



Onboard Devices and Services

You can onboard both live devices and model devices to Security Cloud Control. Model devices are uploaded configuration files that you can view and edit using Security Cloud Control.

Most live devices and services require an open HTTPS connection so that the Secure Device Connector can connect Security Cloud Control to the device or service.

This chapter covers the following sections:

- [Onboard an AWS VPC, on page 1](#)
- [Supported Devices, Software, and Hardware, on page 3](#)

Onboard an AWS VPC

To onboard an AWS VPC to Security Cloud Control, follow this procedure:

Before you begin



Note Security Cloud Control does not support peered AWS VPCs. If you attempt to onboard a peered VPC referencing a security group that is defined on the peer VPC, the onboarding process fails.

Before onboarding your Amazon Web Services (AWS) Virtual Private Cloud (VPC) to Security Cloud Control, review these prerequisites:

- To onboard an AWS VPC, you will need the AWS VPC's access key and secret access key both of which are generated using the Identity and Access Management (IAM) console. See [Understanding and Getting your Security Credentials](#) for more information.
- Configure the permissions to allow Security Cloud Control to communicate with your AWS VPC. See [Changing Permissions for an IAM User](#) for more information. See the following example for the required permissions:


```
"cloudformation:CreateStack",  
"cloudformation:CreateStackInstances",  
"cloudformation:DescribeStackInstance",  
"cloudformation:DescribeStackResource",  
"cloudformation:DescribeStackResources",  
"cloudformation:DescribeStacks",  
"ec2:AllocateAddress",
```

```

"ec2:AllocateHosts",
"ec2:AssignPrivateIpAddresses",
"ec2:AssociateAddress",
"ec2:AssociateDhcpOptions",
"ec2:AssociateRouteTable",
"ec2:AssociateSubnetCidrBlock",
"ec2:AttachInternetGateway",
"ec2:AttachNetworkInterface",
"ec2:AuthorizeSecurityGroupEgress",
"ec2:AuthorizeSecurityGroupIngress",
"ec2:CreateDhcpOptions",
"ec2:CreateEgressOnlyInternetGateway",
"ec2:CreateInternetGateway",
"ec2:CreateNetworkAcl",
"ec2:CreateNetworkInterface",
"ec2:CreateNetworkInterfacePermission",
"ec2:CreateRoute",
"ec2:CreateRouteTable",
"ec2:CreateSecurityGroup",
"ec2:CreateSubnet",
"ec2:CreateTags",
"ec2:DescribeAddresses",
"ec2:DescribeAddressesAttribute",
"ec2:DescribeAvailabilityZones",
"ec2:DescribeDhcpOptions",
"ec2:DescribeEgressOnlyInternetGateways",
"ec2:DescribeInstanceStatus",
"ec2:DescribeInstances",
"ec2:DescribeInternetGateways",
"ec2:DescribeNetworkAcls",
"ec2:DescribeNetworkInterfaceAttribute",
"ec2:DescribeNetworkInterfacePermissions",
"ec2:DescribeNetworkInterfaces",
"ec2:DescribeRegions",
"ec2:DescribeRouteTables",
"ec2:DescribeSecurityGroupReferences",
"ec2:DescribeSecurityGroupRules",
"ec2:DescribeSecurityGroups",
"ec2:DescribeSubnets",
"ec2:DescribeTags",
"ec2:DescribeTransitGatewayVpcAttachments",
"ec2:DescribeTransitGateways",
"ec2:DescribeVpcs",
"ec2:DescribeVpnGateways",
"ec2:ModifyNetworkInterfaceAttribute",
"ec2:ModifySecurityGroupRules",
"ec2:ModifySubnetAttribute",
"ec2:RunInstances",
"sts:GetCallerIdentity"

```

Procedure

- Step 1** In the left pane, click **Security Devices**.
- Step 2** Click  to begin onboarding the device.
- Step 3** Click **AWS VPC**.
- Step 4** Enter the Access Key ID and Secret Access Key credential to connect to the AWS account. The generated list of names are retrieved from the AWS VPC you supplied login credentials to.

- Step 5** Click **Connect**.
- Step 6** Select a Region From the drop-down menu. The region selected should be where the VPC is local to.
- Step 7** Click **Select**.
- Step 8** Use the drop-down menu to select the correct AWS name. The generated list of names are retrieved from the AWS VPC you supplied login credentials to. Select the desired AWS VPC from the drop-down menu. Note that AWS VPC IDs names are unique, and there cannot be two or more instances with the same ID.
- Step 9** Click **Select**.
- Step 10** Enter a name to be shown in the Security Cloud Control UI.
- Step 11** Click **Continue**.
- Step 12** (Optional) Enter a label for the device. Note that if you create labels for an AWS VPC, the tables are not automatically synchronized to your device. You must manually recreate the labels as tags in the AWS console. See [Labels and Tags in AWS VPC](#) for more information.
- Step 13** Click **Continue**.
- Step 14** Return to the **Security Devices** page. After the device has been successfully onboarded, you will see that the Configuration Status is "Synced" and the Connectivity state is "Online."

Related information:

- [Update AWS VPC Connection Credentials](#)
- [AWS VPC Policy](#)
- [AWS VPCs and Security Groups in Security Cloud Control](#)
- [Sharing Objects Between AWS and other Managed Devices](#)

Supported Devices, Software, and Hardware

Security Cloud Control is a cloud-based management solution enabling the management of security policies and device configurations across multiple security platforms. Security Cloud Control centrally manages policy and configuration across:

- Cisco Secure Firewall ASA, both on-premises and virtual
- Cisco Secure Firewall Threat Defense (FTD), both on-premises and virtual
- Cisco Catalyst SD-WAN Manager
- Cisco Secure Firewall Management Center, on-premises
- Cisco Meraki MX
- Cisco IOS devices
- Cisco Umbrella
- AWS Security Groups

The documentation describes devices, software, and hardware Security Cloud Control supports. It does not point out software and devices that Security Cloud Control does not support. If we do not explicitly claim support for a software version or a device type, then we do not support it.

Cisco Secure Firewall ASA

Cisco Adaptive Security Appliance (ASA) is a security device integrating firewall, VPN, and intrusion prevention capabilities. It protects networks from unauthorized access, cyber threats, and data breaches, offering robust security services in a single platform. Security Cloud Control supports the management of ASA devices, offering features to streamline configuration management and ensure regulatory compliance across the network infrastructure.

Cisco Secure Firewall Threat Defense

Firewall Threat Defense integrates traditional firewall features with advanced threat protection capabilities. It offers comprehensive security functions, including intrusion prevention, application control, URL filtering, advanced malware protection, and so on. An FTD can be deployed on ASA hardware appliances, and Cisco firewall hardware appliances, and in virtual environments. Managing threat defense devices is possible through various management interfaces, such as Cisco Firewall Management Center, Security Cloud Control, and Firewall Device Manager.

For more information on software and hardware compatibility, see the [Cisco Secure Firewall Threat Defense Compatibility Guide](#).

Firewall Device Manager is a web-based management interface explicitly designed for threat defense device management. It provides a simplified approach for configuring and monitoring threat defense devices, making it ideal for smaller-scale deployments or organizations preferring an intuitive interface.

FDM offers basic configuration capabilities for network settings, access control policies, NAT rules, VPN configuration, monitoring, and basic troubleshooting. Typically accessed through a web browser, FDM is directly available on the FTD device, eliminating the need for additional management servers or appliances.

Cisco Catalyst SD-WAN Manager

Security Cloud Control offers centralized management for Catalyst SD-WAN and Branch WAN environments, allowing organizations to efficiently configure, monitor, and enforce security policies across their networks. This integration also facilitates advanced troubleshooting, rule optimization, and change management on the Catalyst SD-WAN Manager.

For more information on software and hardware compatibility, see [Cisco Catalyst SD-WAN Device Compatibility](#).

Cisco Secure Firewall Management Center

Security Cloud Control simplifies the management of on-premises Firewall Management Center by establishing a secure integration, discovering security devices, and enabling centralized policy management. Security policies such as firewall rules, VPN settings, and intrusion prevention policies can be efficiently managed and deployed across all devices under FMC.

Cisco Meraki MX

The Meraki MX appliance is an enterprise-grade security and SD-WAN next-generation firewall appliance, designed for decentralized deployments. Security Cloud Control supports managing layer 3 network rules on Meraki MX devices. When you onboard a Meraki device to Security Cloud Control, it communicates with the Meraki dashboard to manage that device. Security Cloud Control securely transfers configuration requests to the Meraki dashboard, which then applies the new configuration to the device. Key features of Security Cloud Control's support for Cisco Meraki MX include centralized policy management, backup and restore, monitoring and reporting, compliance checking, and automation capabilities.

Cisco IOS Devices

Cisco IOS can manage and control network functions, including routing, switching, and other networking protocols. It offers a set of features and commands to configure and maintain Cisco network devices, enabling efficient communication and management within networks of varying sizes and complexities.

Cisco Umbrella

Security Cloud Control manages Cisco Umbrella through integrations such as the Umbrella ASA Integration, which allows administrators to include their Cisco Adaptive Security Appliance (ASA) within their Umbrella configuration using per-interface policies. This integration enables the ASA to redirect DNS queries to Umbrella, enhancing network security by leveraging Umbrella's DNS security, web filtering, and threat intelligence capabilities.

AWS Security Groups

Security Cloud Control offers a simplified management interface for Amazon Web Services (AWS) Virtual Private Clouds (VPCs). Key features include monitoring AWS Site-to-Site VPN connections, tracking changes to AWS devices, and viewing AWS Site-to-Site VPN tunnels.

