Remove a Cloud Service Provider From Multicloud Defense

Use the following procedures to terminate comunications and permissions between Multicloud Defense and your cloud service provider. This action includes removing any gateways or Vnets that have been created within the Multicloud Defense Controller as well as any roles or perissions you have set up within you cloud service provider. You must perform **all** of the steps for a complete cleanup of every Multicloud Defense instance.

Note that some of these procedures do not occur in the Multicloud Defense Controller and that you may need access to the cloud service provider's dashboard to execute these procedures.

Delete a GCP Project From Multicloud Defense

Use the following procedure to delete a GCP account from the Multicloud Defense Controller and remove all instances of Multicloud Defense from your GCP project. You must delete any subnets, VNets, or gateways created in the Multicloud Defense Controller prior to deleting Multicloud Defense from your account.

Note This procedure requires you to remove orchestration preparation from both the Multicloud Defense UI and the GCP dashboard.

Step 1 Delete any curent gateways or VNets from Multicloud Defense:

a) In the Multicloud Defense Controller, navigate to **Manage** > **Gateways** > **Gateways**.

b) Select the gateway associated with the account so its checkbox is checked.

c) Expand the **Actions** drop-down menu and select **Delete.**

d) Confirm the deletion.

e) In the Multicloud Defense Controller, navigate to **Manage** > **Gateways** > **Service VPCs/VNets**.

f) Select the VPCs associated with the account so the checkbox is checked.

      g) Expand the **Actions** drop-down menu and select **Delete.**

      h) Confirm the deletion.

> **Note**   You do not have to delete any affiliated subnets after you delete the VPC and gateway.

Step 2   Delete the GCP project from Multicloud Defense Controller.

      a) In the Multicloud Defense Controller, navigate to **Manage** > **Cloud Accounts** > **Accounts**.

      b) Select the Azure account so the checkbox is checked.

      c) Expand the **Actions** drop-down menu and select **Delete.**

      d) Confirm the deletion.

Step 3   Delete the Multicloud Defense Controller service account from GCP.

      a) Log into the GCP dashboard.

      b) Open IAM in your GCP project.

      c) In the navigation pane to the left, click **Service Accounts**.

      d) Select the project associated with the Multicloud Defense.

      e) Under the **View by Principals** tab, search for the `ciscomcd-controller`.

      f) Click the row's checkbox is checked and then click **Delete**.

Step 4   Delete the Multicloud Defense firewall service account from GCP.

      a) Log into the GCP dashboard.

      b) Open IAM in your GCP project.

      c) In the navigation pane to the left, click **Service Accounts**.

      d) Select the project associated with the Multicloud Defense.

      e) Under the **View by Principals** tab, search for the `ciscomcd-gateway`.

      f) Click the row's checkbox is checked and then click **Delete**.

Delete an AWS Account From Multicloud Defense

Use the following procedure to completely remove an AWS account from your Multicloud Defense.

After you delete the AWS account, it may take up to 24 hours for the cloud service provider to clean up all objects within the S3 bucket that is associated with your account.

Step 1   Log into CDO and launch the Multicloud Defense Controller.

Step 2   Navigate the top menu bar to **Manage** > **Gateways**.

Step 3   Locate the gateway associated with your account and select the checkbox, then click the **Actions** drop-down menu.

Step 4   Select **Disable**. This action automatically removes all virutal machines associated with the account.

Step 5   Make sure the gateway's checkbox is still selected and click the **Actions** drop-down menu again.

Step 6   Select **Delete**. This action removes the load balancers associated with the AWS account.

Step 7   Navigate to **Manage** > **Cloud Accounts** > **Accounts**.

Step 8   Locate the AWS account in the list and select it so the checkbox is check.

Step 9   Click the **Actions** drop-down menu and select **Delete**.

Step 10   Confirm you want to delete the account.

Delete an Azure Account From Multicloud Defense

Use the following procedure to remove any and all instances of the Azure account from Multicloud Defense:

Before you begin

You must delete any subnets and VNets created in the Multicloud Defense Controller prior to deleting Multicloud Defense from your Azure account.

Note   This procedure requires you to remove orchestration preparation from both the Multicloud Defense UI and the GCP dashboard.

Step 1   Log into CDO and launch the Multicloud Defense Controller.

Step 2   If you did not create a user-assigned Managed Identity for the key vault, continue to step 4. If you **did** create a key for the Azure account, do the following:

a)   Navigate to **Manage** > **Security Policies** > **Certificates**.
b)   Select the certificate associated with the account and then open the **Actions** drop-down menu.
c)   Select **Delete** and confirm the deletion of the certificate for the key vault.

Step 3   In the Multicloud Defense Controller, delete any gateways or VNets associated with the account.

a)   Navigate to **Manage** > **Gateways** > **Gateways** to delete any gateways previously created.
b)   Select the gateway associated with the account so its checkbox is checked.
c)   Expand the **Actions** drop-down menu and select **Delete.**
d)   Confirm the deletion.
e)   In the Multicloud Defense Controller, navigate to **Manage** > **Gateways** > **Service VPCs/VNets** to delete any VNets previously created.
f)   Select the VNet associated with the account so the checkbox is checked.
g)   Expand the **Actions** drop-down menu and select **Delete.**
h)   Confirm the deletion.
i)   In the Multicloud Defense Controller, navigate to **Manage** > **Cloud Accounts** > **Accounts**.
j)   Select the Azure account so the checkbox is checked.
k)   Expand the **Actions** drop-down menu and select **Delete**.
l)   Confirm the deletion.

Step 4   Delete the Multicloud Defense Controller role in Azure.

a)   Log into the Azure portal.
b)   Navigate to **App Registrations**.
c)   Select the **Owned Appications** tab.
d)   Select the **ciscomcd-controller-app** application.
e)   Once selected, click **Delete** at the top of the window.
f)   Confirm the deletion.

  g) Navigate to, or search for, **Subscriptions** and click **Access Control (IAM)**.

  h) Select the **Roles** tab at the top of the window.

  i) Search for **ciscomcd-controller-role-rw** and select it so the chekcbox is checked.

  j) Click **Remove** at the top of the window.

Delete an OCI Account From Multicloud Defense

Use the following procedure to remove an OCI cloud environment from Multicloud Defense:

Step 1   Log into the OCI console.

Step 2   Delete the API key. See the "**Deleting API Signing Keys from a Roving Edge Infrastructure Device**" chapter in the Oracle Cloud Infrastructure Documentation for more information.

Step 3   Delete Multicloud Defense Users. See the "**Deleting a User**" chapter in the Oracle Cloud Infastructure Documentation for more information.

> **Note**   When you remove the user from the OCI account, this does not delete the audit data of the user from when it was valid.

Step 4   Delete the Multicloud Defense Group. See the "**Deleting Groups**" chapter in the Oracle Cloud Infastructure Documentation for more information.

Step 5   Delete any and all Multicloud Defense access policies. See the "**Deleting an Access Policy**" chapter in the Oracle Cloud Infastructure Documentation for more information.

Step 6   Delete the OCI account from Multicloud Defense Controller. .

  a) In the Multicloud Defense Controller, navigate to **Manage** > **Cloud Accounts** > **Accounts**.

  b) Select the OCI account so the checkbox is checked.

  c) Expand the **Actions** drop-down menu and select **Delete.**

  d) Confirm the deletion.