# Using VMware Cloud Services Console

VMware Cloud services

You can find the most up-to-date technical documentation on the VMware website at:

https://docs.vmware.com/

**VMware, Inc.**
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

# Contents

# What is Cloud Services Console

1

The VMware Cloud Services Console lets you to manage your entire VMware Cloud services portfolio across hybrid and native public clouds.

To learn how to manage your users and groups, assign them roles to your Organization's resources and services, and view the OAuth apps that have access to your Organization, see our Identity & Access Management documentation.

Looking for information about your current costs and your last billing statement? Do you need to manage your payment methods or change your default payment method? Do you want information about adding promotional credits and commitments? See our Billing & Subscriptions documentation.

To see how to manage your Organizations, create OAuth apps in your Organization, and in the event that you belong to more than one Organization, switch between Organizations, see Managing Your Organizations.

Do you want to change your language and regional formatting, secure your account with MFA, generate API tokens, and edit your user profile? Look no further! See how to Manage Your Account.

# How do I sign up for VMware Cloud Services

2

Whether you need to migrate to the cloud, unify multi-cloud operations, scale on demand, or build modern apps, at VMware Cloud we've got you covered.

There are multiple ways to start using VMware Cloud services. As a new or existing VMware Cloud services user, you can onboard a service by doing one of the following:

- Purchase a service from the VMware Marketing website.
- Sign up for a free or trial service from the VMware Marketing website.
- Purchase a service from VMware Sales.
- Purchase a service from a VMware partner reseller.

Depending on the service you are onboarding, there can be differences in the onboarding workflow.

If your enterprise already uses VMware Cloud services, you can onboard yourself in an existing Organization by requesting access to the Organization. The procedure for requesting and receiving first-time access to a VMware Cloud services Organization can differ based on your account.

- If your account is not federated, see How do I onboard as a user in VMware Cloud Services.
- If your account is federated, see How do I onboard as a user with a federated account.

The typical sequence of steps for signing up for VMware Cloud services through service onboarding is the following:

### Procedure

1. Initiate the onboarding process from the service sign-up or from your invitation link.
2. If you don't have VMware account, follow the steps to create one.
3. If you already have a VMware account, sign in to VMware Cloud Services.
4. Create or select a VMware Cloud services Organization in which to onboard the service.
5. Once you onboard the service in an Organization, you become an Organization Owner who can invite other users and allow access to the Organization and its services:

   a. From the main left-side menu, select **Identity & Access > Active Users**.

   b. Click **Add Users**.

c Type the email address of the user you want to invite.

d Select Organization and service roles.

e Select the checkbox for email invitation to be sent to the new user, then click **Add**.

The user receives an invitation email with a link to onboard themselves in the Organization with the roles you assigned.

### What to do next

For more information and detailed procedures for the different service onboarding workflows, see the Getting Started with VMware Cloud Services guide.

## How do I onboard as a user in VMware Cloud Services

To start using VMware Cloud Services as a new user with no access to any Organization and a non-federated account, you must first obtain Organization and service access from an **Organization Owner** user.

Requesting initial access to VMware Cloud Services is an offline process that can be initiated by you or by the **Organization Owner**. Typically, after the **Organization Owner** grants you Organization and service roles in the Organization, you receive an email with a link to the Organization.

1 Click the **View My Roles** link to access the Organization.

2 If you don't have a VMware account, you will be prompted to create one.

3 If you already have a VMware account, you can log in to the Organization and start using the services according to the Organization roles and services access you have been granted.

If you want to request additional roles in the Organization, see How do I request additional roles.

## How do I onboard as a user with a federated account

As a non-Organization user with a federated domain, your first login to VMware Cloud services with your corporate account opens an onboarding workflow.

During the onboarding process, you request access by self-selecting Organizations, services, Organization and service roles. Your requests must be approved by the **Organization Owners** and this may take some time.

The Organizations available for selection in the onboarding workflow are Organizations in your enterprise federated domain which have been activated for Identity Governance and Administration (IGA). If you have to obtain access to an Organization that is not IGA-activated, you need to be sent an invitation link from an **Organization Owner** to onboard.

### Procedure

**1** Go to https://cloud.vmware.com/ and click **Log In**.

2 In the VMware Cloud services welcome screen, type your corporate account credentials.

   The first step of the onboarding workflow displays the list of IGA-activated Organizations associated with your enterprise.

3 Select the Organization which you want to access and click **Continue**.

4 Select your role in the selected Organization.

   Your Organization role determines the level of access and permissions you have in the Organization. When you onboard with a federated account, you can only request the default **Organization Member** role. After onboarding, you can request additional roles. For more information, see How do I request roles in governance activated Organizations.

5 Click **Continue**.

   The **Select service roles** step of the workflow displays the services available in the selected Organization.

6 For each service you want to access as an **Organization Member**, use the drop-down lists to select service roles.

   **Note** Service roles are service-specific. If not sure what service roles you need, check the documentation for the service you want to access.

7 Click **Continue**.

8 In the **Finalize request** step of the onboarding workflow, define the time period for the service access request.

9 In the **Business Justification** text box, type a message to the **Organization Owner**, then click **Continue**.

   Your request displays in the **Pending requests** list, awaiting approval from an **Organization Owner**.

10 To request access to another IGA-activated Organization in your federated domain, click **Submit a New Request**.

11 Repeat steps 3 to 9.

### What to do next

Receiving approval for the Organization and service roles you requested can take some time. Until then, you can access the Cloud Services Console to check the status of the requests you submitted, cancel a request you created or create a new one.

# How do I log in to Cloud Services Console

# 3

As a VMware Cloud Services user, you log in to Cloud Services Console with your VMware account credentials. If your account is federated, you log in using your corporate account credentials.

When a user logs in to VMware Cloud Services and after successful authentication, an access and refresh tokens are generated for the user's login session. Both tokens are generated in the background using OAuth2.0 app and have default Time to live (TTL) values:

- 30 minutes TTL for the access token.
- 24 hours TTL for the refresh token.

This means that after successful login, the access token remains valid only for 30 minutes. After that, it becomes invalid and the refresh token is used to regenerate the access token so that the user can continue with the login session. After 24 hours the refresh token expires and the user is required to re-log in.

Currently, the default TTL values for the access and refresh tokens cannot be modified.

### Prerequisites

- You must have an Organization role in one or more VMware Cloud Services Organizations.

### Procedure

1 Open a browser window and go to https://console.cloud.vmware.com/.

2 Enter your account email and click **Next**.

3 Type your password then click **Sign In**.

### Results

Upon successful login, the VMware Cloud Services home page displays the services available in the Organization.

# What is a Cloud Services Organization

4

VMware Cloud uses Organizations to provide controlled access to one or more services.

As an enterprise using multiple cloud services, Organizations provide an easy way to map your business groups and processes to different Organizations.

You use the Cloud Services Console to manage your Organization and its resources, such as:

- User and group roles and permissions.
- Onboard additional services.
- Obtain billing and subscriptions information.
- View usage data for your Organization's services.
- Set authentication policies in the Organization.
- Audit event logs.
- Get support.

The Organization roles you have been assigned in the Organization determine your access to features in Cloud Services Console. The service roles you hold within the Organization determine which VMware Cloud services available in the Organization you can access. You can have different roles in multiple Organizations.

# How do I work with the Cloud Services catalog

5

The VMware Cloud Services catalog provides an easy way to view, browse, search or filter services that meet specific criteria.

The services catalog is the first page that opens when you log in to Cloud Services Console. Each catalog item is represented by a separate card which displays information about the service. If a service is available in your Organization, you can request access by clicking the link on the service card.

| From the... | You can... |
|---|---|
| **Services** > **Organization** tab | ■ Under the **My Services** section of the page, you can find all services for which you already have service roles assigned to you. Click a service card to launch a service.<br>■ The **Other Services** section provides a list of all services in your Organization for which you don't have service roles assigned to you.<br>All access requests have to be approved by an **Organization Owner**. For information about submitting an access request for service roles, see How do I request additional roles. |
| **Services** > **Recommended** tab | See a list of service recommendations based on your current service subscriptions. |
| **Services** > **All** tab | Browse or filter the full VMware Cloud Services catalog. You can filter the services catalog by category and pricing model. |
| Any page under **Services** | Use the **Search for a service** box in the upper right corner of the page to find relevant services by keyword. |

This chapter includes the following topics:

## What service catalog actions are available to me

You can manage your access to VMware Cloud services directly from the service cards in the VMware Cloud services catalog. The actions you can take in respect to any given service depends upon your role in the Organization and the type of service you want to access. Different actions are available for free, trial, and paid services.

## Organization Member Actions

| If you have access to… | and the service is… | the action you can take is… | the result from this action is… |
|---|---|---|---|
| to the service | free, active trial, or paid | **Launch Service** | service launches in the Cloud Services Console |
| | free, active trial, or paid with one or more service instances | **Launch Service** with a tooltip if there is one service instance | selected service instance launches in the Cloud Services Console |
| | | **Launch Service** with a drop-down menu if there are multiple instances for the service | |
| to the Organization, but not to the service | free, active trial, or paid | **Request Role** | you are prompted to request a role for the service |
| no access to the service and the service is not in your Organization | free, active trial, or paid | **Access** | you are prompted to onboard the service |
| | | **Learn More** | launches the service details page |
| | expired trial | **Learn More** | opens service details or purchase information page |

## Organization Owner Actions

| If you have access to… | and the service is… | the action you can take is… | the result from this action is… |
|---|---|---|---|
| to the service | free or paid | **Launch Service** | service launches in the Cloud Services Console |
| | active trial | **Launch Service** | service launches in the Cloud Services Console |
| | | **View Trial Details** from the ellipses icon (•••) | opens service trial details page |
| | | **Purchase Service** from the ellipses icon (•••) | opens page with purchase information |
| to the Organization, but not to the service | free, active trial, or paid | **Access** | you are prompted to gain access to the service by editing your roles |
| | | **Learn More** | launches the service details page |

| If you have access to... | and the service is... | the action you can take is... | the result from this action is... |
|---|---|---|---|
| have no access to the service and the service is not in your Oganization | free, paid, or paid with trial | **Access** | you are prompted to onboard the service |
| | expired trial<br>Depending on the Organization setup, one of four actions is displayed. | **Purchase Service** | opens page with purchase information |
| | | **Confirm Payment Method** | opens the **Confirm Payment Method** page in the Cloud Services Console |
| | | **Add Payment Method** | opens the **Payment Information** page in the Cloud Services Consoleand prompts you to add payment method details for your Organization |

# How do I request additional roles

As an **Organization Member** user, you get access to VMware Cloud services available in your Organization either through invitation from an **Organization Owner** user, or by submitting a self-service request.

The self-service request replaces the need to wait for an invitation from an **Organization Owner** and lets you determine the services and roles that you want to access within the Organization as well as the time period for the requested access.

**Note** **Organization Owners** can self-assign additional Organization and service roles to themselves. Refer to How do I manage roles and permissions for more information.

To submit a self-service request, browse the services catalog to locate the service for which you want to request additional roles. Simply click the **Request Access** link in the service card. A pop-up window opens where you use the drop-down menus to select a new service role.

All requests are submitted to the **Organization Owners** who can approve, deny or modify your requests before approving. When your request is processed, you receive an email notification.

## How do I view the self-service requests I submitted?

You can view your pending and past service requests at any time in the **My Request History** section on the **My Account** > **My Roles** page.

## Can I cancel a self-service request I created?

You can only cancel self-service requests with pending status. Open **My Roles** page and click the **Cancel** link for the request you want to delete.

## Why don't I see a **Request Access** link in the service tile?

The option to request additional service roles may be deactivated in Identity Governance and Administration (IGA) activated Organizations with federated domains. In this case you need an invitation from an **Organization Owner**.

# How do I manage my Cloud Services account

6

Your VMware Cloud services account is where you manage your user profile. Select language and regional format preferences, security settings such as your password and MFA settings, and generate and manage API tokens. You can also view the roles you hold in your Organization.

To access your account, click your user name, and then click **My Account**.

This chapter includes the following topics:

## How do I view my user profile

Your user profile consists of the details you provided when you created your VMware customer account. Depending on your customer profile, you might be able to edit your user profile.

**Note** You cannot change the email address with which you registered.

You can view your user profile in the Cloud Services Console or by logging in to your My VMware account at https://customerconnect.vmware.com/.

If your account is not federated, you can modify your profile details in Cloud Services Console, the changes you make are saved to your VMware account, and vice versa.

If your account is federated, your editing options are limited. For example, you cannot change your profile name and can only view your VMware ID details.

### Procedure

1 On the Cloud Services Console toolbar, click your user name and select **My Account**.

2 On the **Profile** page, make your changes, and click **Save**.

## How do I reset my password

Your VMware Cloud services password is the same password as your VMware ID.

You can reset your VMware ID in the VMware Cloud services platform, or by logging in to your VMware Customer Connect account at https://customerconnect.vmware.com/.

### Procedure

1 On the Cloud Services Console toolbar, click your user name and select **My Account > Security**.

2 Enter the information to change your password and click **Change Password**.

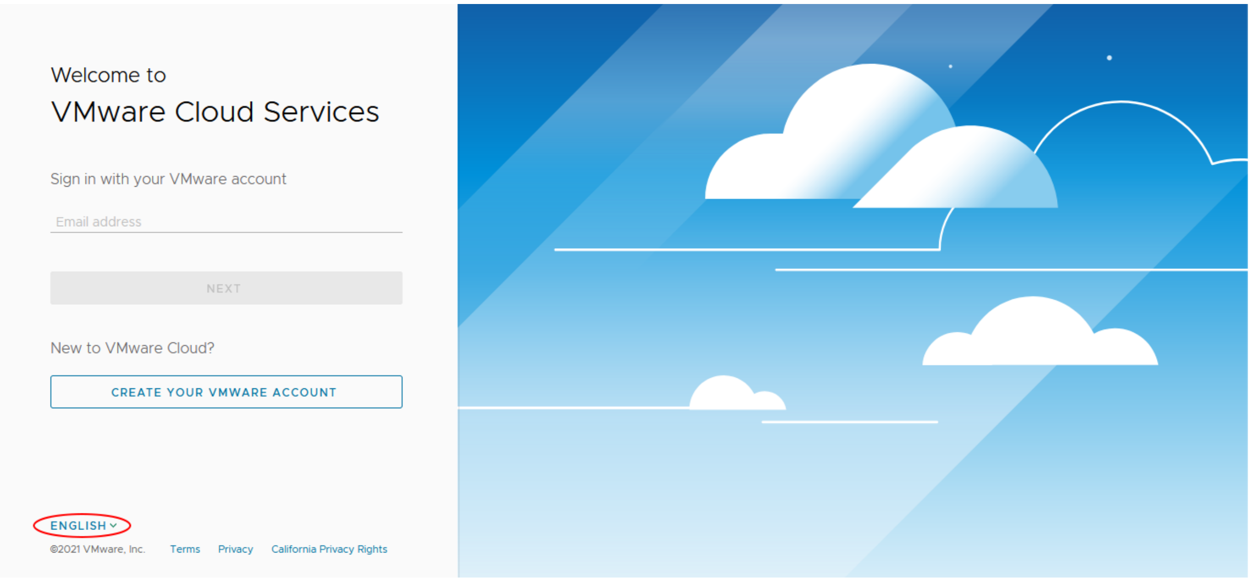
   Your VMware ID is reset.

# How do I change my language and regional format

You can change your display language to your preferred language before you onboard our cloud services, or in your account settings where you can also set your regional format.

## Experience onboarding in your preferred language

If you have not yet onboarded VMware Cloud services, you can choose your preferred language before you sign in. We support the regional format set in your browser.



Welcome to
VMware Cloud Services

Sign in with your VMware account

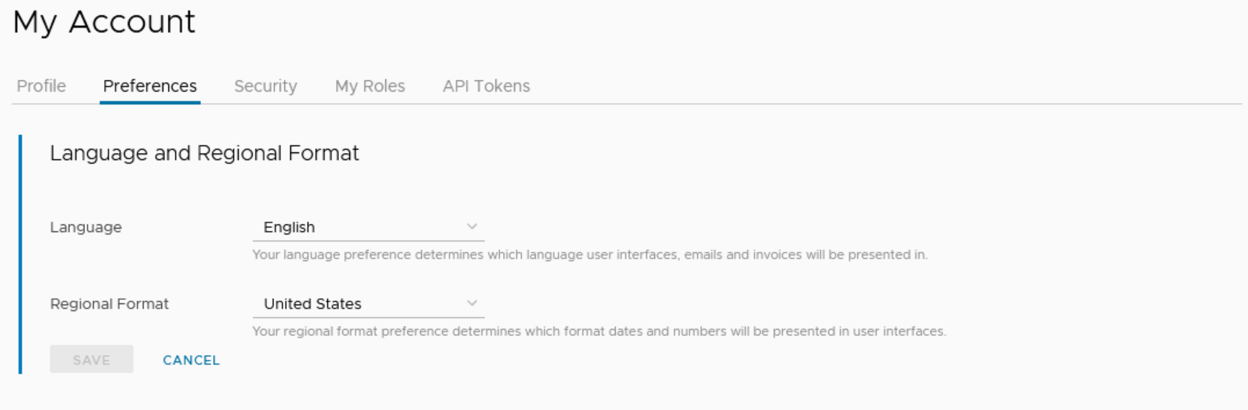
Email address

New to VMware Cloud?

©2021 VMware, Inc.

## Change your language and regional format

To change your language and regional format at any time after you've signed in, click your user name on the menu bar, and select **My Account > Preferences**. Then click **Edit**.



My Account

Language and Regional Format

Language: English

Your language preference determines which language user interfaces, emails and invoices will be presented in.

Regional Format: United States

Your regional format preference determines which format dates and numbers will be presented in user interfaces.

If you change your language, know that not all our pages are displayed in the selected language. In addition, there are some forms that only support English characters. Don't worry, we'll let you know when only English is supported.

## Can I set a regional format that is different from the language

If you set a regional format that is different from your preferred language, there might be cases where the default regional format for the selected language overrides the selected regional format. This might occur in the display of certain emails, statements, and invoices. For example, if you choose English as your preferred language and Japanese as your regional format, some communications might be displayed in the US regional format. Here is a list of languages and their default regional format.

| Language | Default regional format |
|---|---|
| English | US |
| Simplified Chinese | CN |
| Traditional Chinese | TW |
| Spanish | ES |
| Italian | IT |
| French | FR |
| Japanese | JP |
| German | DE |
| Korean | KR |

# How do I secure my account using multi-factor authentication

Multi-factor authentication (MFA) is a security enhancement that requires you to present two pieces of evidence - your credentials - upon signing in. These credentials can be something you know such as your password, and something you have such as an application that generates a one-time passcode. MFA helps protect access to data and applications by adding an extra layer of security.

You have probably already used MFA in some form or another. For example, if you logged into a website that sent a code to your mobile device which you used to gain access to your account.

**Note** If your VMware Cloud Services account is federated, MFA is managed by your enterprise security team.

To secure your VMware Cloud Services account with MFA, you download an authentication application to your mobile device. This creates a virtual MFA device. The application generates a six-digit authentication code that is compatible with the time-based, one-time password standard. You use this code together with your VMware ID and password to log in to cloud services.

When you set up MFA for your account, you receive a set of 10 recovery codes. Save these codes to a safe place. You'll need them to sign in if you don't have your MFA device near by, or if you have lost it.

| How do I? | |
|---|---|
| Activate my MFA device. | 1 Click your user name on the menu, and select **My Account > Security**.<br>2 Click **Activate MFA Device**, and follow the instructions to set up your device.<br>3 MFA is turned on automatically. The next time you sign in, use your VMware ID and password, and an authentication code generated by the app. |
| Turn off MFA so I sign in with my VMware ID and password only. | 1 Click your user name on the menu, and select **My Account > Security**.<br>2 Click the **MFA is turned on** toggle key. |
| Deactivate my MFA device. | 1 Click your user name on the menu, and select **My Account > Security**.<br>2 Click **Deactivate MFA Device**. |
| Regenerate my recovery codes | You can regenerate a new set of recovery codes at any time by accessing **My Account > Security**. |

## What two-factor authentication application can I use?

VMware Cloud services support the following two-factor authentication applications.

You can download the authenticator for your device by clicking the appropriate link below.

| Device | Authentication application |
|---|---|
| iOS | ■ Google Authenticator. See, https://itunes.apple.com/us/app/google-authenticator/id388497605?mt=8.<br>■ Duo Mobile. See, https://duo.com/product/trusted-users/two-factor-authentication/duo-mobile. |
| Android | ■ Google Authenticator. See, https://support.google.com/accounts/answer/1066447?hl=en.<br>■ Duo Mobile. See, https://duo.com/product/trusted-users/two-factor-authentication/duo-mobile. |
| Windows phone | ■ Authenticator. See, https://www.microsoft.com/en-us/store/p/authenticator/9wzdncrfj3rj?rtc=1.<br>■ Duo Mobile. See, https://duo.com/product/trusted-users/two-factor-authentication/duo-mobile. |
| Blackberry | Google Authenticator<br>See, https://support.google.com/accounts/answer/1066447. |

For more information about virtual MFA applications, see https://tools.ietf.org/html/rfc6238.

What actions can I take when I can't log in with MFA

When you activate MFA in VMware Cloud services, you receive a set of 10 recovery codes. You can copy these codes, download them and even print them, but you must save them to a safe place.

## How do I troubleshoot MFA when I can't sign in

When you activate MFA in VMware Cloud services, you receive a set of 10 recovery codes. You can copy these codes, download them and even print them, but you must save them to a safe place.

If you experience issues signing in to VMware Cloud services, you can use a recovery code.

| If... | Do this... |
|---|---|
| I don't have access to my MFA device or the device has been lost | On the VMware Cloud Services sing-in page, click the **Troubleshoot MFA** link. When prompted, enter one of the recovery keys. |
| I can't find my recovery codes | Contact VMware Support by calling a support phone number or by accessing the Login Chat Support on VMware Customer Connect. |

# How do I generate API tokens

You use API tokens to authenticate yourself when you make authorized API connections. Previously called an OAuth Refresh token, an API token is exchanged for an access token and authorizes access per Organization. You generate API tokens from your account page in Cloud Services Console or through the VMware Cloud Services.

Tokens are generated using a special algorithm that picks up alphanumeric characters. Each token is a unique 65 characters combination. When you generate a token, you determine its duration and scopes:

- A token's Time to Live (TTL) can range from several minutes to several months, or set to never expire. The default duration is six months.
- Scopes provide a way to implement control over what areas in an Organization your token can access - specifically which role in an Organization, and what services and the level of permissions.

### Prerequisites

Ensure a secure and protected storage location for your API tokens.

### Procedure

1. On the Cloud Services Console toolbar, click your user name and select **My Account > API Tokens**.
2. Click the **Generate a New API Token** link.
3. Enter a name for the token.
4. Specify the desired lifespan of the token.

   **Note** A non-expiring token can be a security risk if compromised. If this happens, you must revoke the token.

5. Define scopes for the token. Your selection must be based on the roles supported by your user account.

| Scope | Description |
|---|---|
| **Organization Roles** | Organization roles determine a user's access to the Organization's resources.<br>■ Select one or more Organization roles for your API Token. |
| **Service Roles** | Service roles are built in pre-defined sets of permissions that grant access to VMware Cloud services.<br>■ Use the arrow icon next to a service name to expand the roles available for that service, then select one or more service roles for your API Token. |
| **Permissions** | Some services allow you make a more granular selection by assigning a limited set of the permissions available for a service role.<br>■ When you select a service role, the available permissions are displayed in the right side of the table. Select the relevant service permissions for your API Token. |

If required, you can select **All Roles** and give your token access to all the Organization and service roles.

**Note** Even if you assign **All Roles** access to your token, it will have only those access roles which your user account supports. To view the Organization and service roles you have, from the **My Account** page select the **My Roles** tab.

6 (Optional) Select the **Open ID** check box to retrieve an Open ID compliant token with extended user details.

7 (Optional) Set an email preference to receive a reminder when your token is about to expire.

8 Click **Generate**.

9 Save the token credentials to a safe place so you can retrieve them to use later on.

For security reasons, after you generate the token, we only display the name of the token on the API Tokens page and not the token credentials. This means that you will no longer be able to reuse the token by copying the credentials from this page.

10 Click **Continue**.

In addition to API tokens, you can use OAuth apps to authenticate your applications. To see when to use OAuth apps instead of API tokens, see What Is the difference between OAuth apps and API tokens

## Example: Using an API Token to Interact with VMware Cloud Service APIs

You can use an API token to interact with our APIs by exchanging it for an authentication token.

1 Generate an API token.

2 Perform `POST` to https://console.cloud.vmware.com/csp/gateway/am/api/auth/api-tokens/authorize.

3 In the header, include the following requests:

- accept: `application/json`
- content type: `application/x-www-form-urlencoded`/

4 In the body, include the `refresh_token={token value}` request.

5 Use the authentication token in the `csp-auth-token` header in your script's HTTP calls.

## How do I manage my API tokens

As the sole owner of your API tokens, it is your responsibility to securely store, backup and manage them.

To view and manage your API tokens, click your user name, then select **My Account > API Tokens**.

- To regenerate a token, click **Regenerate**. This replaces the existing token with a new one. In order to continue calling the APIs, you must update your token in the API calls.
- To deactivate a token, click **Revoke**. This revokes both the API token and the associated access token.
- To prevent unauthorized access to your Organization's resources, it is strongly recommended that you keep the API tokens you generate in a secure and protected location. VMware Cloud Services does not check for proof of possession, but captures token usage audit events when:
  - a user generates an API token
  - a user revokes one or all personal tokens
  - a user makes an unsuccessful attempt to generate access token by API token refresh

  **Note** To view the audit event logs in VMware Cloud Services, you must have an **Organization Owner** role.
- To add an extra layer of security to your APIs, you can add Multi-Factor Authentication for your API tokens. For more information, see How do I secure my API tokens using multi-factor authentication.
- If your API token has been deactivated by an **Organization Owner** for violating any policy set in the Organization, or for not adhering to the Organization's standards, you will receive an email notification from VMware Cloud Services. On your **My Account > API Tokens** page, deactivated tokens are marked with the label Deactivated .

The following table summarizes the most common API token self-service management tasks:

| If you want to... | Do this... |
|---|---|
| Extend the validity of an API token that has expired. | You must regenerate your token. |
| Regenerate a valid API token. | You can regenerate a token at any time. If you regenerate a token, you revoke all instances of the previous token.<br>If you have used the token, for example in one of your scripts, remember to replace it with the newly generated token. |
| Replace a compromised API token. | If you feel the token has been compromised, you can revoke the token to prevent unauthorized access. You generate a new token to renew authorization. |
| Destroy an API token that is still valid. | You destroy a valid API token by revoking it. |

| | |
|---|---|
| Recover a lost API token. | Lost tokens cannot be recovered. You must revoke the lost token and generate a new one. |
| Reactivate an API token deactivated by an **Organization Owner** | If a deactivated token is still valid, you must contact the **Organization Owner** and ask for its reactivation. |

## How do I secure my API tokens using multi-factor authentication

If you are using API tokens to access VMware Cloud Services APIs, you can add an additional layer of security by activating Multi-Factor Authentication (MFA) on your API tokens.

In this way, even if your API token is compromised in some way, your data and applications are protected from unauthorized access. After you activate MFA, any token you try to exchange for an access token to VMware Cloud Services APIs, is going to require MFA authentication.

To secure your VMware Cloud Services API tokens with MFA, you download an authentication application to your mobile device. This creates a virtual MFA device. The application generates a six-digit authentication code that is compatible with the time-based, one-time password standard. To access the VMware Cloud Services APIs, you must provide a six-digit token generated from your registered MFA device.

| How do I? | |
|---|---|
| Activate my MFA device. | 1 Click your user name on the menu, and select **My Account > API Tokens > MFA**.<br>2 Click **Activate MFA Device**, and follow the instructions to set up your device.<br>3 MFA is turned on automatically. The next time you use an API token to obtain access token, you will need an authentication code generated by the app. |
| Turn off MFA. | 1 Click your user name on the menu, and select **My Account > API Tokens > MFA**.<br>2 Click the **MFA is turned on** toggle switch.<br>**Important** If using MFA on API tokens is enforced by your Organization, you cannot turn off MFA. Even if you can generate API tokens, you cannot exchange them for access tokens unless you provide a six-digit passcode from your registered MFA device. |
| Deactivate my MFA device. | 1 Click your user name on the menu, and select **My Account > API Tokens > MFA**.<br>2 Click **Deactivate MFA Device**. |

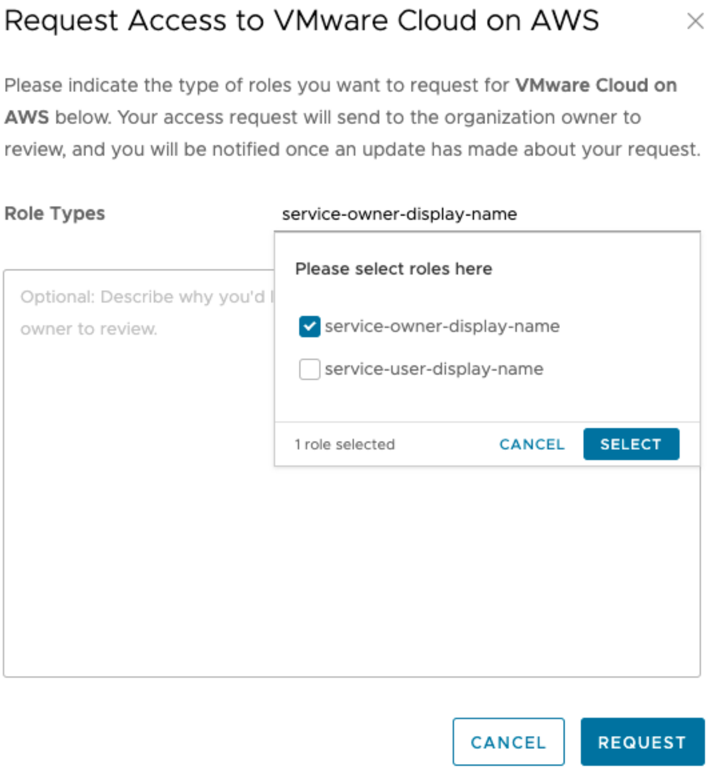
## How do I manage my roles in an Organization

Roles are assigned by users with the **Organization Owner** role. You will typically hold a role in the Organization and a role in one or more of the Organization's services. As an **Organization Member** user, you can request additional service roles for services available in your Organization and you can delete roles already assigned to you. To obtain additional service role access, your request must be approved by an **Organization Owner**.

For more information about Organization roles, see How do I manage roles and permissions.

Here's how you manage your service roles in the Organization:

- To view your roles, see what access you have to services, and request additional roles, click your user name, and select **My Account > My Roles**.
- To delete a service role or an additional Organization role you no longer need, click the service name to expand all roles you have for that service. After locating the service role you want to remove, click **Delete Role**. In order to take effect, your role deletion request must be approved by an **Organization Owner**.
- To view past role requests, scroll down to the **My Request History** section of the page.
- To request additional service roles for services already available in your Organization, click **Request Roles** and make a selection.



Request Access to VMware Cloud on AWS

Please indicate the type of roles you want to request for **VMware Cloud on AWS** below. Your access request will send to the organization owner to review, and you will be notified once an update has made about your request.

**Role Types** service-owner-display-name

Optional: Describe why you'd l owner to review.

Please select roles here

☑ service-owner-display-name

☐ service-user-display-name

1 role selected

If you are a member of an Identity and Governance Administration (IGA) activated Organization, you have the additional option to request new Organization roles. For more information, see How do I request roles in governance activated Organizations.

# How do I request roles in governance activated Organizations

**Organization Owners** of Identity Governance and Administration activated Organizations can allow **Organization Members** to submit self-service access requests instead of granting access through invitation. If this option is available in your Organization, you can request additional roles directly from the Cloud Services Console.

### Procedure

1. Log in to VMware Cloud Services and navigate to the **My Account > My Roles** page.
2. Click the **Add Service Access** link.

   **Note** If you don't see the **Add Service Access** link, this means that the self-service requests option has been deactivated and you can obtain additional access only through an invitation sent to you by an **Organization Owner**.

3. Select additional Organization and service roles that you want to request.
4. Click **Submit**.

### Results

Your request is created and submitted for approval. When an **Organization Owner** processes the request, you will receive a notification.

# How do I manage my Cloud Services Organizations

7

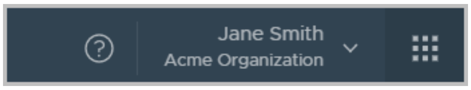
Your VMware account can be associated with one or several VMware Cloud services Organizations. VMware Cloud uses Organizations to provide controlled access to one or more services. To access a cloud service, you must belong to an Organization.

If you are an **Organization Owner** user, you have access to all the resources of the Organization. You add cloud services to your Organization, and then invite users to join. You manage the Organization payment methods and user access. If you hold an **Organization Member** user role, you have limited access to the Organization's resource.

To see what you can do within your Organization with your role, see How do I manage roles and permissions.

## Your Active Organization

When you sign into VMware Cloud services, the Organization you are logged into is displayed under your user name on the menu bar of the Cloud Services Console.



If you belong to more than one Organization, you can switch from the active Organization to another of your Organizations at any given time. You can also select which of your Organizations is displayed by default when you sign in.

## View the Organization ID

Each Organization has a unique ID. You might have to use this ID when interacting with external command-line interfaces such as the VMware Container Engine CLI. You can view the Organization ID by clicking your user name. A shortened version of the ID is displayed under the Organization name. To display the full Organization ID, click the short ID.

## Display the Organization Settings

You can display the Organization name and ID by clicking your user name, and selecting **View Organization**.

If you are an **Organization Owner**, you can change the display name of the Organization.

Depending on your customer profile, you might also view and edit the country and zip/postal code and add or edit the tag that you use when querying VMware APIs.

This chapter includes the following topics:

- How do I access another one of my Organizations
- How do I specify a default Organization
- How do I customize the VMware Cloud Services header

## How do I access another one of my Organizations

If you belong to more than one Organization, you can switch from the active Organization to another of your Organizations at any given time.

When you sign in to VMware Cloud services, your active Organization is displayed. You can see the name of your active Organization on the VMware Cloud Services menu, under your user name.

### Procedure

1. On the VMware Cloud Services menu, click the arrow next to your user name.
2. From the menu, click the arrow next to the Organization name.

   A drop-down list appears displaying the names of your Organizations.
3. Select the Organization you want to display.

## How do I specify a default Organization

If you belong to more than one Organization, you can choose which of your Organizations is displayed by default when you sign in.

Your active Organization is by default the Organization to which you were invited, or the Organization which was displayed when you signed out of VMware Cloud services.

### Procedure

1. On the VMware Cloud Services menu, click the arrow next to your user name.
2. Click **Set Default Organization**.

   A list of your Organizations is displayed.
3. Select the Organization you want to display when you log in.

## How do I customize the VMware Cloud Services header

As an **Organization Owner** user, you can brand and customize the VMware Cloud Services header to reflect your company's brand.

The custom VMware Cloud Services header that you create in this task is visible only to **Organization Members** accessing this particular Organization.

### Prerequisites

- You must have an **Organization Owner** role.
- You must be familiar with your company branding guidelines.

### Procedure

1. Log in to Cloud Services Console and navigate to **Organization** > **Details.**.
2. In the **Organization Customization** section of the Organization details page, click **Edit**.
3. In the **Header Display Name** text box, type the name you want to appear in your Organization instead of VMware Cloud Services.
4. To upload your Organization logo for **Light Theme**, click **Browse** and select the image file from your local machine.

   **Note** Only `.svg` files can be uploaded for logo images.

   The header logo for **Dark Theme** is set to **Same as Light Theme** by default. To upload a different image file for **Dark Theme**, deselect the **Same as Light Theme** checkbox, click **Browse** and select the image from your local machine.

   The **Preview** section refreshes to display the new color changes you made. You can revert the changes you made by clicking **Restore Defaults**.
5. To modify the color palette for your Organization header for both **Light Theme** and **Dark Theme**:

   a. Click in the **Header Background Color** and **Header Text Color** text fields.

   b. Use the color selection tool to define the color for each entry.
6. Click **Save**.

   The **Preview** section refreshes to display the new header logo.
7. Refresh your service page to see the changes you made.

# What's involved in downloading software binaries for my cloud services

8

Some VMware Cloud services require the use of additional software binaries that you download and install separately from the service.

You download additional software by clicking **Downloads** on Cloud Services Console menu. This option is available for the following roles in the Organization:

- **Organization Owner**;
- **Organization Administrator** with **Software installer** role.
- **Organization Member** with **Software installer** role.

The **Downloads** page is your one-stop place for obtaining the software binaries you need for all services in the Organization for which you have service access and at the same time offer additional software for download.

| If... | Do this... |
|---|---|
| If you don't see the **Downloads** menu link | Request an **Organization Owner** or **Software Installer** role in the Organization.<br>Depending on your Organization, you do that either through invitation from an **Organization Owner** or by submitting a self service request. For more information, see How do I request additional roles. |
| If you can open the **Downloads** page, but don't see the service for which you need to download additional software | Request roles for the service. For more information, see How do I manage my roles in an Organization.<br>**Note** If you have service roles assigned in the Organization, but still don't see any software binaries to download for that service, this means there are no binaries or packages associated with the service in VMware Cloud Services<br>. |
| If you are a member of several VMware Cloud Services Organizations | Switch to the Organization in which you have Organization and service roles that allow you to access the software binaries you need to download. For more information, see How do I access another one of my Organizations. |

This chapter includes the following topics:

- How do I download additional software for VMware Cloud Services

# How do I download additional software for VMware Cloud Services

The additional software binaries and packages you need to download for your services can be accessed from the **Downloads** page in Cloud Services Console.

### Prerequisites

To download additional software binaries and packages, you must:

- have an **Organization Owner** role or a **Software Installer** permission if you are an **Organization Administrator** or **Organization Member** in the Organization;
- have service roles assigned to you for the service for which you want to download additional software;
- your Organization has an active subscription for the service for which you want to download additional software.

### Procedure

1. Log in to the Cloud Services Console.
2. On the main menu, click **Downloads**.

   The **Product Explorer** page opens. It shows a list of the services that you have access to and at the same time have additional software for download.
3. To view the software binaries for a service, click the service name.

   The right pane of the **Product Explorer** shows the download binaries associated with the service you selected.
4. Explore the available software downloads:

   a. Click **Read More** to view details for a specific software binary.

   b. Click **Download** to download the software binary on your local machine.

# Identity & Access Management 9

As an **Organization Owner** user, you control user and group access to your Organization and its resources.

This chapter includes the following topics:

- How do I manage roles and permissions
- How do I manage users in my Organization
- How do I work with groups
- How do I set authentication policies in my Organization
- What is enterprise federation and how does it work with VMware Cloud Services
- What is Identity Governance and Administration and how does it work with VMware Cloud Services
- How do I authenticate applications with OAuth 2.0
- How does auditing event logs in VMware Cloud Services work
- How do I create a NIST pre-login notification in VMware Cloud Services
- How do I use the Data Insights Dashboard
- What's involved in working with Projects in Cloud Services Console

## How do I manage roles and permissions

As an **Organization Owner** user, you grant VMware Cloud Services users role-based access when you invite them to join your Organization.

You view and manage user roles in your Organization from the **Identity and Access Management > Active Users** menu in Cloud Services Console.

### Organization Roles and Permissions

Access to an Organization's resources is determined by the role assigned to each user in the Organization. Each user can be assigned one or more of the following roles in an Organization:

- **Organization Owner**

- **Organization Member**
- **Organization Administrator**

To see the permissions for each Organization role, refer to What Organization roles are available in VMware Cloud Services.

**Service Roles and Permissions**

VMware Cloud services come with a pre-defined built-in set of service roles that can be assigned to users in the Organization. **Organization Owner** users grant other users in the Organization access to cloud services according to the roles provided by each cloud service. For more information about built-in service roles, refer to the documentation of the relevant VMware Cloud service.

# What Organization roles are available in VMware Cloud Services

Users of VMware Cloud Services can have any of the following Organization roles in any Organization: **Organization Member**, **Organization Administrator**, or **Organization Owner**.

## Organization roles and permissions

The level of permissions for each Organization varies:

- The **Organization Owner** role has full administrative access to all resources in the Organization. **Organization Owner** users can also self-assign roles to themselves.
- The **Organization Administrator** role has limited administrative access. **Organization Administrator** users can assign services roles to any organization role, but can manage only users, groups and OAuth apps that have roles with lower administrative permissions.

  For example, an **Organization Administrator** user can grant or manage access for other users and groups who have the **Organization Member** role in the Organization, but cannot manage users, groups, or resources who are assigned the **Organization Owner** or **Organization Administrator** role.
- The **Organization Member** role has read-only access to the Organization resources.

Here's what you need to know about the permissions of the three Organization roles in VMware Cloud Services. If a user is assigned roles that conflict with one another, they receive the role that has greater permissions.

| Permission | Organization Owner | Organization Administrator | Organization Member |
|---|---|---|---|
| Belong to one or more Organizations | ☑ | ☑ | ☑ |
| Access one of your other Organizations | ☑ | ☑ | ☑ |
| Specify the Organization that is displayed when you sign in. | ☑ | ☑ | ☑ |

| Permission | Organization Owner | Organization Administrator | Organization Member |
|---|---|---|---|
| View and modify the Organization settings. | ☑ | ☑ View only. | ☑ View only. |
| Add/remove users in your Organization | ☑ | ☑ Only users who have **Organization Member** role. | |
| Manage the service access and roles of users in your Organization. | ☑ | ☑ | |
| Manage and view payment methods and billing. | ☑ | ☑ When the **Billing Read-only** check box is selected, this role provides read-only access to billing-related information and the option to generate usage consumption reports. | ☑ When the **Billing Read-only** check box is selected, this role provides read-only access to billing-related information and the option to generate usage consumption reports. |
| Submit and manage support tickets. | ☑ | ☑ When the **Support User** check box is selected. | ☑ When the **Support User** check box is selected. |
| Query the cloud service APIs for customer usage and data.<br>This permission is available for specific customer profiles only. | ☑ | ☑ When the **Managed Service Provider** check box is selected. | ☑ When the **Managed Service Provider** check box is selected. |
| Create and manage OAuth apps to authorize third-party apps to access protected resources. | ☑ | ☑ Only for OAuth apps created by users in the Organization. | ☑ When the **Developer** check box is selected. |
| Access all audit data for your Organization in the associated vRealize Log Insight Cloud service instance for your Organization. | ☑ | ☑ When the **Access Log Auditor** check box is selected. | ☑ When the **Access Log Auditor** check box is selected. |
| Access additional software binaries and packages download links for your cloud services. | ☑ | ☑ When the **Software Installer** check box is selected. | ☑ When the **Software Installer** check box is selected. |
| Create, modify and manage access to Projects and their resources. | ☑ | ☑ When the **Project Administrator** check box is selected. | ☑ When the **Project Administrator** check box is selected. |

# How do I manage users in my Organization

If you are an **Organization Owner** user, you manage user access and determine the service and Organization level permissions granted to users and groups in your Organization.

You use the **Identity & Access Management** menu in Cloud Services Console to invite users in your Organization, assign Organization and service roles, change user roles or remove users from the Organization.

**Note** Changes to user roles might take up to 30 minutes to take effect in the Organization.

When you invite users to your Organizations, you assign two types of role-based access:

- Access to one or more of the cloud services of the Organization. You grant users access to the service by assigning them one or more of the roles provided by the service. For more information, refer to the documentation of the relevant VMware cloud service.
- Role-based access to the Organization. As an **Organization Owner** user with full access, or as an **Organization Member** user with read-only access.

Assigning access permissions to groups is more efficient than assigning the same permissions to individual users one at a time. As an **Organization Member**, you determine the users that make up your groups and what roles and permissions they are assigned.

## How do I add users to my Organization

As an **Organization Owner**, you invite users to your Organization and grant them access to the services associated with it. You can also track the invitations you send. Invitations are valid for up to seven days. If you have sent an invitation in error, you can revoke it.

The users you invite can hold several roles:

- A role within the Organization - **Organization Owner** or **Organization Member**. To see the permissions assigned to each of these roles, see What Organization roles are available in VMware Cloud Services.
- A role within the cloud service to which you are inviting the user. Each cloud service has its own specific roles. For more information, refer to the documentation of the relevant VMware Cloud services.
- Depending on your customer profile, you might also view the Managed Service Provider role which allows users to query the cloud service APIs for customer usage and data. If you assign this role to users of a tenant Organization, they will have access to all the data within the Organization.

### Procedure

1 On the Cloud Services Console toolbar, click the **VMware Cloud Services** icon and select **Identity & Access Management > Active Users**.

2 Click **Add Users**.

3 On the **Add New Users** page, enter the following information:

   a In the **Users** text box, enter the email address of the user you want to add to your Organization.

   You can add more than one user at a time by separating email addresses by comma or entering each email address on a separate line.

   b In the **Assign Organization Roles** section, assign the role the user will have in the Organization.

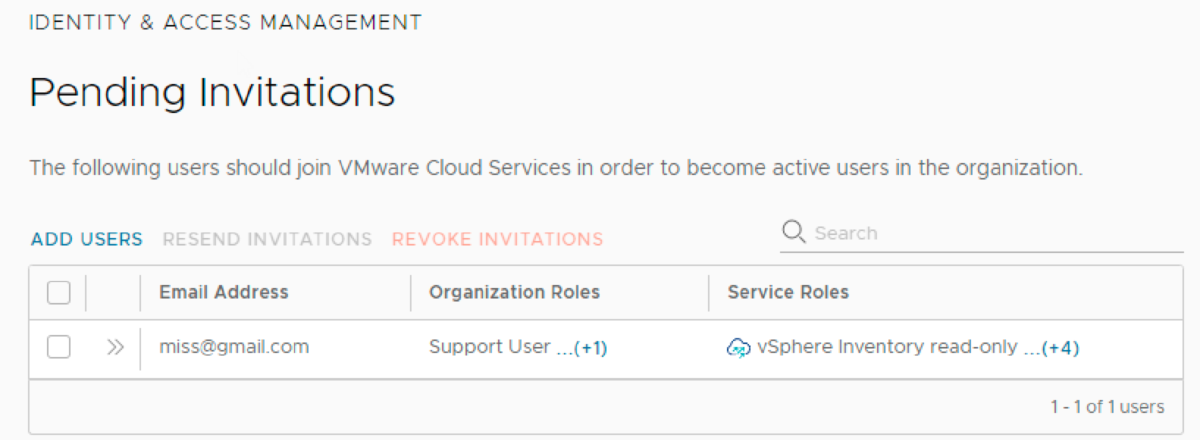
   The **Organization Owner** role has full administrative access. If you select the **Organization Member** role for the new user, consider adding additional access by selecting one or more roles in the **Additional Roles** section.

   c To assign the user service roles in the Organization, click **Add service access** and use the drop-down menus to make a selection.

   d Click **Add service access** again, to give the user access to another service.

4 Click **Add** to send an invitation to the user.

The invitations you send are valid for seven days. You can view the status of the invitation on the **Identity and Access Management** > **Pending Invitations** tab.



Pending Invitations

The following users should join VMware Cloud Services in order to become active users in the organization.

| □ | | Email Address | Organization Roles | Service Roles |
|---|---|---|---|---|
| □ | » | miss@gmail.com | Support User ...(+1) | vSphere Inventory read-only ...(+4) |

1 - 1 of 1 users

5 If you sent an invitation in error, you can revoke it. Select the check box next to the invitation and click **Revoke Invitations**.

The activation link in the email is revoked and the person to whom you sent the mail cannot sign into the service.

## How do I remove users from my Organization

As an **Organization Owner**, you can remove users from the Organization. Users that have been removed won't be able to access the Organization and its services.

### Procedure

1 Open the Cloud Services Console and select **Identity & Access Management** > **Active Users**.

2 Select one or more users and click **Remove Users**.

3. Click **Remove** to permanently remove the user from your Organization.

### How do I change user roles

When users join your Organization, they receive Organization and service roles access granted directly by an **Organization Owner** or they inherit them as members of groups. As an **Organization Owner**, you can view and edit user roles from the Cloud Services Console.

Here's what you need to know about editing the roles of users.

- Users can hold a combination of roles - the roles assigned to them directly and the roles inherited from a group. For example, a direct role assignment for support user and some group-inherited roles such as developer and VMware Cloud on AWS administrator.
- When a user is assigned roles that conflict with one another, they receive the role that has greater permissions. For example, if a user is assigned a read-only role and an administrator role, they receive the administrator role.

#### Procedure

1. On the Cloud Services Console toolbar, click the **VMware Cloud Services** icon and select **Identity & Access Management > Active Users**.
2. Click the double arrow icon ( » ) next to a user's name to view their roles and if they are part of groups.

   Changes you make to the user's role might override their group-assigned roles.
3. Select the check box next to a user and click **Edit Roles**.
4. Change the user's Organization roles and service roles as required.
5. Click **Save**.

## How do I work with groups

Assigning roles to groups is more efficient than assigning the same permissions to individual users one at a time. As an **Organization Owner** user, you create groups and determine the members that make up your groups and what roles they are assigned.

You can also edit groups after they are created or added. As your Organization expands and changes, add or remove members from your groups.

There are two types of groups available in VMware Cloud services – custom groups and enterprise groups. Custom groups can be shared with other Organizations. Enterprise groups can be nested in custom groups.

**Custom Groups**

You create custom groups by entering a name and a description, adding members, and then assigning roles for the Organization and its resources. For example, you can create a custom group and give it an **Organization Member** role to your Organization and a support role, and read-only access to specific services in the Organization. Custom groups can also include enterprise groups.

For custom groups, you can edit the name and description, add or remove members, and change the role assignment of the group.

### Shared Groups

When you create a custom group, you can decide if you want to make it shared or not. As an **Organization Owner**, you associate the shared group with other Organizations which allows the members of the shared group to be assigned roles in the associated Organizations and get access to services without invitation from the **Organization Owners**.

Service roles assigned to shared groups are Organization-specific. The **Organization Owners** from the associated Organizations import the shared group and assign roles to the group within their own Organizations. To import a shared group, the **Organization Owners** must know the group name or ID.

Only the **Organization Owner** of the source Organization – the Organization in which the shared group was created – can modify the members of the group or remove it. Removing a shared group from an associated Organization does not delete it and it can be added back later. See how to How do I manage shared groups.

### Enterprise Groups

Enterprise groups are groups synced from your corporate domain. After you federate your corporate domain with VMware Cloud services, your enterprise groups are available for you to use in your Organization. See how to How do I assign roles to enterprise groups.

For enterprise groups, you can only change the role assignment of the group. You cannot add or remove members from enterprise groups in VMware Cloud services, but you can assign them roles for the Organization and its resources, and add them to custom groups.

### Nested Groups

Adding a group to another group is called nesting. Here's what you need to know about nested groups:

- You can nest an enterprise group in a custom group.
- Nested groups can hold a combination of roles; roles assigned directly to the enterprise group and the roles assigned through the custom group.
- You can edit the roles of a nested enterprise group or add additional roles, but you cannot remove the roles inherited from the custom group.
- You cannot nest a custom group in another custom group.

As an **Organization Owner**, you can also edit groups after they are created or added. For custom groups, you can edit the name and description, add or remove members, and change the role assignment of the group. For enterprise groups, you can only change the role assignment of the group.

As an **Organization Owner** you create groups, manage the groups, and as your Organization expands and changes add or remove members from your groups.

**Note** When you make changes to groups, it may take up to 30 minutes for the changes take effect in the Organization.

## How do I create a new group

As an **Organization Owner** user, you can create new groups in your Organization and assign the group Organization and service roles. These groups are called custom groups.

For information about the permissions assigned with each Organization role, see How do I manage roles and permissions. For information about the permissions assigned with service roles, see the documentation for the service.

### Procedure

1. On the Cloud Services Console, select **Identity & Access Management > Groups**.
2. Click **Add Groups**.
3. Select **Create a new group** and click **Continue**.
4. Enter a name and a description for the group.
5. If you want to share the group with other Organizations, click **Add Organizations**.

   a. Select the Organizations that you want to share the group with: either type the Organization ID for each Organization or make a selection from the list of Organizations displayed in the pop-up window.

   b. Click **Add**.

   **Note** When you create a custom group that is shared, the **Organization Owners** of the associated Organizations can assign roles to the group in their Organization.

6. Click **Add Members** to add members to your group, add then click **Add**.

   Members can be enterprise groups and users. You can choose to skip this step and add members after you have created the group.

7. Assign the group access to the Organization by selecting an Organization role.
8. Assign the group access to services by clicking **Add service access** and selecting a service and the roles you want to assign to the group for this service.
9. To add access to an additional service, click **Add service access**.

10 Click **Create**.

The group is added to the list of groups on the **Identity & Access Management** page.

## How do I assign roles to enterprise groups

If your domain is federated with VMware Cloud services, you can select groups from your corporate source domain and assign them roles in your Organization. These groups are called enterprise groups.

Enterprise groups are groups synced from your corporate domain. You can assign roles to more than one enterprise group at a time, and view the members in a selected group.

The members of the group you assign can hold several roles:

- Organization role: A role within the Organization - **Organization Owner** or **Organization Member**. To see the privileges assigned to each of these roles, see How do I manage roles and permissions.
- Service role: A role within one or more VMware Cloud services. Each cloud service has its own specific roles. For more information, refer to the documentation of the relevant VMware Cloud service.
- Depending on your customer profile, you might also view the Managed Service Provider role which allows users to query the cloud service APIs for customer usage and data. If you assign this role to members of a tenant Organization, they will have access to all the data within the Organization.

### Procedure

1 From the Cloud Services Console main menu, select **Identity & Access Management > Groups**.

2 Click **Select groups from your source domain** and then click **Continue**.

3 Search for the enterprise groups to which you want to assign roles.

4 Assign the group an Organization role.

Refer to the link above to see the permissions of each role.

5 Select a service, and then assign the group one or more roles in the service.

When you select a service, the service default role appears. Click the role to select a different role.

6 To give the group access to another service, click **Add Service Access**, and assign a role.

7 Click **Add**.

To send an email to users with the **Organization Member** role, select the check box. Users with the **Organization Owner** and support user roles are automatically sent an email.

## How do I manage shared groups

When an **Organization Owner** user creates a custom group and associates it with other Organizations, the group becomes shared. The **Organization Owners** of the target Organizations receive and email invitation from the source **Organization's Owner** to import the shared group and assign service roles.

As an **Organization Owner** receiving the invitation to import a shared group created in a different Organization, you assign service roles for the shared group while importing it to your Organization.

You can distinguish imported shared groups from shared groups created in your Organization by their label: Custom | remote 🔒 .

The users of the shared group you imported can access the services in your Organization according to the roles you assigned to the group. This allows cross-Organization access to services at the group level and removes the need to send individual invitations to each user.

**Important** Shared groups imported from other Organizations cannot be edited. You can edit the roles you assign to the shared group or remove the group from your Organization.

### Prerequisites

You must know the name or the Organization ID of the source Organization that created the shared group you want to add.

### Procedure

1. On the Cloud Services Console, select **Identity & Access Management > Groups**.
2. Click **Add Groups**.
3. Select **Import groups from other organizations** and click **Continue**.
4. From the drop-down menu, select the source Organization that created the shared group.
5. Select the shared group you want to import.
6. Select an Organization role to assign the selected group access to your Organization.
7. Click **Add service access** to assign service roles to the selected group:
   a. Use the drop-down menu to select the service in your Organization you want the shared group to access.
   b. Click the roles box and select the service roles you want to assign to the shared group.
   c. Define the time period for the access. You might choose an end date or provide a non-expiration access.
8. To add access to an additional service, click **Add service access** and repeat steps 7.a through 7.c.

9 Leave the **Send emails to all invited users notifying them of this role assignment** checked if you want all users of the shared group to receive invitations to access your service.

10 Click **Import**.

Results

The shared group is added as custom remote group to your Organization.

# How do I set authentication policies in my Organization

As an **Organization Owner** user, you set authentication polices for user access to your VMware Cloud services Organization, such as multi-factor authentication, IP authentication preferences, and user access at domain level.

You create and manage the authentication policies settings for your Organization from the **Organization** > **Authentication Policy** page in Cloud Services Console.

**Important** It may take up to 30 minutes for a new policy or a policy change to take effect.

If several authentication policies are set up for your Organization, each user login will be validated in sequence against all policies. If any policy is violated, the user will not be allowed access to the Organization.

## How do I set multi-factor authentication

When multi-factor authentication (MFA) is enforced, all users in your Organization will be required to provide a six-digit authentication code in addition to their login credentials. To provide the code, they must register an MFA device with VMware Cloud Services. Organization users who fail to provide a valid MFA code will be denied access to the Organization.

If you are an **Organization Owner** of a federated domain, you do not control MFA for your Organization. MFA for federated domains is configured by an **Enterprise Administrator** on the identity provider that your company is using. This procedure applies only to non-federated domains.

Prerequisites

- You must have an **Organization Owner** role in the Organization.
- You must have registered an MFA device with VMware Cloud Services so that you don't lock yourself out of the Organization after enforcing MFA. For detailed instructions, refer to How do I secure my account using multi-factor authentication.

Procedure

1 Log in to Cloud Services Console and click **Organization > Authentication Policy**.

2 In the **Multi-factor authentication** section, click the toggle button so its color changes to green.

Results

MFA is now enforced and all users of your Organization will be required to register an MFA device and provide an MFA token at login.

**Note** It might take up to 30 minutes for the policy to take effect in your Organization.

## How do I define IP authentication preferences

As an **Organization Owner**, you can manage access to your Organization by defining IP addresses or IP ranges to either block or allow user access from specific IPs.

You do that by applying an authentication preference to block or allow user access from an IP range or specific IP address. If your authentication preference is defined for an IP range, you can set exceptions for specific IPs within the range. For example, if you apply block authentication to an IP range, you can then set an exception for one or more IPs within that range that will be allowed access to your VMware Cloud services.

**Note** The IP address you enter must follow CIDR notation for IPv4 and IPv6 IP addresses.

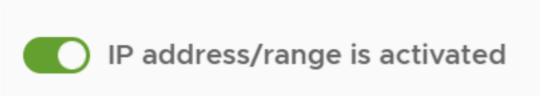
There are two authentication preference options you can define:

- **Block IP**: user logins from specific IP addresses/ranges are blocked access to the Organization.
- **Allow IP**: user logins from specific IP addresses/ranges are allowed access to the Organization.

You can have only one preference activated in your Organization. You can switch between the two preferences, but you can't have both of them activated at the same time.

To set or modify an IP authentication preference in your Organization, log in to the Cloud Services Console and navigate to **Organization > Authentication Policy > IP address/range**.

**Note** It may take up to 30 minutes for your policy settings to take effect in the Organization.

| To | Do this |
|---|---|
| Set an IP authentication preference for your Organization | 1 If setting an IP authentication preference for the first time, select an option and click **Activate**.<br>The policy settings page displays, indicating the IP address/range has been activated in your Organization.<br><br>IP address/range is activated<br>2 Click **Add** and type an IP address or range.<br>3 Click **Add** again.<br>The address or range you entered is added to the list of blocked or allowed addresses and ranges specified for your Organization. |
| Add an exception to your authentication preference | You define exception rules for IP addresses from an IP range that is already specified in the list of allowed or blocked IPs.<br>1 In the **Exception** section of the **IP address/range** page, click **Add an Exception**.<br>2 In the pop-up window that opens, type the IP addresses you want to add as exceptions to the authentication policy in your Organization.<br>If you activated the **Allow IP** preference, users accessing VMware Cloud services from the IPs on the exceptions list will be denied access. Conversely, if you activated the **Block IP** preference, users accessing VMware Cloud services from the IPs on the exceptions list will be allowed access. |
| Modify the IP addresses, ranges, or exceptions for your authentication preference | Once you activated an IP authentication policy, you can add additional IPs, IP ranges, and exceptions. You can also modify or remove existing IPs and ranges from the policy.<br>■ To make a change, first select the IP address or range from the list, then apply the appropriate action. |
| Change your IP authentication preference | If you want to switch the authentication preference in your Organization from **Block IP** to **Allow IP** or vice versa, you must first remove all IP addresses and ranges specified for the current authentication preference.<br>1 On the **IP address/range** page, select all currently defined IP addresses and ranges.<br>2 Click **Remove**.<br>3 Click the **Change** link next to the User IP Authentication Preference option.<br>4 In the pop-up window that opens, select the new option, then click **Save**.<br>5 To define new IP addresses or ranges for the newly selected policy setting, click **Add**. |

### I accidentally blocked myself and want to unblock my IP

If you accidentally added your IP in the **Block IP** list for your Organization, you must file a support ticket to unblock. As you are not able to log in to your Organization and use the **Support Center** in Cloud Services Console, you can do that by calling VMware Support.

### Does blocking a user IP address in my Organization block them from accessing other Organizations to which they are members

If a user belongs to multiple Organizations and IP based policy is enforced in one of these Organizations, they are not allowed access in that particular Organization. Then they have the option to switch to a different Organization upon login.

## How do I manage user access at domain level

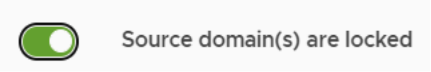
As an **Organization Owner** user, you can determine the domains allowed to access your VMware Cloud Services Organization.

When Source Domain authentication policy is activated, only users from the domains you specify can access your Organization. Access from all other domains is locked even if the groups and users are added or invited in your Organization.

Procedure

1 Log in to Cloud Services Console and navigate to **Organization** > **Authentication Policy** > **Source Domain**.

2 To activate the policy, click the slider and change its position to show source domains are locked.



Source domain(s) are locked

3 Enter the domain name you are allowing access to the Organization.

4 To add more domains and sub-domains to the allowed domains list, click the **Add domains** link.

5 Click **Save**.

Results

Source Domain is now activated for the domains and subdomains you specified. Only Organization members logging in from the allowed domains can access your Organization. Access for users logging in from a different domain is locked.

**Note** It may take up to 30 minutes for the policy to take effect in the Organization.

If you or another **Organization Owner** accidentally locks you out from accessing the Organization by not including your domain to the list of source domains that are allowed access to the Organization, open a help support ticket.

# What is enterprise federation and how does it work with VMware Cloud Services

As an enterprise using VMware Cloud services, you can set up federation with multiple corporate domains. By federating your corporate domains, you activate single sign-on for users in your enterprise. Enterprise federation with VMware Cloud services is set up through a self-service workflow and supports integration with SAML 2.0 based identity providers.

By adopting a federated identity access for VMware Cloud services users and Organizations in your enterprise, you activate the following:

- All users in your enterprise access VMware Cloud services using their corporate account.
- **Organization Owners** can control authentication to Organizations and services by assigning Organization and service roles to the groups synced from your corporate directory.
- Your security team can set up and enforce enterprise-level security and access policies for VMware Cloud services, including multi-factor authentication.

As an **Organization Owner** of an unfederated domain, you initiate the self-service federation workflow for your entire enterprise domain. After completing the setup, enterprise federation becomes available to all users from your corporate domain and applies to all services across all Organizations.

**Attention** Your enterprise must own the domains you want to federate for access with VMware Cloud services and you must verify the ownership during the first step of the self-service workflow. You cannot federate domains that belong to a service provider.

For detailed instructions on setting up enterprise federation through the self-service federation workflow, refer to the Setting Up Enterprise Federation with VMware Cloud Services Guide.

## What is the difference between federated and unfederated authentication?

If your corporate domain is not federated, your access to VMware Cloud services is authenticated through your VMware ID account. If you are new to VMware Cloud services, visit my.vmware.com to create a VMware ID.

If your corporate domain is federated, your access to VMware Cloud services is authenticated through your corporate account. A hosted Workspace ONE Access tenant is used as an identity broker to set up federation with your identity provider. The hosted tenant is configured for validation with your corporate identity provider and active directory. You manage user and group access to VMware Cloud services by configuring the Workspace ONE Access connector to sync users and groups from your corporate active directory. Only a subset of required user profile attributes, such as `username`, `firstname`, `lastname`, and email address, is configured to be synced. You can add more attributes later.

**Note** User passwords are never synced, nor cached.

.

## Can I undo the federation for my corporate domain?

If you decide to undo the federation setup or undo federation for any of the federated corporate domains you initially configured, you must file a support ticket.

## What's involved in setting up enterprise federation for your corporate domain

Setting up enterprise federation for your corporate domain is a self-service process that involves multiple steps, users, and roles.

Here's who and what's involved in federating your corporate domain with VMware Cloud services.

**Organization Owner**

**Organization Owner** users of unfederated domains can kick off the federation setup from the Cloud Services Console. Any **Organization Owner** can initiate the self-service federation process and assign one or more **Enterprise Administrators** to complete the setup.

**Organization Owners** who hold system administrator roles with their enterprise and have sufficient knowledge of the enterprise directory service and identity provider configuration, can act as **Enterprise Administrators** for the federation setup.

**Enterprise Administrator**

The **Enterprise Administrator** is a system administrator who belongs to the central security team for your enterprise and manages the directory services and identity providers. As the designated person to set up enterprise federation for your corporate domain, the **Enterprise Administrator** completes the configuration and validation steps of the self-service setup process. Setting up enterprise federation might involve representatives of different security teams. The designated **Enterprise Administrator** can invite other administrators to help with the setup.

**The Enterprise Federation Organization**

When an **Organization Owner** initiates the self-service federation workflow for their corporate domain by inviting one or more **Enterprise Administrators**, a special Federation Organization becomes available for the set-up. Everyone involved in the self-service federation process receives an email notification with a link to access the special Federation Organization. The purpose of this Organization is to set up enterprise federation for the corporate domain and to modify the initial setup.

**Linking corporate accounts to VMware IDs**

Existing users of VMware Cloud services whose accounts are federated must link their corporate accounts to their VMware ID accounts in order to access the services in their Organization. New users onboarding to VMware Cloud services after federation set up for their domains was activated don't need to create a VMware ID unless they need to view billing information or file support tickets.

VMware requires users of VMware Cloud services who work with VMware for the purposes of billing and support, to have a VMware ID and link their corporate account with their VMware ID.

**VMware Workspace ONE Access tenant**

Setting up federated identity management requires the customer to configure and manage a VMware Workspace ONE Access tenant. The tenant is created as part of the self-service federation process. The Workspace ONE Access tenant acts as an identity broker (service provider) to your identity provider and is not involved in the actual user authentication.

**The self-service federation setup workflow**

The self-service federation setup involves multiple steps that can be performed at various times by different **Enterprise Administrators**. The workflow resumes from the place it was left last. **Enterprise Administrators** involved in the setup must have VMware Cloud services accounts with a VMwareID. All steps in the federation setup are completed through the **Set up Enterprise Federation** workflow in the special Federation Organization.

## Why do I need to link my VMware ID

If you are an **Organization Owner** or **Support User** with a federated account, you still need to have a VMware ID linked to your corporate account so that you access billing information and customer support.

### Why can't I see all my cloud services?

You must link your VMware ID account to your federated account so that you can access all the services from your VMware ID account. If you have any tokens, they will automatically be transferred.

### How do I link my cloud services account?

Link your account by clicking **My Account > Profile** on the Cloud Services Console.

If you used your corporate email address when you created your VMware ID, click the **Link VMware ID** button in the Cloud Services Console banner. If you close the banner before linking your account, you can link your account later by clicking **My Account > Profile** on the Cloud Services Console.

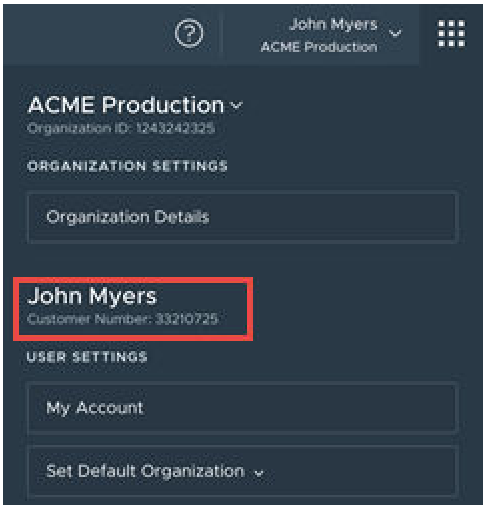
You can view the details of your linked account in the Profile page.

### How does this impact Organization Owners and users with Support roles?

If you are an **Organization Owner** or hold a **Support User** role, you must link your VMware ID account so that you continue to access billing information and customer support. After you link your account, you'll receive a customer number. Going forward, when you create a new Organization, you'll link your VMware ID account as you set up the Organization.

### Where do I view my customer number?

As an **Organization Owner** or a **Support User** , you require a customer number. After you link your account, your customer number appears under your name on the **User/Organization Settings** menu.



Organization ID: 1243242325

John Myers

Customer Number: 33210725

You can also view your customer number and other details of your linked account on the Profile page.

### What happens to my OAuth clients?

OAuth clients are used to integrate third-party applications with VMware Cloud services.

In cases where the user name of your federated account is the same as your VMware ID, for example joe@acme.com, any OAuth clients you created while logged in with your VMware ID, will be transferred to your federated account when you link your VMware ID.

If the user name of your VMware ID is not the same as your federated account, for example, joe@gmail.com and joe@acme.com, your clients are not transferred to your federated account, and you should create new clients.

For more information about creating OAuth clients, see How do I authenticate applications with OAuth 2.0.

## Why do I need to link my corporate identity provider

If your domain is federated, you can use the advanced Identity and Governance Administration (IGA) features to easily onboard non-Organization users to VMware Cloud services.

One way to activate IGA is to ask an **Enterprise Administrator** to make the change in the Enterprise Federation Organization dashboard. Another way is to link your Organization to your Identity Provider (IdP). Only **Organization Owners** of federated domains can link their Organizations to their IdP.

1 Log in to Cloud Services Console and click **Organization > Details**.

2 In the **Domains Linked to Identity Provider** section, click **Link Identity Provider**.

The IdP and domains associated with your Organization display in a pop-up window.

3 Click **Link**, then click **Continue**.

For more information about IGA features, see What is Identity Governance and Administration and how does it work with VMware Cloud Services.

## What is Identity Governance and Administration and how does it work with VMware Cloud Services

Identity Governance and Administration (IGA) is a service that allows your enterprise to obtain data for audit trail and certification, and helps **Organization Owner** users to manage self-service access requests, approvals, violations, and API tokens in real time.

The IGA service comes with two sets of features: basic and advanced. It is only available to Organizations with federated domains.

- To start using the basic IGA features, an **Organization Owner** must activate the IGA service by clicking the **Get Started** link on the **Identity & Access Management > Governance** page.
- To start using the advanced IGA features, see How do I activate advanced Identity Governance and Administration in my Organization.

Using the IGA service in an Organization, lets VMware Cloud Services users do the following:

| As an | with basic IGA | with advanced IGA |
|---|---|---|
| **Organization Owner** user | ■ Access the IGA dashboard from the **Identity & Access Management > Governance** page in the Cloud Services Console.<br>■ Activate or deactivate your **Organization Members** ability to submit self-service requests for additional roles.<br>■ Govern access to services in your Organization by managing incoming Organization and service role requests.<br>■ Monitor violations and immediately respond to threats. | ■ Onboard a service in any governance activated Organization linked to your corporate identity provider. |
| **Organization Member** | ■ If activated in the Organization, submit self-service access requests for additional Organization and service roles. See How do I request roles in governance activated Organizations. | ■ Onboard yourself in any governance activated Organization linked to your corporate identity provider. See How do I onboard as a user with a federated account. |

## How do I activate advanced Identity Governance and Administration in my Organization

If your domain is federated, additional Advanced Identity Governance and Administration (IGA) features can be activated for all Organizations in the federated domain.

Activating the advanced IGA features in your Organization requires the following:

- An **Organization Owner** from the federated domain must link your corporate identity provider to VMware Cloud Services. See Why do I need to link my corporate identity provider.
- An **Enterprise Administrator** must activate the advanced IGA features for some or all VMware Cloud services Organizations that are linked to their corporate Identity Provider. For more information, see Enable Advanced IGA Features for Federated Domains.

For more information about enterprise federation, see What is enterprise federation and how does it work with VMware Cloud Services.

When advanced IGA features are activated, non-Organization users can request Organization and service roles access in linked Organizations during onboarding. See How do I onboard as a user with a federated account to learn more about this feature.

## How do I manage self-service requests for additional roles

As an **Organization Owner** user of an Identity Governance and Administration (IGA) activated Organization, you manage Organization and service roles requests through the **Governance > Requests** page in Cloud Services Console.

The option to submit self-service requests is available to **Organization Member** users only if this option is activated in your Organization.

| If request for additional roles is activated, Organization Member users request access by... | If request for additional roles is not activated... |
|---|---|
| clicking the **Request Access** link on a service tile in the Cloud Services catalog. | the **Request Access** link in the service tile is not clickable. |
| clicking the **Request Roles** link on the **My Account > My Roles** page. | the **Request Roles** link is not displayed on the **My Account > My Roles** page. |

### How do I activate or deactivate self-service requests

To activate or deactivate self-service requests for additional roles in your Organization, do the following:

1. Go to **Governance > Requests** and click **Settings**.
2. Click the **Request for additional roles** slider to either activate or deactivate the setting.
3. Click **Save**.

### How do I process pending requests?

All incoming requests for Organization and service role access are listed in the **Pending Requests** section. The **Past Requests** lets you view historical data for all requests created in your Organization.

To approve or deny requests, select one or several entries in the **Pending Requests** list and click the respective button. The users requesting the role access receive an email notification when their request is approved or denied.

### Can I modify access requests before I approve them?

As an **Organization Owner**, you can modify the time period for service role access requested by an **Organization Member**. You view the time period of the original request by clicking the **Request ID** link. To change the requested time period, click **Approve**, then select **Approve with modification**. Change the setting and submit the change you made.

**Note** The **Approve with modification** option is available only for service role access requests and is not applicable for Organization roles.

**Organization Owners** cannot modify the service or role access originally requested by the **Organization Member**. If you want to provide guidance to the requester about the proper level of access you are willing to approve, you have the option to include a message when denying their request. The requester receives an email notification and can submit a new access request with the appropriate Organization and service roles.

## How do I monitor violations of policies in my Organization

As an **Organization Owner** user in an Identity Governance and Administration (IGA) activated Organization, you monitor access violations for user logins and logins with OAuth apps and API tokens in your Organization. You define and modify the policies for triggering violations.

You set up violation policies for logins in your IGA-activated Organization by activating various triggers for OAuth apps and API tokens, such as inactive API tokens, inactive OAuth owners, broad service scopes, insecure or unapproved URIs for OAuth apps.

**Note** If Source Domain authentication policy is activated, User Access violations are captured for all login attempts originating from domains that are not allowed by the policy setting.

#### Procedure

1. Log in to the Cloud Services Console with your corporate account.
2. Navigate to **Identity and Access Management** > **Governance** > **Violations**.
3. Click **Settings**.
4. In the **Violation Settings** page that opens, modify the settings for OAuth Apps and API tokens as appropriate.
5. Click **Save**.

Results

The **Violations** dashboard is refreshed to display violations according to the new settings.

The information on the dashboards is updated daily.

## How do I take action against violations of policies in my Organization

As an **Organization Owner** user in an Identity Governance and Administration (IGA) activated Organization that monitors violations, you can take action against the violations discovered in your Organization. You access the full list of violations by navigating to **Identity and Access Management > Governance > Violations**.

The violations captured in your Organization are grouped by the type of authentication method used to log in to VMware Cloud Services that triggered the violation. Click on the respective tab to view the full list and possible actions you can take to respond to a violation.

- The **OAuth Apps** tab displays the name of the app that triggered the violation, its severity, description, and email of the Organization user who created the OAuth app.
- The **API Tokens** tab displays the name of the API token that triggered the violation, its severity, description, and the email of the Organization user who created the API token.
- The **User Access** tab displays the email of the Organization user whose login attempt triggered the violation, its severity, the date the violation took place, and the source domain from which it occurred. A user access violation is captured for login attempts from any domain that is not allowed by the Source Domain authentication policy. For more information, see How do I manage user access at domain level.

The following table describes the actions you can take in response to violations in your Organization.

| To... | Do the following... |
|---|---|
| Change the visibility of a violation | This action changes the visibility status of a violation from `Active` to `Hidden`. It does not delete the violation and can be reverted.<br>1 Locate the violation you want to hide and click its corresponding double arrow ( » ) to expand its details.<br>2 Select the check box next to the active violation you want to hide.<br>3 Click **Hide**.<br>The violation is no longer displayed in the details section. |
| Display a violation that has been hidden | This action displays violations with `Hidden` status.<br>■ Expand a violation's details section and switch on the **Display All** toggle. All violations that have been hidden are displayed. |

| To... | Do the following... |
|---|---|
| Remove an OAuth app from your Organization | This action removes the OAuth app and blocks it from accessing the Organization. The OAuth app is not deleted, yet no further violations will be reported from this app. The removal action cannot be reverted from the **Violations** page – to monitor violations from this OAuth app it has to be added to the Organization again.<br>1 On the **Violations** page, open the **OAuth Apps** tab.<br>2 Locate the app you want to remove.<br>3 Select the check box next to its name.<br>4 Click **Remove**. |
| Edit the severity of a violation | Based on your Organization's needs, you can define the severity for any violation criterion.<br>1 On the **Violations** page, click **Settings**.<br>2 Use the **Severity** drop-down menu to change the setting for each violation criterion you want to modify.<br>3 Click **Save**. |

## How do I manage API tokens in my Organization

As an **Organization Owner** user in an Identity Governance and Administration (IGA) activated Organization, you monitor the API tokens created in your Organization and set constraints for idle and maximum Time to live (TTL) for all newly created tokens.

To access the **API Tokens** dashboard, open the Cloud Services Console and navigate to **Identity & Access Management > Governance > API Tokens**. The dashboard that opens gives you a list of all API tokens created by users in your Organization.

For each API token, you can view details, such as token name, name of the Organization user who created the API token, creation and expiration dates, the date the token was last used, and the scopes of the token – the Organization roles assigned to the token.

The **API Tokens** dashboard list displays an alert icon (⚠) if the TTL policies for your Organization have been violated. The TTL policies set for your Organization apply to all new API tokens created by the users in your Organization. If you change a TTL policy, an alert icon will appear next to all previously created API tokens which are violating the new setting.

There are two TTL policy settings you can activate, deactivate or modify:

- **Idle Token TTL**.

  This setting defines what is the allowed idle Time to live for an API token before it violates the policy.

- **Max Token TTL**.

  This setting defines what is the maximum allowed Time to live for any API token created in your Organization. Organization users will not be able to generate API tokens with a Max Token TTL greater than the one defined by this setting.

### What can I do if an API token violates any policy or guideline in the Organization

If an API token violates a TTL policy in your Organization or in any way looks suspicions to you, you can deactivate the token from the **API Tokens** dashboard. This way it cannot be used to access the resources in the Organization.

1 On the **API Tokens** dashboard, select the API token you want to deactivate.

2 Click the **Deactivate** link.

   The API token status changes from Activated to Deactivated. The owner of the API token receives an email notification from VMware Cloud Services that a token they've been using to access the Organization has been deactivated by an **Organization Owner**.

   To reactivate an API token that has been deactivated, select the API token on the dashboard, then click the **Activate** link. The owner of the API token receives an email notification confirming the reactivation.

### How do I change the TTL policies for API tokens in my Organization

To modify the API tokens TTL policies, do the following:

1 On the **API Tokens** dashboard, click **Settings**.

| To... | Do this... |
|---|---|
| Activate or deactivate a policy. | Use the **Policy status** slider. |
| Change a TTL setting | Enter a new value in the respective TTL setting section and select a time unit from the drop-down list. The time unit can be minutes, hours, or days. |

2 Click **Save**.

Validation runs of existing tokens against the policies take place once in 24hours. This means it may take some time before the **API Tokens** dashboard list of violations gets updated as a result of the change you made.

## How do I assign default roles in my Organization

As an **Organization Owner** user in an Identity and Access Governance (IGA) activated Organization, you can assign default Organization and service roles to users in your Organization by setting up a policy.

The default roles granted through that policy apply to all users logging in the Organization from a specified federated domain and cannot be edited at the user level. To change the default role entitlements, you must modify the policy.

**Important** There is a known issue that as an **Organization Owner**, you cannot view the users in your Organization who have been granted default roles based on the policy and who have no other roles in the Organization. These users will not display on the **Active Users** list in Cloud Services Console unless they request additional roles and the requests are approved. Once users with default roles obtain additional roles in the Organization, they appear on the **Active Users** list and as an **Organization Owner**, you can grant them additional roles.

#### Prerequisites

- Your corporate identity provider is linked to VMware Cloud Services.
- Advanced IGA features are activated in the Organization.
- You have an **Organization Owner** role in the Organization.

#### Procedure

1 Log in to the Cloud Services Console with your corporate account.

2 Navigate to **Identity and Access Management > Governance > Requests**.

3 Click **Settings**.

4 In the **Grant Default Roles** section of the page, click the **Add Domain Policy** link.

5 Enter a name and description for the new policy.

6 Select the domain to which you want to apply the policy.

7 Select the Organization and service roles that you want to automatically assign to all users logging into your Organization from the specified domain.

8 Click **Save**.

#### Results

The roles you specified become available to all users from the specified domain upon their login to VMware Cloud Services.

## How do I authenticate applications with OAuth 2.0

VMware Cloud Services Console uses OAuth 2.0 so that you can give your applications secure delegated access to the protected resources in your Organization. VMware Cloud Services supports web application access where users of your app authorize access, and server-to-server interactions where access tokens are issued directly to your app.

## What is OAuth 2.0

OAuth 2.0 is an authorization protocol that lets you grant your apps secure access to your resources. Your client is authorized through an access token. The access token has a scope which defines which resources the token can access. For information about OAuth 2.0, see the OAuth specification at https://tools.ietf.org/html/rfc6749#page-8, or look at this blog post called OAuth 2.0 Simplified at https://aaronparecki.com/oauth-2-simplified/.

## How does OAuth 2.0 work with VMware Cloud Services

VMware Cloud services covers several use cases for app authorization leveraging different grant types, such as `client credentials`, `authorization code`, and `public client` with `authorization code`. Depending on your goals, you choose to create one of three types of OAuth apps that correspond to each grant type – respectively Server to server app, Web app, and Native/Mobile app.

Let's say you are an **Organization Owner** with access to VMware Cloud on AWS. You've developed an app that helps you trade in stocks. You call the app `Trading 1.0`. You want to run the app on virtual machines that are managed by a vCenter Server, but first, you must authorize your app with the VMware Cloud on AWS APIs.

1 You create an OAuth 2.0 app in the Cloud Services Console. Think of this as a way of registering your `Trading 1.0` app. You initiate the app's creation by clicking **Create App** in the **Organization > OAuth Apps** menu and go through a series of steps. At the end of the process, we issue client credentials in the form of an app ID and app secret that are used to identify your client with the APIs. You paste these credentials into your script.

2 Your app has been created in the Organization, but not yet given access to it. You grant access by adding it to the Organization. This allows the app to access the services and resources in the Organization that you defined when creating the app. This step is required only for apps that are of the Server to server app type, it is not applicable for Web and Native/Mobile apps.

3 When you run your `Trading 1.0` client app, it requests an access token from the authorization server. When authorized, the authorization server sends an access token to the APIs and your client is granted access.

## Who can create and manage OAuth apps

As an **Organization Owner** user, or an **Organization Member** user with the **Developer** role, you create and manage your OAuth apps.

You can also manage the OAuth apps created or added by other **Organization Owners** in your Organization.

## Can I regenerate an app secret

Yes, as **Organization Owner**, you can regenerate the app secret of an OAuth app in your Organization. This is useful if the **Organization Owner** who created the OAuth app is no longer with your business enterprise and you want to continue running the app.

## Can I use an API Token authentication instead of an OAuth app

Yes, if an API mandates that a user is the authenticated entity in the authorization process, you must use an API token instead. To see when to use OAuth apps versus API tokens, see What Is the difference between OAuth apps and API tokens

## How to manage OAuth 2.0 apps

As an **Organization Owner** user, you create, view and modify the details of the OAuth 2.0 apps in your Organization.

You can also:

- manage the OAuth apps created or added by other **Organization Owner** users in your Organization;
- grant access to apps created in any Organization in which you hold the **Organization Owner** role.

| To... | Do this... |
|---|---|
| View the OAuth apps that have access to your Organization. | Click **Identity & Access Management > OAuth Apps**.<br>Here you can view the apps created in other Organizations with access to your Organization. |
| Add an OAuth app created in another Organization. | 1 Click **Identity & Access Management > OAuth Apps**.<br>2 Click **Add OAuth App**.<br>3 From the drop-down menu, select the Organization in which you created the OAuth App.<br>The **Organization** drop-down menu shows only the Organizations where you have **Organization Owner** access.<br>4 From the **OAuth App** drop-down menu, select the app you want to grant access to this Organization.<br>5 Review the App Details and click **Add**. |
| Remove an OAuth app created in another Organization that has access to your Organization. | 1 Click **Identity & Access Management > OAuth Apps**.<br>2 From the list of OAuth apps that displays, select the app you want to prevent from accessing your Organization.<br>3 Click **Remove**. |

| To... | Do this... |
|---|---|
| To view the apps created in your Organization. | Click **Organization > OAuth Apps**.<br>Here you can view all the apps that were created in your Organization.<br>■ Modify an app. If you change the scoping of an app, your changes are not included to instances of the app located in other Organizations. To update the scoping, **Organization Owner** users must remove the app from their Organization, and add it again, or edit the app to reflect the updated scoping.<br>■ Remove an app from the Organization.<br>■ Add an app that has been created in the Organization but not yet given access to the Organization.<br>■ Create an app. |
| To create a new OAuth app in your Organization. | 1 Click **Organization > OAuth Apps**.<br>2 Select the type of app you want to add:<br>■ For Server to server app, see How to use OAuth 2.0 for server to server apps<br>■ For Web app, see How to use OAuth 2.0 for web apps<br>■ For Native/Mobile app, see How to use OAuth 2.0 for native and mobile apps |
| To manage the OAuth apps created in your Organization. | Click **Organization > OAuth Apps** and select the app you want to manage:<br>■ To modify the OAuth app, click **Edit**.<br>**Note** If you change the scoping of an app, your changes are not included to instances of the app located in other Organizations. To update the scoping, **Organization Owner** users must remove the app from their Organization, and add it again, or edit the app to reflect the updated scoping.<br>■ To remove an app, click **Delete**.<br>**Note** This action cannot be reverted. Any application using these client credentials will no longer be able to access protected resources and the credentials will be invalidated.<br>■ To add a server to server app that has been created in the Organization but not yet given access to the Organization, click **Add to Org**. |

## How to use OAuth 2.0 for server to server apps

If your application requires direct access to another server, without user authorization, you create a `Server to server app`. This option is based on the OAuth 2.0 `client credentials` grant type. During this flow, your app uses its OAuth credentials to retrieve an access token.

Scoping has special importance in server to server apps. Scopes provide a way to implement control over what areas in an Organization your client can access - specifically which role in an Organization, and what services and the level of permissions. As an **Organization Owner** user, you can add your server to server app to any of your Organizations. So while you can specify a wide range of access for your app over many cloud services, access is eventually determined by the services contained in an Organization. You receive notification when you add an OAuth app to an Organization that does not include the services included in the scope of the app.

### Prerequisites

- You have the required permissions for adding and managing OAuth apps in this Organization. See What Organization roles are available in VMware Cloud Services.

### Procedure

1. Log in to Cloud Services Console.
2. Click **Organization > OAuth Apps**, and then click **Create New OAuth App**.
3. Select **Server to server app**.
4. Register your client by entering a name and description.
5. Set **Access Token TTL** value for the new OAuth app.

   The Access Token time to live (TTL) defines the time period the token is valid.

   - the default Access Token TTL time is 30 minutes;
   - the maximum Access Token TTL time you can set is 300 minutes (five hours);
   - The minimum Access Token TTL time you can set is 1 minute.
6. Define scopes.

   Scopes provide a way to implement control over what areas in an Organization your client can access - specifically which role in an Organization, and what services and the level of permissions.
7. Click **Create** to generate the client credentials.
8. On the **OAuth app created** pop-up window, copy the credentials or download a JSON file, and click **Continue**.

   You are responsible for storing your credentials in a safe place.
9. (Optional) Add the app to the active Organization.

   You can skip this step and add the app to this Organization, and other Organizations later. See, How to manage OAuth 2.0 apps.

### What to do next

Paste the credentials into your script.

## How to use OAuth 2.0 for web apps

If your application is a regular web app that runs on a server, and requires user authorization, you create a `Web app`. This option is based on the OAuth 2.0 `authorization code` grant type. During this flow, users authorize your application before it accesses any resources, and your app retrieves an access token and optionally a refresh token.

### Prerequisites

- You have the required permissions for adding and managing OAuth apps in this Organization. See What Organization roles are available in VMware Cloud Services.

### Procedure

1 Log in to Cloud Services Console.

2 Click **Organization > OAuth Apps**, and then click **Create New OAuth App**.

3 Select **Web app** and click **Continue**.

4 Register your app by entering the app details:

   a Type a name and description for the new Oauth app.

   b Enter at least one redirect URI.

   After a user authorizes your client, the authorization server redirects the user back to your client to the URI you specified with an access token. It is best practice to add more than one URI. Use the format http://acme.com.

   c Specify a time span for your access token.

   The default Access Token time to live (TTL) setting is 30 minutes. The maximum value you can set is 300 minutes (five hours). The minimum value you can set is 1 minute.

   d If you want your access token to authorize requests continuously, select the **Issue a refresh token** and set **Refresh Token TTL** value.

   The default Refresh Token TTL is 30 minutes. The maximum value you can set is 300 minutes (five hours). The minimum value you can set is 1 minute.

5 Define scopes.

Scopes provide a way to implement control over what areas in your Organization your client can access - specifically which of your services and the level of permission.

6 Select the **Open ID** check box to get information about the users that authorize your app.

7 Click **Create** to generate the client credentials.

8 Copy the credentials or download a JSON file that contains your credentials. You are responsible for storing your credentials in a safe place.

9 Click **Continue**.

### What to do next

Paste the credentials into your script.

## How to use OAuth 2.0 for native and mobile apps

Public clients such as native and mobile apps cannot maintain the confidentiality of a client secret. When using OAuth 2.0 for native and mobile apps, we generate an app ID, and use the Public Key for Code Exchange (PKCE) to provide additional verification.

PKCE is a technique to secure public clients that don't use a client secret. See this blog for more information about using PKCE with mobile apps.

### Prerequisites

- You have the required permissions for adding and managing OAuth apps in this Organization. See What Organization roles are available in VMware Cloud Services.

### Procedure

1 Click your user name and select **View Organization > OAuth Apps**, and then click **Create New OAuth App**.

2 Select **Native/Mobile app** and click **Continue**.

3 Register your app by entering the app details:

   a Type a name and description for the new Oauth app.

   b Enter at least one redirect URI.

   After a user authorizes your client, the authorization server redirects the user back to your client to the URI you specified with an access token. It is best practice to add more than one URI. Use the format http://acme.com.

   c Specify a time span for your access token.

   The default Access Token time to live (TTL) setting is 30 minutes. The maximum value you can set is 300 minutes (five hours). The minimum value you can set is 1 minute.

   d If you want your access token to authorize requests continuously, select the **Issue a refresh token** and set **Refresh Token TTL** value.

   The default Refresh Token TTL is 30 minutes. The maximum value you can set is 300 minutes (five hours). The minimum value you can set is 1 minute.

4 Define scopes.

   Scopes provide a way to implement control over what areas in your Organization your client can access - specifically which of your services and the level of permission.

5 Select the **Open ID** check box to get information about the users that authorize your app.

6 Click **Create** to generate the client credentials.

7 Copy the app ID or download a JSON file that contains the app ID. You are responsible for storing these credentials in a safe place.

8 Click **Continue**.

### What to do next

Paste the credentials into your script.

## What Is the difference between OAuth apps and API tokens

You use both OAuth apps and API tokens to interact with the VMware Cloud Services APIs.

API tokens are issued by users in an Organization and are associated with the user's account and the Organization from which they generated the API token. Once created by a user in an Organization, OAuth apps act as entities in Server to server interactions and can be used in multiple Organizations. Only the users who created the API tokens can manage them. The owner of the OAuth app is the Organization in which it was created, and can be managed by users who are **Organization Owners** or **Organization Members** with a **Developer** role.

You can use both OAuth apps and API tokens to automate processes that interact with the VMware Cloud Services APIs. The difference is that API tokens incorporate the user account in the access token while OAuth apps perform authorization without a user account. When you make a choice of using an API token or an OAuth app to make an API call, you must consider the specific requirements of the API service involved in the interaction. Some APIs require a user account to be the authenticated entity while others don't. For example, if you call an API to fetch Billing and Subscription information for your Organization in VMware Cloud Services, you can use either an OAuth app of the Server to server type or an API token to make calls to the API service as it does not require authentication through user credentials and accepts client credentials as well. If an API is used by the users of an Organization to update their passwords, the API requires a user to act as the authenticating entity.

**Important** Before using OAuth apps of the Server to server type for automated calls to your cloud services, you must first consult the relevant API documentation.

# How does auditing event logs in VMware Cloud Services work

As an **Organization Owner** user you audit users' activity in your VMware Cloud services Organization by reviewing event logs. By using an associated instance of VMware Aria Operations for Logs, you can monitor events triggered by your Organization users as a result of activity with user logins, user management, API Tokens, OAuth Applications, and billing.

VMware Aria Operations for Logs is a VMware Cloud service and you need a paid or trial subscription to use it. For information about different subscription options, see vRealize Log Insight Cloud Subscriptions and Billing.

By using the VMware Aria Operations for Logs service, you get a wide range of auditing capabilities such as log filtering, archiving and forwarding. You access audit data for your Organization by starting the VMware Aria Operations for Logs service in the Cloud Services Console. This way, you open the **Audit Events for VMware Cloud Services** dashboard where you see a visual overview of the events in your Organization. If the dashboard is not activated by default, select it for viewing from the **Content Pack Dashboards** tab of the **Dashboards** page.

For more information on using VMware Aria Operations for Logs refer to Using VMware vRealize Log Insight Cloud.

**Note** If your Organization does not have a VMware Aria Operations for Logs service subscription and you still want to view VMware Cloud services log events for the present or past period, as a workaround you obtain an audit report by Chapter 11 How do I get support. You receive the report for the specified time period in an encrypted CSV file by email within 48 hours of creating your support request.

## Who can view audit data in vRealize Log Insight Cloud

As an **Organization Owner** user with **vRealize Log Insight Cloud Admin** service role, you can access all audit data for your Organization in the associated VMware Aria Operations for Logs service instance for your Organization.

**Organization Owners** can access all audit data for your Organization in the associated VMware Aria Operations for Logs service instance for your Organization.

## What Audit Events are captured by VMware Cloud Services

Event logs provide information about user actions, such as event name, the user who triggered the event, and the time and location of the event. As an **Organization Owner** user, you review audit events for your Organization by using an associated instance of VMware Aria Operations for Logs.

VMware Cloud services captures a range of audit events about users' activity in Cloud Services Console with access and account management, billing and subscription. If automation is used to manage some resources in your Oganization, some events may be triggered by a caller instead of a user.

### Searching and Filtering VMware Cloud Services Audit Events

You can search for and filter the log events for your Organization in one of two ways: by using saved queries from the **Audit Events for VMware Cloud Services** content pack and by creating custom queries.

You access content packs from the **Content Packs** menu of your vRealize Log Insight Cloud instance. For more information, see Working with Content Packs.

You can search for and filter log events in the **Explore Logs** page of vRealize Log Insight Cloud service by using custom queries for VMware Cloud Services audit events. To view only audit events for VMware Cloud Services, as a search criteria, select **log_type**, then **Contains** and enter **`csp-audit`**. To search for specific events, create a query that contains the event type.

## Audit Events for VMware Cloud Services

### Table 9-1. Account Management

| Audit Event Name | Event Type | Description |
|---|---|---|
| UserLogin | csp__user_login | Successful user login. |
| UserLogout | csp__user_logout | Successful user logout. |
| GenerateApiToken | csp__generate_api_token | User generated a personal API token. |
| RevokeApiToken | csp__revoke_api_token | User revoked a personal API token. |
| RevokeAllApiTokens | csp__revoke_all_api_tokens | User revoked all personal API tokens. |
| RefreshTokenExchangeFailed | csp__refresh_token_exchange_failed | User made an unsuccessful attempt to generate access token by API token refresh. |
| FirstLogin | csp__first_login | User was assigned the roles from the invitation upon first log in. |
| LinkAccount | csp__link_account | User linked their corporate federated account to their VMware ID account. This action allowed user to log in VMware Cloud Services with their corporate credentials. |
| UnlinkAccount | csp__unlink_account | User changed the account linked to their VMware ID. |
| CreateOrgOAuthApp | csp__create_org_o_auth_app | Caller created an OAuth app in an Organization. |
| UpdateOrgOAuthApp | csp__update_org_o_auth_app | Caller updated an OAuth app in an Organization. |
| DeleteOrgOAuthApp | csp__delete_org_o_auth_app | Caller deleted an OAuth app in an Organization. |
| OrgOAuthAppNewSecretRotation | csp__org_o_auth_app_new_secret_rotation | Caller rotated the secret of an OAuth app in an Organization. |
| ActivateMfa | csp__activate_mfa | User with VMware ID activated an MFA device. |
| DeactivateMfa | csp__deactivate_mfa | User with VMware ID deactivated an MFA device. |
| TurnOnMfa | csp__turn_on_mfa | User with VMware ID turned on Multi-factor authentication for their account. |

### Table 9-1. Account Management (continued)

| Audit Event Name | Event Type | Description |
|---|---|---|
| TurnOffMfa | csp__turn_off_mfa | User with VMware ID turned off Multi-factor authentication for their account. |
| RegenerateMfaRecoveryCodes | csp__regenerate_mfa_recovery_codes | User with VMware ID regenerated a new set of recovery codes for Multi-factor authentication. |
| UpdateMfaAttributes | csp__update_mfa_attributes | User with VMware ID updated the MFA settings for their account. |
| GenerateNewMfaActivationSecret | csp__generate_new_mfa_activation_secret | User with VMware ID generated a new activation secret for setting up MFA for their account. |
| InvitationSentAck | csp__invitation_sent_act | Internal notification created when an invitation was sent to a user. |
| CreateMspInvitation | csp__create_msp_invitation | Email invitation to onboard a new provider Organization was sent to a new service provider. |
| UpdateMspInvitation | csp__update_msp_invitation | An updated email invitation to onboard a new provider Organization was sent to a new service provider. |
| DeleteMspInvitation | csp__delete_msp_invitation | Email invitation to onboard a new provider Organization sent to a new service provider was revoked. |

### Table 9-2. Organization Management

| Audit Event Name | Event Type | Description |
|---|---|---|
| CreateOrganization | csp__create_org | User created a new Organization. |
| UpdateOrganization | csp__update_org | User updated an existing Organization. |
| DeleteOrganization | csp__delete_org | User deleted an existing Organization. |
| InviteExistingUserToOrganization | csp__invite_existing_user_to_org | Existing user was added to an Organization. |
| RemoveUserFromOrganization | csp__remove_user_from_org | Existing user was removed from an Organization. |
| UpdateUserRolesOnOrganization | csp__update_user_roles_on_org | The roles of an existing user were updated. |
| InviteNonExistingUserToOrganization | csp__invite_non_existing_user_to_org | Email invitation was sent to a new user. |
| RevokeUserInvitations | csp__revoke_user_invitations | Invitations sent to users by email were revoked. |

## Table 9-2. Organization Management (continued)

| Audit Event Name | Event Type | Description |
|---|---|---|
| RemoveClientFromOrganization | csp__remove_client_from_org | User removed an OAuth app assigned to an Organization. The action did not delete the OAuth app. |
| AssignRolesToClientOnOrganization | csp__assign_roles_to_client_on_org | Caller assigned service/Organization roles to a client in an Organization. The action indicates a first time assignment to a client that had never had roles assigned before. |
| UpdateClientRolesOnOrganization | csp__update_client_roles_on_org | Caller updated service/Organization roles to a client in an Organization. |
| UpdateUserDefaultOrganization | csp__update_user_default_org | User updated the default Organization displayed for their account. This action applies only to users who are members of more than one Organization. |

## Table 9-3. Groups

| Audit Event Name | Event Type | Description |
|---|---|---|
| RemoveGroupFromOrganization | csp__remove_group_from_org | User removed an existing group from an Organization. |
| AssignRolesToGroupOnOrganization | csp__assign_roles_to_group_on_org | User assigned Organization and service roles to a newly created group in an Organization. |
| UpdateGroupRolesOnOrganization | csp__update_group_roles_on_org | User updated role assignments of an existing group in an Organization. |
| CustomGroupAddClients | csp__custom_group_add_clients | User added new members to a custom group in an Organization. |
| CustomGroupRemoveClients | csp__custom_group_remove_clients | User removed existing members from a custom group in an Organization. |

## Table 9-4. Billing and Subscription

| Audit Event Name | Event Type | Description |
|---|---|---|
| CreateSubscription | csp__create_subscription | User created a subscription for a new or existing service. |
| AddOrgPaymentMethod | csp__add_org_payment_method | User added a new payment method to their Organization. |
| RemoveOrgPaymentMethod | csp__remove_org_payment_method | User removed a payment method from their Organization. |
| UpdateOrgDefaultPaymentMethod | csp__update_org_default_payment_method | User updated the default payment method of an Organization. |

## Table 9-4. Billing and Subscription (continued)

| Audit Event Name | Event Type | Description |
|---|---|---|
| AddDetailsToOrg | csp__add_details_to_org | User added a company address and/or other Billing and Subscription details to an Organization. |
| UpdateOrgAddress | csp__update_org_address | User updated the company's address in the Billing and Subscription details for their Organization. |
| UpdateOrgCommerceData | csp__update_org_commerce_data | User updated the Billing and Subscription details for their Organization (currency, annual billing date, etc.) |
| UpdateOrgTaxId | csp__updated_org_tax_id | User updated the Tax ID in the Billing and Subscription details for their Organization. |
| UpdateOrgPoReferenceNumber | csp__update_org_po_reference_number | User set a new Organization PO reference number. |
| IncomingOrder | csp__incoming_order | Caller created an order for a service subscription. |

## Table 9-5. Identity Governance and Administration

| Audit Event Name | Event Type | Description |
|---|---|---|
| ApproveDenyEntitlementRequest | csp__iga_entitlements_requests_approval | An entitlement request was approved or denied by **Organization Owner**. |
| CreateEntitlementRequest | csp__iga_register_entitlements_request | User created an entitlement request. |
| CreateEntitlementRequestForNonOrgMember | csp__iga_register_entitlements_request_non_org_member | New non Organization user created an entitlement request. |
| CancelEntitlementRequest | csp__iga_delete_entitlement_request | User canceled an entitlement request. |
| CancelEntitlementRequestForNonOrg | csp__iga_delete_entitlement_request_non_org_member | New non Organization user canceled an entitlement request that was already submitted by the same user. |
| EnablingGovernance | csp__iga_status_change | Identity Governance and Administration was activated for Organization. |
| UpdateGovernancePolicies | csp__iga_update_governance_policies_request | User updated Identity Governance and Administration policies. |

# How do I create a NIST pre-login notification in VMware Cloud Services

To meet NIST 800-53 AC-8 audit requirements, you must be able to show a pre-login notification to **Organization Member** users accessing your Organization.

The NIST notification is applied to the domain from which users are logging in to VMware Cloud Services regardless of the Organization to which they belong. When users log-in to an Organization from a domain for which a NIST notification has been created, they see a dialog asking them to read and accept the terms of the notification before proceeding to the password entry page.

As an **Organization Owner**, you request your custom NIST 800-53 AC-8 notification message by opening a support request on VMware Customer Connect. Include the following information in your support request:

- the enterprise domain for which you want to apply NIST notification;
- the text you want displayed in the NIST notification dialog;
- localized versions of the text in all languages that you need;
- the name of your VMware Cloud Services Organization.

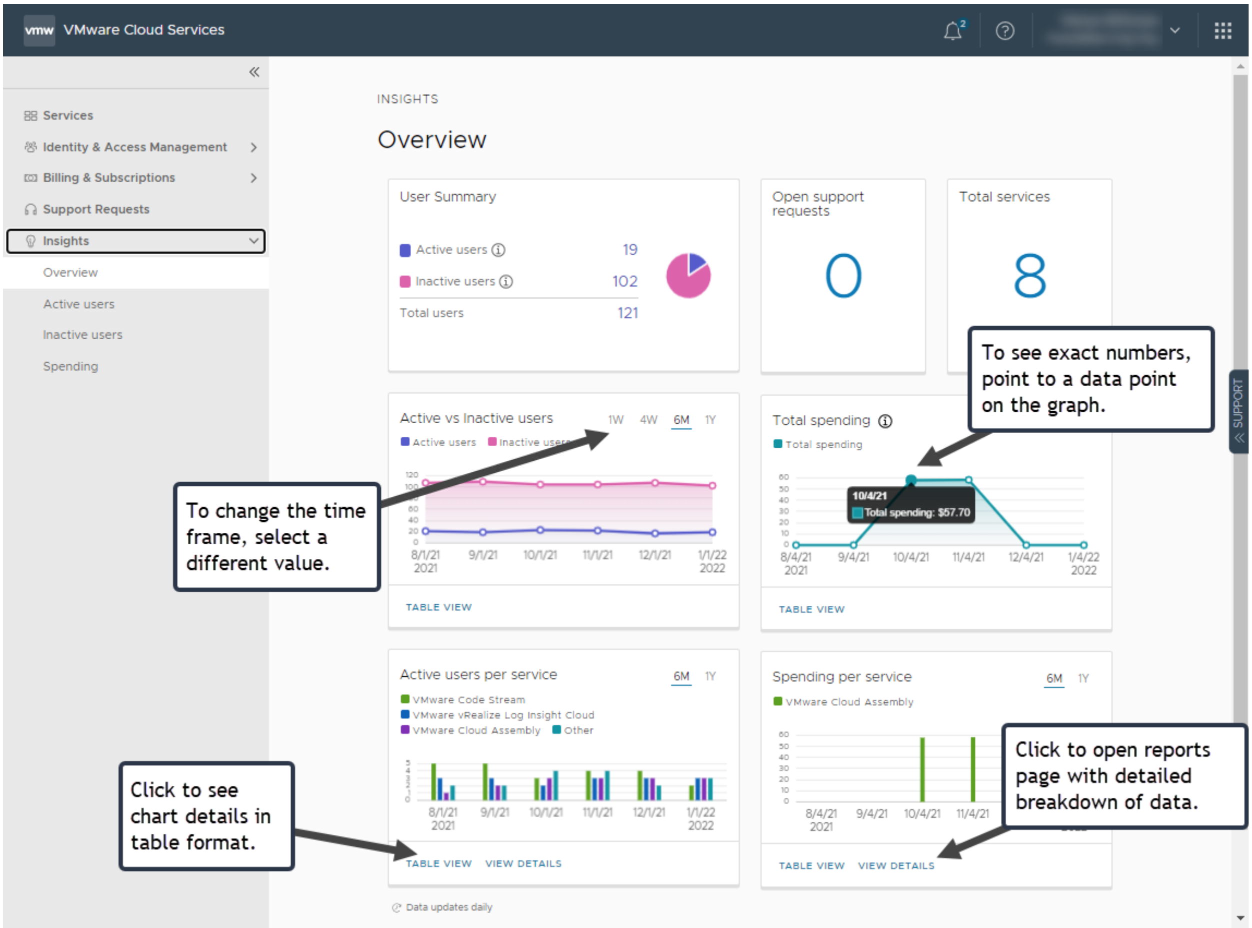
The NIST notification is implemented manually by VMware Technical support after your **Organization Owner** status and domain are verified.

# How do I use the Data Insights Dashboard

As an **Organization Owner** user, you view how the services in your Organization are used over time through the **Insights** dashboard in the Cloud Services Console.

To access the **Insights** dashboard, select **Insights > Overview**.

The **Insights** dashboard displays a visual snapshot of the activity level of users in your Organization over a pre-defined time period. You obtain information about the total number active and inactive users in your Organization, active and inactive users per services, total spending for all services, and spendings per service breakdown.



To see exact numbers, point to a data point on the graph.

To change the time frame, select a different value.

Click to see chart details in table format.

Click to open reports page with detailed breakdown of data.

The data on the **Insights** dashboard updates daily.

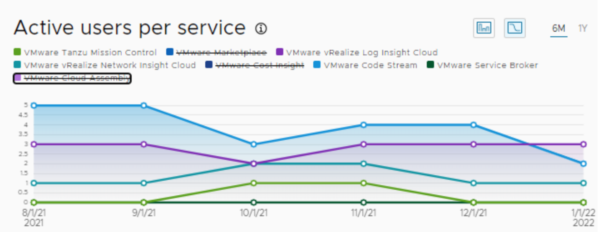
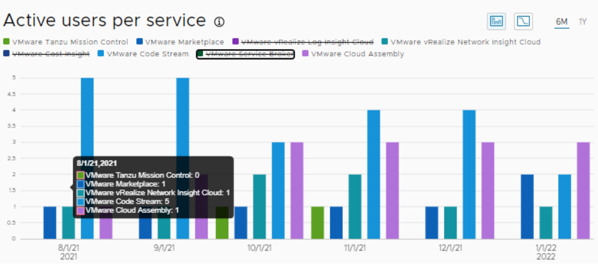
## What else can I do with the Data Insights Dashboard

As an **Organization Owner** user, you can obtain detailed breakdown of data for your services, usage and costs by accessing the **Active users**, **Inactive users** and **Spendings** dashboards. You can filter the data to view subsets of the information displayed on each tab.

### The Active users dashboard

The **Active users** dashboard displays information about all active users per service in your Organization. Active users are those users who have signed in to VMware Cloud services at least once over a period of 60 days.

| To... | Do this... |
|---|---|
| Switch between graph and chart views of the data | Click the graph (📈) or chart (📊) icons in the top right corner of the dashboard. |
| To change the time period for the data report | Select a different time period by clicking on the respective icon in the top right corner of the dashboard. You can choose between six months and one year. |

| To... | Do this... |
|---|---|
| To filter active users per specific services | Click the names of the services you want to exclude from the view.<br><br> Active users per service ⓘ<br>6M<br>1Y<br>VMware Tanzu Mission Control<br>~~VMware Marketplace~~<br>VMware vRealize Log Insight Cloud<br>VMware vRealize Network Insight Cloud<br>~~VMware Cost Insight~~<br>VMware Code Stream<br>VMware Service Broker<br>~~VMware Cloud Assembly~~<br>5<br>4.5<br>4<br>3.5<br>3<br>2.5<br>2<br>1.5<br>1<br>0.5<br>0<br>8/1/21 2021<br>9/1/21<br>10/1/21<br>11/1/21<br>12/1/21<br>1/1/22 2022<br>Excluded services names appear crossed out. To include a service back in the data view, click on its name. |
| See a breakdown of active users per service in a specific month | Point over a data point in the chart or graph.<br><br> Active users per service ⓘ<br>6M<br>1Y<br>VMware Tanzu Mission Control<br>VMware Marketplace<br>~~VMware vRealize Log Insight Cloud~~<br>VMware vRealize Network Insight Cloud<br>~~VMware Cost Insight~~<br>VMware Code Stream<br>~~VMware Service Broker~~<br>VMware Cloud Assembly<br>8/1/21,2021<br>VMware Tanzu Mission Control: 0<br>VMware Marketplace: 1<br>VMware vRealize Network Insight Cloud: 1<br>VMware Code Stream: 5<br>VMware Cloud Assembly: 1<br>5<br>4.5<br>4<br>3.5<br>3<br>2.5<br>2<br>1.5<br>1<br>0.5<br>0<br>8/1/21 2021<br>9/1/21<br>10/1/21<br>11/1/21<br>12/1/21<br>1/1/22 2022 |
| View chart details in a table view | Click the **Show Details in a Table View** link. |
| View active user details | The table below the data chart provides details about all active users in your Organization, such as name, email, and days since last login.<br>Scroll the pages in the table by clicking the back and forth icons. |

## The Inactive users dashboard

The **Inactive users** dashboard displays information about all inactive users per service in your Organization. Inactive users are those users who have not signed in to VMware Cloud services for the past 60 days.

| To... | Do this... |
|---|---|
| Switch between graph and chart views of the data | Click the graph (📈) or chart (📊) icons in the top right corner of the dashboard. |
| To change the time period for the data report | Select a different time period by clicking on the respective icon in the top right corner of the dashboard. You can choose between six months and one year. |
| To filter inactive users per service | Click the names of the services you want to exclude from the view. |
| To see a breakdown of inactive users per services in a specific month | Point over a data point in the chart or graph. |
| View chart details in a table view | Click the **Show Details in a Table View** link. |

| To... | Do this... |
|---|---|
| View inactive user details | The table below the data chart provides details about inactive users in your Organization, such as name, email, days since last login, and date of last action.<br>Scroll the pages in the table by clicking the back and forth icons. |
| Remove an inactive user from your Organization | Select the check box next to the user's name, then click **Remove From Org** |

### The Spending per service dashboard

This dashboard displays the monthly spending per service in your Organization over a period of time. The cost value you see is in the default currency of your Organization.

| To... | Do this... |
|---|---|
| Switch between graph and chart views of the data | Click the graph (📈) or chart (📊) icons in the top right corner of the dashboard. |
| To change the time period for the data report | Select a different time period by clicking on the respective icon in the top right corner of the dashboard. You can choose between six months and one year. |
| To filter the services for which spending is displayed | Click the names of the services you want to exclude from the view. |
| To see cost breakdown for the services in a specific month | Point over a data point in the chart or graph. |
| View chart details in a table view | Click the **Show Details in a Table View** link. |

## What’s involved in working with Projects in Cloud Services Console

VMware Cloud Services uses Projects as a way to group an Organization’s resources into distinct buckets and assign user and group access to the resources in each bucket. This allows **Organization Owners** to logically organize, map and track usage of their cloud services resources.

When you think of resources in VMware Cloud Services, imagine pre-defined, measurable and logical segments of a specific service. By organizing the services resources in Projects, **Organization Owner** users can measure and track the usage of cloud services in their enterprise across departments or Cost Centers.

**Important** Only a few VMware Cloud services have been enabled so far to use the Projects feature in Cloud Services Console. To learn if a service you are using can utilize Projects for resource grouping purposes, consult the documentation for that service or contact VMware Support.

Let's say you have two Projects in your Organization – Project 1 and Project 2, and three services – Service A, Service B, and Service C.

- Services A and B are enabled for Project 1.
- Services B and C are enabled for Project 2.

The resource grouping of the enabled services allows resources of service B to be used in both Projects, while resources of service A and service C are used in one Project each.

## How do I create a Project in Cloud Services Console

To set up and manage Projects, you must have an **Organization Owner** or a **Project Administrator** role in the Organization. You set up a new Project from the **Identity and Access Management > Projects** in Cloud Services Console.

There are three steps involved in setting up a new Project:

1. Define a name for the new Project.

   Your new Project will remain empty until the services you plan to use with it are enabled.

2. View the enabled services and resources for your Project.

   You know a service is enabled for your Project if it is listed under the **Enabled Services** section and resources are listed in the **Resources** table.

3. Assign user and/or group access to the new Project.

## How do I delete a Project from my Organization

You can delete a Project only if these two conditions are met:

- The Project does not have enabled services and resources associated with it.
- Users and/or groups do not have access permissions assigned for the Project.

# Billing & Subscriptions 10

VMware Cloud Services users with **Organization Owner** role can view billing and subscription details and manage payment methods for their Organization. **Organization Member** users with additional **Billing Read-Only** role can view billing and subscription details for their Organization without the option to manage payment methods.

Each Organization in VMware Cloud Services is associated with a billing account.

You can use VMware Cloud services on demand or by purchasing subscriptions for a term period of 1 or 3 years. The purchase order outlines the capacity, term start and end dates, and negotiated price of the commitments in the subscription. VMware Cloud Services bills you according to the terms laid out in the purchase order.

You receive one monthly invoice or Activity Statement for all costs incurred by the Organization's services purchased through VMware.

If your Organization purchased services from multiple sellers, the **Billing and Subscriptions** page displays information for all sellers. However, incurred costs and service charges information for the services purchased through non-VMware sellers is not available through the Cloud Services Console. Contact the seller to obtain this information.

This chapter includes the following topics:

## Getting started with VMware Cloud Services billing and subscriptions

When you purchase VMware Cloud Services subscriptions for the first time, you receive an email with a link that opens the VMware Cloud Services onboarding workflow.

As a first time user and an **Organization Owner** you provide address and default payment method when you set up the Organization. VMware Cloud Services bills each Organization based on the billing details set up during onboarding:

- The **Address** of your enterprise determines the selling unit, currency options, taxation, and payment methods available to the Organization.

  For example, US addresses are charged in US dollars and subject to sales tax, while UK addresses are charged in British pounds, and are subject to VAT. In addition, each Organization registered in the European Union has the option of entering a tax ID.
- The **Currency to pay with** in the Organization is determined by the selling unit, which is derived from the country where your business address resides. Each Organization can have a default currency and pre-approved exceptions currencies based on the address of the Organization. Different selling units can be associated with one or more currencies. To learn more, see How is my payment currency determined.
- The **Default Payment Method** can be either VMware prepaid funds, credit card, or Pay by Invoice (PBI). The default payment methods available to your Organization at onboarding vary based on your billing account.

  For example, some users can only select a PBI as their payment method, while others can select VMware funds and credit cards.

### Prerequisites

- You are onboarding a paid cloud service in a new Organization in VMware Cloud Services.

### Procedure

1. On the **Create an Organization** step of the service onboarding workflow, provide the billing details for your Organization:

   a. Enter a name for your Organization.

   b. Provide the address of your enterprise.

      **Important** The business address you provide on this step must pass an address validation check and comply with the validation rules. To learn more, see What do I need to know about address validation.

   c. If several currency options are available, select the currency in which your Organization will be billed.

   d. Select the default payment method.

   **Note** After a service is onboarded in an Organization, **Organization Owner** users can How do I change my Organization's default payment method used to cover your invoices at any time. The currency in which your Organization is billed cannot be changed in Cloud Services Console. To switch to a different currency, you must file a support ticket.
2. Click **Complete**.

### Results

Your Organization billing account is now created. You can now get billing information, manage payment methods and service subscriptions from the **Billing and Subscription** menu in Cloud Services Console.

## What do I need to know about address validation

VMware Cloud Services applies validation criteria to the business address provided for your Organization.

As an **Organization Owner** you enter a business address when you set up the Organization during service onboarding or when you add new services or subscriptions to an existing Organization. To pass validation, an Organization's address must contain correct information about street address, postal code, city, state or province (if applicable), and country. The validation check is performed automatically when:

- You enter or update the business address during service/subscription onboarding.
- You update the business address from the **Organization > Details** page.

The following table provides details about the possible outcomes of the validation check and what actions you can take if needed.

| If... | Then... |
|---|---|
| Organization address validation is successful. | You proceed to the next step of the service/subscription onboarding workflow. |
| Organization address does not comply with the validation rules. Compliant address is suggested. | The **Edit or Select an Address** pop-up window opens to display the original address and a suggested address which is compliant with the validation rules.<br>■ If you select the suggested address, you proceed to the next step of the workflow.<br>■ If you decide to keep the original address, you must acknowledge that it does not comply with the validation rules and provide your consent to authorize VMware to make all the necessary changes to the address so that it becomes compliant. You do that by selecting the respective check box on the **Edit or Select an Address** pop-up window.<br>■ To modify the original address provided for the Organization, click the **Edit Address** button. This takes you back to the Organization Profile page where you can make the necessary changes. |

| If... | Then... |
|---|---|
| Organization address could not be validated. No compliant address is suggested. | When the address validation fails and no alternative address is suggested, a pop-up window opens promting you to do one of the following:<br>■ Edit the address.<br>■ Provide your consent to authorize VMware to make all the necessary changes to the Organization address so that it complies with the validation rules by selecting the respective check box. Only after accepting the consent you can proceed with the service/ subscription onboarding. |
| Organization address updated by VMware after **Organization Owner** provided consent. | When you log in as an **Organization Owner** in VMware Cloud Services, a pop-up window opens showing the updated address.<br>■ If you accept the new validated address, it replaces the existing Organizaiton address. All **Organization Owner** users will receive an in-app notification about the change.<br>■ If you dismiss the new validated address, whenever you open the onboarding service/subscription workflow, you will be prompted to change the address to comply with the validation rules. |

## How do I use the billing and subscriptions pages in VMware Cloud Services

The **Billing & Subscriptions** section in Cloud Services Console has a few basic pages that help you see your Organization's activity and manage the payment methods used for your services and subscriptions.

| | |
|---|---|
| **Overview** | The **Overview** page displays the current accrued costs and charges for the past month for all the services in the Organization. If you purchased subscriptions through multiple sellers, you can access details for each seller from this page.<br>To learn more, see How do I get billing information for my Organization |
| **Manage Payment Methods** | The **Manage Payment Methods** page allows you to add new payment methods to your Organization and to change the default payment method.<br>To learn more, see How do I manage the payment methods for my Organization |
| **Subscriptions** | The **Subscriptions** page displays details for all VMware Cloud Services subscriptions purchased in your Organization.<br>To learn more, see How do I work with VMware Cloud Services subscriptions and commitments |

| | |
|---|---|
| **Promotional Credits** | The **Promotional Credits** page displays the available promotional credits that you can apply and redeem against the Organization's monthly costs.<br>To learn more, see How to pay with promotional credits |
| **Invoices & Statements** | The **Invoices & Statements** page lets you view and download the activity statements and invoices for your Organization.<br>To learn more, see How do I view statements and invoices |

## How do I get billing information for my Organization

Billing information for your Organization can be viewed from the **Overview** page under the **Billing & Subscriptions** menu in Cloud Services Console.

As an **Organization Owner** user or an **Organization Member** user with additional **Billing Read-only** role permissions, you can view the following billing information for all services purchased from VMware:

- accrued costs and charges for the current billing period for all services purchased from VMware;
- promotional credits applied to current costs;
- payments and outstanding balance for the past billing period for all services purchased from VMware;
- a detailed account of all purchases, charges, discounts, etc. for all services by month.

**Note** For billing information for services purchased through a seller, you must access the seller's billing console. To learn more, see How do I view seller information.

### Your Current Costs

The **Current Costs** section reflects the costs of the services you purchased from VMware. For example, hourly usage of private clouds per CPU. These are accrued costs, and reflect usage for services from the beginning of the current billing period, up until and including the day you view them. The accrued costs reflect only on-demand usage of services in your Organization and do not include commitments costs. This information is refreshed daily.

The **Current Costs** section also provides information about any promotional credits and discounts you might have received from the VMware Discount program.

### Your Last Billing Period

In the **Last Billing Statement** section, you can view itemized charges accrued over the previous billing period. The billing period is determined by the date the first service was set up in the Organization and lasts one month. For example, if an **Organization Owner** onboarded the first service of the Organization on the 15th of the month, the billing period for all the services in the Organization runs from the 15th of one month to the 14th of the next.

The **Last Billing Statement** section provides a summary of the charges for both on-demand and commitment services accrued during the past billing period. To view, download and print a detailed activity statement file for the past billing period, click the **View Statement (PDF)** link at the bottom of the **Last Billing Statement** section .

To view and print any of your last 15 activity statements, on-demand invoices and yearly commitment invoices, click the **All Statements** link. For more information, see How do I view statements and invoices.

There might be cases where a cloud service estimates current cost usage for certain items on a different date to that of the start of your billing period. In this case, there might be a time lag between when the usage occurs and when it shows up on your bill. For more information about how cloud services estimate their current costs, see How Are My Current Costs Estimated.

## How are my current costs estimated

The **Current Costs** section in your billing overview reflects the costs of the services in your Organization at any given time. The costs displayed in this section are only for the services purchased from VMware. They are accrued costs, and reflect usage for services from the beginning of a defined period. This defined period might be different from your billing period.

To see how our cloud services estimate their current costs and how these costs affect your billing cycle, see the following table.

| VMware Cloud service | How your current costs are estimated |
|---|---|
| VMware Cloud on AWS | Host usage for VMware Cloud on AWS is tracked in alignment with your billing cycle. The host usage shown on your bill is the entirety of your host usage during the billing period.<br>Other types of usage, including data transfer out, IP address usage and remaps, and EBS usage are received on the fifth of each month and include usage up to the last day of the previous month. For these types of usage, there is a time lag between when the usage occurs and when it shows up on your bill. The amount of time lag depends on where the beginning of your billing cycle is in relation to the fifth of the month.<br>For more information, see VMC billing information. |

## How is my payment currency determined

VMware Cloud services support the payment for services in various currencies using a credit card, funds, and promotional credits. The payment currency is selected from a list of options during the Organization setup.

When you set up an Organization, the business address you enter determines the currency options presented to you on the **Organization and Payment** step of the onboarding workflow. An Organization can pay with its default currency, with a pre-approved exception currency, or with USD if the `Global USD` option is selected. For detailed information about service onboarding, refer to the Getting Started with VMware Cloud Services guide.

If you need to change the payment currency to a different option from the one already defined in the Organization, you can do that at any time. See How do I change the payment currency in my Organization.

VMware Cloud services support two selling units: one for US customers and one for non-US customers. While US customers are only billed in US dollars, countries within the non-US selling unit are billed in various currencies. How might this affect you?

- The address of the Organization also determines the type of taxes - sales taxes or VAT, for example. Tax IDs are used to facilitate the administration of local taxes. You might want to enter a tax ID if you have a tax exemption status, or similar. You can enter a tax ID when you set up your Organization. You can also do this later on the Organization page, by clicking your user name and selecting **View Organization**.
- You can use any credit card with any billing address to pay for your services. You might incur foreign transaction fees from your credit card provider if the payment currency of the Organization is different than the card currency.
- If you want to change the address of your Organization, the new address must be located in the same selling unit as the original address. In addition, you cannot change the address to one residing in a country with a currency different to that of the original address. See the table below to learn more.

  If you need to change to an address located in a different selling unit or a country with different currency, submit a support request.

  If you need to change the payment currency to a different currency from the one set for the Organization, you must create a support ticket. To learn how, see Chapter 11 How do I get support.
- You can use any fund as a payment method in your Organization if the currency of the fund is the same as the Organization's currency, and it belongs to the same selling unit. To pay with a fund, your billing account currency must match the fund currency, and the fund currency must match the order subscription currency.

## VMware Cloud Services Selling Units

Use the information in these tables to determine the currency in which you are charged for your services.

## Table 10-1. Selling Unit International Exchange for Non-US Customers

| If the address of your Organization is in this country… | Your default payment currency is… |
|---|---|
| Afghanistan, Algeria, American Samoa, Angola, Anguilla, Antarctica, Antigua and Barbuda, Argentina, Armenia, Aruba, Azerbaijan, Bahamas, Bahrain, Bangladesh, Barbados, Belarus, Belize, Benin, Bermuda, Bhutan, Bolivia, Bonaire, Sint Eustatius and Saba, Botswana, Bouvet Island, Brazil, British Indian Ocean Territory, Brunei Darussalam, Burkina Faso, Burundi, Cambodia, Cameroon, Canada, Cape Verde, Cayman Islands, Central African Republic, Chad, Chile, Colombia, Comoros, Congo, Cook Islands, Costa Rica, Cote D'Ivoire, Cuba, Curacao, Djibouti, Dominica, Dominican Republic, East Timor, Ecuador, Egypt, El Salvador, Equatorial Guinea, Eritrea, Estonia, Ethiopia, Falkland Islands, Faroe Islands, Fiji, Finland, French Guiana, French Polynesia, French Southern Terr., Gabon, Gambia, Georgia, Ghana, Grenada, Guadeloupe, Guam, Guatemala, Guinea, Guinea-Bissau, Guyana, Haiti, Heard Island and Mcdonald Islands, Honduras, Hong Kong, India, Indonesia, Iran, Iraq, Israel, Jamaica, Jordan, Kazakhstan, Kenya, Kiribati, Republic of Korea, Kuwait, Kyrgyzstan, Lao, Lebanon, Lesotho, Liberia, Libya, Macao, Madagascar, Malawi, Malaysia, Maldives, Mali, Marshall Islands, Martinique, Mauritania, Mauritius, Mayotte, Mexico, Micronesia, Moldova, Montserrat, Morocco, Mozambique, Myanmar, Namibia, Nauru, Nepal, Netherlands Antilles, New Caledonia, New Zealand, Nicaragua, Niger, Nigeria, Niue, North Korea, Northern Mariana Islands, Oman, Pakistan, Palau, Occupied Palestinian Territory, Panama, Papua New Guinea, Paraguay, Peru, Philippines, Pitcairn, Puerto Rico, Qatar, Reunion, Russian Federation, Rwanda, Saint Barthelemy, Saint Helena, Saint Kitts and Nevis, Saint Lucia, Saint Martin, Saint Pierre and Miquelon, Saint Vincent and the Grenadines, Samoa, Sao Tome and Principe, Saudi Arabia, Senegal, Seychelles, Sierra Leone, Singapore, Solomon Islands, Somalia, South Africa, South Georgia and the South Sandwich Islands, South Sudan, Sri Lanka, Sudan, Suriname, Svalbard and Jan Mayen, Swaziland, Syria, Taiwan, Tajikistan, Tanzania, Thailand, Timor-Leste, Togo, Tokelau, Tonga, Trinidad and Tobago, Tunisia, Turkey, Turkmenistan, Turks and Caicos Islands, Tuvalu, Uganda, Ukraine, United Arab Emirates, United States Minor Outlying Islands, Uruguay, Uzbekistan, Vanuatu, Venezuela, Vietnam, Virgin Islands, Wallis and Futuna, Western Sahara, Yemen, | USD |
| Albania, Andorra, Austria, Belgium, Bosnia and Herzegovina, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, France, Germany, Greece, Greenland, Hungary, Iceland, Ireland, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Macedonia, Malta, Monaco, Montenegro, Norway, Poland, Portugal, Romania, San Marino, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, The Netherlands, Vatican City State, Yugoslavia, Zambia, Zimbabwe, Aland Islands | EUR |
| Gibraltar, Guernsey, Isle of Man, Jersey, United Kingdom, | GBP |
| Japan | JPY |
| China, Mongolia | CNY |
| Australia, Christmas Island, Cocos (Keeling) Islands, Norfolk Island | AUD |

## Table 10-2. Selling Unit US for US Customers

| If the address of your Organization is in this country | You are charged in |
|---|---|
| United States of America | USD |

## How do I change the payment currency in my Organization

Your payment currency is determined as part of the service onboarding workflow when you set up the Organization. The **Organization Owner** user setting up the Organization selected either the default currency or a pre-approved exception.

Your Organization payment currency can be one of the following:

- The default currency based on your business address.
- Global USD.
- A different pre-approved currency.

### Prerequisites

To change the payment currency in your Organization, you must create a support ticket with VMware Customer Connect. Organization owners can initiate the change at any time through Cloud Services Console.

.

### Procedure

1. Log in to Cloud Services Console and select **Billing and Subscriptions > Manage Payment Methods**.
2. Click the **Change Currency** button.
3. In the dialog window that opens, click **Create Support Request**.

   This opens the VMware Support page on VMware Customer Connect.
4. Under **Non-technical Support**, click **Get Guided Support**.
5. Under **Cloud Services** click **Billing and Usage** and follow the prompts to create the request.

# How do I view seller information

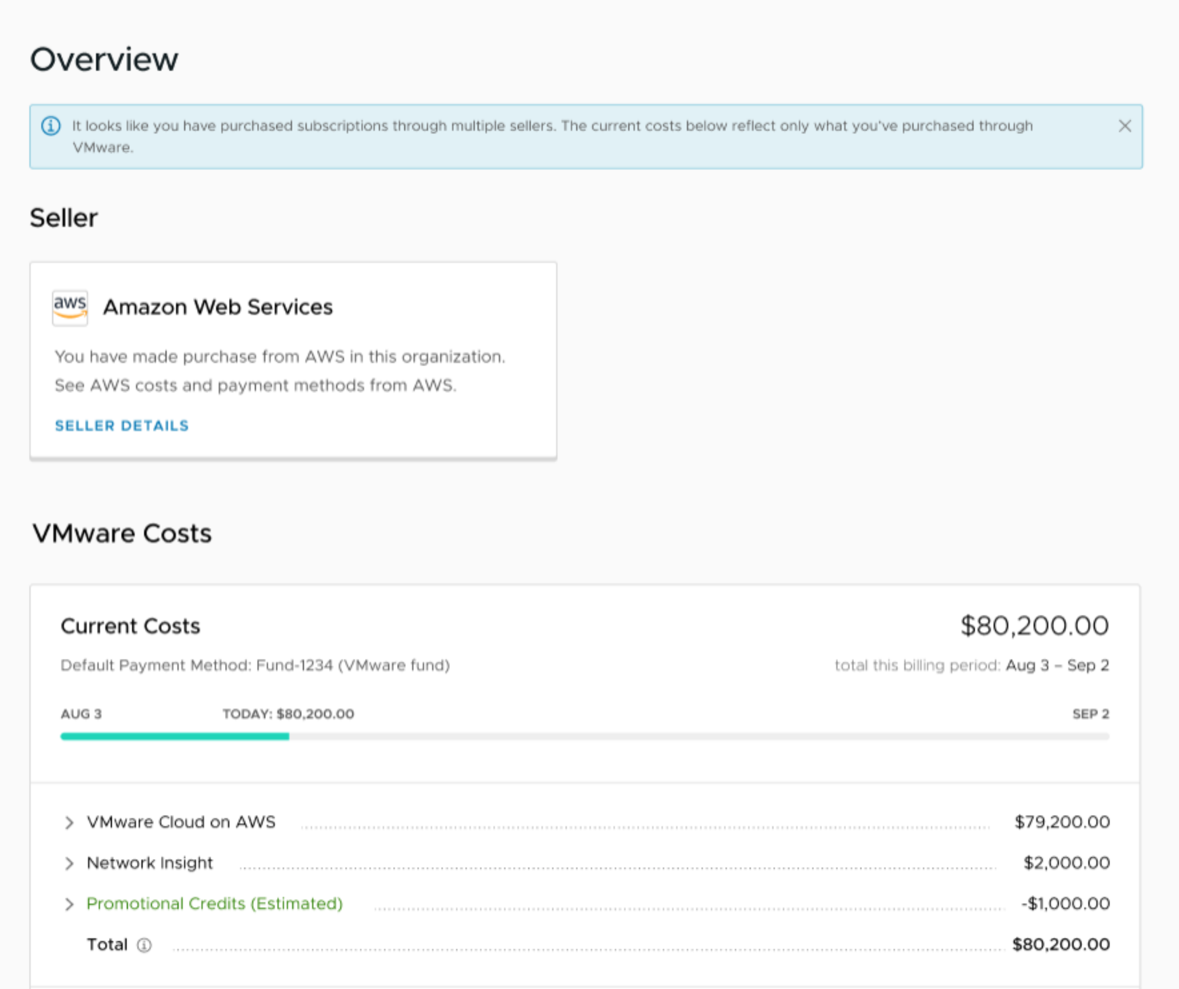
Seller information is available only if your Organization has services and subscriptions purchased from one or more VMware partners.

Each seller in your Organization is represented by a separate tile.

### Procedure

1. Log in to Cloud Services Console and select **Billing and Subscriptions > Overview**.

   The **Sellers** section lists the sellers from which your Organization has purchased services. For example, if an Organization has purchased services from VMware and Amazon Web Services, you will see two sellers.



Overview

It looks like you have purchased subscriptions through multiple sellers. The current costs below reflect only what you've purchased through VMware.

Seller

Amazon Web Services

You have made purchase from AWS in this organization. See AWS costs and payment methods from AWS.

SELLER DETAILS

VMware Costs

Current Costs $80,200.00

Default Payment Method: Fund-1234 (VMware fund)

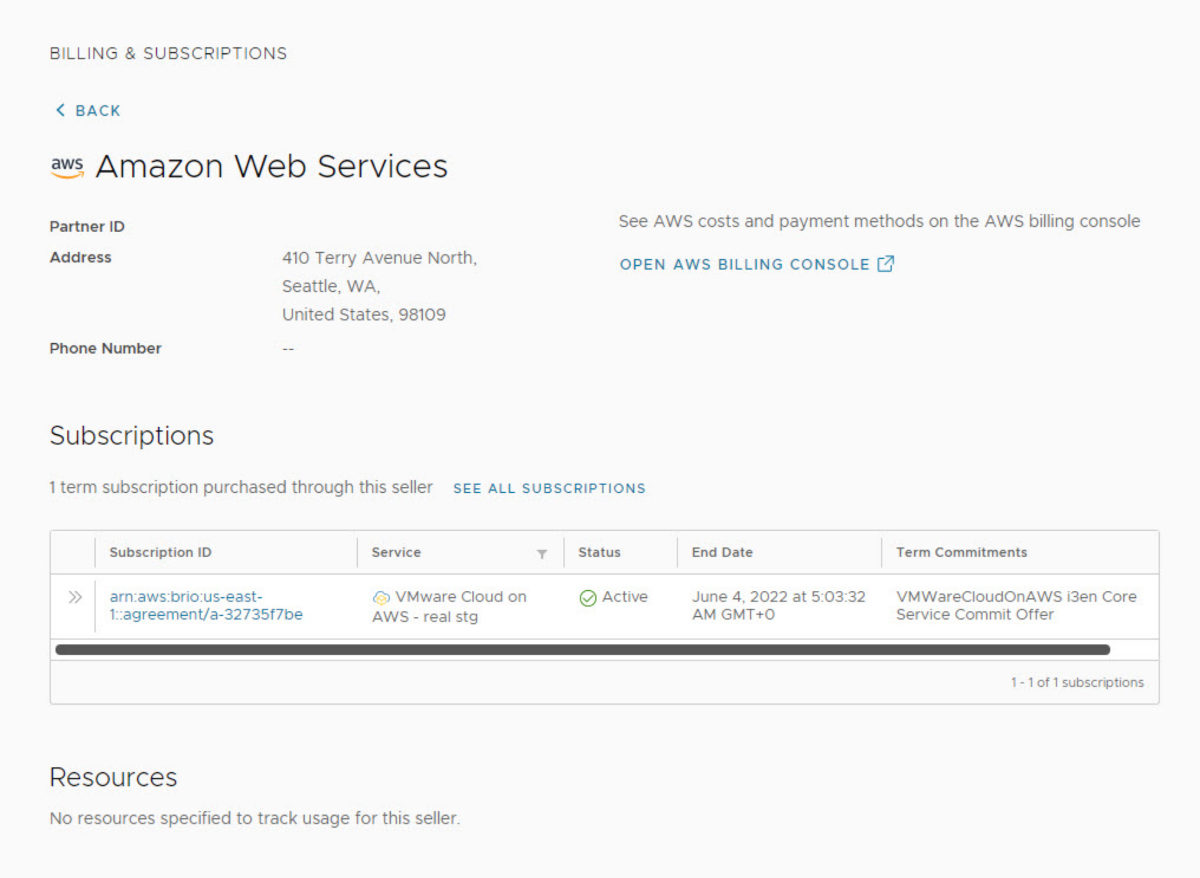
total this billing period: Aug 3 – Sep 2

AUG 3 TODAY: $80,200.00 SEP 2

| | |
|---|---|
| VMware Cloud on AWS | $79,200.00 |
| Network Insight | $2,000.00 |
| Promotional Credits (Estimated) | -$1,000.00 |
| Total | $80,200.00 |

2 To view the services and subscriptions purchased from any VMware partner seller in your Organization, click the **Seller Details** link in its respective tile.

The seller's details page opens.



BILLING & SUBSCRIPTIONS

< BACK

aws Amazon Web Services

Partner ID

Address 410 Terry Avenue North,
Seattle, WA,
United States, 98109

Phone Number --

See AWS costs and payment methods on the AWS billing console

OPEN AWS BILLING CONSOLE

Subscriptions

1 term subscription purchased through this seller SEE ALL SUBSCRIPTIONS

| | Subscription ID | Service | Status | End Date | Term Commitments |
|---|---|---|---|---|---|
| » | arn:aws:brio:us-east-1::agreement/a-32735f7be | VMware Cloud on AWS - real stg | ✓ Active | June 4, 2022 at 5:03:32 AM GMT+0 | VMWareCloudOnAWS i3en Core Service Commit Offer |

1 - 1 of 1 subscriptions

Resources

No resources specified to track usage for this seller.

3 To view costs and payment methods associated with this seller, click the link to its billing console.

4 To view the details for a subscription purchased from this seller, click the **Subscription ID** link.

This opens the subscription details page where you view additional details, such as term commitments, subscription start and end dates, payment method, subscription history, etc.

### What to do next

If you don't have VMware as a seller in your Organization, learn How do I add VMware as a seller so that you can purchase cloud services directly.

## How do I register my partner seller contract code with VMware Cloud Services

When you purchase a subscription through a non-VMware partner seller, your order might contain discounts. As an **Organization Owner** user, you must register the contract code provided by your partner seller with Cloud Services Console after the service is onboarded in your Organization.

By associating the contract code with the seller profile in VMware Cloud Services, you ensure that the discounts from your order will be reflected in your bill.

### Prerequisites

- You have an **Organization Owner** role in the Organization.

- You have the contract number for the subscription purchased through the partner seller.
- You have onboarded the service and the seller is in the Organization.

### Procedure

1 Log in to Cloud Services Console and select **Billing and Subscriptions > Overview**.

The **Sellers** section of the page lists the sellers from which your Organization has purchased services.

2 Click the **Add Contract** link in the seller details tile or page.

3 In the pop-up window that opens, type the contract number, then click **Submit**

### Results

The contract code is now associated with your Organization and all related discounts are applied.

You also gain the ability to independently create subscriptions for the related service.

## How do I add VMware as a seller

If your Organization purchased VMware Cloud services from a non-VMware seller, you can add VMware when onboarding with the service, or later. This way you can purchase VMware Cloud services directly from VMware along with your existing seller.

Adding VMware as a seller to your Organization means you have to create a billing account with VMware and complete the profile for your Organization. You create the billing account by adding a business address for your Organization and preferred payment method.

### Prerequisites

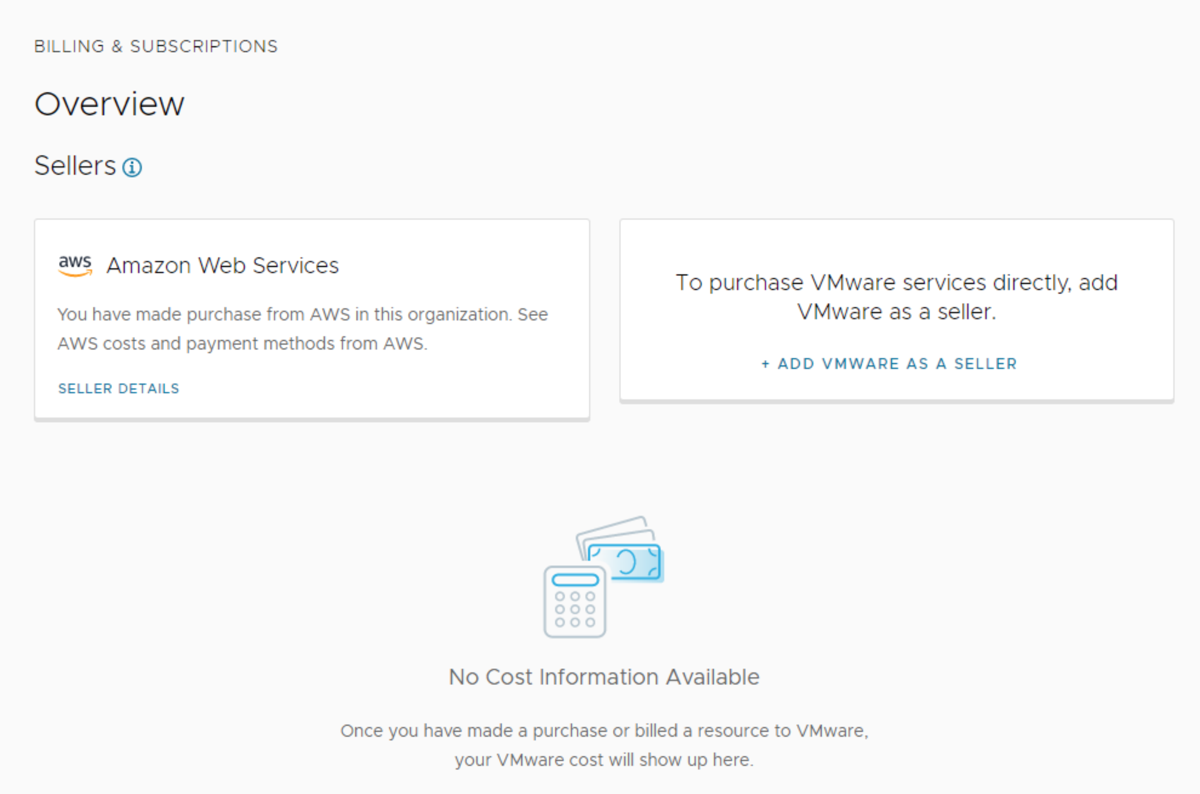
To add VMware as a seller in Cloud Services Console, you must have an **Organization Owner** role and your Organization must have purchased services from a non-VMware seller.

### Procedure

1 Log in to Cloud Services Console with your My VMware account.

2 Go to **Billing & Subscriptions > Overview**.

The **Sellers** section displays the non-VMware sellers in your Organization.



BILLING & SUBSCRIPTIONS

Overview

Sellers ⓘ

aws Amazon Web Services

You have made purchase from AWS in this organization. See AWS costs and payment methods from AWS.

SELLER DETAILS

To purchase VMware services directly, add VMware as a seller.

+ ADD VMWARE AS A SELLER

No Cost Information Available

Once you have made a purchase or billed a resource to VMware, your VMware cost will show up here.

3 Click the **Add VMware as a Seller** link.

4 Complete your Organization's profile by entering a billing address and selecting the currency and payment method.

> **Note** To change the currency of the Organization after you create the billing account, you must file a support ticket.

5 Review and agree to the **Terms of Service**.

6 Click **Complete**.

### Results

VMware is now added as a seller in your Organization.

## How do I manage the payment methods for my Organization

Your billing account determines the payment methods available to your Organization. You may use funds, credit cards or link an unrestricted Pay by Invoice account.

### Funds

To use one of your VMware funds to cover your Organization's costs, you link them to your Organization, and set one of them as your default payment method. In this way, you can use the same fund across all your Organizations. You can use any fund if it is within the VMware Entitlement account associated with VMware Cloud services, and in the same currency that is used by the Organization. For more information, see How to pay with funds.

### Credit cards

You can use a credit card to pay for your services unless there are no limitations to credit card use for your country. For more information, see What are the limitations for using credit cards as a payment method.

If the payment currency of your Organization is different than the card currency, you might incur foreign transaction fees from your credit card provider. For more information, see How to pay by credit card.

### Pay by Invoice Account

If a sales order for a new service is associated with a Pay by Invoice (PBI) account, it appears as a payment method during service onboarding. In this case, the PBI payment method is restricted and can be applied only to the subscriptions included in the sales order but cannot be added as a default payment method to the Organization.

If you want to use a PBI account as the default payment method to cover any purchases, resources and overages accrued by your Organization, you must activate unrestricted PBI for payment authorization for all services in your Organization. Enabling unrestricted PBI involves an offline approval process that you initiate by submitting a support request. For more information, see How to pay by invoice.

You can add as many payment methods to your Organization as you like, but only one of them can be set as a default payment method.

## How do I add a new payment method

As an **Organization Owner** user, you can add new payment methods to your Organization. The payment methods defined at the Organization's level become available to all **Organization Owner** users.

### Procedure

1 Open Cloud Services Console and navigate to **Billing & Subscriptions > Manage Payment Methods**.

2 In the **Other Payment Methods** area of the page, click **Add Payment Method**.

3 Select the type of payment method you want to add.

| To | Do this |
|---|---|
| **Link Pay by Invoice Accounts** | Select one or more of the available Pay by Invoice accounts that you want to add and click **Link Accounts**.<br>**Note** You can only add unrestricted PBI accounts as payment methods at the Organization level. If the PBI account you want to add is restricted, you must first activate unrestricted PBI by filing a support ticket. |
| **Link VMware funds** | Select the VMware fund that you want to add as a payment method, then click **Link Funds**. |
| **Add a Credit Card** | Add the credit card details and click **Add Card**.<br>**Note** By clicking **Add Card and Make Default**, you will change the default payment method for the Organization and this will affect all services and subscriptions that use the default payment method. |

# What is default payment method

When you sign up for VMware Cloud services, you add the payment method that you want to use to cover your Organization's costs. This payment method becomes the default payment method for your Organization and can be used by all **Organization Owner** users within the Organization.

The default payment method will apply to all your purchases, resources and overages in your Organization unless you specify a different payment method for your purchase. You can add new payment methods or change the default payment method for your Organization from the **Billing and Subscription > Manage Payment Methods** tab in the Cloud Services Console.

You may add funds, credit cards or link an unrestricted Pay by Invoice account as payment methods in your Organization, but only one of them can be set as default payment method.

When you set up your Organization, the address of the Organization determines the currency in which you pay for the Organization's services. For more information about payment methods and currency, see How is my payment currency determined.

When you subscribe to additional services, purchase add-ons, and apply commitments to your Organization, your sales order can determine a different payment method for the subscription or term commitment which applies only to that specific purchase. You may later change the payment method for a subscription. For more information, see How do I change my subscription payment method.

## How do I change my Organization's default payment method

As an **Organization Owner** user, you can change the default payment method for your Organization.

All payment methods available for your Organization are listed in the **Other Payment Methods** section of the **Manage Payment Methods** page in the Cloud Services Console. If you want to change the default payment method for your Organization to a new payment method that is not listed, you must first add the payment method.

#### Procedure

1. Open Cloud Services Console and navigate to **Billing & Subscriptions > Manage Payment Methods**.
2. In the **Default Payment Method** area of the page, click Change Default Payment Method.
3. From the list of available payment methods that displays, select the payment method that you want to use.
4. Click **Confirm**.

   The new default payment method is applied immediately.

## How do I change my subscription payment method

When you onboard a new service in your Organization or add a new subscription to an existing service, you can select the default payment method or add a different payment method for the new subscription. You can later change the payment method for any subscription in your Organization.

Changing the payment method for a current subscription does not affect the default payment method for the Organization. The default payment method will still apply to other purchases and resources that are using it. The newly defined payment method will be used to pay only for the costs of the current subscription until changed by an **Organization Owner** user.

#### Procedure

1. Open Cloud Services Console and go to **Billing & Subscriptions > Subscriptions**.
2. From the list of subscriptions in your Organization, click the **Subscription ID** link of the one you want to change.

   The **Subscription Details** page opens.
3. In the **Payment Method** area of the page, click **Change**.
4. From the list of available payment methods in your Organization, select the new payment method for the subscription.
5. Click **Confirm**.

#### Results

The subscription's details page refreshes to display the new payment method you selected.

## How to pay by invoice

As an **Organization Owner** user, you can change the default payment method for your Organization to Pay by Invoice (PBI) if unrestricted PBI is activated. Enabling unrestricted PBI involves an offline approval process that you initiate by submitting a support request.

Once activated, PBI can be applied as the default payment method for all services and subscriptions across the Organization. You can also apply unrestricted PBI as a payment method for current subscriptions.

### Procedure

1. On the Cloud Services Console, select **Support Center** and click **Create Support Request**.
2. In the **Category** text box, select **VMware Cloud Services - Billing and Usage**.
3. In the **Subject** text box, enter **`Activate Unrestricted PBI`**.
4. Enter the support request details, and click **Create Support Request**.

   A VMware Cloud services representative will contact you about your request. When unrestricted PBI is activated, you will receive a notification.

## How to pay by credit card

VMware Cloud services support payment with various credit cards. You can use your personal or corporate Mastercard, Visa, American Express, Discover, JCB, Diners Club credit cards. You can also use a Mastercard, Visa, or American Express debit card.

If you want to use a credit card to pay for your services:

- Your credit card limit and your payment processor determine the size of your transactions. The maximum amount you can spend in a single transaction is $25,000. For more information about your credit limit, you should contact your issuing bank.
- The address of your Organization determines the currency in which you are charged. For a list of countries and their relevant currencies, see How is my payment currency determined.
- There are certain What are the limitations for using credit cards as a payment method to the use of credit cards based on the address of your Organization and the billing address of your credit card.

  **Important** If your Organization's billing address is in a country that is a member of the European Economic Area (EEA) or a cooperating country, your credit card payments are impacted by the European Union's Second Payment Service Directive (2015/2366 PSD2). PSD2 requires Strong Customer Authentication (SCA) for electronic transactions through a two-factor authentication. When required, the SCA prompt will appear during the checkout flow requesting you to provide additional security information that will then be verified by your bank or card issuer.

- When you add a credit card as a payment method, we don't charge your card, but we do check that it is valid. A validity check might include a pre-authorization request by your banking institution. You might see a pending authorization request of $1.00 or equivalent on your statement. The pre-authorization is not a charge, and no funds are debited from your account.

You can add a credit card as a payment method when you onboard a cloud service, or later by selecting **Billing and Subscriptions > Manage Payment Methods** in the Cloud Services Console.

See How do I change my Organization's default payment method for more information.

## What are the limitations for using credit cards as a payment method

Due to risk and fraud considerations, certain limitations to the use of credit cards as a payment method can apply. These are based on the address of your Organization or the billing address of your credit card.

### List of Countries Where Limitations for Using Credit Cards Apply

If your country falls under a limitation for using credit cards, the payment method will be deactivated in VMware Cloud Services.

| You cannot use a credit card as a payment method if... | |
|---|---|
| | |
| The address of your Organization is in one of these countries: | Afghanistan, Netherlands Antilles, Angola, Bosnia and Herzegovina, Bangladesh, Burkina Faso, Bahrain, Brazil, Belarus, The Democratic Republic of Congo, Cameroon, China, Cuba, Cape Verde, Cyprus, Eritrea, Falkland Islands, French Guiana, Guadeloupe, Guam, Haiti, Isle of Man, Iraq, Iran, Korea, Kuwait, Lao, Mongolia, Mali, Martinique, Montserrat, Mexico, Nigeria, Nepal, Occupied Palestinian Territory, Sudan, Senegal, Syria, Turkmenistan, East Timor, Ukraine, Vatican City State, Venezuela, Mayotte, Zimbabwe. |
| The billing address of the credit card is in one of these countries: | Afghanistan, Netherlands Antilles, Angola, Antarctica, Aland Islands, Bosnia and Herzegovina, Bangladesh, Burkina Faso, Bahrain, Saint Barthelemy, Bonaire, Sint Eustatius and Saba, Brazil, Bouvet Island, Belarus, Cocos, Democratic Republic of Congo, Central African Republic, Cameroon, China, Cuba, Cape Verde, Curacao, Christmas Islands, Cyprus, Western Sahara, Eritrea, Falkland Islands, French Guiana, Guadeloupe, South Georgia and the South Sandwich Islands, Guam, Hong Kong, Heard Island and McDonald Islands, Haiti, Isle of Man, India, British Indian Ocean Territory, Iraq, Kiribati, Korea, Kuwait, Lao,Lithuania, Luxembourg, Latvia, Saint Martin, Mali, Montserrat, Mexico, Malaysia, Norfolk, Island, Nigeria, Norway, Nepal, Nauru, Niue, Pitcairn, Occupied Palestinian Territory, Rwanda, Sudan, Sweden, Singapore, Svalbard and Jan Mayen, Senegal, Somalia, South Sudan, Sao Tome and Principe, Syria, Chad, French Southern Territory, Thailand, Tokelau, Turkmenistan, East Timor, Turkey, Tuvalu, United States Minor Outlaying Islands, Vatican City State, Venezuela, Mayotte, Zimbabwe |

## How to pay with promotional credits

If you have promotional credits for any of your VMware Cloud services, you can apply them to one of your Organizations, and redeem them against the Organization's monthly costs.

Promotional credits can be service-specific meaning that you can use them against the monthly costs of a specific service, a group of services, or apply them to all services. Make sure that you note the expiration date of the credit, and redeem it before it expires.

Promotional credits can be redeemed against any of the VMware Cloud services-supported currencies. Promotional credits are sometimes given when you onboard one of our services for the first time. These credits are redeemed for you as you onboard the service.

Procedure

1 On the Cloud Services Console, click **Billing & Subscriptions > Promotional Credits**.

  All promotional credits that can be applied in the Organization are displayed on the **Available Credits** tab.

2 To redeem a promotional credit, click the **Activate** link on its details tile.

  The credit is redeemed during the next billing period. You can check the balance of the promotional credit at any time by navigating to **Billing & Subscriptions > Promotional Credits > Activated Credits**.

## What do I need to know about VMware funds

VMware funds are a VMware-specific payment method that can be used to purchase services or products. Each fund is made of one or several deposits.

When you want to add "money" to your fund, you can work with Sales and purchase a new deposit. A deposit consists of “Credits” which is money you can spend on VMware services and products.

You view details and manage the settings of your linked funds through the Fund Management platform on VMware Connect portal which requires access permissions. For more information, see Overview of My Funds Page, Fund Details Page and Navigation.

To use VMware funds to pay for your cloud services and subscriptions, you must link each fund as a payment method to your VMware Cloud services Organization. Funds can be linked as a default payment method or a one time payment method for Organizations and subscriptions. They can also be used to pay outstanding invoices directly form Cloud Services Console. To cover your Organization's costs with linked funds, they must have a positive balance and enough "money" in them.

Note that to link a fund in Cloud Services Console:

- You must have an **Organization Owner** role in the Organization in which you want to link the fund.
- Only funds that are within your VMware Entitlement account can be associated with your VMware Cloud services Organization.
- The currency and the selling unit of the fund must match that of the Organization.

If a linked fund used as a default payment method in the Organization is depleted, expires or is orphaned, the fund must be replaced with another fund, known as a survivor fund, or with a different payment method. Orphan funds are empty fund groups that disrupt payment flows and must be replaced immediately.

To allow **Organization Owner** users to manage their funds in a timely manner, VMware Cloud Services sends email and in-app notifications about the status and changes to the funds in their Organization. For more information, see How do I manage VMware funds in VMware Cloud Services.

## How to pay with funds

As an **Organization Owner** user, you can use linked VMware funds to cover the costs for your services. In addition to using funds as the default payment method in your Organization, you can pay outstanding invoices directly from the Cloud Services Console.

| To... | Do this... |
|---|---|
| Set a linked VMware fund as the default payment method in your Organization. | See How do I change my Organization's default payment method |
| Set a linked VMware fund as payment method for an active subscription. | See How do I change my subscription payment method |
| Pay an outstanding overage or term commitment invoice. | 1 Log in to Cloud Services Console and navigate to **Billing and Subscriptions > Invoices and Statements > Invoices**.<br>2 Locate the unpaid invoice you want to pay and click the vertical ellipses icon ⋮ .<br>3 Click the **Pay Now** link.<br>4 In the pop-up window that opens, review the invoice details and select the fund you want to use for this payment.<br>**Note** The **Payment Method** drop-down shows only the funds that are linked to the Organization and have a positive balance.<br>5 Click **Pay Now**.<br>The payment is submitted and the **Invoices** page is refreshed, showing an `In Progress` status (⟳ In Progress) next to the invoice you paid for.<br>When the transaction is completed, you will receive an email notification. The transaction may complete instantaneously or take a few hours. The invoice balance will update only after the transaction is completed.<br>It is possible to make an additional payment while the first partial payment is in progress. The updated invoice will reflect both payments and an updated balance. |
| To view payment history for invoices paid with funds through the Cloud Services Console | 1 Go to **Billing and Subscriptions > Invoices and Statements > Invoices.**<br>2 Locate the invoice you want to check payments for, then click the vertical ellipses icon ⋮ .<br>3 Click the **Payment History** link.<br>The **Payment History** section shows payment method, status and amount paid for the selected invoice. |

## How do I manage VMware funds in VMware Cloud Services

As an **Organization Owner** user, you can link and unlink VMware funds as a payment method in your Organization in Cloud Services Console. Only funds linked to the Organization can be set as a default payment method or used to pay outstanding overage and term commitment invoices.

**Note** In Cloud Services Console, you manage only the linking of the funds to your Organization. You manage the actual funds through the VMware Connect portal which requires access permissions.

Notifications about the changes made for VMware funds in your Organization are automatically sent by email and in-app to all **Organization Owner** users and **Organization Member** users with **Billing Read-only** role in the Organization.

The following table describes how to work with the VMware funds payment method in your VMware Cloud Services Organization.

| To... | Do this... |
|---|---|
| To link a VMware fund as a payment method in your Organization. | You can use any fund if it is within the VMware Entitlement account associated with VMware Cloud services, and in the same currency that is used by the Organization.<br>1 Log in to the Cloud Services Console and navigate to **Billing and Subscriptions > Manage Payment Methods**.<br>2 In the **Other Payment Methods** section of the page, click **Add Payment Method**.<br>3 Select **Link VMware Funds** and click **Continue**.<br>4 From the list of available VMware funds that displays, select the fund you want to link as a payment method in your Organization.<br>**Note** This list will show only VMware funds linked to your VMware account.<br>5 Link the fund you selected:<br>■ To link the fund as the default payment method in the Organization, click **Link fund and make default**.<br>■ To link the fund and make it available as a payment method in the Organization, click **Link funds**. |
| To unlink a fund that is already linked as a payment method in your Organization. | The payment methods in your Organization are available to all **Organization Owner** users. If you want to remove an active fund from the Organization, do this:<br>1 Open the **Manage Payment Methods** page.<br>2 Click the horizontal ellipses icon (•••) next to the fund's name and select **Unlink fund** |

| To... | Do this... |
|---|---|
| To view details for a fund that is already linked as a payment method in your Organization. | 1 Go to **Billing and Subscriptions > Manage Payment Methods**.<br>2 Click the horizontal ellipses icon (⋯) next to the fund name and select **View Details on MyVMware**.<br>This opens the VMware Customer Connect website where you can view your fund's details after you login with your VMware account. |
| To manage an expired fund already linked as the default payment method in your Organization. | If you are using a fund as the default payment method in your Organization, you receive an email notification before the expiry date. For a fund that is pending expiration, you can take one of the following actions:<br>■ Change the default payment method for your Organization to another active fund that is linked in your Organization.<br>■ Change the default payment method to credit card or PBI.<br>■ If you have another active fund that is not linked in your Organization, you can link it to the Organization, and then set it as a default payment method. |
| To manage a depleted fund | If the fund you are using as a default payment method or for an invoice payment does not have enough "money" in it to cover the full invoice amount, the invoice will show up as partially paid. Another fund with enough "credits" or a different payment method must be used to cover the remaining cost. |
| To manage an orphaned fund linked as the default payment method in your Organization | A fund can become orphaned for one of the following reasons:<br>■ change of fund owner<br>■ fund merge<br>■ change of **Organization Owner**<br>■ **Organization Owner** is removed from being fund user<br>When that happens, VMware Cloud Services notifies the **Organization Owner** users of the fund that has become orphaned and replaces the orphaned fund with a survivor fund. An additional notification is sent to all **Organization Owner** users about the updated default payment method. If any further change to the payment is required, see How do I manage the payment methods for my Organization. |

# How do I work with VMware Cloud Services subscriptions and commitments

VMware Cloud services subscriptions allow you to save money by committing to buy a certain amount of capacity for a pre-defined period of one or three years, at a reduced or negotiated rate.

You can use VMware Cloud services on demand or by purchasing subscriptions for a period of 1 or 3 years. On demand service usage is billed at a higher rate while service subscriptions are billed at a discounted rate. You purchase subscriptions through the Subscription Purchase Program (SPP) or Pay by Invoice.

You can purchase and use multiple commitments for each service in the subscription. Start and end dates for each commitment term can vary. The purchase order outlines the capacity, term, and negotiated price of the commitment.

VMware Cloud Services bills you according to the terms laid out in the commitment for the service subscription.

Any extra usage not covered by the terms of the commitment is charged based on the on-demand pricing you agreed to when you signed up with your service.

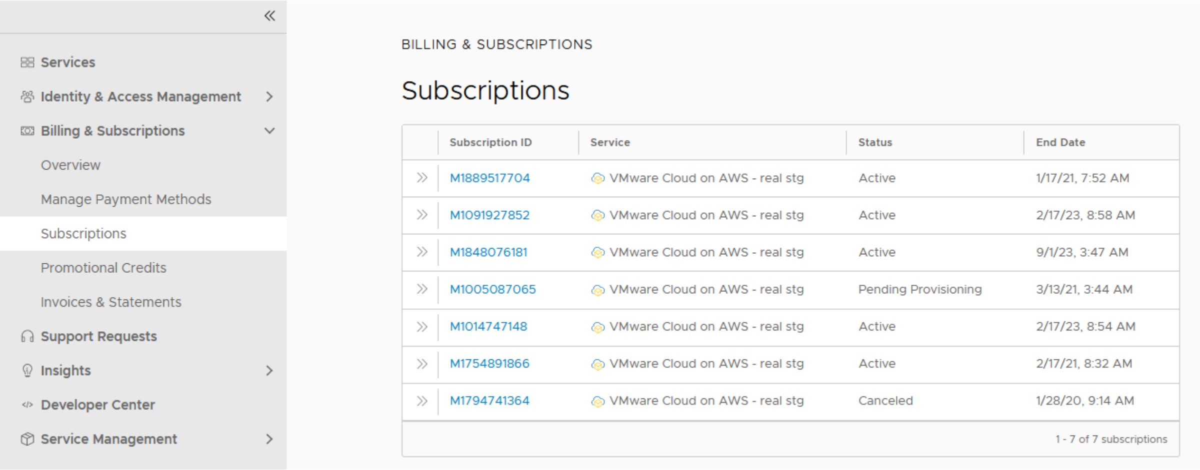
## How do I view subscription details for services in my Organization

To view subscriptions details in your Organization, you must have either an **Organization Owner** role or an **Organization Member** role with **Billing Read-only** permissions.

### Procedure

1 In Cloud Services Console, navigate to **Billing and Subscriptions > Subscriptions**.

   The table that opens provides information about all subscriptions in your Organization. It lists each subscription's ID, the VMware Cloud services for which it was purchased, and the term commitments that are included in the subscription.

   BILLING & SUBSCRIPTIONS

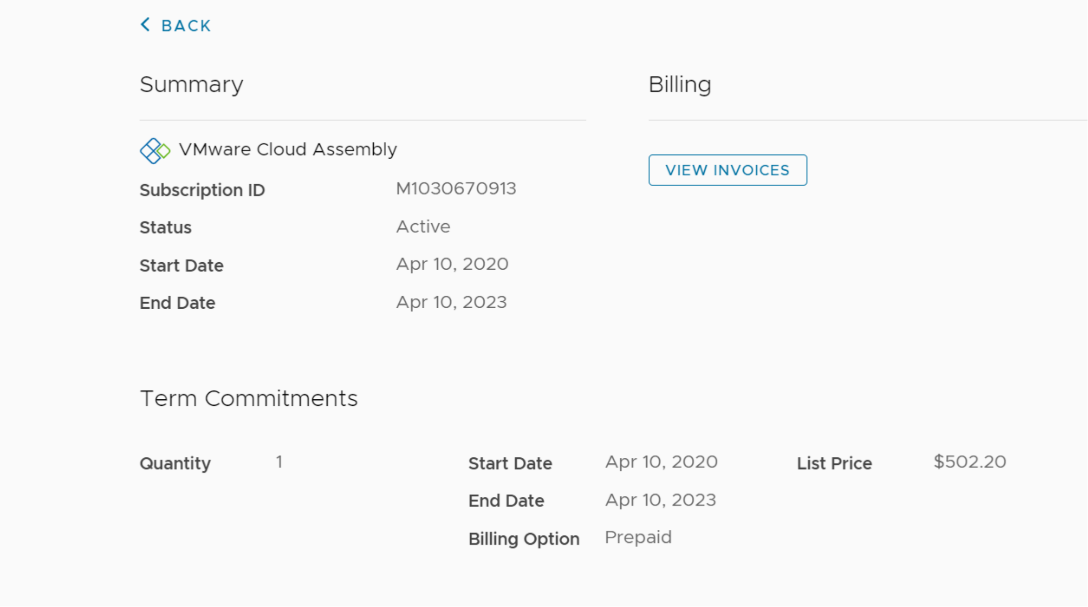
   Subscriptions

   | | Subscription ID | Service | Status | End Date |
   |---|---|---|---|---|
   | » | M1889517704 | VMware Cloud on AWS - real stg | Active | 1/17/21, 7:52 AM |
   | » | M1091927852 | VMware Cloud on AWS - real stg | Active | 2/17/23, 8:58 AM |
   | » | M1848076181 | VMware Cloud on AWS - real stg | Active | 9/1/23, 3:47 AM |
   | » | M1005087065 | VMware Cloud on AWS - real stg | Pending Provisioning | 3/13/21, 3:44 AM |
   | » | M1014747148 | VMware Cloud on AWS - real stg | Active | 2/17/23, 8:54 AM |
   | » | M1754891866 | VMware Cloud on AWS - real stg | Active | 2/17/21, 8:32 AM |
   | » | M1794741364 | VMware Cloud on AWS - real stg | Canceled | 1/28/20, 9:14 AM |

   1 - 7 of 7 subscriptions

2 To view more detailed information for a specific subscription, locate the subscription you want to view and click its **Subscription ID** link.

   The page that opens displays additional details about the subscription and the term commitments purchased with the subscription.



< BACK

Summary

VMware Cloud Assembly

| | |
|---|---|
| Subscription ID | M1030670913 |
| Status | Active |
| Start Date | Apr 10, 2020 |
| End Date | Apr 10, 2023 |

Billing

VIEW INVOICES

Term Commitments

| | | | | | |
|---|---|---|---|---|---|
| Quantity | 1 | Start Date | Apr 10, 2020 | List Price | $502.20 |
| | | End Date | Apr 10, 2023 | | |
| | | Billing Option | Prepaid | | |

3 (Optional) To view and download invoices, click **View Invoices** in the **Billing** section of the page.

## How to set up a commitment

If you are an **Organization Owner** user, contact your VMware sales representative to negotiate a quote and arrange payment for a commitment.

Once the purchase is complete, you will receive a notification email indicating that your commitment is active. For each commitment, you receive an email with a unique link.

1 To apply the commitment to one of your current Organizations or to a new Organization, click the link in the email.

2 Follow the steps in the service onboarding workflow.

For more information about commitments, see Why do I need to apply commitments to my Organization.

For more information about the onboarding workflows, see How do I onboard a paid cloud service purchased through VMware Sales.

## Why do I need to apply commitments to my Organization

You can purchase multiple subscriptions for different VMware Cloud Services as well as multiple term commitments for each subscription. Each subscription can be used in one Organization. If you have more than one VMware Cloud services Organizations, you can apply the newly purchased commitments to an Organization of your choice.

When you purchase a commitment, the sales offer outlines the capacity, term, and negotiated price. As an **Organization Owner** user, you apply the commitment to a new or existing Organization after the purchase is complete. You do so by opening the link for the new commitment and following the steps in the workflow.

Once associated with a specific Organization, the commitment can be used by the members of that Organization until its term expires.

## How do I change my subscription renewal preference

As an **Organization Owner** user, you manage renewals for your subscriptions from the **Subscription Details** page in Cloud Services Console.

Each subscription in your Organization has a default renewal preference that can be changed up to 30 days before the subscription expires.

| If your renewal preference is set to... | Then... |
|---|---|
| **Auto Renewal** | Your subscription will renew automatically with no additional input needed on your side. |
| **Manual Renewal** | An account manager will contact you prior to the renewal date to discuss the renewal details.<br>You can also submit a support request to inquire about renewal options. |

You can also cancel a subscription before it is renewed. In this case, your Organization loses entitlement to the subscription past its expiration date.

### Prerequisites

You must have an **Organization Owner** role.

### Procedure

1 Log in to the Cloud Services Console, then navigate to **Billing & Subscriptions > Subscriptions**.

2 From the list of subscriptions that displays, click the subscription's ID.

This opens the **Subscription Details** page.

3 In the **Renewal Preference** section, click **Change**.

4 Select a new default renewal preference for the subscription and click **Confirm**.

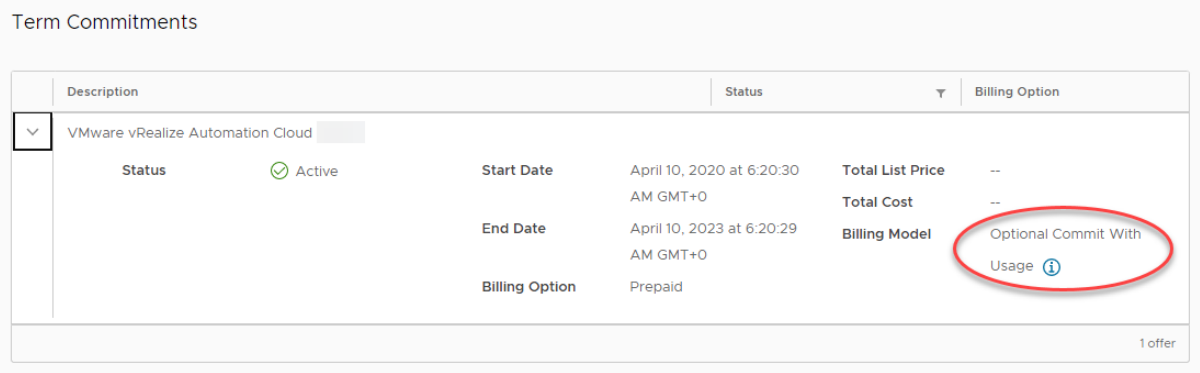
## What is a billing model

VMware Cloud Services utilizes three different billing models. The billing model for your subscription determines how your Organization is charged for the services and commitments purchased and used within the Organization.

Billing model information is displayed as part of the **Term Commitments** details for a subscription.

1 Log in to Cloud Services Console and go to **Billing & Subscriptions > Subscriptions**.

2 Click a subscription's ID to open its details page, then expand the **Term Commitments** section.



Term Commitments

| Description | Status | Billing Option |
|---|---|---|
| VMware vRealize Automation Cloud | | |

Status: Active

Start Date: April 10, 2020 at 6:20:30 AM GMT+0

End Date: April 10, 2023 at 6:20:29 AM GMT+0

Billing Option: Prepaid

Total List Price: --

Total Cost: --

Billing Model: Optional Commit With Usage ⓘ

1 offer

**Note** You can view the billing model only for subscriptions purchased through VMware.

The following table explains the differences between the three billing models.

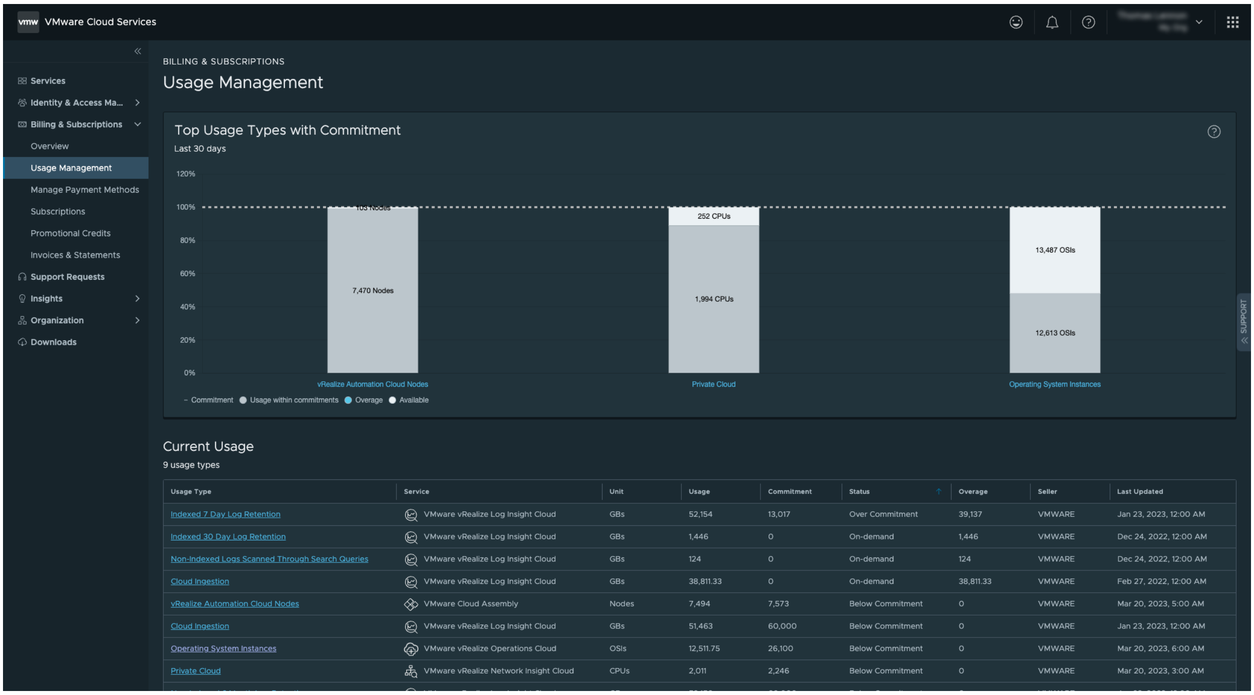
| | Commit only | Optional Commit with Usage | Mandatory Commit with Usage |
|---|---|---|---|
| Description: | You must purchase subscriptions to utilize the service. | You do not need subscriptions to start using the service, but you may incur on-demand usage. | You must purchase subscriptions to utilize the service and you may be charged for overage usage. |
| Default payment method: | Not required | Required | Not required |
| Cost detrmined by: | Commitments | Commitments + On-demand usage (if any) | Commitments + Overage usage (if any) |

## How do I work with the Usage Management dashboard

As an **Organization Owner** user, you can track how the services in your Organization are used over time and according to usage type through the **Usage Management** dashboard in the Cloud Services Console.

**Note** Usage management is not available for all VMware Cloud services. Some of the services that currently provide data about usage are VMware Cloud on AWS, VMware Aria Operations for Networks, VMware Aria Operations, VMware Aria Operations for Logs, VMware Aria Automation, VMware Cloud Disaster Recovery, VMware Cloud Director, VMware Lab Platform.

You access the **Usage Management** dashboard by navigating to **Billing & Subscriptions > Usage Management**.



BILLING & SUBSCRIPTIONS

Usage Management

Top Usage Types with Commitment

Last 30 days

Current Usage

9 usage types

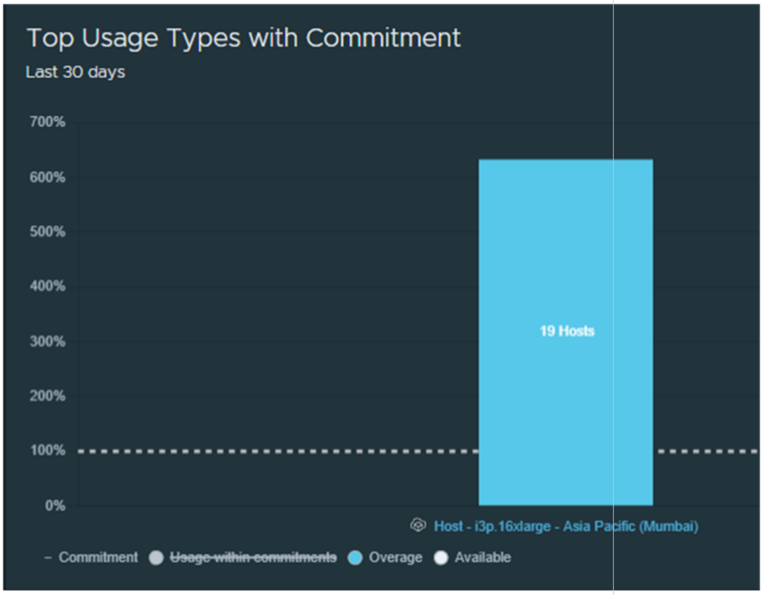
| Usage Type | Service | Unit | Usage | Commitment | Status | Overage | Seller | Last Updated |
|---|---|---|---|---|---|---|---|---|
| Indexed 7 Day Log Retention | VMware vRealize Log Insight Cloud | GBs | 52,154 | 13,017 | Over Commitment | 39,137 | VMWARE | Jan 23, 2023, 12:00 AM |
| Indexed 30 Day Log Retention | VMware vRealize Log Insight Cloud | GBs | 1,446 | 0 | On-demand | 1,446 | VMWARE | Dec 24, 2022, 12:00 AM |
| Non-Indexed Logs Scanned Through Search Queries | VMware vRealize Log Insight Cloud | GBs | 124 | 0 | On-demand | 124 | VMWARE | Dec 24, 2022, 12:00 AM |
| Cloud Ingestion | VMware vRealize Log Insight Cloud | GBs | 38,811.33 | 0 | On-demand | 38,811.33 | VMWARE | Feb 27, 2022, 12:00 AM |
| vRealize Automation Cloud Nodes | VMware Cloud Assembly | Nodes | 7,494 | 7,573 | Below Commitment | 0 | VMWARE | Mar 20, 2023, 5:00 AM |
| Cloud Ingestion | VMware vRealize Log Insight Cloud | GBs | 51,463 | 60,000 | Below Commitment | 0 | VMWARE | Jan 23, 2023, 12:00 AM |
| Operating System Instances | VMware vRealize Operations Cloud | OSIs | 12,511.75 | 26,100 | Below Commitment | 0 | VMWARE | Mar 20, 2023, 6:00 AM |
| Private Cloud | VMware vRealize Network Insight Cloud | CPUs | 2,011 | 2,246 | Below Commitment | 0 | VMWARE | Mar 20, 2023, 3:00 AM |

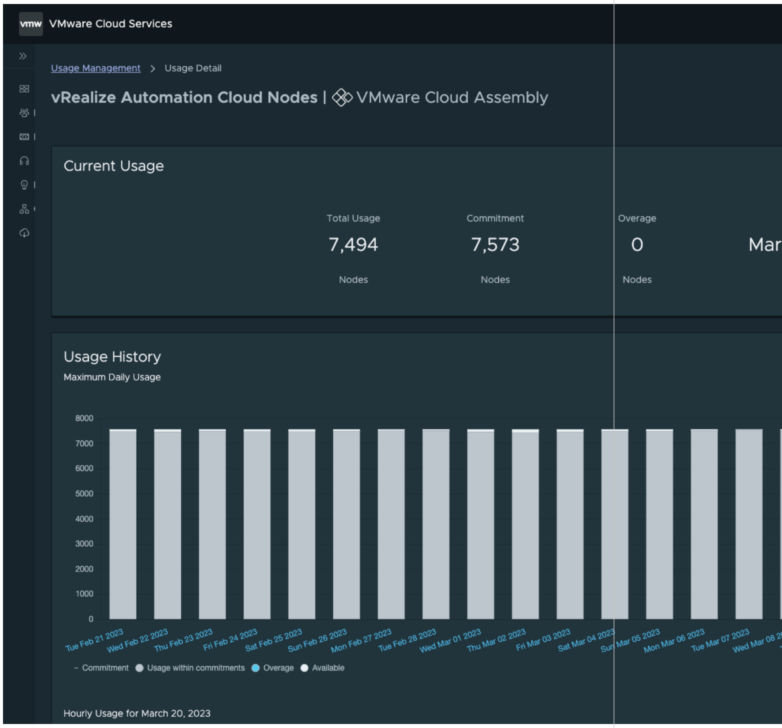
The usage data is organized in two sections: a chart shwoing the top usage types in the Organization for the past 30 days, and a table showing details about the current usage for all usage types in the Organization.

VMware Cloud services use many usage types. The usage type is based on the specific service provisioned in your Organization and includes the units used to measure the committed capacity for the service. The most common units used are Cores, Hosts, vCPUs, CPUs and OSIs. Here are a few examples of usage types:

- `Operating System Instances`
- `Cloud Director Cores`
- `Host - r.5metal - Europe (Ireland)`

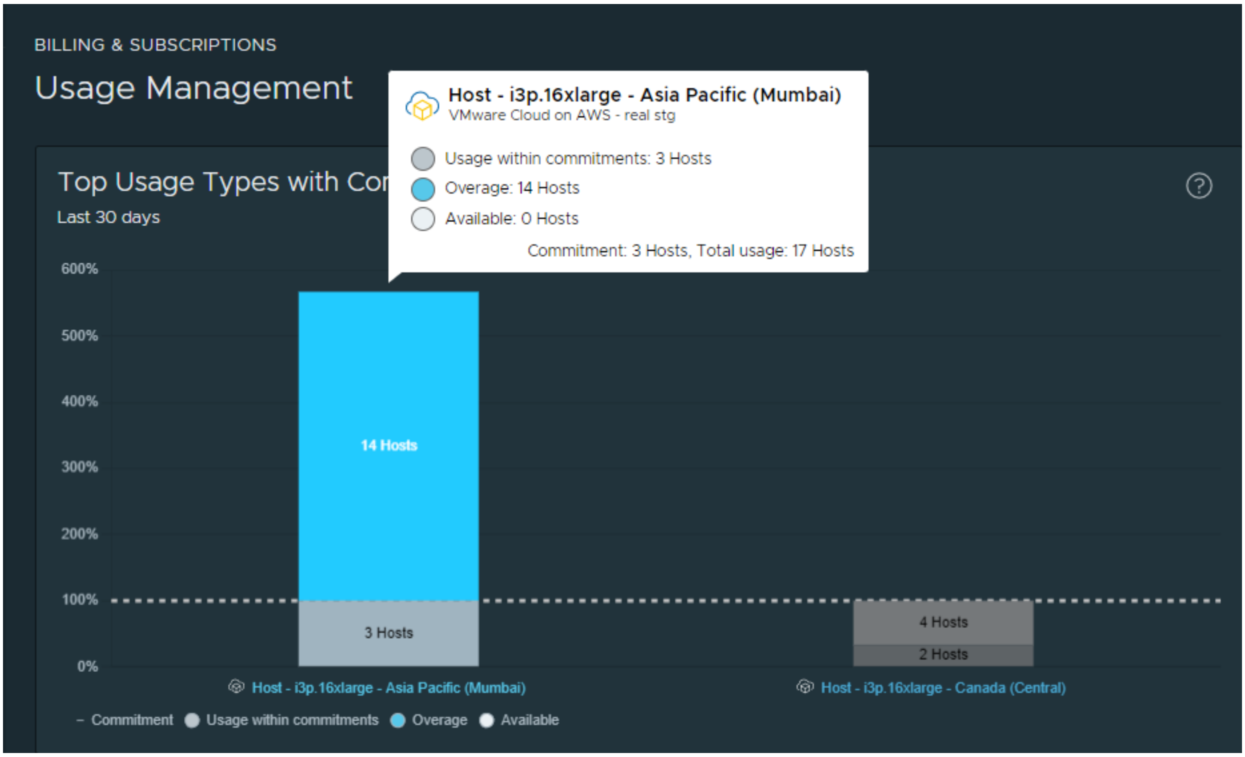
| To... | Do this... |
|---|---|
| Learn more about working with the top usage types. | See What do I need to know about the Top Usage Types with Commitment Chart. |
| To learn more about working with current usage. | See What do I need to know about the Current Usage table. |

| To… | Do this… |
|---|---|
| To filter usage based on capacity, such as usage with commitments, overage or available commitment. | In the **Top Usage Types with Commitment** section of the **Usage Management** dashboard, click the label under the chart that corresponds to the information you want to exclude from the view.<br>For example, if you want to view only the overage for the top usage types, click the **Usage with commitments** label. As the label gets crossed out, the view refreshes to display only the usage types that are in overage.<br><br> Top Usage Types with Commitment<br>Last 30 days<br>700%<br>600%<br>500%<br>400%<br>300%<br>200%<br>100%<br>0%<br>19 Hosts<br>Host - i3p.16xlarge - Asia Pacific (Mumbai)<br>– Commitment<br>~~Usage within commitments~~<br>Overage<br>Available |
| To view current and historical usage per usage type | Click the usage type link for which you want to vew current and historical usage details. If the usage type is in the **Top Usage Types with Commitment** section, the link is just below the respective bar on the graph. If the usage type is listed in the **Current Usage** section, you will find the link in in the Usage Type column.<br>A page opens, showing the current and historical usage view for the selected usage type. |

| To... | Do this... |
|---|---|
|  | <br>VMware Cloud Services<br>Usage Management > Usage Detail<br>vRealize Automation Cloud Nodes \| VMware Cloud Assembly<br>Current Usage<br>Total Usage 7,494 Nodes<br>Commitment 7,573 Nodes<br>Overage 0 Nodes<br>Mar<br>Usage History<br>Maximum Daily Usage<br> 8000<br>7000<br>6000<br>5000<br>4000<br>3000<br>2000<br>1000<br>0<br>Tue Feb 21 2023<br>Wed Feb 22 2023<br>Thu Feb 23 2023<br>Fri Feb 24 2023<br>Sat Feb 25 2023<br>Sun Feb 26 2023<br>Mon Feb 27 2023<br>Tue Feb 28 2023<br>Wed Mar 01 2023<br>Thu Mar 02 2023<br>Fri Mar 03 2023<br>Sat Mar 04 2023<br>Sun Mar 05 2023<br>Mon Mar 06 2023<br>Tue Mar 07 2023<br>Wed Mar 08 2<br>Commitment<br>Usage within commitments<br>Overage<br>Available<br>Hourly Usage for March 20, 2023<br>To learn more about current and historical usage, see What do I need to know about current and historical usage details. |

## What do I need to know about the Top Usage Types with Commitment Chart

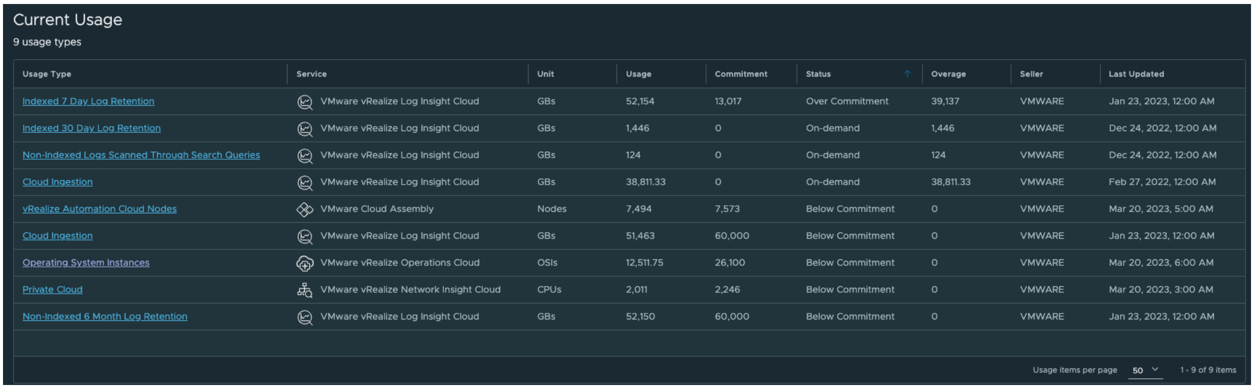
The **Top Usage Types with Commitment** chart of the **Usage Management** dashboard shows a summary of the high-water mark of usage for the top usage types within your Organization in the past 30 days, sorted by percentage of commitment.



Commitment is the number of units purchased in your Organization through subscription. The dotted horizontal line shows the 100% commitment level. Bars that are below this line indicate that you are under-utilizing for this service and usage type. The blue portions of the bars indicate that you have exceeded your commitment and can consider either reducing your usage or purchasing additional commitments. In the chart, the number of units by which your Organization's usage has exceeded the commitment, is shown as overage.

## What do I need to know about the Current Usage table

The **Current Usage** table is located below the main **Top Usage Types with Commitment** section of the **Usage Management** dashboard in the Cloud Services Console.



Current Usage

9 usage types

| Usage Type | Service | Unit | Usage | Commitment | Status | Overage | Seller | Last Updated |
|---|---|---|---|---|---|---|---|---|
| Indexed 7 Day Log Retention | VMware vRealize Log Insight Cloud | GBs | 52,154 | 13,017 | Over Commitment | 39,137 | VMWARE | Jan 23, 2023, 12:00 AM |
| Indexed 30 Day Log Retention | VMware vRealize Log Insight Cloud | GBs | 1,446 | 0 | On-demand | 1,446 | VMWARE | Dec 24, 2022, 12:00 AM |
| Non-Indexed Logs Scanned Through Search Queries | VMware vRealize Log Insight Cloud | GBs | 124 | 0 | On-demand | 124 | VMWARE | Dec 24, 2022, 12:00 AM |
| Cloud Ingestion | VMware vRealize Log Insight Cloud | GBs | 38,811.33 | 0 | On-demand | 38,811.33 | VMWARE | Feb 27, 2022, 12:00 AM |
| vRealize Automation Cloud Nodes | VMware Cloud Assembly | Nodes | 7,494 | 7,573 | Below Commitment | 0 | VMWARE | Mar 20, 2023, 5:00 AM |
| Cloud Ingestion | VMware vRealize Log Insight Cloud | GBs | 51,463 | 60,000 | Below Commitment | 0 | VMWARE | Jan 23, 2023, 12:00 AM |
| Operating System Instances | VMware vRealize Operations Cloud | OSIs | 12,511.75 | 26,100 | Below Commitment | 0 | VMWARE | Mar 20, 2023, 6:00 AM |
| Private Cloud | VMware vRealize Network Insight Cloud | CPUs | 2,011 | 2,246 | Below Commitment | 0 | VMWARE | Mar 20, 2023, 3:00 AM |
| Non-Indexed 6 Month Log Retention | VMware vRealize Log Insight Cloud | GBs | 52,150 | 60,000 | Below Commitment | 0 | VMWARE | Jan 23, 2023, 12:00 AM |

Usage items per page 50 1 - 9 of 9 items

The table provides high level usage details about usage types of services provisioned in your Organizations. Here's a detailed explanation about the information you can find in each table column:

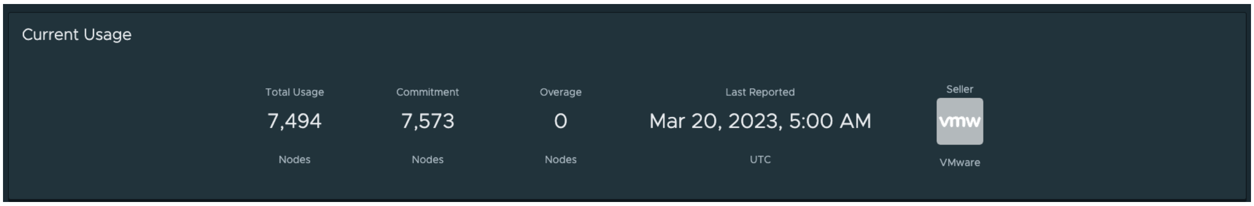
| Column | Description |
|---|---|
| Usage Type | Usage against a specific service provisioned in the Organization and the units used to measure the committed capacity for that service. For example, `Host - r5.metal - US West Oregon`.<br>Usage type is displayed as a link. Clicking on the link opens a details page showing current and historical usage for the selected usage type. |
| Service | The cloud services that specific usage type is tied to. For example, VMware Cloud on AWS. |
| Unit | Represents the measurement unit for the specific usage type. For example, Hosts, Cores, GB (storage), IP/EIPs, CPUs/vCPUs, etc. |
| Usage | Represents actual usage being used at the time of the report: the number of units currenlty in use. |
| Commitment | The number of units purchased through subscriptions in the Organization. |
| Status | Represents a summary of the state of the usage. The options are:<br>■ Over commitment: when your usage exceeds your commitment.<br>■ On-demand: when you have usage for a usage type with no commitment.<br>■ At or below commitment: some services to not have data when usage is at or below commitment. This status indicates you are not consuming more than you purchased. It does not show the specific quantity being used. |
| Overage | Represents how much the usage exceeds the commitment. |
| Seller | Represents the seller you purchased the subscription from. Can show overconsumption that may be billed for the usage. |
| Last Updated | Represents the timestamp of when the data was last fetched. |

## What do I need to know about current and historical usage details

For each usage type shown in the **Usage Management** dashboard in your Organization, you can view current and historical usage details. To open the details, click the usage type link.

### Current Usage

The **Current Usage** dashboard shows a high level view of some basic details.



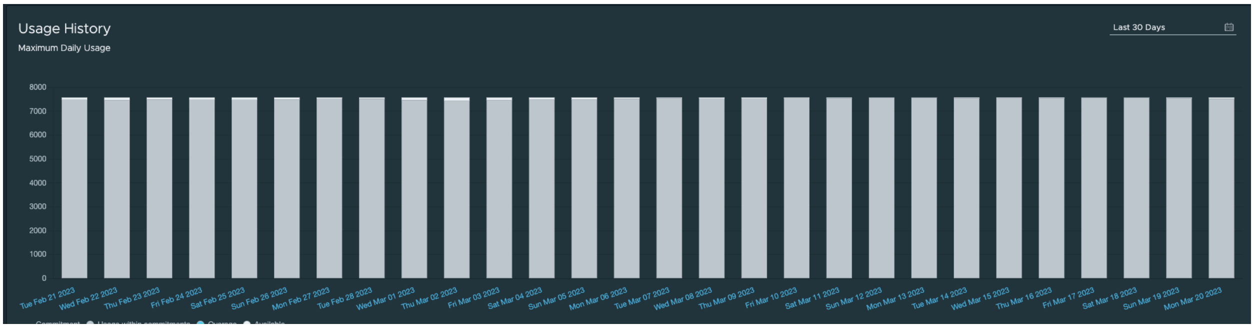
Current Usage

| Total Usage | Commitment | Overage | Last Reported | Seller |
|---|---|---|---|---|
| 7,494 | 7,573 | 0 | Mar 20, 2023, 5:00 AM | vmw |
| Nodes | Nodes | Nodes | UTC | VMware |

- **Total Usage** shows the units of total usage and usage metric type. For example, `7,494 Nodes`.
- **Commitment** shows the units committed for usage for the specific service subscription. For example, `7,573 Nodes`.
- **Overage** shows if actual usage exceeds the committed usage, the difference is reflected by a units value.
- **Last Reported** shows the timestamp when current usage type details were last updated.
- **Seller** represents the seller of the subscription's usage type.

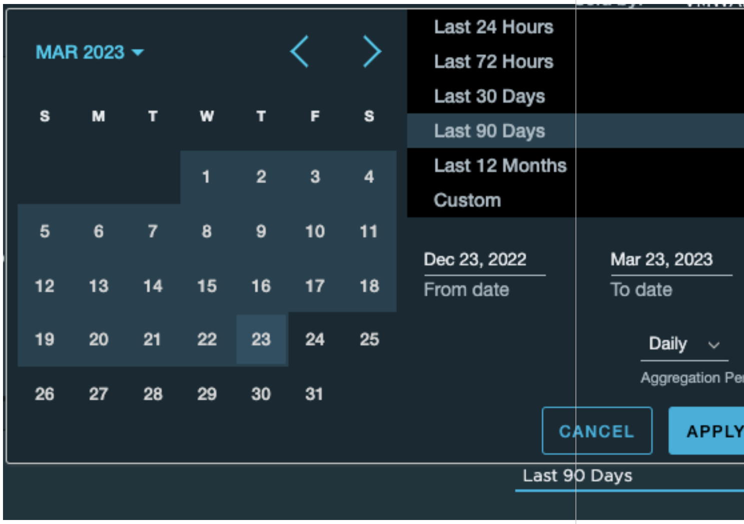
## Usage History

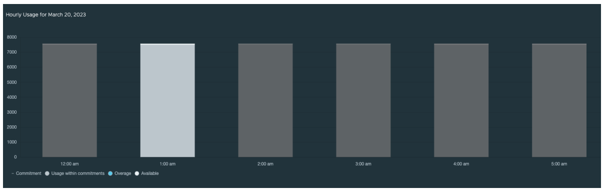
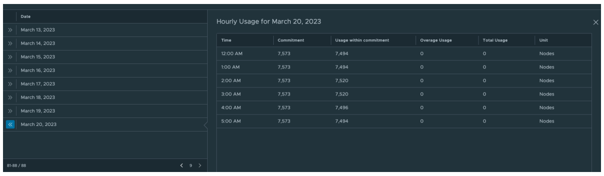
The **Usage History** view shows the maximum daily usage over a pre-defined period of time and hourly usage for a specific date.



- The vertical axis in the **Maximum Daily Usage** view represents the usage metric and amount of units.
- The horizontal axis represents the timeframe of the data displayed on the chart.

## How to work with the current and historical usage view

| To... | Do this... |
|---|---|
| View more detailed information about usage. | Hover your mouse over a chart bar. You can see:<br>■ The time stamp for the chart.<br>■ Usage within commitments: the number of units available through commitments that were being used at that time.<br>■ Overage: the number of units resulting in overage at that time, the percentage result of overage.<br>■ Available: The number of units available to use at that time. |
| Modify the **Maximum Daily Usage** chart time period. | 1 Click the Calendar icon in the top right corner of the **Maximum Daily Usage** chart.<br>The default time period for this view is 30 days. The minimum time period for which you can filter maximum daily usage data is 24 hours. The maximum time period is 2 years.<br><br> MAR 2023<br>S M T W T F S<br>1 2 3 4<br>5 6 7 8 9 10 11<br>12 13 14 15 16 17 18<br>19 20 21 22 23 24 25<br>26 27 28 29 30 31<br>Last 24 Hours<br>Last 72 Hours<br>Last 30 Days<br>Last 90 Days<br>Last 12 Months<br>Custom<br>CANCEL<br>APPLY<br>Dec 23, 2022 From date<br>Mar 23, 2023 To date<br>Daily Aggregation Pe<br>Last 90 Days<br>2 Change the time period settings and click **Apply**. |

<table>
<tr><th>To...</th><th>Do this...</th></tr>
<tr><td>View the <b>Hourly Usage</b> chart for a specific date.</td><td>Click on any date bar in the <b>Maximum Daily Usage</b> chart. The <b>Hourly Usage</b> chart refreshes to show an hourly breakdown of usage for the selected day.<br>

<br>
<b>Note</b> Hourly usage data is only available for the past 30 days.</td></tr>
<tr><td>View hourly usage in a table format.</td><td>You can see a breakdown of the hourly usage in the table just below the <b>Hourly Usage</b> chart.<br>

<table>
<tr><th>Date</th></tr>
<tr><td>March 13, 2023</td></tr>
<tr><td>March 14, 2023</td></tr>
<tr><td>March 15, 2023</td></tr>
<tr><td>March 16, 2023</td></tr>
<tr><td>March 17, 2023</td></tr>
<tr><td>March 18, 2023</td></tr>
<tr><td>March 19, 2023</td></tr>
<tr><td>March 20, 2023</td></tr>
</table>
81-88 / 88 ‹ 9 ›<br>
Hourly Usage for March 20, 2023
<table>
<tr><th>Time</th><th>Commitment</th><th>Usage within commitment</th><th>Overage Usage</th><th>Total Usage</th><th>Unit</th></tr>
<tr><td>12:00 AM</td><td>7,573</td><td>7,494</td><td>0</td><td>0</td><td>Nodes</td></tr>
<tr><td>1:00 AM</td><td>7,573</td><td>7,494</td><td>0</td><td>0</td><td>Nodes</td></tr>
<tr><td>2:00 AM</td><td>7,573</td><td>7,520</td><td>0</td><td>0</td><td>Nodes</td></tr>
<tr><td>3:00 AM</td><td>7,573</td><td>7,520</td><td>0</td><td>0</td><td>Nodes</td></tr>
<tr><td>4:00 AM</td><td>7,573</td><td>7,496</td><td>0</td><td>0</td><td>Nodes</td></tr>
<tr><td>5:00 AM</td><td>7,573</td><td>7,494</td><td>0</td><td>0</td><td>Nodes</td></tr>
</table>
Click the double arrow icon next to any date to get the expanded hourly usage view organized under the following columns:
<ul>
<li>Time: the specific time of day the data refers to.</li>
<li>Commitment : represents the quantity your Organization has committed to with a subscription.</li>
<li>Usage within commitment: represents the actual usage that is considered as part of your Organization's commitment.</li>
<li>Overage usage: represents the amount of usage that is outside your Organization's commitment and considered as overage.</li>
<li>Total usage: represents the overall usage combining whatever is within your Organization's commitment along with any overage.</li>
<li>Unit: the metic applicable for the selected usage type, ie hosts / IP / EIP / CPU / vCPU etc</li>
</ul></td></tr>
</table>

## Usage Management FAQ

This topic covers frequently asked questions (FAQs) about the **Usage Management** dashboard in Cloud Services Console.

### Q: Why is my purchase not showing in the Usage Management page?

A: All usage data is processed on a daily basis. Depending on when your service usage occurred, it may take up to 48 hours to show in this report. Note that some services provide data on a monthly basis.

## Q: Why is my usage delayed?

A: All usage data is processed on a daily basis. Depending on when your service usage occurred, it may take up to 48 hours to show in this report. Note that some services provide data on a monthly basis.

## Q: How do I find the cost information?

A: You can view the charges for your services by looking at your Activity Statements. For details, refer to How to read my activity statement.

## Q: I don’t see my usage data. Why?

A: Usage management is not available for all VMware Cloud services. Some of the services that currently provide data about usage are VMware Cloud on AWS, VMware Aria Operations for Networks, VMware Aria Operations, VMware Aria Operations for Logs, VMware Aria Automation, VMware Cloud Disaster Recovery, VMware Cloud Director, VMware Lab Platform. If your service is supported, depending on when your service usage occurred , it may take up to 48 hours to show in this report. Note that some services provide data on a monthly basis.

## Q: How far back can I view usage data for?

A: The default time period shown in the dashboard is 30 days. The minimum time period for which you can filter maximum daily usage data is 24 hours. The maximum time period is two years. Note that at any given time the chart displays data for a maximum of one year period.

## Q: I don’t see any hourly data. Why?

A: Hourly data is only available for the last 30 days. Beyond that, only daily data is available.

## My usage data does not reflect my bill. Why?

A: Most services bill based on the sum of hourly overage that occurred during your billing period. In this chart, you will see the actual usage for a given hour, and the maximum usage for a given day.

## Q: I don't see the Top Usage chart. Why?

A: The **Top Usage** chart only shows usage that occurred in the last 30 days for a service you have a commitment for. If there is no service with usage that qualifies, the chart will not be shown at all. There are a few reasons you may not see your usage:

- All of your usage is for an On Demand service. On Demand usage does not show in the Top Usage chart.
- Your usage is for a service that does not provide data about usage.
- Your usage occurred over 30 days in the past.

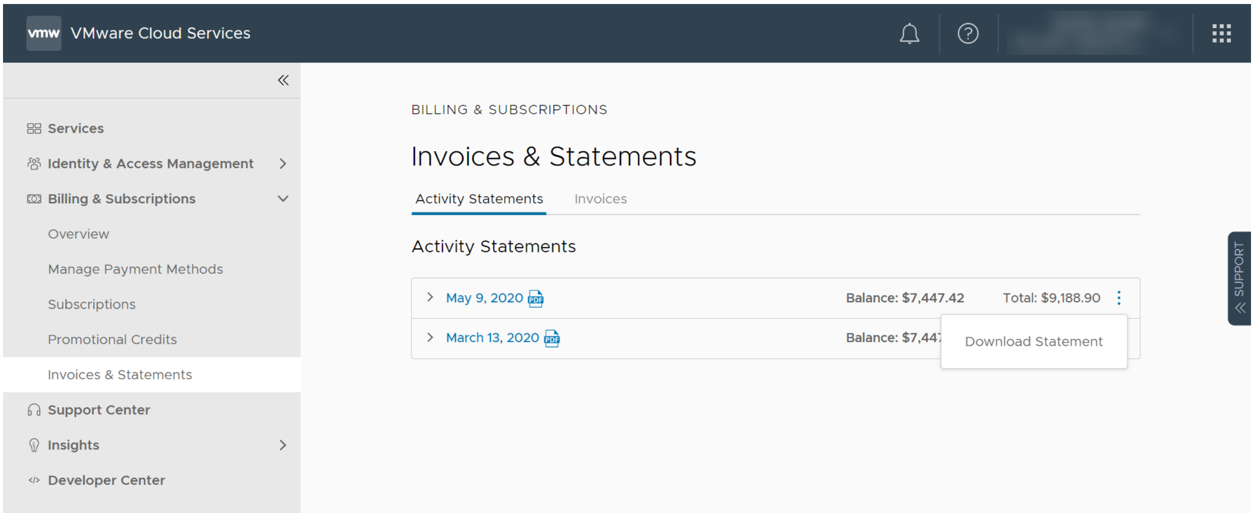
# How do I view statements and invoices

As an **Organization Owner** user, you can view and print the last 15 activity statements, on-demand invoices, and yearly commitment invoices.

View your statements and invoices by selecting **Billing & Subscriptions > Invoices and Statements** on the Cloud Services Console.

## Your Activity Statements

The **Activity Statements** page displays monthly summaries for all services consumed in a given billing period. Each activity statement provides a summary of payments made against charges, promotional credits, and balances. You view and download activity statements by clicking on its link, or by selecting an option from the vertical ellipsis icon next to it.



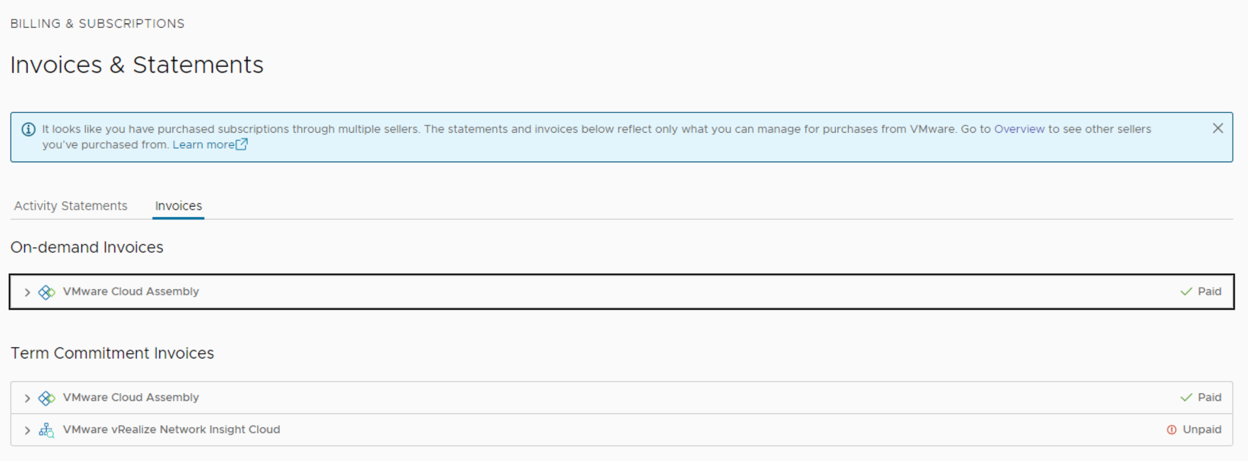
May 9, 2020 Balance: $7,447.42 Total: $9,188.90

March 13, 2020 Balance: $7,44

## Your Invoices

To access your invoices, click the **Invoices** tab on the **Invoices & Statements** page.

- The **On-demand Invoices** section of the page lists billing costs for on-demand subscriptions.
- The **Term Commitment Invoices** section lists the invoices for your subscription's term commitments.



BILLING & SUBSCRIPTIONS

Invoices & Statements

It looks like you have purchased subscriptions through multiple sellers. The statements and invoices below reflect only what you can manage for purchases from VMware. Go to Overview to see other sellers you've purchased from. Learn more

On-demand Invoices

| | |
|---|---|
| VMware Cloud Assembly | ✓ Paid |

Term Commitment Invoices

| | |
|---|---|
| VMware Cloud Assembly | ✓ Paid |
| VMware vRealize Network Insight Cloud | Unpaid |

You download an invoice by clicking on its link, or by selecting **Download** from the vertical ellipsis icon ( ⋮ ) menu next to it.

## How to read my activity statement

As an **Organization Owner** user, you can view detailed information about all services consumed by your Organization during a given billing period in the Activity Statement for that billing period. The Activity Statement is not an invoice.

### What's Included in the Activity Statement

Each Activity Statement provides a summary and detailed breakdown for all service charges accrued in the billing period, and the payments made against the service charges.

#### Billing Period Summary

The Billing Period Summary is an overview of the total charges, credits, discounts, adjustments, and payments for the billing period. The Balance amount shows unpaid charges for the current period, while the Outstanding Balance shows the balance from the previous billing period if that is unpaid.

**Note** Payments made after the statement generation date of the Activity Statement are not reflected in it.

#### Charges Breakdown

The Charges Breakdown section provides a visual pie chart representation of the charges accrued for each service in your Organization. The amount shown for each service is the net amount of any charges after deduction of all discounts, promotions, and adjustments. This chart is only populated if your Organization has incurred charges for more than one service.

#### Charges History

If your Organization has incurred charges for more than one billing period, the Charges History section displays a line graph with a history of charges by service for up to 12 months. The amount shown for each service is the net amount of any charges after deduction of all discounts, promotions, and adjustments.

### Service Charges

The Service Charges includes charges and credits incurred within the billing period, and any payments applied against those charges. The credits cover all discounts, promotions, and adjustments made per service and appear with a minus sign in front of the amount. Service charges can be for services with term commitments, services used on-demand, and additional charges related to service usage. Term Commitments, On-Demand Usage and Other Charges Subtotals appear by line, followed by payments and the current Balance. Payments include all discounts, promotions, and adjustments per service.

### On-Demand Details

All charges for on-demand services used by your Organization are reflected in the On-demand Details section. Charges are incurred only if your Organization used on-demand services and only for the time they were used.

### Other Charges Details

Any additional charges incurred by your Organization, such as Data Transfer, Direct Connect, EBS, Elastic IP charges, and Sign-up Credits appear under Other Charges. Charges are aggregated by unique Region and SID (Subscription ID).

## Glossary of Abbreviations Used in Activity Statement

Your activity statement shows abbreviations of products, services and units of measure that contribute to cost calculation. The glossary below provides a quick reference to assist you when reading your statements.

Table 10-3. VMware Cloud Services Abbreviations Glossary

| Product Name | Unit of Measure | Unit of Measure Description |
|---|---|---|
| vRealize Automation Cloud | EA | Each |
| | NDH | Node per Hour |
| vRealize Log Insight Cloud | EA | Each |
| | NDH | Node per Hour |
| | GB | Gigabyte |
| vRealize Network Insight Cloud | CPU | Central Processing Unit |
| | GB | Gigabyte |
| | EA | Each |
| | VCP | Virtual Central Processing Unit |

Table 10-3. VMware Cloud Services Abbreviations Glossary (continued)

| Product Name | Unit of Measure | Unit of Measure Description |
|---|---|---|
| NSX Cloud | CRM | Core per Month |
| | EA | Each |
| Tanzu Application Catalog | EA | Each |
| Tanzu Application Service | COH | Compute Unit Hour |
| | EA | Each |
| VMware Cloud Director | CRM | Core per Month |
| | EA | Each |
| VMware SD-WAN by VeloCloud | EA | Each |
| VMware Learning Platform | ALH | Active Lab Hour |
| | BIH | Bring Your Own Cloud |
| | COH | Compute Unit Hour |
| | EA | Each |
| | STH | Storage Unit Hour |
| | WIH | Windows Unit Hour |
| VMware Cloud on AWS | ATG | Attachment per GB |
| | ATH | Attachment per Hour |
| | EA | Each |
| | GB | Gigabyte |
| | GBM | Gigabyte Month |
| | HST | Host |
| | HPH | Host per Hour |
| | IPR | IP Address per Hour |
| | IP | IP Address |
| | VMH | Virtual Machine per Hour |
| VMware Cloud on AWS GovCloud (US) | EA | Each |
| | HPH | Host per Hour |
| | IP | IP Address |
| | VMH | Virtual Machines per Hour |

Table 10-3. VMware Cloud Services Abbreviations Glossary (continued)

| Product Name | Unit of Measure | Unit of Measure Description |
|---|---|---|
| | ATH | Attachment per Hour |
| | ATG | Attachment per Giga Byte |
| | IPR | IP Address per Hour |
| | GB | Gigabyte |
| VMware Cloud on DELL EMC | EA | Each |
| | NDM | Node per Month |
| | EDM | Edge per Month |
| vRealize Operations Cloud | EA | Each |
| | OSI | Operating System Instance |

## How do I insert a PO number in my invoice

To process the payment for your invoice, you may need to include additional information, such as a PO number in the invoice. You add the reference information and reprint your invoice from the **Invoices** page in Cloud Services Console.

### Prerequisites

You must have an **Organization Owner** role in the Organization in which the invoice has been generated.

### Procedure

1 Log in to Cloud Services Console and navigate to **Billing &Subscriptions** > **Invoices & Statements** > **Invoices**.

2 Locate the invoice which you want to reprint and click the vertical ellipses ( ⋮ ) icon next to it.

3 From the menu that opens, select **Insert Reference #**.

**Note** The **Insert Reference #** link is available only if the invoice is available as a downloadable PDF, it is not yet paid, and the payment method is not a credit card. It is not available if the invoice has already been submitted for reprinting, but the updated invoice is not yet available for download.

4 In the pop-up window that opens, enter the PO number you want included in the invoice, then click **Submit**.

**Important** Regenerating the new invoice may take up to 24 hours. You will receive an email notification once the invoice is reprinted.

# How do I get support

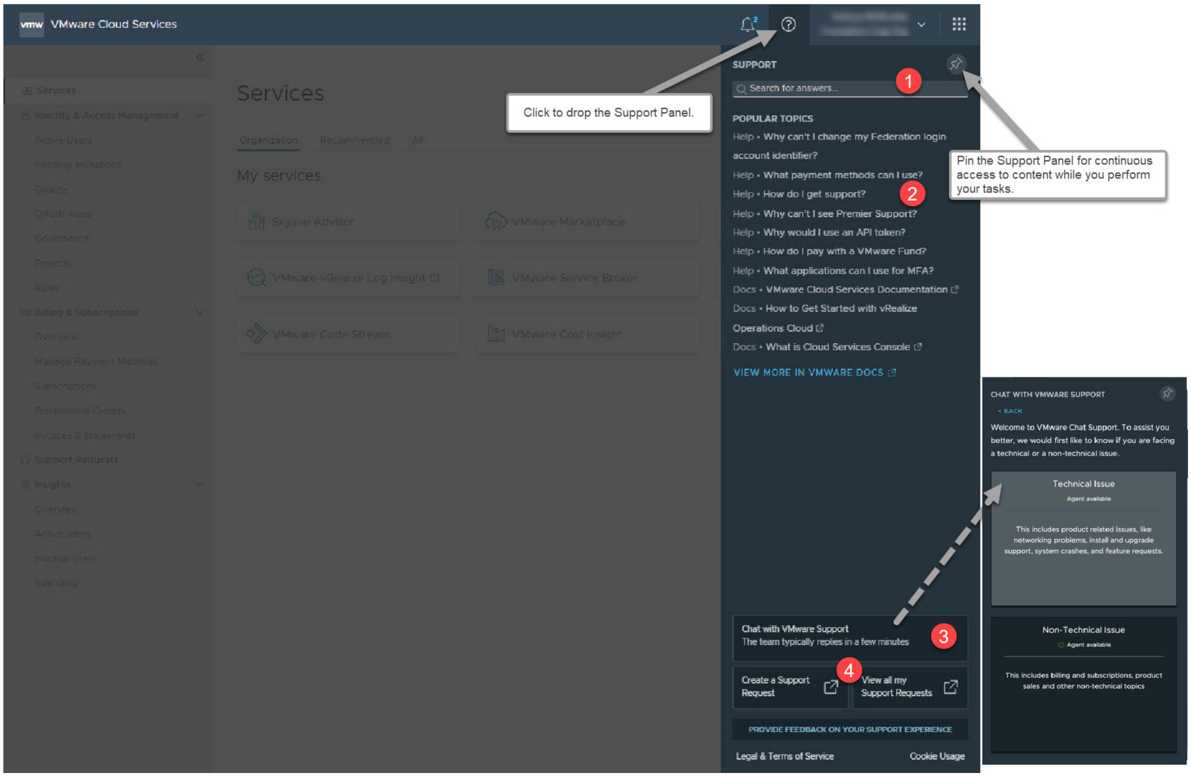
11

Welcome to our VMware Cloud services in-product support experience. Here you can view contextual help content to help you perform your tasks, search for answers to your questions, and for those times when you want to chat, contact a member of our customer support team.

Our support experience is constantly evolving with new features being rolled out for all our cloud services. Currently, you might view some or all the following features in your Support panel.

Procedure

1 Open the Support panel by clicking the **Question** icon on the menu, or the **Support** tab on the right side of the pane.



Click to drop the Support Panel.

Pin the Support Panel for continuous access to content while you perform your tasks.

SUPPORT

Search for answers...

POPULAR TOPICS

Help • Why can't I change my Federation login account identifier?

Help • What payment methods can I use?

Help • How do I get support?

Help • Why can't I see Premier Support?

Help • Why would I use an API token?

Help • How do I pay with a VMware Fund?

Help • What applications can I use for MFA?

Docs • VMware Cloud Services Documentation

Docs • How to Get Started with vRealize Operations Cloud

Docs • What is Cloud Services Console

VIEW MORE IN VMWARE DOCS

Chat with VMware Support
The team typically replies in a few minutes

Create a Support Request

View all my Support Requests

PROVIDE FEEDBACK ON YOUR SUPPORT EXPERIENCE

Legal & Terms of Service

Cookie Usage

CHAT WITH VMWARE SUPPORT

< BACK

Welcome to VMware Chat Support. To assist you better, we would first like to know if you are facing a technical or a non-technical issue.

Technical Issue
Agent available

This includes product related issues, like networking problems, install and upgrade support, system crashes, and feature requests.

Non-Technical Issue
Agent available

This includes billing and subscriptions, product sales and other non-technical topics

2 Access the level of support you require.

The **Support** panel provides contextual help content and a powerful search to help you discover more content and answer questions - all without contacting support. For those times when you want to chat with a customer support representative, you can continue to interact with your cloud service while chatting.

| Access this support feature… | To help you… |
|---|---|
| 1. Intelligent search. | Search our content to find answers to your question. We search through our documentation, specially written help topics, communities, and knowledge-based articles. |
| 2. Page-relevant content. | Perform your tasks. When you open the **Support** panel, you see page-related help topics that contain just enough information to assist you with your tasks. As you work your way through your tasks, and move from page to page, the help content changes accordingly. This list of content also displays your search results. Search results include more help topics, Knowledge Base articles, content from our Documentation Center, and content from our communities.<br>If you don't find what you're looking for, click **View more in VMware Docs** to perform a search related to the page you are viewing, or if you have typed a search item, related to the search item. Your results are displayed in our Documentation Center. |

| Access this support feature... | To help you... |
|---|---|
| 3. Chat with VMware Support. | Contact our support engineers and customer support representatives.<br>Here's what you need to know about live support chat:<br>■ Starting a chat with VMware support is context-sensitive. This means that when you start a live chat with VMware Support from the Cloud Services Console, you can get help for issues with Cloud Services Console. To access chat support for a service, make sure you initiate a chat after logging in to the service.<br>■ You can continue to interact with the Cloud Services Console or with Cloud Services Console while chatting with our customer support engineers. You can always return back to the chat by clicking the **Support** button located at the right edge of browser window « SUPPORT, then clicking the **Return to chat** icon .<br>■ Customer support engineers can also help you open a support request.<br>■ Depending on the language settings configured for your browser and VMware Cloud Services profile, you will receive online support either in English or Japanese language.<br>■ When using live support chat in Cloud Services Console:<br>  ■ You must first select if the issue you're seeking help with is technical or non-technical. This ensures your request gets to the right customer support representative.<br>  ■ You can't have multiple support chats simultaneously. To open a new chat for a new issue, you must close the current chat.<br>  ■ During the chat, you have the option to send files or screenshots to the customer support representative directly from the chat window.<br>**Note** To avoid any time-out issues during an active chat session, it's recommended that you keep the browser window/tab open in the foreground. |
| 4. Create a Support Request / View All My Support Requests. | Opens VMware Customer Connect where you create and manage support requests. |

3 To manage your support requests, click the **Support Requests** link in the Cloud Services Console menu.

All support-related functionality is now available through the VMware Customer Connect portal.

a Click **Create a Support Request**.

The **VMware Support** page on Customer Connect opens. For detailed instructions on creating a new support request, see How to file a Support Request in Customer Connect and via Cloud Services Portal.

You might need additional service-related information before you open a support request. For example, in VMC on AWS you might require the support information for your SDDC.

b To access all open and closed Support Requests for your Organization, click **View Support Request History**.

The **Support Request History** page on Customer Connect opens.

You can then filter your support requests by Organization, type, and time period. You can also sort and export the data.

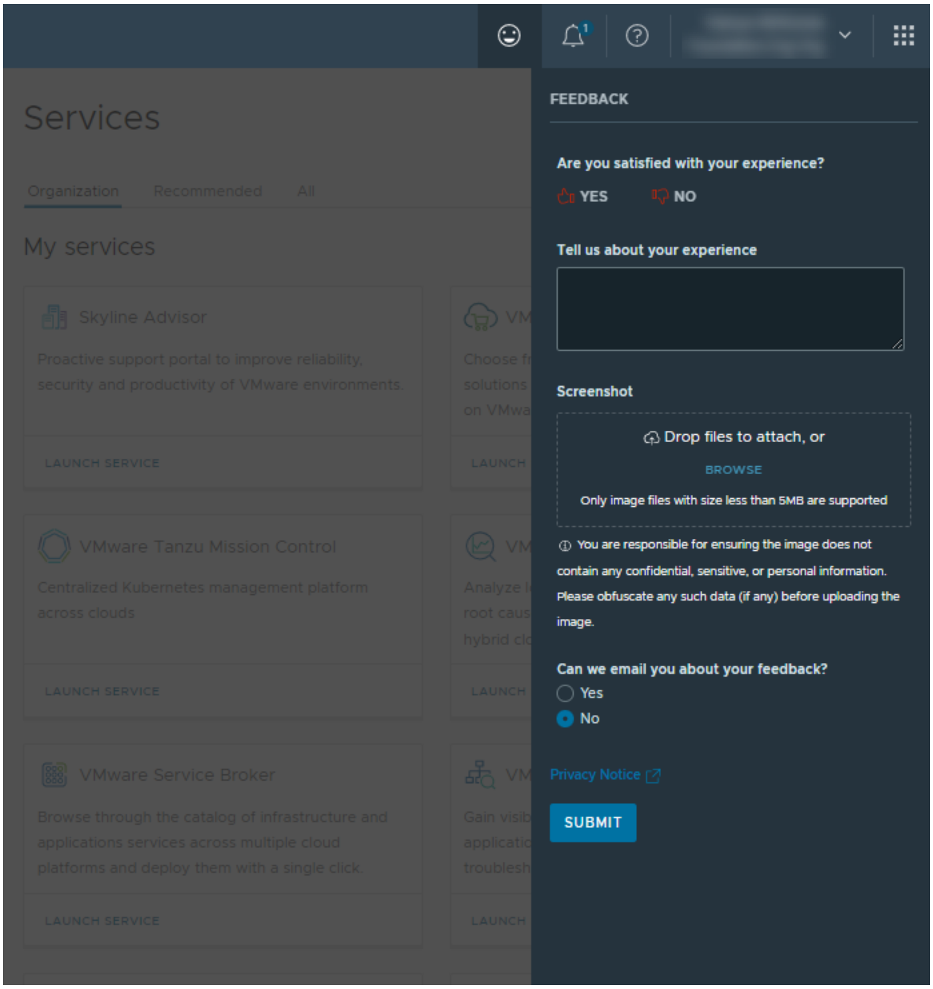
# How do I provide feedback

12

Feedback helps us make our products better. You can submit your feedback for Cloud Services Console directly from the product.

1 On the horizontal menu in Cloud Services Console, click the **Offer Feedback** icon (☺).

The feedback panel opens.



Proactive support portal to improve reliability, security and productivity of VMware environments.

Centralized Kubernetes management platform across clouds

Browse through the catalog of infrastructure and applications services across multiple cloud platforms and deploy them with a single click

FEEDBACK

Are you satisfied with your experience?

YES NO

Tell us about your experience

Screenshot

Drop files to attach, or

BROWSE

Only image files with size less than 5MB are supported

ⓘ You are responsible for ensuring the image does not contain any confidential, sensitive, or personal information. Please obfuscate any such data (if any) before uploading the image.

Can we email you about your feedback?

○ Yes

● No

Privacy Notice

SUBMIT

2 Use one or more of the available options to provide your feedback:

- Use the thumbs up or thumbs down icon to communicate your satisfaction with using Cloud Services Console.

- Use the text field to describe your experience in more detail.
- If you want to visually enhance your feedback message, attach a screenshot by clicking **Browse** or dragging and dropping an image in the designated field.
- Let us know if you'd like to engage further with the VMware Cloud Services Console team regarding your feedback.

3 Click **Submit.**