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/
Contents

1 What is Cloud Services Console  5

2 How Do I Sign up for VMware Cloud Services  6

3 Onboarding With a Federated Account  7

4 Manage Your Account  9
   How Do I Edit My User Profile  9
   Reset Your Password  9
   How Do I Change My Language and Regional Format  10
   How Do I Secure My Account Using Multi-Factor Authentication  12
   How Do I Troubleshoot MFA When I Can't Sign In  12
   What Two-Factor Authentication Application Can I Use?  13
   How Do I Generate API Tokens  14
      How Do I Manage My API Tokens  15
   How Do I Secure My API Tokens Using Multi-Factor Authentication  16
   How Do I View My Roles in an Organization  17

5 Managing Your Organizations  19
   Access One of Your Other Organizations  20
   Specify a Default Organization  20
   How Do I Request Additional Roles  20
   How Do I Use the Data Insights Dashboard  22

6 Identity & Access Management  23
   Organization Roles and Permissions  23
   Add Users to Your Organization  25
      Edit User Roles  26
   Manage Users  27
   Setting Authentication Policies  27
      How Do I Define IP Authentication Preferences  30
   Working with Groups  32
      Create a New Group  34
   Assign Roles to Enterprise Groups  35
   Manage Shared Groups  35
   Setting Up Enterprise Federation with VMware Cloud Services  37
      What’s Involved in Setting Up Enterprise Federation  38
   Why Do I Need to Link My VMware ID  39
What is Cloud Services Console

The VMware Cloud Services Console™ enables 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

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.

Sign up for one or more VMware Cloud services at https://cloud.vmware.com/ and complete the steps in the onboarding flow.

During the onboarding process, you create a cloud service account with your VMware ID. If you do not have a My VMware account, you create one as you sign up. You also set up an organization. VMware Cloud uses organizations to provide controlled access to one or more services. Your VMware Cloud services account is contained within an organization.

Procedure

1. Initiate the onboarding process from the service sign-up or from your invitation link.
2. Follow the steps to create your VMware Cloud services account.
3. Sign in to VMware Cloud services with your VMware ID.

   When you have set up your account, you can invite other people to join your organization. They will receive an email with a link to onboard.
Onboarding 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 enabled for Identity Governance and Administration (IGA). If you have to obtain access to an organization that is not IGA-enabled, 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-enabled organizations associated with your enterprise.
3. Select the organization which you want to access and click Continue.
4. Select the organization roles you want to have in the selected organization. Your organization role determines the level of access and permissions you have in the organization. For more information, see Organization Roles and Permissions.
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-enabled 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.
Manage Your Account

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 Edit My User Profile
- How Do I Change My Language and Regional Format
- How Do I Secure My Account Using Multi-Factor Authentication
- How Do I Generate API Tokens
- How Do I View My Roles in an Organization

How Do I Edit My User Profile

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

You can change your user profile in the Cloud Services Console or by logging in to your My VMware account at https://my.vmware.com. When you modify your details in the Cloud Services Console, the changes you make are saved to your My VMware account, and vice versa.

You cannot change the email address with which you registered.

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.

Reset Your 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 My VMware account at https://my.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.

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.
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.

**Setting 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.

<table>
<thead>
<tr>
<th>Language</th>
<th>Default regional format</th>
</tr>
</thead>
<tbody>
<tr>
<td>English</td>
<td>US</td>
</tr>
<tr>
<td>Simplified Chinese</td>
<td>CN</td>
</tr>
<tr>
<td>Traditional Chinese</td>
<td>TW</td>
</tr>
<tr>
<td>Spanish</td>
<td>ES</td>
</tr>
<tr>
<td>French</td>
<td>FR</td>
</tr>
<tr>
<td>Japanese</td>
<td>JP</td>
</tr>
<tr>
<td>German</td>
<td>DE</td>
</tr>
<tr>
<td>Korean</td>
<td>KR</td>
</tr>
</tbody>
</table>
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**.
2. Click **Activate MFA Device**, and follow the instructions to set up your device.
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**.
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**.
2. Click **Deactivate MFA Device**.

### 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.
You can regenerate a new set of recovery codes at any time by accessing My Account > Security.

I don't have access to my MFA device

If you don't have your MFA device at hand, or if you have lost it, you can use one of your recovery codes to sign in. On the VMware Cloud services sign in page click Troubleshoot MFA. You can regenerate a new set of recovery codes at any time by accessing My Account > Security.

I can't find my MFA recovery codes

If you can't find your set of recovery codes, contact VMware Support to turn off MFA for your account. Then, sign in to VMware Cloud services with your user name and password, and activate MFA for your account. See How Do I Secure My Account Using Multi-Factor Authentication.

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 applications

<table>
<thead>
<tr>
<th>Device</th>
<th>Authentication application</th>
</tr>
</thead>
</table>
| iOS                    | - Google Authenticator.  
| Android                | - Google Authenticator.  
| Blackberry             | Google Authenticator  
  See, [https://support.google.com/accounts/answer/1066447](https://support.google.com/accounts/answer/1066447). |


**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 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. Enter a name for the token.

3. 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.

4. Define scopes for the 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.

5. Select the **Open ID** check box to retrieve an Open ID compliant token with extended user details.

6. Click **Generate**.

7. 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.

8. 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

What to do next

**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 disable 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 recommend 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.

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

<table>
<thead>
<tr>
<th>If you want to...</th>
<th>Do this...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Extend the validity of an API token that has expired.</td>
<td>You must regenerate your token.</td>
</tr>
<tr>
<td>Regenerate a valid API token.</td>
<td>You can regenerate a token at any time. If you regenerate a token, you revoke all instances of the previous token. If you have used the token, for example in one of your scripts, remember to replace it with the newly generated token.</td>
</tr>
<tr>
<td>Replace a compromised API token.</td>
<td>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.</td>
</tr>
<tr>
<td>Destroy an API token that is still valid.</td>
<td>You destroy a valid API token by revoking it.</td>
</tr>
<tr>
<td>Recover a lost API token.</td>
<td>Lost tokens cannot be recovered. You must revoke the lost token and generate a new one.</td>
</tr>
</tbody>
</table>

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 enabling 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 enable 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. In order to access 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**.
2. Click **Activate MFA Device**, and follow the instructions to set up your device.
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**.
2. Click the **MFA is turned on** toggle switch.

**Important** If using MFA on API tokens is enforced by your organization, you are not able to turn off MFA. Even if you are able to generate API tokens, you won't be able to 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**.
2. Click **Deactivate MFA Device**.

## How Do I View My Roles in an Organization

Roles are assigned by organization owners. 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, you can request additional service roles for services available in your organization. To obtain additional service role access, your request must be approved by an organization owner.

For more information about the organization's roles, see [Organization Roles and Permissions](#).

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 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.

Optional: Describe why you'd like owner to review

If you are a member of an Identity and Governance Administration (IGA) enabled organization, you have the additional option to request new organization roles. For more information, see How Do I Request Additional Roles.
Managing Your Organizations

VMware Cloud services accounts are contained within organizations. VMware Cloud uses organizations to provide controlled access to one or more services. You must belong to an organization before you can access a cloud service.

If you are an organization owner, you have access to all the resources of the organization. You add cloud services to your organization, and then invite users. You manage the organization's payment methods and the organization's user accounts. If you hold the role of organization member, you have limited access to the organization's resource.

To see what you can do within your organization with your role, see Organization Roles and Permissions.

Your Active Organization

When you sign in to 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 may need 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. Click the ID to display the full organization 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:

- Access One of Your Other Organizations
- Specify a Default Organization
- How Do I Request Additional Roles
- How Do I Use the Data Insights Dashboard

**Access One of Your Other 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.

**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 Request Additional Roles**

As an organization member of a VMware Cloud services organization, you can submit self-service requests for additional service roles.
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. If you are an organization member of an Identity Governance and Administration (IGA) enabled organization and your account is federated, you can submit self-service requests for organization roles as well as for service roles.

**Note** Organization owners can self-assign additional organization and service roles to themselves. Refer to [Manage Users](#) for more information.

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.

<table>
<thead>
<tr>
<th>To...</th>
<th>Do the following...</th>
</tr>
</thead>
</table>
| Submit a new self-service request in a non-IGA organization | 1. Log in to your VMware Cloud services organization.  
2. Browse or filter the services catalogue to locate the service for which you want to request additional roles.  
3. In the service's tile, click Request Role.  
4. Use the drop-down menu to select a new service role.  
5. Optionally, provide a business justification for your request.  
6. Click Request. |

| Submit a new self-service request an IGA enabled organization | 1. Log in to VMware Cloud services with your federated account.  
2. On the menu bar, click your user name.  
4. Click Request Roles.  
5. To change your role in the organization, select the appropriate entries under Organization Roles.  
6. To request service roles, click Add Service Access and use the drop-down lists to make a selection.  
7. Optionally, in the Business Justification text box, type a message to the organization owner.  
8. Click Request.  
   Your request is submitted for approval to the organization owners. |

| View your pending and past requests | 1. On the menu bar in VMware Cloud services, click your user name.  
2. Select My Account > My Roles.  
   The My Request History section of the page displays a list of all requests you submitted. If a request is still pending approval, you can cancel it. |

| Cancel a self-service request | 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. |
How Do I Use the Data Insights Dashboard

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

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 service, total spending for all services, and spendings per service breakdown. The data on the **Insights** dashboard updates daily.

To change the time frame for which information is displayed, select a different value in the respective dashboard tile.

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

The **Active users**, **Inactive users** and **Spending** reports provide a detailed breakdown of data for your services, usage, and costs.
Identity & Access Management

As an organization owner, you control user access to your organization and its resources.

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 with full access, or as an organization member 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 owner, you determine the members that make up your groups and what roles and permissions they are assigned.

This chapter includes the following topics:

- Organization Roles and Permissions
- Add Users to Your Organization
- Manage Users
- Setting Authentication Policies
- Working with Groups
- Setting Up Enterprise Federation with VMware Cloud Services
- Identity Governance and Administration
- Authenticating Your Applications with OAuth 2.0
- Auditing Event Logs in VMware Cloud Services

Organization Roles and Permissions

As an organization owner, you invite users to your organization and give them role-based access to the organization's resources.
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 cloud service according to the roles provided by each cloud service. For more information, refer to the documentation of the relevant VMware Cloud service.
- Role-based access to the organization. As an organization owner with full access, or as an organization member with read-only access.

**Organization Roles and Permissions**

You view users and roles in your organization from the Identity and Access Management > Active Users menu in Cloud Services Console. To view the roles in your organization, click your user name on the menu bar and select My Account > My Roles.

To see the permissions each organization role enables, see the following table.

<table>
<thead>
<tr>
<th>Permission</th>
<th>Organization Owner</th>
<th>Organization Member</th>
</tr>
</thead>
<tbody>
<tr>
<td>Belong to one or more organizations</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Access one of your other organizations</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Specify the organization that is displayed when you sign in.</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>View and modify the organization settings.</td>
<td>✓</td>
<td>✓ View only.</td>
</tr>
<tr>
<td>Add/remove users in your organization</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Manage the service access and roles of users in your organization.</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Manage and view payment methods and billing.</td>
<td>✓</td>
<td>✓ 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.</td>
</tr>
<tr>
<td>Submit and manage support tickets.</td>
<td>✓</td>
<td>✓ When the Support User check box is selected.</td>
</tr>
<tr>
<td>Query the cloud service APIs for customer usage and data.</td>
<td>✓</td>
<td>✓ When the Managed Service Provider check box is selected.</td>
</tr>
<tr>
<td>Create and manage OAuth apps to authorize third-party apps to access protected resources.</td>
<td>✓</td>
<td>✓ When the Developer check box is selected.</td>
</tr>
</tbody>
</table>
Add Users to Your Organization

As an organization owner, you invite users to your organization and give 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 privileges assigned to each of these roles, see Organization Roles and Permissions.

- 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 enables 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.

2. Click Add Users.

3. On the Active Users tab, enter the email address of the user you want to add to your organization.

   You can add more than one user at a time.

4. In the Role in organization text box, assign the role that the user will use in the organization.

5. The organization owner role includes access to the Support Center. If you are assigning the role of organization member and you want to give the user access to the Support Center, select the Support User check box.
6. To give the user access to a service in the organization, click **Add service access**.

![Add New Users](image)

7. The first service that appears in your list of services is selected. To change the service to another service, click the downward arrow next to the service name, and scroll the list of services in your organization.

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

9. 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 **Invitations** tab.

![Users](image)

10. 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.

### Edit User Roles

You define the access of the users in your organization by assigning roles. Users are granted access to the organization and services when you assign roles to them directly or if they inherit them as members of groups.
You can edit the roles of users in your organization, and view the groups to which they belong. 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**.
2. Select the check box next to a user and click **Edit Roles**.
3. Change the user's organization roles and service roles as required.
4. If the user has roles that were assigned through groups, click **Show** to view the roles and the groups.
   
   Changes you make to the user's role might override their group-assigned roles.
5. Click **Save**.

**Manage Users**

If you are an organization owner, you can change the role users hold in your organization and the services they can access. You can also remove users from your organization.

**Procedure**

1. On the Cloud Services Console toolbar, click the VMware Cloud Services icon and select **Identity & Access Management**.
2. To modify a role:
   
   a. Select a user and click **Edit Roles**.
   b. Make your required changes and click **Save**.
3. To remove a user from the organization:
   
   a. Select one or more users and click **Remove Users**.
   b. Click **Remove** to permanently remove the user from your organization.

**Setting Authentication Policies**

As an organization owner, you set authentication policies to user access to your VMware Cloud services. You can define IP addresses or IP ranges that either block or allow user access from these IPs.
You set authentication policies for your organization from the **Organization > Authentication Policy** page in the Cloud Services Console. You can select one of two authentication policy preferences: **Block IP** or **Allow IP**.

**Note**  You can have only one authentication policy preference at any given time.

You apply the authentication preference of your choice to 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.
<table>
<thead>
<tr>
<th>To</th>
<th>Do this</th>
</tr>
</thead>
</table>
| Set an IP authentication preference for your organization | 1. On the menu bar in the Cloud Services Console, click your user name.  
2. In the settings panel that displays, click **View Organization**.  
3. Click **Authentication Policy**.  
   - If this is the first time you are creating an authentication policy for your organization, the **Authentication Policy** page displays the two IP authentication preferences you can choose from:  
     - **Block IP**  
     - **Allow IP**  
4. Make a selection and click **Enable**.  
5. To define the IP address or range for the selected policy setting, click **Add** and type the IP address or range.  
6. Click **Add** again. |
| Change your IP authentication preference | If you want to switch from **Block IP** to **Allow IP** authentication preference or vice versa, you must remove the IP addresses and ranges specified for your current authentication preference.  
1. In the Authentication Policy page, select all IP addresses and ranges that are currently defined.  
2. Click Remove.  
3. Click the Change link next to the User IP Authentication Preference option.  
4. In the pop up window that opens, select the preferred option, then click Save.  
5. Define new IP addresses or ranges for the newly selected policy setting.  
Navigate to **Organization > Authentication Policy** and click **Change**. Since you can only enable one preference or the other, any IP addresses or ranges you defined in the current policy will be lost when you apply the new setting. |
To Add an exception to your authentication preference

Do this

You define exception rules for IP addresses from an IP range that is already specified in the list of allowed or blocked IPs.

1. In the Exception section of the Authentication Policy page, click Add an Exception.
2. In the pop up that opens, type the IP addresses you want to add as exceptions to the authentication policy.

   If you enabled the Allow IP preference, users accessing VMware Cloud services from the IPs on the exceptions list will be denied access. Conversely, if you enabled the Block IP preference, users accessing VMware Cloud services from the IPs on the exceptions list will be allowed access.

To Modify the IP ranges for your authentication preference

Do this

Once you enabled an IP authentication policy, you can add additional IPs or IP ranges, edit or remove existing ranges.

To make a change, first select the IP address or range from the list, then apply the appropriate action.

---

### 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 Define IP Authentication Preferences

You define 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.
### To Do this

**Set an IP authentication preference for your organization**

1. On the menu bar in the Cloud Services Console, click your user name.
2. In the settings panel that displays, click **View Organization**.
3. Click **Authentication Policy**.
   - If this is the first time you are creating an authentication policy for your organization, the **Authentication Policy** page displays the two IP authentication preferences you can choose from:
     - **Block IP**
     - **Allow IP**
4. Make a selection and click **Enable**.
5. To define the IP address or range for the selected policy setting, click **Add** and type the IP address or range.
6. Click **Add** again.

**Change your IP authentication preference**

If you want to switch from **Block IP** to **Allow IP** authentication preference or vice versa, you must remove the IP addresses and ranges specified for your current authentication preference.

1. In the Authentication Policy page, select all IP addresses and ranges that are currently defined.
2. Click Remove.
3. Click the Change link next to the User IP Authentication Preference option.
4. In the pop up window that opens, select the preferred option, then click Save.
5. Define new IP addresses or ranges for the newly selected policy setting.

Navigate to **Organization > Authentication Policy** and click **Change**. Since you can only enable one preference or the other, any IP addresses or ranges you defined in the current policy will be lost when you apply the new setting.
To | Do this
--- | ---
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.
1. In the Exception section of the Authentication Policy page, click **Add an Exception**.
2. In the pop up that opens, type the IP addresses you want to add as exceptions to the authentication policy.
   
   If you enabled the **Allow IP** preference, users accessing VMware Cloud services from the IPs on the exceptions list will be denied access. Conversely, if you enabled the **Block IP** preference, users accessing VMware Cloud services from the IPs on the exceptions list will be allowed access.

Modify the IP ranges for your authentication preference | Once you enabled an IP authentication policy, you can add additional IPs or IP ranges, edit or remove existing ranges.

To make a change, first select the IP address or range from the list, then apply the appropriate action.

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.

**Working 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, 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 – these are the custom group and the enterprise group. 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’s 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 [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. Here’s what federation means and how you can federate your domain. See how to [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.

Create a New Group

As an organization owner, 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 Organization Roles and Permissions. For information about the permissions assigned with service roles, see the documentation for the service.

Procedure

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.
Assign Roles to Enterprise Groups

If you have 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. Learn more about how to sync groups and set up federation for your 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 Organization 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 members 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

2. Select Select groups from your source domain and 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.

Manage Shared Groups

When an organization owner 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.

The members of the shared group you imported can use 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**

2. Click *Add Groups.*
3. Select *Import groups from other organizations,* and click *Continue.*
4. From the drop-down list, 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 may 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 members 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.

Setting Up Enterprise Federation 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 enable 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 enable 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.

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**

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 owners of unfederated domains receive notification from VMware Cloud services with a link to kick off the federation setup. 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
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 enabled 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. Here's what linking your account means.

**Self-service federation kick-off**

Any organization owner of an unfederated domain can kick off the federation setup. A notification with a link to initiate federation setup appears in the Notifications list in the Cloud Services Console. Clicking the link opens a one-step online form where the organization owner identifies the Enterprise Administrator to complete the setup. An email invitation with a setup link is sent to the designated Enterprise Administrator who kicks off the federation setup process by clicking the link.

**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 initiated from the invitation link.

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.

**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 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 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 or Users with Support Roles?
If you are an organization owner or hold a support 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.

![Customer Number](image)

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 Authenticating Your Applications with OAuth 2.0.

**Why Do I Need to Link My IdP**

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

One way to enable 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 your user name in the menu bar.
2. Select View Organization.
3. In the Domains Linked to Identity Provider section of the Details page, click Link Identity Provider.
   
   The IdP and domains associated with it display in a pop up window.
4. Click Link, then click Continue.

For more information about IGA features, see Identity Governance and Administration.

**Identity Governance and Administration**

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

Organization owners can start using the IGA service by clicking the Get Started link on the Identity & Access Management > Governance page. Using the IGA service in an organization, lets users do the following:
As an | You can
---|---
organization owner

- Access the IGA dashboard from the **Identity & Access Management > Governance** page in the Cloud Services Console.
- Govern access to services in your organization by managing incoming organization and service role requests. See **Identity Governance and Administration**.
- Monitor violations and immediately respond to threats. See **Monitor Violations**.

organization member

- Submit self-service access requests for additional organization and service roles. See **How Do I Request Additional Roles**.

### Advanced IGA Features for Federated Domains

If your domain is federated, additional IGA features can be enabled for all organizations in the federated domain that are linked to the corporate Identity Provider. See **Why Do I Need to Link My IdP**.

When advanced IGA features are enabled, non-organization members can request organization and service roles access in linked organizations during onboarding. See **Chapter 3 Onboarding With a Federated Account** to learn more about this feature.

**Enterprise Administrators** of federated domains can enable 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 **Setting Up Enterprise Federation with VMware Cloud Services**.

### Manage Pending Requests

As an organization owner of an Identity Governance and Administration (IGA) enabled organization, you manage organization and service roles requests through the **Governance > Requests** page in Cloud Services Console.

All incoming requests for organization and service role access are listed in the **Pending Requests** list. 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.

Monitor Violations

As an organization owner in an Identity and Access Governance enabled organization, you define policies, monitor access violations for logins with OAuth apps and API tokens, and take action on suspicious login activity in your organization.

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

**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. You view details about the trigger on a violation by clicking the double arrow in the table next to its name.

**Authenticating Your 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 View 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, or an organization member with the Developer role, you create and manage your OAuth apps.
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 corporation 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

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, 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.

Procedure

1. Click your user name and select View Organization > OAuth Apps, and then click Create New OAuth App.
2 Select **Server to server app**.

3 Register your client.

4 Define scopes.
   Scopes provide a way to implement granular access control to your app.

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

6 Copy the credentials or download a JSON file, and click **Continue**.
   You are responsible for storing your credentials in a safe place.

7 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, **Manage OAuth 2.0 Apps**.

**What to do next**

Paste the credentials into your script.
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.

Procedure

1. Click your user name and select View Organization > OAuth Apps, and then click Create New OAuth App.
2. Select Web app and click Continue.
3. Register your app by entering the app details. 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. Then, specify a time span for your access token. If you want your access token to authorize requests continuously, issue a refresh token.
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 credentials or download a JSON file that contains your credentials. You are responsible for storing your credentials in a safe place.
8. Click Continue.

What to do next

Paste the credentials into your script.

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.

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.
   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. Then, specify a time span for your access token. If you want your access token to authorize requests continuously, issue a refresh token.

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.

**Manage OAuth 2.0 Apps**

You can view and modify the details of the OAuth 2.0 apps you created. You can also grant access to apps created in any organization in which you hold the organization owner role.
To... | Do this...
---|---
To view and manage the apps created in your organization. | Click your username, and then click View Organization > OAuth Apps. Here you can view all the apps that were created in your organization, and perform the following actions:
- 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 owners must remove the app from their organization, and add it again, or edit the app to reflect the updated scoping.
- Remove an app from the organization.
- Add an app that has been created in the organization but not yet given access to the organization.
- Create an app.

To view and manage the apps that have access to your organization. These apps were created in organizations in which you have an organization role. | Click Identity & Access Management > OAuth Apps. Here you can view the apps that have access to your organization, and perform the following actions:
- Add an app.
- Remove an app.

**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.
Auditing Event Logs in VMware Cloud Services

As an organization owner you audit users' activity in your VMware Cloud services organization by reviewing event logs. By using an associated instance of vRealize Log Insight Cloud, 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.

vRealize Log Insight Cloud 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 vRealize Log Insight Cloud 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 vRealize Log Insight Cloud 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 enabled by default, select it for viewing from the Content Pack Dashboards tab of the Dashboards page.

For more information on using vRealize Log Insight Cloud refer to Using VMware vRealize Log Insight Cloud.

Note If your organization does not have a vRealize Log Insight Cloud 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 filing a support ticket. 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 with vRealize Log Insight Cloud Admin service role, you can access all audit data for your organization in the associated vRealize Log Insight Cloud service instance for your organization.

VMware Cloud Services Audit Events

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, you review audit events for your organization by using an associated instance of vRealize Log Insight Cloud.

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 organization, 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 6-1. Account Management**

<table>
<thead>
<tr>
<th>Audit Event Name</th>
<th>Event Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>UserLogin</td>
<td>csp__user_login</td>
<td>Successful user login.</td>
</tr>
<tr>
<td>UserLogout</td>
<td>csp__user_logout</td>
<td>Successful user logout.</td>
</tr>
<tr>
<td>GenerateApiToken</td>
<td>csp__generate_api_token</td>
<td>User generated a personal API token.</td>
</tr>
<tr>
<td>RevokeApiToken</td>
<td>csp__revoke_api_token</td>
<td>User revoked a personal API token.</td>
</tr>
<tr>
<td>RevokeAllApiTokens</td>
<td>csp__revoke_all_api_tokens</td>
<td>User revoked all personal API tokens.</td>
</tr>
<tr>
<td>RefreshTokenExchangeFailed</td>
<td>csp__refresh_token_exchange_failed</td>
<td>User made an unsuccessful attempt to generate access token by API token refresh.</td>
</tr>
<tr>
<td>FirstLogin</td>
<td>csp__first_login</td>
<td>User was assigned the roles from the invitation upon first log in.</td>
</tr>
<tr>
<td>LinkAccount</td>
<td>csp__link_account</td>
<td>User linked their corporate federated account to their VMware ID account.</td>
</tr>
<tr>
<td>UnlinkAccount</td>
<td>csp__unlink_account</td>
<td>User changed the account linked to their VMware ID.</td>
</tr>
<tr>
<td>CreateOrgOAuthApp</td>
<td>csp__create_org_o_auth_app</td>
<td>Caller created an OAuth app in an organization.</td>
</tr>
<tr>
<td>UpdateOrgOAuthApp</td>
<td>csp__update_org_o_auth_app</td>
<td>Caller updated an OAuth app in an organization.</td>
</tr>
<tr>
<td>DeleteOrgOAuthApp</td>
<td>csp__delete_org_o_auth_app</td>
<td>Caller deleted an OAuth app in an organization.</td>
</tr>
<tr>
<td>OrgOAuthAppNewSecretRotation</td>
<td>csp__org_o_auth_app_new_secret_rotation</td>
<td>Caller rotated the secret of an OAuth app in an organization.</td>
</tr>
<tr>
<td>ActivateMfa</td>
<td>csp__activate_mfa</td>
<td>User with VMware ID activated an MFA device.</td>
</tr>
<tr>
<td>DeactivateMfa</td>
<td>csp__deactivate_mfa</td>
<td>User with VMware ID deactivated an MFA device.</td>
</tr>
</tbody>
</table>
### Table 6-1. Account Management (continued)

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

### Table 6-2. Organization Management

<table>
<thead>
<tr>
<th>Audit Event Name</th>
<th>Event Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CreateOrganization</td>
<td>csp__create_org</td>
<td>User created a new organization.</td>
</tr>
<tr>
<td>UpdateOrganization</td>
<td>csp__update_org</td>
<td>User updated an existing organization.</td>
</tr>
<tr>
<td>DeleteOrganization</td>
<td>csp__delete_org</td>
<td>User deleted an existing organization.</td>
</tr>
<tr>
<td>InviteExistingUserToOrganization</td>
<td>csp__invite_existing_user_to_org</td>
<td>Existing user was added to an organization.</td>
</tr>
<tr>
<td>RemoveUserFromOrganization</td>
<td>csp__remove_user_from_org</td>
<td>Existing user was removed from an organization.</td>
</tr>
<tr>
<td>UpdateUserRolesOnOrganization</td>
<td>csp__update_user_roles_on_org</td>
<td>The roles of an existing user were updated.</td>
</tr>
<tr>
<td>InviteNonExistingUserToOrganization</td>
<td>csp__invite_non_existing_user_to_org</td>
<td>Email invitation was sent to a new user.</td>
</tr>
</tbody>
</table>
Table 6-2. Organization Management (continued)

<table>
<thead>
<tr>
<th>Audit Event Name</th>
<th>Event Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RevokeUserInvitations</td>
<td>csp__revoke_user_invitations</td>
<td>Invitations sent to users by email were revoked.</td>
</tr>
<tr>
<td>RemoveClientFromOrganization</td>
<td>csp__remove_client_from_org</td>
<td>User removed an OAuth app assigned to an organization. The action did not delete the OAuth app.</td>
</tr>
<tr>
<td>AssignRolesToClientOnOrganization</td>
<td>csp__assign_roles_to_client_on_org</td>
<td>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.</td>
</tr>
<tr>
<td>UpdateClientRolesOnOrganization</td>
<td>csp__update_client_roles_on_org</td>
<td>Caller updated service/organization roles to a client in an organization.</td>
</tr>
<tr>
<td>UpdateUserDefaultOrganization</td>
<td>csp__update_user_default_org</td>
<td>User updated the default organization displayed for their account. This action applies only to users who are members of more than one organization.</td>
</tr>
</tbody>
</table>

Table 6-3. Groups

<table>
<thead>
<tr>
<th>Audit Event Name</th>
<th>Event Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RemoveGroupFromOrganization</td>
<td>csp__remove_group_from_org</td>
<td>User removed an existing group from an organization.</td>
</tr>
<tr>
<td>AssignRolesToGroupOnOrganization</td>
<td>csp__assign_roles_to_group_on_org</td>
<td>User assigned organization and service roles to a newly created group in an organization.</td>
</tr>
<tr>
<td>UpdateGroupRolesOnOrganization</td>
<td>csp__update_group_roles_on_org</td>
<td>User updated role assignments of an existing group in an organization.</td>
</tr>
<tr>
<td>CustomGroupAddClients</td>
<td>csp__custom_group_add_clients</td>
<td>User added new members to a custom group in an organization.</td>
</tr>
<tr>
<td>CustomGroupRemoveClients</td>
<td>csp__custom_group_remove_clients</td>
<td>User removed existing members from a custom group in an organization.</td>
</tr>
</tbody>
</table>

Table 6-4. Billing and Subscription

<table>
<thead>
<tr>
<th>Audit Event Name</th>
<th>Event Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CreateSubscription</td>
<td>csp__create_subscription</td>
<td>User created a subscription for a new or existing service.</td>
</tr>
<tr>
<td>AddOrgPaymentMethod</td>
<td>csp__add_org_payment_method</td>
<td>User added a new payment method to their organization.</td>
</tr>
<tr>
<td>RemoveOrgPaymentMethod</td>
<td>csp__remove_org_payment_method</td>
<td>User removed a payment method from their organization.</td>
</tr>
</tbody>
</table>
### Table 6-4. Billing and Subscription (continued)

<table>
<thead>
<tr>
<th>Audit Event Name</th>
<th>Event Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>UpdateOrgDefaultPaymentMethod</td>
<td>csp__update_org_default_payment_method</td>
<td>User updated the default payment method of an organization.</td>
</tr>
<tr>
<td>AddDetailsToOrg</td>
<td>csp__add_details_to_org</td>
<td>User added a company address and/or other Billing and Subscription details to an organization.</td>
</tr>
<tr>
<td>UpdateOrgAddress</td>
<td>csp__update_org_address</td>
<td>User updated the company’s address in the Billing and Subscription details for their organization.</td>
</tr>
<tr>
<td>UpdateOrgCommerceData</td>
<td>csp__update_org_commerce_data</td>
<td>User updated the Billing and Subscription details for their organization (currency, annual billing date, etc.)</td>
</tr>
<tr>
<td>UpdateOrgTaxId</td>
<td>csp__updated_org_tax_id</td>
<td>User updated the Tax ID in the Billing and Subscription details for their organization.</td>
</tr>
<tr>
<td>UpdateOrgPoReferenceNumber</td>
<td>csp__update_org_po_reference_number</td>
<td>User set a new organization PO reference number.</td>
</tr>
<tr>
<td>IncomingOrder</td>
<td>csp__incoming_order</td>
<td>Caller created an order for a service subscription.</td>
</tr>
</tbody>
</table>

### Table 6-5. Identity Governance and Administration

<table>
<thead>
<tr>
<th>Audit Event Name</th>
<th>Event Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ApproveDenyEntitlementRequest</td>
<td>csp__iga_entitlements_requests_approval</td>
<td>An entitlement request was approved or denied by organization owner.</td>
</tr>
<tr>
<td>CreateEntitlementRequest</td>
<td>csp__iga_register_entitlements_request</td>
<td>User created an entitlement request.</td>
</tr>
<tr>
<td>CreateEntitlementRequestForNonOrgMember</td>
<td>csp__iga_register_entitlements_request_non_org_member</td>
<td>New non organization user created an entitlement request.</td>
</tr>
<tr>
<td>CancelEntitlementRequest</td>
<td>csp__iga_delete_entitlement_request</td>
<td>User canceled an entitlement request.</td>
</tr>
<tr>
<td>CancelEntitlementRequestForNonOrg</td>
<td>csp__iga_delete_entitlement_request_non_org_member</td>
<td>New non organization user canceled an entitlement request that was already submitted by the same user.</td>
</tr>
<tr>
<td>EnablingGovernance</td>
<td>csp__iga_status_change</td>
<td>Identity Governance and Administration was enabled for organization.</td>
</tr>
<tr>
<td>UpdateGovernancePolicies</td>
<td>csp__iga_update_governance_policies_request</td>
<td>User updated Identity Governance and Administration policies.</td>
</tr>
</tbody>
</table>
Billing & Subscriptions

VMware Cloud Services organization owners can view billing and subscription details and manage payment methods for their organization. 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, and negotiated price of the commitments in the subscription. VMware Cloud Services invoices you according to the terms laid out in the purchase order.

You receive one monthly invoice 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 Subscription
- Managing Payment Methods
- Working with Subscriptions
- View Statements and Invoices

Getting Started with VMware Cloud Services Billing and Subscription

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 operating unit, currency, 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 **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.

**Note**  After onboarding the organization, you can change the default payment used to cover your invoices, but you can’t change the currency in which you are billed.

**Procedure**

1. Create your VMware Cloud Services account or log in if you already have one.

2. From the list of subscriptions and commitments that displays, select those that apply to your organization.

3. Click **Continue**.

4. On the **Create an Organization** step that opens, provide the billing details for your organization:
   a. Enter a name for your organization.
   b. Provide the address of your enterprise.
   c. Select the default payment method.

5. Click **Complete**.

**What to do next**

**Billing and Subscriptions Overview**

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.

<table>
<thead>
<tr>
<th>Overview</th>
<th>The <strong>Overview</strong> 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 view details for each seller. To learn more, see How Do I Get Billing Information for My Organization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manage Payment Methods</td>
<td>The <strong>Manage Payment Methods</strong> page allows you to add new payment methods to your organization and to change the default payment method. To learn more, see Managing Payment Methods</td>
</tr>
</tbody>
</table>
Subscriptions

The Subscriptions page displays details for all VMware Cloud Services subscriptions purchased in your organization.
To learn more, see Working with Subscriptions

Invoices & Statements

The Invoices & Statements page lets you view and download the activity statements and invoices for your organization.
To learn more, see View Statements and Invoices

Promotional Credits

The Promotional Credits page displays the available promotional credits that you can apply and redeem against the organization’s monthly costs.
To learn more, see Pay with Promotional Credits

How Do I Get Billing Information for My Organization

As an organization owner, you can view current accrued costs and charges for the past month for the services in your organization that have been purchased from VMware.

View your billing information by selecting Billing & Subscriptions on the Cloud Services Console.

Overview

<table>
<thead>
<tr>
<th>Current Costs</th>
<th>$80,200.00</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default Payment Method: Fund-1234 (VMware fund)</td>
<td></td>
</tr>
<tr>
<td>Aug 3 - Sep 2</td>
<td></td>
</tr>
</tbody>
</table>

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

- Payments: -$80,000.00
- Payment (August 1, 2020): -$75,000.00

Last Billing Period

Total last billing period: Jul 3 - Aug 2

- VMware Cloud on AWS: $80,000.00
- Network Insight: $2,000.00
- Promotional Credits: -$1,800.00
- Tax: $2,000.00
- Total: $82,200.00

The billing information for your organization is organized in three sections – Seller, Current Costs and Last Billing Statement.

Seller
The Seller section displays only if you have purchased services through multiple sellers. Each non-VMware seller is represented by a separate tile. To view information for a specific seller, click the Seller Details link in its tile. The overview information page for the seller opens to display details about the seller, and the services and subscriptions you purchased from them. You can also access the billing console for that seller where the cost information for your service usage resides.

### 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

<table>
<thead>
<tr>
<th>Description</th>
<th>Amount</th>
</tr>
</thead>
<tbody>
<tr>
<td>Current Costs</td>
<td>$80,200.00</td>
</tr>
<tr>
<td>Default Payment Method: Fund-1234 (VMware fund)</td>
<td></td>
</tr>
<tr>
<td>Aug 3</td>
<td>TODAY: $80,200.00</td>
</tr>
<tr>
<td>Sep 2</td>
<td></td>
</tr>
<tr>
<td>VMware Cloud on AWS</td>
<td>$79,200.00</td>
</tr>
<tr>
<td>Network Insight</td>
<td>$2,000.00</td>
</tr>
<tr>
<td>Promotional Credits (Estimated)</td>
<td>-$1,000.00</td>
</tr>
<tr>
<td>Total</td>
<td>$80,200.00</td>
</tr>
</tbody>
</table>

**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 discounts you might have received from the VMware Discount program.

**Last Billing Statement**
In the **Last Billing Statement** section, you can view itemized all 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 15th 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.

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](#).

To view and print any of your last 15 billing statements, on-demand invoices and yearly commitment invoices, click the **All Statements** link. For more information, see [View Statements and Invoices](#).

### 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.

<table>
<thead>
<tr>
<th>VMware Cloud service</th>
<th>How your current costs are estimated</th>
</tr>
</thead>
</table>
| 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.  
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.  
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. When you set up an organization, the address of your organization determines the currency in which you pay for the organization's services.

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?

- An organization can pay with a single currency. The address of the organization determines the payment currency of the organization’s transactions.

- 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 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.

- You can use any fund as 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.

VMware Cloud Services Selling Units

Use the information in these tables to determine the currency in which you are charged for your services.
### Table 7-1. Selling Unit IE for Non-US Customers

<table>
<thead>
<tr>
<th>If the address of your organization is in this country...</th>
<th>You are charged in...</th>
</tr>
</thead>
<tbody>
<tr>
<td>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,</td>
<td>USD</td>
</tr>
<tr>
<td>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</td>
<td>EUR</td>
</tr>
<tr>
<td>Gibraltar, Guernsey, Isle of Man, Jersey, United Kingdom,</td>
<td>GBP</td>
</tr>
<tr>
<td>Japan</td>
<td>JPY</td>
</tr>
<tr>
<td>China, Mongolia</td>
<td>CNY</td>
</tr>
<tr>
<td>Australia, Christmas Island, Cocos (Keeling) Islands, Norfolk Island</td>
<td>AUD</td>
</tr>
</tbody>
</table>

### Table 7-2. Selling Unit US for US Customers

<table>
<thead>
<tr>
<th>If the address of your organization is in this country</th>
<th>You are charged in</th>
</tr>
</thead>
<tbody>
<tr>
<td>United States of America</td>
<td>USD</td>
</tr>
</tbody>
</table>
Managing Payment Methods

Your customer profile 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 any credit card with any billing address to pay for your services. 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 enable 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. Learn more about Default Payment Method.

How Do I Add a New Payment Method

As an organization owner, you can add new payment methods to your organization. The payments defined at the organization's level become available to all organization owners.

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.

<table>
<thead>
<tr>
<th>To</th>
<th>Do this</th>
</tr>
</thead>
<tbody>
<tr>
<td>Link Pay by Invoice Accounts</td>
<td>Select one or more of the available Pay by Invoice accounts that you want to add and click Link Accounts.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> 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 enable unrestricted PBI by filing a support ticket.</td>
</tr>
<tr>
<td>Link VMware funds</td>
<td>Select one or more of the available VMware funds that you want to add as payment methods, then click Link Funds.</td>
</tr>
<tr>
<td>Add a Credit Card</td>
<td>Add the credit card details and click Add Card.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> 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.</td>
</tr>
</tbody>
</table>

**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 owners 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.

**How Do I Change My Organization's Default Payment Method**

As an organization owner, 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 to Pay by Invoice**

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

Once enabled, 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 Enable 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 enabled, 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 limitations to the use of credit cards based on the address of your organization and the billing address of your credit card. See the table below for more information.

**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.
Due to risk and fraud considerations, you cannot use a credit card as a payment method under the following circumstances.

<table>
<thead>
<tr>
<th>The address of your organization is in one of these countries.</th>
<th>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.</th>
</tr>
</thead>
<tbody>
<tr>
<td>The billing address of the credit card is in one of these countries.</td>
<td>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 Outlying Islands, Vatican City State, Venezuela, Mayotte, Zimbabwe.</td>
</tr>
</tbody>
</table>

You can add a credit card as a payment method when you onboard a cloud services, 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.

**How to Pay with Funds**

As an organization owner, you use VMware funds as a payment method for your VMware Cloud services by linking them to your organization.
VMware funds are a VMware-specific payment method that can be used to purchase services or products. Each fund is associated with a service or product order and 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.

**Important** You can use a fund as a payment method in your organization only if the currency of the fund is the same as the organization's currency, and it belongs to the same selling unit. For more information, see [How Is My Payment Currency Determined](#).

You link VMware funds as payment methods to your organization in the Cloud Services Console. You view and manage your linked funds through the MyVMware portal which requires access permissions. Only funds that are within your VMware Entitlement account can be associated with your VMware Cloud services organization. The currency of the fund must be the same as the currency used by your organization.

- To link a VMware fund in the Cloud Services Console, go to Billing and Subscriptions > Manage Payment Methods. For more information, see [Managing Payment Methods](#).
- To view details for a fund that is already linked as a payment method in your VMware Cloud services organization, click the ellipses icon next to the fund's name and select View Details on MyVMware.

For more information, see [Overview of My Funds Page, Fund Details Page and Navigation](#).

**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.

**Procedure**

1. On the Cloud Services Console, click Billing & Subscriptions > Promotional Credits.
2. Select the credit that you want to use, and click Activate.

   The credit is redeemed during the next billing period. You can check the balance of the promotional credit at any time.

**Working with Subscriptions**

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. Subscriptions allow you to save money by committing to buy a certain amount of capacity for a defined period through Subscription Purchase Program (SPP) or Pay by Invoice. You can purchase and use multiple commitments for each service in the subscription. The purchase order outlines the capacity, term, and negotiated price of the commitment. VMware Cloud Services invoices 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 Subscriptions Details for My Organization

Prerequisites
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.

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 subscription details as well as details about the term commitments purchased with the subscription.
How to Set Up a Commitment

If you are an organization owner, 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. Click the link in the email to apply your commitment to one of your current organizations or to a new organization.

For more information, see Why Do I Need to Apply Commitments to My Organization.

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 need to apply the newly purchased commitments to the organization of your choice.

When you purchase a commitment, the sales offer outlines the capacity, term, and negotiated price. As an organization owner, 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.
View Statements and Invoices

As an organization owner, 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.

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.

You view and download the invoices for the costs incurred by your organization from the Invoices tab of the Invoices and Statements page. The On-demand Invoices section lists billing costs for on-demand subscriptions and overages and the Term Commitment Invoices section lists the invoices for your subscription’s term commitments.
Expand the section for the selected service subscription, then download an invoice by clicking on its link, or by selecting an option from the vertical ellipsis icon next to it.

How to Read My Activity Statement

As an organization owner, 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.

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.

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.

**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 7-3. VMware Cloud Services Abbreviations Glossary**

<table>
<thead>
<tr>
<th>Product Name</th>
<th>Unit of Measure</th>
<th>Unit of Measure Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vRealize Automation Cloud</td>
<td>EA</td>
<td>Each</td>
</tr>
<tr>
<td></td>
<td>NDH</td>
<td>Node per Hour</td>
</tr>
<tr>
<td>vRealize Log Insight Cloud</td>
<td>EA</td>
<td>Each</td>
</tr>
<tr>
<td></td>
<td>NDH</td>
<td>Node per Hour</td>
</tr>
<tr>
<td></td>
<td>GB</td>
<td>Gigabyte</td>
</tr>
<tr>
<td>vRealize Network Insight Cloud</td>
<td>CPU</td>
<td>Central Processing Unit</td>
</tr>
<tr>
<td></td>
<td>GB</td>
<td>Gigabyte</td>
</tr>
<tr>
<td></td>
<td>EA</td>
<td>Each</td>
</tr>
<tr>
<td></td>
<td>VCP</td>
<td>Virtual Central Processing Unit</td>
</tr>
<tr>
<td>NSX Cloud</td>
<td>CRM</td>
<td>Core per Month</td>
</tr>
<tr>
<td></td>
<td>EA</td>
<td>Each</td>
</tr>
<tr>
<td>Tanzu Application Catalog</td>
<td>EA</td>
<td>Each</td>
</tr>
<tr>
<td>Tanzu Application Service</td>
<td>COH</td>
<td>Compute Unit Hour</td>
</tr>
<tr>
<td></td>
<td>EA</td>
<td>Each</td>
</tr>
<tr>
<td>VMware Cloud Director</td>
<td>CRM</td>
<td>Core per Month</td>
</tr>
<tr>
<td></td>
<td>EA</td>
<td>Each</td>
</tr>
<tr>
<td>VMware SD-WAN by VeloCloud</td>
<td>EA</td>
<td>Each</td>
</tr>
<tr>
<td>VMware Learning Platform</td>
<td>ALH</td>
<td>Active Lab Hour</td>
</tr>
<tr>
<td></td>
<td>BIH</td>
<td>Bring Your Own Cloud</td>
</tr>
<tr>
<td></td>
<td>COH</td>
<td>Compute Unit Hour</td>
</tr>
</tbody>
</table>
## Table 7-3. VMware Cloud Services Abbreviations Glossary (continued)

<table>
<thead>
<tr>
<th>Product Name</th>
<th>Unit of Measure</th>
<th>Unit of Measure Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>VMware Cloud on AWS</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>EA</td>
<td>Each</td>
<td></td>
</tr>
<tr>
<td>STH</td>
<td>Storage Unit Hour</td>
<td></td>
</tr>
<tr>
<td>WIH</td>
<td>Windows Unit Hour</td>
<td></td>
</tr>
<tr>
<td><strong>VMware Cloud on AWS GovCloud (US)</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>EA</td>
<td>Each</td>
<td></td>
</tr>
<tr>
<td>GB</td>
<td>Gigabyte</td>
<td></td>
</tr>
<tr>
<td>GBM</td>
<td>Gigabyte Month</td>
<td></td>
</tr>
<tr>
<td>HST</td>
<td>Host</td>
<td></td>
</tr>
<tr>
<td>HPH</td>
<td>Host per Hour</td>
<td></td>
</tr>
<tr>
<td>IPR</td>
<td>IP Address per Hour</td>
<td></td>
</tr>
<tr>
<td>IP</td>
<td>IP Address</td>
<td></td>
</tr>
<tr>
<td>VMH</td>
<td>Virtual Machine per Hour</td>
<td></td>
</tr>
<tr>
<td><strong>VMware Cloud on DELL EMC</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>EA</td>
<td>Each</td>
<td></td>
</tr>
<tr>
<td>NDM</td>
<td>Node per Month</td>
<td></td>
</tr>
<tr>
<td>EDM</td>
<td>Edge per Month</td>
<td></td>
</tr>
<tr>
<td><strong>vRealize Operations Cloud</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>EA</td>
<td>Each</td>
<td></td>
</tr>
<tr>
<td>OSI</td>
<td>Operating System Instance</td>
<td></td>
</tr>
</tbody>
</table>
How Do I Get Support

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.

2. Access the level of support you require.

   The Support panel provides contextual help content and a powerful search to enable you to search for 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.
<table>
<thead>
<tr>
<th>Access this support feature...</th>
<th>To help you...</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Intelligent search.</td>
<td>Search our content to find answers to your question. We search through our documentation, specially written help topics, communities, and knowledge-based articles.</td>
</tr>
<tr>
<td>2. Page-relevant content.</td>
<td>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 Based articles, content from our Documentation Center, and content from our communities. 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.</td>
</tr>
<tr>
<td>3. Chat with VMware Support.</td>
<td>Contact our support engineers and customer support representatives. You can continue to interact with VMware Cloud Services while chatting with our customer support engineers. Customer support engineers can also help you open a support request.</td>
</tr>
<tr>
<td>4. Support requests.</td>
<td>Create and manage support requests.</td>
</tr>
<tr>
<td>5. Ask the Community.</td>
<td>Engage and pose questions to actively moderated communities backed by passionate VMware support engineers and experts around the globe.</td>
</tr>
<tr>
<td>6. Service Health.</td>
<td>Review the live status of your VMware Cloud services, and receive important service notifications.</td>
</tr>
</tbody>
</table>

3 To manage your support requests, open a new support request and even search for answers to your questions, access the Support Center from the Cloud Services Console.

You must have a support role to access the Support Center. To get the required permissions to open and manage support tickets for your organization, contact your organization owner.

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.
When you manage your support requests, you do so within the context of your currently active organization. If you belong to several organizations, make sure that the organization for which you want to manage the request is your active organization. See, Access One of Your Other Organizations.