

Bereitstellen eines FTDv-Clusters in Azure mithilfe von MCD

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konfigurieren](#)

[Registrieren einer Anwendung](#)

[Benutzerdefinierte Rolle erstellen](#)

[Benutzerdefinierte Rolle zuweisen](#)

[Azure-Konto mit MCD verbinden](#)

[Erstellen eines VNet](#)

[Erstellen des Azure MCD FTDv-Gateways](#)

[Überprüfung](#)

[Zugehörige Informationen](#)

Einleitung

In diesem Dokument wird beschrieben, wie Sie Microsoft Azure-Voraussetzungen konfigurieren und ein virtuelles Gateway für Firewall Threat Defense (FTDv) über MCD bereitstellen.

Voraussetzungen

- Ein Azure-Abonnement, das erworben und registriert und mit der Microsoft Entra-ID verknüpft wird. Bestätigen Sie dies in der Liste der App-Registrierungen im Azure-Portal.
- Eine benutzerdefinierte Rolle, die für das Azure-Abonnement erstellt wurde und Multicloud Defense (MCD)-Zugriff auf die spezifischen Ressourcen und Aktionen gewährt, die andernfalls blockiert werden.
- Ein Abonnement für Azure Event Grid, damit MCD Echtzeit-Updates vom Azure-Abonnement erhalten kann.
- Das Azure-Abonnement, das über das MCD-Dashboard mit dem Multicloud Defense Controller verbunden ist.
- Die in Azure akzeptierten Cisco Marketplace-Bedingungen, wenn das Azure-Konto zum ersten Mal in MCD integriert wird.

- (Optional) Eine vom Benutzer zugewiesene verwaltete Identität wird konfiguriert, wenn Sie Zugriff auf Key Vault oder Blob Storage benötigen.
- Ein neues Service-VNet. VNets, die vor Einführung der FTDv-Gateway-Unterstützung erstellt wurden, können nicht für eine FTDv-Gateway-Bereitstellung verwendet werden.
- Ein aktives Abonnement für Cloud-Delivered Firewall Management Center (cdFMC), das die Zugriffskontrollrichtlinien für das FTDv-Gerät verwaltet.
- Mindestens eine FTDv-Lizenz, die Sie über Ihren Cisco Verkäufer oder Partner erworben haben.

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Navigation im Microsoft Azure-Portal
- Microsoft Entra ID (Azure AD)-Anwendungsregistrierung und rollenbasierte Zugriffskontrolle (RBAC)
- Cisco Multicloud Defense (MCD)
- Cisco Secure Firewall Threat Defense Virtual (FTDv)

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardware-Versionen beschränkt.

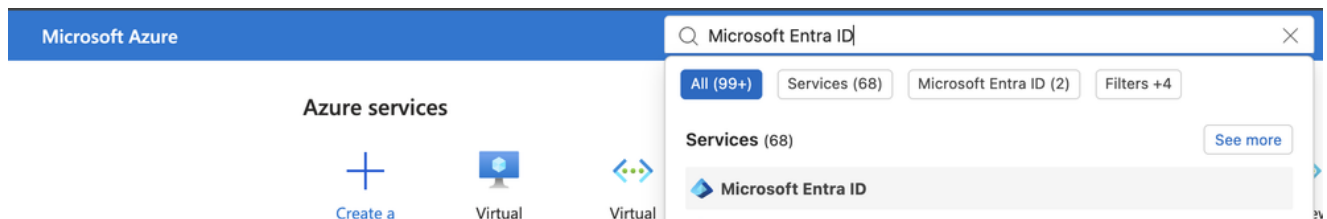
Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Konfigurieren

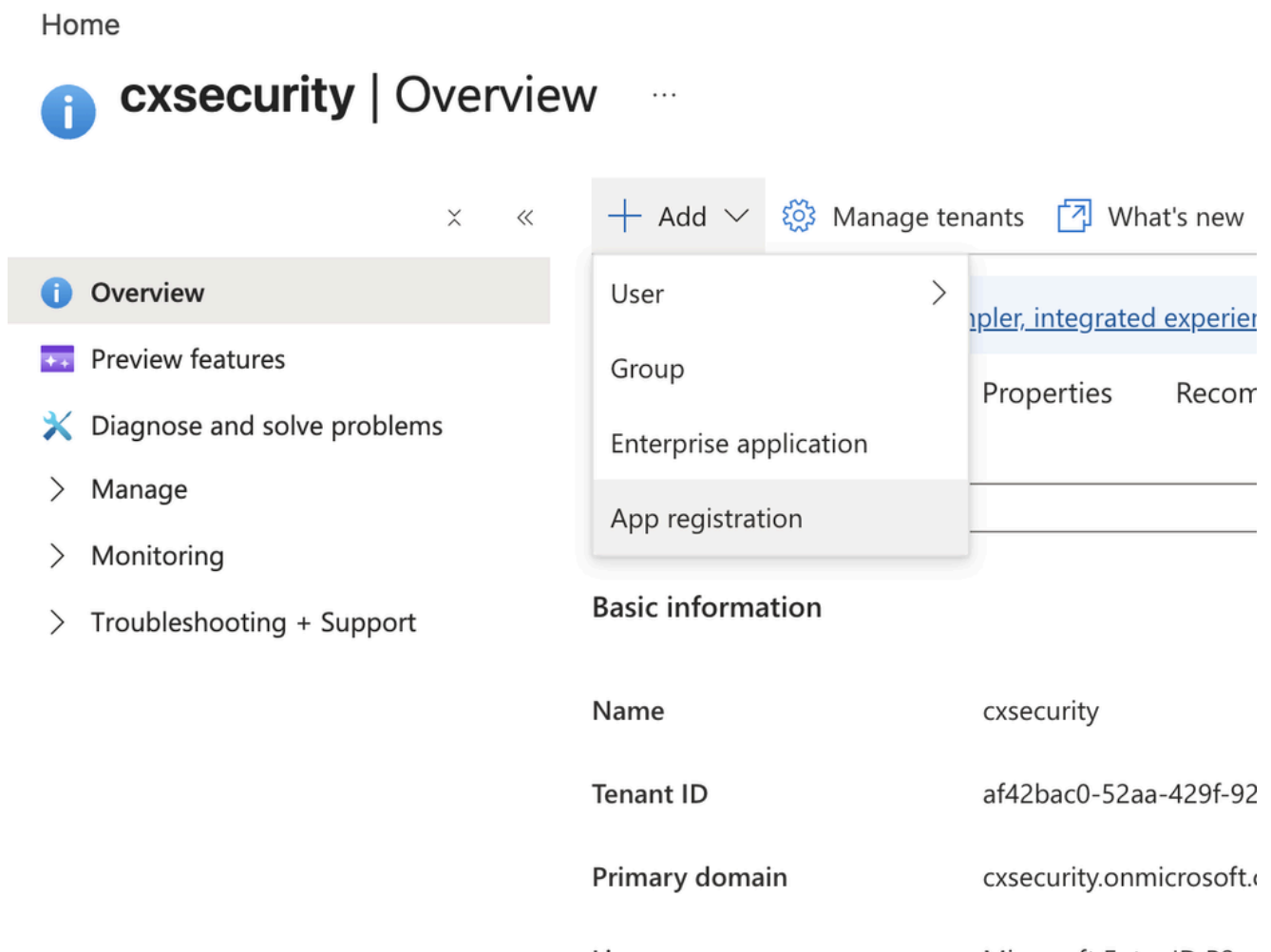
Verwenden Sie diese Verfahren, um Microsoft Azure vorzubereiten, Ihr Azure-Konto mit MCD zu verbinden und ein FTDv-Gateway bereitzustellen.

Registrieren einer Anwendung

1. Navigieren Sie mit der Suchleiste des Azure-Portals zu Microsoft Entra ID.



2. Klicken Sie auf Hinzufügen, und wählen Sie dann App-Registrierung aus.



3. Geben Sie im Formular Anmeldung registrieren folgende Werte ein:

- Name: Ein leicht identifizierbarer Name für die Anwendung.
- Unterstützte Kontotypen: Wählen Sie die Option aus, die am besten zu Ihrer Umgebung passt. In diesem Dokument wird nur ein Tenant verwendet.

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

- Single tenant only - cxsecurity
- Single tenant only - cxsecurity
- Multiple Entra ID tenants
- Any Entra ID Tenant + Personal Microsoft accounts
- Personal accounts only

[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. Wählen Sie für Redirect URI (optional) die für Ihre Umgebung geeignete Option aus. In diesem Dokument wird kein Umleitungs-URI konfiguriert.

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.

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

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

5. Klicken Sie auf Registrieren.
6. Nach der Registrierung der Anwendung wird die Übersichtsseite angezeigt. Kopieren Sie die Anwendungs-ID (Client) und die Verzeichnis-ID (Tenant), und speichern Sie sie auf einem Notizblock.

Home > cxsecurity | Overview

Multicloud Defense Controller

Search

Deactivate Delete Endpoints

Overview

Quickstart

Integration assistant

Diagnose and solve problems

Manage

Support + Troubleshooting

Essentials

Display name : Multicloud Defense Controller

Application (client) ID : e5e0d63d-6f62-4ff9-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 L... : 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. Navigieren Sie in der linken Navigationsleiste der Anwendungsseite zu Verwalten > Zertifikate und Schlüssel.



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. Klicken Sie auf Neuer Clientschlüssel.

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. Geben Sie auf der Seite Add a client secret (geheimen Client hinzufügen) folgende Werte ein, und klicken Sie dann auf Add (Hinzufügen):

- Beschreibung: Eine passende Beschreibung für den geheimen Schlüssel des Clients.
- Gültig bis: Wählen Sie aus dem Dropdown-Menü die Option aus, die am besten zu Ihrer Umgebung passt.



Anmerkung: Sie müssen einen neuen geheimen Schlüssel erstellen, wenn der aktuelle geheime Schlüssel abläuft.

Add a client secret

Description: swesnitz-mcd-secret

Expires: Recommended: 180 days (6 months)

10. Kopieren Sie die Wert- und die geheime ID und speichern Sie sie auf einem Notizblock.



Warnung: Sie können den geheimen Wert nur zum Zeitpunkt der Erstellung anzeigen.

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]



Tipp: Der geheime Schlüssel des Clients wird in der Spalte Wert aufgeführt.

Benutzerdefinierte Rolle erstellen

1. Navigieren Sie mit der Suchleiste des Azure-Portals zu Abonnements.

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. Klicken Sie auf Ihr 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. Klicken Sie auf Zugriffskontrolle (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...

Subscription: **cx-tac-rtp-fw-azure (cxsecurity)**

Subscription ID: 560f3235-2739-42bf-947e-e6ee1cc2b999

My role: Specified access

Current cost: \$1,418.01

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-e6ee1cc2b999

Directory: cxsecurity (cxsecurity.onmicrosoft.com)

My role: Specified access

Offer: Enterprise Agreement

Offer ID: MS-AZR-0017P

Parent management group: Americas

4. Klicken Sie auf Hinzufügen, und wählen Sie dann im Dropdown-Menü die Option Benutzerdefinierte Rolle hinzufügen aus.

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

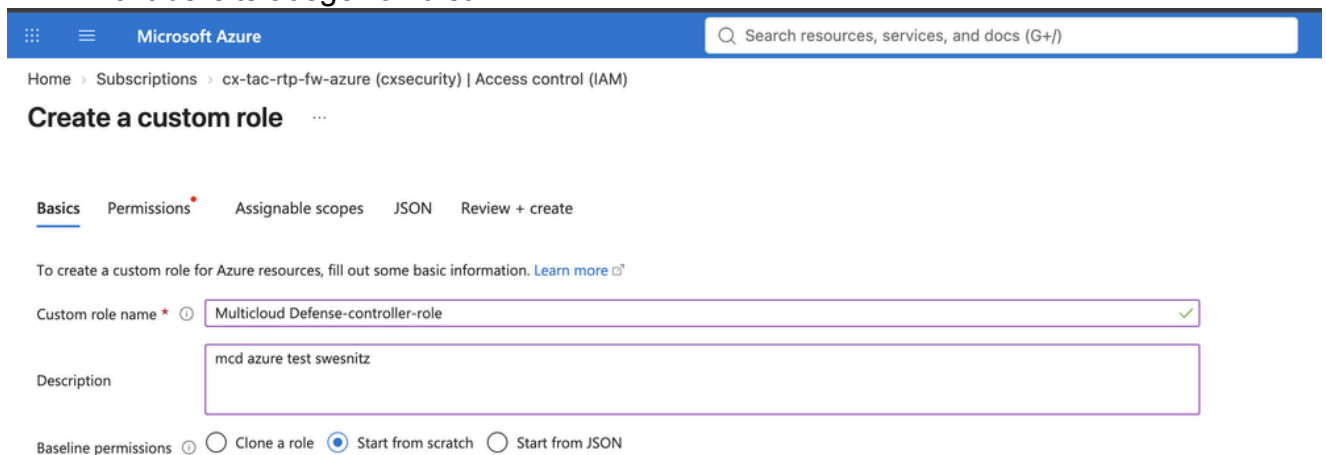
Add role assignment Add custom role

users have elevated access in your tenant. View role assignments

5. Geben Sie folgende Werte ein:

- Benutzerdefinierter Rollenname: Ein leicht identifizierbarer Name für die benutzerdefinierte Rolle.

- Beschreibung: Eine Beschreibung der Rolle.
- Basisberechtigungen: Klicken Sie auf das Optionsfeld Von Grund auf starten, wenn es nicht bereits ausgewählt ist.



Microsoft Azure

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



Anmerkung: Die bereitgestellte JSON, nicht die Registerkarte Berechtigungen, weist der benutzerdefinierten Rolle Berechtigungen zu.

6. Klicken Sie auf JSON.
7. Klicken Sie auf Bearbeiten.
8. Fügen Sie diesen Codeblock in die eckigen Klammern ein, um Aktionen auszuführen:

```
"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"
```

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

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 }
```



Anmerkung: Überprüfen Sie den richtigen Abstand und die richtigen Registerkarten für den JSON-Codeblock.

Dies ist ein Beispiel für die abgeschlossene Rollendefinition:

```
{
  "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/*",
```

```

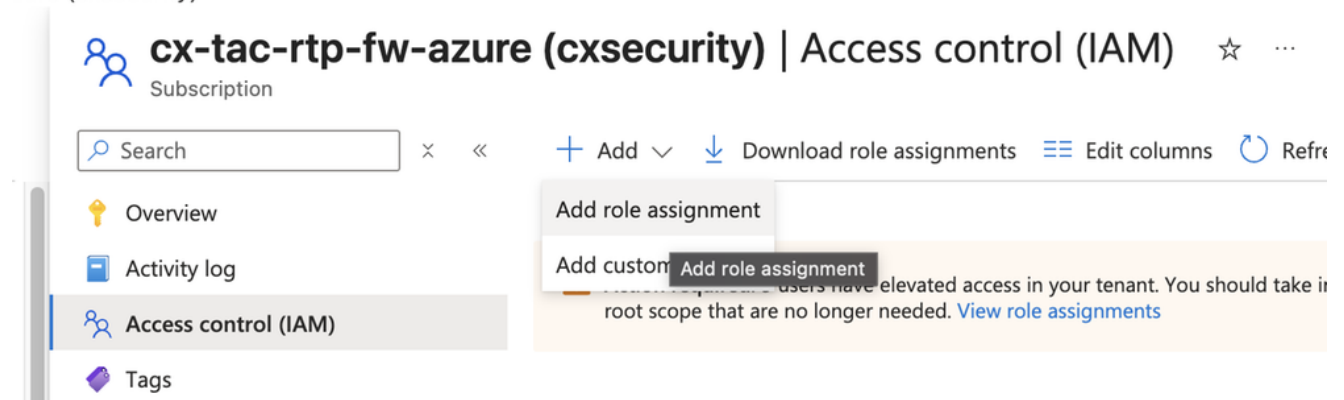
"Microsoft.Compute/disks/*",
"Microsoft.Compute/images/read",
"Microsoft.Compute/sshPublicKeys/read",
"Microsoft.Compute/virtualMachines/*",
"Microsoft.ManagedIdentity/userAssignedIdentities/read",
"Microsoft.ManagedIdentity/userAssignedIdentities/assign/action",
"Microsoft.Network/loadBalancers/*",
"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",
...

```

Benutzerdefinierte Rolle zuweisen

1. Klicken Sie auf der Seite der Abonnement-Zugriffskontrolle (IAM) auf Rollenzuweisung hinzufügen.

zure (cxsecurity)



2. Suchen Sie nach der Rolle, die Sie im Abschnitt Benutzerdefinierte Rolle erstellen erstellt haben.

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. Klicken Sie auf Weiter, und belassen Sie Zuweisen des Zugriffs auf Benutzer, Gruppe oder Dienstprinzipal unverändert.

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. Klicken Sie auf Mitglieder auswählen.

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. Fügen Sie die Rolle hinzu, die Sie im Abschnitt Benutzerdefinierte Rolle erstellen erstellt haben.

Select members



 Multi 



Multicloud - Azure - RTP
Application



Multicloud Defense Controller
Application

Selected members:



Multicloud Defense Controller
Application



6. Klicken Sie auf Weiter, und kopieren Sie dann die Abonnement-ID.

Add role assignment ...

Role Members Conditions Assignment type Review + assign

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

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

7. Klicken Sie auf Prüfen + zuweisen.

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	

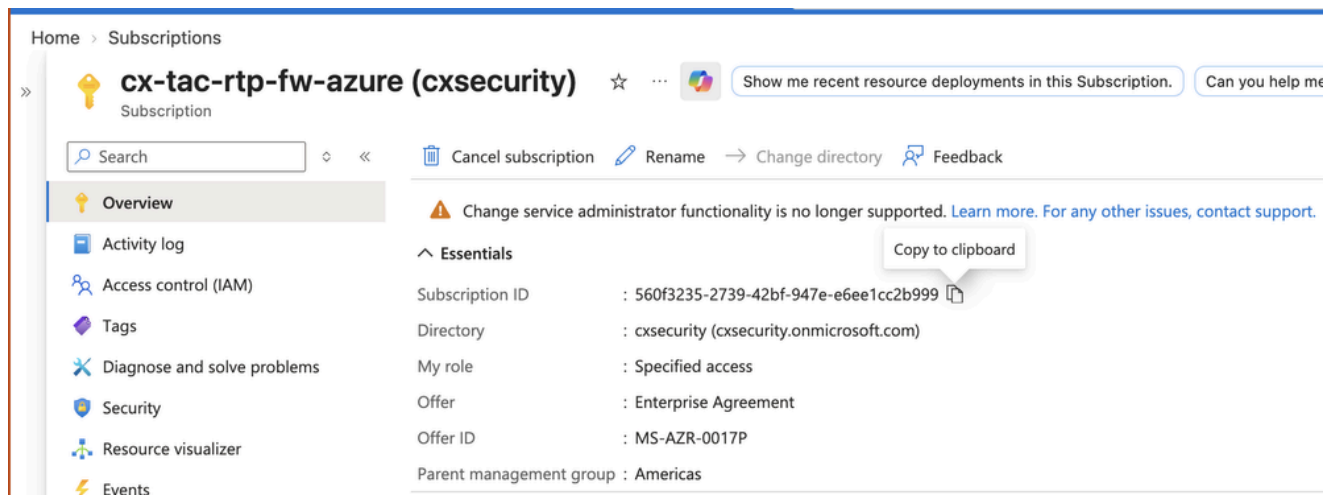
Review + assign

Review + assign

Previous

Next

8. Die Übersichtsseite für das Abonnement wird angezeigt. Navigieren Sie im Menü auf der linken Seite zu Overview (Übersicht), und kopieren Sie die Abonnement-ID.



Damit sind die Azure-Voraussetzungen zum Hinzufügen des Azure-Kontos zu MCD abgeschlossen. Diese Verfahren beschreiben die Integration und Bereitstellung über MCD.

Azure-Konto mit MCD verbinden

1. Navigieren Sie zu SCC > Multicloud Defense.



Security Cloud Control



Organization
cisco-swesnitz



Ho



Home

Products



Firewall



Multicloud Defense

Platform services



Favorites



Security Devices



Platform Management



2. Klicken Sie im Bereich "Cloud-Konten" auf Konto hinzufügen.

Dashboard

Cloud Accounts

Discover ×

1	1 	0 
	0 	0 

[Add Account](#)

[View More](#)

3. Klicken Sie auf das Azure-Symbol.

Select Your Cloud Account
Please select Account Type you want to set up









[Close](#)[Back](#)

4. Geben Sie auf der Seite Azure-Konto verbinden folgende Werte ein:

- Azure-Kontoname: Der Name des Azure-Kontos aus der MCD-Perspektive.
- Verzeichnis-ID: Die Verzeichnis-ID, die Sie im Abschnitt Registrieren einer Anwendung gespeichert haben.
- Abonnement-ID: Die Abonnement-ID, die Sie im Abschnitt Benutzerdefinierte Rolle zuweisen gespeichert haben.
- Anwendungs-ID: Die Anwendungs-ID, die Sie im Abschnitt Registrieren einer Anwendung gespeichert haben.
- Client-Schlüssel: Der Wert, den Sie im Abschnitt Anwendung registrieren gespeichert haben.

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 erkennt und zeigt die Azure-Ressourcen an. Klicken Sie auf Next (Weiter).

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. Klicken Sie auf Close (Schließen).

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. Sie können das integrierte Konto jetzt über Infrastruktur > CSP-Konten anzeigen.



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

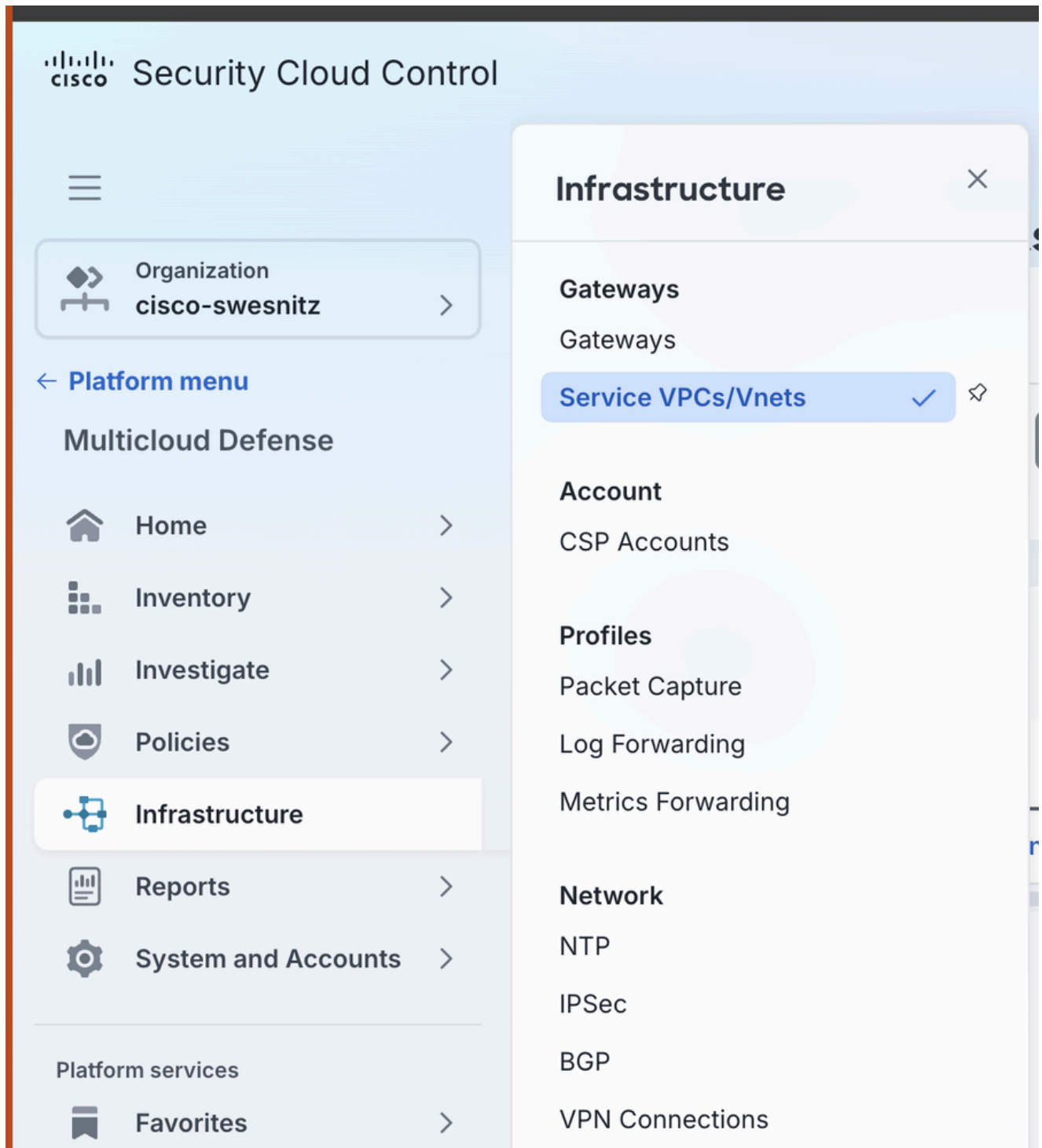
IPSec

BGP

VPN Connections

Erstellen eines VNet

1. Navigieren Sie zu Infrastruktur > Service-VPCs/VNets.



2. Klicken Sie auf Erstellen.

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. Geben Sie folgende Werte ein:

- Name: Ein leicht identifizierbarer Name für das VNet, der durch dieses Verfahren für das FTDv-Gateway erstellt wird.
- CSP-Konto: Der Name, den Sie im Abschnitt Azure-Konto mit MCD verbinden zugewiesen haben.
- Region: Die Region, in der das FTDv-Gateway bereitgestellt wird.
- CIDR-Block: Ein eindeutiger IP-Block für das Transit-Gateway, das dem VNet zugeordnet ist.
- Verfügbarkeitsbereiche: Wählen Sie aus Gründen der Ausfallsicherheit mindestens zwei Verfügbarkeitsbereiche aus.
- Ressourcengruppe: Wählen Sie + Ressourcengruppe erstellen aus dem Dropdown-Menü aus.
- Ressourcengruppenname: Ein Name für die Ressourcengruppe.
- Ressourcengruppen-Region: Der Bereich, der mit dem Bereich übereinstimmt, den Sie für Region ausgewählt haben.

Klicken Sie auf Speichern.

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. Eine Erfolgsmeldung wird angezeigt.



Success

Service VPC/VNet created successfully.

OK

Bestätigen Sie die Erstellung des VNet auf Azure-Seite, und navigieren Sie zu Network Foundation > Virtual Networks Overview > Virtual Networks.

Home > Network foundation

Network foundation | Virtual Network overview

Preview

Search

Overview

Virtual network

Virtual Network overview

Virtual networks

NAT gateways

Public IP addresses

Network interfaces

Network security groups

Application security groups

Virtual network

Network foundation

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

Enhanced security through isolated, secure environments.

Flexible, scalable without physical changes.

Secure connectivity across Azure regions

Learn more

CreateView resources

Connectivity

Home > Network foundation

Network foundation | Virtual networks

Preview

Search

Overview

Virtual network

Virtual Network overview

Virtual networks

NAT gateways

Public IP addresses

Network interfaces

CreateManage viewRefreshExport to CSVOpen query

mcdSubscription equals allResource Group equals all

Name ↑

mcd_test_vnet-swesnitz

Das VNet wechselt in den Status "Active", sobald es erstellt wurde.

Create

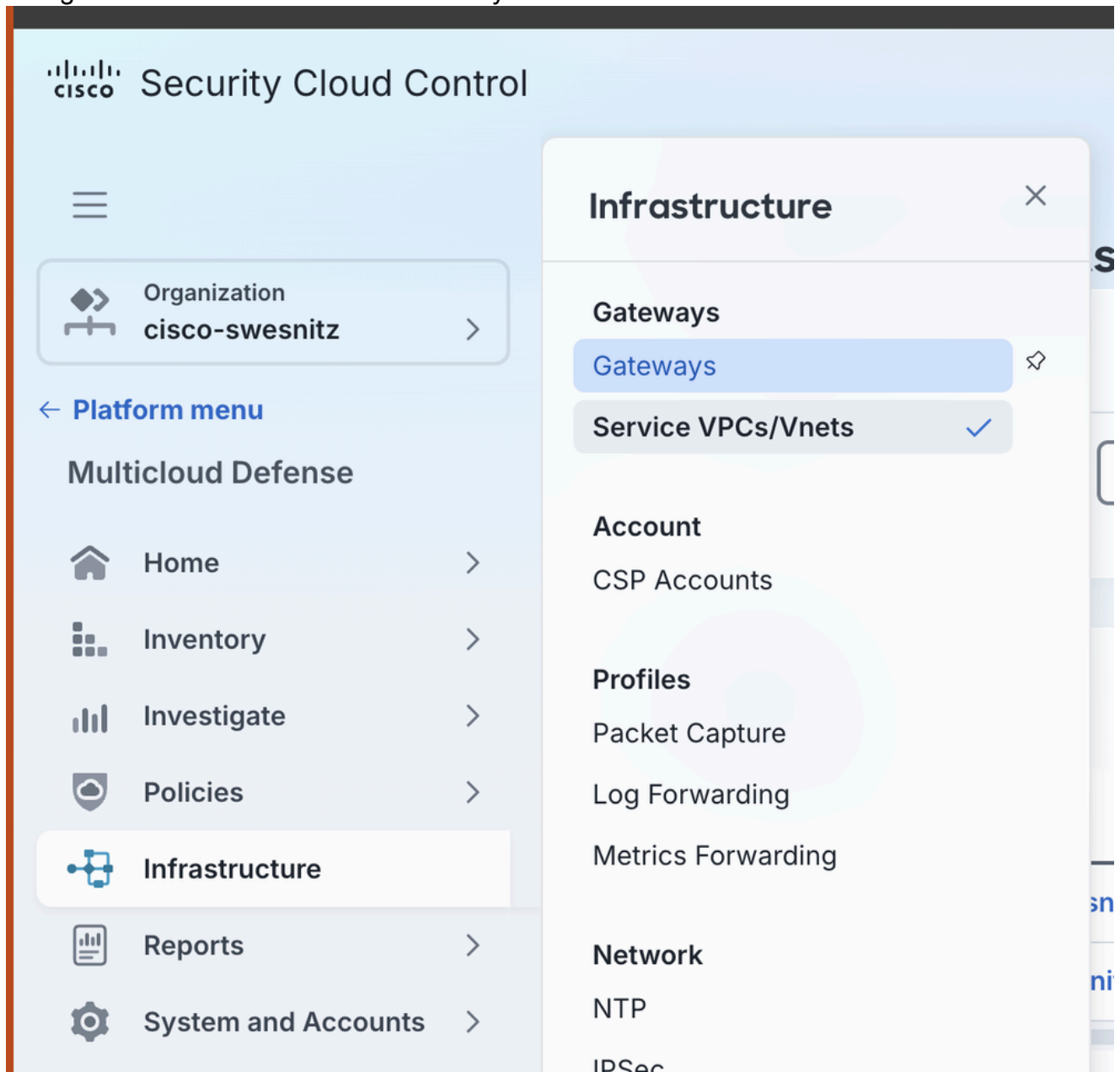
Actions

Refresh

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

Erstellen des Azure MCD FTDv-Gateways

1. Navigieren Sie zu Infrastruktur > Gateways.



2. Klicken Sie auf Gateway hinzufügen.

The screenshot shows the Cisco Security Cloud Control web interface. On the left is a navigation sidebar with a 'Platform menu' containing 'Multicloud Defense' and 'Infrastructure' (highlighted). The main content area is titled 'Gateways: 1' and includes a 'Quick Filters' section with a 'Name' dropdown and a 'CSP Account' field. Below this is an 'Add Gateway' button, an 'Actions' dropdown, and a 'Recommended' toggle. A table with columns 'Name' and 'State' is partially visible at the bottom.

3. Geben Sie folgende Werte ein:

- Kunden: Wählen Sie aus dem Dropdown-Menü das Azure-Konto aus, das Sie im Abschnitt Azure-Konto mit MCD verbinden verknüpft haben.
- Gateway-Typ: Wählen Sie FTDv Gateway aus.
- Name: Ein leicht identifizierbarer Name für das FTDv-Gateway.
- Instanztyp: Der Instanztyp, der für Ihre Umgebung geeignet ist.
- Minimale Instanzen: Wählen Sie im Dropdown-Menü mindestens eine Instanz aus.
- Maximale Instanzen: Die gewünschte Anzahl von FTDv-Instanzen für Ihre Umgebung. Der maximal zulässige Wert ist 10.
- HealthCheck-Port: Der Standardwert ist 65534. Dieser Wert wird in diesem Dokument nicht geändert.

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

Anmerkung: Der HealthCheck-Port ist die Portnummer, die der Multicloud Defense Load Balancer verwendet, um die Integrität der Instanzen zu überprüfen. Die den Instanzen zugewiesenen DataPath-Sicherheitsgruppen müssen Datenverkehr auf diesem Port zulassen.

4. Geben Sie folgende Werte ein:

- Eigenschaften: Wählen Sie Egress oder Ost-West aus.
- FTDv-Version: Die am besten auf die Umgebung abgestimmte Softwareversion.
- Richtlinien-Regelsatz: Die Zugriffskontrollrichtlinie (ACP, Access Control Policy) für

diesen FTDv-Cluster.

- Kennwort: Ein Passwort für die FTDv-Instanzen.
- Lizenzmodell: Das gewünschte Lizenzierungsmodell.
- Leistungsstufe: Die Ebene, die für den erwarteten Gerätedurchsatz geeignet ist.
- Lizenztypen: Die für diese Bereitstellung erworbenen Lizenztypen.
- Region: Die Region, in der diese FTDv-Instanzen bereitgestellt werden.
- VPC/VNet-ID: Das Service-VNet, das Sie im Abschnitt Erstellen eines VNet erstellt haben.

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. Erstellen Sie ein öffentliches Schlüsselpaar. Weitere Informationen finden Sie unter [Erstellen eines SSH-Schlüsselpaars unter Windows](#).

```

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. Geben Sie die Werte für den öffentlichen SSH-Schlüssel und die Ressourcengruppen ein.

Create Gateway

Key Selection

SSH Public Key

SSH Key Pair

SSH Public key *

ssh-rsa
AAAAAB3NzaC1yc2EAAAADAQABAAQChvSlgyD
Kk+X6zGCgM3AxV3iPcxZIF7QtWB7WiagDgo+IRKcH
cPNUofBzsgvIOSuP1mYf6LZQp6Xdhk/9UG6Cg6R0O
IXvmuK/DY2UcDm/R0CFeww/cKCMToG6Oax8IK/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. Deaktivieren Sie die öffentliche IP, und klicken Sie auf Weiter.

Create Gateway

✓

✓

3

4

Gateway Information

Gateway Details

Advanced Settings

Review

Public IP

☒ Disable Public IP

8. Überprüfen Sie alle von Ihnen angegebenen Werte.

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. Nachdem Sie die Werte überprüft und das Laden der Ressourcen abgeschlossen haben, klicken Sie auf Beenden.

Create Gateway

Performance Tier

FTDv20

License Type

Base

Region

eastus

VPC/VNet ID

mcd_test_vnet-swesnitz | mcd_test_vnet-swesnitz

SSH Public Key

ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQChvSlgyDr

Resource Groups

mcd_swesnitz

Mgmt. Security Group

mcd_test_vnet-swesnitz-mgmt-sg

Datapath Security Group 1

mcd_test_vnet-swesnitz-datapath-sg

Datapath Security Group 2

mcd_test_vnet-swesnitz-second-datapath-sg

EBS Encryption

AZURE EBS encryption key

Instance Details

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

Recommendations

loading...

Resources Info

loading...

Advanced Settings

Edit

Disable Public IP

enabled

Cancel

Back

Finish

Dashboard-Ansicht, sobald Ressourcen geladen wurden.

Instance Details

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

Resources Info



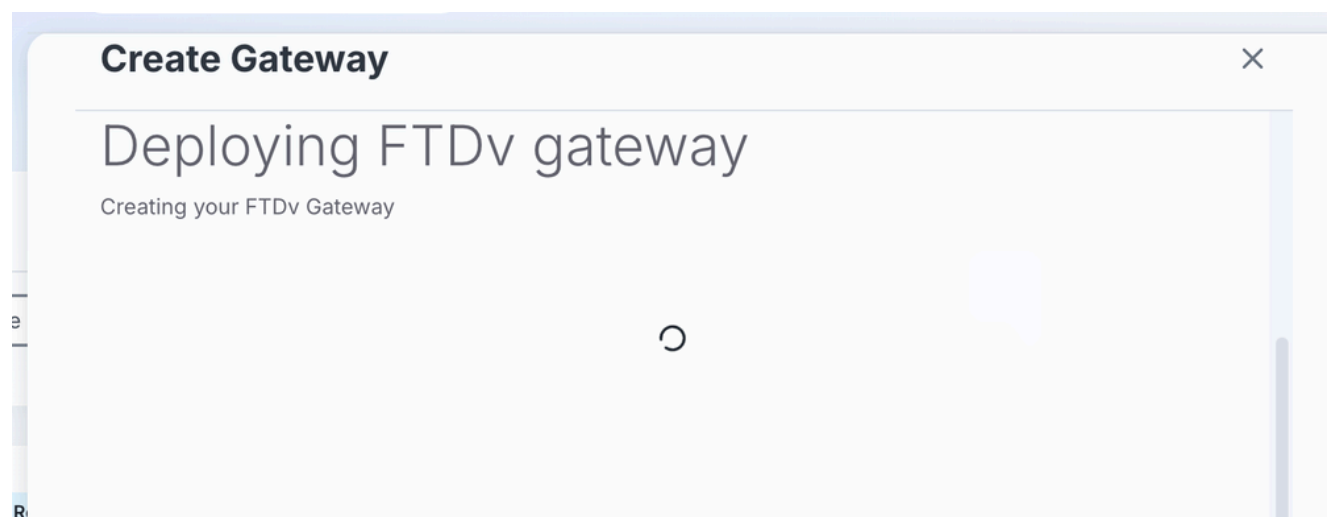
Resource	Limit	In Use	Min Usage for Gateway	Max Usage for Gateway	Recommendation
Private IPs in Subnets	254	0	1	3	
Elastic IPs	1000	51	1	3	
Load Balancers	1000	8	1	1	
Instances	25000	31	2	6	
Virtual CPUs	350	0	16	48	

Advanced Settings

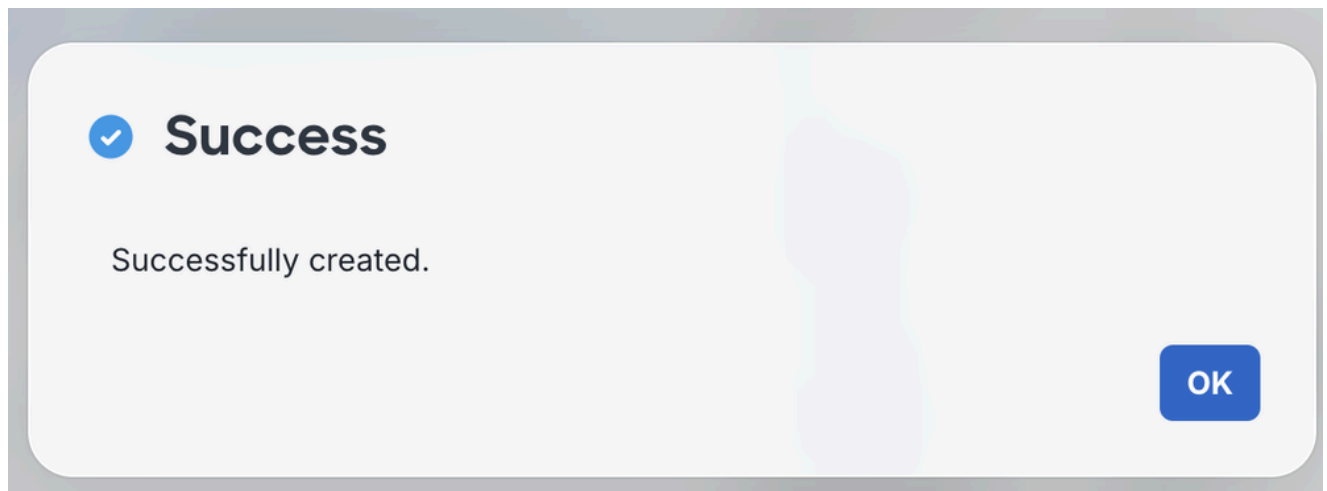
[Edit](#)**Disable Public IP**

enabled

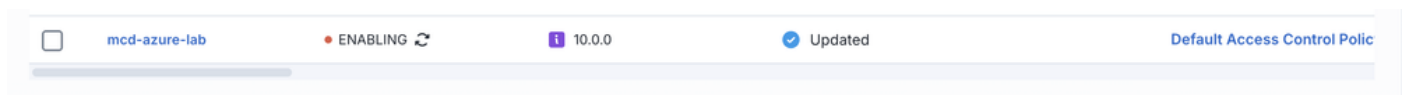
Dashboard-Ansicht der Gateway-Bereitstellung



10. Nachdem das Kabelmodem erstellt wurde, wird eine Erfolgsmeldung angezeigt. Klicken Sie auf OK.



Im MCD-Dashboard wird als Status ENABLING (AKTIVIEREN) angezeigt.



Überwachen Sie den Status über die Registerkarten Zusammenfassung und Instanzen.

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.

Zugehörige Informationen

- [Erstellen eines Service-VPC oder -VNet](#)
- [FTDv-Integrationsverfahren](#)
- [Konfigurieren der Gateway-Voraussetzungen](#)
- [Multicloud-Schutz für Azure - Überblick](#)
- [Erstellen und Verwenden eines öffentlich-privaten SSH-Schlüsselpaars für Linux-VMs in Azure](#)
- [Technischer Support und Dokumentation für Cisco Systeme](#)

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.