

Een FTDv-gateway implementeren in Azure met behulp van MCD

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Configureren](#)

[Een aanvraag registreren](#)

[Een aangepaste rol maken](#)

[De aangepaste rol toewijzen](#)

[Verbind de Azure-account met MCD](#)

[Een VNet maken](#)

[De Azure MCD FTDv-gateway maken](#)

[Verifiëren](#)

[Gerelateerde informatie](#)

Inleiding

In dit document wordt beschreven hoe u de Microsoft Azure-vereisten configureert en een Firewall Threat Defense Virtual (FTDv)-gateway implementeert via MCD.

Voorwaarden

- Een Azure-abonnement dat is aangeschaft en geregistreerd en dat is gekoppeld aan Microsoft Entra ID. Bevestig dit in de lijst met App-registraties in de Azure-portal.
- Een aangepaste rol die is gemaakt voor het Azure-abonnement waarmee Multicloud Defense (MCD) toegang krijgt tot de specifieke bronnen en acties die anders zijn geblokkeerd.
- Een abonnement op het Azure Event Grid, zodat MCD realtime updates kan ontvangen van het Azure-abonnement.
- Het Azure-abonnement is verbonden met de Multicloud Defense Controller vanaf het MCD-dashboard.
- De Cisco Marketplace-voorwaarden worden geaccepteerd in Azure, als dit de eerste keer is dat het Azure-account wordt geactiveerd naar MCD.

- (Optioneel) Een door de gebruiker toegewezen beheerde identiteit is geconfigureerd als u Key Vault- of Blob Storage-toegang nodig hebt.
- Een nieuwe service van VNet. VNets die zijn gemaakt voordat FTDv-gatewayondersteuning werd geïntroduceerd, kunnen niet worden gebruikt voor een FTDv-gatewayimplementatie.
- Een actief abonnement op het Cloud-Delivered Firewall Management Center (cdFMC), dat het toegangscontrolebeleid voor het FTDv-apparaat beheert.
- Ten minste één FTDv-licentie gekocht via uw Cisco-verkoper of -partner.

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Navigatie van de Microsoft Azure-portal
- Microsoft Entra ID (Azure AD) applicatie registratie en role-based access control (RBAC)
- Cisco Multicloud Defense (MCD)
- Cisco Secure Firewall Threat Defense Virtual (FTDv)

Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies.

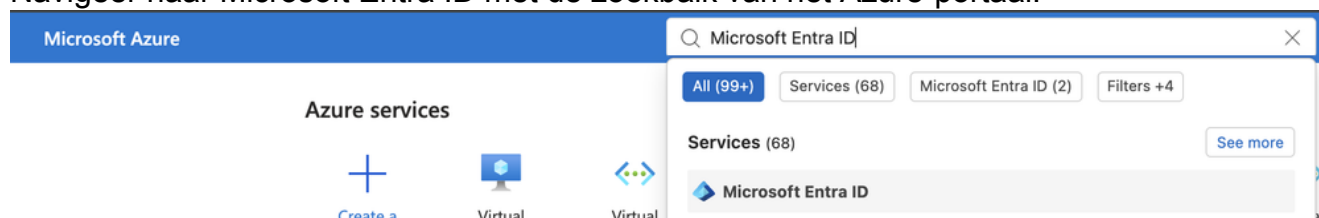
De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Configureren

Gebruik deze procedures om Microsoft Azure voor te bereiden, uw Azure-account aan MCD te koppelen en een FTDv-gateway te implementeren.

Een aanvraag registreren

1. Navigeer naar Microsoft Entra ID met de zoekbalk van het Azure-portaal.



2. Klik op Toevoegen en selecteer vervolgens App-registratie.

Home

cxsecurity | Overview ...

Overview

Preview features

Diagnose and solve problems

> Manage

> Monitoring

> Troubleshooting + Support

+ Add ▾

Manage tenants

What's new

User

Group

Enterprise application

App registration

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

3. Voer de volgende waarden in op het aanvraagformulier registreren:

- Naam: Een gemakkelijk identificeerbare naam voor de toepassing.
- Ondersteunde accounttypen: Selecteer de optie die het beste bij uw omgeving past. In dit document wordt alleen gebruikgemaakt van één huurder.

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](#)

Communicating 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. Kies voor Redirect URI (optioneel) de optie die geschikt is voor uw omgeving. Dit document configureert geen omleidings-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.

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

5. Klik op Registreren.
6. Nadat u de aanvraag hebt geregistreerd, verschijnt de overzichtspagina. Kopieer en sla de Application (client) ID en de Directory (tenant) ID op een notitieblok.

The screenshot shows the 'Overview' page for the 'Multicloud Defense Controller' application. The page includes a search bar, navigation links (Quickstart, Integration assistant, Diagnose and solve problems, Manage, Support + Troubleshooting), and a list of essentials. The essentials section displays the following information:

Field	Value	Action
Display name	Multicloud Defense Controller	
Application (client) ID	e5e0d63d-6f62-4f99-aaed-2eabd850c772	
Object ID	ec1746e4-bd16-4a00-aa7d-3b8e7e52496a	
Directory (tenant) ID	a442bac0-52aa-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 L...	Multicloud Defense Controller	
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. Ga in de linkernavigatie van de toepassingspagina naar Beheren > Certificaten en geheimen.



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](#)

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

Object ID : ec1746e4-bd16-4a

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

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



Welcome to the new and improved App reg



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

Get Started

Documentation

The Mi

8. Klik op Nieuw clientgeheim.



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. Voer op de pagina Een clientgeheim toevoegen deze waarden in en klik vervolgens op Toevoegen:
- Beschrijving: Een passende beschrijving voor het cliëntgeheim.
 - Verloopt: Kies in het vervolgkeuzemenu de optie die het beste bij uw omgeving past.



Opmerking: u moet een nieuw geheim maken wanneer het huidige geheim verloopt.

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

Add a client secret

Description

swesnitz-mcd-secret

Expires

Recommended: 180 days (6 months)

10. Kopieer en sla zowel de Waarde als de Geheime ID op in een notitieblok.



Waarschuwing: je kunt de geheime waarde alleen bekijken op het moment van creatie.

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

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

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

+ New client secret

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

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



Tip: Het clientgeheim wordt vermeld in de kolom Waarde.

Een aangepaste rol maken

1. Navigeer naar Abonnementen met de zoekbalk van het Azure-portaal.

Microsoft Azure

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

Create a custom role ...

sub

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

Services (19) See more

Subscriptions

2. Klik op je abonnement.

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. Klik op Toegangsbeheer (IAM).

Microsoft Azure

Search resources, services, and docs (G+)

Home > Subscriptions

Subscriptions

cxsecurity (cxsecurity.onmicrosoft.com)

+ Add Manage Policies ...

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

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

Search for any field...

Subscriptions

My role

Status

Administrators

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

Subscription

Search

Cancel subscription Rename Change directory

Change service administrator functionality is no longer supported

Essentials

Subscription ID	: 560f3235-2739-42bf-947e-e6ee1cc2b
Directory	: cxsecurity (cxsecurity.onmicrosoft.com)
My role	: Specified access
Offer	: Enterprise Agreement
Offer ID	: MS-AZR-0017P
Parent management group	: Americas

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Security

Resource visualizer

Events

4. Klik op Toevoegen en selecteer Aangepaste rol toevoegen in het vervolgkeuzemenu.

azure (cxsecurity)

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

Subscription

Search

+ Add Download role assignments Edit

Overview

Activity log

Access control (IAM)

Tags

Add role assignment

Add custom role

users have elevated access in your tenant at the root scope that you can manage. [View role assignments](#)

5. Voer de volgende waarden in:

- Aangepaste rolnaam: een gemakkelijk identificeerbare naam voor de aangepaste rol.
- Beschrijving: Een beschrijving van de rol.
- Basislijnmachtigingen: Klik op de knop Start from scratch als deze nog niet is geselecteerd.

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

Opmerking: De JSON die u opgeeft, niet het tabblad Rechten, wijst machtigingen toe aan de aangepaste rol.

6. Klik op JSON.
7. Klik op Edit (Bewerken).
8. Plak dit codeblok binnen de vierkante haakjes voor acties:

```
"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 }
```



Opmerking: Controleer de juiste afstand en tabbladen voor het JSON-codeblok.

Dit is een voorbeeld van de voltooide roldefinitie:

```

{
  "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/*",

```

```

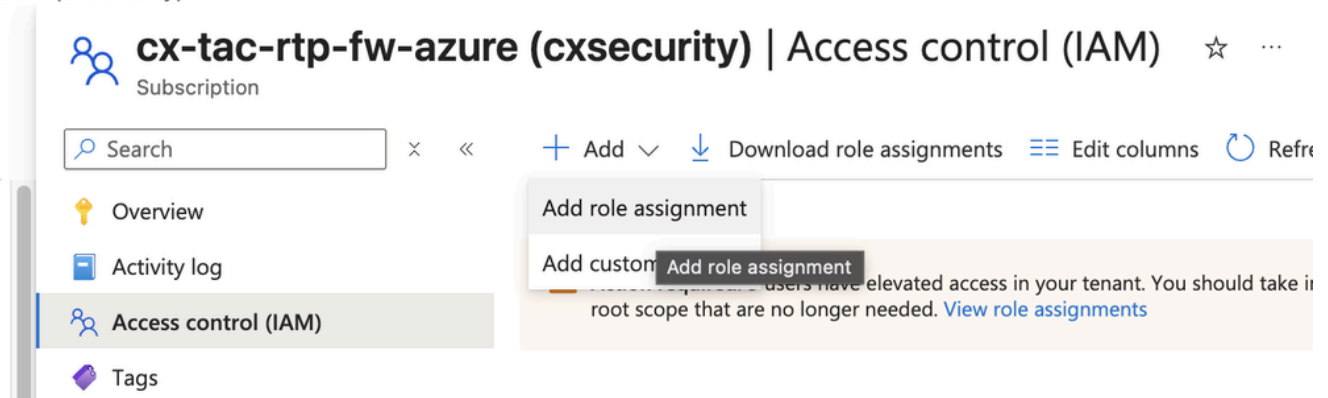
"Microsoft.Network/routeTables/*",
"Microsoft.Network/virtualNetworks/*",
"Microsoft.Network/virtualNetworks/subnets/*",
"Microsoft.Resources/subscriptions/resourcegroups/*",
"Microsoft.Storage/storageAccounts/blobServices/*",
"Microsoft.Storage/storageAccounts/listkeys/action",
"Microsoft.Network/networkWatchers/*",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

```

De aangepaste rol toewijzen

1. Klik op de pagina Toegangsbeheer voor abonnementen (IAM) op Roltoewijzing toevoegen.

zure (cxsecurity)



2. Zoek naar de rol die u hebt gemaakt in het gedeelte Aangepaste rol maken.

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. Klik op Volgende en laat Toegang toewijzen aan ingesteld op Gebruiker, groep of

servicepresident.

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. Klik op Leden selecteren.

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. Voeg de rol toe die u hebt gemaakt in het gedeelte Aangepaste rol maken.

Select members



 Multi 



Multicloud - Azure - RTP
Application



Multicloud Defense Controller
Application

Selected members:



Multicloud Defense Controller
Application



6. Klik op Volgende en kopieer de ID van het abonnement.

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. Klik op Beoordelen + toewijzen.

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	

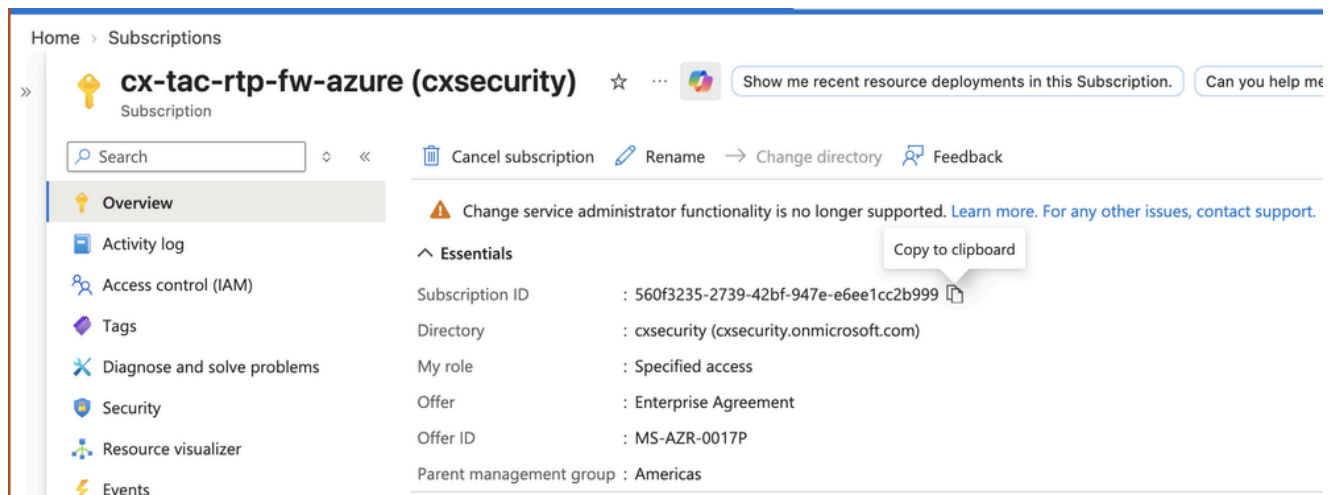
Review + assign

Review + assign

Previous

Next

8. De overzichtspagina voor het abonnement wordt weergegeven. Ga in het linkermenu naar Overzicht en kopieer de ID van het abonnement.



Hiermee worden de Azure-vereisten voltooid om het Azure-account aan MCD toe te voegen. Deze procedures beschrijven de integratie en implementatie via MCD.

Verbind de Azure-account met MCD

1. Navigeer naar SCC > Multicloud Defense.



Security Cloud Control



Organization
cisco-swesnitz



Home

Products



Firewall



Multicloud Defense

Platform services



Favorites



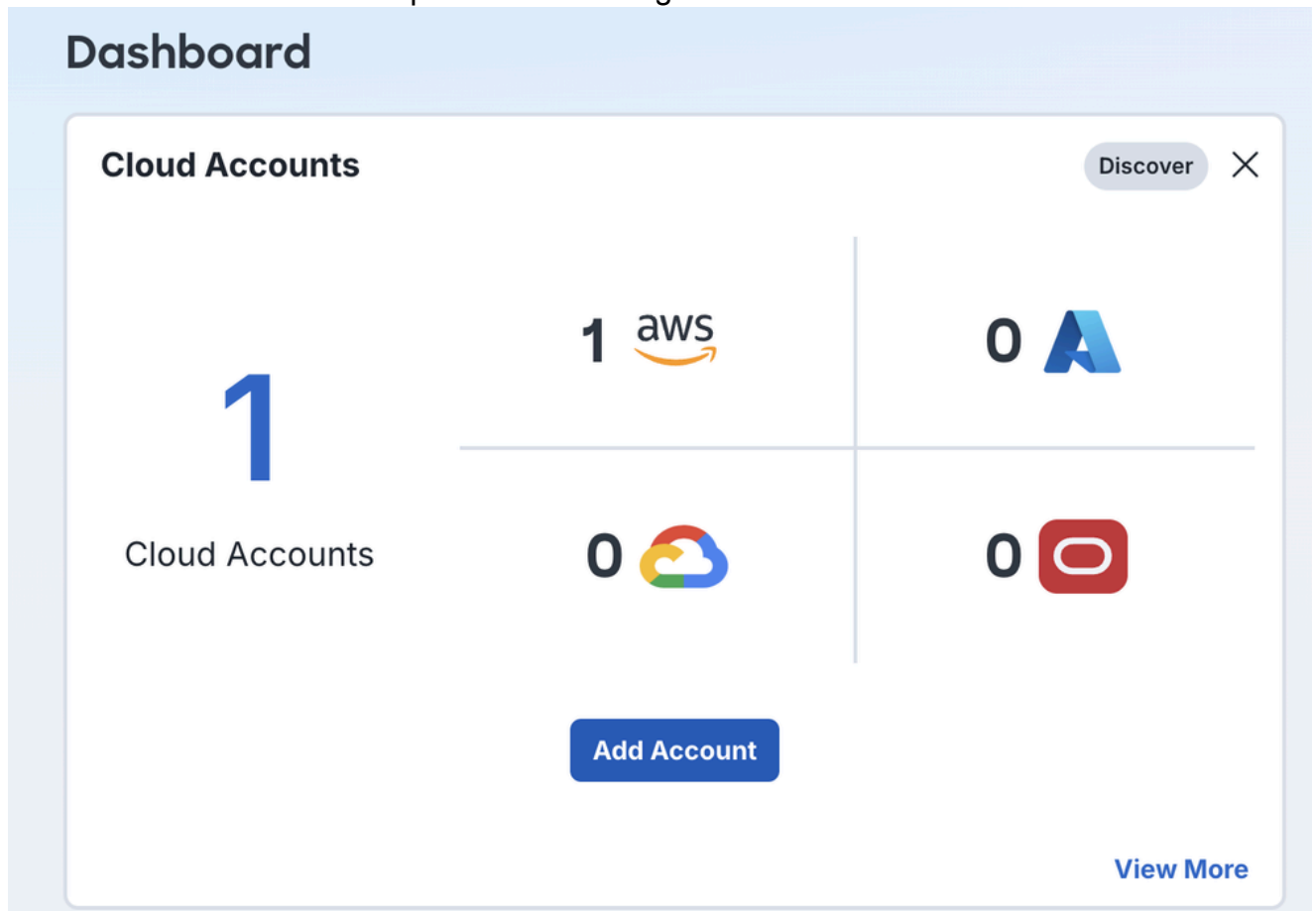
Security Devices



Platform Management



2. Klik in het hoofddashboard op Account toevoegen in het deelvenster Cloud Accounts.



3. Klik op het Azure icoon.

Select Your Cloud Account

Please select Account Type you want to set up









Close

Back

4. Voer op de pagina Verbind uw Azure-account de volgende waarden in:
- Azure-accountnaam: de naam van het Azure-account vanuit het MCD-perspectief.
 - Directory-ID: de directory-ID die u hebt opgeslagen in het gedeelte Een toepassing registreren.
 - Abonnement-ID: de abonnement-ID die u hebt opgeslagen in het gedeelte Aangepaste rol toewijzen.
 - Applicatie-ID: de applicatie-ID die u hebt opgeslagen in het gedeelte Een toepassing registreren.
 - Clientgeheim: de waarde die u hebt opgeslagen in het gedeelte Een toepassing registreren.

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 ontdekt en toont de Azure-elementen. Klik op Next (Volgende).

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

CancelBackNext

6. Klik op Close (Sluiten).

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. U kunt de onboarding account nu bekijken vanuit Infrastructure > CSP Accounts.



Organization
cisco-swesnitz >

< Platform menu

Multicloud Defense



Home >



Inventory >



Investigate >



Policies >



Infrastructure



Reports >



System and Accounts >

Platform services



Favorites >



Security Devices



Platform Management >

Infrastructure ×

Gateways

Gateways

Service VPCs/Vnets

Account

CSP Accounts ✓

Profiles

Packet Capture

Log Forwarding

Metrics Forwarding

Network

NTP

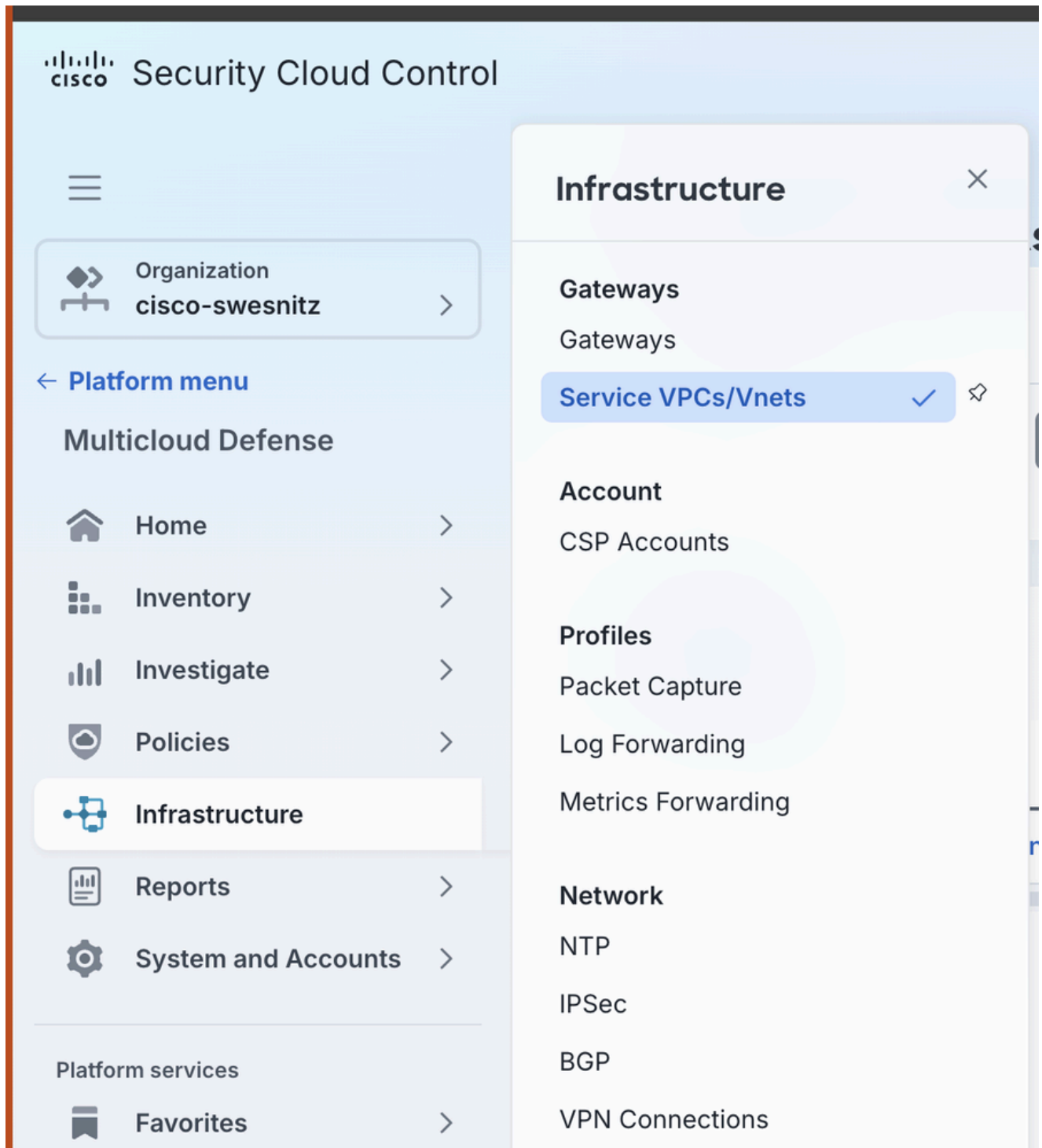
IPSec

BGP

VPN Connections

Een VNet maken

1. Navigeer naar Infrastructuur > Service-VPC's/VNets.



2. Klik op Maken.

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. Voer de volgende waarden in:

- Naam: Een gemakkelijk identificeerbare naam voor de VNet die deze procedure maakt voor de FTDv Gateway.
- CSP-account: de naam die u hebt toegewezen in het gedeelte Azure-account verbinden met MCD.
- Regio: De regio waar de FTDv Gateway wordt geïmplementeerd.
- CIDR-blok: een uniek IP-blok voor de transit-gateway die is gekoppeld aan de VNet.
- Beschikbaarheidszones: Selecteer ten minste twee beschikbaarheidszones voor veerkracht.
- Bronnengroep: Selecteer + Bronnengroep maken in het vervolgkeuzemenu.
- Naam brongroep: een naam voor de brongroep.
- Resource Group Region: De regio die is afgestemd op de regio die u hebt geselecteerd voor Region.

Klik op Save (Opslaan).

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. Er verschijnt een succesbericht.



Success

Service VPC/VNet created successfully.

OK

Bevestig de creatie van de VNet vanaf de Azure-kant, navigeer naar Netwerkbasis > Overzicht virtuele netwerken > Virtuele netwerken.

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 ↑

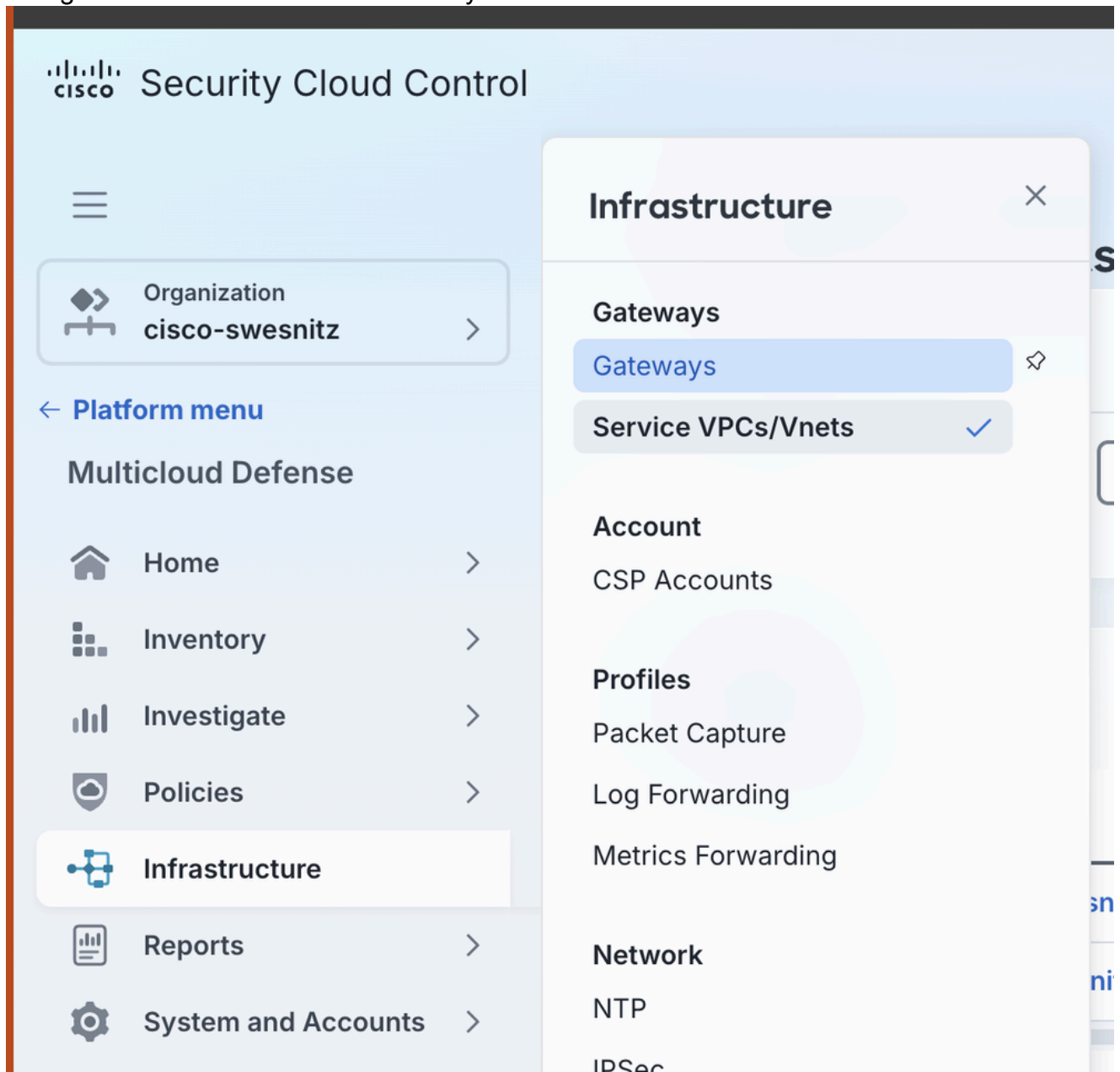
☐ mcd_test_vnet-swesnitz

De VNet gaat over naar een actieve staat zodra deze is gemaakt.

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

De Azure MCD FTDv-gateway maken

1. Navigeer naar Infrastructuur > Gateways.



2. Klik op Gateway toevoegen.

Gateways: 1

Quick Filters Advanced

Name CSP Account

Add Gateway Actions Recommended

	Name ↓↑	State ▼
--	---------	---------

3. Voer de volgende waarden in:

- Accounts: Selecteer in het vervolgkeuzemenu de Azure-account die u hebt gekoppeld in de sectie De Azure-account verbinden met MCD.
- Type gateway: Selecteer FTDv-gateway.
- Naam: Een gemakkelijk identificeerbare naam voor de FTDv Gateway.
- Instantietype: het instantietype dat geschikt is voor uw omgeving.
- Minimale instanties: selecteer ten minste één instantie in het vervolgkeuzemenu.
- Maximale instanties: het gewenste aantal maximale FTDv-instanties voor uw omgeving. Het maximaal toegestane aantal is 10.
- HealthCheck-poort: de standaardwaarde is 65534. Dit document wijzigt deze waarde niet.

Create Gateway

Gateway InformationGateway DetailsAdvanced SettingsReview

Properties

Accounts * ⓘ

cx-tac-rtp-fw-azureX v

Gateway Type *

FTDv GatewayX v

Name * ⓘ

mcd-azure-labX

Description

Optional

Instance Type * ⓘ

8 Virtual CPU | AZURE_D8S_V5X v

Minimum Instances * ⓘ

1v

Maximum Instances * ⓘ

3v

HealthCheck Port * ⓘ

65534X

Cancel

Next



Opmerking: de HealthCheck-poort is het poortnummer dat de Multicloud Defense-taakverdelers gebruikt om de status van de instanties te controleren. De beveiligingsgroepen voor het gegevenspad die aan de instanties zijn toegewezen, moeten verkeer op deze poort toestaan.

4. Voer de volgende waarden in:

- Eigenschappen: Selecteer Egress of Oost-West.
- FTDv-versie: de softwareversie die het meest geschikt is voor de omgeving.
- Beleidsregels: Het toegangscontrolebeleid (ACS) dat van toepassing is op dit FTDv-

cluster.

- Wachtwoord: Een wachtwoord voor de FTDv-instanties.
- Licentiemodel: het gewenste licentiemodel.
- Prestatielaag: de laag die geschikt is voor de verwachte doorvoer van het apparaat.
- Licentietypen: de licentietypen die voor deze implementatie zijn gekocht.
- Regio: De regio waar deze FTDv-instanties worden geïmplementeerd.
- VPC/VNet-ID: De service VNet die u hebt gemaakt in de sectie Een VNet maken.

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. Maak een public key pair. Raadpleeg [Een SSH-sleutelpaar maken op Windows](#) voor richtlijnen.

```
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. Voer de waarden in voor SSH Public Key en Resource Groups.

Create Gateway

Key Selection

SSH Public Key

SSH Key Pair

SSH Public key *

ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAQChvSlgyD
Kk+X6zGCgM3AxV3iPcxZIF7QtWB7WiagDgo+IRKcH
cPNUofBzsgvIOSuP1mYf6LZQp6Xdhk/9UG6Cq6R0O
IXymuK/DY2LlcDm/P0CFeww/cKCMToG6Oqx8IK/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. Schakel het openbare IP uit en klik op Volgende.

Create Gateway

✓

✓

3

4

Gateway Information

Gateway Details

Advanced Settings

Review

Public IP

☒ Disable Public IP

8. Bekijk alle waarden die u hebt opgegeven.

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. Nadat u de waarden hebt bekeken en de bronnen zijn geladen, klikt u op Voltooien.

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

Dashboardweergave zodra de bronnen zijn geladen.

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



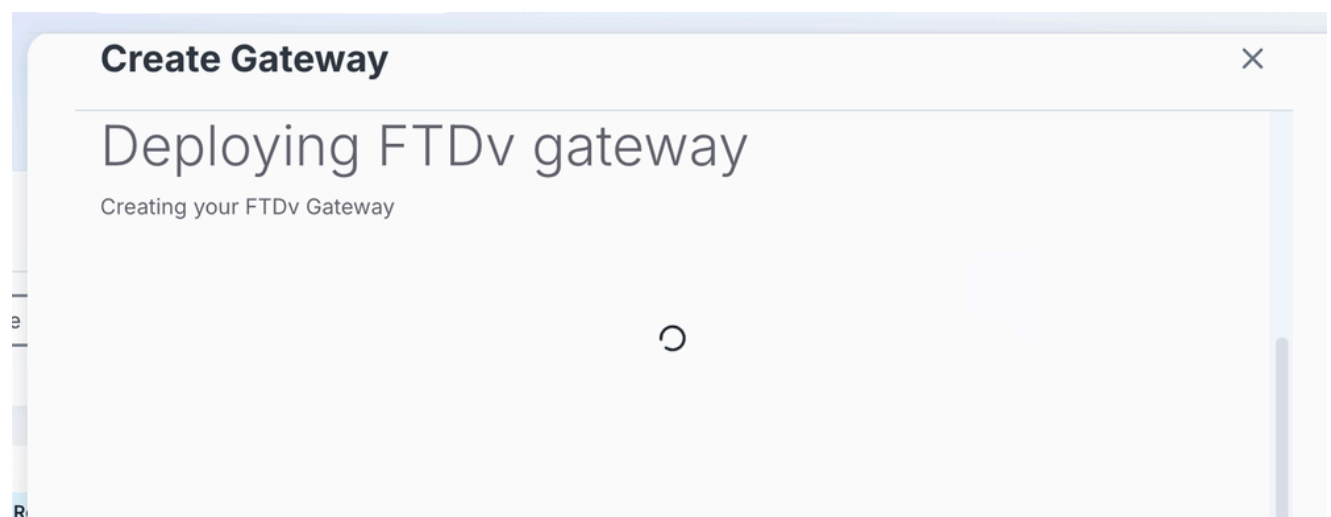
Resource	Limit	In Use	Min Usage for Gateway	Max Usage for Gateway	Recommendation
Private IPs in Subnets	254	0	1	3	
Elastic IPs	1000	51	1	3	
Load Balancers	1000	8	1	1	
Instances	25000	31	2	6	
Virtual CPUs	350	0	16	48	

Advanced Settings

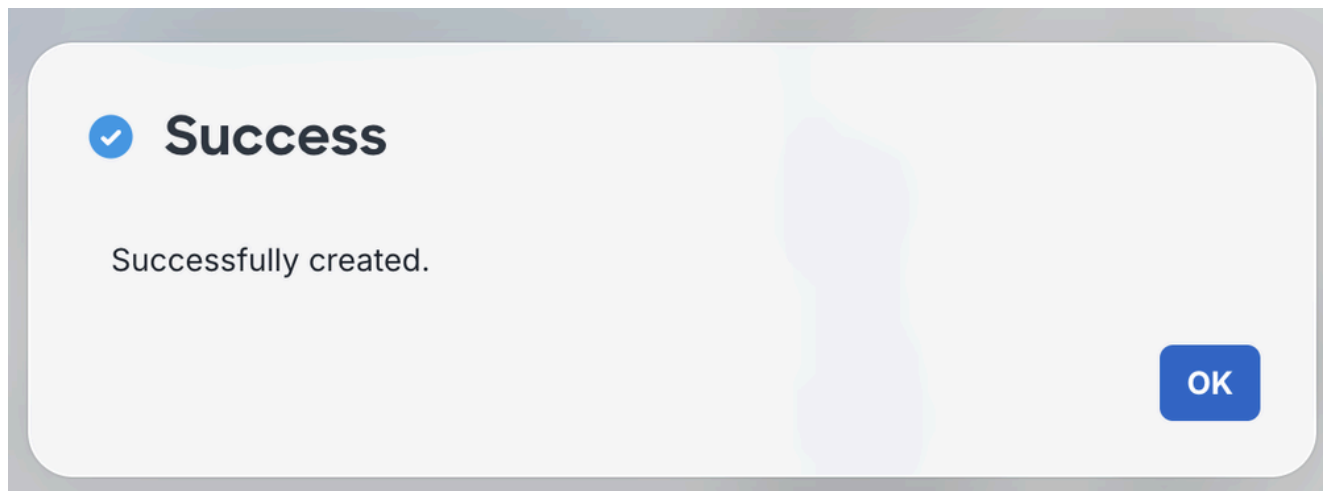
[Edit](#)**Disable Public IP**

enabled

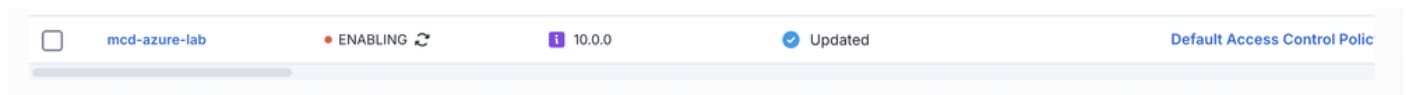
Dashboardweergave van gateway-implementatie.



10. Nadat de gateway is gemaakt, verschijnt er een succesbericht. Klik op OK.



Vanaf het MCD-dashboard wordt de status ENABLING (INSCHAKELEN) weergegeven.



Controleer de status via de tabbladen Overzicht en instanties.

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

Verifiëren

Gebruik deze sectie om te controleren of uw configuratie goed werkt.

- Onder Compute > Virtuele machines in Azure controleert u de FTDv-instanties. De status verandert van Aanmaken naar Uitvoeren.

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

+ 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-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 ...

- Bevestig de gateway-status vanaf het MCD-dashboard.

Summary

Cloud Details

Interfaces

Instances

Settings

Troubleshooting

Terraform

Availability Zone	Number of Instances
1	1
2	1

AVAILABILITY ZONES DETAILS

Refresh

Instance: 1

Instance Actions

Instance ID

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

Instance Name

ciscomcd-mcd-azure-lab-psprorne

Datapath Private IP

Datapath 2 Private IP

Datapath 2 Public IP

-

Mgmt Private IP

-

Mgmt Public IP

-

State

● INIT

Created

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

Last Heartbeat

NA

Image Version

10.0.0

Policy Updates

Please check cdFMC for policy update status.

Gerelateerde informatie

- [Een service-VPC of VNet maken](#)
- [FTDv-integratieprocedure](#)
- [Gateway-vereisten configureren](#)
- [Multicloud Defense voor Azure Overzicht](#)
- [Maak en gebruik een SSH publiek-privaat sleutelpaar voor Linux VM's in Azure](#)
- [Technische ondersteuning en documentatie – Cisco Systems](#)

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.