Setup with the Multicloud Defense Wizard

The Multicloud Defense Controller provides a SaaS-delivered centralized control plane to deploy and manage Multicloud Defense and its security policy.

The **Setup** helps guide users through the process of setting up Multicloud Defense security using a series of these simple steps:

- **Connect your Account** - This process onboards your cloud service provider account to Multicloud Defense and simultaneously discovers regions and additional inventory and assets affiliated with your account.
- **Enable Traffic Visibility** - Utilizing the easy setup method enables the collection of logs to understand the flow of traffic.
- **Secure Your Account** - This procedure facilitates setting up a VNET or VPC, depending on the cloud account you have, and a Multicloud Defense Gateway to secure your experience.

- Connect Cloud Account, on page 1
- Enable Traffic Visibliity, on page 7
- Secure Your Account, on page 9

Connect Cloud Account

The first step is to onboard a set of one or more coud accounts. This allows the Multicloud Defense Controller to interact with each account by discovering inventory, enabling traffic and logs, orchestrating security deployment, and creating and managing policy.

Use the following procedures to connect you cloud service provider account to Multicloud Defense Controller.

Connect AWS Account

Use the following procedure to connect to an AWS subscription through Multicloud Defense's easy setup wizard.

Before you begin

- You must have an active Amazon Web Services (AWS) account.
- You must have an Admin or Super Admin user role in your CDO tenant.

- You must have Multicloud Defense enabled for your CDO tenant.

Note Multicloud Defense Controller version 23.10 defaults to IMDSv2 in the AWS EC2 instance when using Multicloud Defense Gateway version 23.04 or newer. For more information about the difference beween IMDSv1 and IMDSv2, see AWS documentation.

Step 1 From the Multicloud Defense Controller dashboard, click **Setup** located to the left of the window.

Step 2 Select **Connect Account**.

Step 3 Select the AWS icon.

Step 4 Enter the following information in the modal:

a) Click **Launch Stack** to download and deploy our CloudFormation template. This should open up another tab to deploy the template. Login to AWS is required.

b) Copy and paste the controller IAM role ARN from the CloudFormation stack output in the CloudFormation template.

c) In the Multicloud Defense Controller easy setup modal, enter the **AWS Account Number**. This number can be found in the output value **Current Account** of the CloudFormation Template.

d) Enter an **Account Name** that will be assigned to your account in the Multicloud Defense Controller.

e) (Optional) Enter an account **Description**.

f) Enter the **External ID**. This is a random string for IAM role's trust policy. This value will be used in the controller IAM role created. You can edit or regenerate the External ID.

g) Enter the **Controller IAM Role**. This is the IAM role created for the Multicloud Defense Controller during CloudFormation Template (CFT) deployment. Look for the output value MCDControllerRoleArm in CFT stack. It should be something similar to this: `arn:aws:iam::<Acc Number>:role/ciscomcdcontrollerrole`.

h) Enter the **Inventory Monitor Role**. This is the IAM role created for Multicould Defense Inventory during CFT deployment. Look for the output value MCDInventoryRoleArn in CFT stack. Should be something similar to this: `arn:aws:iam::<Acc Number>:role/ciscomcdinventoryrole`.

Step 5 Click **Next**. The account is onboarded to the Multicloud Defense Controller.

What to do next

Once you've connected the account, Multicloud Defense Controller automatically starts to discover assets and inventory associated with the cloud service provider account. Note that this is different from discovering traffic. Because Multicloud Defense Controller discovers account assets and inventory by default, the next step in this wizard is to Enable Traffic for an Azure Account.

Connect Azure Account

Use the following procedure to connect to an Azure subscription through Multicloud Defense Controller's easy setup wizard:

Before you begin

- You must have an active Azure subscription.
- You must have an Admin or Super Admin user role in your CDO tenant.

- You must have Multicloud Defense enabled for your CDO tenant.

Step 1 In the CDO dashboard, click the **Multicloud Defense** tab located in the left naviation pane.

Step 2 Click **Multicloud Defense Controller** located in the upper right window.

Step 3 From the Multicloud Defense Controller dashboard, click **Setup** located to the left of the window.

Step 4 Select **Connect Account**.

Step 5 Select the Azure icon.

Step 6 Enter the following information in the modal:

a) Click the link to open an Azure Cloud Shell in bash mode.
b) In the Azure account modal, click **Copy** to copy the onboading script and execute it in the bash shell that was opened in step 1.
c) In the Azure account modal, provide a name for this Azure account. You can choose to name this the same as your Azure subscription name. This name is visible on the Multicloud Defense Controller accounts page only.
d) (Optional) Provide a description for the subscription.
e) Enter the **Directory ID**, also referred as the Tenant ID.
f) Enter the **Subscription ID** for the subscription being onboarded.
g) Enter the **Application ID**, also referred to as the Client ID, created by the onboarding script.
h) Enter the **Client Secret**, also referred to as the Secret ID.

Step 7 Click **Next**.

What to do next

Once you've connected the account, Multicloud Defense Controller automatically starts to discover assets and inventory associated with the cloud service provider account. Note that this is different from discovering traffic. Because Multicloud Defense Controller discovers account assets and inventory by default, the next step in this wizard is to Enable Traffic for an Azure Account.

Connect Google Cloud Platform Account

Use the following procedure to use the Multicloud Defense Controller's easy setup wizard to onboard a singular GCP project as an account:

Before you begin

- You must have an active Google Cloud Platform (GCP) project.
- You must have the necessary permissions to create VPCs, subnets, and a service account withint your GCP project. See GCP doucmentation for more information.
- You must have an Admin or Super Admin user role in your CDO tenant.
- You must have Multicloud Defense enabled for your CDO tenant.

Step 1 From the Multicloud Defense Controller dashboard, click **Setup** located to the left of the window.

Step 2 Select **Connect Account**.

Step 3 Select the GCP icon.

Step 4 Click the **Cloud Platform Cloud Shell** to launch the Cloud Shell. Alternatively, log into your GCP account and launch the Cloud Shell from the project you want to connect to Multicloud Defense; note that the script automatically modifies the project name to the name of the project you launch the cloud shell from.

a) Copy the command generated in the Multicloud Defense Controller easy setup modal and paste the command into the Cloud Shell. Execute it to initiate the onboarding process. This script automatically creates user accounts for the Multicloud Defense Controller to communicate directly with your GCP project.

b) If you have multiple GCP projects, you are prompted to select the project via a numbered list. Select the value for the project you want to connect and submit.

c) When prompted with `Continue configuring this project? [y/n]` note that you only need to type either "y" or "n". Do not hit **enter** to submit your selection.

Note that if the GCP project you are connecting to Multicloud Defense has been previously onboarded, you may get an error about the GCP could storage bucket already existing. If that is not amenable, create a new storage bucket in your GCP account to handle the flow logs on this project afer it is connected to Multicloud Defense.

Step 5 Enter the following information in the setup modal:

a) Enter the **GCP Account Name**. This name is displayed only in Multicloud Defense.

b) (Optional) Enter a **Description**.

c) Enter the **Project ID** for the GCP project. This can be found at the top of the private key generated by the script from step 1.

d) Enter the **Client Email** for the service account created as part of the onboarding process. This is included in the private key generated by the script from step 1.

e) Copy and paste the **Private key** of the service account from the script output.

Step 6 Click **Next**.

What to do next

GCP does not automatically include the regions your project is confugred for. After your project is connected to Multicloud Defense we **strongly** recommend going to **Manage** > **Inventory** to manually modify and add any and all appropriate regions.

Once you've connected the account, Multicloud Defense Controller automatically starts to discover assets and inventory associated with the cloud service provider account. Note that this is different from discovering traffic. Because Multicloud Defense Controller discovers account assets and inventory by default, the next step in this wizard is to Enable Traffic for an Azure Account.

Connect to an OCI Account

Read through the following procedures and prepare your OCI account before you connect it to Multicloud Defense.

Prepare Your OCI Account

This procedure automates the connection between Multicloud Defense and your OCI account; it also directs you to create a policy with the correct permissions. Without all of the permissions listed as part of the procedure, some features are unavailable.

Execute the following procedure to connect to an Oracle Cloud (OCI) account with Multicloud Defense's setup wizard:

Step 1 Log into your OCI tenant.

Step 2 Navigate to **Identity & Security** > **Groups**.

Step 3 Click **Create Group**.

Step 4 Enter the following:

- **Name:** Multicloud Defense-controller-group
- **Description:** Multicloud Defense Group

Step 5 Click **Create**.

Step 6 Create a Network Firewall Policy in OCI. See OCI documentation for information but include the following information when creating the policy;

- **Name:** Multicloud Defense-controller-policy.
- **Description:** Multicloud Defense Policy.
- **Compartment:** [Must be the "root" Compartment].

a) Add the following permissions under the **Show Manual Editor** tab:

```
Allow group <group_name> to inspect instance-images in compartment <compartment_name>
Allow group <group_name> to read app-catalog-listing in compartment <compartment_name>
Allow group <group_name> to use volume-family in compartment <compartment_name>
Allow group <group_name> to use virtual-network-family in compartment <compartment_name>
Allow group <group_name> to manage volume-attachments in compartment <compartment_name>
Allow group <group_name> to manage instances in compartment <compartment_name>
Allow group <group_name> to {INSTANCE_IMAGE_READ} in compartment <compartment_name>
Allow group <group_name> to manage load-balancers in compartment <compartment_name>
Allow group <group_name> to read marketplace-listings in tenancy
Allow group <group_name> to read marketplace-community-listings in tenancy
Allow group <group_name> to inspect compartments in tenancy
Allow group <group_name> to manage app-catalog-listing in compartment <compartment_name>
Allow group <group_name> to read virtual-network-family in tenancy
Allow group <group_name> to read instance-family in tenancy
Allow group <group_name> to read load-balancers in tenancy
```

- **group_name:** Multicloud Defense-controller-group.
- **compartment_name:**[Compartment where Multicloud Defense will be deployed].

Note When replacing the **<compartment_name>** with the name of the compartment where the policy will apply, if the compartment is a sub-compartment, the name format is **compartment:sub-compartment** (e.g., Prod:App1).

If the **<compartment_name>** is specified as the root compartment (e.g., multicloud (root)), OCI will not accept the policy and will produce an error: *Invalid parameter*. The policy will need to be defined for an specific compartment and that compartment cannot be the root compartment.

b) Click **Create**.

Step 7 Create a User in OCI. See OCI documentation for more information, but provide the following configuration information when creating a user:

- **Name:** *Multicloud Defense-controller-user*
- **Description:** *Multicloud Defense User*

Step 8 Create an API Key. See OCI documentation for more information.

Be sure to download both the private key and the public key before you add the API Key.

Step 9 Accept the **Terms and Conditions** for an OCI account. See OCI documentation for more information, and be sure to access the **Change image** section of the UI to add the following "community image" information specific to Multicloud Defense:

a) **Check the box** for Multicloud Defense.
b) **Check the box** for *I have reviewed and accept the Publishers terms of use, Oracle Terms of Use, and the Oracle General Privacy Policy*.
c) We **strongly** recommend clicking **Exit** without deploying the image prior to connecting the account to Multicloud Defense

You may have to repeat the steps for each Compartment you plan to deploy a Multicloud Defense Gateway.

Connect Oracle Account

Use the following procedure to connect to an OCI account through Multicloud Defense Controller's easy setup wizard:

Before you begin

- You must have an existing Oracle Cloud (OCI) account.
- You must have the prerequisites for you OCI account completed prior to onboarding. See Prepare Your OCI Account, on page 4 for more information.
- You must have an Admin or Super Admin user role in your CDO tenant.
- You must have Multicloud Defense enabled for your CDO tenant.

Step 1 From the Multicloud Defense Controller dashboard, click **Setup** located to the left of the window.

Step 2 Select **Connect Account**.

Step 3 Select the OCI icon.

Step 4 Click **Oracle Cloud Shell** to launch the native shell prompt.

Step 5 Copy the command provided in the Multicloud Defense Setup wizard and paste it into your cloud shell. Execute the command.

This command automates the process of creating an IAM policy, OCI group, and an OCI user that facilitate the communication between your OCI account and the Multicloud Defense.

Step 6 Enter the following information in the setup modal:

a) Enter an **OCI Account Name**. This name is used only within the Multicloud Defense Controller and used for idenfitication purposes.
b) (Optional) Enter a **Description** of your account.

c) Enter you **Tenancy OCID** . This is your Tenancy Oracle Cloud Identifier obtained from the OCI User.
d) Enter the **Private Key** that is assigned to the OCI User.

Step 7 Click **Next**.

What to do next

Once you've connected the account, Multicloud Defense Controller automatically starts to discover assets and inventory associated with the cloud service provider account. Note that this is different from discovering traffic. Because Multicloud Defense Controller discovers account assets and inventory by default, the next step in this wizard is to Enable Traffic for an Azure Account.

Enable Traffic Visibliity

Enabling traffic visibility provides awareness into the traffic flows within the Cloud Accounts by collecting the following logs:

- NSG Flow Logs
- (**AWS only**) VPC Flow Logs
- DNS Logs
- Route53 Query Logging

The flow and DNS query logs are used by Multicloud Defense to understand traffic flow, correlate with threat intelligence feeds, and provide insight into existing threats that can be protected using Multicloud Defense.

Enabling traffic visibility is a different process for every cloud account type, but typically you will need to identiy account characteristics such as your cloud account's region, VPC/VNet you want to monitor, network security groups, and a cloud storage account for logs.

Enable Traffice for an AWS Account

Use the following procedure to enable traffic visibility for an AWS account with the Setup wizard:

Step 1 In the Multicloud Defense Controller portal click **Setup** in the left navigation bar.

Step 2 In the setup wizard, click **Enable Traffic Visibility**.

Step 3 Enter the following information into the modal:

a) **CSP Account** - Use the drop-down menu to select the cloud service provider account to which Multicloud Defense Controller deploys the Service VPC/VNet.
b) **Region** - Use the drop-down menu to select the region where the cloud service provider you selected is located.
c) **VPCs** - Scroll through the table of available available VPCs that are applicable to the type of cloud service provider you selected and check the appropriate VPC. Note that if you do not immediately see the VPC, click the **Refresh** icon to refresh the current list.
d) **S3 Bucket** - Use the drop-down menu to select an existing S3 bucket from your account; this is where DNS queries and VPC/VNet flow logs are stored. This S3 bucket was created in the previous step.

Step 4 Click **Next**.

What to do next

Secure your account.

Enable Traffic for an Azure Account

Use the following procedure to enable traffic visibility for an Azure account from the Setup wizard:

Step 1 In the Multicloud Defense Controller portal click **Setup** in the left navigation bar.

Step 2 In the setup wizard, click **Enable Traffic Visibility**.

Step 3 Enter the following information into the modal:

a) **CSP Account** - Use the drop-down menu to select the cloud service provider account to which Multicloud Defense Controller deploys the Service VPC/VNet.

b) **Region** - Use the drop-down menu to select the region where the cloud service provider you selected is located.

c) **Copy and run the script**. Note that if you are re-onboarding an Azure account and are reusing a cloud storage bucket, the script does not automatically create a new storage bucket. It is possible to use the default, or preexisting storage bucket, but otherwise you must create a new storage bucket in the Azure dashboard or manually edit this script command prior to executing to include the name of the storage bucket you want the flow logs for your account to be stored in.

d) **NSGs** - Select at least one network security group (NSG) for traffic to be visible on. Scroll through the table of available available NSGs that are applicable to the type of cloud service provider you selected and check the appropriate NSG. Note that if you do not immediately see the NSG, click the **Refresh** icon to refresh the current list.

e) **Storage Account** - eEnter the full Resource ID in the selected region above.

Step 4 Click **Next**.

What to do next

Secure your account.

Enable Traffic for a GCP Project

Use the following procedure to enable traffic visibility for a GCP account with the Setup wizard:

Step 1 In the Multicloud Defense Controller portal click **Setup** in the left navigation bar.

Step 2 In the setup wizard, click **Enable Traffic Visibility**.

Step 3 Enter the following information into the modal:

a) **CSP Account** - Use the drop-down menu to select the cloud service provider account to which Multicloud Defense Controller deploys the Service VPC/VNet.

b) **Cloud Storage** - Select an available cloud storage bucket that has already been assigned to the GCP project you selected.

c) **Select VPC(s)** - Select at least one VPC for traffic to be visible on. Scroll through the table of available available VPCs that are applicable to the type of cloud service provider you selected and check the appropriate VPC. Note that if you do not immediately see the VPC, click the **Refresh** icon to refresh the current list.

d) **Copy and run the script**. Note that if you are re-onboarding a GCP project and are reusing a cloud storage bucket, the script does not automatically create a new storage bucket. It is possible to use the default, or preexisting storage bucket, but otherwise you must create a new storage bucket in the GCP dashboard or manually edit this script command prior to executing to include the name of the storage bucket you want the flow logs for your GCP project to be stored in.

Step 4 Click **Next**.

What to do next

Secure your account.

Enable Traffic for an OCI Account

Use the following procedure to enable traffic visibility for an OCI account from the Setup wizard:

Step 1 In the Multicloud Defense Controller portal click **Setup** in the left navigation bar.

Step 2 In the setup wizard, click **Enable Traffic Visibility**.

Step 3 **CSP Account** - Use the drop-down menu to select the cloud service provider account to which Multicloud Defense Controller deploys the Service VPC/VNet.

Step 4 **Region** - Use the drop-down menu to select the region where the cloud service provider you selected is located.

Step 5 Scroll through the table of available available VPCs that are applicable to the type of cloud service provider you selected and check the appropriate VPC. Note that if you do not immediately see the VPC, click the **Refresh** icon to refresh the current list.

Step 6 (Optional) Use the drop-down menu to select the S3 bucket in your account where DNS queries and VPC flow logs are stored. The S3 bucket selected is created by Multicloud Defense as part of the process when enabling traffic.

Step 7 Click **Next**.

What to do next

Secure your account.

Secure Your Account

Secure your account with a gateway deployed in either a centralized or a distributed model.

In a **Centralized** model, Multicloud Defense orchestrates and deploys a VPC or VNet to contain the gateway. This means that the VPC or VNet and all the additional components required are orchestrated as well as the deployment of the gateway within this construct.

In a **Distributed** model, Multicloud Defense builds and deploys a gateway within the existing infrastructure that your network already has available.

Continue with either of the procedures below to secure your account.

Centralized Model: Add a VPC or VNet

Use the following procedure to create and add a VPC or VNet to house your gateway and secure your account:

Before you begin

You must have at least one cloud service provider connected to the Multicloud Defense Controller before you begin this wizard. Note that this procedure changes for some providers based on their required parameters.

Step 1 In the Multicloud Defense Controller portal click **Setup** in the left navigation bar.

Step 2 In the setup wizard, click **Secure Account**.

Step 3 Select **Centralized** so it is highlighted.

Step 4 Click **Next**.

Step 5 Add a Service VPC/VNet:

a) **Name** - Enter a name for the service VPC/VNet. Once created, this name is displayed in the **Manage** > **Gateways** > **Service VPC/VNETS** page.

b) (AWS only)**CSP Account** - Use the drop-down menu to select a cloud service provider account that is already connected to the Multicloud Defense Controller. The Service VPC/VNet is deployed to the selected account.

c) **Region** - Use the drop-down menu to select the region where the selected cloud service provider is located.

d) **CIDR Block** - Enter the unique value for the Transit Gateway that the Service VPC/VNet is attaching to.

e) (GCP only) **Datapath CIDR Block** - Enter a valid CIDR block for datapath VPC which should not overlap with spoke VPCs.

f) (GCP only) **Management CIDR Block** - Enter a valid CIDR block for the management VPC.

g) **Availablity Zones** - Of the generated list, select at least one availability zone. We **strongly** recommend selected two zones for best results.

h) (Azure only) **Resource Group** - Use the drop-down menu to select a resource group to associate the gateway to. If there are none currently listed, you can **Create Resource Group** from this screen.

i) (AWS only) **Transit Gateway** - Use the drop-down menu to select an available transit gateway for the VPC to assocaite with. If you do not have one available, click **create_new** to create a transit gateway from this window.

j) (AWS and Azure only) **Use NAT Gateway** - check this option if you want all egress traffic to be directed through the NAT gateway. Multicloud Defense automatically creates a NAT gateway for each availability zone that is selected.

Step 6 Click **Next**.

What to do next

Add a Gateway.

Distributed Model

For a distributed gateway model, use the following procedures according to which cloud service provider you are using.

Azure Distributed Model: Create a Gateway

Use the following procedure to create a gateway for an Azure account with the distributed model:

Step 1 In the Multicloud Defense Controller portal click **Setup** in the left navigation bar.

Step 2 In the setup wizard, click **Secure Account**.

Step 3 Select **Distributed** so it is highlighted.

Step 4 Click **Next**.

Step 5 Enter the following Gateway Information:

a) **Account** - Use the drop-down menu to select an Azure account you want to deploy the gateway to.
b) **Name** - Enter a name for the gateway. This name is displayed in the **Manage** > **Gateways** page.
c) (Optional) **Description** - Enter a description for the gateway that might help identify it from other gateways.
d) **Instance Type** - Use the drop-down menu to select the instance type that deploys the Gateway.
e) **Minimum Instances** - Select the minimum number of instances deployed in auto scaling group per availability zone.
f) **Maximum Instance** - Select the maximum number of instances deployed in auto scaling group per availability zone.
g) **HealthCheck Port** - Enter the healthcheck port number. Multicloud Defense Controller uses `65534` as the default value.
h) **User Name** - Enter the user name used to access the gateway once created.
i) **Packet Capture Profile** - Use the drop-down menu to select where packets are stored in the cloud storage bucket. If there are no option listed, click **Create Packet Capture Profile** to create one from this window.
j) **Log Profile** - Use the drop-down menu to select which cloud service provider is used to forward logging to.
k) **Metrics Profile** - Use the drop-down menu to select an entity to forward metrics to. If there are no option listed, click **Create Metrics Forward Profile** to create one from this window.
l) **NTP Profile** - Use the drop-down menu to select the NTP profile associated with the gateway. If there are no options listed, click **Create** to create one from this window.
m) **Security** - Select the type of traffic flow your gateway is expected to handle. Ingress security targets traffic that flows from the public internet to a private network; east-west & egress security targets traffic that is outbound from your private network and traffic that moves between your data centers.
n) **Gateway Image** - Use the drop-down menu to select the gateway image to be deployed to the gateway.
o) **Policy Ruleset** - Use the drop-down menu to select a policy rulset to be deployed and start processing traffic. If there is not ruleset listed, click **Create new** to create a policy rulset from this window.
p) **Region** - Use the drop-down menu to select the region your gateway is deployed to.
q) **VPC/VNet ID** - Use the drop-down menu to select the VPC where the gateway is deployed to.
r) **Key Selection** - Select either an SSH Public key or an SSH Key Pair. Enter the value that is applied to the gateway in the next text field.
s) **Resource Group** - Use the drop-down menu to select an existing resource group that is applied to the gateway.
t) **User Assigned Identity ID** - Enter a valid value.
u) **Mgmt. Security Group** - Use the drop-down menu to select a security group used for the gateway management interface. Note that if you select a Multicloud Defense-created service VPC, a security group is created specifically for management.
v) **Datapath Security Group** - Use the drop-down menu to select a security group used for the gateway datapath interface. If selecting Multicloud Defense-created service VPC, a security group is created specifically for the datapath.
w) **Disk Encryption** - Enable disk encryption with either the Azure managed encryption or a customer-managed encryption key. Note that if you opt for a customer-managed encryption key, you need to create and deploy an IAM policy for successful deployment.
x) **Availability Zone** - Use the drop-down menu to select an availablilty zone.

y) **Mgmt. Subnet** - Use the drop-down menu to select a management subnet for the management interface.
z) **Datapth Subnet** - Use the drop-down menu to select a datapath subnet for the datapth interface.

To add more instance types, click the "+" icon. Subseuqntly, you can remove additional instance types with the "-" icon.

Step 6 Click **Next**.

Step 7 Enter the following Advanced Settings:

a)

Step 8 Click **Next**.

Step 9 Review

What to do next