FORESCOUT

Forescout

eyeSegment Module

Configuration Guide

Version 2.0

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

Legal Notice

2019-11-10 11:19

Table of Contents

About This Guide **4**

About eyeSegment **4**

How It Works 5
Additional Forescout Components 5
eyeSegment Components 6
Requirements 7

What to Do **7**

Ensure That the Component Is Running **7**

Prepare Groups for the eyeSegment Matrix **8**

Best Practices for Creating eyeSegment Zones 8
Best Practices for Creating eyeSegment Filters 9

Create an eyeSegment Policy Compliance Policy **10**

Open the eyeSegment Web Portal **12**

Considerations and Troubleshooting **14**

Notifications Not Received 14

Additional Forescout Documentation **15**

Documentation Downloads 15
Documentation Portal 16
Forescout Help Tools 16

About This Guide

This guide provides information about the new, de-centralized Forescout eyeSegment Module responsible for aggregating traffic from various sources, and for the eyeSegment web portal where you can simplify segmentation planning and automate ACL/VLAN assignment to reduce your attack surface.

Refer to the *eyeSegment Web Portal How-to Guide* for information about using the eyeSegment web portal to view and leverage dynamic zone-to-zone relationship mapping data. The guide is available from the eyeSegment web portal menu and from your Forescout sales representative.

About eyeSegment

eyeSegment allows you to analyze your physical network traffic from a dynamic zone perspective. This helps you decouple the static constraints of a physical network from the dynamic business logic that modern segmentation policies require.

The eyeSegment product provides:

- Segmentation intelligence driven by the fusion of dynamic zone context and dynamic flow context
- A network traffic baseline using traffic data accumulated over time
- A consolidated visibility pane for mapping and analyzing traffic to and from various sources in and out of the network, and for identifying simulated traffic rule violations and conflicts
- A policy management pane for creating an eyeSegment policy using rules that simulate allowing or denying specific traffic

Use the eyeSegment product to:

- Monitor traffic to understand device dependencies, then map, plan, and deploy network segments.
- Assess devices on the fly to automate segmentation assignment.
- Monitor the network for anomalous communication.
- Use dynamic Source and Destination zones to easily create and visualize an eyeSegment policy that simulates denying traffic for a specific segment and filter, and enable notification when a simulated traffic violation is detected.
- Identify simulated traffic violations to improve your enforcement and eyeSegment policy rules.
- Visualize the policy rules as a layer in the matrix, and ensure that devices do not have conflicting rules.

You can define a single matrix that shows traffic for the eyeSegment zones you select.

The eyeSegment product does not support:

- *Certification Compliance mode*

- *Devices that do not have IPv4 addresses*

How It Works

1. The managing Appliances receive and analyze the mirrored traffic data captured by the Forescout Packet Engine and the Forescout Flow Collector.
2. The Forescout Cloud Uploader compresses the traffic data, and then uses encrypted protocol to send it to the cloud where the data is processed and analyzed.
3. The communication patterns between dynamic policy groups and zones is dynamically mapped in a web-based matrix of network traffic connectivity.
4. Drill down into the matrix to learn:
   - The ports used by the traffic.
   - The traffic volume between any pair of zones.
   - The IP addresses and other details of the devices that used each traffic pattern.
5. Use the displayed information to:
   - Redefine your matrix to focus on traffic of interest.
   - Plan your eyeSegment policy for controlling the traffic between specific zones.
   - Refine your eyeSegment policy to ensure that it tags suspicious traffic.
   - Visualize a dashboard for SOC monitoring.
6. If a device sends or receives traffic that violates a simulated eyeSegment policy rule:
   - A Forescout policy can send email and Syslog notifications. (Optional)
   - You can apply a network or endpoint action, such as a Switch Block or Virtual Firewall action. (Optional)

Additional Forescout Components

The feature is based on the following additional Forescout components:

- Flow Collector Plugin – Supplies flow information that populates the traffic layer in the network connectivity matrix.
- Packet Engine Plugin – Parses and analyzes the mirrored data that populates the traffic layer in the network connectivity matrix.
- Cloud Uploader Plugin - Manages access to the cloud where the traffic data is stored. For information about the Cloud Uploader and its configuration, contact your Forescout sales representative.

eyeSegment Components

In this version, you can define a single matrix that shows traffic for the eyeSegment zones you select.

eyeSegment uses the following components:

- eyeSegment zones – Dynamically tagged devices based on detected characteristics, such as function, user role and/or location. Zones are based on standard Forescout policy groups that can be populated manually or via a policy. Single IP addresses and Forescout segment objects can be groups. Groups can be arranged in hierarchal levels where each level of the nested structure below Level 0 is a sub-group.

  The eyeSegment module automatically creates virtual zones to includes devices that are not in any of the Forescout policy groups selected as matrix zones. Virtual zone names begin with <).

  eyeSegment zones can include the following:

Forescout policy groups	These groups are selected by the user to be included in the matrix. *Note: Each level of a nested structure includes all of its sub-groups.*
<) **Internal Network**	Contains all IP addresses included in Forescout's internal network and not in another user-defined Source or Destination zone in the matrix.
<) **Private Network**	Contains all IP addresses that are not in Forescout's internal network but are in the company's private network.
<) **Multicast/Broadcast**	Contains multicast and broadcast address ranges.
<) **Internet**	Contains all IP addresses that are not in any other zone.

  Each eyeSegment zone can be designated as a Source zone or a Destination zone or both.

- Filters (optional) – Groups or services used to filter the displayed matrix traffic to specific conditions, such as *London Office*, *High-Risk Assets*, and *Remote Devices*, so that the matrix shows only traffic of interest. Filters can be used to create accurate, intersected eyeSegment policy rules.
- Forescout properties - The following device properties are updated upon detection of traffic that violates a simulated eyeSegment policy rule:
  - *Traffic Was Denied from This Client*: Lists all simulated eyeSegment policy rules that denied traffic from the device.
  - *Traffic Was Denied to This Server*: Lists all simulated eyeSegment policy rules that denied traffic to the device.
- eyeSegment Policy Compliance policy template – A template accessible from the Console for creating policies that send notifications when a device's client or server traffic violates an eyeSegment policy rule.

Requirements

Refer to the *eyeSegment Module Release Notes* for the list of requirements for eyeSegment.

What to Do

1. Verify that your environment meets the requirements. Refer to the eyeSegment Module Release Notes.
2. To ensure that traffic data is collected from port mirroring, configure channels in the Console using the Channel Configuration dialog box. Refer to the Forescout Administration Guide for more information.

   To access the Forescout Administration Guide, see Additional Forescout Documentation.
3. Ensure That the Component Is Running.
4. Prepare Groups for the eyeSegment Matrix.
5. Ensure that eyeSegment web portal users know their Forescout web portal credentials. To create users, refer to the User Management section in the Forescout Administration Guide.
6. In the eyeSegment web portal, create and fine-tune a simulated eyeSegment policy. The connectivity matrix shows you the traffic that your eyeSegment policy rules would allow or deny.

   In this version, you can define a single matrix that shows traffic for the eyeSegment zones you select.
7. In the Console, use the eyeSegment Policy Compliance policy template to create and fine-tune a Forescout policy that sends email and Syslog messages when a device violates your simulated eyeSegment policy rules. See Prepare Groups for the eyeSegment .

Ensure That the Component Is Running

After installing the component (and configuring it, if necessary), ensure that it is running.

To verify:

1. Select **Tools** > **Options** > **Modules**.
2. Navigate to the component and hover over the name to view a tooltip indicating if it is running on Forescout devices in your deployment. In addition, next to the component name, you will see one of the following icons:
   - - The component is stopped on all Forescout devices.

- – - The component is stopped on some Forescout devices.
- – - The component is running on all Forescout devices.

3. If the component is not running, select **Start**, and then select the relevant Forescout devices.
4. Select **OK**.

Prepare Groups for the eyeSegment Matrix

Forescout groups dynamically tag devices based on detected characteristics, such as IP taxonomy, function, user role and/or location. eyeSegment zones are based on these standard Forescout groups that can be populated manually or via a policy. Single IP addresses and Forescout segment objects can be groups. Groups can be arranged in hierarchal levels where each level of the nested structure below Level 0 is a sub-group.

Ensure that the policies that manage the groups are run on the devices to be included in the matrix.

To create groups, refer to the Forescout Administration Guide. To access the Forescout Administration Guide, see Additional Forescout Documentation.

Ensure that specific groups defined in your configuration contain the devices whose traffic you want to track. You can define sub-groups within groups to further narrow the device scope of a zone within an eyeSegment policy rule. Devices that are not members of any of your Forescout policy groups are automatically assigned to a virtual zone by the eyeSegment module.

The Console Groups Manager does not allow you to delete a group that is used in the network connectivity matrix or in an eyeSegment policy rule. You must first remove the group from the matrix in the eyeSegment web portal's Matrix Settings window and from all eyeSegment policy rules.

Best Practices for Creating eyeSegment Zones

To create groups to be used as eyeSegment zones:

1. To easily identify your potential eyeSegment zones, define a parent group named 'IP Taxonomy Zones'.
2. Create lower level sub-groups under this parent group for all the device types in your environment. The more levels you create, the more you will be able to pinpoint specific traffic patterns in eyeSegment. ***Define the sub-groups so that each device in your network is added to one, and only one, of these sub-groups.***
3. Use policies to assign all the devices in your network to their respective sub-groups in this structure.
4. In the eyeSegment web portal, select your eyeSegment zones from these sub-groups.

Each level of the nested structure includes all of its sub-groups.

The following are sample group levels in an 'IP Taxonomy Zones' structure:

IP Taxonomy Zones

A. Servers/Services/Applications

1. User/Client Enterprise Management (Distributed)
   a. AD
   b. Inventory
   c. Vulnerability Assessment
   d. Patch Management
   e. Software Deployment
   f. MDM
2. Enterprise Services
   a. Email
   b. Intranet
   c. Time Clock
   d. Instant Messaging
   e. HR
   f. Finances
   g. Legal
   h. Document Sharing
   i. Help Desk
   j. GRC
3. Infrastructure
   a. Network Devices
   b. Telecom
   c. Physical Security Servers
      (i) Digital Video Records
      (ii) Badge System Database
   d. Security Systems
      (i) Proxy
      (ii) SIEM
      (iii) WAF
      (iv) DLP
      (v) EPP
      (vi) EDR
      (vii) ATD
   e. Network Packet Brokers
   f. Virtual
   g. Out-of-Band Server Management
   h. SAN/Storage
   i. Print Servers
   j. DNS/DHCP
   k. Load Balancers
   l. Network and System Monitoring
4. Company Production
   a. Company & Resource Planning
      (i) CAD
      (ii) Enterprise Resource Planning
      (iii) Manufacturing Execution Systems
   b. Company Software Development
      (i) Source Repos, Build Systems, Bug Systems
   c. Research and Development
      (i) Corporate & Academic
   d. Operations
      (i) Licensing
      (ii) Warehousing
      (iii) Customer Success
5. Customer Production
   a. Customer Payment Card Data
   b. Customer Health Records
   c. Customer Education Records
   d. Customer Financial Records
      (i) Internal Customer Service
      (ii) External Customer Website
      (iii) Money Movement
         i. Installed Applications *contains* OpenSpan
   e. Customer Telemetry Records
   f. Customer Usage and Billing

B. Users

1. By Department/Role from AD
   a. User Directory

C. Clients

1. Workstation Without a User
2. Enterprise IoT
   a. Printers
   b. Telecon
   c. Videocon
   d. Smart Meeting room
      (i) Exterior Room Schedule
      (ii) Smart White Board
      (iii) Smart Projector
      (iv) Room Control
      (v) Zoom Room, Webex Room
   e. Digital Signage
   f. Guest Kiosks
   g. Mobile Devices
      (i) Customer demo
      (ii) Productivity
3. Building IoT(OT)
   a. Physical Security
      (i) Cameras
      (ii) Door Access Control
   b. Physical Safety
      (i) Fire Detection, Alarm, Suppression
      (ii) Severe Weather Alarm
      (iii) Shooter Detection
      (iv) Public Safety Integration
   c. Environmental Controls
      (i) Lighting
      (ii) Elevators, Escalators
      (iii) Climate
   d. Energy Controls
      (i) Battery Storage
      (ii) UPS
      (iii) Generators
4. Company Production IoT
   a. Financial Services
      (i) Cash Machines
      (ii) ATMs
   b. Retail
      (i) Point of Sale
      (ii) Smart Shopper
   c. Entertainment
      (i) Gaming, Gambling
      (ii) Bowling, Arcade, Golf
   d. Travel
      (i) Check-In Systems
      (ii) Information Systems
      (iii) Mobile Safety & Customer Service Devices
   e. Medical Equipment
      (i) Medical Imaging
      (ii) Clinical Engineering
   f. Smart City
      (i) Parking
      (ii) Lighting
      (iii) Mass Transit Ticketing

D. OT (ICS Systems)

1. Energy Generation and Distribution
2. Oil & Gas Production
3. Manufacturing
4. Travel

Best Practices for Creating eyeSegment Filters

Set up your Forescout environment so that the devices in your network belong also to groups that are not part of the 'IP Taxonomy Zones' structure. Define these additional group structures based on attributes, such as:

- product lifecycle
- connectivity
- network access layer

- location
- vendor
- compliance
- risk

Each device in your network can belong to multiple sub-groups in these structures. Use these additional groups as filters in the eyeSegment web portal.

The intersection of one or more filter groups with the Source and Destination zones enables you to focus on specific types of devices without the need for a complex taxonomy structure.

Create an eyeSegment Policy Compliance Policy

Use a Forescout policy template to easily create a policy that sends email and Syslog messages when both of the following occur:

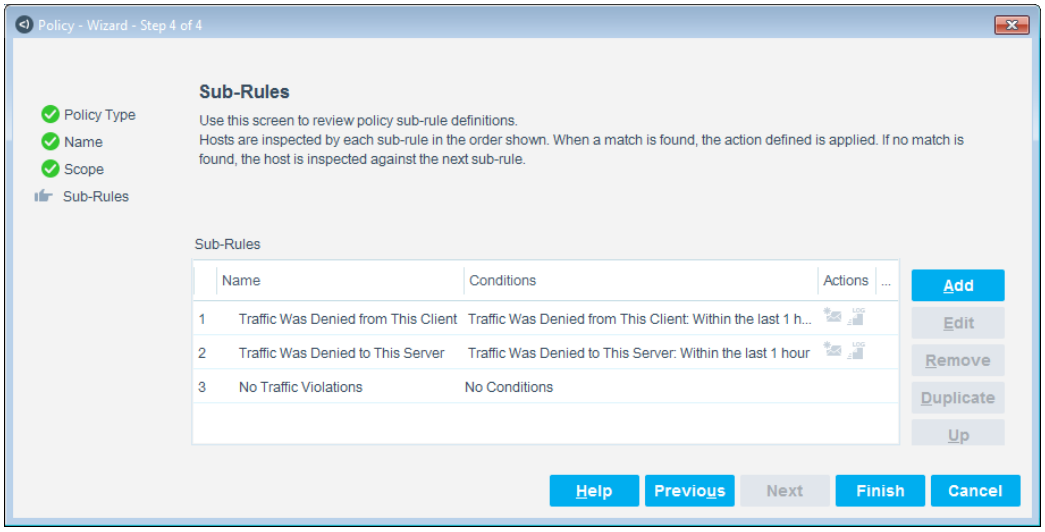
- Traffic violates a simulated eyeSegment policy rule.
- The Notification option was selected in the violated rule.

In the policy template, all sub-rule actions are disabled by default.

Policy conditions created from this template use properties that include the names of your eyeSegment policy rules. You cannot delete a rule from your eyeSegment policy in the web portal unless the rule name is removed from all policy conditions in the Console.

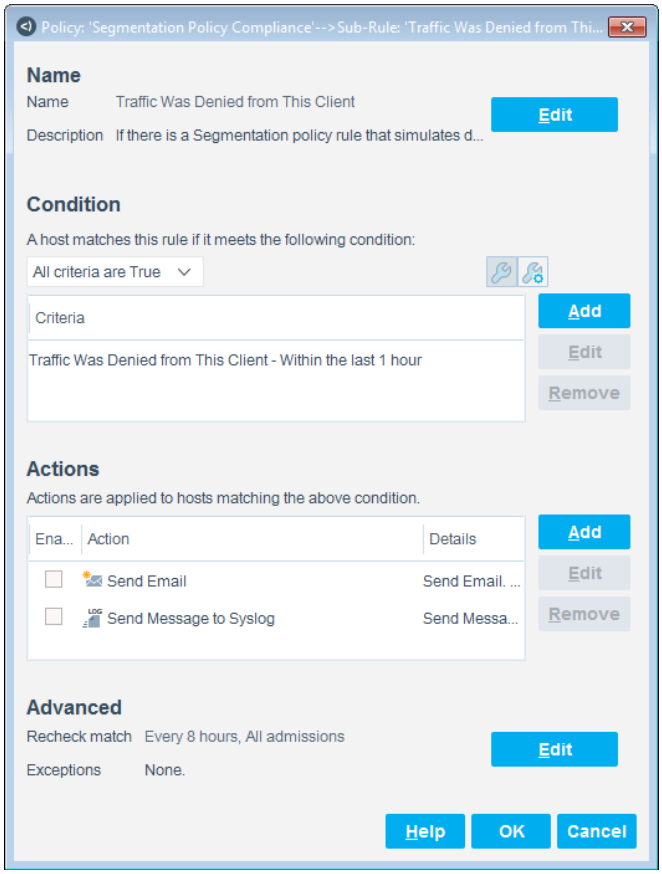
To create a policy:

1. In the Console Policy tab, select **Add**.
2. In the Compliance folder, select **eyeSegment Policy Compliance**, and follow the wizard.
3. In the IP Address Range window, select **All IPs**, and continue to the Sub-Rules window.

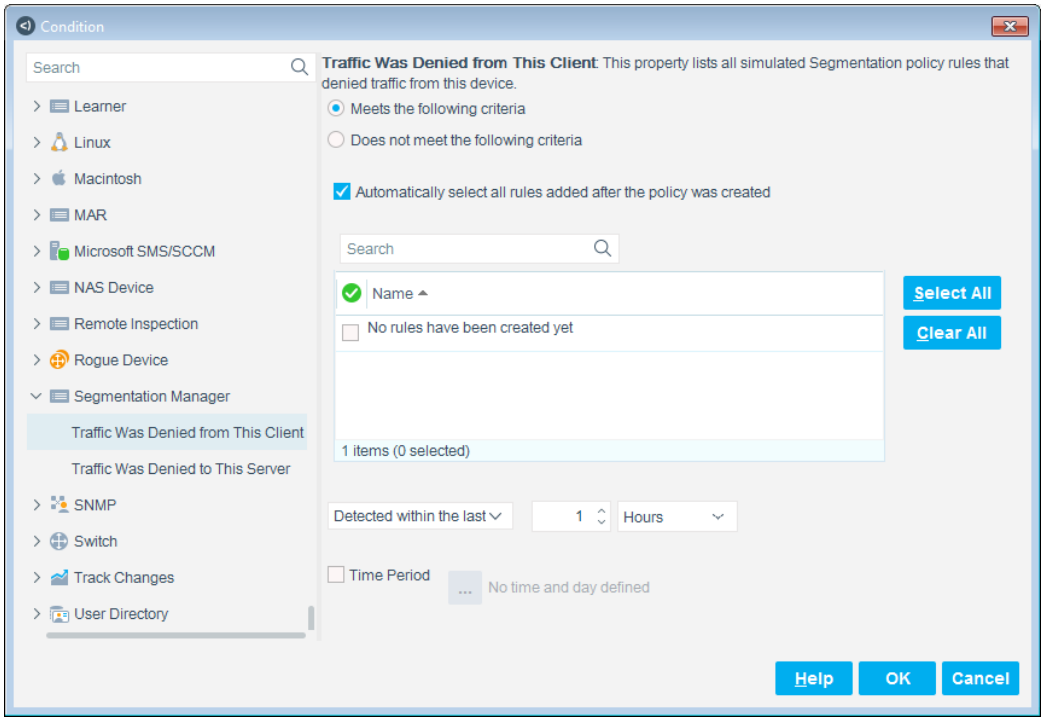


4. For each of the first two sub-rules:

   a. Select and edit the sub-rule.



   b. Select and edit the condition.



› To ensure that violations of future simulated rules will trigger notifications, select **Automatically select all rules added after the policy was created**.

› To ensure that violations of existing simulated rules will trigger notifications, select **Select All**.

c. In the Actions area, enable one or both actions.

When you enable the Send Email action, open the action for editing and make at least one change in the Message to email recipient field. For example, add a space character at the end of the message.

5. After both sub-rules have been edited, save and apply the policy.

Open the eyeSegment Web Portal

If you have a valid *Forescout eyeSegment* license for the eyeSegment Module, you can open the eyeSegment web portal from a web browser or directly from the Console.

To access the eyeSegment web portal:

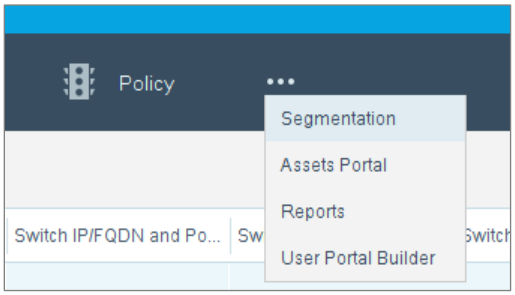
1. Do one of the following:

– Browse to the following URL to log in from a web browser:

https://<Device_IP>/seg

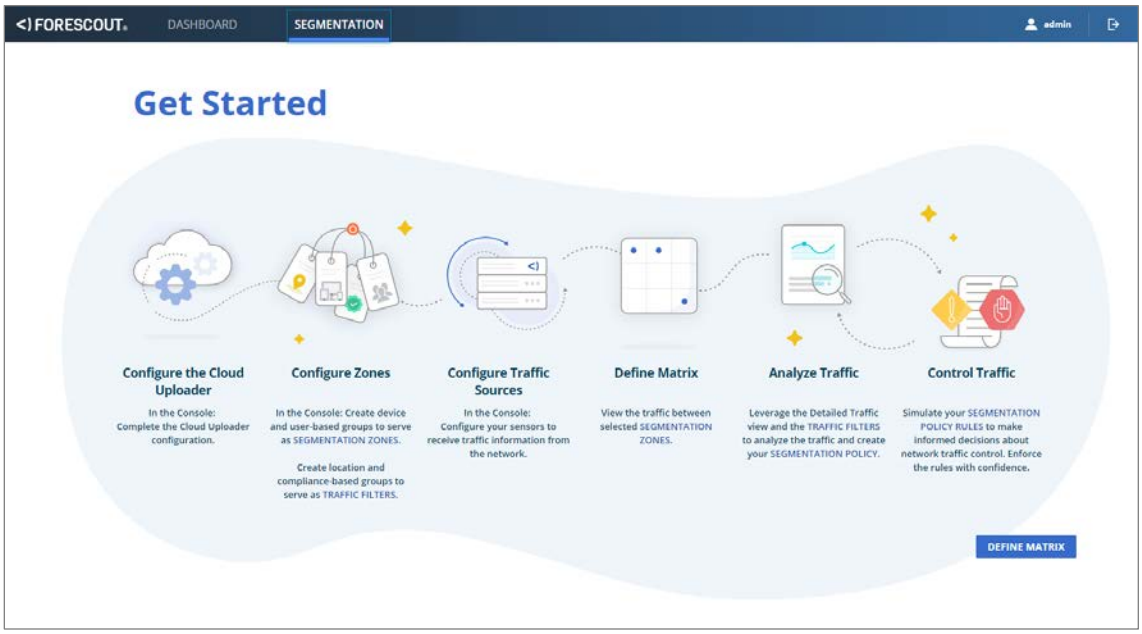
where <Device_IP> is the IP address of the Enterprise Manager or standalone Appliance.

– Select the **Ellipsis icon** ••• from the Console toolbar, and then select **Segmentation** from the dropdown menu.



2. If your configuration requires you to log in, enter your Forescout credentials. Your network configuration might require:
   – Smart Card authentication with or without two-factor authentication
   – acceptance of corporate terms and conditions

3. Select the Segmentation view.
4. The first time you open the eyeSegment web portal, the **Get Started** diagram opens.



Refer to the *eyeSegment Web Portal How-to Guide* for information on leveraging dynamic zone-to-zone relationship mapping data. The guide is available from the eyeSegment web portal menu and from your Forescout sales representative.

Considerations and Troubleshooting

Consider the following when using eyeSegment:

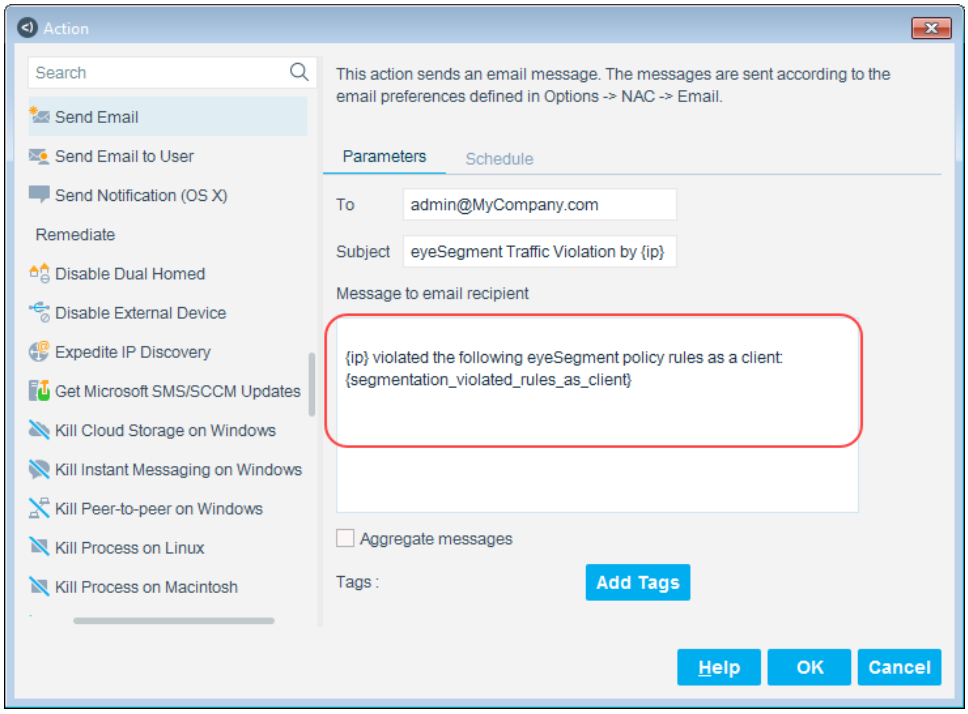
- Notifications Not Received

Notifications Not Received

In this version, the eyeSegment Policy Compliance policy requires a change to the *Message to email recipient* field before it can send email notifications. If your policy is not sending email notifications, ensure that a change is made to this field.

To ensure that the policy can send email messages:

1. In the Console Policy tab, select your eyeSegment Policy Compliance policy, and select **Edit**.
2. In the Sub-Rules area, select **Traffic Was Denied from This Client**, and select **Edit**.
3. In the Actions area, select **Send Email**, and select **Edit**.
4. Make at least one change to the *Message to email recipient* field. For example, add a space character at the end of the message.



5. Select **OK** twice.
6. In the Sub-Rules area, select **Traffic Was Denied to This Server**, and select **Edit**.
7. In the Actions area, select **Send Email**, and select **Edit**.
8. Make at least one change to the *Message to email recipient* field. For example, add a space character at the end of the message.
9. Select **OK** until the policy is updated, and then select **Apply** to apply the changes.

Additional Forescout Documentation

For information about other Forescout features and modules, refer to the following resources:

- Documentation Downloads
- Documentation Portal
- Forescout Help Tools

Documentation Downloads

Access documentation downloads from the Forescout Resources Page, or one of two Forescout portals, depending on which licensing mode your deployment is using.

- ***Per-Appliance Licensing Mode*** – Product Updates Portal
- ***Flexx Licensing Mode*** – Customer Portal

Software downloads are also available from these portals.

To identify your licensing mode:

- From the Console, select **Help > About Forescout**.

Forescout Resources Page

The Forescout Resources Page provides links to the full range of technical documentation.

To access the Forescout Resources Page:

- Go to https://www.Forescout.com/company/resources/, select **Technical Documentation,** and search for documents.

Product Updates Portal

The Product Updates Portal provides links to Forescout version releases, Base and Content Modules, and eyeExtend products, as well as related documentation. The portal also provides a variety of additional documentation.

To access the Product Updates Portal:

- Go to https://updates.forescout.com/support/index.php?url=counteract and select the version you want to discover.

Customer Portal

The Downloads page on the Forescout Customer Portal provides links to purchased Forescout version releases, Base and Content Modules, and eyeExtend products, as well as related documentation. Software and related documentation only appear on the Downloads page if you have a license entitlement for the software.

To access documentation on the Forescout Customer Portal:

- Go to https://Forescout.force.com/support/ and select **Downloads**.

Documentation Portal

The Forescout Documentation Portal is a searchable, web-based library containing information about Forescout tools, features, functionality, and integrations.

If your deployment is using Flexx Licensing Mode, you may not have received credentials to access this portal.

To access the Documentation Portal:

- Go to https://updates.forescout.com/support/files/counteract/docs_portal/ and use your customer support credentials to log in.

Forescout Help Tools

Access information directly from the Console.

Console Help Buttons

Use context-sensitive *Help* buttons to access information about tasks and topics quickly.

Forescout Administration Guide

- Select **Forescout Help** from the **Help** menu.

Plugin Help Files

- After installing the plugin, select **Tools** > **Options** > **Modules**, select the plugin, and then select **Help**.

Online Documentation

- Select **Online Documentation** from the **Help** menu to access either the Forescout Resources Page (Flexx licensing) or the Documentation Portal (Per-Appliance licensing).