FORESCOUT

Forescout

eyeSegment Module

Configuration Guide

Version 3.9

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

2020-11-17 11:19

Table of Contents

About the eyeSegment Module

The de-centralized Forescout eyeSegment Module aggregates traffic from various sources so that you can simplify segmentation planning and automate ACL/VLAN assignment to reduce your attack surface.

> *For information about using the eyeSegment application to view and leverage dynamic zone-to-zone relationship mapping data, refer to the* eyeSegment Application How-to Guide*. You can access this guide from the eyeSegment application menu* ***Help*** *option.*

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.
- Focus on a matrix row, column, or cell to view a matrix of all the sub-zones of the selected Source or Destination parent zone. This ‘focus’ feature allows you to see multiple types and levels of information for hierarchical structures.
- 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 or other actions 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.
- Export details about selected traffic for further study.

You can define and manage 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 the eyeSegment Module Works

1. The managing Appliances receive and analyze the mirrored traffic data captured by the traffic sensors configured in your environment.
2. The Forescout Cloud Uploader Plugin 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 among Forescout policy groups and eyeSight segments 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.
   - Which traffic violated your eyeSegment policy rules.
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 an 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)

eyeSegment Components

In this version, you can define a single matrix for all users that shows traffic for the eyeSegment zones you select. Each user can create and maintain their own Find & Filter criteria for the shared matrix.

eyeSegment uses the following components:

- eyeSegment zones – – Dynamically tagged devices based on detected characteristics, such as function, user role and/or location. Zones are selected from:
  - Forescout eyeSight segments
  - Standard Forescout policy groups that can be populated manually or via a Forescout policy

Single IP addresses can be zones. Segments and groups can be arranged in hierarchal levels where each level of the nested structure below Level 0 is a sub-zone.

In addition to the user-selected zones, the eyeSegment module automatically creates virtual zones to include devices that are not in any of the eyeSight segments or Forescout policy groups selected as matrix zones. Virtual zone names include the symbol <).

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.*
eyeSight segments	These segments are selected by the user to be included in the matrix. *Note: Each level of a nested structure includes all of its sub-segments.*
<) **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.

- *Find & Filter* criteria (optional) – A combination of policy groups, Forescout eyeSight segments, IP addresses, services, inspected protocols, and time range. These criteria filter the displayed matrix traffic to specific conditions, such as *London Office*, *High-Risk Assets*, *Remote Devices*, and the past week, so that the matrix shows only traffic of interest. The *Find & Filter* criteria can be used to create accurate, intersected eyeSegment policy rules, and for finding specific traffic.

  Each user can create and maintain their own *Find & Filter* criteria for the shared matrix.

- Forescout properties - The following device properties are updated upon detection of traffic that violates an eyeSegment policy rule:

  – *Traffic Was Denied from This Client*: Lists each eyeSegment policy rule that traffic from the device violated.

  – *Traffic Was Denied to This Server*: Lists each eyeSegment policy rule that traffic from the device violated.

  – *Server Groups to Which Traffic Was Denied*: Lists the lowest-level Forescout policy group or virtual zone (for devices that are not members of any of your Forescout policy groups) in each eyeSegment policy rule, including exceptions, that contains members to which the rule denied traffic from this client.

  - *Client Groups from Which Traffic Was Denied*: Lists the lowest-level Forescout policy group or virtual zone (for devices that are not members of any of your Forescout policy groups) in each eyeSegment policy rule, including exceptions, that contains members from which the rule denied traffic to this server.

    The following zones are not written to the Server Groups to Which Traffic Was Denied *or* Client Groups from Which Traffic Was Denied *properties:*

    - *Internal Network*
    - *- Any –*
    - *zones that are eyeSight segments*

- 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

If your environment includes devices whose traffic data you do not want uploaded to the cloud, see Prevent Data Upload for Specific Devices.

1. Verify that your environment meets the Requirements.
2. Ensure that the Prepare Traffic Sensors for eyeSegment in your environment are configured to collect and pass traffic data to eyeSegment.
3. Prepare Groups for the eyeSegment Matrix. (Optional)
4. Assign eyeSegment User Permissions.

   To create users and set user permissions, refer to the Managing Users *section in the* Forescout Administration Guide*.*

5. Install the eyeSegment Module.
6. Ensure Connectivity.
7. Ensure that eyeSegment application users know their Forescout web portal credentials.
8. In the eyeSegment application's matrix settings, users with Permissions to Update can select Source and Destination zones whose traffic is of interest.

   The connectivity matrix indicates if there was traffic between these zones.
9. In the eyeSegment application, users with Permissions to View or Permissions to Update can 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.

10. In the eyeSegment application, users with Permissions to Update can create and fine-tune an eyeSegment policy.

    The connectivity matrix shows which traffic the simulated eyeSegment policy rules allow or deny.

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

11. In the Console, use the eyeSegment Policy Compliance policy template to create and fine-tune a Forescout policy that sends email and Syslog messages whenever a device violates your eyeSegment policy rules. See Create an eyeSegment Policy Compliance Policy.

Prepare Traffic Sensors for eyeSegment

eyeSegment displays traffic data captured by traffic sensors configured in your environment. In this version, these traffic sensors can be provided by:

- Forescout Flow Collector
- Forescout Packet Engine
- Forescout SilentDefense
- AWS Virtual Private Cloud
- Medigate

eyeSegment uses the Forescout Cloud Uploader to upload the data provided by these traffic sources to the Forescout cloud. For information about the Cloud Uploader and its configuration, refer to the *Cloud Uploader Configuration Guide*.

Forescout Flow Collector

The Flow Collector is a plugin in the Forescout Core Extensions Module. The Flow Collector supplies information to eyeSegment from switches, routers, and other network devices that report flow session data. To ensure that flow data is collected, configure the Flow Collector in the Console. For information about the Flow Collector and its configuration, refer to the *Forescout Flow Collector Configuration Guide*.

Forescout Packet Engine

The Packet Engine is a plugin in the Forescout Core Extensions Module. The Packet Engine parses and analyzes mirrored data, and passes it to eyeSegment. To ensure that traffic data is collected from port mirroring, configure channels in the Console using the Channel Configuration dialog box. For more information, refer to the *Working with Appliance Channel Assignments* section in the *Forescout Administration Guide*.

Forescout SilentDefense

SilentDefense offers better visibility of your OT devices and their traffic, with no additional device or traffic configuration. SilentDefense's Deep-Packet Inspection (DPI) techniques provide inspected protocol values that are more accurate than standard Linux port-to-protocol mapping. SilentDefense sensors automatically pass traffic data to eyeSegment.

Ensure that the Forescout Operational Technology Module (OTSM) is configured to share NetFlow data with eyeSegment. Refer to the *Operational Technology Module Configuration Guide* or Release Notes for more information.

Refer to the *eyeSegment Module Release Notes* for the list of supported Forescout Operational Technology Module versions.

AWS Virtual Private Cloud

AWS offers better visibility of your AWS devices and their traffic. The AWS Plugin periodically pulls the flow logs from AWS VPCs, and extracts and passes the flow session data to eyeSegment.

In the AWS dashboard, create flow logs containing data about communication between hosts. Be sure to:

- Set the **Destination** option to **Send to an S3 bucket**.
- Set the **Log record format** option to **Custom format**, and include the following fields:
  - srcaddr
  - dstaddr
  - srcport
  - dstport
  - protocol
  - action
  - account-id
  - log-status
  - vpc-id
  - tcp-flags

In the Forescout AWS Plugin configuration, for each VPC:

- Include the Amazon Resource Names (ARNs) of the S3 buckets.
- Set how frequently the flow log data is to be pulled from the VPC.

Refer to the *Forescout AWS Plugin Configuration Guide* for more information.

Refer to the *eyeSegment Module Release Notes* for the list of supported Forescout Amazon Web Services (AWS) Plugin versions.

Medigate

Medigate offers better visibility of your medical devices and their traffic, with no additional device or traffic configuration. Medigate's Deep-Packet Inspection (DPI) techniques provide inspected protocol values that are more accurate than standard Linux port-to-protocol mapping. The Forescout Medigate Plugin automatically passes data from Medigate Collection Servers to eyeSegment.

In the Forescout Medigate Plugin configuration:

- Select **Enable eyeSegment integration**.
- Set the appropriate port number for integration with eyeSegment.

Refer to the *Forescout Medigate Module Configuration Guide* for more information. Refer to the *eyeSegment Module Release Notes* for the list of supported Forescout Medigate Module versions.

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 can be based on these standard Forescout groups that can be populated manually or via a policy. Single IP addresses and Forescout eyeSight 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 *Working with Forescout Groups* section in the *Forescout Administration Guide*.

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 application'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 application, 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 *Find & Filter* criteria in the eyeSegment application.

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

Assign eyeSegment User Permissions

Ensure that each user who needs access to the eyeSegment application is assigned the appropriate eyeSegment permission level.

To manage users at the Forescout Console and set their permissions, refer to the *Managing Users* section in the *Forescout Administration Guide*.

Permissions to View

Users with *View* level permissions can use the eyeSegment application to:

- View the traffic matrix
- Click the widgets on the Matrix page to see more information
- Toggle the matrix Policy Visualization view
- Toggle the matrix Traffic Violations view
- Manage their own Find & Filter criteria
- Focus on a matrix row, column, or cell
- Drill down to view traffic details
- Drill down to view device properties
- Export selected traffic information to a CSV file for further evaluation
- View the eyeSegment policy and its rules
- Run a health check
- Access the online eyeSegment Application How-to Guide

Permissions to Update

Update level permissions include all *View* level permissions, and they also allow the user to:

- Configure the matrix settings
- Ignore traffic of specific devices
- Refresh the Traffic Coverage widget information
- Manage the eyeSegment policy
- Permanently delete some or all collected traffic data

> *Although deleted data is no longer displayed in the eyeSegment application, it is retained in the Forescout cloud for a certain period. For more information, refer to the* Data Security Schedule for Customer Network Data in the Forescout Cloud Service *at https://www.forescout.com/company/legal/data-security-schedule/.*

These activities affect what all users see in their eyeSegment application.

Install the eyeSegment Module

If your environment includes devices whose traffic data you do not want uploaded to the cloud, see Prevent Data Upload for Specific Devices ***before installing the module.***

To install the eyeSegment module:

1. Download the **`.fpi`** file from one of two Forescout portals, depending on which licensing mode your deployment is using:
   - ***Per-Appliance Licensing Mode*** – Go to https://updates.forescout.com/support/index.php?url=counteract&section=product_download&version=8.2.0-1565.
   - ***Flexx Licensing Mode*** – Go to https://Forescout.force.com/support/ and select **Downloads**.

   > *To identify your licensing mode at the Console, select* ***Help > About Forescout****.*
2. Save the file to the machine where the Console is installed.
3. Log into the Console and select **Options** from the **Tools** menu.
4. Select **Modules**, and then select **Install**. The Open dialog box opens.
5. Browse to and select the saved module **`.fpi`** file.
6. Select **Install**. The Installation screen opens.

   > *Note that the End User License Agreement (EULA) displayed in this procedure is not appropriate for this module.*

7. Select **I agree to the License Agreement**, and then select **Install**.

   The installation will begin immediately after selecting Install, and cannot be interrupted or canceled.

8. When the installation completes, select **Close** to close the window. The installed module is displayed in the Modules pane.

   Some components are not automatically started following installation.

9. After this installation is complete, Access the License Agreement from the Console. If you do not agree to the terms, uninstall the module.

Access the License Agreement from the Console

To access the EULA (End User Licensing Agreement):

1. From the Console, select **Tools** > **Options** > **Modules**, select **eyeSegment** module, and then select **About**.
2. When the *Forescout Console* dialog box opens, select the **License Agreement** link, and read the terms of the agreement. If you do not agree to these terms, uninstall the module.

Configure the Module

You can allow Forescout to use your network traffic context to improve the overall customer experience. This feature is enabled by default.

For more information about sharing data with Forescout, refer to the eyeSegment appendix in the *Forescout Research Program Terms & Conditions*.

To configure the eyeSegment Module:

1. From the Console, select **Tools** > **Options** > **eyeSegment**.

2. To opt in or out of sharing your traffic context with Forescout, select or clear the **Share network traffic context with Forescout** checkbox.
3. Select **Apply** to save the configuration.

Ensure That the eyeSegment Module Is Running

If your environment includes devices whose traffic data you do not want uploaded to the cloud, see Prevent Data Upload for Specific Devices ***before starting the module.***

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

To verify:

1. Select **Tools** > **Options** > **Modules**.
2. In the *Modules* pane, hover over the eyeSegment Module name to view a tooltip indicating if it is running on Forescout devices in your deployment.

   The name is preceded by one of the following icons:

   –  - The eyeSegment Module is stopped on all Forescout devices.

   –  - The eyeSegment Module is stopped on some Forescout devices.

   –  - The eyeSegment Module is running on all Forescout devices.
3. If the eyeSegment Module is not running, select **Start**, and then select the relevant Forescout devices.
4. Select **OK**.

Ensure Connectivity

Your Forescout Enterprise Manager must be able to access the Internet. Ensure that your Enterprise Manager's firewall allows incoming connections from **.forescoutcloud.net*.

For the Forescout Cloud Uploader to report traffic data to the cloud, ensure that your managing Appliances' firewalls allow outgoing connections to **.forescoutcloud.net*. If traffic cannot be reported, the data shown in your matrix will not be up-to-date.

- When using a Forescout platform version below 8.2, configure the Cloud Uploader using the credentials provided by your Forescout sales representative.
- When using Forescout platform version 8.2.x, either complete the Customer Verification process during login, or configure the Cloud Uploader using the credentials provided by your Forescout sales representative.

For information about the Cloud Uploader and its configuration, refer to the *Cloud Uploader Configuration Guide*.

Test the module to ensure that your cloud authentication credentials are valid, and that the module can connect to the eyeSegment server.

To test the eyeSegment Module:

- Do one of the following:

  – From the Console, select **Tools** > **Options** > **Modules** > **eyeSegment**, and select the **Test** button.

  – From the Console, select **Tools** > **Options** > **eyeSegment**, and select the **Test** button.

Create an eyeSegment Policy Compliance Policy

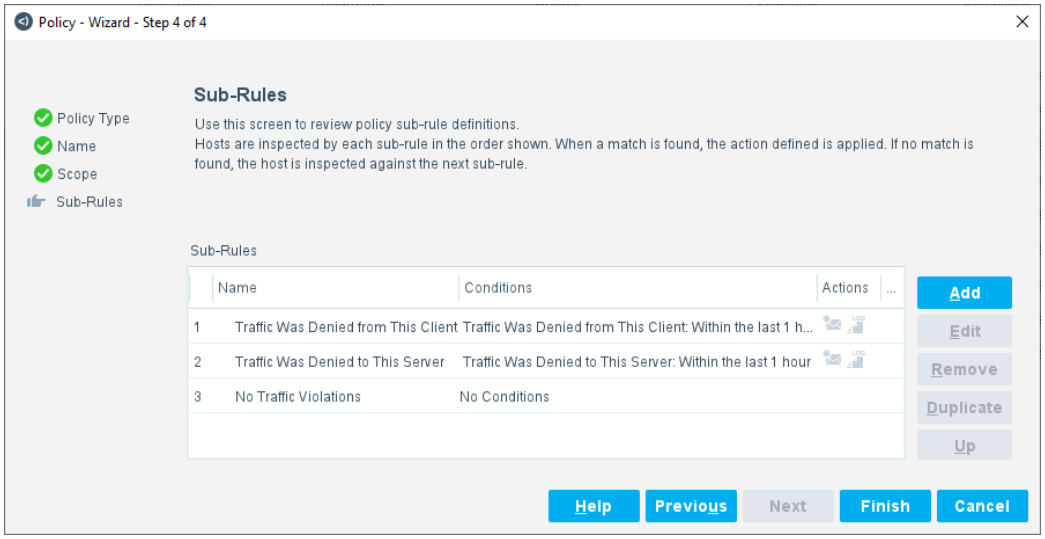
Use a Forescout policy template to easily create a policy that sends email and Syslog messages whenever traffic to or from the endpoint violated an eyeSegment policy rule whose status is **Response**.

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

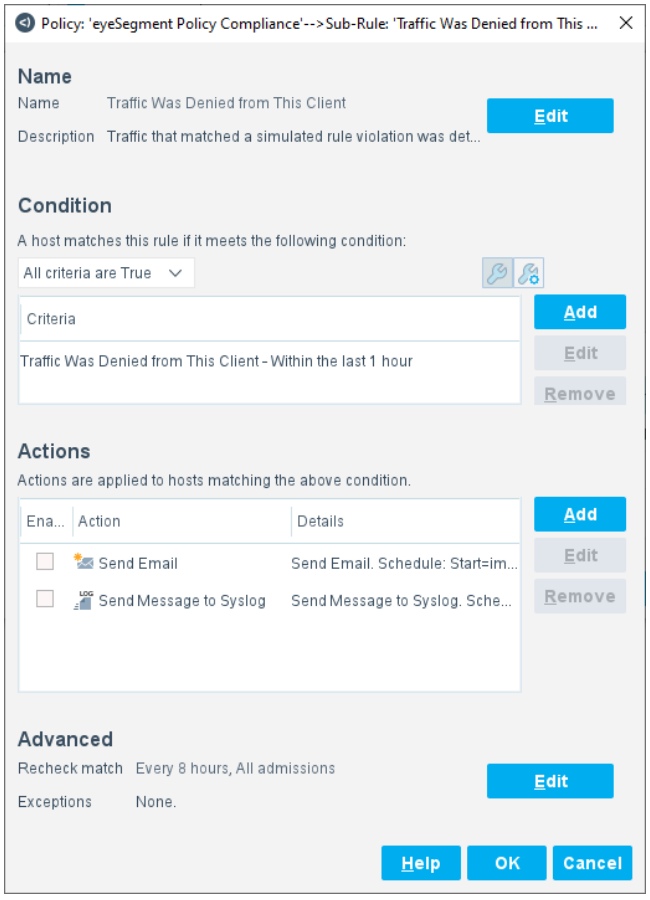
Policy conditions created from this template use properties that include the names of one or more of your eyeSegment policy rules. You cannot delete a rule from your eyeSegment policy unless the rule name is removed from all policy conditions in the Console.

To create a policy:

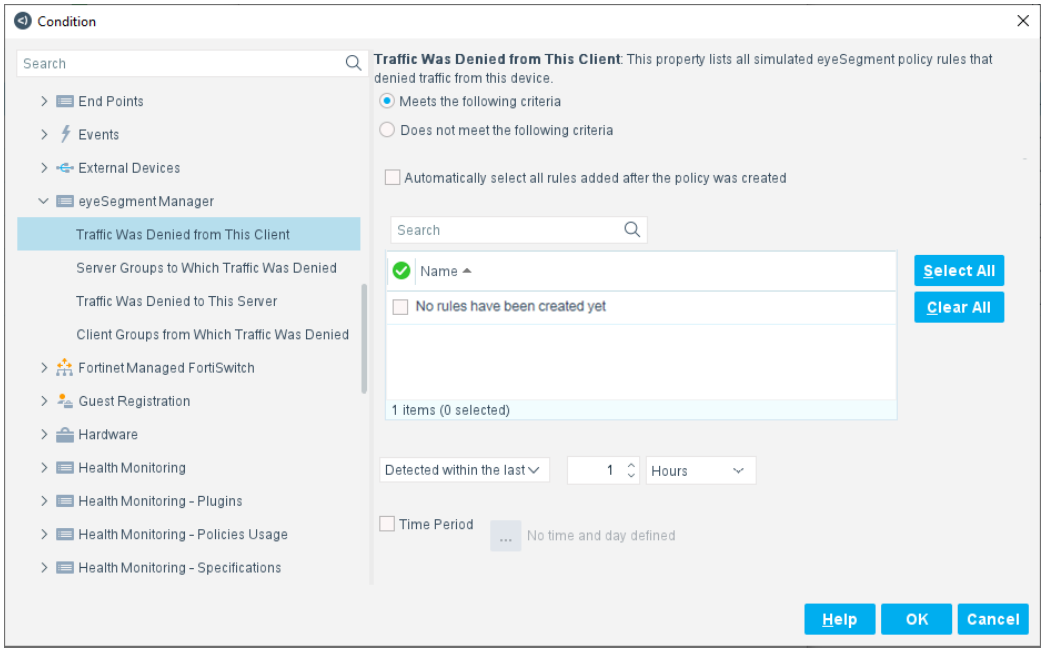
1. In the Console Policy tab, select **Add**.
2. In the Compliance folder, select **eyeSegment Policy Compliance**, and follow the wizard.
3. In the IP Address Range window, select **All IPs**, and continue to the Sub-Rules window.



4. For each of the first two sub-rules:
   a. Select and edit the sub-rule.



b. Select and edit the condition. All eyeSegment policy rule names are displayed.



› Select the policies for which you want notifications to be triggered upon violation. If you want violations of all existing rules to trigger notifications, select **Select All**.

Notifications can only be triggered by eyeSegment policy rules in which the Response status was selected. All other selected rules are ignored by Forescout policies.

› If you want all violations of all future rules to trigger notifications, select **Automatically select all rules added after the policy was created**. This is not selected by default.

c. In the Actions area, enable one or both actions, or add a different action.

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.

If you did not select **Automatically select all rules added after the policy was created**, eyeSegment policy rules that are added after this Forescout policy is saved will not trigger notifications because they are not selected. If you add a rule later and want it to trigger notifications, edit this Forescout policy, and select the new rule in step 4.

Additional Properties

In addition to the device properties used in the eyeSegment Policy Compliance policy template, two other properties are also updated upon detection of traffic that violates an eyeSegment policy rule whose status is **Response**:

- *Server Groups to Which Traffic Was Denied*: Lists the lowest-level Forescout policy group or virtual zone (for devices that are not members of any of your Forescout policy groups) in each eyeSegment policy rule, including exceptions, that contains members to which the rule denied traffic from this client.
- *Client Groups from Which Traffic Was Denied*: Lists the lowest-level Forescout policy group or virtual zone (for devices that are not members of any of your Forescout policy groups) in each eyeSegment policy rule, including exceptions, that contains members from which the rule denied traffic to this server.

The following zones are not written to the Server Groups to Which Traffic Was Denied *or* Client Groups from Which Traffic Was Denied *properties:*

- *Internal Network*
- *– Any –*
- *zones that are eyeSight segments*

Open the eyeSegment Application

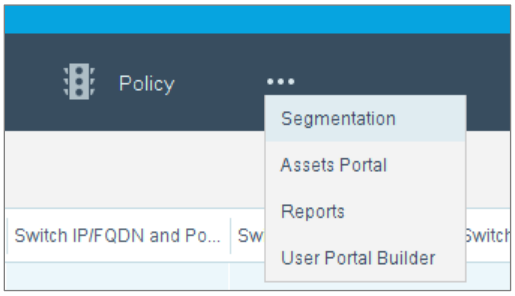
If you have a valid *Forescout eyeSegment* license for the eyeSegment Module, you can open the eyeSegment application from a web browser or directly from the Console. The application is accessed through the Forescout Web Client.

To access the eyeSegment application:

1. Do one of the following:
   - Browse to the following URL to log in from a web browser:

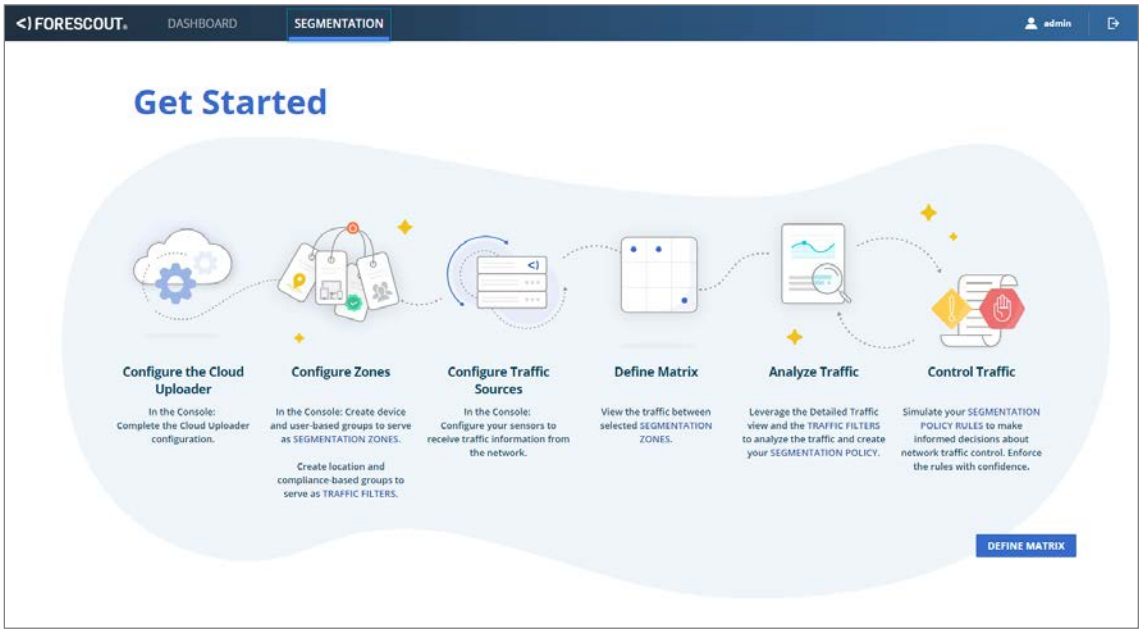
     https://<Device_IP>/forescout-client

     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 application, the **Get Started** diagram opens.



Refer to the *eyeSegment Application How-to Guide* for information on leveraging dynamic zone-to-zone relationship mapping data. The guide is available from the eyeSegment application menu **Help** option.

eyeSegment Module Considerations and Troubleshooting

Use the information in this section for troubleshooting.

- Prevent Data Upload for Specific Devices
- Notifications Not Received

Prevent Data Upload for Specific Devices

By default, eyeSegment processes all the traffic data it receives from your Prepare Traffic Sensors for eyeSegment and uploads it to the cloud. In the eyeSegment web application, you can instruct Forescout to ignore traffic data to and from specific devices. Traffic data for those devices will not be uploaded in the future, but the data that was already uploaded remains in the cloud.

Depending on whether your environment uses an Enterprise Manager or a Standalone Appliance:

- Prevent Specific Data Upload for Enterprise Managers
- Prevent Specific Data Upload for Standalone Appliances

Prevent Specific Data Upload for Enterprise Managers

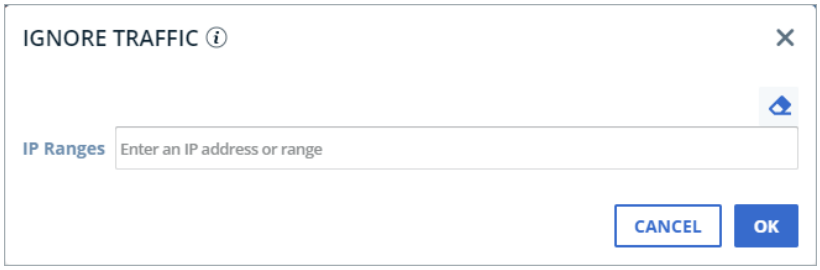
To ensure that no traffic data for specific devices is ever uploaded, don't start the eyeSegment Module on your Appliances until you've instructed the eyeSegment web application to ignore all traffic for the specific devices.

To ensure that no traffic data for specific devices is ever uploaded:

1. Install the eyeSegment Module, but do not Ensure That the eyeSegment Module Is Running.
2. Log into the Console and start the module on the Enterprise Manager only. Do not start the module on any other Forescout device.
3. Open the eyeSegment Application.
4. Select the **Define Matrix** button, and then select **Save**. An empty matrix is displayed.

   Configure the matrix after this procedure is completed. For more information, refer to the eyeSegment Application How-to Guide*.*

5. On the eyeSegment Matrix page, select the menu icon, and select **Ignore Traffic**.



6. Enter an IPv4 address or range for which both incoming and outgoing traffic must be ignored, and press **Enter**. You can enter multiple IPv4 addresses and ranges.

   Do not enter a subnet mask.

7. After you enter all the devices to be ignored, select **OK**.
8. At the Console, start the eyeSegment Module on all Appliances. See Ensure That the eyeSegment Module Is Running.

Prevent Specific Data Upload for Standalone Appliances

To ensure that no traffic data for specific devices is ever uploaded, *before* you install the eyeSegment Module and before any traffic data can be uploaded, stop the Cloud Uploader which uploads data to the cloud. Then install the eyeSegment Module, and instruct the eyeSegment Module to ignore traffic for the specific devices before you restart the data upload to the cloud.

To ensure that no traffic data for specific devices is ever uploaded:

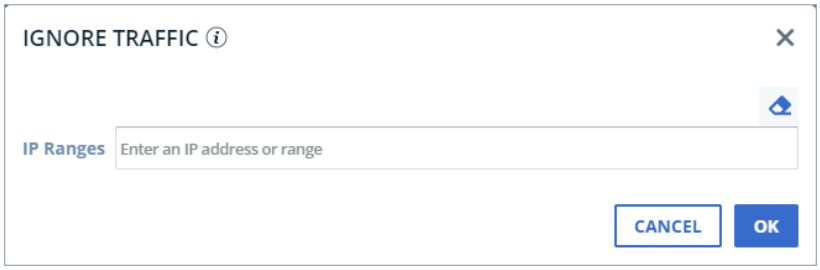
1. Before installing the eyeSegment Module, log into the Console and select **Tools > Options > Modules**.
2. Select **Cloud Uploader**, and select the **Stop** button.
3. Install the eyeSegment Module.
4. Ensure That the eyeSegment Module Is Running.

   The module test is expected to fail at this point because the Cloud Uploader is not running.

5. Open the eyeSegment Application.
6. Select the **Define Matrix** button, and then select **Save**. An empty matrix is displayed.

   Configure the matrix after this procedure is completed. For more information, refer to the eyeSegment Application How-to Guide.

7. On the eyeSegment Matrix page, select the menu icon , and select **Ignore Traffic**.



8. Enter an IPv4 address or range for which both incoming and outgoing traffic must be ignored, and press **Enter**. You can enter multiple IPv4 addresses and ranges.

   Do not enter a subnet mask.

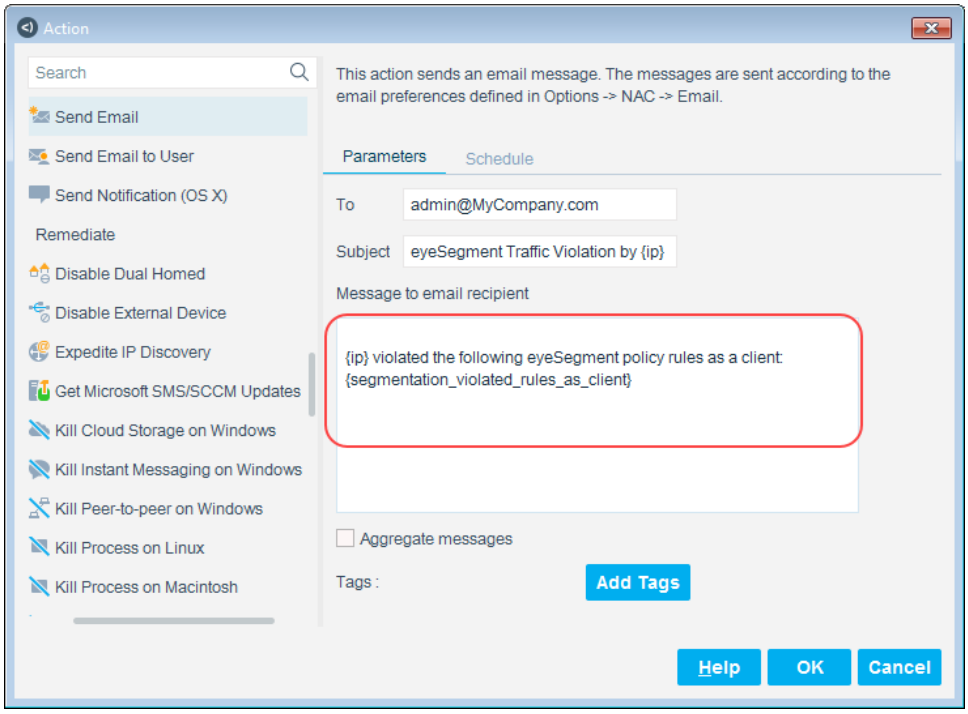
9. After you enter all the devices to be ignored, select **OK**.
10. At the Console, select **Tools > Options > Modules**.
11. Select **Cloud Uploader**, and select the **Start** button. Detected traffic data is uploaded for all devices that are not in the *Ignore Traffic* IP ranges.

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.