Manage > Certificates & secretsの順に選択します。



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 registration



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

Get Started

Documentation

The Microsoft

8. New client secretをクリックします。

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. Add a client secretページで、次の値を入力してから、Addをクリックします。

- Description : クライアントシークレットの適切な説明。
- Expires : ドロップダウンメニューから、環境に最適なオプションを選択します。



注：現在のシークレットの有効期限が切れたときに、新しいシークレットを作成する必要があります。

Copilot

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

Add a client secret

Description

swesnitz-mcd-secret

Expires

Recommended: 180 days (6 months)

10. ValueとSecret IDの両方をコピーし、メモ帳に保存します。



警告：シークレット値は作成時にのみ表示できます。

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]



ヒント：クライアントシークレットが[値]列に表示されます。

カスタムロールの作成

1. Azureポータルを検索バーで、[サブスクリプション]に移動します。

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. サブスクリプションをクリックします。

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. Access control (IAM)をクリックします。

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...

Subscription

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

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をクリックし、ドロップダウンメニューからAdd custom roleを選択します。

azure (cxsecurity)

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

Subscription

Search

Overview

Activity log

Access control (IAM)

Tags

+ Add

Download role assignments

Edit

Add role assignment

Add custom role

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

5. 次の値を入力してください。

- カスタムロール名：カスタムロールの識別しやすい名前。
- 説明：ロールの説明。
- ベースラインアクセス許可:Start from scratchオプションボタンが選択されていない場合は、これをクリックします。

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

注：指定したJSONは、[権限]タブではなく、カスタムロールに権限を割り当てます。

6. JSONをクリックします。
7. [Edit] をクリックします。
8. 次のコードブロックをactionの角括弧内に貼り付けます。

```
"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 }
```



注:JSONコードブロックの正しい間隔とタブを確認してください。

完成したロール定義の例を示します。

```

{
  "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/*",

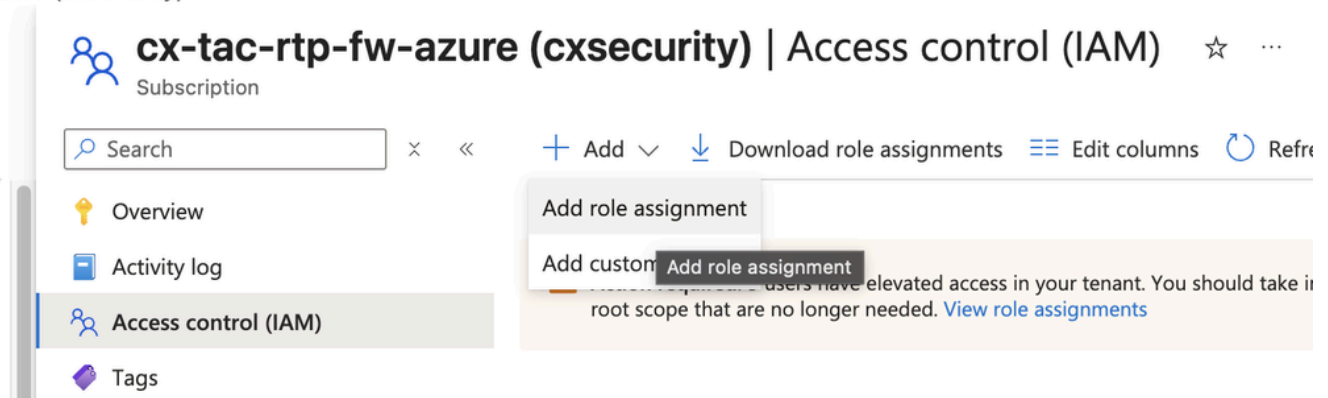
```

```
"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",
...
```

カスタムロールの割り当て

1. Subscription Access control (IAM)ページで、Add role assignmentをクリックします。

zure (cxsecurity)



2. 「カスタムロールの作成」セクションで作成したロールを検索します。

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をクリックし、Assign accessをUser、group、またはservice principalに設定したまま

にします。

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

4. Select membersをクリックします。

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

5. 「カスタムロールの作成」セクションで作成したロールを追加します。

Select members



 Multi 



Multicloud - Azure - RTP
Application



Multicloud Defense Controller
Application

Selected members:



Multicloud Defense Controller
Application



6. Nextをクリックして、サブスクリプションIDをコピーします。

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 + assignをクリックします。

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	

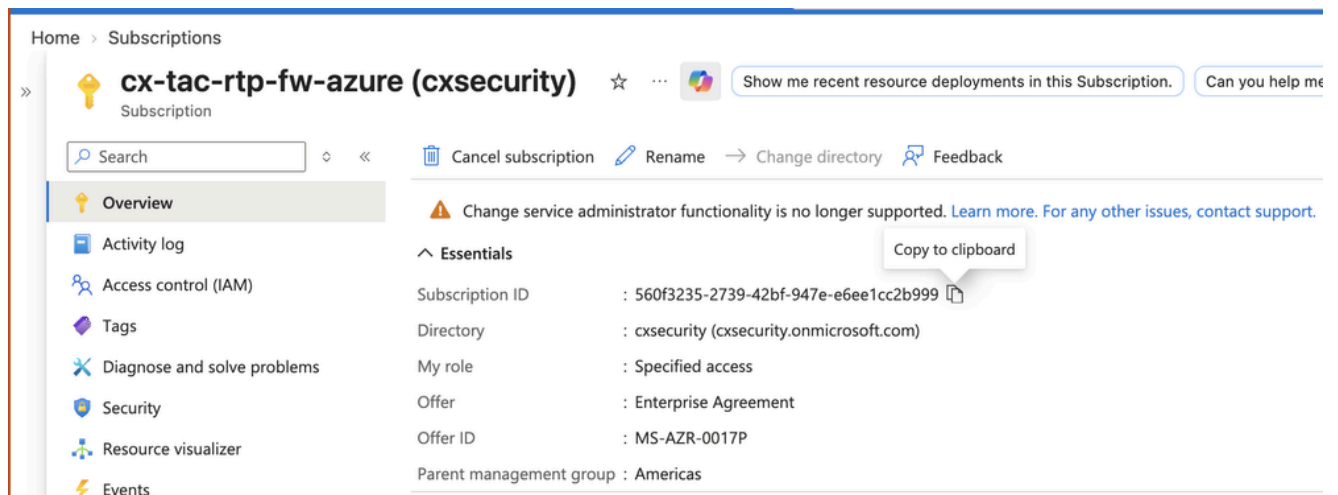
Review + assign

Review + assign

Previous

Next

- サブスクリプションの概要ページが表示されます。左側のメニューからOverviewに移動し、サブスクリプションIDをコピーします。



これで、AzureアカウントをMCDに追加するためのAzureの前提条件が完了しました。これらの手順では、MCDを使用した統合と展開について説明します。

AzureアカウントをMCDに接続する

1. SCC > Multicloud Defenseの順に移動します。



Security Cloud Control



Organization
cisco-swesnitz



Home

Products



Firewall



Multicloud Defense

Platform services



Favorites



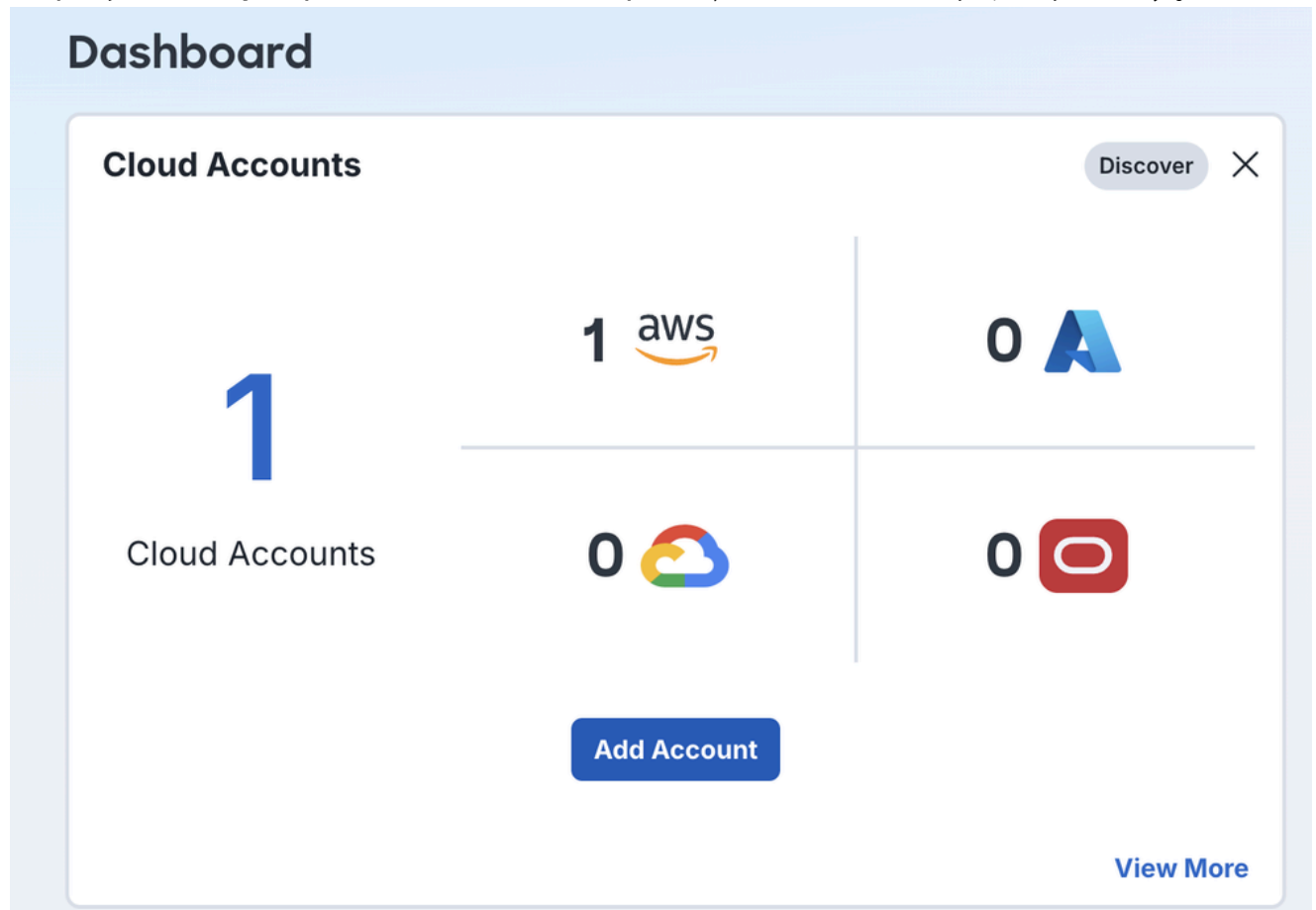
Security Devices



Platform Management



2. メインダッシュボードのCloud Accountsペインで、Add Accountをクリックします。



3. Azureアイコンをクリックします。

Select Your Cloud Account

Please select Account Type you want to set up



Close Back

4. [Azureアカウントへの接続]ページで、次の値を入力します。

- Azureアカウント名: MCDの観点からのAzureアカウントの名前。
- ディレクトリID: 「アプリケーションの登録」セクションで保存したディレクトリID。
- サブスクリプションID: カスタムロールの割り当てセクションで保存したサブスクリプションID。
- アプリケーションID: 「アプリケーションの登録」セクションで保存したアプリケーションID。
- Client Secret : アプリケーションの登録セクションで保存した値。

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は、Azureアセットを検出して表示します。[next] をクリックします。

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

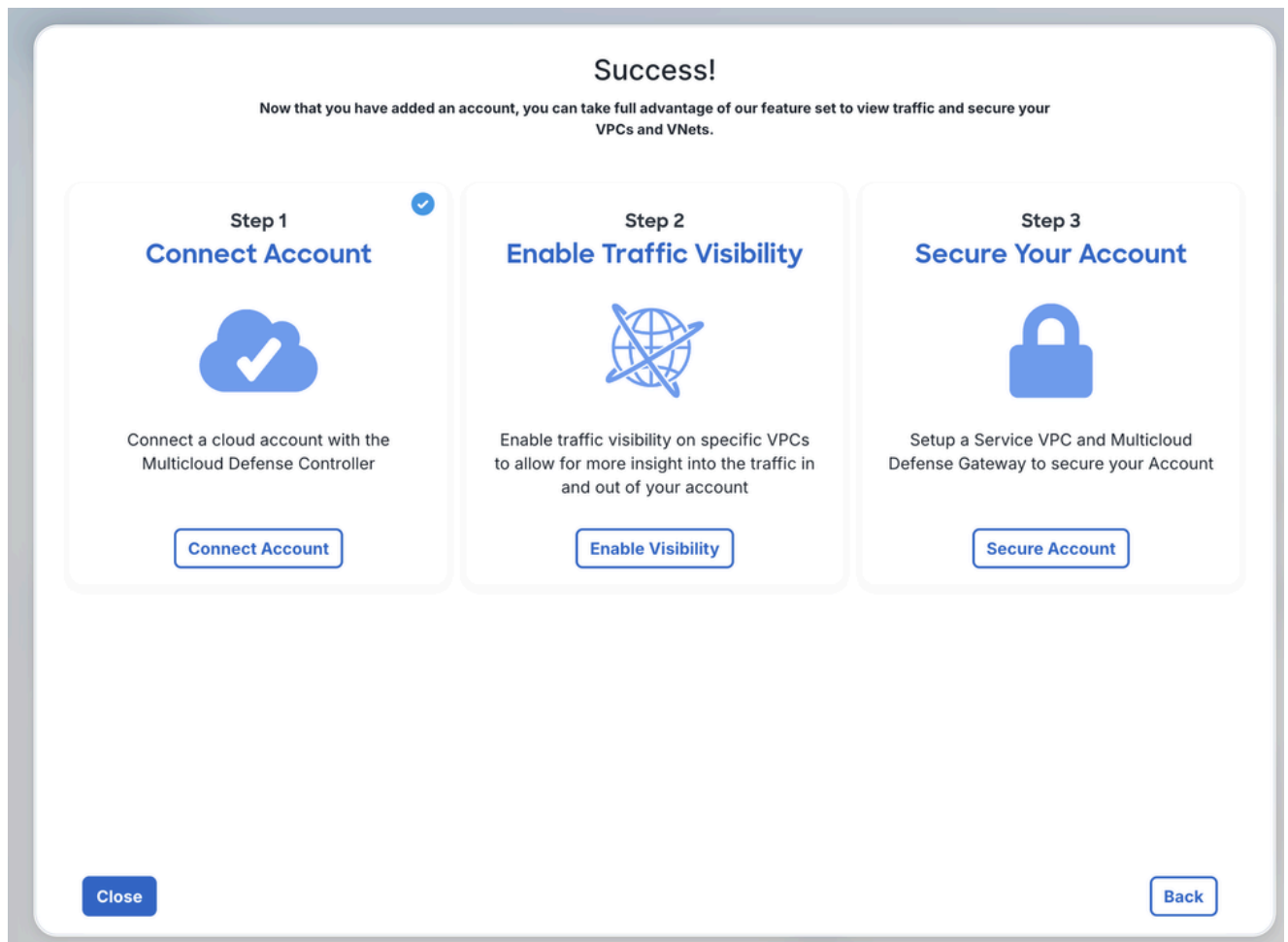
-
Applications

-
Certificates

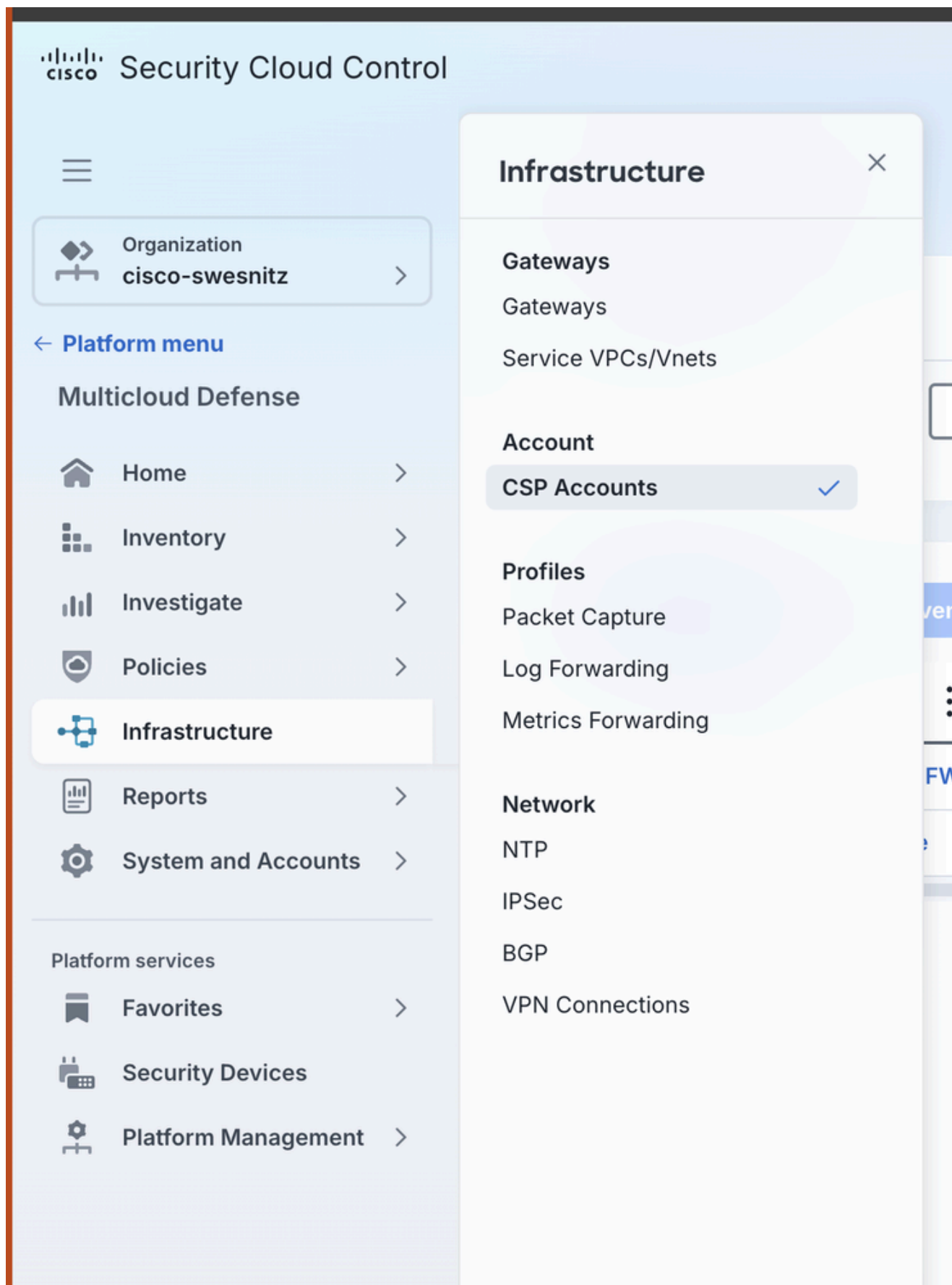
Cancel

BackNext

6. [Close] をクリックします。

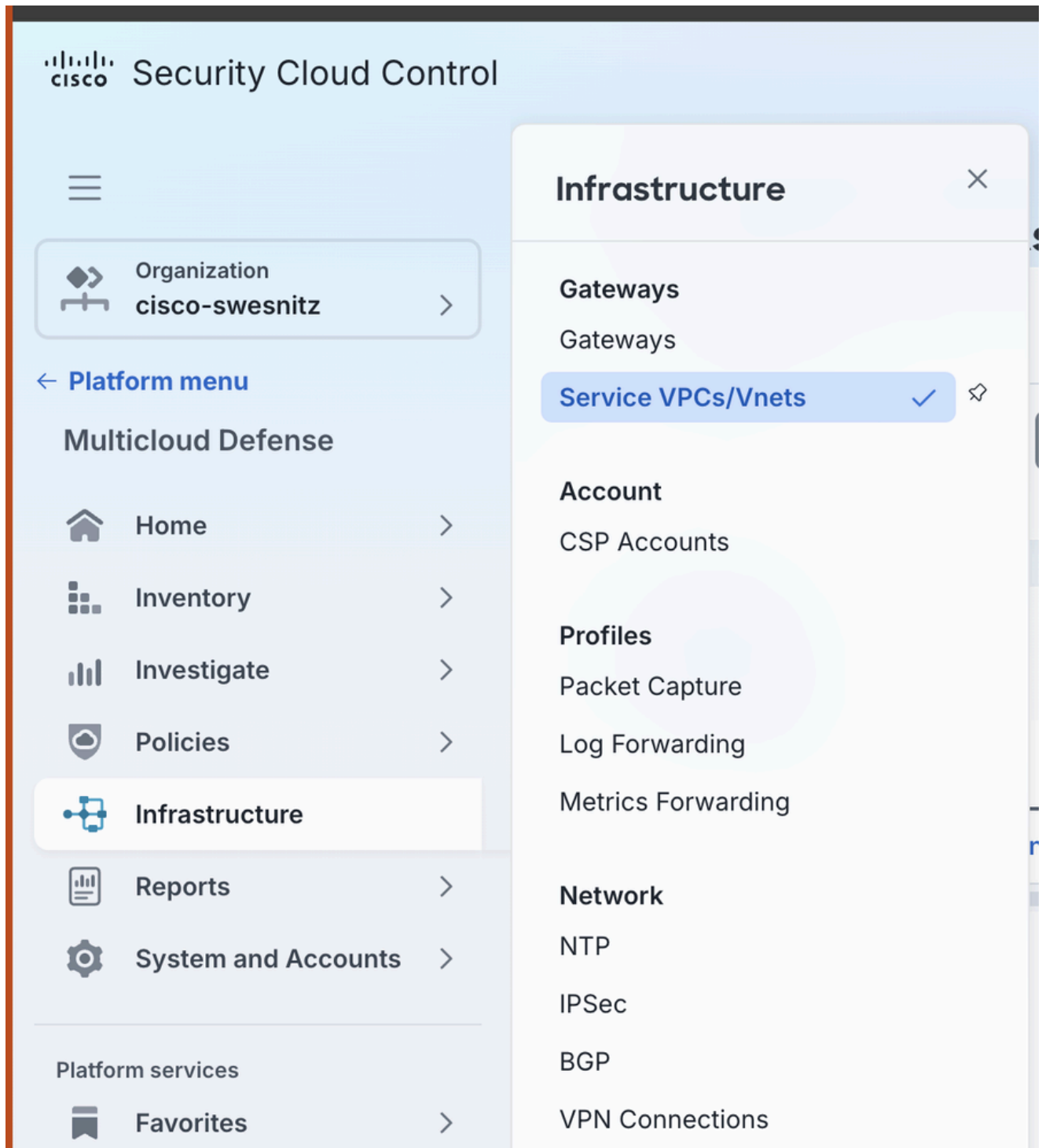


7. これで、オンボーディングされたアカウントをInfrastructure > CSP Accountsから表示できるようになりました。



VNetの作成

1. Infrastructure > Service VPCs/VNetsの順に移動します。



2. [Create] をクリックします。

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. 次の値を入力してください。

- Name：この手順でFTDvゲートウェイに対して作成される、VNetの簡単に識別できる名前。
- CSPアカウント：[AzureアカウントをMCDに接続する]セクションで割り当てた名前。
- リージョン：FTDvゲートウェイが導入されているリージョン。
- CIDRブロック：VNetに関連付けられた中継ゲートウェイ用の一意のIPブロック。
- 可用性ゾーン：復元力を確保するには、少なくとも2つの可用性ゾーンを選択します。
- Resource Group：ドロップダウンメニューから+ Create Resource Groupを選択します。
- リソースグループ名：リソースグループの名前。
- リソースグループリージョン：「リージョン」で選択したリージョンに合わせたリージョン。

[Save] をクリックします。

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. 成功のメッセージが表示されます。

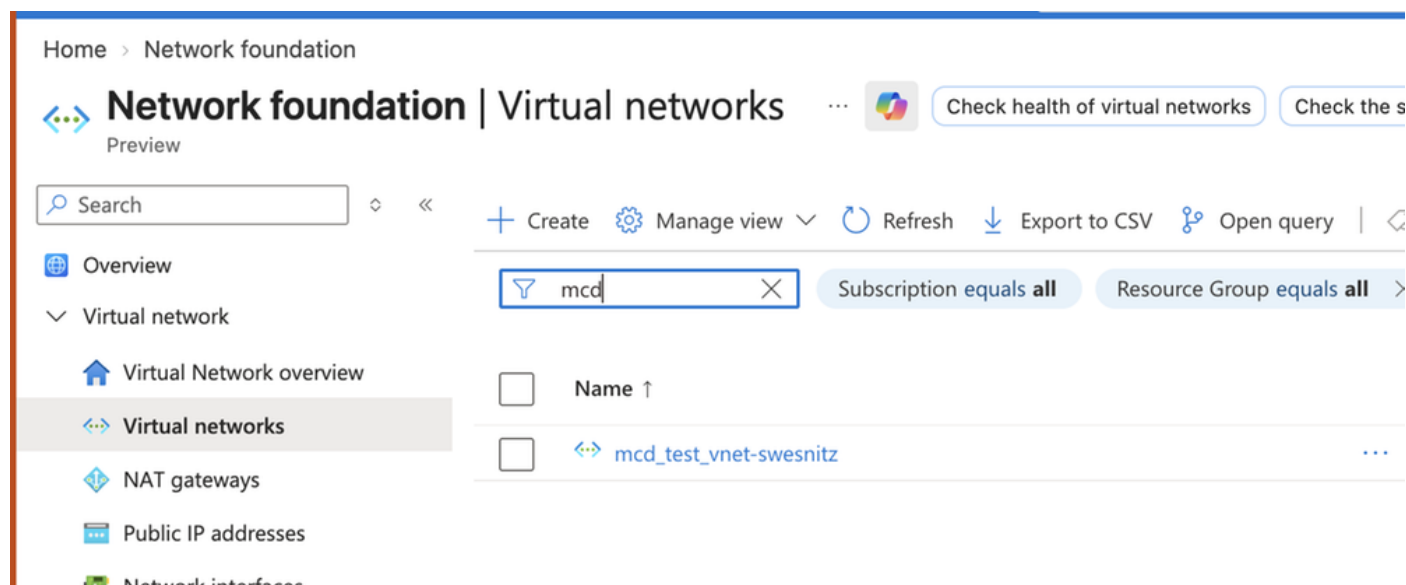
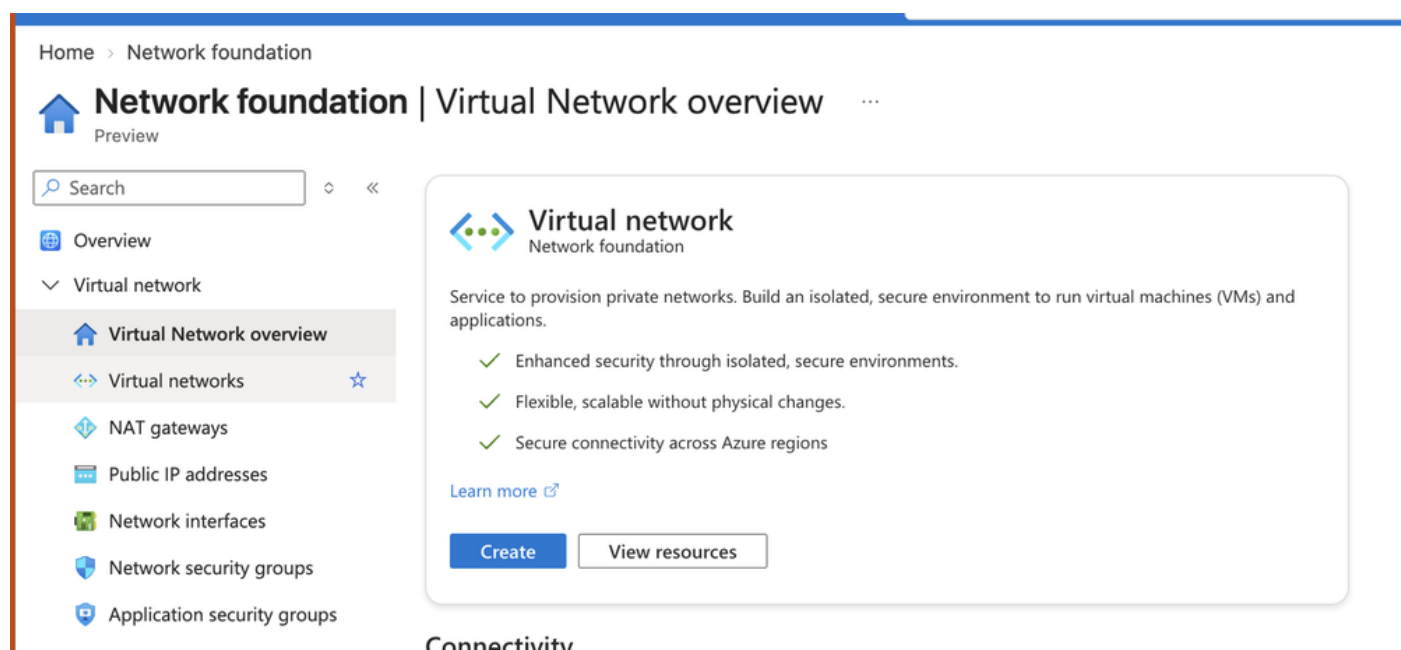


Success

Service VPC/VNet created successfully.

OK

Azure側からVNetの作成を確認し、Network foundation > Virtual networks overview > Virtual Networksの順に選択します。

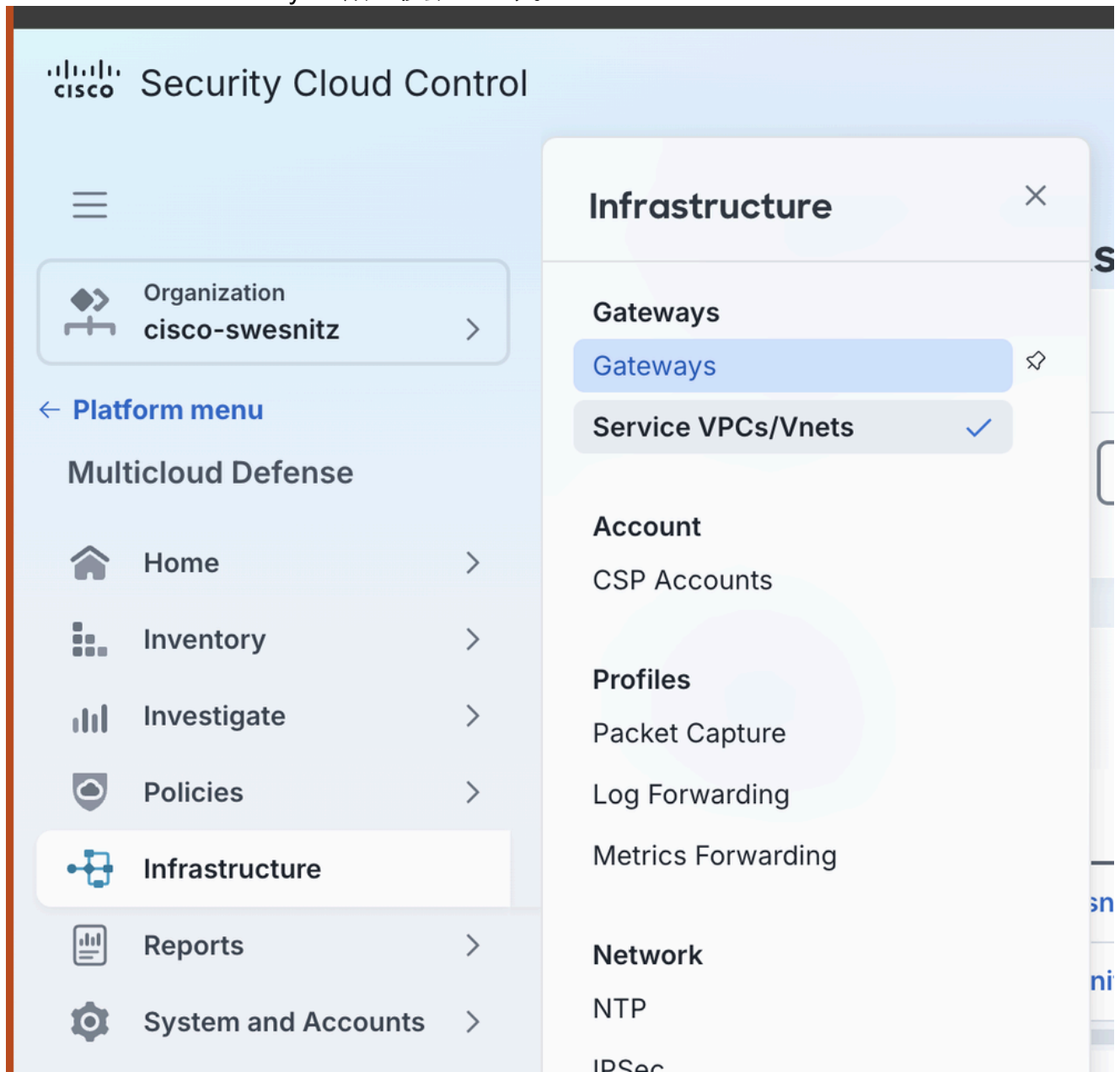


VNetは、作成されるとアクティブ状態に移行します。

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 Gatewayの作成

1. Infrastructure > Gatewaysの順に移動します。



2. Add Gatewayをクリックします。

Gateways: 1

Quick Filters Advanced

Name CSP Account

Add Gateway Actions Recommended

	Name ↓↑	State ▼
☐	med lab cluster	ACTIVE

3. 次の値を入力してください。

- アカウント：ドロップダウンメニューから、「AzureアカウントをMCDに接続する」セクションでリンクしたAzureアカウントを選択します。
- Gateway Type:FTDv Gatewayを選択します。
- Name:FTDvゲートウェイの簡単に識別できる名前。
- インスタンスタイプ：環境に適したインスタンスタイプ。
- 最小インスタンス：ドロップダウンメニューから少なくとも1つのインスタンスを選択します。
- 最大インスタンス数：環境に必要な最大FTDvインスタンス数。許容される最大値は10です。
- HealthCheck Port：デフォルトは65534です。このドキュメントでは、この値を変更しません。

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

注:HealthCheck Portは、インスタンスの健全性を確認するためにマルチクラウド防御ロードバランサが使用するポート番号です。インスタンスに割り当てられたデータパスセキュリティグループは、このポートでのトラフィックを許可する必要があります。

4. 次の値を入力してください。

- Properties:EgressまたはEast-Westを選択します。
- FTDv Version：環境に最も適したソフトウェアバージョン。
- ポリシールールセット：このFTDvクラスタに適用するアクセスコントロールポリシー (ACP)。

- Password:FTDvインスタンスのパスワード。
- ライセンスモデル：目的のライセンスモデル。
- パフォーマンス層：期待されるデバイススループットに適した層。
- ライセンスタイプ：この導入用に購入したライセンスタイプ。
- リージョン：これらのFTDvインスタンスがデプロイされているリージョン。
- VPC/VNet ID:「VNetの作成」セクションで作成したサービス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. 公開キーペアを作成します。手順については、「[WindowsでのSSHキーペアの作成](#)」を参照してください。

```

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. SSH公開キーとリソースグループの値を入力します。

Create Gateway

SSH Public Key

SSH Key Pair

SSH Public key *

ssh-rsa
AAAAAB3NzaC1yc2EAAAADAQABAAQChvSlgyD
Kk+X6zGCgM3AxV3iPcxZIF7QtWB7WiagDgo+IRKcH
cPNUofBzsgvIOSuP1mYf6LZQp6Xdhk/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. パブリックIPを無効にしてから、Nextをクリックします。

Create Gateway

✓

✓

3

4

Gateway InformationGateway DetailsAdvanced SettingsReview

Public IP

☒ Disable Public IP

8. 指定したすべての値を確認します。

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. 値を確認し、リソースのロードが完了したら、Finishをクリックします。

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

リソースがロードされた後のダッシュボードビュー。

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



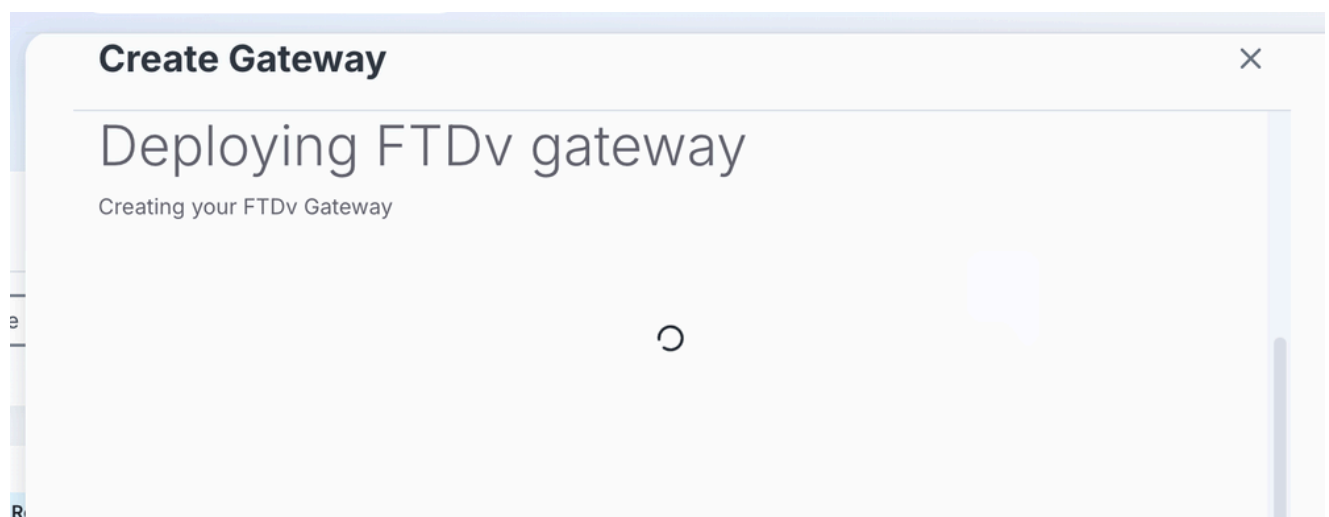
Resource	Limit	In Use	Min Usage for Gateway	Max Usage for Gateway	Recommendation
Private IPs in Subnets	254	0	1	3	
Elastic IPs	1000	51	1	3	
Load Balancers	1000	8	1	1	
Instances	25000	31	2	6	
Virtual CPUs	350	0	16	48	

Advanced Settings

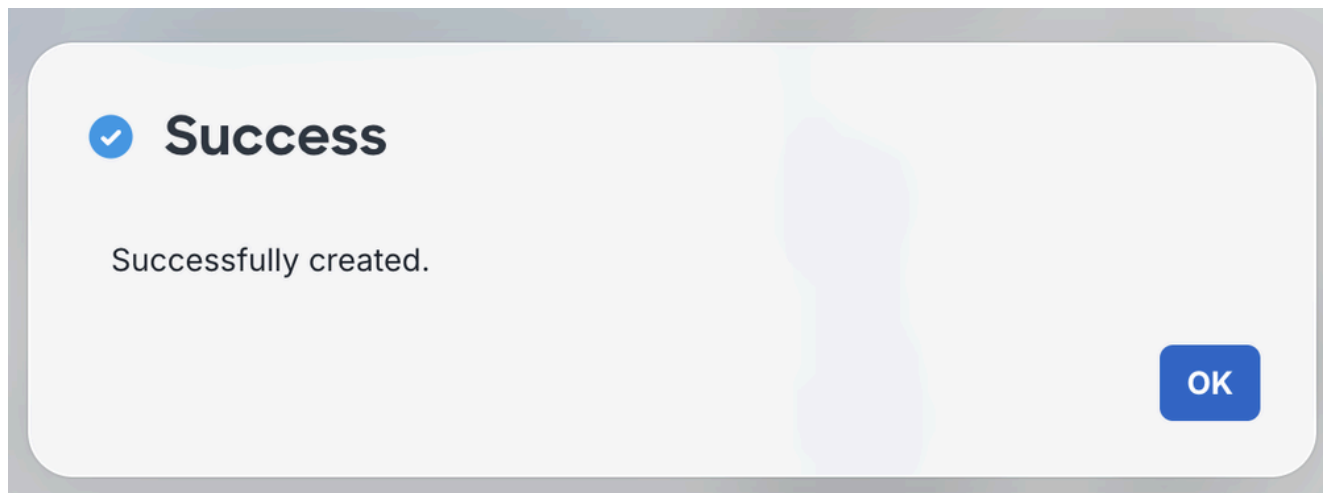
[Edit](#)**Disable Public IP**

enabled

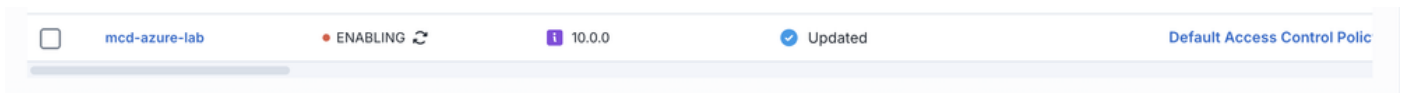
ゲートウェイ導入のダッシュボードビュー。



- ゲートウェイの作成が開始されると、成功を示すメッセージが表示されます。[OK] をクリックします。



MCDダッシュボードでは、ステータスにENABLINGが表示されます。



SummaryタブとInstancesタブでステータスを監視します。

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

確認

ここでは、設定が正常に機能しているかどうかを確認します。

- AzureのCompute > Virtual machinesの下で、FTDvインスタンスを監視します。ステータスがCreatingからRunningに変わります。

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ダッシュボードからゲートウェイステータスを確認します。

[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.

関連情報

- [サービスVPCまたはVNetの作成](#)
- [FTDv統合手順](#)
- [ゲートウェイの前提条件の設定](#)
- [Azure向けマルチクラウド防御の概要](#)
- [AzureでLinux VM用のSSH公開/秘密キーペアを作成して使用する](#)
- [テクニカル サポートとドキュメント – Cisco Systems](#)

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせ、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。