



Multicloud Fabric Onboarding

Table of Contents

Multicloud Fabric Onboarding	1
Introduction	2
Cloud account integration requirement	2
What cloud account integration enables	2
Before you start	3
Integration workflow	4
Activate your Multicloud Fabric trial subscription	4
Integrate an AWS account	8
Integrate an Azure account	10
Create an Azure gateway subnet	11
Create a service principal	11
Connect an Azure subscription to Multicloud Fabric	12
Integrate a Google Cloud account	15
Create a service account	15
Generate a JSON key	16
Connect a Google Cloud account to Multicloud Fabric	16
Verify cloud access in your provider console	20
AWS	20
Azure	20
Google Cloud	20
Access provider console information	20
Manage cloud account integrations	22
View cloud account details	22
Update cloud account access credentials	22
Disconnect a cloud account	22
Navigate Multicloud Fabric	24
Overview	24
Cloud Access	24
Event Log	25
Access Multicloud Fabric pages	25
Subscription and usage management	27
Multicloud Fabric pricing	27
Subscription models	27
Usage calculation	27
Data transfer charges	27
Usage guidelines and limitations	27
General Availability transition	28
Multicloud Fabric documentation	29

Multicloud Fabric Onboarding

Introduction

Multicloud Fabric is Cisco's fully managed networking service for connecting site-to-cloud and cloud-to-cloud networks. It supports networks in AWS, Azure, and Google Cloud, as well as Meraki sites.

In Multicloud Fabric, you:

1. Authorize cloud access for the cloud providers you use.
2. Onboard the networks you want to include in the fabric.
3. Choose which resources should communicate.

Multicloud Fabric then provisions the routing, tunnels, and policies needed to realize those connections. It simplifies multicloud networking by giving you a way to:

- Discover and manage network resources.
- Define specific connectivity between the resources you choose.
- Monitor connection health and events, including event history, to help you investigate connectivity issues.

Rather than automatically connecting every onboarded network, Multicloud Fabric's Zero Trust Routing capability distributes only the routes authorized by your connection choices.

Cloud account integration requirement

Your AWS, Azure, or Google Cloud environment is administered outside Multicloud Fabric. As a result, Multicloud Fabric needs an explicit, customer-authorized cloud identity to call the selected provider's control-plane APIs for the approved scope. This authorization lets Multicloud Fabric discover your network inventory, as well as create and manage the Multicloud Fabric-owned cloud connectivity resources needed for integration.

What cloud account integration enables

Refer to this table for a description of what cloud account integration enables for Multicloud Fabric.

Enabled capability	What Multicloud Fabric is authorized to do	When it takes effect
Cloud discovery	Read the data required to show eligible resources in Multicloud Fabric, such as the authorized account, subscription, CIDR, and related inventory.	Initial discovery starts after the integration validates.
Network onboarding	Create and manage the connectivity resources for a selected network, such as the supported cloud-side VPN, gateway, and tunnel.	Only after you select a discovered network and submit onboarding.

Enabled capability	What Multicloud Fabric is authorized to do	When it takes effect
Connections and route exchange	Use onboarded cloud networks as connection endpoints, and apply the explicit route-exchange intent.	Only after the endpoints are onboarded and you create a connection.
Operations and lifecycle	Correlate status for items such as integration, discovery, attachment, and events. Support approved update and offboarding workflows	As resources and operations exist, and only when you initiate the applicable lifecycle action.

Before you start

You need access to create or modify the required identity and access resources. Based on your company policies, you may need your IT or cloud administration team to provision these rights.

Refer to this table for a description of what you configure for your cloud account.

Provider	Your scope	Identity you configure	How Multicloud Fabric uses it
AWS	Your AWS account	A cross-account IAM role ARN with the Multicloud Fabric principal and external ID in its trust relationship.	Multicloud Fabric assumes the role through AWS STS and validates the requested access.
Azure	Your Azure subscription	A Microsoft Entra service principal: Tenant ID, client/application ID, client secret, and the intended subscription role assignment.	Multicloud Fabric authenticates the service principal and validates Azure Resource Manager access.
Google Cloud	Your Google Cloud project or a supported parent scope	A service-account identity or material with the required IAM roles and enabled APIs.	Multicloud Fabric authenticates the service account and validates access to the selected Google Cloud scope.

Integration workflow

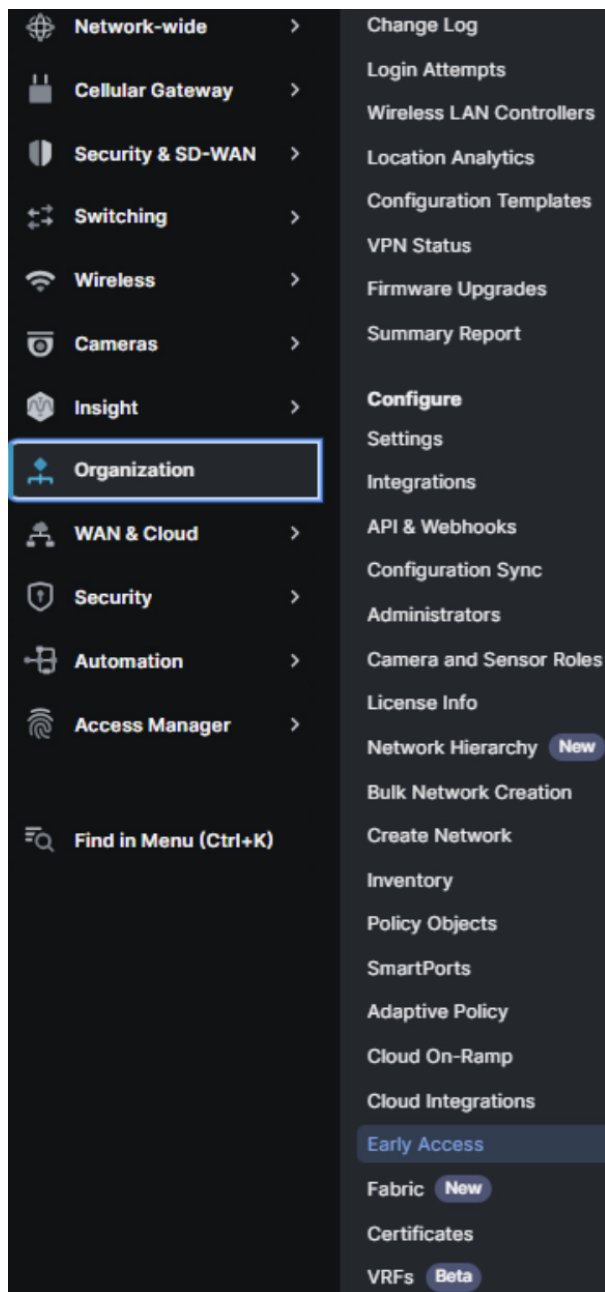
Complete these tasks to access and set up Multicloud Fabric for use:

1. Onboard to Cisco Cloud Control. Refer to [Cisco Cloud Control Getting Started](#).
2. [Activate your Multicloud Fabric trial subscription](#).
3. Integrate your cloud service provider (CSP) account by completing the relevant procedure:
 - [AWS](#)
 - [Azure](#)
 - [Google Cloud](#)

Activate your Multicloud Fabric trial subscription

Before you begin

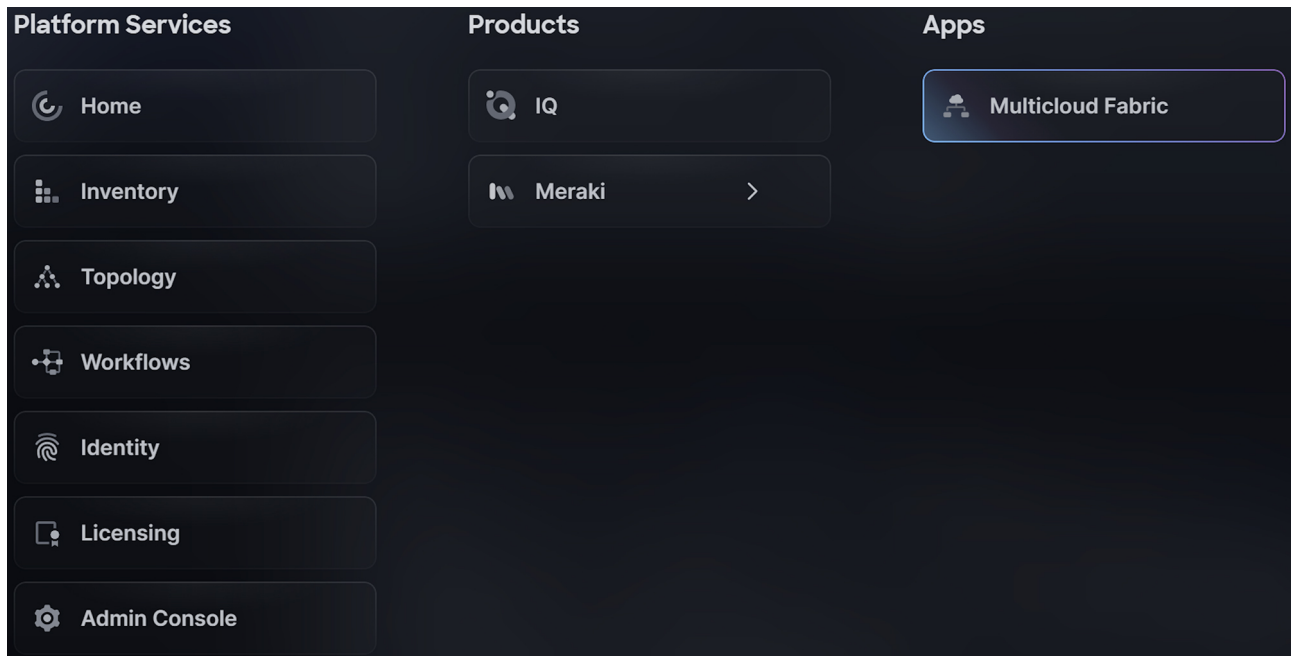
- You must be a Meraki organization administrator and use a Meraki identity to activate Multicloud Fabric for use.
- Before accessing Multicloud Fabric, you must enable the Early Access API in the Meraki Dashboard:
 1. Select **Organization > Early Access**.



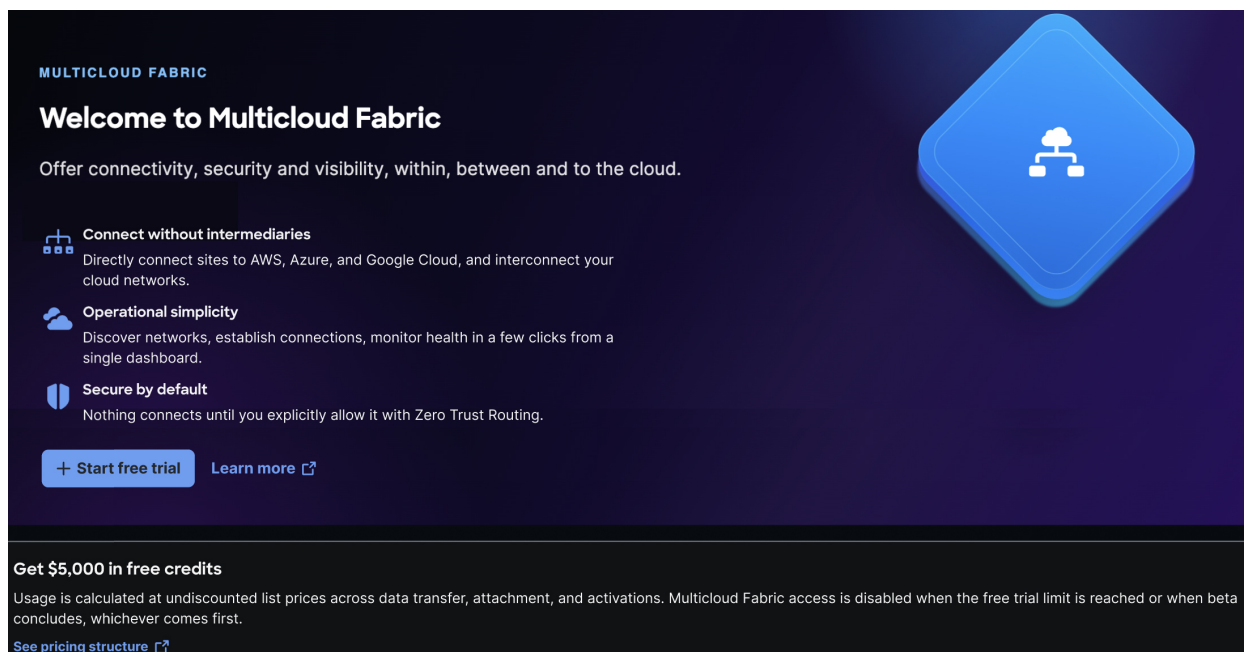
2. In **Meraki Early Access Program**, scroll down to the **Early API Access** section.
3. Select the opt-in toggle to enable the API.
For additional information, refer to this [page](#).

Follow these steps to activate your trial subscription for Multicloud Fabric:

1. Open Cisco Cloud Control and sign in with your existing Meraki credentials.
2. Select .
3. Under **Apps**, select **Multicloud Fabric**.



- o If Multicloud Fabric is already enabled for you, Multicloud Fabric’s overview page opens and you should not be prompted to sign in a second time. Skip ahead to Step 7.
- o If you are not yet authorized to access Multicloud Fabric, a splash page opens.



Proceed to Step 4.

4. Select **Start free trial**.
5. Complete these actions:
 - a. Select the tenant you want to enable Multicloud Fabric for.
If you have grouped tenants, select the single Meraki tenant in which you want to enable Multicloud Fabric.
 - b. Review Multicloud Fabric’s terms and conditions.
 - c. Check the check boxes.
 - d. Type **Subscribe**, then select **Confirm**.

Start Free Trial

Get \$5,000 in free credits

Usage is calculated at undiscounted list prices across data transfer, attachment, and activations. Multicloud Fabric access is disabled when the free trial limit is reached or when beta concludes, whichever comes first.

[See pricing structure](#) 

 All members of this tenant will have access to Multicloud Fabric

☒ Enable Multicloud Fabric for MCF-lab tenant under **ACME** tenant group

☒ I understand Multicloud Fabric beta is for non-production workloads only

☒ I have read and accept the [Cisco Multicloud Fabric Terms and Conditions](#) 

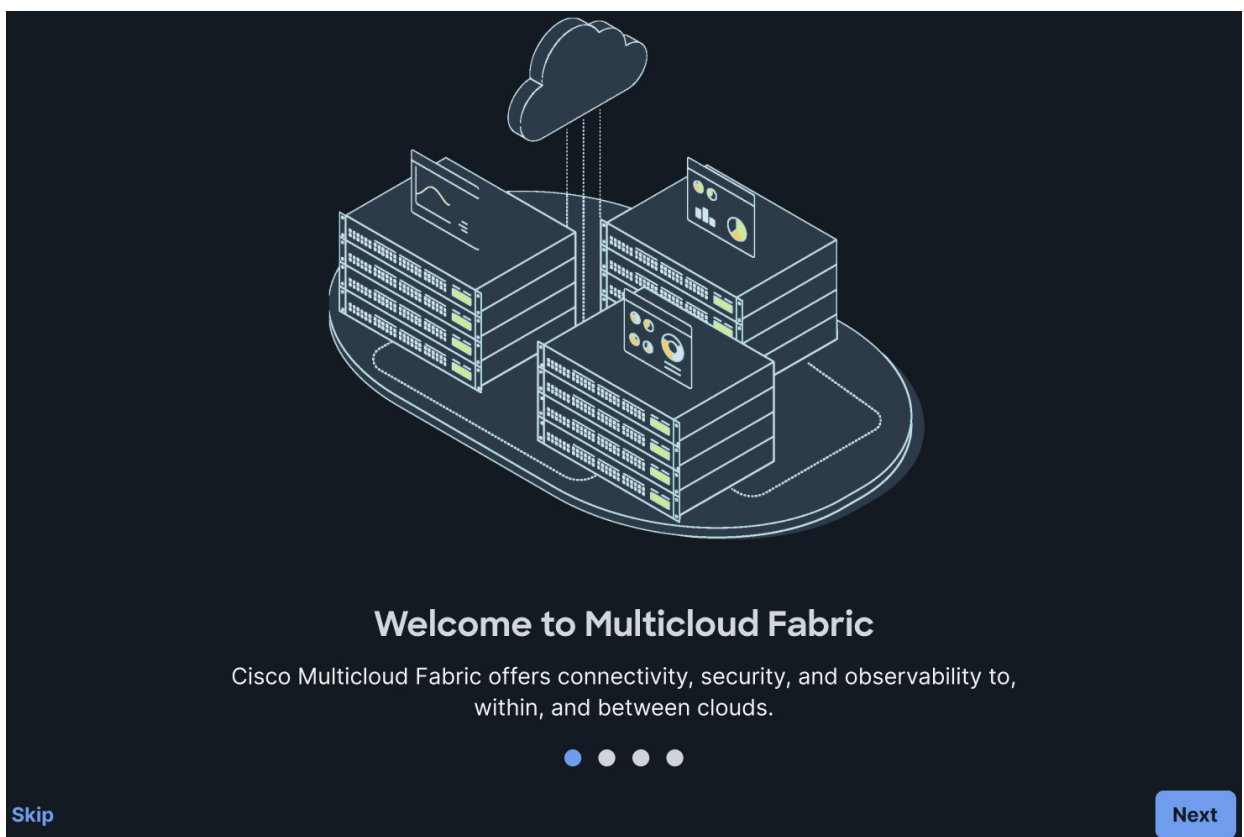
Type "Subscribe" to confirm.

Subscribe

Cancel

Confirm

After your access is enabled, the **Welcome to Multicloud Fabric** slider opens.



6. Select **Next** to cycle through the slider's screens, which describe Multicloud Fabric's core features.

7. In the last screen, select **Onboard network** to open Multicloud Fabric's **Overview**.

Integrate an AWS account

Complete the AWS integration workflow to establish IAM access for Multicloud Fabric and provide the necessary role Amazon Resource Name (ARN).

1. In Multicloud Fabric's left navigation, select **Cloud Access**.
2. Select **Add cloud integration > AWS**.
Review access rights opens.

Connect AWS Multicloud Network

1 ————— 2 ————— 3

Review access rights Create IAM roles Enter ARNs

Review access rights

At a minimum, Cisco can discover cloud account information.
Grant write access to allow Cisco to perform cloud networking actions.

- ✓ **Account discovery**
Discover account metadata, such as account names and IDs; VPC names, IDs, tags; and subnets and route tables.
- ✓ **Create onboarding resources**
Create virtual private gateways (VGWs), transit gateway attachments (TGWs), and endpoints. Change route table propagation if needed.

Cancel Next

3. Review the access rights that you are granting Multicloud Fabric, then select **Next**.
Create IAM roles opens.

Connect AWS

Multicloud Network

1

Review access rights

2

Create IAM roles

3

Enter ARNs

Create IAM roles

Follow the instructions to create IAM roles in AWS.

- Create IAM roles**
Create a new IAM role in one or more AWS accounts.
- Apply permission and trust policies**
Apply the permission and trust policies below in each new IAM role.

Copy permission policy

Download

```
1  {
2    "Version": "2012-10-17",
3    "Statement": [
4      {
5        "Sid": "VpcLattice",
6        "Effect": "Allow",
7        "Action": [
8          "vpc-lattice:*",
9          "vpc-lattice-svcs:*"
10       ],
11       "Resource": "*"
12     }
13   ]
14 }
```

Cancel

Back

Next



For Beta, an IAM role is already configured, as well as the required permission and trust policies.

- In the trust policy, copy the role's ARN (**arn:aws:iam::xxxxxxxxxxxx:role/mcn-integrations-role**) and then select **Next**.

Amazon Resource Names (ARNs) opens.

Connect AWS

Multicloud Network

✓

Review access rights

✓

Create IAM roles

3

Enter ARNs

Amazon Resource Names (ARNs)

Copy and paste the role ARN created in each AWS account.

Role ARN #1 *

Next steps

Cisco will query AWS to confirm the IAM roles have been created. This query will happen automatically every few minutes and when a “refresh” is requested, until access is confirmed. Review account status in [Integrations](#).

Once confirmed, Cisco will discover networking elements (e.g., VPCs, subnets) and subscribe to configuration updates. Discovered resources will be shown in Multicloud Fabric (MCF).

Cancel

Back

Save

5. Paste the role’s ARN into **Role ARN #1**, then select **Save**.

Integrate an Azure account

The Azure integration workflow consists of these tasks:

1. [Create an Azure gateway subnet](#).
2. [Create a service principal and grant subscription access](#).
3. [Connect an Azure subscription to Multicloud Fabric](#).



Azure VNets that are onboarded to Multicloud Fabric must not use or overlap the 10.254.0.0/16 address range. Multicloud Fabric’s Beta release reserves this range for internal IPsec tunnel addressing and BGP peering. If an Azure VNet’s address space overlaps this range, the VNet cannot be onboarded successfully. Choose a non-overlapping address range before onboarding.

Create an Azure gateway subnet

Before integrating Azure, create a gateway subnet in the Azure virtual network that Multicloud Fabric should attach to.

1. In the Azure portal, search for and select **virtual networks**.
2. In **Virtual networks**, select the virtual network you want to add a subnet to.
3. In the left navigation, select **Subnets**.
4. Select **+ Subnet**.
5. Enter this information for the subnet, then select **Save**:
 - **Subnet purpose**: enter **Virtual Network Gateway**
 - **Name**: enter **GatewaySubnet**
 - **Include an IPv4 address space**: select this option
 - **IPv4 address range**: enter the appropriate address range
 - **Starting address**: enter the range's starting IP address
 - **Size**: enter a subnet size of /27 or larger

Multicloud Fabric relies on the **GatewaySubnet** name to select the correct attachment subnet. Multicloud Fabric does not automatically choose the subnet address range because that range must come from your Azure virtual network space.

Create a service principal

To create a service principal and grant access to subscriptions in Azure, complete these tasks:

1. [Register a new application](#).
2. [Create a client secret](#).
3. [Add a role assignment to a subscription](#).

Register a new application

1. In the Azure portal, select **Microsoft Entra ID**.
2. From the left navigation, select **App registrations**.
3. Select **New registration**.
4. Enter the application's name.
5. In **Supported account types**, select **Accounts in this organization directory only (Default Directory only - Single tenant)**.
6. Select **Register**.

Create a client secret

1. In the Azure portal, select **Manage > Certificates & secrets > Client secrets**.
2. Select **New Client Secret**.
3. In **Add a client secret**:

- a. Enter a description for the secret.
- b. Set how long the secret will be valid.
- c. Select **Add**.
Make sure to record the secret's value.

Add a role assignment to a subscription

1. From the left navigation, select **Access control (IAM)**.
2. Select **Add > Add role assignment**.
3. In **Job function roles**, select **Network Contributor**, and then select **Next**.
4. Select **Members**.
5. In **Assign access to**, select **User, group, or service principal**.
6. Choose **Select members**.
7. Select the application you created previously, and then choose **Save**.
8. Select **Next**.
9. Select **Review + assign**, and then select **Review + assign**.

Connect an Azure subscription to Multicloud Fabric

Complete the Azure integration workflow to provide service principal credentials to Multicloud Fabric and grant Multicloud Fabric access to the Azure subscriptions that it should connect to.

1. In Multicloud Fabric's left navigation, select **Cloud Access**.
2. Select **Add cloud integration > Azure**.
Access rights opens.

Connect Azure Multicloud Network

1

Review access
rights

2

Configure access

3

Confirm
subscriptions

Access rights

Cisco can discover cloud subscription information and perform cloud networking actions.



Subscription discovery

Discover subscription metadata, such as subscription names and IDs; VNet names, IDs, tags; and subnets and route tables.



Create onboarding resources

Create virtual network gateways, local network gateways, VPN sites, and site-to-site connections. Change route table propagation if needed

Cancel

Next

3. Review the access rights that you are granting Multicloud Fabric, then select **Next**. **Configure access to Azure subscriptions** opens.

Connect Azure

Multicloud Network

1

Review access rights

2

Configure access

3

Confirm subscriptions

Configure access to Azure subscriptions

Follow the instructions below to create a service principal and grant access to subscriptions in Azure

- Create a service principal**

Create a service principal in your active directory and share its credentials here.

How will these credentials be used?

Directory (tenant) ID

The unique identifier for your Azure AD tenant.

Client (application) ID

The unique identifier for your application.

Client secret

[Show](#)

The secret value you create for the application.
- Grant access to subscriptions**

[Cancel](#)[Back](#)[Next](#)

4. Enter this information, then select **Next**:

- o Your Azure tenant's ID and client ID (in the Azure portal, select **Overview** to view these values)
- o Your application's client secret (in the Azure portal, select **Manage > Certificates & secrets > Client secrets**).

Confirm subscriptions opens.

Connect Azure

Multicloud Network

✓

Review access rights

✓

Configure access

3

Confirm subscriptions

Confirm subscriptions

Review current subscriptions in Acme-Services. If a subscription is missing, ensure it has been granted access to this service principal.

☒ Automatically include access to new and future subscriptions

1 results
Refresh

Name	Id
mcn-azure-	0f5fe80a-a853-

Cancel

Back

Save

- Confirm that the subscriptions configured for your Azure account are displayed. Then select **Save**.

Integrate a Google Cloud account

To onboard a Google Cloud account, complete these tasks:

- [Create a service account.](#)
- [Generate a JSON key.](#)
- [Connect a Google Cloud account to Multicloud Fabric.](#)

Create a service account

- In your Google Cloud project, ensure these APIs are enabled:
 - Compute Engine API
 - Cloud Resource Manager API
 - Logs API
- Sign in to the Google Cloud console and select **Identity & Access > Service Accounts**.
- Select **Create project**.
- Enter a service account name and description, then select **Create and continue**.
The Google Cloud console generates a service account ID based on the name you enter. If you need to, change the ID. You will not be able to do so later.
- Set these permissions:

- o Logs Viewer
- o Network Administrator
- o Viewer

6. Select **Continue**, then select **Done**.

Generate a JSON key

1. In **Identity & Access > Service Accounts**, select  > **Manage keys**.
2. Select **Add key > Create new key**.
3. Ensure **JSON** is set as the key type, then select **Create**.
4. Download a copy of the JSON file.

Connect a Google Cloud account to Multicloud Fabric

1. In Multicloud Fabric's left navigation, select **Cloud Access**.
2. Select **Add cloud integration > Google Cloud**.
Review access rights opens.

Connect Google Cloud Multicloud Network

1

Review access
rights

2

Configure access

3

Confirm account
scope

Review access rights

Cisco can discover cloud subscription information and perform cloud networking actions.

✓ **Project discovery**

Discover project metadata, such as project names and IDs; VPC names, IDs, labels; and subnets and route tables.

✓ **Create onboarding resources**

Create cloud and peer VPN gateways, cloud VPN tunnels, and cloud routers. Change route table propagation if needed.

Cancel

Next

3. Review the access rights that you are granting Multicloud Fabric, then select **Next**. **Configure access to Google projects** opens.



Review access
rights

2

Configure access

3

Confirm account
scope

Configure access to Google projects

Follow the instructions below to configure discovery scope and access to projects in Google Cloud.

1) Select discovery scope

Choose how you want to discover Google Cloud resources.

- ☒ Single Project Discovery
- ☐ Organization-wide Discovery
- ☐ Folder-based Discovery

Discover networks and subnets for one GCP project

2) Enable required APIs

In your Google Cloud project, ensure the following APIs are enabled:

- ✓ Compute Engine API
- ✓ Cloud Resource Manager API
- ✓ Logs API

3) Create a service account

In your main Google Cloud project, add a new service account. Create a JSON key file for the service account and upload it here.

[How will this key be used?](#)

Cancel

Back

Next

4. Complete these tasks, then select **Next**.

- a. Set **Single Project Discovery** as the discovery scope.
- b. In **Create a service account**, drag the JSON key you created previously.
Confirm projects opens.

Connect Google Cloud

Multicloud Network

✓

Review access rights

✓

Configure access

3

Confirm account scope

Confirm projects

Review current projects in mc-n-service-account@gcp-mcnqagcptoniak-nprd-81276.iam.gserviceaccount.com. If a project is missing, ensure it has been granted access to this service account.

✓

 Automatically include access to new and future projects

Q Search by name

1 results

Refresh

Name	Id
mc-n-qa-	gcp-mcn-

Cancel

Back

Save

5. Confirm that the projects configured for your Google Cloud account are displayed. Then select **Save**.

Verify cloud access in your provider console

If an integration does not validate, or if you want to confirm the configured scope, compare the values shown in your provider console against those in **Cloud Access**.

AWS

1. In AWS, select **AWS Console > IAM > Roles**.
2. Select the same role that is shown in **Cloud Access**.
3. In **Trust relationships**, confirm that the Multicloud Fabric principal and external ID match the values presented by Multicloud Fabric.
4. In **Permissions**, confirm that the attached or inline policy corresponds to the access rights you selected.

Azure

1. In the Azure portal, select **Subscriptions**.
2. Select the target subscription.
3. Select **Access control (IAM) > Role assignments** or **Check access**.
4. Select the Multicloud Fabric service principal.
5. Compare the subscription, tenant, client/application ID, role, and assignment scope values with those provided in **Cloud Access**.
6. Select **Microsoft Entra ID > App registrations** to confirm application identity and secret expiry.

Google Cloud

1. In the Google Cloud console, select the target project.
2. View these pages:
 - Select **IAM & Admin > IAM** to confirm the service-account principal and roles.
 - Select **IAM & Admin > Service Accounts** to confirm the service-account email and key status.
 - Select **APIs & Services > Enabled APIs & services** to confirm that the required APIs are enabled.
3. Compare the project ID and service-account identity with the values displayed in **Cloud Access**.

Access provider console information

Refer to these pages for more information about verifying cloud access in your provider's console:

- [AWS IAM trust-policy verification](#)
- [AWS third-party role and external-ID guidance](#)
- [Azure role-assignment and check access guidance](#)
- [Google Cloud IAM access guidance](#)

- [Google Cloud enabled-API guidance](#)

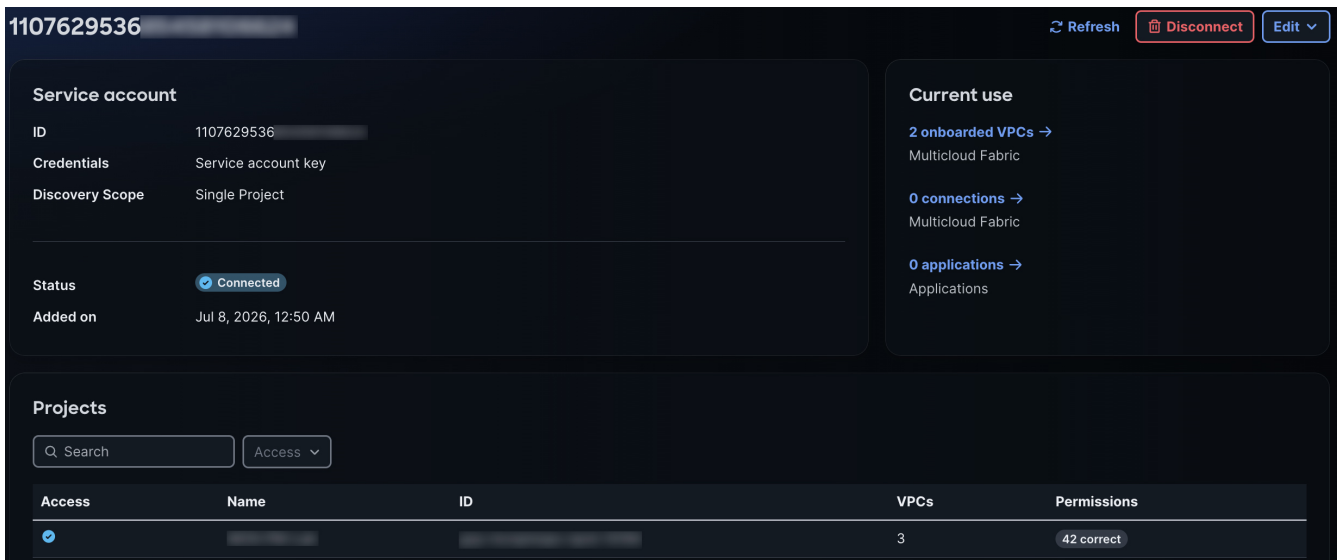
Manage cloud account integrations

View cloud account details

From the details page for a cloud account that has been integrated with Multicloud Fabric, you can:

- View information such as the account's ID, current status, and configured projects or subscriptions.
- Update the account's inventory information (in Multicloud Fabric Deployment, refer to the "Configure and verify discovery" topic)
- [Update the account's access credentials.](#)
- [Disconnect the account from Multicloud Fabric.](#)

To open a cloud account's details page, select its link in **Cloud Access**. You can also select  **> See details.**



1107629536 Refresh Disconnect Edit

Service account

ID: 1107629536

Credentials: Service account key

Discovery Scope: Single Project

Status: Connected

Added on: Jul 8, 2026, 12:50 AM

Current use

2 onboarded VPCs →
Multicloud Fabric

0 connections →
Multicloud Fabric

0 applications →
Applications

Projects

Q Search Access

Access	Name	ID	VPCs	Permissions
Connected			3	42 correct

Update cloud account access credentials

Follow these steps to update the access credentials for either an Azure or Google Cloud account.

1. Select **Cloud Access**.
2. Select the account whose access credentials you want to update to open its details page.
3. Select **Edit > Rotate credentials**.
4. Update the account's credentials:
 - For an Azure account, enter the new client secret.
 - For a Google Cloud account, upload the new service account key (.json).
5. Select **Save**.

Disconnect a cloud account

Follow these steps if you need to disconnect a cloud account that has been integrated with Multicloud

Fabric.

1. Select **Cloud Access**.
2. Select the account you want to disconnect to open its details page.
3. Select **Disconnect**.

Disconnect integration

Multicloud Fabric

Disconnect multicloud network's integration with your 1107629536 account.

Remove VPCs

Action required

Remove all VPCs in this account from Multicloud Fabric before removing the integration.

2 Onboarded VPCs

Q Search

Status

MCF Region

Status	VPC name	VPC ID	Tags	Subnets	MCF region
	app-	360531824		1	Remove
	client-	246996074		1	Remove

Rows per page 10 1-2 of 2 < 1 >

Disconnect

Cancel

Cisco will permanently forget this account's credentials and delete VPC details.

4. In **Disconnect integration**:
 - a. Select **Remove** for every VPC or VNet that was onboarded with this account.
You will not be able to disconnect the account without doing this first.
 - b. Select **Disconnect**.

Navigate Multicloud Fabric

Three components comprise Multicloud Fabric's UI:

- [Overview](#)
- [Cloud Access](#)
- [Event Log](#)

Overview

Overview serves as the starting point for your Multicloud Fabric session:

- Scan the tiles at the top of this page to quickly determine the status of the connections, Multicloud Fabric regions, sites, and VPCs that are managed by Multicloud Fabric.
- Select **Onboard network** to initiate the onboarding workflow for new VPCs/VNets and Meraki networks.
- Select **Connect resources** to connect cloud resources and sites.
- Select **Connections**, **Sites**, or **VPCs** to view the items that have been configured for these categories and manage them.

Networking

Connections 9 total

9 Enabled 0 Disabled

MCF regions 7 total

4 Healthy 0 Degraded 0 Offline

Sites 5 total

2 Healthy 0 Degraded 0 Offline

VPCs 9 total

6 Healthy 0 Degraded 0 Offline

[+ Onboard network](#) [Connect resources](#)

Connections **MCF regions** **Sites** **VPCs**

Search Provider ☐ Show default VPCs Filters

☐		VPC name	VPC ID	Tags	Subnets	MCF region and AZ	Provider	Route table propagation	
☐		app-analytics		2	2	eastus	Azure	Specific routes	...
☐		app-datalake			1		Google Cloud	Specific routes	...
☐		app-inventory		1	1	us-east-1	AWS	Specific routes	...

Cloud Access

In **Cloud Access**, you can view the cloud accounts that have been onboarded with Multicloud Fabric. From here, you can:

- Onboard new cloud accounts.
- Select a cloud account to [view its details page](#).

Cloud Access

+ Add cloud integration

Integrate cloud accounts to let Multicloud Fabric view and onboard cloud networks.

Q Search

Provider

VPC use

Access rights

Status

Filters

Name	Provider	Accounts	VPCs	Credentials	Access rights	Status	
	AWS	1	17 4 in MCF	IAM role	Onboarding resources	Connected	...
	Google Cloud	1	3 2 in MCF	Access keys	Onboarding resources	Connected	...
	Azure	1	3 3 in MCF	Access keys	Onboarding resources	Connected	...

Rows per page

10

1-3 of 3

1

Event Log

The **Event Log** lists all the events that have taken place in your Multicloud Fabric environment over the time period you specify. From here, you can:

- View the chart to quickly identify times where there has been more activity than usual.
- Select an event to view its details.

Event Log

A chronological record of configuration changes, connectivity state transitions, and system-initiated actions across the MCF environment.

Q Search

Last 24 hours

Entity type

Entity

Filters

577 results

Sep 16, 2026, 15:53 – Sep 17, 2026, 15:53

Time	Entity type	Entity	Event	Details	User	VPC	
Sep 17, 2026, 15:49:31	Integration		Discovery finished	Discovery finished with status "succeeded"	—	—	
Sep 17, 2026, 15:49:31	Integration		Discovery started	Discovery started for integration	—	—	
Sep 17, 2026, 15:44:31	Integration		Discovery finished	Discovery finished with status "succeeded"	—	—	

Access Multicloud Fabric pages

The navigation paths for Multicloud Fabric pages vary slightly, depending on whether you are a North American customer accessing Multicloud Fabric through Cisco Cloud Control or a European customer accessing Multicloud Fabric through the Meraki Dashboard. The available functionality is identical in both.

Cisco Cloud Control (North American customers)

1. In the Cisco Cloud Control top navigation bar, select .
2. Under **Apps**, select **Multicloud Fabric**.
3. From the left navigation, select **Overview**, **Cloud Access**, or **Event Log** to open the corresponding page.

Meraki Dashboard (European customers)

1. From the left navigation, select **WAN & Cloud**.
2. Select **Overview**, **Cloud Access**, or **Event Log** to open the corresponding page.

Subscription and usage management

Multicloud Fabric pricing

Multicloud Fabric uses a consumption-based pricing model that is tracked through drawdown PIDs. This model mirrors cloud-native billing, so your costs align precisely with your infrastructure usage.

Subscription models

Two subscription models are available:

- **MCF-UNCOMMITTED:** A pay-as-you-go option suited for variable usage, or for cases where an upfront commitment is not feasible.
- **MCF-COMMITTED:** A subscription suited for cases where usage can be estimated in advance and higher discounts are desirable. This option requires an upfront commitment of at least \$10,000, which is drawn down as usage is reported.



You do not need to manage individual drawdown PIDs. The platform tracks usage automatically.

Usage calculation

Usage is calculated from the following meters:

- Attachments: Billed per hour for each attached site, VPC, and Multicloud Fabric region.
- Data transfer: Billed per GB. Refer to [Data Transfer Charges](#) for more information.
- Premium services: Billed per service used, such as NAT and security service chaining.

Data transfer charges

Data transfer is priced according to a rate table that varies by cloud provider and by the direction of egress. Charges apply to traffic sent:

- Across availability zones
- Across regions
- Across clouds or to the internet (internet-out)

Ingress to a cloud is never billed, so you pay only for outbound traffic and service usage. This transparent, consumption-driven structure lets you align networking spend with your organization's multicloud traffic patterns.

Usage guidelines and limitations

- **Non-production policy:** The public Beta is strictly for non-production evaluation. You must not use production data or production workloads.
- **Spend cap:** The trial includes up to \$5,000 in usage, calculated using undiscounted list prices. Usage includes data transfer costs, attachment costs, and Multicloud Fabric-region activation

costs. Access is disabled when this limit is reached. All connections are disabled, and Multicloud Fabric-routed traffic is stopped. However, your configuration settings are preserved.

- **Usage warnings:**

- **Threshold notifications:** A notification appears when usage reaches 50% (\$2,500) and again at 90% (\$4,500) of the usage limit. The 90% notification reappears after each login until you dismiss it.
- **Usage visibility:** Notifications are the only indicator of consumption. The dashboard displays a warning banner when a usage threshold is crossed, but it does not display your actual dollar amount of usage.
- **End-of-program warnings:** Warnings begin two weeks before the public Beta ends and include a daily countdown until the program concludes.

General Availability transition

- **Retirement:** The public Beta program will end when Multicloud Fabric achieves General Availability (GA) in November 2026.
- **Commercial conversion:** At GA, free trial access is disabled. You can transition to commercial access by purchasing a license through Cisco Commerce Workspace (CCW) or a supported CSP marketplace.
- **License claiming:** To claim your Multicloud Fabric license:
 1. With Multicloud Fabric open, select **Subscription** in the left navigation.
 2. Select **Claim license key**.
 3. Enter the key for your organization or tenant.
A valid claim replaces free trial access with commercial access.
- **Retention window:** After GA, Beta environments and connection settings are retained for 30 days. A valid claim within this window restores your previous Multicloud Fabric connection configuration. If no claim is made by the 30-day deadline, all retained Beta environments and settings are deleted.



To move Beta network configurations to a commercial subscription, you must complete the standard license claim process.

Multicloud Fabric documentation

- [Multicloud Fabric Onboarding \(this document\)](#)
- [Multicloud Fabric Deployment](#)
- [Multicloud Fabric Troubleshooting](#)
- [Release Notes for Multicloud Fabric](#)