

Distribuire un gateway FTDv in Azure tramite MCD

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Configurazione](#)

[Registra applicazione](#)

[Crea un ruolo personalizzato](#)

[Assegna ruolo personalizzato](#)

[Connetti l'account di Azure a MCD](#)

[Creazione di una rete virtuale](#)

[Crea il gateway FTDv MCD di Azure](#)

[Verifica](#)

[Informazioni correlate](#)

Introduzione

In questo documento viene descritto come configurare i prerequisiti di Microsoft Azure e distribuire un gateway virtuale Firewall Threat Defense (FTDv) tramite MCD.

Prerequisiti

- Sottoscrizione di Azure acquisita e registrata e associata a Microsoft Entra ID. Confermare l'operazione nell'elenco delle registrazioni app nel portale di Azure.
- Ruolo personalizzato creato per la sottoscrizione di Azure che concede l'accesso MCD (Multicast Defense) alle risorse e alle azioni specifiche che sono altrimenti bloccate.
- Una sottoscrizione alla griglia eventi di Azure, in modo che MCD possa ricevere aggiornamenti in tempo reale dalla sottoscrizione di Azure.
- La sottoscrizione di Azure si è connessa a Multicast Defense Controller dal dashboard MCD.
- Condizioni di Cisco Marketplace accettate in Azure, se è la prima volta che l'account di Azure viene eseguito su MCD.
- (Facoltativo) Identità gestita assegnata dall'utente configurata, se è necessario l'accesso all'insieme di credenziali delle chiavi o all'archivio BLOB.

- Una nuova rete di servizi. Le VPN create prima dell'introduzione del supporto del gateway FTDv non possono essere utilizzate per una distribuzione del gateway FTDv.
- Una sottoscrizione attiva a CdFMC (Cloud-Delivered Firewall Management Center), che gestisce i criteri di controllo di accesso per il dispositivo FTDv.
- Almeno una licenza FTDv acquistata tramite il venditore o il partner Cisco.

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Esplorazione del portale di Microsoft Azure
- Registrazione dell'applicazione Microsoft Entra ID (Azure AD) e controllo degli accessi basato sui ruoli (RBAC)
- Cisco Multicast Defense (MCD)
- Cisco Secure Firewall Threat Defense Virtual (FTDv)

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

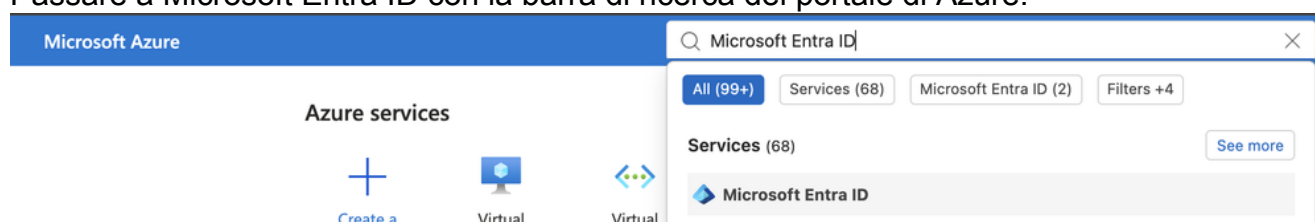
Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Configurazione

Utilizzare queste procedure per preparare Microsoft Azure, connettere l'account Azure a MCD e distribuire un gateway FTDv.

Registra applicazione

1. Passare a Microsoft Entra ID con la barra di ricerca del portale di Azure.



2. Fare clic su Add (Aggiungi), quindi selezionare App registration (Registrazione app).

×

«

+ Add ▾

⚙ Manage tenants

📄 What's new

Overview

Preview features

Diagnose and solve problems

> Manage

> Monitoring

> Troubleshooting + Support

User >

Group

Enterprise application

App registration

Properties

Recom

Basic information

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

3. Nel modulo Registra applicazione immettere i valori seguenti:

- Nome: Nome facilmente identificabile dell'applicazione.
- Tipi di account supportati: Selezionare l'opzione più adatta al proprio ambiente. In questo documento viene utilizzato solo il tenant singolo.

Home > cxsecurity | Overview

Register an application ...

* Name

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

Multicloud Defense Controller ✓

Supported account types

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

Single tenant only - cxsecurity ▾

Single tenant only - cxsecurity

Multiple Entra ID tenants

Any Entra ID Tenant + Personal Microsoft accounts

Personal accounts only

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

Select a platform ▾

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

[Help me choose](#)

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

4. Per Redirect URI (facoltativo), scegliere l'opzione appropriata per l'ambiente in uso. Questo documento non configura un URI di reindirizzamento.

Redirect URI (optional)

We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Select a platform

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

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

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

5. Fare clic su Registra.
6. Dopo aver registrato l'applicazione, viene visualizzata la pagina Panoramica. Copiare e salvare l'ID applicazione (client) e l'ID directory (tenant) in un blocco note.

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	Client credentials	: Add a certificate or secret
Application (client) ID	: e5e0d63d-6f62-4f99-aaed-2eabd850cf72	Redirect URIs	: Add a Redirect URI
Object ID	: ec1746e4-bd16-4a00-aa7d-3b8e7e52496a	Application ID URI	: Add an Application ID URI
Directory (tenant) ID	: af42bac0-52aa-429f-92db-925819967d17	Managed application in L...	: Multicloud Defense Controller
Supported account types	: My organization only	State	: Activated

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. Dalla navigazione a sinistra della pagina dell'applicazione, passare a Gestisci > Certificati e segreti.



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. Fare clic su Nuovo segreto client.



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

i 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. Nella pagina Aggiungi segreto client immettere questi valori e quindi fare clic su Aggiungi:

- Descrizione: Descrizione appropriata per il segreto client.
- Scade: Dal menu a discesa, scegliere l'opzione più adatta al proprio ambiente.



Nota: È necessario creare un nuovo segreto alla scadenza del segreto corrente.

Copilot

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

Add a client secret

Description

swesnitz-mcd-secret

Expires

Recommended: 180 days (6 months)

10. Copiare e salvare il valore e l'ID segreto in un blocco note.



Avviso: È possibile visualizzare il valore segreto solo al momento della creazione.

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]



Suggerimento: Il segreto client è elencato nella colonna Valore.

Crea un ruolo personalizzato

1. Passare a Sottoscrizioni con la barra di ricerca del portale di Azure.

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. Fare clic sulla sottoscrizione.

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. Fare clic su Controllo accesso (IAM).

Microsoft Azure

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)

Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Security, Resource visualizer, Events

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

4. Fare clic su Add (Aggiungi), quindi selezionare Add custom role (Aggiungi ruolo personalizzato) dal menu a discesa.

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 tenanted root scope that is not inherited. [View role assignments](#)

5. Immettere i seguenti valori:
- Nome ruolo personalizzato: Nome facilmente identificabile per il ruolo personalizzato.
 - Descrizione: Descrizione del ruolo.
 - Autorizzazioni baseline: Fare clic sul pulsante di opzione Inizia da zero, se non è già selezionato.

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 *

Description

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



Nota: Il file JSON specificato, non la scheda Autorizzazioni, assegna le autorizzazioni al ruolo personalizzato.

6. Fare clic su JSON.
7. Fare clic su Edit (Modifica).
8. Incollare questo blocco di codice tra parentesi quadre per le azioni:

```
"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 }
```



Nota: Verificare la spaziatura e le schede corrette per il blocco di codice JSON.

Questo è un esempio della definizione di ruolo completata:

```

{
  "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/*",

```

```

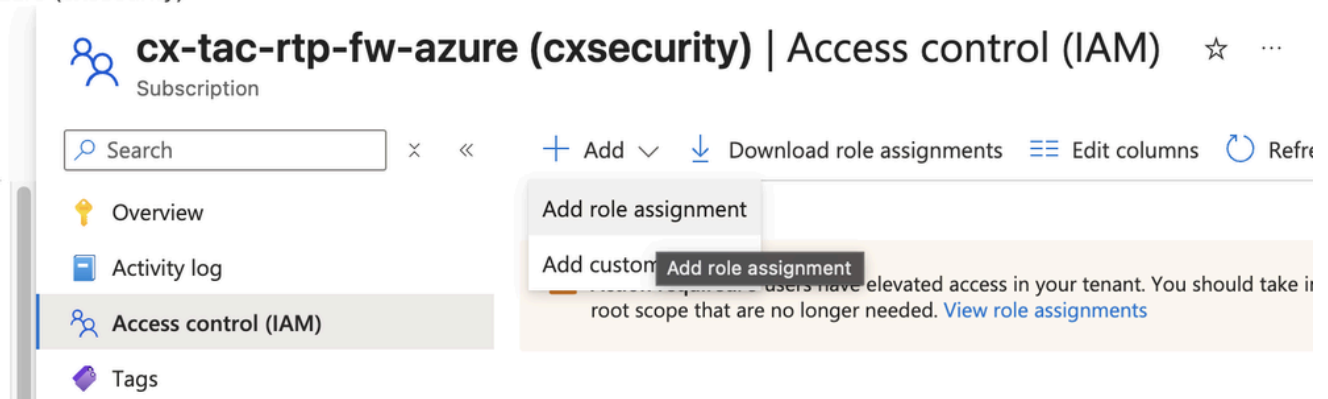
"Microsoft.Network/routeTables/*",
"Microsoft.Network/virtualNetworks/*",
"Microsoft.Network/virtualNetworks/subnets/*",
"Microsoft.Resources/subscriptions/resourcegroups/*",
"Microsoft.Storage/storageAccounts/blobServices/*",
"Microsoft.Storage/storageAccounts/listkeys/action",
"Microsoft.Network/networkWatchers/*",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

```

Assegna ruolo personalizzato

1. Nella pagina Controllo di accesso della sottoscrizione, fare clic su Aggiungi assegnazione ruolo.

zure (cxsecurity)



2. Cercare il ruolo creato nella sezione Creazione di un ruolo personalizzato.

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. Fare clic su Avanti e lasciare attiva Assegna accesso per impostare su Utente, gruppo o entità servizio.

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. Fare clic su Seleziona membri.

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. Aggiungere il ruolo creato nella sezione Creazione di un ruolo personalizzato.

Select members



 Multi 



Multicloud - Azure - RTP
Application



Multicloud Defense Controller
Application

Selected members:



Multicloud Defense Controller
Application



6. Fare clic su Avanti, quindi copiare l'ID sottoscrizione.

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. Fare clic su Rivedi + assegna.

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

- Viene visualizzata la pagina di panoramica della sottoscrizione. Dal menu a sinistra, passare a Panoramica e copiare l'ID della sottoscrizione.

Home > Subscriptions

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

Search

Cancel subscription Rename Change directory Feedback

Overview

- Activity log
- Access control (IAM)
- Tags
- Diagnose and solve problems
- Security
- Resource visualizer
- Events

Change service administrator functionality is no longer supported. [Learn more.](#) For any other issues, contact support.

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

Copy to clipboard

Verranno completati i prerequisiti di Azure per aggiungere l'account di Azure a MCD. Queste procedure descrivono l'integrazione e la distribuzione tramite MCD.

Connetti l'account di Azure a MCD

1. Passare a SCC > Multicast Defense.



Security Cloud Control



Organization
cisco-swesnitz



Home

Products



Firewall



Multicloud Defense

Platform services



Favorites



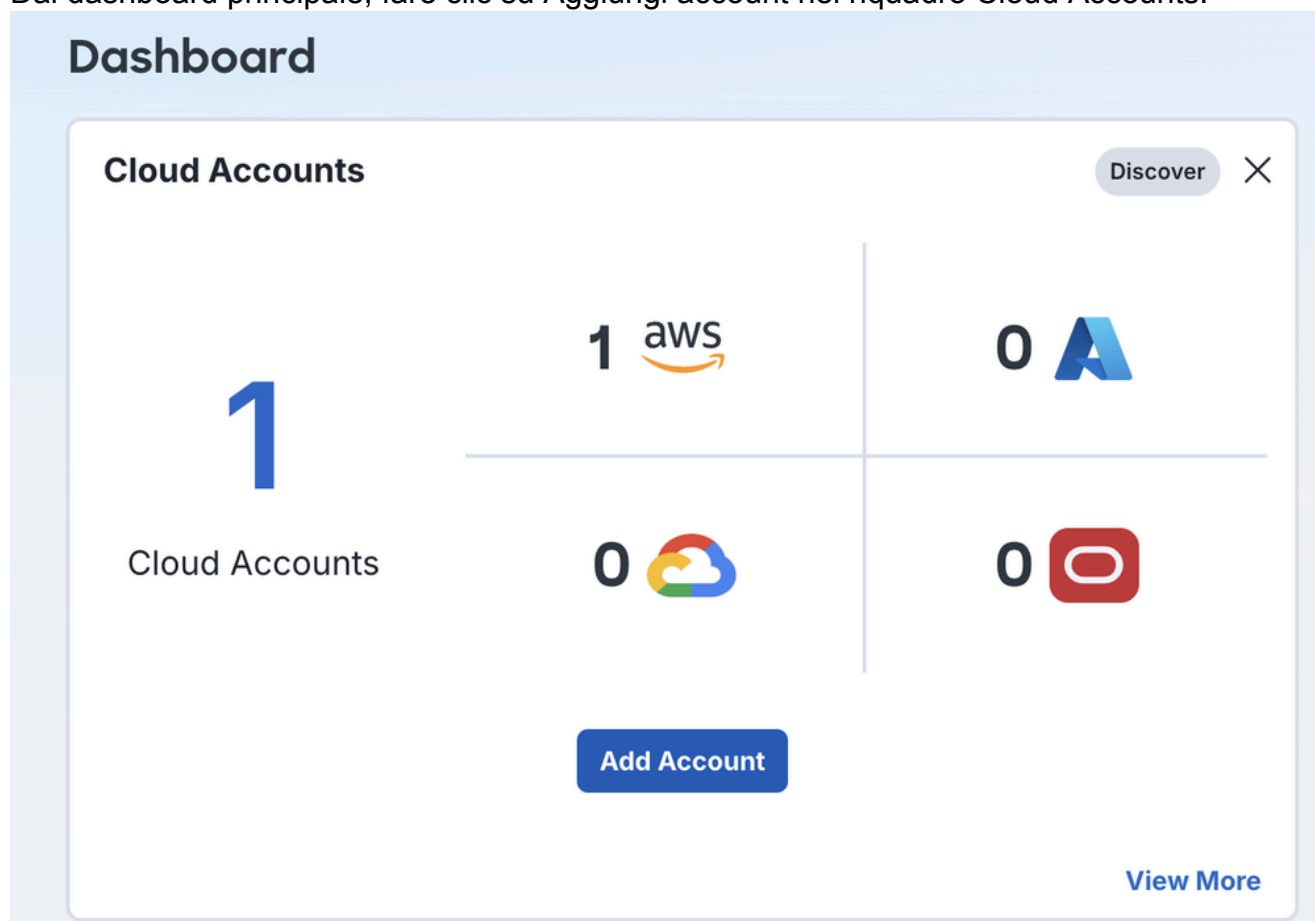
Security Devices



Platform Management



2. Dal dashboard principale, fare clic su Aggiungi account nel riquadro Cloud Accounts.



3. Fare clic sull'icona Azure.

Select Your Cloud Account

Please select Account Type you want to set up



Close Back

4. Nella pagina Connetti l'account Azure, immettere i valori seguenti:
- Nome account di Azure: Il nome dell'account di Azure dalla prospettiva MCD.
 - ID directory: ID di directory salvato nella sezione Registra un'applicazione.
 - ID sottoscrizione: L'ID sottoscrizione salvato nella sezione Assegna il ruolo personalizzato.
 - ID applicazione: ID dell'applicazione salvato nella sezione Registra un'applicazione.
 - Segreto client: Valore salvato nella sezione Registra un'applicazione.

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 individua e visualizza le risorse di Azure. Fare clic su Next (Avanti).

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. Fare clic su Close (Chiudi).

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



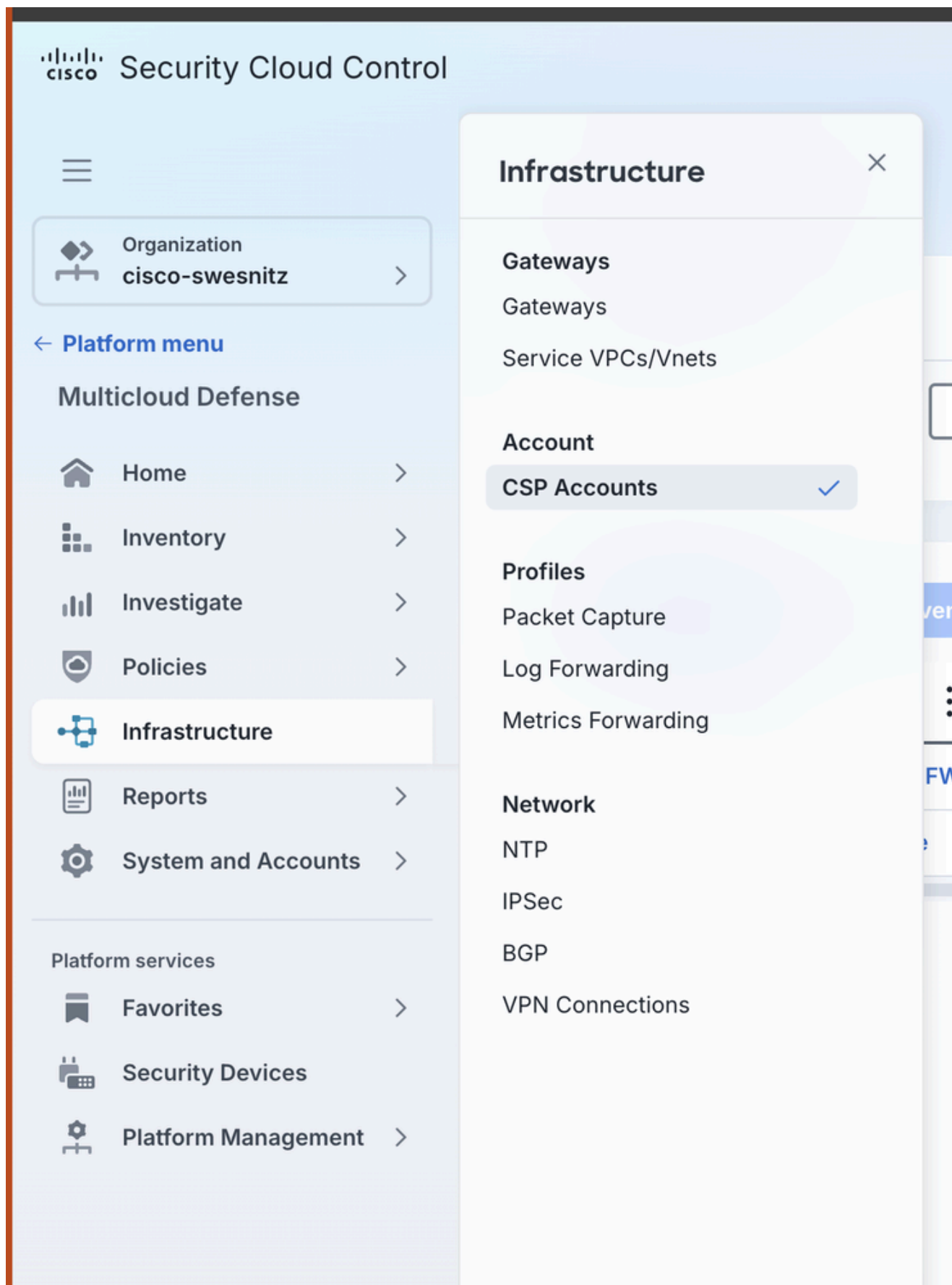
Setup a Service VPC and Multicloud Defense Gateway to secure your Account

Secure Account

Close

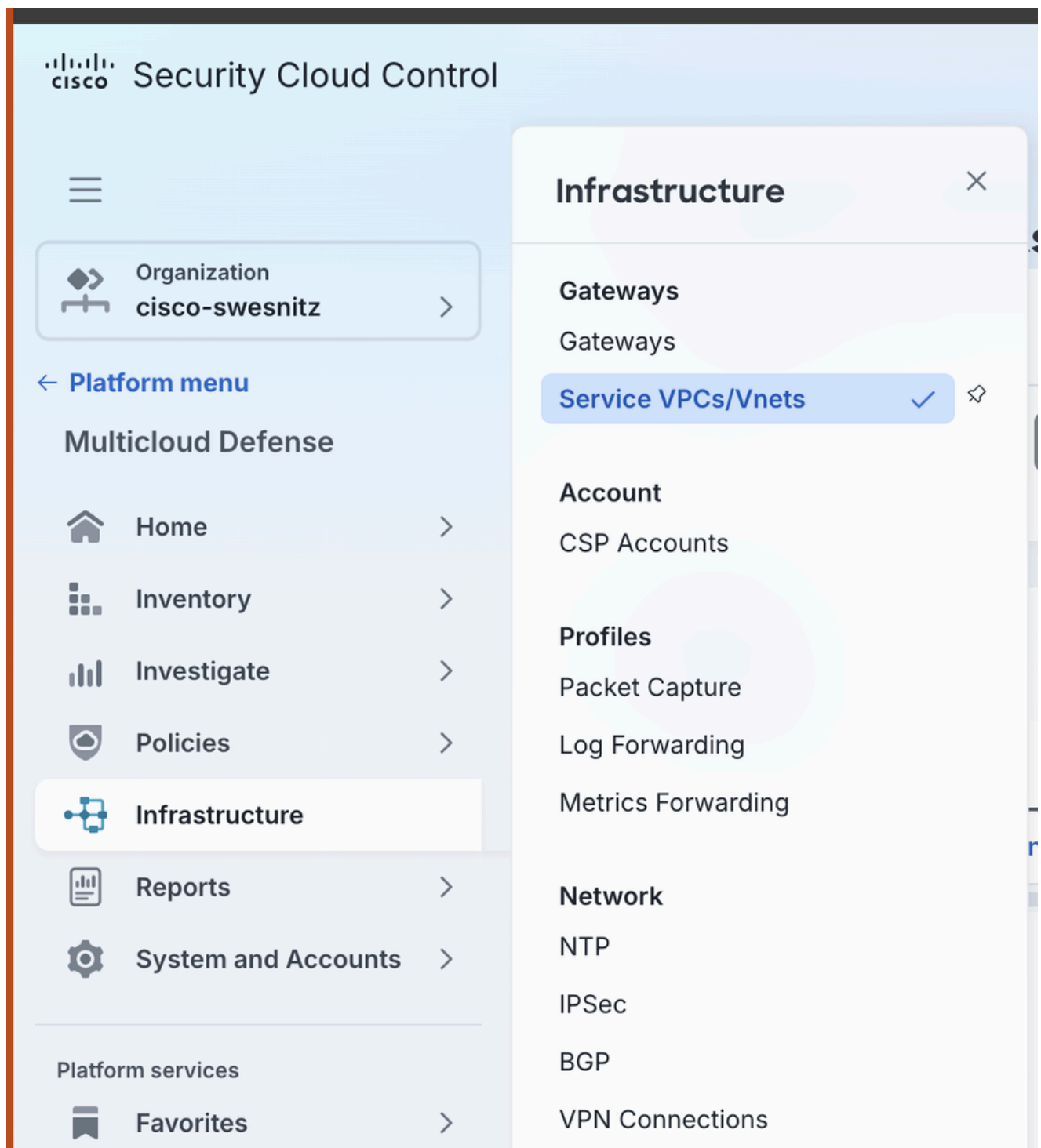
Back

7. È ora possibile visualizzare l'account caricato da Infrastruttura > Account CSP.



Creazione di una rete virtuale

1. Selezionare Infrastruttura > VPC/VPN di servizio.



2. Fare clic su Crea.

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. Immettere i seguenti valori:

- Nome: Un nome facilmente identificabile per la rete virtuale che questa procedura crea per il gateway FTDv.
- Account CSP: Il nome assegnato nella sezione Connessione dell'account di Azure a MCD.
- Regione: Area in cui viene distribuito il gateway FTDv.
- Blocco CIDR: Blocco IP univoco per il gateway di transito associato alla rete virtuale.
- Zone di disponibilità: Selezionare almeno due zone di disponibilità per la resilienza.
- Gruppo di risorse: Selezionare + Crea gruppo di risorse dal menu a discesa.
- Nome gruppo di risorse: Nome del gruppo di risorse.
- Area gruppo di risorse: Area allineata con l'area selezionata per Area.

Fare clic su Save (Salva).

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. Viene visualizzato un messaggio di operazione riuscita.

✓

Success

Service VPC/VNet created successfully.

OK

Confermare la creazione della rete virtuale dal lato di Azure, passare a Base di rete > Panoramica delle reti virtuali > Reti virtuali.

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	...

Una volta creata, la rete VPN passa a uno stato attivo.

Create

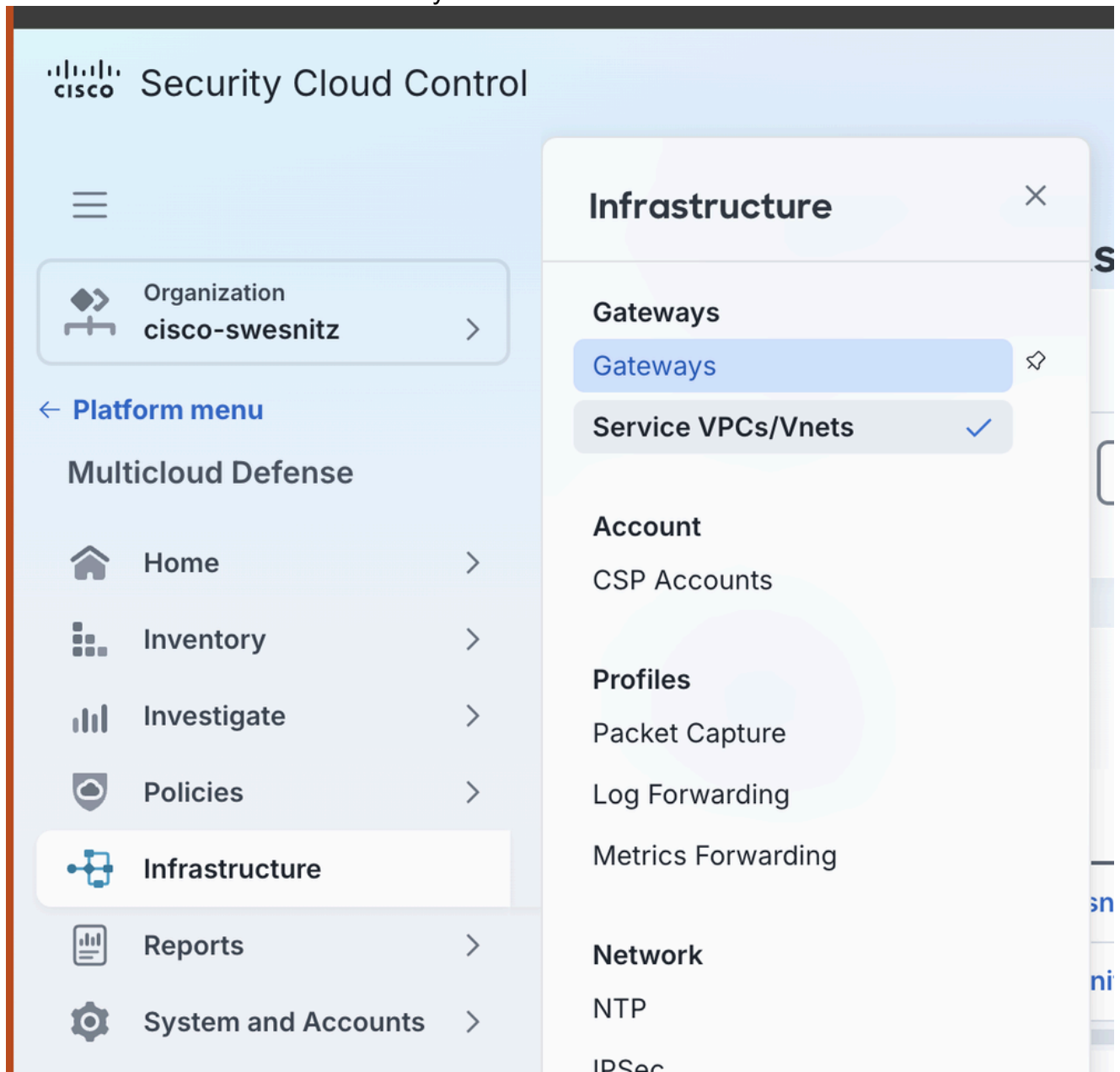
Actions

Refresh

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

Crea il gateway FTDv MCD di Azure

1. Selezionare Infrastruttura > Gateway.



2. Fare clic su Add Gateway.

The screenshot displays 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 'Name' and 'CSP Account' dropdowns. Below this is a table with columns for 'Name' and 'State'. A table row is partially visible with the name 'med lab cluster' and state 'ACTIVE'.

3. Immettere i seguenti valori:

- Account: Dal menu a discesa, selezionare l'account di Azure collegato nella sezione Connessione dell'account di Azure a MCD.
- Tipo di gateway: Selezionare FTDv Gateway.
- Nome: Un nome facilmente identificabile per il gateway FTDv.
- Tipo istanza: Il tipo di istanza appropriato per l'ambiente.
- Numero minimo di istanze: Selezionare almeno un'istanza dal menu a discesa.
- Numero massimo di istanze: Il numero desiderato di istanze FTDv massime per l'ambiente. Il massimo consentito è 10.
- Porta HealthCheck: Il valore predefinito è 65534. Questo documento non modifica questo valore.

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✕

Cancel

Next



Nota: La porta HealthCheck è il numero di porta utilizzato dal servizio di bilanciamento del carico di Multicast Defense per controllare lo stato delle istanze. I gruppi di sicurezza datapath assegnati alle istanze devono consentire il traffico su questa porta.

4. Immettere i seguenti valori:

- Proprietà: Selezionare Esci o Est-Ovest.
- Versione FTDv: La versione del software più adatta all'ambiente.
- Set di regole dei criteri: I criteri di controllo di accesso (ACP) da applicare a questo cluster FTDv.

- Password: Una password per le istanze FTDv.
- Modello licenza: Il modello di licenza desiderato.
- Livello prestazioni: Il livello appropriato per il throughput del dispositivo previsto.
- Tipi di licenza: Tipi di licenza acquistati per questa distribuzione.
- Regione: Area in cui vengono distribuite queste istanze FTDv.
- ID VPC/VNet: La rete virtuale del servizio creata nella sezione Creazione di una rete virtuale.

Create Gateway

Security * ⓘ

East West X

FTDv Version *

10.0.0

Policy Ruleset * ⓘ

Default Access Control Policy X

FTDv

Admin Password

.....
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

VPC/VNet ID * ⓘ

mcd_test_vnet-swesnitz | mcd_test_vnet-swesnitz X

Key Selection

Cancel
Back
Next

5. Creare una coppia di chiavi pubbliche. Per ulteriori informazioni, fare riferimento a [Creazione di una coppia di chiavi SSH in 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. Immettere i valori per la chiave pubblica SSH e i gruppi di risorse.

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. Disabilitare l'IP pubblico, quindi fare clic su Avanti.

Create Gateway

✓

✓

3

4

Gateway InformationGateway DetailsAdvanced SettingsReview

Public IP

☒ Disable Public IP

8. Esaminare tutti i valori specificati.

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. Dopo aver esaminato i valori e completato il caricamento delle risorse, fare clic su Fine.

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

Visualizzazione dashboard dopo il caricamento delle risorse.

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



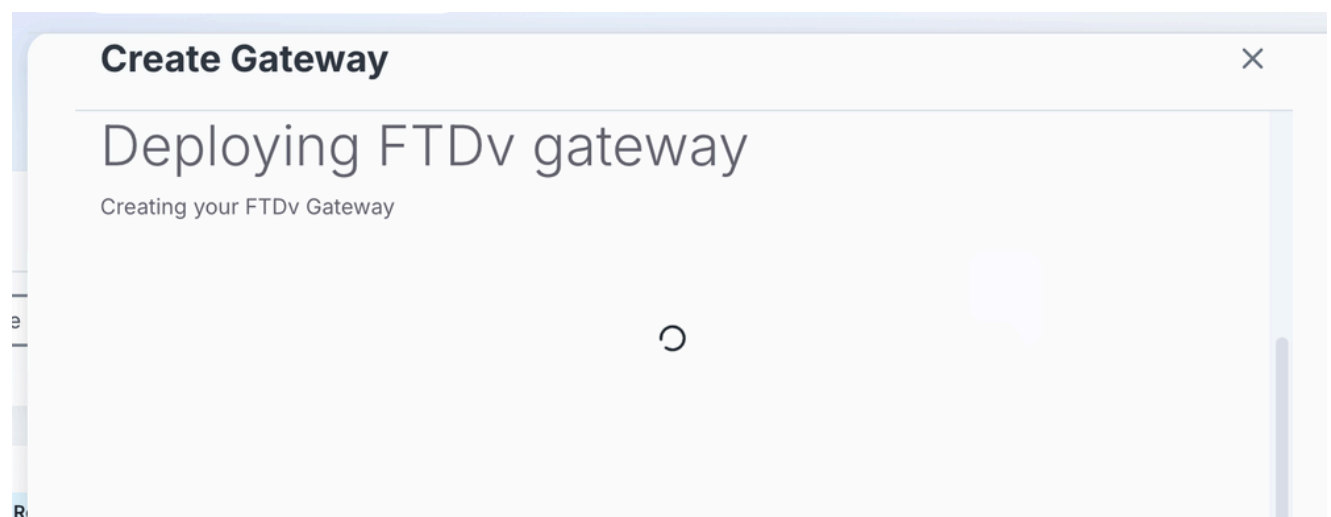
Resource	Limit	In Use	Min Usage for Gateway	Max Usage for Gateway	Recommendation
Private IPs in Subnets	254	0	1	3	
Elastic IPs	1000	51	1	3	
Load Balancers	1000	8	1	1	
Instances	25000	31	2	6	
Virtual CPUs	350	0	16	48	

Advanced Settings

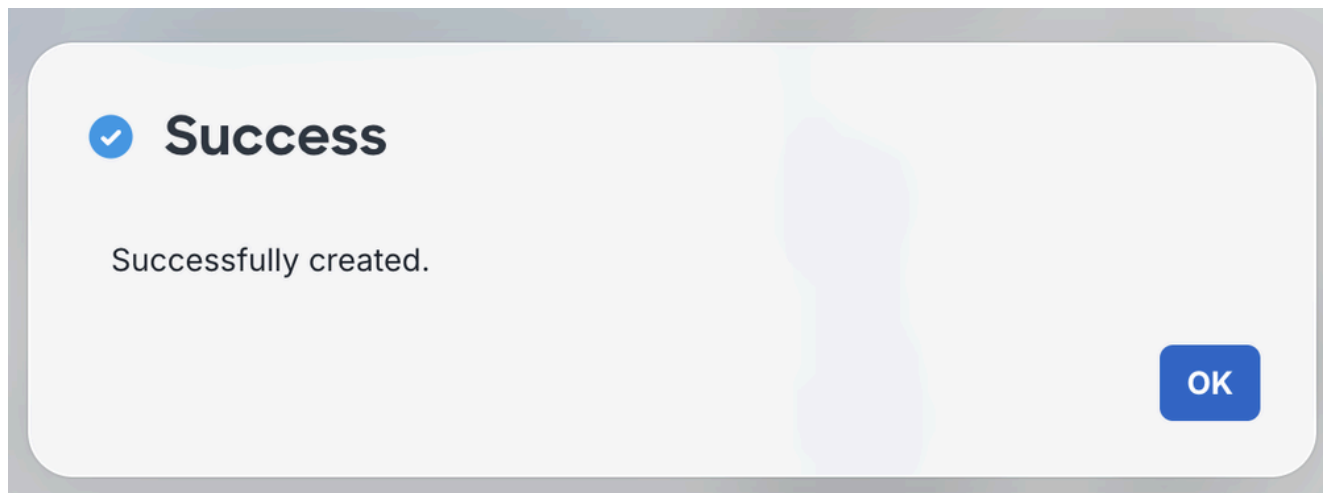
[Edit](#)**Disable Public IP**

enabled

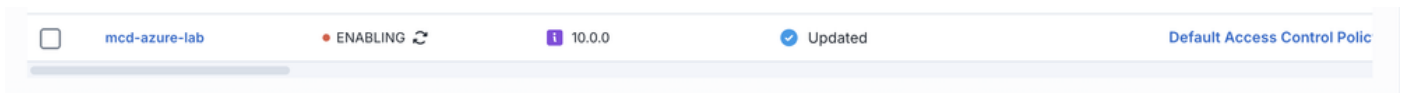
Visualizzazione dashboard della distribuzione del gateway.



10. Quando il gateway inizia la creazione, viene visualizzato un messaggio di operazione riuscita. Fare clic su OK.



Dal quadro comandi MCD, viene visualizzato lo stato ABILITAZIONE (ENABLING).



Controllare lo stato dalle schede Riepilogo e Istanze.

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

Verifica

Fare riferimento a questa sezione per verificare che la configurazione funzioni correttamente.

- In Calcola > Macchine virtuali in Azure, monitorare le istanze FTDv. Lo stato passa da Creazione a In esecuzione.

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-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 ...

- Confermare lo stato del gateway dal dashboard MCD.

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.

Informazioni correlate

- [Creare una VPC o una VNet del servizio](#)
- [Procedura di integrazione FTDv](#)
- [Configura prerequisiti gateway](#)
- [Panoramica di Difesa multicolore per Azure](#)
- [Creare e utilizzare una coppia di chiavi pubblica-privata SSH per le macchine virtuali Linux in Azure](#)
- [Documentazione e supporto tecnico – Cisco Systems](#)

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).