FORESCOUT

Forescout

Working with Overlapping IP Addresses

How-to Guide

Forescout Version 8.2

Contact Information

Forescout Technologies, Inc.

190 West Tasman Drive

San Jose, CA 95134 USA

https://www.Forescout.com/support/

Toll-Free (US): 1.866.377.8771

Tel (Intl): 1.408.213.3191

Support: 1.708.237.6591

About the Documentation

- Refer to the Technical Documentation page on the Forescout website for additional documentation: https://www.Forescout.com/company/technical-documentation/
- Have feedback or questions? Write to us at documentation@forescout.com

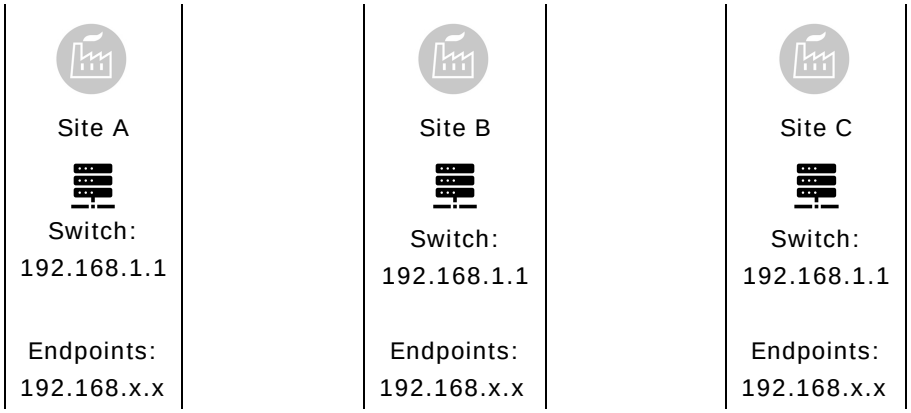
Legal Notice

2020-03-09 13:19

Table of Contents

Working with Overlapping IP Addresses

Overlapping IP addresses occur when IP addresses repeat across your network, as in retail branches, Operational Technology environments, or merged corporate networks.



By default, the Internal Network defined in Forescout only supports a single domain of unique IP addresses. This guide describes configuration options and tools that support networks with overlapping IPs. When these options are enabled, you can configure segments with overlapping IPs and assign these segments to Appliances.

Part of Forescout's Total Solution for OT/IoT and Automation Networks

Overlapping network structures are commonly used in Operational Technology and other automation environments. In addition to the configuration and usage approach described in this guide, the Operational Technology Module and Forescout SilentDefense components are typically deployed to support these environments. See the *Operational Technology Module Configuration Guide* for detailed information about the Forescout solution for Operational Technology/automation environments.

For version requirements and limitations, refer to the Release Notes for the Forescout platform and for related modules and components.

About IP Reuse Domains

IP Reuse Domains distinguish each instance of an overlapping IP address. Within each IP Reuse Domain, IP addresses are unique and cannot overlap.

When support for overlapping IPs is enabled in the Forescout platform, you define IP Reuse Domains as you assign Appliances to various areas of the Internal Network. Endpoints with overlapping IP addresses are identified by the IP Reuse Domain of the Appliance that discovers and reports them.

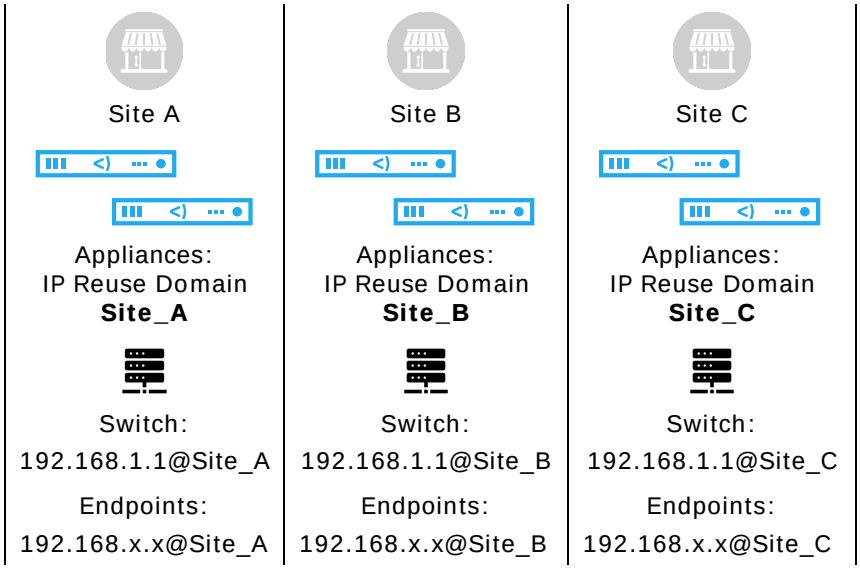
The IP Reuse Domain field appears in relevant areas of the Console, and the IP Reuse Domain is added to IP addresses or segments in NAC view and other views, using the following format:

<IPv4>@IP_Reuse_Domain

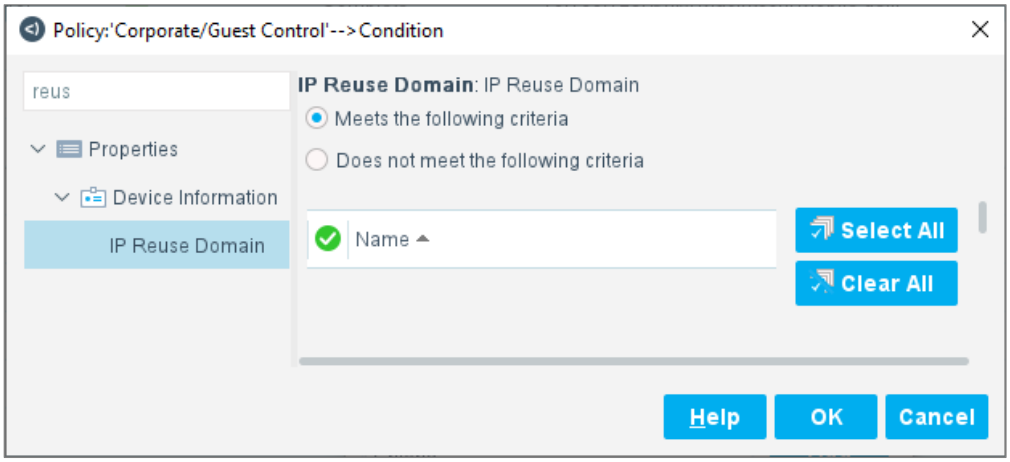
For example:

192.168.0.1@Site_A

IP Reuse Domain settings only appear when this feature is enabled.



The **IP Reuse Domain** host property lets you use the IP Reuse Domain to select endpoints in Forescout policies, and to list endpoints by IP Reuse Domain in Asset Inventory view.



Enable and Disable Support for Overlapping IP Addresses

To enable support for Overlapping IP addresses:

1. Open the Options window and select **Advanced > Overlapping IPs** and select **Allow Overlapping IP Addresses**.

2. (Optional) When SecureConnector is deployed in your network, perform these configuration steps:
   a. In the Options window, select **Linux**. Select the **SecureConnector** tab.
   b. In the *Overlapping IP Addresses* area:
      - Enable the **Specify a local Appliance interface for SecureConnector communication** checkbox.
      - In the **Local Appliance interface name** field, enter the text label of a local interface on the Appliance.
   c. In the Options window, select **Mac OS X**. Repeat these settings in the *Overlapping IP Addresses* area of the **SecureConnector** tab.

   See Deploy SecureConnector in Networks with Overlapping IP Addresses for more information about these settings.
3. Use IP Reuse Domains to Assign Overlapping IP Addresses to Appliances
4. Configure Switches and Controllers in IP Reuse Domains
5. (In OT/automation environments) Map IP Reuse Domains in Operational Technology Environments. When the Operational Technology Module and other SilentDefense components are deployed in your environment, you must map the IP Reuse Domains you define in the Forescout platform to the IP Reuse Domains defined in Forescout SilentDefense components.
6. (Optional) If you use Splunk to process data from the Forescout platform, you must review and edit Splunk queries. See Reference IP Reuse Domains in Splunk Queries

Once you create and use IP Reuse Domains, you cannot disable support for overlapping IPs until you remove all IP Reuse Domain assignments and delete all defined IP Reuse Domains.

Use IP Reuse Domains to Assign Overlapping IP Addresses to Appliances

This section describes how to configure IP Reuse Domains when you assign segments to Appliances. Perform this procedure after you enable support for overlapping IP addresses, as described in Enable and Disable Support for Overlapping IP Addresses.

To assign overlapping IP addresses to Appliances:

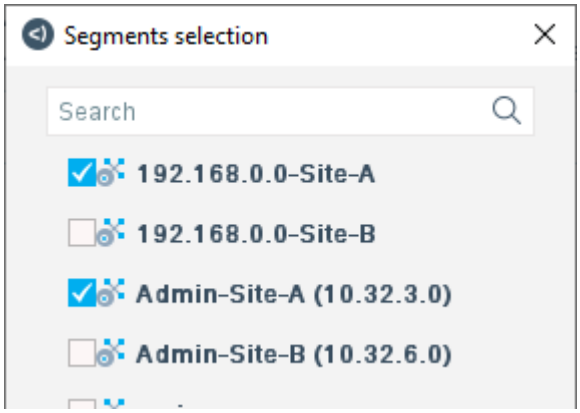
1. In Segment Manager, define segments that reflect repeated structures while distinguishing each instance. For example, in a simple case of branch offices:

Site A	Site B
Segment 192.168.0.0-Site-A	Segment 192.168.0.0-Site-B
Admin-Site-A (10.32.3.0)	Admin-Site-B (10.32.6.0)

Segments in Site A and Site B share overlapping IP addresses (192.168.0.0). Each site also has a segment without overlapping IP addresses, that should be configured as part of the default/global network.

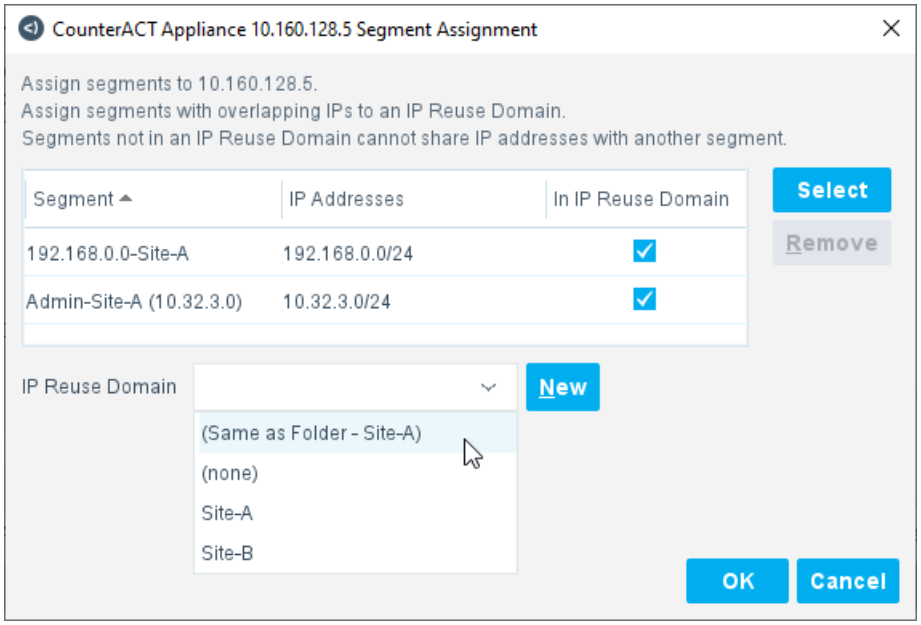
2. (Recommended) Define IP Reuse Domains before you configure overlapping areas of the Appliance tree. Go to **Options > CounterACT Devices > Overlapping IPs Management**. Define an IP Reuse Domain for each overlapping site. You can also define IP Reuse Domains as you configure the Appliance tree, as described in the following steps.
3. If your environment includes a SilentDefense deployment with IP Reuse Domains, plan the IP Reuse Domains in the Forescout platform to correspond to the IP Reuse Domains defined in Command Center. See Map IP Reuse Domains in Operational Technology Environments.
4. Go to **Options > CounterACT Devices > IP Assignment and Failover**. As you work in this pane, use IP Reuse Domains to distinguish sites with overlapping IP addresses.
   a. Assign segments of an overlapping site to Appliance(s) or folder(s) dedicated to that site. To open the *Segment Assignment* dialog, do one of the following:
      › Right-click a folder and select **Assign Segments**.
      › Select an Appliance and select **Assign**.

      Then select **Select** to choose segments of one overlapping site.



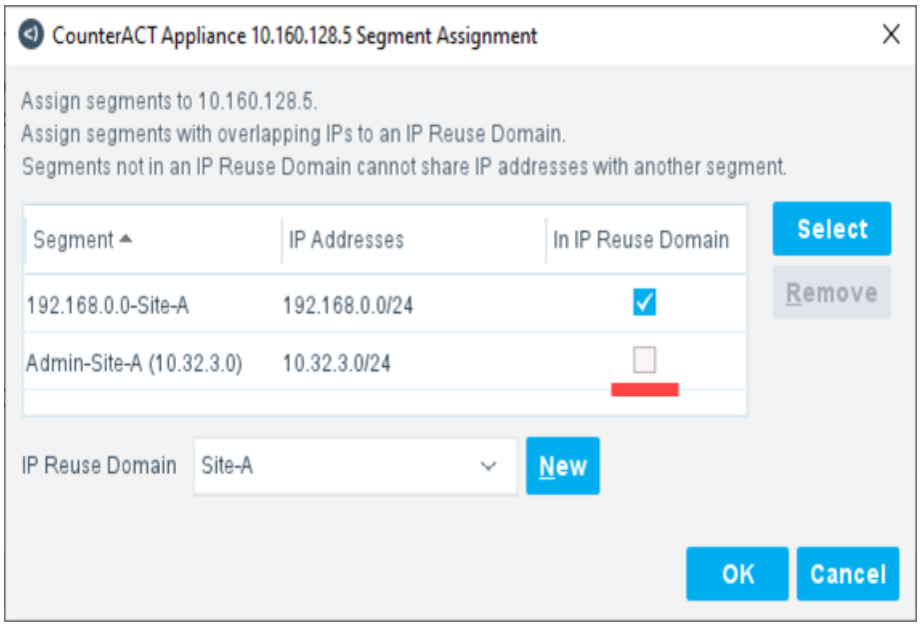
   b. In the IP Reuse Domain field, do one of the following:
      › Select an existing IP Reuse Domain
      › Select **New** to create a new IP Reuse Domain.
      › Select *(none)* to exclude this Appliance/folder from all IP Reuse Domains. This Appliance/folder is in the default/global network.
      › Select *(Same as Folder)* to inherit this setting from parent folders.

Tip: When several Appliances support an overlapping site, place the Appliance tree that handles the site under a folder. Assign an IP Reuse Domain to that top-level folder, and use the Same as Folder *option in child folders and Appliances.*



c. (Optional) When an Appliance/folder is assigned to an IP Reuse Domain, you can exclude individual segments from the IP Reuse Domain. Clear the **In IP Reuse Domain** checkbox for a segment to place it in the default/global network.

In the example shown, segment Admin-Site-A is excluded from the IP Reuse Domain, but is still managed by an Appliance that handles Site A. This segment is in the default/global network.



Use this method to configure Wireless/SDN controllers in overlapping sites. See Configure Switches and Controllers in IP Reuse Domains.

5. If the overlapping site includes switches, Appliances in the site's IP Reuse Domain manage the switches. See Use IP Reuse Domains for Switches with Overlapping IP Addresses.
6. Repeat this procedure for the other sites. Assign overlapping sites to different Appliances, and give Appliances of each site a unique IP Reuse Domain. The IP Reuse Domain uniquely identifies each instance of an overlapping IP address.

Note that:

- Areas of the network without overlap are largely unaffected when you enable support for overlapping IP addresses. Nodes of the Appliance tree that do not contain overlapping IP addresses do not require IP Reuse Domains. All these nodes form a single default/global network. IP addresses must be unique in this default/global network.
- When you enable support for overlapping IP addresses, there are limitations in Failover Cluster functionality:
  - You can define failover clusters as in previous releases when folders do not include overlapping sites.
  - You cannot define failover between two overlapping sites. A failover cluster cannot include Appliances in two different IP Reuse Domains.
  - Similarly, a failover cluster cannot include both segments in the global/default network and segments in an IP Reuse Domain.
- Failover clusters may not work in branches of the Appliance tree that handle overlapping sites. In particular, failover does not work when you configure a failover cluster in a folder that includes both segments in the global/default network and segments in an IP Reuse Domain.
- Once you create and use IP Reuse Domains, you cannot disable support for overlapping IPs until you remove all IP Reuse Domain assignments and delete all defined IP Reuse Domains.
- Segments that include IPv6 addresses cannot be placed in IP Reuse Domains. Typically overlapping networks are supported by the larger IPv6 address space.
- Endpoints discovered based on their MAC address are not assigned to an IP Reuse Domain until their IP address is learned.
- To simplify management, it is strongly recommended to place all instances of overlapping IP addresses in IP Reuse Domains. Technically it is possible to keep a single instance of an overlapping IP address in the default/global network. This may be useful when a merge of new and existing networks causes overlap. The current network definition remains unchanged, and newly incorporated sites are assigned to one or more IP Reuse Domains.

Configure Switches and Controllers in IP Reuse Domains

This section describes how to configure switches and controllers to support overlapping IP addresses.

Switches and wireless/SDN controllers interact with two Appliances:

- The Connecting Appliance you specify when you add the device in the Switch Plugin or Wireless Plugin configuration pane.
- The Appliance that handles the switch's IP address, as defined in the Appliance tree.

To report endpoints with overlapping IP addresses, switches or controllers in an overlapping site must be managed by a Connecting Appliance with the IP Reuse Domain of that site. Endpoints reported by these devices receive the IP Reuse Domain of the Connecting Appliance. Switch and controller deployment should parallel IP Reuse Domains so that endpoints can be resolved to an IP Reuse Domain.

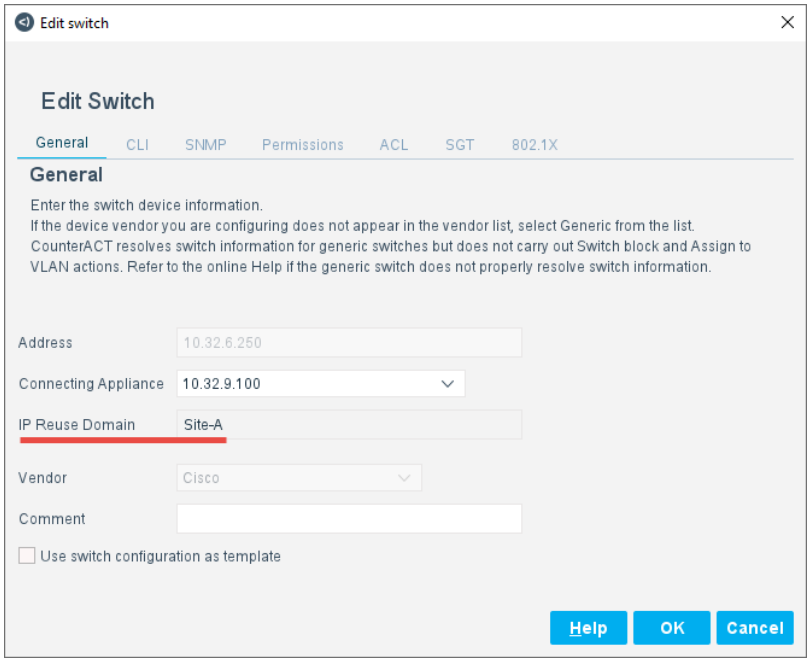
To configure multiple switches with an overlapping IP address, recall that each switch interacts with two Appliances:

- The Connecting Appliance
- The Appliance that handles the switch's IP address

Both these Appliances must be in the same IP Reuse Domain for each switch.

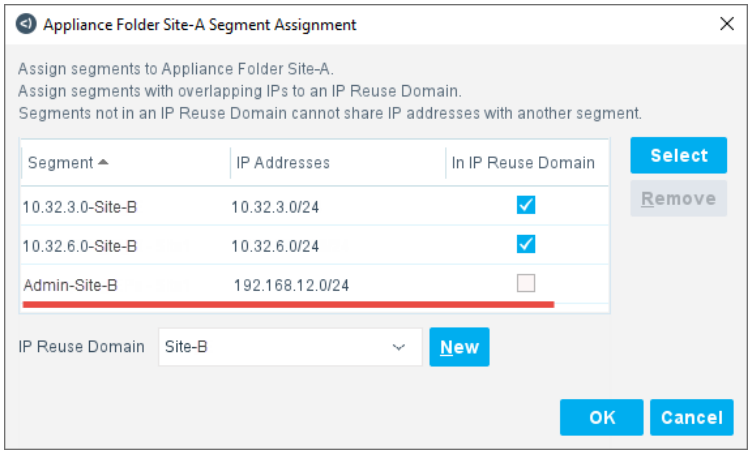
This option is not available for wireless/SDN controllers.

You may define a switch in the Forescout platform with an FQDN instead of an IP address. If your network has a directory server in each branch site, assign all segments of the branch site to the IP Reuse Domain of the site.



When the IP address of a switch or controller is unique, you can place it in the default/global network, not in an IP Reuse Domain. Typically, a segment containing this IP address is included in the Appliance folder that handles the overlapping site, but the **In IP Reuse Domain** checkbox is cleared for this segment.

- *This is the only configuration option available for wireless/SDN controllers. You cannot configure multiple controllers with overlapping IP addresses.*
- *Specify a Connecting Appliance that is in an IP Reuse Domain.*



Map IP Reuse Domains in Operational Technology Environments

This section describes additional configuration steps for environments that include SilentDefense components.

Networks in plant/production, building automation, and other Operational Technology environments often contain duplicate sites and network structures. IP addresses repeat, or *overlap*, across the network.

To support these networks, the Forescout platform and the SilentDefense solution use *IP Reuse Domains* to distinguish several instances of an overlapping IP address. You define a unique IP Reuse Domain for each repeated segment or network branch. IP addresses are unique in each IP Reuse Domain.

- In the Forescout platform, IP Reuse Domains are assigned to Appliances. Identical segments are distinguished from each other by the IP Reuse Domain of the Appliance that manages each segment.
- In SilentDefense, IP Reuse Domains are defined in the Command Center Console and assigned to selected Sensors.

The IP Reuse Domains you define in the Forescout platform must correlate to the IP Reuse Domains defined in your SilentDefense deployment.

The Operational Technology Module integrates the Forescout platform with your SilentDefense deployment. Use this module to:

- Define the Forescout platform connection to Command Center.
- Define the mapping between IP Reuse Domains, as described below.

For more information about Operational Technology support in the Forescout platform, refer to the *Operational Technology Module Configuration Guide*.

Before you begin, review the IP Reuse Domains defined in Command Center, as described in the *SilentDefense Installation and Configuration Guide*.

To map IP Reuse Domains to Command Center:

1. To review IP Reuse Domains defined in the Forescout platform, go to **Options > CounterACT Devices > Overlapping IPs Management** in the Console. The table shows segments in each IP Reuse Domain.

   To work with IP Reuse Domain information outside the Console (for example, to compare IP Reuse Domains between the Forescout platform and Command Center) select **Export**.

2. Go to **Options>Operational Technology** and select the *IP Reuse Domain Mapping* tab.
3. To define mapping between an IP Reuse Domain defined in the Forescout Internal Network and IP Reuse Domains defined in the SilentDefense Command Center:
   a. Select **Add** or select an existing rule and select **Edit**.
   b. In the **Internal Network IP Reuse Domain** drop-down, select an IP Reuse Domain.
   c. In the **Command Center IP Reuse Domains** field, enter a comma-separated list of IP Reuse Domains defined in the SilentDefense Command Center.
   d. Select **OK**.
4. Repeat this procedure to define a mapping rule for each IP Reuse Domain defined in the Forescout platform.
5. Select **Test** to test the mapping rules. The SilentDefense IP Reuse Domains listed in mapping rules must be present in the Command Center defined in the Command Center tab.
6. Select **Apply** to save the definitions.

Define Policy Scope with Overlapping IP Addresses

When overlapping IP addresses are legal in the Internal Network, you can define multiple segments with the same IP address range.

IP Reuse Domains distinguish each instance of an overlapping IP address. Within each IP Reuse Domain, IP addresses are unique and cannot overlap.

When you define the scope of a policy, remember that:

- Segments only inherit an IP Reuse Domain when they are assigned to an Appliance in the Internal Network.
- When a segment with overlapping IP addresses is included in the scope of a policy, the IP Reuse Domain of the Appliance that manages the segment restricts the policy scope.

  Endpoints with the same IP addresses that are discovered outside this IP Reuse Domain are *not* in the scope of the policy.

In addition, you can use the **IP Reuse Domain** host property to explicitly match endpoints in specified IP Reuse Domains.

In the following example, segments define overlapping IP addresses in different sites of the network.

Segment name	IP range	Appliance	IP Reuse Domain
Segment_1_Site_A	192.168.0.0-192.168.0.99	Appliance Handling Site A	Site_A
Segment_1_Site_B	192.168.0.0-192.168.0.99	Appliance Handling Site B	Site_B

When you add *only* **Segment_1_Site_A** to the scope of the policy:

- Endpoint 192.168.0.3@Site_A is in the policy scope.
- Endpoint 192.168.0.3@Site_B is *not* in the policy scope.

Deploy SecureConnector in Networks with Overlapping IP Addresses

SecureConnector is a small-footprint executable that runs on the endpoint. It reports endpoint information to the Forescout platform and implements actions on the endpoint.

To deploy SecureConnector on an endpoint, Appliances generate an installer package. This package can be downloaded to the endpoint in an interactive session with the end user, or distributed in the background to devices by the network administrator.

The installer refers the endpoint to the address and port that the Appliance exposes for SecureConnector communication.

- In the default/global network, Forescout devices can redirect SecureConnector communication to the endpoint's home Appliance. A single installer package can be distributed across the network.
- In the part of the network that is configured with IP Reuse Domains, Appliances cannot redirect SecureConnector communication. In each overlapping site, SecureConnector must be downloaded from an Appliance in the site. Once installed, SecureConnector can only communicate with this Appliance. This is true even if the IP address of the endpoint is logically part of the default/global network and is excluded from the IP Reuse Domain.

Configuration options that redirect endpoints between Appliances are not available when overlapping endpoints are managed by SecureConnector. For example, Automatic IP allocation for load sharing and failover cluster definition are not supported.

Reference IP Reuse Domains in Splunk Queries

eyeExtend for Splunk integrates between the Forescout platform and Splunk.

This section describes changes to Splunk integration when overlapping IP addresses are supported in the Forescout Internal Network.

IP Reuse Domains are used to distinguish several instances of an overlapping IP address. IP addresses are unique in each IP Reuse Domain and cannot overlap within a domain.

Splunk support for IP Reuse Domains is asymmetrical: Splunk can retrieve the IP Reuse Domain value and use it to distinguish endpoints with overlapping IPv4 addresses in retrieved data. However, eyeExtend for Splunk cannot use the IP Reuse Domain to apply actions or adaptive response functions to an endpoint with an overlapping IP address.

Modify Splunk Queries to Include IP Reuse Domain Information

Follow these guidelines to modify Splunk queries so they retrieve IP Reuse Domain information and distinguish endpoints with overlapping IP addresses. The IP Reuse Domain is provided by the **area_code** field.

Modify queries or dashboard/alert statements that use **ct_hostinfo** as a datasource, or have **fillnull**, **dedup ip** or **ip** statements.

To use the area_code variable in a Splunk query to distinguish overlapping IP addresses:

1. Add the following statement:

   rename host_properties.area_code{}.value as area_code

2. Add **area_code** to **fillnull** statements.

3. Add **area_code** as part of **dedup** statements.

In the following example, the query **es_trigger_bad_dns_notification** is modified.

Original Query

```
`get_index` `get_sourcetypes`
`ct_hostinfo` dnsniff_event

rename
host_properties.dnsniff_event{}.value
as dnsniff_event
```

Modified Query

```
`get_index` `get_sourcetypes`
`ct_hostinfo` dnsniff_event

rename
host_properties.dnsniff_event{}.value
as dnsniff_event

rename
host_properties.area_code{}.value as
area_code
```

```
mvexpand dnsniff_event

rex field=dnsniff_event "DNS Query
Type:\s*(?<DNSQueryType>[^;^$]);DNS
Query/Response: Query;DNS Zone: ;DNS
Addresses."

search DNSQueryType="A"

fillnull value="" ip ipv6 mac

eventstats count as eventcount by ip
ipv6 mac

dedup ip, ipv6, mac

where eventcount>5 AND eventcount<=10
```

```
mvexpand dnsniff_event

rex field=dnsniff_event "DNS Query
Type:\s*(?<DNSQueryType>[^;^$]);DNS
Query/Response: Query;DNS Zone: ;DNS
Addresses."

search DNSQueryType="A"

fillnull value="" ip ipv6 mac
area_code

eventstats count as eventcount by ip
ipv6 mac area_code

dedup ip, ipv6, mac area_code

where eventcount>5 AND eventcount<=10
```