# Configuring AWS Devices

This chapter covers the following sections:

- Update AWS VPC Connection Credentials, on page 1
- Monitor AWS VPC Tunnels using AWS Transit Gateway , on page 2
- Search and Filter Site-to-Site VPN Tunnels, on page 3
- View a history of changes made to the AWS VPC tunnels, on page 4
- Manage Security Policies in Security Cloud Control, on page 4
- Manage Virtual Private Network Management in Security Cloud Control, on page 8
- About Device Configuration Changes, on page 17
- Read All Device Configurations, on page 18
- Preview and Deploy Configuration Changes for All Devices, on page 19
- Deploy Changes to a Device, on page 20
- Bulk Deploy Device Configurations, on page 21
- About Scheduled Automatic Deployments, on page 21
- Check for Configuration Changes, on page 24
- Discard Configuration Changes, on page 24
- Out-of-Band Changes on Devices, on page 25
- Synchronizing Configurations Between Security Cloud Control and Device, on page 26
- Conflict Detection, on page 26
- Automatically Accept Out-of-Band Changes from your Device, on page 27
- Resolve Configuration Conflicts, on page 28
- Schedule Polling for Device Changes, on page 30

## Update AWS VPC Connection Credentials

If you create a new access key and secret access key to connect to the AWS VPC, you must update the connection credentials in Security Cloud Control. Update the credentials in the AWS console and then update the credentials from the Security Cloud Control console using the procedure below. See *Managing Access Keys for IAM Users* (https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_access-keys.html) or *Creating, Disabling, and Deleting Access Keys for Your AWS Account Root User* (https://docs.aws.amazon.com/general/latest/gr/managing-aws-access-keys.html) for more information.

You **cannot** change the access key or secret access key from Security Cloud Control; you must manually manage the connection credentials from the AWS console or the AWS CLI console.

**Note** If you have multiple AWS VPCs onboarded to your Security Cloud Control tenant, you must update the credentials for one device at a time.

### Procedure

**Step 1** In the left pane, click **Security Devices**.

**Step 2** Click the **Devices** tab and then click **AWS VPC**.

**Step 3** Select the AWS VPC whose connection credentials you want to update.

You can use the filter and search functionalities to find the required device.

**Step 4** In the **Device Action** pane, click **Update Credentials**.

**Step 5** Enter the new **access key** and **secret access key** you want to use to connect to the AWS VPC.

**Step 6** Click **Update**.

**Note**
If Security Cloud Control fails to sync the device, the connectivity status in Security Cloud Control may show "Invalid Credentials." If that's the case, you may have tried to use an invalid username and password combination. See Troubleshoot Invalid Credentials

**Related Information**

- Onboard an AWS VPC

# Monitor AWS VPC Tunnels using AWS Transit Gateway

Amazon Web Service (AWS) Transit Gateway acts as a cloud router connecting enterprise virtual private clouds (VPCs) to AWS VPCs through a central hub that allows for simplified peering relationships.

Security Cloud Control allows you to monitor the connection status of your onboarded AWS VPCs using AWS Transit Gateway.

### Procedure

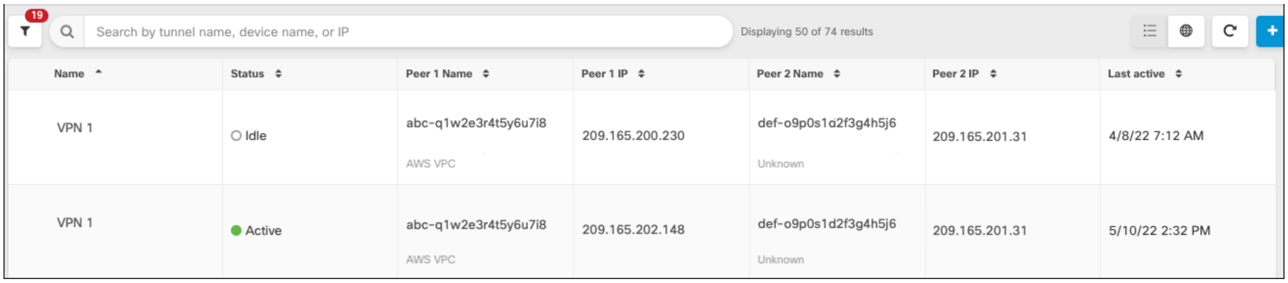
**Step 1** In the left pane, click **Secure Connections** > **Site to Site VPN** > **ASA & FDM**.

**Step 2** The **VPN Tunnels** page displays the connection status for all network tunnels managed by your Security Cloud Control tenant. The connection status for the VPN tunnel can be Search and Filter Site-to-Site VPN Tunnels.

**Step 3** Select a VPC and under **Actions** click **Check Connectivity** to trigger a real-time connectivity check against the tunnel and identify whether the tunnel is currently Search and Filter Site-to-Site VPN Tunnels. Unless you click the on-demand connectivity check link, a check across all tunnels, available across all onboarded devices, occurs every ten minutes.

**Note**

Security Cloud Control prompts a notification if a VPN tunnel's connection goes down. However, there is no notification prompt if the link is back up.



19
Search by tunnel name, device name, or IP
Displaying 50 of 74 results

| Name | Status | Peer 1 Name | Peer 1 IP | Peer 2 Name | Peer 2 IP | Last active |
|---|---|---|---|---|---|---|
| VPN 1 | ○ Idle | abc-q1w2e3r4t5y6u7i8<br>AWS VPC | 209.165.200.230 | def-o9p0s1a2f3g4h5j6<br>Unknown | 209.165.201.31 | 4/8/22 7:12 AM |
| VPN 1 | ● Active | abc-q1w2e3r4t5y6u7i8<br>AWS VPC | 209.165.202.148 | def-o9p0s1d2f3g4h5j6<br>Unknown | 209.165.201.31 | 5/10/22 2:32 PM |

# Search and Filter Site-to-Site VPN Tunnels

Use the filter sidebar in combination with the search field to focus your search of VPN tunnels presented in the VPN tunnel diagram.

### Procedure

**Step 1** In the left pane, click **Secure Connections** > **Site to Site VPN** > **ASA & FDM** to open the VPN page.

**Step 2** Click the filter icon to open the filter pane.

**Step 3** Use these filters to refine your search:

- **Filter by Device**-Click **Filter by Device**, select the device type tab, and check the devices you want to find by filtering.
- **Tunnel Issues-**Whether or not we have detected either side of the tunnel has issues. Some examples of a device having issues may be but not limited to is: missing associated interface or peer IP address or access list, IKEv1 proposal mismatches, etc. (Detecting tunnel issues is not yet available for AWS VPC VPN tunnels.)
- **Devices/Services**-Filter by type of device.
- **Status**–Tunnel status can be active or idle.
  - **Active**-There is an open session where network packets are traversing the VPN tunnel or a successful session was established and hasn't been timed-out yet. Active can assist to indicate that tunnel is active and relevant.
  - **Idle** - Security Cloud Control is unable to discover an open session for this tunnel. The tunnel may either be not in use or there is an issue with this tunnel.
- **Onboarded** - Devices could be managed by Security Cloud Control or not managed (unmanaged) by Security Cloud Control.
  - **Managed** – Filter by devices that Security Cloud Control manages.
  - **Unmanaged** – Filter by devices that Security Cloud Control does not manage.

- **Device Types** - Whether or not either side of the tunnel is a live (connected device) or model device.

**Step 4** You can also search the filtered results by device name or IP address by entering that information in the search bar. The search is case-insensitive.

# View a history of changes made to the AWS VPC tunnels

To view a history of changes made to AWS VPC tunnels:

### Procedure

**Step 1** In the left pane, click **Events & Logs** > **Change Log**.

**Step 2** On the **Change Log** page, click the filter icon and select **Filter by device** tab and then click **AWS VPC** .

**Step 3** Select the AWS VPC whose history you want to review and click **OK**.

**Related Information**

- Manage Change Logs in Security Cloud Control

# Manage Security Policies in Security Cloud Control

Security policies examine network traffic with the ultimate goal of allowing the traffic to its intended destination or dropping it if a security threat is identified. You can use Security Cloud Control to configure security policies on many different types of devices.

- AWS VPC Policy, on page 4

## AWS VPC Policy

Security Cloud Control provides users the ability to keep security policies consistent across an Amazon Web Services (AWS) Virtual Private Cloud (VPC) associated with your AWS account. You can also use Security Cloud Control to share objects across multiple device types. See the following topics for more information:

### AWS VPCs and Security Groups in Security Cloud Control

### AWS VPC Security Groups Rules

AWS security groups are a collection of rules that govern inbound and outbound network traffic to all the AWS EC2 instances, and other entities, associated with the security group.

Similar to the Amazon Web Services (AWS) console, Security Cloud Control displays each rule individually. As long as your SDC has access to the Internet, you can create and manage AWS Virtual Private Cloud (VPC) rules for the following environments:

- A security group allowing information to or from another security group within the same AWS VPC.
- A security group allowing to or from an IPv4 or IPv6 address.

When creating a rule in Security Cloud Control that contains an AWS security group, keep the following limitations in mind:

- For a rule allowing inbound traffic, the source can be one or more security group objects in the same AWS VPC, an IPv4 or IPv6 CIDR block, or a single IPv4 or IPv6 address. Inbound rules can only have **one** security group object as the destination.
- For a rule allowing outbound traffic, the destination can be one or more security group objects in the same AWS VPC, a prefix list ID, an IPv4 or IPv6 CIDR block, a single IPv4 or IPv6 address. Outbound rules can only have **one** security group object as the source.
- Security Cloud Control translates rules that contain multiple entities, such as more than one port or subnet, into separate rules before deploying them to an AWS VPC.
- When you add or remove rules, the changes are automatically applied to all AWS entities associated with the security group.
- An AWS security group is limited to hosting a maximum of 60 inbound rules and 60 outbound rules. This limit is enforced separately for IPv4 rules and IPv6 rules; any additional rules created in Security Cloud Control are inclusive to the total number of rules. In short, you cannot exceed the 60 rule limitation by onboarding to Security Cloud Control.

**Warning** Any edits made to existing rules will result in the edited rule being deleted and a new rule created with the new details. This will cause traffic that depends on that rule to be dropped for a very brief period of time until the new rule can be created. This does not occur if you create a brand new rule.

If you need more information on the types of rules you can create from the AWS console, see AWS Security Group Object. See AWS Security Groups and Cloud Security Group Objects for more information on objects that can be associated with AWS VPCs.

**Related Information**

- Create a Security Group Rule, on page 5
- Edit a Security Group Rule, on page 7
- Delete a Security Group Rule, on page 7

## Create a Security Group Rule

By default, Amazon Web Services (AWS) Virtual Private Cloud (VPC) blocks all network traffic. This means that any rules are automatically configured to **Allow** traffic. You cannot edit this action.

**Note** When you create a new security group rule you must associate it with a security group.

The AWS console does not support rules that contain more than one source or destination. This means that if you deploy a single security group rule that contains more than one entity, Security Cloud Control translates the rule into separate rules before deploying it to the AWS VPC. For example, if you create an inbound rule that allows traffic from two port ranges into one cloud security group object, Security Cloud Control translates it into two separate rules: (1) to allow traffic from the first port range to the security group and (2) to allow traffic from the second port range to the security group.

Use this procedure to create a security group rule:

## Procedure

**Step 1** In the left pane, click **Security Devices**.

**Step 2** Click the **Template** tab.

**Step 3** Click the **AWS** tab and select the AWS VPC device template whose access control policy you want to edit..

**Step 4** In the Management pane at the right, select **Policy**.

🛡

**Step 5** Click the blue plus button next to the security group you wish to add the rule to.

+

**Step 6** Click **Inbound** or **Outbound**.

- **Inbound** rules - The source network can contain one or multiple IPv4 addresses, IPv6 addresses, or cloud security group objects. The destination network **must** be defined as a single cloud security group object.
- **Outbound** rules - The source network **must** be defined as a single cloud security group object. The destination network can contain one or multiple IPv4 addresses, IPv6 addresses, or security group objects

**Step 7** Enter the rule name. You can use alphanumeric characters, spaces, and these special characters: + . _ -

**Step 8** Define the traffic matching criteria by using any combination of attributes in the following tabs:

- **Source** - Click the **Source** tab and add or remove networks (which includes networks and continents). You cannot define a port or port range as the source.
- **Destination** - Click the **Destination** tab and add or remove networks (which includes networks and continents), or ports on which the traffic arrives. The default value is "Any."
  - **Note:**

    If no network object is defined, it will be translated into two rules in the AWS Console: one for IPv4 (0.0.0.0/0) and one for IPv6 (::0/0)

**Step 9** Click **Save**.

**Step 10** Preview and Deploy Configuration Changes for All Devices now the changes you made, or wait and deploy multiple changes at once.

**Caution**

If the deploy fails, Security Cloud Control attempts to return the state of the AWS VPC to what it was before you made the deployment attempt. This is done on a "best effort" basis. Because AWS doesn't maintain a state, this rollback attempt could fail. In that case, you will have to log in to the AWS management console and manually return the AWS VPC to its previous configuration and then About Device Configuration Changes into Security Cloud Control.

## Edit a Security Group Rule

Use this procedure to edit an access control rule for an AWS VPC using Security Cloud Control:

### Procedure

**Step 1** In the left pane, click **Security Devices**.

**Step 2** Click the **Devices** tab to locate the device or the **Templates** tab to locate the model device.

**Step 3** Click the **AWS** tab and select the AWS VPC whose access control policy you want to edit.

**Step 4** In the **Management** pane on the right, select 🛡 **Policy**.

**Step 5** To edit an existing security group rule, select the rule and click the edit icon ✎ in the Actions pane. (Simple edits may also be performed inline without entering edit mode.) See AWS VPC Security Groups Rules for rule limitations and exceptions.

**Step 6** Click **Save**.

**Step 7** Preview and Deploy Configuration Changes for All Devices now the changes you made, or wait and deploy multiple changes at once.

**Caution**

If the deployment fails, Security Cloud Control attempts to return the state of the AWS VPC to what it was before you made the deployment attempt. This is done on a "best effort" basis. Because AWS doesn't maintain a state, this rollback attempt could fail. In that case, you will have to log in to the AWS management console and manually return the AWS VPC to its previous configuration and then poll for changes between the AWS VPC device configuration and the configuration in Security Cloud Control.

## Delete a Security Group Rule

### Procedure

**Step 1** In the left pane, click **Security Devices**.

**Step 2** Click the **Devices** tab to locate the device or the **Templates** tab to locate the model device.

**Step 3** Click the **AWS** tab and select the AWS VPC whose access control policy you want to edit.

**Step 4** In the **Management** pane on the right, select 🛡 **Policy**.

**Step 5** To delete a security group rule you no longer need, select the rule and click the remove icon 🗑 in the **Actions** pane.

**Step 6** Preview and Deploy Configuration Changes for All Devices now the changes you made, or wait and deploy multiple changes at once.

**Caution**

If the deployment fails, Security Cloud Control attempts to return the state of the AWS VPC to what it was before you made the deployment attempt. This is done on a "best effort" basis. Because AWS doesn't maintain a "state," this rollback attempt could fail. In that case, you will have to log in to the AWS management console and manually return the AWS VPC to its previous configuration and then poll for changes between the AWS VPC device configuration and the configuration in Security Cloud Control.

# Manage Virtual Private Network Management in Security Cloud Control

A virtual private network (VPN) connection establishes a secure tunnel between endpoints over a public network such as the Internet.

This section applies to Remote Access and Site-to-site VPNs on device. It also describes the SSL standards that are used to build and remote access VPN connections on .

Security Cloud Control supports the following types of VPN connections:

- Introduction to Site-to-Site Virtual Private Network, on page 8

## Introduction to Site-to-Site Virtual Private Network

A site-to-site VPN tunnel connects networks in different geographic locations. You can create site-to-site IPsec connections between managed devices and between managed devices and other Cisco or third-party peers that comply with all relevant standards. These peers can have any mix of inside and outside IPv4 and IPv6 addresses. Site-to-site tunnels are built using the Internet Protocol Security (IPsec) protocol suite and Internet Key Exchange version 2 (IKEv2). After the VPN connection is established, the hosts behind the local gateway can connect to the hosts behind the remote gateway through the secure VPN tunnel.

### VPN Topology

To create a new site-to-site VPN topology you must provide a unique name, specify a topology type, choose the IKE version that is used for IPsec IKEv1 or IKEv2, or both and authentication method. Once configured, you deploy the topology to .

### IPsec and IKE Protocols

In Security Cloud Control, site-to-site VPNs are configured based on IKE policies and IPsec proposals that are assigned to VPN topologies. Policies and proposals are sets of parameters that define the characteristics of a site-to-site VPN, such as the security protocols and algorithms that are used to secure traffic in an IPsec tunnel. Several policy types may be required to define a full configuration image that can be assigned to a VPN topology.

### Authentication VPN Tunnels

For authentication of VPN connections, configure a pre-shared key in the topology on each device. Pre-shared keys allow a secret key, used during the IKE authentication phase, to be shared between two peers.

### About Extranet Devices

You can add non-Cisco or unmanaged Cisco devices to a VPN topology as "Extranet" devices with either static or dynamic IP addresses.

- Non-Cisco Device: You cannot use Security Cloud Control to create and deploy configurations to non-Cisco devices.
- Unmanaged Cisco Device: Cisco device not managed by your organization, such as spokes in networks managed by other organizations within your company, or a connection to a service provider or partner's network.

**Related Information:**

- Monitor AWS Site-to-Site Virtual Private Networks

## Monitor AWS Site-to-Site Virtual Private Networks

Security Cloud Control allows you to monitor already existing site-to-site VPN configurations on onboarded AWS devices. It doesn't allow you to modify or delete the site-to-site configuration.

### Check Site-to-Site VPN Tunnel Connectivity

Use the **Check Connectivity** button to trigger a real-time connectivity check against the tunnel to identify whether the tunnel is currently Search and Filter Site-to-Site VPN Tunnels. Unless you click the on-demand connectivity check button, a check across all tunnels, available across all onboarded devices, occurs once an hour.

**Note**

- Security Cloud Control runs this connectivity check command on the to determine if a tunnel is active or idle:

```
show vpn-sessiondb l2l sort ipaddress
```

- Model ASA device(s) tunnels will always show as **Idle**.

To check tunnel connectivity from the VPN page:

#### Procedure

**Step 1** In the left pane, click **Secure Connections** > **Site to Site VPN** > **ASA & FDM**.

**Step 2** Search and Filter Site-to-Site VPN Tunnels the list of tunnels for your site-to-site VPN tunnel and select it.

**Step 3** In the Actions pane at the right, click **Check Connectivity**.

### Site-To-Site VPN Dashboard

Security Cloud Control provides a consolidated information about site-to-site VPN connections created in the tenant.

In the left pane, click **Secure Connections** > **Site to Site VPN**. The **Site-to-Site VPN** provides the information in the following widgets:

- **Sessions & Insights**: Displays a bar graph representing Active VPN Tunnels and Idle VPN Tunnels, each in appropriate colors.
- **Issues**: Shows the total number of tunnels detected with issues.
- **Pending Deploy**: Shows the total number of tunnels with pending deployment.

By clicking on a value in the pie chart or any link in the widget, the site-to-site VPN listing page is displayed with a filter based on the selected value. For instance, in the **VPN Tunnel Status** widget, on clicking the **Active VPN Tunnels**, you will be directed to the site-to-site VPN listing page with the **Active** status filter applied, showing only the active tunnels.

## Identify VPN Issues

Security Cloud Control can identify VPN issues on . (This feature is not yet available for AWS VPC site-to-site VPN tunnels.) This article describes:

- Find VPN Tunnels with Missing Peers
- Find VPN Peers with Encryption Key Issues
- Find Incomplete or Misconfigured Access Lists Defined for a Tunnel
- Find Issues in Tunnel Configuration

  Resolve Tunnel Configuration Issues, on page 12

### *Find VPN Tunnels with Missing Peers*

The "Missing IP Peer" condition is more likely to occur on ASA devices than FDM-managed devices.

#### Procedure

**Step 1** In the left pane, click **Secure Connections** > **Site to Site VPN** > **ASA & FDM** to open the VPN page.

**Step 2** Select **Table View**.

**Step 3** Open the Filter panel by clicking the filter icon ▼.

**Step 4** Check **Detected Issues**.

**Step 5** Select each device reporting an issue ⚠ and look in the Peers pane at the right. One peer name will be listed. Security Cloud Control reports the other peer name as, "[Missing peer IP.]"

### *Find VPN Peers with Encryption Key Issues*

Use this approach to locate VPN Peers with encryption key issues such as:

- IKEv1 or IKEv2 keys are invalid, missing, or mismatched
- Obsolete or low encryption tunnels

### Procedure

**Step 1** In the left pane, click **Secure Connections** > **Site to Site VPN** > **ASA & FDM** to open the VPN page.

**Step 2** Select **Table View**.

**Step 3** Open the Filter panel by clicking the filter icon ▼.

**Step 4** Select each device reporting an issue ⚠ and look in the Peers pane at the right. The peer information will show you both peers.

**Step 5** Click on **View Peers** for one of the devices.

**Step 6** Double-click the device reporting the issue in the Diagram View.

**Step 7** Click **Key Exchange** in the Tunnel Details panel at the bottom. You will be able to view both devices and diagnose the key issue from that point.

## *Find Incomplete or Misconfigured Access Lists Defined for a Tunnel*

The "incomplete or misconfigured access-list" condition could only occur on ASA devices.

### Procedure

**Step 1** In the left pane, click **Secure Connections** > **Site to Site VPN** > **ASA & FDM** to open the VPN page.

**Step 2** Select **Table View**.

**Step 3** Open the Filter panel by clicking the filter icon ▼.

**Step 4** Select each device reporting an issue ⚠ and look in the Peers pane at the right. The peer information shows you both peers.

**Step 5** Click on **View Peers** for one of the devices.

**Step 6** Double-click the device reporting the issue in the Diagram View.

**Step 7** Click **Tunnel Details** in the Tunnel Details panel at the bottom. You will see the message, "Network Policy: Incomplete"

## *Find Issues in Tunnel Configuration*

The tunnel configuration error can occur in the following scenarios:

- When the IP address of a site-to-site VPN interface changes, the "Peer IP Address Value has changed".
- When the IKE value of a VPN tunnel doesn't match the other VPN tunnel, the "IKE value Mismatch" message appears.

### Procedure

**Step 1** In the left pane, click **Secure Connections** > **Site to Site VPN** > **ASA & FDM** to open the VPN page.

**Step 2** Select **Table View**.

**Step 3** Open the Filter panel by clicking the filter icon ▼.

**Step 4** In the **Tunnel Issues**, click **Detected Issues** to view the VPN configuration reporting errors. You can view the configuration reporting issues ⚠.

**Step 5** Select the VPN configuration reporting issues.

**Step 6** In the **Peers** pane on the right, the ⚠ icon appears for the peer having the issue. Hover over the ⚠ icon to see the issue and resolution.

Next Step: Resolve Tunnel Configuration Issues.

### *Resolve Tunnel Configuration Issues*

This procedure attempts to resolve these tunnel configuration issues:

- When the IP address of a site-to-site VPN interface changes, the "Peer IP Address Value has changed".
- When the IKE value of a VPN tunnel doesn't match the other VPN tunnel, the "IKE value Mismatch" message appears.

See Find Issues in Tunnel Configuration for more information.

#### Procedure

**Step 1** In the left pane, click **Security Devices**.

**Step 2** Click the **Devices** tab.

**Step 3** Click the appropriate device type tab and select the device associated with the VPN configuration reporting an issue.

**Step 4** Resolve the Conflict Detected Status.

**Step 5** In the left pane, click **VPN** > **ASA/FDM Site-to-Site VPN** to open the VPN page.

**Step 6** Select the VPN configuration reporting this issue.

**Step 7** In the **Actions** pane, click the **Edit** icon.

**Step 8** Click **Next** in each step until you click the **Finish** button in step 4.

**Step 9** Preview and Deploy Configuration Changes for All Devices, on page 19.

## Search and Filter Site-to-Site VPN Tunnels

Use the filter sidebar ▼ in combination with the search field to focus your search of VPN tunnels presented in the VPN tunnel diagram.

#### Procedure

**Step 1** In the left pane, click **Secure Connections** > **Site to Site VPN** > **ASA & FDM** to open the VPN page.

**Step 2** Click the filter icon ▼ to open the filter pane.

**Step 3** Use these filters to refine your search:

- **Filter by Device**-Click **Filter by Device**, select the device type tab, and check the devices you want to find by filtering.
- **Tunnel Issues-**Whether or not we have detected either side of the tunnel has issues. Some examples of a device having issues may be but not limited to is: missing associated interface or peer IP address or access list, IKEv1 proposal mismatches, etc. (Detecting tunnel issues is not yet available for AWS VPC VPN tunnels.)
- **Devices/Services**-Filter by type of device.
- **Status**–Tunnel status can be active or idle.
  - **Active**-There is an open session where network packets are traversing the VPN tunnel or a successful session was established and hasn't been timed-out yet. Active can assist to indicate that tunnel is active and relevant.
  - **Idle** - Security Cloud Control is unable to discover an open session for this tunnel. The tunnel may either be not in use or there is an issue with this tunnel.
- **Onboarded** - Devices could be managed by Security Cloud Control or not managed (unmanaged) by Security Cloud Control.
  - **Managed** – Filter by devices that Security Cloud Control manages.
  - **Unmanaged** – Filter by devices that Security Cloud Control does not manage.
- **Device Types** - Whether or not either side of the tunnel is a live (connected device) or model device.

**Step 4** You can also search the filtered results by device name or IP address by entering that information in the search bar. The search is case-insensitive.

## Onboard an Unmanaged Site-to-Site VPN Peer

Security Cloud Control will discover a site-to-site VPN tunnel when one of the peers is onboarded. If the second peer is not managed by Security Cloud Control, you can filter the list of VPN tunnels to find the unmanaged device and onboard it:

### Procedure

**Step 1** In the left pane, click **Secure Connections** > **Site to Site VPN** > **ASA & FDM** to open the VPN page.

**Step 2** Select **Table View**.

**Step 3** Open the filter panel by clicking ▼.

**Step 4** Check **Unmanaged**.

**Step 5** Select a tunnel from the table from the results.

**Step 6** In the **Peers** pane on the right, click **Onboard Device** and follow the instructions on the screen.

**Related Information:**

- Onboard Devices and Services

- Onboard an AWS VPC

## Viewing AWS Site-to-Site VPN Tunnels

AWS site-to-site VPN connects your Virtual Private Cloud (VPC) to your enterprise network through a secure tunnel.

All site-to-site VPN configuration occurs in the AWS Management Console. Once you onboard your VPC, Security Cloud Control is able to display the site-to-site VPN connections maintained by your AWS VPC and display them on the VPN Tunnels page so that you can manage them along with all your other site-to-site connections. Each VPN connection from your network to your VPC is made up of two separate VPN tunnels.

From the VPN Tunnels page in Security Cloud Control, you can View Site-to-Site VPN Tunnel Information, Search and Filter Site-to-Site VPN Tunnels of the VPC, and Onboard an Unmanaged Site-to-Site VPN Peer.

Security Cloud Control polls the AWS Management Console every 10 minutes looking for changes to the site-to-site VPN configuration. If Security Cloud Control finds that there has been a change, it polls for changes in that configuration and stores the changes in its database. Security Cloud Control administrators will then be able to view the new configurations in Security Cloud Control.

### Amazon Web Services (AWS) Reference Material

AWS Virtual Private Network Documentation

## View IKE Object Details of Site-To-Site VPN Tunnels

You can view the details of the IKE objects configured on the peers/devices of the selected tunnel. These details appear in a tree structure in a hierarchy based on the priority of the IKE policy object.

**Note** Extranet devices don't show the IKE Objects details.

### Procedure

**Step 1** In the left pane, click **Secure Connections** > **Site to Site VPN** > **ASA & FDM** to open the VPN page.

**Step 2** In the **VPN Tunnels** page, click the name of the VPN tunnel that connects the peers.

**Step 3** Under **Relationships** on the right, expand the object that you want to see its details.

## View Last Successful Site-to-Site VPN Tunnel Establishment Date

### Procedure

**Step 1** View Site-to-Site VPN Tunnel Information.

**Step 2** Click the **Tunnel Details** pane.

**Step 3** View the **Last Seen Active** field.

## View Site-to-Site VPN Tunnel Information

The site-to-site VPN table view is a complete listing of all site-to-site VPN tunnels available across all devices onboarded to Security Cloud Control. A tunnel only exists once in this list. Clicking on a tunnel listed in the table provides an option in the right side bar to navigate directly to a tunnel's peers for further investigation.

In cases where Security Cloud Control does not manage both sides of a tunnel, you can click Onboard an Unmanaged Site-to-Site VPN Peer to open the main onboarding page an onboard the unmanaged peer. In cases where Security Cloud Control manages both side of a tunnel, the Peer 2 column contains the name of the managed device. However, in the case of an AWS VPC, the Peer 2 column contains the IP address of the VPN gateway.

To view site-to-site VPN connections in the table view:

### Procedure

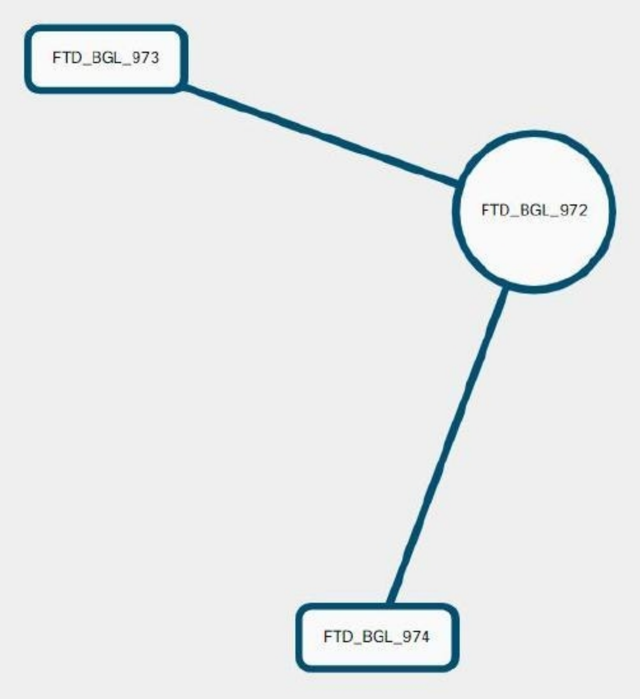
**Step 1** In the left pane, click **Secure Connections** > **Site to Site VPN** > **ASA & FDM** to open the VPN page.

**Step 2** Click the **Table view** ☰ button.

**Step 3** Use Search and Filter Site-to-Site VPN Tunnels to find a specific tunnel, or zoom into the Global View graphic to find the VPN gateway and its peers that you are looking for.

### *Site-to-Site VPN Global View*

This is an example fo the global view. In the illustration, 'FTD_BGL_972' has a site-to-site connection with FTD_BGL_973 and FTD_BGL_974 devices.



### Procedure

**Step 1** In the left pane, click **Secure Connections** > **Site to Site VPN** > **ASA & FDM**.

**Step 2** Click the **Global view** button.

**Step 3** Use Search and Filter Site-to-Site VPN Tunnels to find a specific tunnel, or zoom into the Global View graphic to find the VPN gateway and its peers that you are looking for.

**Step 4** Select one of the peers represented in the Global View.

**Step 5** Click **View Details**.

**Step 6** Click the other end of the VPN tunnel and Security Cloud Control displays Tunnel Details, NAT Information, and Key Exchange information for that connection:

- **Tunnel Details**-Displays the name and connectivity information about the tunnel. Clicking the Refresh icon updates the connectivity information for the tunnels.
- **Tunnel Details specific to AWS connections**-Tunnel details for AWS site-to-site connections are slightly different than for other connections. For each connection from the AWS VPC to your VPN gateway, AWS creates two VPN tunnels. This is for high availability.
  - The name of the tunnel represents the name of the VPC your VPN gateway is connected to. The IP address named in the tunnel is the IP address that your VPN gateway knows as the VPC.
  - If the Security Cloud Control Connectivity status shows **active**, the AWS tunnel state is **Up**. If the Security Cloud Control Connectivity state is **inactive**, the AWS tunnel state is **Down**.
- **NAT Information**-Displays the type of NAT rule being used, original and translated packet information, and provides links to the NAT table to view the NAT rule for that tunnel. (Not yet available for AWS VPC site-to-site VPN.)
- **Key Exchange**-Displays the cryptographic keys in use by the tunnel and key-exchange issues. (Not yet available for AWS VPC site-to-site VPN.)

## *Site-to-Site VPN Tunnels Pane*

The Tunnels pane displays a list of all the tunnels associated with a particular VPN gateway. For site-to-site VPN connections between your VPN gateway and an AWS VPC, the tunnels pane shows all the tunnels from your VPN gateway to the VPC. Since each site-to-site VPN connection between your VPN gateway and an AWS VPC has two tunnels, you will see double the number of tunnels you normally would for other devices.

### VPN Gateway Details

Displays the number of peers connected to the VPN gateway and the IP address of the VPN gateway. This is only visible in the VPN Tunnels page.

### View Peer

After you select a site-to-site VPN peer pair, the peers pane lists the two devices in the pair and allows you to click **View Peer** for one of the devices. By clicking **View Peer**, you see any other site-to-site peer that device is associated with. This is visible in the Table view and in the Global view.

### Delete a Security Cloud Control Site-To-Site VPN Tunnel

#### Procedure

**Step 1** In the left pane, click **Secure Connections** > **Site to Site VPN** > **ASA & FDM** to open the VPN page.

**Step 2** Select the desired site-to-site VPN tunnel that you want to delete.

**Step 3** In the **Actions** pane on the right, click **Delete**.

The selected site-to-site VPN tunnel is deleted.

# About Device Configuration Changes

In order to manage a device, Security Cloud Control must have its own copy of the device's configuration stored in its local database. When Security Cloud Control "reads" a configuration from a device it manages, it takes a copy of the device's configuration and saves it. The first time Security Cloud Control reads and saves a copy of a device's configuration is when the device is onboarded. These choices describe reading a configuration for different purposes:

- **Discard Changes**: This action is available when a device's configuration status is "Not Synced." In the Not Synced state, there are changes to the device's configuration pending on Security Cloud Control. This option allows you to undo all pending changes. The pending changes are deleted and Security Cloud Control overwrites its copy of the configuration with copy of the configuration stored on the device.

- **Check for Changes**: This action is available if the device's configuration status is Synced. Clicking Checking for Changes directs Security Cloud Control to compare its copy of the device's configuration with the copy of the configuration stored on the device. If there is a difference, Security Cloud Control immediately overwrites its copy of the device's configuration with the copy stored on the device.

- **Review Conflict** and **Accept Without Review**: If you have enabled Conflict Detection on a device, Security Cloud Control checks for configuration changes made on the device every 10 minutes. If the copy of the configuration stored on the device has changed, Security Cloud Control notifies you by displaying the "Conflict Detected" configuration status.

    - **Review Conflict**: Click Review Conflict allows you to review changes made directly on a device and accept or reject them.

    - **Accept Without Review**: This action overwrites Security Cloud Control's copy of a device's configuration with the latest copy of the configuration stored on the device. Security Cloud Control does not prompt you to confirm the differences in the two copies of the configuration before taking the overwriting action.

**Read All**: This is a bulk operation. You can select more than one device, in any state, and click **Read All** to overwrite all the devices' configurations stored on Security Cloud Control with the configurations stored on the devices.

- **Deploy Changes**: As you make changes to a device's configuration, Security Cloud Control saves the changes you make to its own copy of the configuration. Those changes are "pending" on Security Cloud

Control until they are deployed to the device. When there are changes to a device's configuration that have not been deployed to the device, the device is in the Not Synced configuration state.

Pending configuration changes have no effect on the network traffic running through the device. Only after Security Cloud Control deploys the changes to the device do they have an effect. When Security Cloud Control deploys changes to the device's configuration, it only overwrites those elements of the configuration that were changed. It does not overwrite the entire configuration file stored on the device. Deployments can be initiated for a single device or on more than one device simultaneously.

- **Discard All** is an option that is only available after you click **Preview and Deploy...**. After clicking Preview and Deploy, Security Cloud Control shows you a preview of the pending changes in Security Cloud Control. Clicking **Discard All** deletes all pending changes from Security Cloud Control and does not deploy anything to the selected device(s). Unlike "Discard Changes" above, deleting the pending changes is the end of the operation.

# Read All Device Configurations

If a configuration change is made to a device outside of Security Cloud Control, the device's configuration stored on Security Cloud Control and the device's local copy of its configuration are no longer the same. You many want to overwrite Security Cloud Control's copy of the device's configuration with the configuration stored on the device to make the configurations the same again. You can perform this task on many devices simultaneously using the **Read All** link.

See About Device Configuration Changes for more information about how Security Cloud Control manages the two copies of the device's configuration.

Here are three configuration statuses where clicking **Read All** will overwrite Security Cloud Control's copy of the device's configuration with the device's copy of the configuration.

- **Conflict Detected**-If conflict detection is enabled, Security Cloud Control polls the devices it manages every 10 minutes for changes made to their configurations. If Security Cloud Control finds that the configuration on the device has changed, Security Cloud Control displays a "Conflict detected" configuration status for the device.

- **Synced**-If the device is in a synced state, and you click **Read All**, Security Cloud Control immediately checks the devices to determine if there have been any changes made to its configurations directly. After clicking **Read All**, Security Cloud Control confirms your intent to overwrite its copy of the device's configuration and then Security Cloud Control performs the overwrite.

- **Not Synced**-If the device is in the Not Synced state, and you click **Read All**, Security Cloud Control warns you that there are pending changes made to to the device's configuration using Security Cloud Control and that proceeding with the Read All operation will delete those changes and then overwrite Security Cloud Control's copy of the configuration with the configuration on the device. This Read All functions like Discard Configuration Changes.

### Procedure

**Step 1** In the left pane, click **Security Devices**.

**Step 2** Click the **Devices** tab.

**Step 3** Click the appropriate device type tab.

**Step 4** (Optional) Create a change request label to identify the results of this bulk action easily in the Change Log.

**Step 5** Select the devices whose configurations you want to save Security Cloud Control. Notice that Security Cloud Control only provides command buttons for actions that can be applied to all the selected devices.

**Step 6** Click **Read All**.

**Step 7** Security Cloud Control warns you if there are configuration changes staged on Security Cloud Control, for any of the devices you selected, and asks if you want to continue with the bulk reading configurations action. Click **Read All** to continue.

**Step 8** Look at the notifications tab for the progress of the Read All configurations operation. If you want more information about how individual actions in the bulk operation succeeded or failed, click the blue Review link and you will be directed to the Jobs page.

**Step 9** If you created and activated a change request label, remember to clear it so that you don't inadvertently associate other configuration changes with this event.

**Related Information**

- About Device Configuration Changes
- Discard Configuration Changes
- Check for Configuration Changes

# Preview and Deploy Configuration Changes for All Devices

Security Cloud Control informs you when you have made a configuration change to a device on your tenant, but you have not deployed that change, by displaying an orange dot on the Deploy icon . The devices affected by these changes show the status "Not Synced" in the Devices and **Services** page. By clicking **Deploy**, you can review which devices have pending changes and deploy the changes to those devices.

**Note** For every new FDM or FTD network object or group that you create and make changes to, Security Cloud Control creates an entry in this page for all on-premises management centers that are managed by Security Cloud Control.

This deployment method is available for all supported devices.

You can use this deployment method for single configuration changes or wait and deploy multiple changes at once.

### Procedure

**Step 1** In the top right corner of the screen, click the **Deploy** icon .

**Step 2** Select the devices with changes you want to deploy. If a device has a yellow caution triangle, you can not deploy changes to that device. Hover your mouse over the yellow caution triangle to find out why you can't deploy changes to that device.

**Step 3** (Optional) If you want to see more information about a pending change, click the **View Detailed Changelog** link to open the change log associated with that change. Click the **Deploy** icon to return to the **Devices with Pending Changes** page.

**Step 4** (Optional) Create a change request to track your changes without leaving the **Devices with Pending Changes** page.

**Step 5** Click **Deploy Now** to deploy the changes immediately to the devices you selected. You'll see the progress in the Active jobs indicator in the Jobs tray.

**Step 6** (Optional) After the deployment has finished, click **Jobs** in the Security Cloud Control navigation bar. You will see a recent "Deploy Changes" job showing the results of the deployment.

**Step 7** If you created a change request label, and you have no more configuration changes to associate with it, clear it.

### What to do next

- About Scheduled Automatic Deployments

# Deploy Changes to a Device

### Procedure

**Step 1** After you make a configuration change for a device using Security Cloud Control and save it, that change is saved in Security Cloud Control instance of the device's configuration.

**Step 2** In the navigation bar, click **Security Devices**.

**Step 3** Click the **Devices** tab.

**Step 4** Click the appropriate device type tab. You should see that the configuration status of the device you made changes to is now "Not synced."

**Step 5** Deploy the changes using one of these methods:

- Select the device and in the Not Synced pane on the right, click **Preview and Deploy.** On the Pending Changes screen, review the changes. If you are satisfied with the pending version, click **Deploy Now**. After the changes are deployed successfully, you can view the change log to confirm what just happened.
- Click the **Deploy** icon at the top-right of the screen. See Preview and Deploy Configuration Changes for All Devices, on page 19 for more information.

# Cancelling Changes

If, when deploying a change from Security Cloud Control to a device, you click **Cancel**, the changes you made are not deployed to the device. The process is canceled. The changes you made are still pending on Security Cloud Control and can be edited further before you finally deploy them to FDM-managed device.

## Discarding Changes

If, when previewing changes, you click **Discard all**, the changes you made, and any other changes any other user made but did not deploy to the device, are deleted. Security Cloud Control reverts its pending configuration to the last read or deployed configuration before any changes were made.

# Bulk Deploy Device Configurations

If you have made changes to multiple devices, for instance by editing a shared object, you can apply those change to all of the affected devices at once:

### Procedure

**Step 1** In the left pane, click **Security Devices**.

**Step 2** Click the **Devices** tab.

**Step 3** Click the appropriate device type tab.

**Step 4** Select all of the devices for which you have made configuration changes on Security Cloud Control. These devices should show "Not Synced" status.

**Step 5** Deploy the changes using one of these methods:

- Click the button at the top-right of the screen to view the **Devices with Pending Changes** window. This gives you a chance to review the pending changes on the devices you selected before you deploy them. Click **Deploy Now** to deploy the changes.

  **Note**
  If you see a yellow warning triangle next to a device on the **Devices with Pending Changes** screen, you cannot deploy a change to that device. Hover your mouse over the warning triangle for information about why changes cannot be deployed to that device.

- Click **Deploy All** on the details pane. Review any warnings and click **OK**. The bulk deployment starts immediately without a review of the changes.

**Step 6** (Optional) Click the Jobs icon in the navigation bar to view the results of the bulk deploy.

# About Scheduled Automatic Deployments

Using Security Cloud Control, you can make configuration changes to one or more of the devices it manages and then schedule the changes to be deployed to those devices at a time that is convenient for you.

You can only schedule deployments if you Enable the Option to Schedule Automatic Deployments in the **Tenant Settings** tab of the Settings page. Once this option is enabled, you can create, edit, or delete scheduled deployments. A scheduled deployment deploys all the staged changes saved on Security Cloud Control at the date and time set. You can also view and delete scheduled deployments from the Jobs page.

If there were changes made directly to the device that have not been About Device Configuration Changes to Security Cloud Control, the scheduled deployment will be skipped until that conflict is resolved. The Jobs page will list any instance where a scheduled deployment fails. If **Enable the Option to Schedule Automatic Deployments** is turned off, all scheduled deployments are deleted.

**Caution** If you schedule a new deployment for multiple devices, and some of those devices already have deployments scheduled, the new scheduled deployment overwrites the existing scheduled deployments.

**Note** When you create a scheduled deployment, the schedule is created in your local time, not in the time zone of the device. Scheduled deployments *do not* automatically adjust for daylight savings time.

# Schedule an Automatic Deployment

The deployment schedule can be a single event or a recurring event. You may find recurring automatic deployments a convenient way to line up recurring deployments with your maintenance window. Follow this procedure to schedule a one-time or a recurring deployment for a single device:

**Note** If you schedule a deployment for a device that has an existing deployment scheduled, the new scheduled deployment overwrites the existing deployment.

### Procedure

**Step 1** In the left pane, click **Security Devices**.

**Step 2** Click the **Devices** tab.

**Step 3** Click the appropriate device type tab.

**Step 4** Select one ore more devices.

**Step 5** In the Device Details pane, locate the Scheduled Deployments tab and click **Schedule**.

**Step 6** Select when the deployment should occur.

- For a one-time deployment, click the **Once on** option to select a date and time from the calendar.
- For a recurring deployment, click the **Every** option. You can choose either a daily or once a week deployment. Select the **Day** and **Time** the deployment should occur.

**Step 7** Click **Save**.

# Edit a Scheduled Deployment

Follow this procedure to edit a scheduled deployment:

### Procedure

**Step 1** In the left pane, click **Security Devices**.

**Step 2** Click the **Devices** tab.

**Step 3** Click the appropriate device type tab.

**Step 4** Select one or more devices.

**Step 5** In the **Device Details** pane, locate the Scheduled Deployments tab and click **Edit** .

✎

**Step 6** Edit the recurrence, date, or time of a scheduled deployment.

**Step 7** Click **Save**.

## Delete a Scheduled Deployment

Follow this procedure to delete a scheduled deployment:

**Note** If you schedule a deployment for multiple devices, and then change or delete the schedule for some of the devices, the original scheduled deployment for the remaining devices will be preserved.

### Procedure

**Step 1** In the left pane, click **Security Devices**.

**Step 2** Click the **Devices** tab.

**Step 3** Click the appropriate device type tab.

**Step 4** Select one or more devices.

**Step 5** In the **Device Details** pane, locate the Scheduled Deployments tab and click **Delete** 🗑.

#### What to do next

- About Device Configuration Changes
- Read All Device Configurations, on page 18
- Preview and Deploy Configuration Changes for All Devices, on page 19

# Check for Configuration Changes

**Check for Changes** to determine if the device's configuration has been changed directly on the device and it is no longer the same as the copy of the configuration stored on Security Cloud Control. You will see the this option when the device is in the "Synced" state.

To check changes:

## Procedure

**Step 1** In the left pane, click **Security Devices**.

**Step 2** Click the **Devices** tab.

**Step 3** Click the appropriate device type tab.

**Step 4** Select the device, whose configuration you suspect may have been changed directly on the device.

**Step 5** Click **Check for Changes** in the Synced pane on the right.

**Step 6** The behavior that follows is slightly different depending on the device:

- For AWS device if there has been a change to the device's configuration, you will receive the message:

  ```
  Reading the policy from the device. If there are active deployments on the device, reading will
  start after they are finished.
  ```

  - Click **OK** to continue. The configuration on the device will overwrite the stored configuration on Security Cloud Control.
  - Click **Cancel** to cancel the action.

- For device:

a. Compare the two configurations presented to you. Click **Continue**. The configuration labeled **Last Known Device Configuration** is the configuration stored on Security Cloud Control. The configuration labeled **Found on Device** is the configuration saved on the ASA.

b. Select either:

   1. **Reject** the out-of-band changes to keep the "Last Known Device Configuration."
   2. **Accept** the out-of-band changes to overwrite the device's configuration stored in Security Cloud Control with the configuration found on the device.

c. Click **Continue**.

# Discard Configuration Changes

Click **Discard Changes** when you want to "undo" all the *undeployed* configuration changes you made to a device's configuration using Security Cloud Control. When you click **Discard Changes**, Security Cloud

Control *completely overwrites* its local copy of a device's configuration with the configuration stored on the device.

When you click **Discard Changes**, your device's configuration status is in a **Not Synced** state. After you discard your changes, the copy of the configuration on Security Cloud Control will be the same as the copy of the configuration on the device and the configuration status in Security Cloud Control will return to Synced.

To discard, or "undo," all of your undeployed configuration changes for a device:

**Procedure**

**Step 1** In the left pane, click **Security Devices**.

**Step 2** Click the **Devices** tab.

**Step 3** Click the appropriate device type tab.

**Step 4** Select the device you have been making configuration changes to.

**Step 5** Click **Discard Changes** in the **Not Synced** pane on the right.

- For FDM-managed devices-Security Cloud Control warns you that "Pending changes on Security Cloud Control will be discarded and the Security Cloud Control configuration for this device will be replaced with the configuration currently running on the device." Click **Continue** to discard your changes.
- For Meraki devices-Security Cloud Control deletes the change immediately.
- For AWS devices-Security Cloud Control displays what you are about to delete. Click **Accept** or **Cancel**.

# Out-of-Band Changes on Devices

Out-of-band changes refer to changes made directly on the device without using Security Cloud Control. These changes may be made using the device's command-line interface over an SSH connection or by using a local manager like the Adaptive Security Device Manager (ASDM) for the ASA, the FDM for the FDM-managed device, or for an On-Premises Firewall Management Center on the On-Premises Firewall Management Center user interface. An out-of-band change causes a conflict between the device's configuration stored on Security Cloud Control and the configuration stored on the device itself.

### Detecting Out-of-Band Changes on Devices

If Conflict Detection is enabled for an ASA, or an FDM-managed device, a Cisco IOS device, or an On-Premises Firewall Management Center, Security Cloud Control checks the device every 10 minutes searching for any new changes made directly to the device's configuration outside of Security Cloud Control.

If Security Cloud Control finds that there are changes to the device's configuration that are not stored on Security Cloud Control, it changes the **Configuration Status** of that device to the "Conflict Detected" state.

When Security Cloud Control detects a conflict, one of two conditions is likely:

- There have been configuration changes made to the device directly that have not been saved to Security Cloud Control's database.

- In the case of an FDM-managed device, there may be "pending" configuration changes on the FDM-managed device that have not been deployed.
- In the case of an On-Premises Firewall Management Center, there may be changes made, for instance, to objects outside Security Cloud Control, which are pending to be synchronized with Security Cloud Control or changes made in Security Cloud Control which are pending to be deployed to the On-Premises Firewall Management Center.

# Synchronizing Configurations Between Security Cloud Control and Device

### About Configuration Conflicts

In the **Security Devices** page, you may see devices or services have the status "Synced," "Not Synced," or "Conflict Detected." To know the status of an On-Premises Firewall Management Center that you manage using Security Cloud Control, navigate **Tools & Services** > **Firewall Management Center**.

- When a device is **Synced**, the configuration on Security Cloud Control) and the configuration stored locally on the device are the same.
- When a device is **Not Synced**, the configuration stored in Security Cloud Control was changed and it is now different that the configuration stored locally on the device. Deploying your changes from Security Cloud Control to the device changes the configuration on the device to match Security Cloud Control's version.
- Changes made to devices outside of Security Cloud Control are called **out-of-band changes**. When out-of-band changes are made, you'll see the device state change to "Conflict Detected," if conflict detection is enabled for the device. Accepting the out-of-band changes, changes the configuration on Security Cloud Control to match the configuration on the device.

# Conflict Detection

When conflict detection is enabled, Security Cloud Control polls the device for the default interval to to determine if a change has been made to the device's configuration outside of Security Cloud Control. If Security Cloud Control detects that a change was made, it changes the configuration status for the device to **Conflict Detected**. Changes made to a device outside of Security Cloud Control are called "out-of-band" changes.

In the case of an On-Premises Firewall Management Center that is managed by Security Cloud Control, if there are changes that are staged and the device is in **Not Synced** state, Security Cloud Control stops polling the device to check for changes. When there are changes made outside Security Cloud Control which are pending to be synchronized with Security Cloud Control and changes made in Security Cloud Control which are pending to be deployed to the on-premises management center, Security Cloud Control declares the on-premises management center to be in the **Conflict Detected** state.

Once this option is enabled, you can configure how often conflicts or OOB changes are detected per device. See Schedule Polling for Device Changes, on page 30 for more information.

# Enable Conflict Detection

Enabling conflict detection alerts you to instances where changes have been made to a device outside of Security Cloud Control.

### Procedure

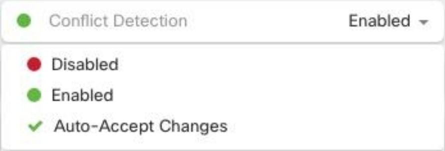
**Step 1** In the left pane, click **Security Devices**.

**Step 2** Click the **Devices** tab.

**Step 3** Select the appropriate device type tab.

**Step 4** Select the device or devices for which you want to enable conflict detection.

**Step 5** In the **Conflict Detection** box at the right of the device table, select **Enabled** from the list.



# Automatically Accept Out-of-Band Changes from your Device

You can configure Security Cloud Control to automatically accept any change made directly to a managed device by enabling auto-accept changes. Changes made directly to a device without using Security Cloud Control are referred to as out-of-band changes. An out-of-band change creates a *conflict* between the device's configuration stored on Security Cloud Control and the configuration stored on the device itself.

The auto-accept changes feature is an enhancement to conflict detection. If you have auto-accept changes enabled on your device, Security Cloud Control checks for changes every 10 minutes to determine if there have been any out-of-band changes made to the device's configuration. If there have been configuration changes, Security Cloud Control automatically updates its local version of the device's configuration without prompting you.

Security Cloud Control will ***not*** automatically accept a configuration change if there are configuration changes made on Security Cloud Control that have not yet been deployed to the device. Follow the prompts on the screen to determine your next action.

To use auto-accept changes, you first enable the tenant to display the auto-accept option in the Conflict Detection menu on the **Security Devices** page; then, you enable auto-accept changes for individual devices.

If you want Security Cloud Control to detect out-of-band changes but give you the option to accept or reject them manually, enable Conflict Detection, on page 26 instead.

## Configure Auto-Accept Changes

**Procedure**

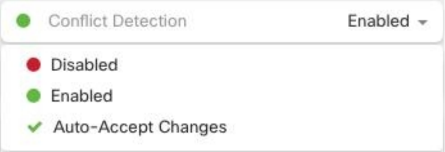
**Step 1** Log in to Security Cloud Control using an account with Admin or Super Admin privileges.

**Step 2** In the left pane, click **Administration** > **General Settings**.

**Step 3** In the **Tenant Settings** area, click the toggle to **Enable the option to auto-accept device changes**. This enables the Auto-Accept Changes menu option to appear in the Conflict Detection menu on the **Security Devices** page.

**Step 4** In the left pane, click **Security Devices** and select the device for which you want to automatically accept out-of-band changes.

**Step 5** In the **Conflict Detection** menu, select **Auto-Accept Changes** in the drop-down menu.



## Disabling Auto-Accept Changes for All Devices on the Tenant

**Procedure**

**Step 1** Log-in to Security Cloud Control using an account with Admin or Super Admin privileges.

**Step 2** In left pane, click **Administration** > **General Settings**.

**Step 3** In the **Tenant Settings** area, disable the "**Enable the option to auto-accept device changes**" by sliding the toggle to the left so it shows a grey X. This disables Auto-Accept Changes option in the Conflict Detection menu and disables the feature for every device on your tenant.

**Note**
Disabling "Auto-Accept" will require you to review each device conflict before you can accept it into Security Cloud Control. This includes devices previously configured to auto-accept changes.

# Resolve Configuration Conflicts

This section provides information about resolving configuration conflicts that occur on the device.

## Resolve the Not Synced Status

Use the following procedure to resolve a device with a "Not Synced" Configuration Status:

### Procedure

**Step 1** In the navigation bar, click **Security Devices**.

**Note**
For an On-Premises Firewall Management Center, click **Administration** > **Firewall Management Center** and select the FMC that is in **Not Synced** state and continue from Step 5.

**Step 2** Click the **Devices** tab to locate the device or the **Templates** tab to locate the model device.

**Step 3** Click the appropriate device type tab.

**Step 4** Select the device reported as Not Synced.

**Step 5** In the **Not synced** panel to the right, select either of the following:

- **Preview and Deploy...** -If you want to push the configuration change from Security Cloud Control to the device, Preview and Deploy Configuration Changes for All Devices the changes you made now, or wait and deploy multiple changes at once.
- **Discard Changes** -If you do **not** want to push the configuration change from Security Cloud Control to the device, or you want to "undo" the configuration changes you started making on Security Cloud Control. This option overwrites the configuration stored in Security Cloud Control with the running configuration stored on the device.

# Resolve the Conflict Detected Status

Security Cloud Control allows you to enable or disable conflict detection on each live device. If Conflict Detection, on page 26 is enabled and there was a change made to the device's configuration without using Security Cloud Control, the device's configuration status will show **Conflict Detected**.

To resolve a "Conflict Detected" status, follow this procedure:

### Procedure

**Step 1** In the navigation bar, click **Security Devices**.

**Note**
For an On-Premises Firewall Management Center, click **Administration** > **Firewall Management Center** and select the FMC that is in **Not Synced** state and continue from Step 5.

**Step 2** Click the **Devices** tab to locate your device.

**Step 3** Click the appropriate device type tab.

**Step 4** Select the device reporting the conflict and click **Review Conflict** in the details pane on the right.

**Step 5** In the **Device Sync** page, compare the two configurations by reviewing the highlighted differences.

- The panel labeled "Last Known Device Configuration" is the device configuration stored on Security Cloud Control.
- The panel labeled "Found on Device" is the configuration stored in the running configuration on the ASA.

**Step 6** Resolve the conflict by selecting one of the following:

- **Accept Device changes**: This will overwrite the configuration **and any pending changes stored on** Security Cloud Control with the device's running configuration.

  **Note**
  As Security Cloud Control does not support deploying changes to the Cisco IOS devices outside of the command line interface, your only choice for a Cisco IOS device will be to select **Accept Without Review** when resolving the conflict.

- **Reject Device Changes**: This will overwrite the configuration stored on the device with the configuration stored on Security Cloud Control.

**Note**
All configuration changes, rejected or accepted, are recorded in the change log.

# Schedule Polling for Device Changes

If you have Conflict Detection, on page 26 enabled, or if you **Enable the option to auto-accept device changes** from the Settings page,Security Cloud Control polls the device for the default interval to determine if a change has been made to the device's configuration outside of Security Cloud Control. You can customize how often Security Cloud Control polls for changes per device. These changes can be applied to more than one device.

If there is no selection configured for a device, the interval is automatically configured for "tenant default".

**Note** Customizing the interval per device from the **Security Devices** page overrides the polling interval selected as the Default Conflict Detection Interval from the **General Settings** page.

After you enable **Conflict Detection** from the **Security Devices** page or **Enable the option to auto-accept device changes** from the Settings page, use the following procedure to schedule how often you want Security Cloud Control to poll your devices:

### Procedure

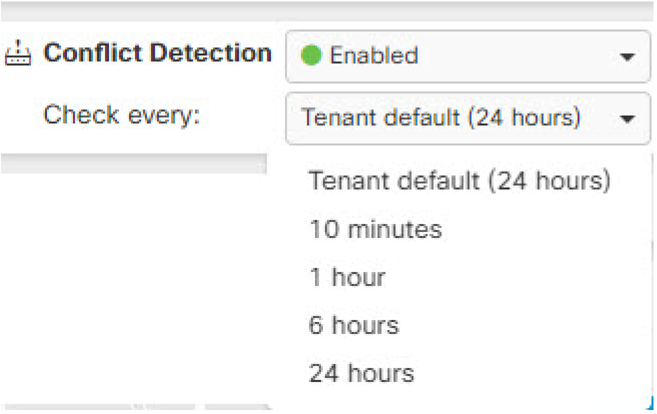
**Step 1** In the left pane, click **Security Devices**.

**Step 2** Click the **Devices** tab to locate your device.

**Step 3** Click the appropriate device type tab.

**Step 4** Select the device or devices for which you want to enable conflict detection.

**Step 5** In the same area as **Conflict Detection**, click the drop-down menu for **Check every** and select the desired polling interval:



Conflict Detection ● Enabled

Check every: Tenant default (24 hours)