



## 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](#)

## 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](#)

