



# Fore Scout

## eyeSegment Module

Release Notes

**Version 3.6**



## 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](mailto:documentation@forescout.com)

## Legal Notice

© 2020 Forescout Technologies, Inc. All rights reserved. Forescout Technologies, Inc. is a Delaware corporation. A list of our trademarks and patents can be found at <https://www.Forescout.com/company/legal/intellectual-property-patents-trademarks>. Other brands, products, or service names may be trademarks or service marks of their respective owners.

2020-10-07 17:21

## Table of Contents

<b>About eyeSegment v3.6 .....</b>	<b>4</b>
<b>Forescout Platform Dependencies &amp; Known Issues for eyeSegment v3.6 ....</b>	<b>5</b>
<b>eyeSegment v3.6 Integration with Other Products .....</b>	<b>8</b>

## About eyeSegment v3.6

Forescout eyeSegment accelerates the design, planning and deployment of dynamic network segmentation across the extended enterprise. It simplifies the process of creating context-aware segmentation policies and allows visualization and simulation of policies prior to enforcement for proactive fine-tuning and validation. Use eyeSegment to automatically map traffic flows to a logical taxonomy of users, applications, services and devices across the entire enterprise network without deploying agents.

eyeSegment is a licensed Forescout product.

### What's New

- When used with the new eyeSegment Data Collector Plugin, eyeSegment can now deliver a unified eyeSegment application for networks of multiple Enterprise Managers. For more information, refer to the *eyeSegment Data Collector Release Notes and Configuration Guide*.
- In previous versions, only Forescout policy groups could be selected as zones for the eyeSegment matrix and for eyeSegment policy rules. In version 3.6, eyeSight segments can also be selected as zones.
  - 📄 *It is recommended to not share IP addresses between different segments. If there is traffic for an IP address that is included in two different segments on the matrix, its traffic is shown for only one of the segments.*
- Unlike groups, eyeSight segments can be deleted from the Forescout platform even if they are used in the eyeSegment matrix or in an eyeSegment policy rule. After a segment is deleted from the Forescout platform:
  - The name of the segment is changed to - **Deleted Zone** -.
  - The matrix continues to show the traffic reported for the segment before it was deleted.
  - Subsequent traffic is no longer associated with that segment.
  - The segment is removed from all filter fields.
  - The name - **Deleted Zone** - is displayed in policy rules that used that segment, but the zone is ignored.

It is recommended to edit the matrix and your policy rules to remove these deleted segments.

- The displayed traffic is always *within* the date range of the applied filter regardless of the filter's **Exclude Traffic** setting.

### Upgrade Considerations

All traffic data is stored in the Forescout cloud. The data is not affected by eyeSegment Module upgrades or rollbacks.

### Upgrading from a Version Earlier Than 3.0

If you upgrade from a version earlier than 3.0, the application retains the same matrix zones and eyeSegment policy rules that you already set, but not your filter settings. To easily recreate your filter settings, we recommend saving them before upgrading to this version.

In versions 3.0 and above, you can no longer export traffic details from a page that shows zone levels. You must first drill down to the *Traffic by Service* page.

### Rollback Considerations

eyeSegment version 3.6 cannot be rolled back to a version earlier than 3.0.

If you uninstall version 3.6 to reinstall a version earlier than 3.0, your eyeSegment application configuration will be lost. To easily recreate your configuration should you need to reinstall a version earlier than 3.0, we recommend saving the following information before upgrading to this version:

- the names of your selected Source and Destination zones
- your filter criteria
- your eyeSegment policy rules

Even if you uninstall eyeSegment, all traffic data that you have not actively deleted remains available.

### eyeSegment Documentation

For information on configuring your environment for eyeSegment, refer to the *eyeSegment Module Configuration Guide*.

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.

## Forescout Platform Dependencies & Known Issues for eyeSegment v3.6

We recommend using the latest Forescout platform version.

The following table maps each supported Forescout platform version to the recommended Forescout plugin versions.

Platform Version	Recommended Component Versions							* Known Issues & Limitations
	Required Plugins		Traffic Sensor Plugins					
	Web Client	Cloud Uploader	Flow Collector	Packet Engine	Medigate Module	OTSM	AWS Plugin	
8.1.0	1.0.0.1013	1.2	1.0	8.1.0	N/A	N/A	N/A	a, b, c, d, e, f, g

Platform Version	Recommended Component Versions							* Known Issues & Limitations
	Required Plugins		Traffic Sensor Plugins					
	Web Client	Cloud Uploader	Flow Collector	Packet Engine	Medigate Module	OTSM	AWS Plugin	
8.1.1	1.1.2	1.2	1.0	8.1.1	N/A	N/A	N/A	a, b, c, d, e, f, g
8.1.2	1.1.2	1.2	1.0	8.1.2	N/A	N/A	N/A	a, b, c, d, e, f, g
8.1.3	1.1.2	1.2	1.0	8.1.3	N/A	N/A	N/A	a, b, c, d
8.1.3.1	1.1.2	1.2	1.0.1	8.1.3	N/A	N/A	N/A	a
8.1.4	1.1.3	1.2	1.0.2	8.1.4	1.1	N/A	N/A	a, h
8.2	1.2	1.2	1.1	8.2	N/A	N/A	N/A	a
8.2.0.2	1.2	1.2	1.1	8.2.0.2	1.1	1.3.0.2	2.2.2	a, i, j
8.2.1	1.2.1	1.2	1.1.1	8.2.1	1.1	1.3.1.2	2.2.2	a, i, j

**\*Known Issues and Limitations:**


- a. The following known issues and limitations apply to all Forescout platform versions:
- › Certification Compliance mode is not supported.
  - › Only devices that have IPv4 addresses are supported.
  - › Flows detected by the deprecated NetFlow Plugin are not supported.
  - › Random high port (above 20k) UDP traffic to or from Forescout Appliances is usually a result of a specific HPS Plugin configuration for open port scans. eyeSegment does not display this traffic.
  - › After the installation or upgrade of the eyeSegment Module, the Packet Engine automatically restarts.
  - › If the Traffic by Service traffic pattern has more than 100,000 entries, the data cannot be exported. To reduce the number of records to be exported, apply *Find & Filter* criteria that narrow the scope to specific traffic of interest.
  - › All time fields in the graphic user interface use the Appliance Console's time zone preference and are translated to UTC internally.
  - › Your *Find & Filter* date range is compared to the UTC date on which the cloud received the traffic data. If the upload was delayed, such as by an internet problem, the date the cloud received the data might be later than when the traffic actually occurred.
  - › Dates in *Find & Filter* criteria are exported as UTC times.
  - › Protocols in *Find & Filter* criteria are exported as protocolId decimal values. For more information, refer to <https://www.iana.org/assignments/protocol-numbers/protocol-numbers.xhtml>.

- › If more than 5,000 top-level segments are defined in your Forescout Console, your eyeSegment application browser might lock for several minutes after you enter any character into the *Find & Filter* window's Source or Destination field.
- b. RBAC (Role-Based Access Control) user permissions are not supported.
- c. NetFlow v5 protocol (with or without Flexible NetFlow technology) is not supported.
- d. The Flow Collector might consume ghost eyeSight licenses and report incorrect devices. Should this happen, contact eyeSegment support.
- e. The Packet Engine reports the traffic sources as servers, and the traffic destinations as clients. In these versions, traffic data reported by the Packet Engine will appear in the matrix the reverse of its actual direction.
- f. When the *Notification* feature is activated, the endpoint property is sent to all Appliances, instead of only to the Appliance that manages the specific endpoint. Sending many properties to many Appliances might slow other Appliance functions.
- g. It might take several minutes to save the eyeSegment policy.
- h. Speak to your Forescout sales representative if you need to integrate with components that this version does not normally support.
- i. The following known issues and limitations apply when using AWS VPC as a traffic sensor:
  - › Flow sessions from AWS VPCs cannot be pulled more frequently than once every 10 minutes. The actual interval is set in the Forescout AWS Plugin configuration.
  - › It is recommended to run Appliances in the cloud, and not on-premises, for cloud endpoints and for flows that are part of the eyeSegment deployment. The cost of pulling flow log data from AWS to eyeSegment is likely to be higher for on-premises Appliances than for Appliances in the cloud. To understand what the cost might be, review the aggregate size of your daily VPC flow logs across all your accounts, and then put that data into the AWS calculator.
- j. When using the Operational Technology Module (OTSM):
  - › The OT Monitoring Sensor version must be 4.1.2.
  - › Configure the sensors to share NetFlow data with eyeSegment. Refer to the *Operational Technology Module Configuration Guide* or Release Notes for more information.

### eyeSegment Performance Specifications


The table below summarizes capacity in terms of *Flows handled per second* (average number of traffic flows that eyeSegment processed per second, during the past two minutes), for specific Appliance models:


# of Flows	Forescout 5120	Forescout 5140	Forescout 5160
SPAN	N/A	52000 flows / sec	52000 flows / sec
Flow	N/A	79800 flows / sec	79800 flows / sec
Flow and SPAN	N/A	115800 flows / sec	115800 flows / sec

 *The data listed here does not reflect the underlying capacities of Forescout product Flow or SPAN functionalities.*

## eyeSegment v3.6 Integration with Other Products

- You can integrate eyeSegment with SilentDefense for:
  - better visibility of your OT devices and their traffic, with no additional device or traffic configuration
  - accurate protocols based on Deep-Packet Inspection (DPI)
- You can integrate eyeSegment with Medigate for:
  - better visibility of your medical devices and their traffic, with no additional device or traffic configuration
  - accurate protocols based on Deep-Packet Inspection (DPI)
- You can integrate eyeSegment with AWS Virtual Private Cloud (VPC). The AWS Plugin periodically pulls the flow logs from AWS VPCs, and extracts and passes the flow session data to eyeSegment for better visibility of your AWS devices and their traffic.

 **Important:** When integrating eyeSegment with AWS VPC, it is recommended to run Appliances in the cloud, and not on-premises, for cloud endpoints and for flows that are part of the eyeSegment deployment. The cost of pulling flow log data from AWS to eyeSegment is likely to be higher for on-premises Appliances than for Appliances in the cloud. To understand what the cost might be, review the aggregate size of your daily VPC flow logs across all your accounts, and then put that data into the AWS calculator.

 *This does not apply to Forescout deployments that do not require flow logs, such as for eyeSight visibility only.*