

Provisioning Multicloud Defense

Once you enrol for Multicloud Defense, Security Provisioning and Administration creates an account for your tenancy. Security Provisioning and Administration is a web application that provides centralized management of Cisco Secure product instances, user identity, and user access management across Cisco Security Cloud.

Refer to the Cisco Security Provisioning and Administration User Guide for more information for any of these steps for:

- Purchasing and claiming a subscription license.
- Activating the account or cloud instance on Security Cloud Control.

- Prerequisites for Multicloud Defense, on page 1
- Licensing and Support in Multicloud Defense, on page 1
- Set up Multicloud Defense, on page 2
- Architecture of Multicloud Defense, on page 3
- Multicloud Defense Workflow, on page 4

Prerequisites for Multicloud Defense

To use Multicloud Defense, you need to:

- Install and use a Chrome browser to view the Multicloud Defense controller dashboard.
- Upgrade to a Multicloud Defense Gateway version that specifically supports IMDSv2 in the **Required** mode for optimal security with Amazon EC2 instances.
- Activate Multicloud Defense in Security Cloud Control.

Licensing and Support in Multicloud Defense

When you log into your Security Cloud tenant, you will see a wizard that guides you through connecting your cloud accounts to Multicloud Defense so that you can manage them with a free 90-day trial of Multicloud Defense Controller. The 90-day trial experience offers the full functionality of a paid-subscription to Multicloud Defense Controller.

For paid licensing, see the Cisco Multicloud Defense Ordering Guide.

When you enrol with Multicloud Defense, you can provision and activate Multicloud Defense in Security Cloud Control. For more information, see the Cisco Security Provisioning and Administration User Guide.

Set up Multicloud Defense

Click **Get Started** to begin your 90-day trial. This begins the process of provisioning the Multicloud Defense Controller.

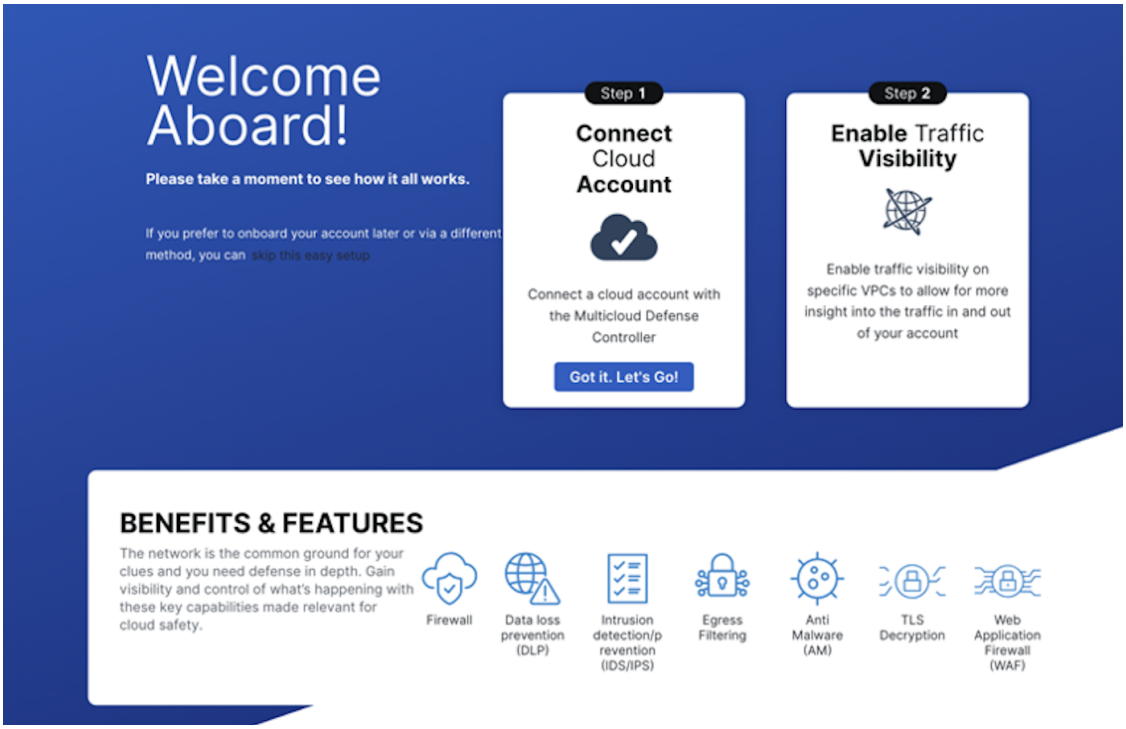
Easy Setup supports the following features for Cloud Providers:

- Account Onboarding: AWS, Azure, GCP, OCI.
- Enable Traffic Visibility: AWS (Flow Logs, DNS Query Logs), Azure (Flow Logs), GCP (VPC flow logs, DNS Query Logs).
- Create Services VPC/VNet: AWS, Azure, GCP.
- Create Gateways: AWS, Azure, GCP.

Cloud Account Easy Setup

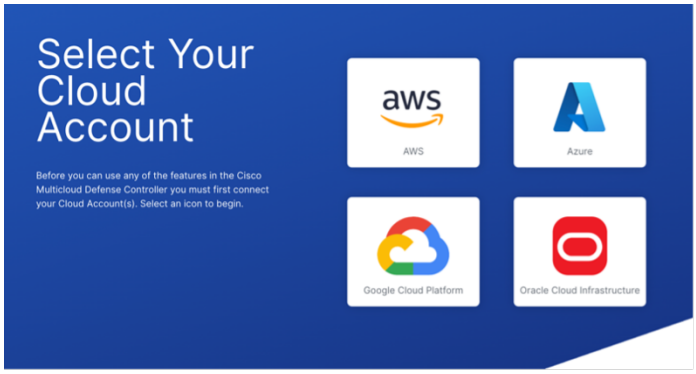
Once you log into Security Cloud Control, you can follow the on-screen guided wizard to set up your cloud account in Multicloud Defense.

Figure 1: On-screen guided wizard



Select your cloud account and provide details.

Figure 2: Select Your Cloud Account



The process of setting up Multicloud Defense security is a series of these simple steps:

- **Connect your Account:** Onboard your cloud service provider account to Multicloud Defense and simultaneously discover regions and additional inventory and assets affiliated with your account.
- **Enable Traffic Visibility:** Utilize the easy setup method to enable the collection of logs to understand the flow of traffic.
- **Secure Your Account:** -Set up a VNet or VPC, depending on the cloud account that you have, and a Multicloud Defense Gateway to secure your account.

Architecture of Multicloud Defense

Cisco Multicloud Defense has two main components:

- Multicloud Defense Gateways
- Multicloud Defense Controller.

Multicloud Defense Gateways

Multicloud Defense Gateway is a network-based security platform that contains network load balancers with a cluster of Multicloud Defense Gateway instances. Some of the key features are:

- Autoscaling and Self-healing: Operate as autoscaling, self-healing Platform-as-a-Service (PaaS), serving as inline network-based security enforcement nodes.
- Simplified Management: Eliminate the need for constructing virtual firewalls, configuring high-availability setups, or managing software installations.
- Advanced Security Profiles: Implement granular security profiles within a single pass datapath pipeline, without the need for traffic offloading to third-party engines.

Multicloud Defense supports these gateway use cases:

- Egress
- Ingress
- East-West

- Distributed
- Centralized / Hub
- Advanced Gateway Configuration: Use Your Own Load Balancer

To manage gateways, see the Multicloud Defense User Guide.

Multicloud Defense Controller

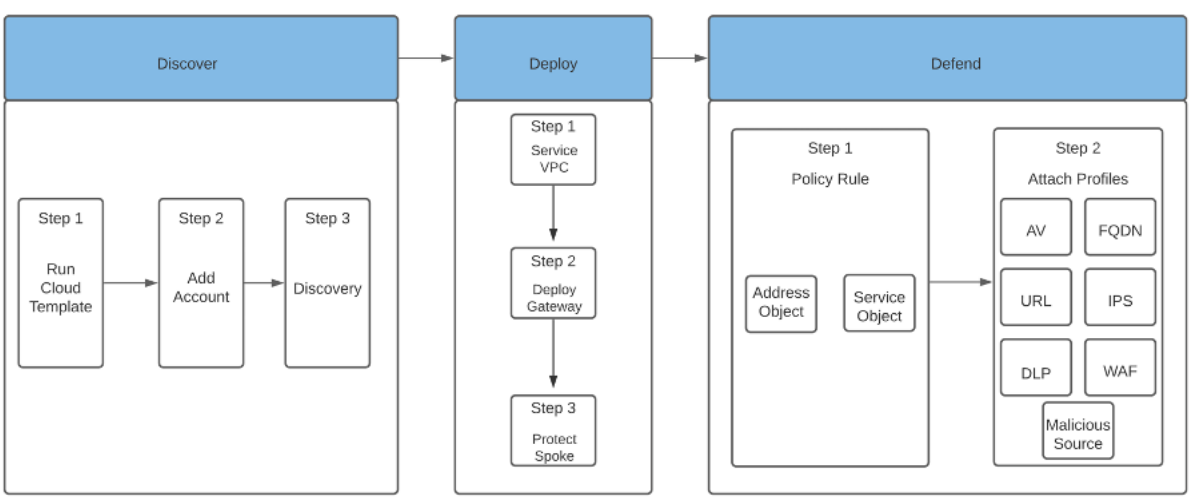
The Multicloud Defense Controller uses an architecture that contains:

- SaaS-based management: The Software-as-a-Service (SaaS) controller manages the Gateway stack and includes an API Server for orchestration of CSP load balancers (LBs) and Gateway Instances.
- Dynamic scaling: Facilitates dynamic horizontal scaling through instance additions and removals from the load balancer's "target pool," monitored for high availability.
- Continuous communication: Engages in continuous communication with Cloud Service Provider (CSP) accounts to keep security policies up-to-date.
- Dynamic policy and cloud-to-controller communication.
- Dynamic address objects: Uses cloud-native constructs to define dynamic address objects, automatically updating them as cloud resources change.
- Tag-based policy rules: Allows for granular policy rules based on instance tags, automatically inheriting security policies for new instances with appropriate tags.
- Full decryption using CSP-native key stores.
- Ensuring chain-of-custody: Multicloud Defense Gateways can directly access private keys stored in CSP-native key stores, such as Azure Key Vault, ensuring chain-of-custody, data sovereignty, and PKI adherence.
- Secure key management: Private keys remain within the organization's perimeter and are actively maintained by the key store.
- Proxies: These serve as intermediaries between clients and servers, facilitating various types of network communications. Cisco Multicloud Defense performs both reverse proxy and forward proxy functions.

Multicloud Defense Workflow

In Multicloud Defense, follow these series of steps to Discover, Deploy, and Defend your cloud securely.

Figure 3: Workflow of Discover, Deploy, and Defend



Discover contains the first phase of connecting your cloud accounts, by onboarding them and discovering all your cloud inventory and traffic. Deploy contains setting up your VPCs and Gateways and deploying them. Defend contains the final phase of creating and managing policies using rules, rulesets, and profiles, to enable protection.