Terraform

About Terraform

Multicloud Defense customers can use the **Terraform Provider** to: **discover** - onboard public cloud accounts, gain continuous asset visibility and detect indicators of compromise (IoC); **deploy** - Multicloud Defense Gateways to protect ingress, egress and east-west traffic; and **defend** - with multi-cloud (AWS, Azure, GCP, OCI) dynamic policies with continuously discovered cloud assets.

Attention As of Multicloud Defense Controller version 23.10, you can connect a GCP folder as well as a GCP project using the terraform provider. See Terraform Repository, on page 2 for more information.

The Multicloud Defense terraform provider is a “Verified” provider available from the terraform registry. Customers can now use the terraform provider for Multicloud Defense to bake security into their operations, i.e. on-board their cloud accounts into Multicloud Defense, deploy Multicloud Defense Gateways and specify security policies to protect against ingress attacks from the Internet (WAF, IDS/IPS, Geo-IP), stop exfiltration on egress traffic (TLS decryption, IDS/IPS, AV, DLP, FQDN/URL filtering), and prevent east-west attacks between VPCs/VNets. The security policies can be specified based on cloud asset tags (e.g., “dev”, “test”, “prod”, “pci”, “web”, “app1” etc.)

For more information, refer to:

- Download the Terraform Provider for Multicloud Defense (https://registry.terraform.io/providers/valtix-security/valtix/latest).
- Documentation (https://registry.terraform.io/providers/valtix-security/valtix/latest/docs).
- Examples in GitHub (https://github.com/valtix-security).
- Multicloud Defense Blog on Terraform (https://valtix.com/blog/official-hashicorp-terraform-provider/).

Terraform Repository

Use case	Description	Github Repository
AWS onboarding	This is for onboarding AWS account using Terraform.	Github Repo
AWS discovery CFT	This CFT deployment will include all necessary privileges needed to use Multicloud Defense's discovery feature. For full feature set, please use the in product CFT.	Github Repo
AWS discovery	This is for onboarding AWS account for discovery only mode using Terraform.	Github Repo
Azure onboarding	This is for onboarding Azure Subscription using Terraform.	Github Repo
GCP Project onboarding	This is for onboarding GCP project using Terraform.	Github Repo
GCP Folder onboarding	This is for onboarding GCP folder using Terraform.	Github Repo

Exporting Configuration as Terraform Block

Customers can export security profiles into terraform resource blocks from Multicloud Defense Controller. To export configuration into Terraform block, navigate and select the intended security profile and click on **Export** button. This will download a file that has the terraform block for the selected object/security profile.

All objects and profiles support terraform export with the exception of:

- Gateways
- Service VPCs/VNets
- Diagnostics