



ForeScout

eyeSegment Application

How-to Guide

Version 3.3



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 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.

2020-08-25 14:38

Table of Contents

Welcome	4
About eyeSegment	4
How It Works.....	5
eyeSegment Components.....	5
What You Need	7
Use the eyeSegment Application	9
Open the eyeSegment Application	9
Configure the Matrix	11
View the Matrix Page	13
Matrix	14
Matrix Visualization Settings	15
Legend.....	16
Menu	18
Widgets	18
Find & Filter Specific Traffic	22
Focus on a Matrix Row, Column, or Cell	25
Focus on a Row or Column	26
Focus on a Cell.....	28
View and Export Traffic Details.....	30
View IP-to-IP Traffic Details	34
Delete Traffic	35
Ignore Traffic of Specific Devices.....	37
Run a Health Check	38
About the eyeSegment Policy.....	39
About Simulated Rules.....	39
Visualize the eyeSegment Policy in the Matrix	41
Create eyeSegment Policy Rules	41
Edit or Delete Policy Rules	43
Configure Policy Rules.....	43
Considerations and Troubleshooting	45
Additional Forescout Documentation.....	47
Documentation Downloads	47
Documentation Portal	48
Forescout Help Tools.....	48

Welcome

Welcome to eyeSegment, where you can simplify segmentation planning and automate ACL/VLAN assignment to reduce your attack surface.

Your version of the release might differ slightly from the version described in this guide.

If you are the Forescout Console administrator, refer to the *eyeSegment Module Configuration Guide* for information about configuring your Forescout platform to enable viewing and leveraging dynamic zone-to-zone relationship mapping data. See [Additional Forescout Documentation](#) for information on how to access this guide.

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.
- Focus on a matrix row, column, or cell to view a matrix of all the sub-groups of the selected Source or Destination parent group. 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 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 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 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 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 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

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 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.

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

eyeSegment zones can include the following:

Forescout policy groups	These groups are selected by the user to be included in the matrix. <i>Note: Each level of a nested structure includes all of its sub-groups.</i>
< 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*, and *Remote Devices*, 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.
- 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.

Verify that your [license](#), [browser](#), [cloud](#), and [Forescout group](#) requirements are ready.

For other requirements, see the eyeSegment Module Release Notes.

What You Need

To use the eyeSegment application in your environment, the following items must be configured:

- [eyeSegment License](#)
- [Supported eyeSegment Browsers](#)
- [Cloud Connectivity](#)
- [User Permissions](#)
- [Groups for the eyeSegment Matrix](#)

eyeSegment License

Ensure that you have a valid *Forescout eyeSegment* license for the eyeSegment Module.

For information about the license, refer to the *Forescout Administration Guide* or the *Flexx License How-to Guide*. See [Additional Forescout Documentation](#) for information on how to access these guides.

Supported eyeSegment Browsers

The eyeSegment application is accessed through the Forescout Web Client using any of the following browsers:

- Microsoft Edge
- Mozilla Firefox 43.0 and above
- Safari 9.0 and above on MAC OS
- Chrome 46 and above

 *Internet Explorer is not supported.*

Cloud 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.

For information about the Cloud Uploader and its configuration, refer to the *Cloud Uploader Configuration Guide*. See [Additional Forescout Documentation](#) for information on how to access this guide.

User Permissions

To use eyeSegment features, you must have permissions configured for you at the Forescout Console.

If you have *View* level permissions, you can use the eyeSegment application to:

- View the traffic matrix
- Click the Matrix page widgets to see more information
- Toggle the matrix Policy Visualization view
- Toggle the matrix Traffic Violations view
- Manage your own Find & Filter fields
- 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

If you also have *Update* level permissions, you can do the following activities that affect what all users see in their application:

- [Configure the Matrix](#)
- [Delete Traffic](#)
- [Ignore Traffic of Specific Devices](#)
- Refresh the [Traffic Coverage widget](#) information
- [Create eyeSegment Policy Rules](#)

Groups for the eyeSegment Matrix

If you are the Forescout Console administrator, ensure that specific groups defined in your Forescout Console configuration contain the devices whose traffic you want to track. To further narrow the device scope of an eyeSegment policy rule, arrange groups in hierarchal levels. 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 prepare groups for the eyeSegment matrix, refer to the best practice recommendations in the *eyeSegment Module Configuration Guide*. See [Additional Forescout Documentation](#) for information on how to access this guide.

Use 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.


If you have the required [User Permissions](#), you can do the following in the application:

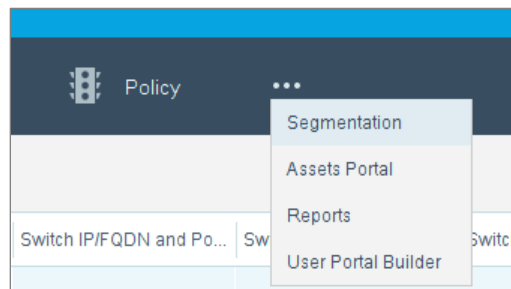
- [Open the eyeSegment Application](#)
- [Configure the Matrix](#)
- [View the Matrix Page](#)
- [Find & Filter Specific Traffic](#)
- [Focus on a Row or Column](#)
- [Focus on a Cell](#)
- [View and Export Traffic Details](#)
- [View IP-to-IP Traffic Details](#)
- [Delete Traffic](#)
- [Ignore Traffic of Specific Devices](#)
- [Run a Health Check](#)

Open the eyeSegment Application

The application is accessed through the Forescout Web Client.

To access the eyeSegment application:

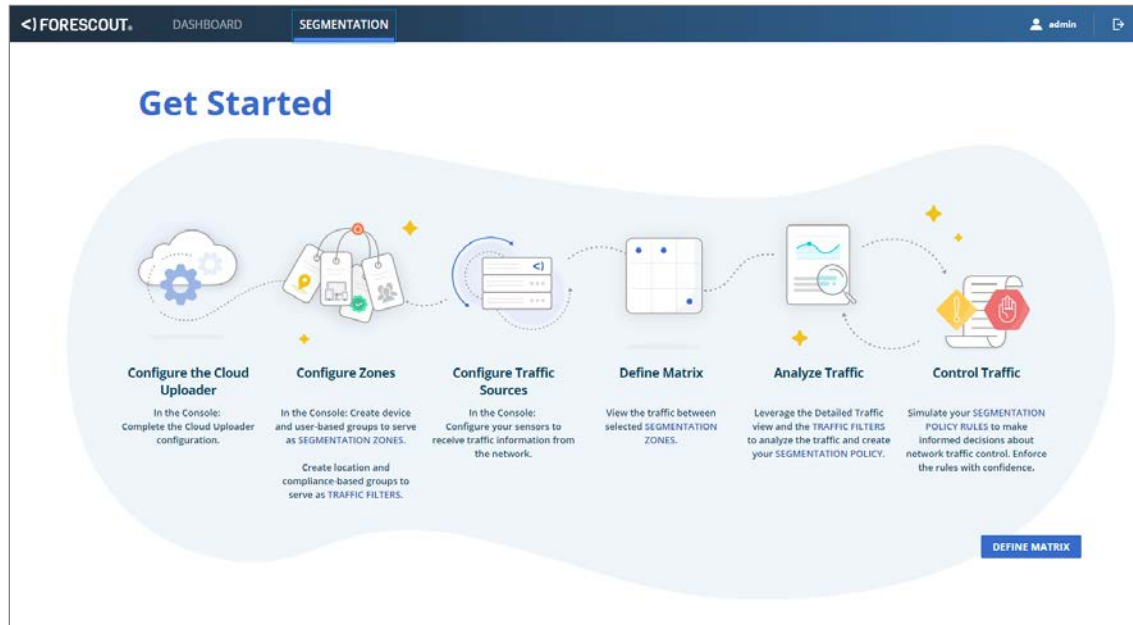
1. Do one of the following:
 - Browse to the following URL to log in from a web browser:
https://<Device_IP>/forescout-client
where <Device_IP> is the IP address of the Enterprise Manager or standalone Appliance.
 - Select the **Ellipsis icon**  from the Console toolbar, and then select **Segmentation** 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.



Select the **Define Matrix** button to configure the matrix.


Configure the Matrix

eyeSegment provides an easily configured matrix made of eyeSegment zones.

By default, the matrix includes the following virtual zones as both Source and Destination zones (unless otherwise noted):

< 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. (Destination zone only)
< Internet	Contains all IP addresses that are not in any other zone.

The matrix shows the traffic from each Source zone to each Destination zone. You can add policy groups of interest as Source and Destination zones.

 *To configure the matrix settings, you might need to have additional permissions configured for you at the Forescout Console.*

To configure the matrix settings:

1. If this is not the first time you are opening the eyeSegment application, select **Matrix Settings** from the menu icon  on the eyeSegment Matrix page.

MATRIX SETTINGS ⓘ

Matrix Title

Matrix

New Matrix Zones ⓘ

Expand to select from your existing groups...

ADD AS BOTH | ▾

Source Zones (3)

☒ ☐ ☐ ☐ ☐ Search...

<> Internal Network

<> Private Network

<> Internet

Destination Zones (4)

☒ ☐ ☐ ☐ ☐ Search...

<> Internal Network

<> Private Network

<> Multicast/Broadcast

<> Internet

ⓘ Some zones cannot be moved or removed from the matrix.

CANCEL

SAVE

2. Configure the following matrix settings:

Matrix Title	Enter a meaningful name to be shown in the eyeSegment application.
New Matrix Zones	<p>The matrix shows traffic from selected Source zones to selected Destination zones. Groups already included in the matrix as zones are shown in the Source and Destination Zone Lists below.</p> <p>To add groups to the matrix:</p> <ol style="list-style-type: none">Expand the dropdown menu to view the list of groups in your Forescout configuration. <p>An arrow indicates a <i>nested structure</i> of groups. Select it to expand the structure if you want to select sub-groups.</p> <div><div>MATRIX SETTINGS ⓘ</div><div><div>Matrix Title</div><div>Finance Matrix</div></div><div><div>New Matrix Zones ⓘ</div><div>Expand to select from your existing groups...</div><div><div>Search...</div><div><div><input type="checkbox"/> Corporate Hosts</div><div><input type="checkbox"/> CounterACT Devices</div><div><input type="checkbox"/> Demo_4_6</div><div><input checked="" type="checkbox"/> ▾ Devices with Vulnerable Credentials</div><div><input type="checkbox"/> Commonly Used Credentials</div><div><input type="checkbox"/> Custom Credentials</div><div><input type="checkbox"/> Factory Default Credentials</div></div></div></div></div>


Version 3.3

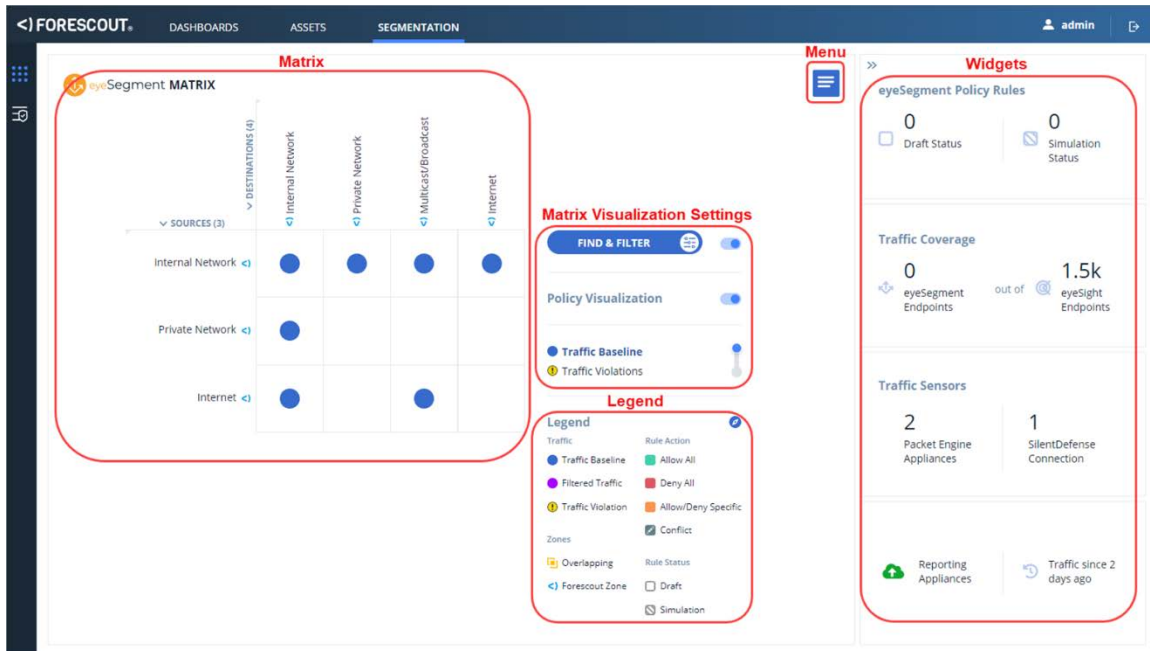
12

	<p>2. Select one or more groups to be added as Source zones or Destination zones or both. If your Forescout Console administrator followed the best practice recommendations in in the <i>eyeSegment Module Configuration Guide</i>, only select sub-groups in the 'IP Taxonomy Zones' structure.</p> <p><i>Note: The number of Source zones need not match the number of Destination zones. The matrix can have up to 50 Source zones and 50 Destination zones.</i></p>
Add As	<ul style="list-style-type: none"> ▪ Select Add as Source if you want the matrix to show traffic originating from any IP address in the groups you just selected. ▪ Select Add as Destination if you want the matrix to show traffic that ended at any IP address in the groups you just selected. ▪ Select Add as Both if you want the matrix to show traffic that originated or ended at any IP address in the groups you just selected.
Source and Destination Zone Lists	<p>The groups selected as Source and Destination zones are listed in the order in which they appear in the matrix. You can select one or more to remove from the matrix, or select one and use the arrow buttons to change its position in the matrix.</p> <p><i>Note: You cannot remove the Internal Network or Private Network zone from the Source or Destination zone lists.</i></p>
Save/Cancel	Save or cancel your changes.

View the Matrix Page

After the initial matrix definition, the matrix is shown whenever you open the eyeSegment application.

-  *The matrix might take a minute or two to appear the first time the data is loaded. After the matrix appears, it is refreshed periodically. To see the latest traffic in the matrix, refresh the browser.*



The eyeSegment Matrix page includes the following areas:

- [Matrix](#)
- [Matrix Visualization Settings](#)
- [Legend](#)
- [Menu](#)
- [Widgets](#)

Depending on the width of your window, you might need to hover your mouse over, or click the chevron « at the right side of the Matrix page to see the widget area.

Matrix

The matrix area contains:



- The matrix title.
- The Source and Destination zone names for each cell.

You can select a row, column, or cell to see its lower level sub-groups. See [Focus on a Matrix Row, Column](#) and [Focus on a Cell](#).

- Traffic icons inside cells to indicate that traffic was detected from the Source zone to the Destination zone during the time range shown at the bottom right of the page.

Traffic is only shown if it occurred within the past 90 days.

- A blue ● icon indicates that the traffic is not filtered, and all detected traffic is indicated in the matrix.





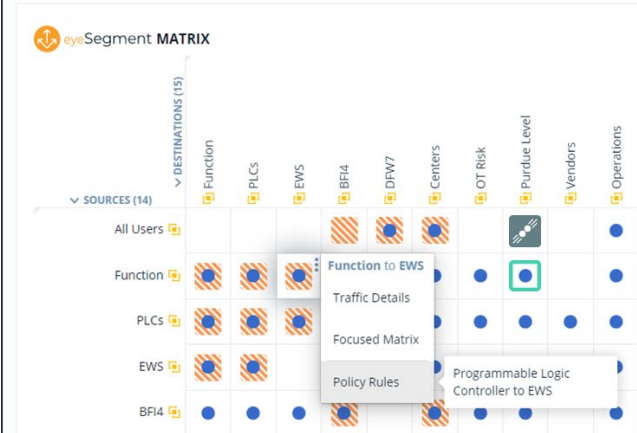
- A violet  icon indicates that *Find & Filter* criteria are applied, and that additional traffic might have been detected but is not shown due to the filter.
- A yellow  icon indicates traffic that violated one of your simulated policy rules.



You can select a traffic icon to view details of the detected traffic. See [View and Export Traffic Details](#).

- If *Find & Filter* criteria are applied, a filter indicator **FILTERED BY** followed by the filter criteria are displayed as a tag at the bottom of the matrix. If the criteria list is very long, hover over the tag to see all the filter criteria.


Matrix Visualization Settings

Use the matrix visualization settings to display additional levels of information in the matrix.

	<p>Select to view or change the Date Range, Source, Destination and Service (port/inspected protocol) filter fields for the traffic shown in the matrix. See Find & Filter Specific Traffic.</p> <p> Blue indicates that all the traffic is shown, and <i>Find & Filter</i> criteria are not applied.</p> <p> Violet indicates that the criteria set in the <i>Find & Filter</i> window are applied. See Find & Filter Specific Traffic.</p> <p>Use the toggle to apply or remove the <i>Find & Filter</i> criteria from the matrix.</p>
	<p>If you've created eyeSegment policy rules, use the Policy Visualization toggle to apply or remove a color-coded visualization of your policy rules on each cell in the matrix.</p> <p>Hover over a color-coded indicator and select Policy Rules to view the name of the eyeSegment policy rule that applies to that traffic.</p>  <p>For more information, see Visualize the eyeSegment Policy in the Matrix.</p>












 **Traffic Baseline**
 **Traffic Violations**

If you've created eyeSegment policy rules in Simulation status, select **Traffic Violations** to hide all traffic except traffic that violated any of your simulated policy rules.

Select  to view details of the traffic. See [View and Export Traffic Details](#).

Legend

Legend

Traffic	Rule Action
 Traffic Baseline	 Allow All
 Filtered Traffic	 Deny All
 Traffic Violation	 Allow/Deny Specific
	 Conflict
Zones	Rule Status
 Overlapping	 Draft
 Forescout Zone	 Simulation

Traffic


Traffic Baseline icons show that there was traffic between the Source and Destination zones.

Filtered Traffic icons are only displayed when *Find & Filter* criteria are applied.

Traffic Violation icons are only displayed when the **Traffic Violations** is selected.

Zones

Overlapping Zones

The Overlapping Zones icon  is displayed next to the zones that have shared members. If a device is a member of more than one zone in the matrix, there is a risk that different eyeSegment policy rules will apply conflicting actions to it. If the device's traffic violates a policy rule, the traffic violation information displayed in the matrix might be incorrect.


Hover over an icon to view the names of the other zones with which it shares one or more devices.

Some devices in this zone are also in:

Computer
Linux/Unix

Use a traffic filter to identify the shared devices.

CentOS-113.103 

 *This feature is not displayed in a focused matrix.*

To identify the devices shared among different zones:

1. For *each* Source Zone in the Overlapping Zones popup window:
 - a. [Find & Filter Specific Traffic](#) for both of the following Source filters:
 - > the Source Zone in the matrix row
 - > the zone in the Overlapping Zones popup window
 - b. For each Filtered Traffic icon, drill down into the matrix to view the IP addresses common to both zones.
2. For *each* Destination Zone in the Overlapping Zones popup window:
 - a. [Find & Filter Specific Traffic](#) for both of the following Destination filters:
 - > the Destination Zone in the matrix column
 - > the zone in the Overlapping Zones popup window
 - b. For each Filtered Traffic icon, drill down into the matrix to view the IP addresses common to both zones.





You can use this information to adjust your Forescout group definitions and/or your matrix zones.

Forescout Zones

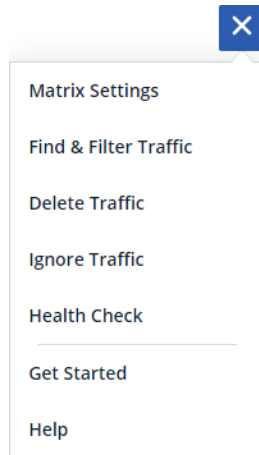
To ensure that the matrix includes traffic to and from all devices, devices that are not in other zones on your matrix are included in [virtual zones](#). These zones are not standard Forescout policy groups.

Rule Action and Rule Status

The Rule Action and Rule Status indicators are only displayed in the matrix when **Policy Visualization** is applied. The color indicates the rule action for all traffic from the matrix cell's Source zone to its Destination zone:

-  Allow all traffic.
-  Deny all traffic.
-  Allow or Deny traffic, but with exceptions.
-  At least one rule denies this traffic and at least one rule allows this traffic. The results of this conflict are unpredictable.

Menu





Select the menu icon  to select the following options:

- **Matrix Settings** to view or modify the matrix name, its zones, and their order in the matrix. See [Configure the Matrix](#).
- **Find & Filter Traffic** to add Date Range, Source, Destination and Service (port/inspected protocol) filter criteria to the traffic shown in the matrix. See [Find & Filter Specific Traffic](#).
- **Delete Traffic** to permanently delete some or all the traffic data saved to date. The deleted data is cleared from the matrix. See [Delete Traffic](#).
- **Ignore Traffic** to stop saving traffic data for specific IP addresses. See [Ignore Traffic of Specific Devices](#).
- **Heath Check** to ensure that eyeSegment can connect to the eyeSegment server. See [Run a Health Check](#).
- **Get Started** to view the Get Started diagram in a different browser tab.
- **Help** to view this How-to Guide in your browser.

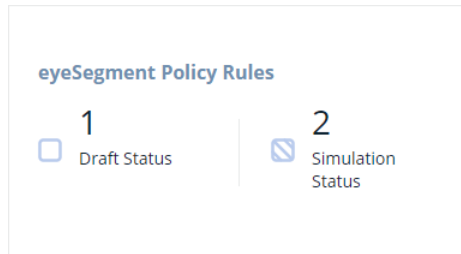
Widgets

Widgets display helpful information about your eyeSegment configuration.

- To see the widgets if the widget area is hidden:
Depending on the width of your window, either click the chevron  at the top right of the Matrix page, or hover your mouse over the right side of the page.
- To hide the widget area:
Depending on the width of your window, either click the chevron  on the left side of the widget area, or move your mouse to the left.

eyeSegment Policy Rules Widget

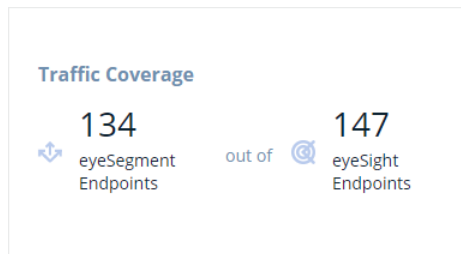
The **eyeSegment Policy Rules** widget indicates how many of your policy rules are in Draft status and how many are in Simulation status.



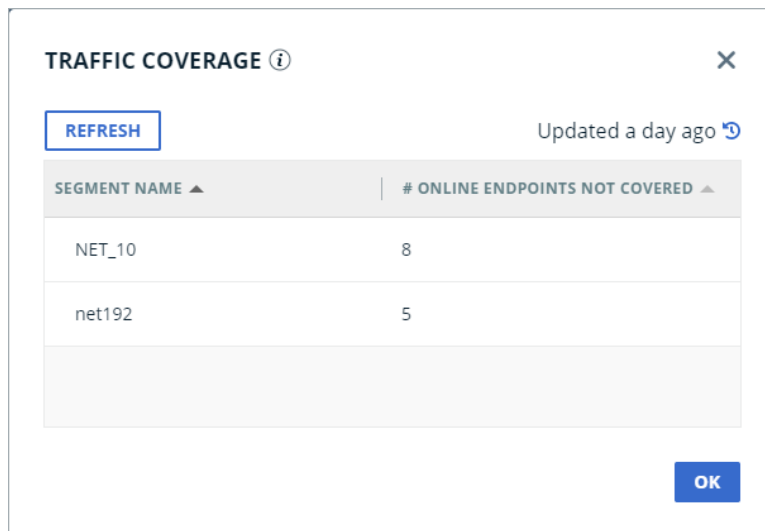
Click anywhere in the widget to open the eyeSegment Policy page that lists all your rules.

Traffic Coverage Widget

The **Traffic Coverage** widget indicates how many endpoints eyeSegment received traffic data for, and how many endpoints are online in your internal eyeSight network.




Click anywhere in the widget to discover which Forescout eyeSight segments in your internal network contain endpoints that haven't reported traffic data to eyeSegment. Endpoints that are not included in any defined segment are listed in the virtual segment named 'N/A'.



You can select **Refresh** to retrieve the latest data.

It might take a few minutes to load the data.

 To refresh the Traffic Coverage data, you might need to have additional permissions configured for you at the Forescout Console.


Traffic Sensors Widget

The **Traffic Sensors** widget shows information about the devices that report traffic data to eyeSegment. A sensor is shown if it has uploaded traffic data to eyeSegment within the last 12 hours.




Depending on the configuration of your environment, your traffic sensors can include:

- **Flow Exporters:** switches, routers, and other network devices that report flow session data. Click the text to view the IP addresses of these network devices.

 *Note: These are not Appliances.*

- **Packet Engine Appliances:** Forescout Appliances on which the Packet Engine is configured to parse, analyze, and report mirrored traffic data. Click the text to view the IP addresses of these Appliances.

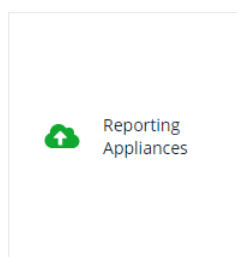
 *If the Packet Engine count is lower than expected, verify that the channels were configured correctly on the Appliances missing from the list.*

- **SilentDefense Connections:** Forescout Appliances that use the Forescout Operational Technology Module to audit network traffic. Click the text to view the IP addresses of these Appliances.
- **Medigate Servers:** Medigate Collection Servers (MCS) that capture and collect network traffic. Click the text to view the IP addresses of these Medigate servers.
- **AWS Virtual Private Clouds:** Amazon VPCs from which the Forescout AWS Plugin periodically pulls flow logs containing flow session data. Click the text to view information about these VPCs.

AWS VIRTUAL PRIVATE CLOUDS ⓘ						×
REPORTING APPLIANCE ▲	VPC ID ▲	AWS OWNER ▲	REGION ▲	BUCKET NAME ▲	LAST SUCCESSFUL UPLOAD ▲	
			us-west-1	aws-flow-logs-call	Thu Jun 18 13:15:14	
						OK

Reporting Appliances Widget





Use the **Reporting Appliances** widget to determine the connectivity of your Appliances that are expected to upload data to eyeSegment. An Appliance is included if it has reported traffic data to eyeSegment within the last 36 hours.




A red icon indicates that some of your reporting Appliances are not reporting any traffic data.

Click the text to view the following information for each Forescout Appliance that reports traffic data:

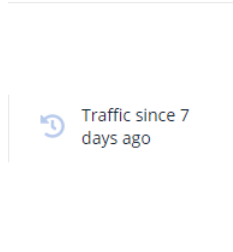
- Current connectivity status to the cloud
- Forescout Appliance name or IP address
- Time stamp of the last successful traffic data upload to the cloud
- Average number of traffic flows that eyeSegment processed per second during the past ten minutes
- Traffic data sources: Packet Engine, Flow Collector, or other traffic sensors


REPORTING APPLIANCES ⓘ					×
CONNECTIVITY ▲	REPORTING APPLIANCE ▲	LAST SUCCESSFUL UPLOAD ▲	FLows HANDLED PER SECOND ▲	TRAFFIC DATA SOURCE ▲	
		Thu Sep 12 00:57:43	27	Packet Engine	
		Thu Sep 12 16:43:25	39	Flow Collector, Packet Engine	
					OK

 If Packet Engine is not listed as a data source, and you believe it should be, verify that the channels were configured correctly on the Appliance.

Traffic Collection Duration Widget

The **Traffic Collection Duration** widget shows how long the real-time traffic data shown in the matrix has been collected. Traffic that occurred more than 90 days ago is not shown in the matrix.




 *Traffic collection does not begin until the Forescout Cloud Uploader Plugin is configured correctly and running.*

Find & Filter Specific Traffic

A filter enables you to intersect one or more filter groups and other filter criteria with the Source and Destination zones and their traffic, letting you focus on traffic between specific types of devices without the need for a complex taxonomy structure. When *Find & Filter* criteria are applied, traffic from each Source zone to each Destination zone is only shown if it meets all the criteria.

You can create and maintain your own *Find & Filter* criteria for the shared matrix. Among the criteria, you can include any Forescout policy group, segment, or IP as a Source or Destination filter. For example, you can filter the matrix to only display traffic sent from the devices that are in the Source zones defined in the matrix and that are also in *all* of the following groups and segment:

- London Office
- High-Risk Assets
- Remote Devices

 *Ensure that the policies that manage the filter groups are run on the devices to be shown in the matrix.*

To add or modify your *Find & Filter* criteria:

1. Select the **Find & Filter** button ( or ) to open a **Find & Filter** window.

The screenshot shows a 'FIND & FILTER' dialog box with a close button (X) in the top right. It contains a 'Date Range' dropdown with the text 'Select the first and last dates'. Below this is a section with three dropdowns: 'Source' (with a hint icon), 'Destination' (with a hint icon), and 'Service' (with a hint icon). The 'Source' dropdown shows 'IP, segment, groups'. The 'Destination' dropdown shows 'IP, segment, groups'. The 'Service' dropdown shows 'Ranges, inspected protocols'. To the right of these is an 'Exclude Traffic' toggle switch. At the bottom right are three buttons: 'APPLY', 'CANCEL', and 'OK'.

2. Enter one or more filter field parameters. Each *Find & Filter* field — Date Range, Source, Destination, Service — is only applied if at least one value is defined for it.

- In the **Date Range** field, you can select two dates within the past 90 days to define a range. Select the same date twice for a one-day range.

Traffic that occurred more than 90 days ago is never shown in the matrix.

The filter matches when the traffic data was received by the Forescout cloud during the date range selected.

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.

- In the **Source** and **Destination** fields, you can enter any combination of:
 - > multiple groups
 - > one segment
 - > one IP address


*Make sure to press the **Enter** key after typing an IP address.*

The Source and Destination dropdown's **Groups** and **Segments** lists are shown in alphabetical order. Sub-groups and sub-segments are listed under their Level 0 in the hierarchy.

The **Source** filter matches when the traffic was from a device that belongs to *all* the selected groups *and* to the selected Forescout eyeSight segment, *and* that has the provided IP address.

The **Destination** filter matches when the traffic was to a device that belongs to *all* the selected groups *and* to the selected Forescout eyeSight segment, *and* that has the provided IP address.

- In the **Service** field, you can enter any combination of:
 - > multiple services
 - > multiple inspected protocols

 The available services are based on standard Linux port-to-protocol mapping. When Medigate or SilentDefense reports traffic data, their Deep-Packet Inspection (DPI) techniques provide inspected protocol values that are more accurate than the standard mapping.


The filter matches when the traffic used *any* of the selected services or inspected protocols.

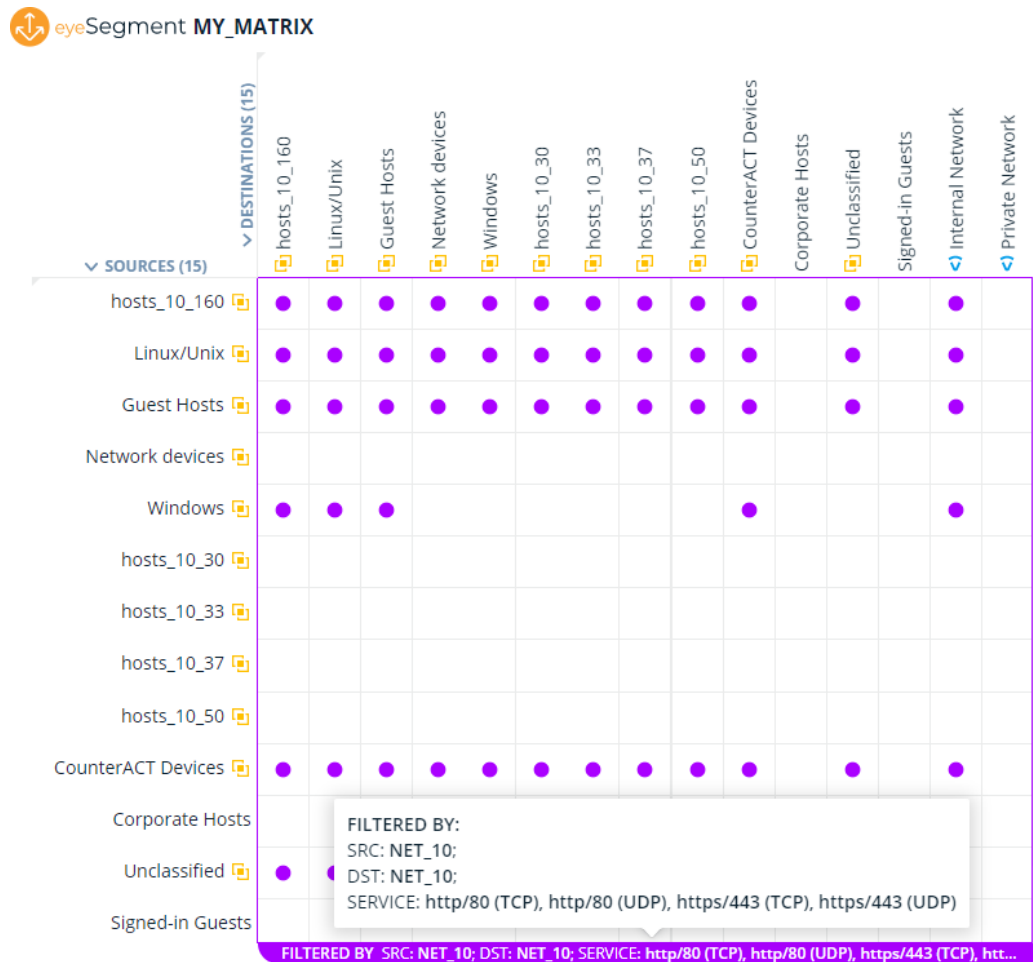
- If **Exclude Traffic** is *not* selected, traffic is only shown if it meets all of the following conditions:
 - The traffic data was uploaded to the cloud during the range in the **Date Range** field. The matrix shows no other traffic.
 - The traffic originated at a device that matches the **Source** filter field. The matrix shows no other traffic.
 - The traffic ended at a device that matches the **Destination** filter field. The matrix shows no other traffic.
 - The traffic used one of the **Service** filter fields. The matrix shows no other traffic.
- If **Exclude Traffic** is selected, traffic is only shown if it meets all of the following conditions:
 - The traffic data was uploaded to the cloud within the past 90 days but outside the range in the **Date Range** field.
 - The traffic originated at a device that does not match the **Source** filter field.
 - The traffic ended at a device that does not match the **Destination** filter field.
 - The traffic did not use any of the **Service** filter fields.

 You can use the Clear Filter icon  to clear all the filter fields except the date range.

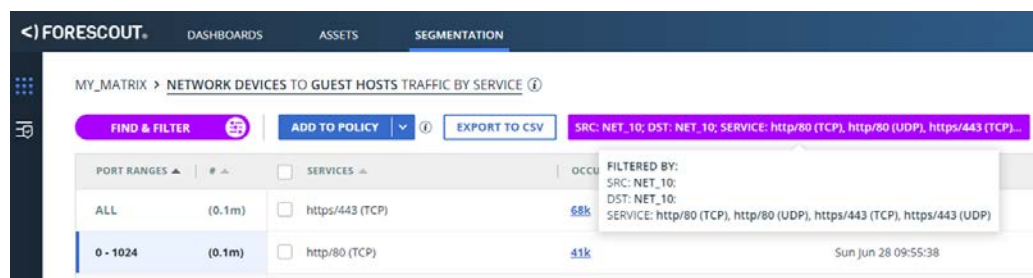
3. Select **Apply** to see how your filter selections affect the displayed traffic without closing the Find & Filter window.
4. Select **OK** to close the Find & Filter window and save the filter.

When *Find & Filter* criteria are applied:

- The traffic icons are violet to indicate that the matrix shows only traffic that matches the filter.
- The **Find & Filter** button is violet.
- A filter indicator  followed by the filter criteria are displayed as a tag at the bottom of the matrix. If the criteria list is very long, hover over the tag to see all the filter criteria.



- In traffic detail pages, the filter criteria are displayed in a violet box above the table. If the criteria list is very long, hover over the tag to see all the filter criteria.



Focus on a Matrix Row, Column, or Cell

With one click you can focus the matrix on a single row, column, or cell. If the selected Source and/or Destination zone is a nested structure, its next-level sub-groups are expanded in the focused matrix. To create a focused matrix:

- Select the zone name of a matrix row or column.

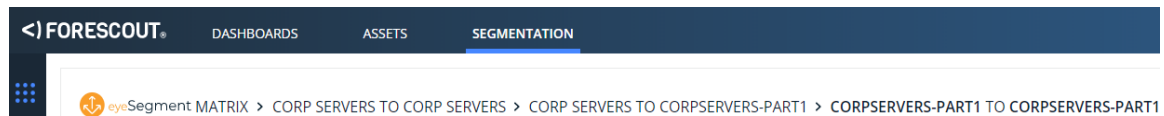
- Hover over the cell of a Source and Destination zone pair, and select **Focused Matrix**.

You can continue to select a zone name or cell in the focused matrix to further focus on lower-level sub-groups.

 A focused matrix does not display [Overlapping Zones](#) indicators.

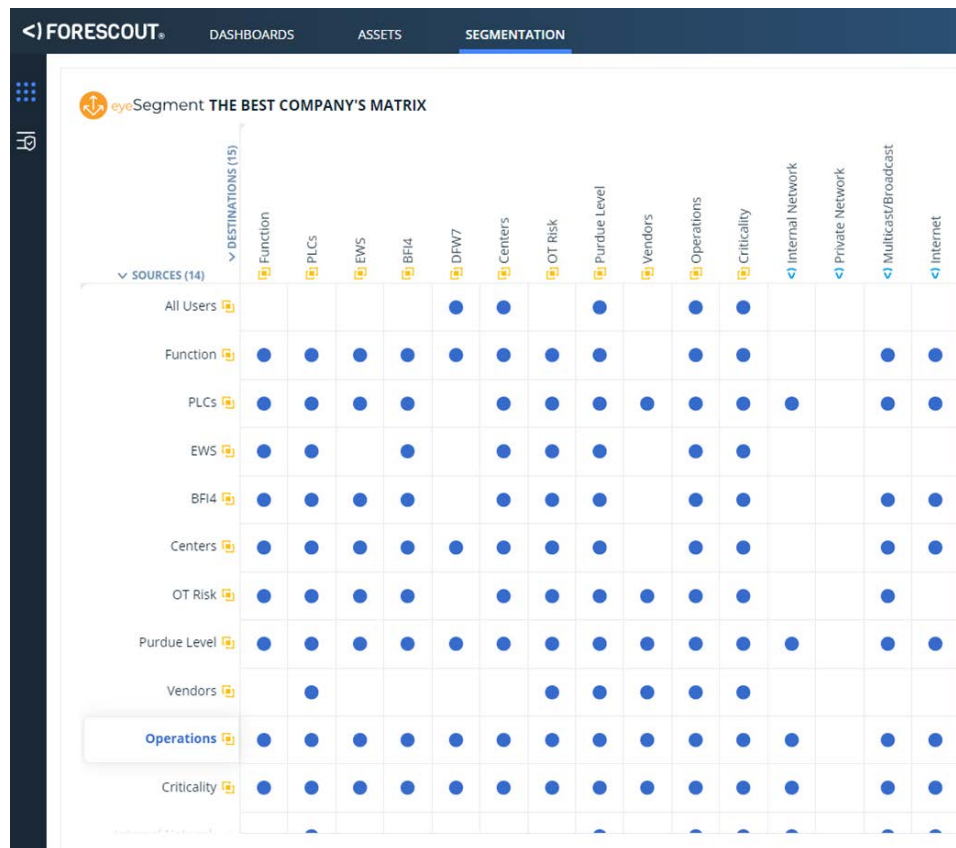
Devices in the selected Source or Destination zone that are not members of any lower-level sub-group are included under the name of the lowest-level group they are in, followed by '- Other'. If a selected zone has no lower-level sub-groups, all of its devices are included under the name of the zone.

The breadcrumb next to the matrix name indicates that only a selection of the original matrix is displayed. You can select any part of the breadcrumb to return to an earlier display.

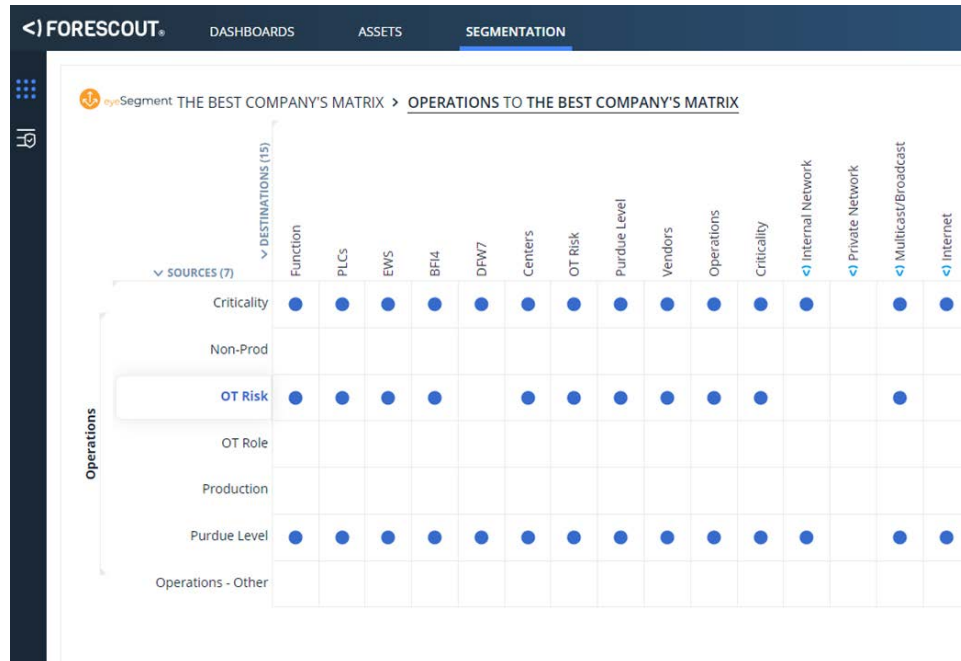


Focus on a Row or Column

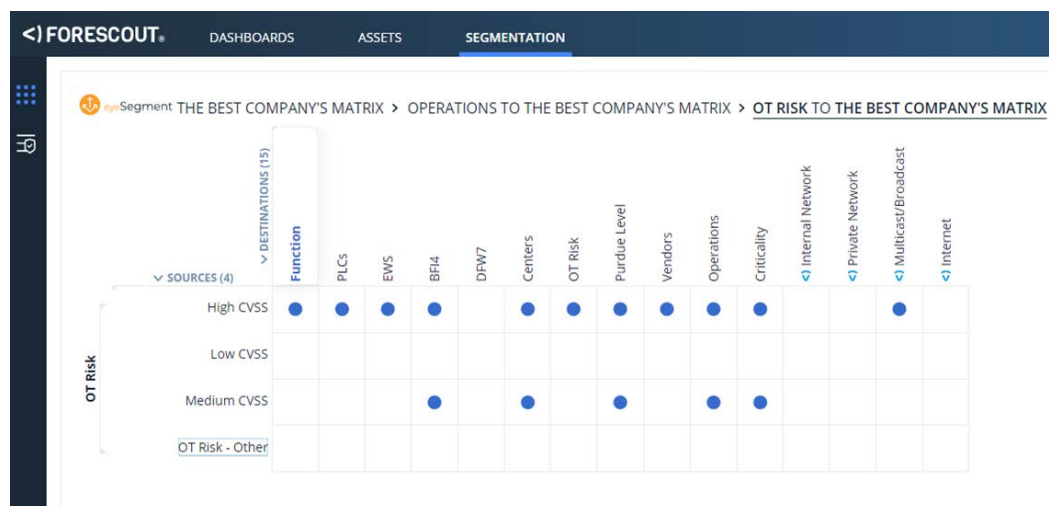
In the following illustration, a user focuses on rows and columns in a matrix named *The Best Company's Matrix*.



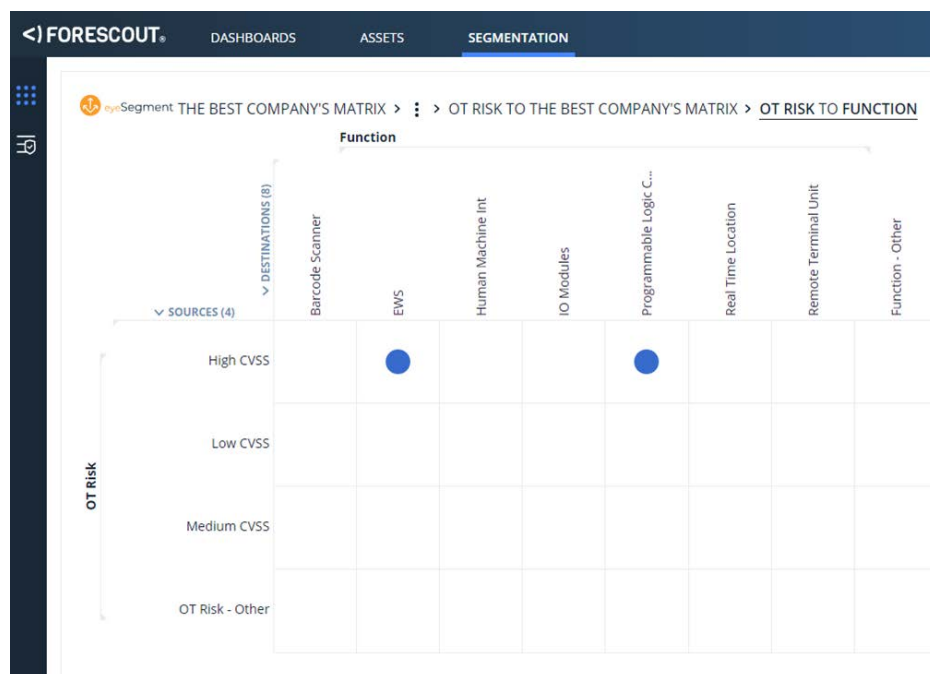
1. The user selects the **Operations** Source zone. This expands the entire Source zone, showing its next-level sub-groups as individual Source zones. All other Source zones are removed from the matrix. The Destination zones are unchanged.



2. Next, the user selects the **OT Risk** Source zone sub-group. That sub-group is expanded, showing its next-level sub-groups as individual Source zones. All other Source zone sub-groups are removed from the matrix. The Destination zones are unchanged.



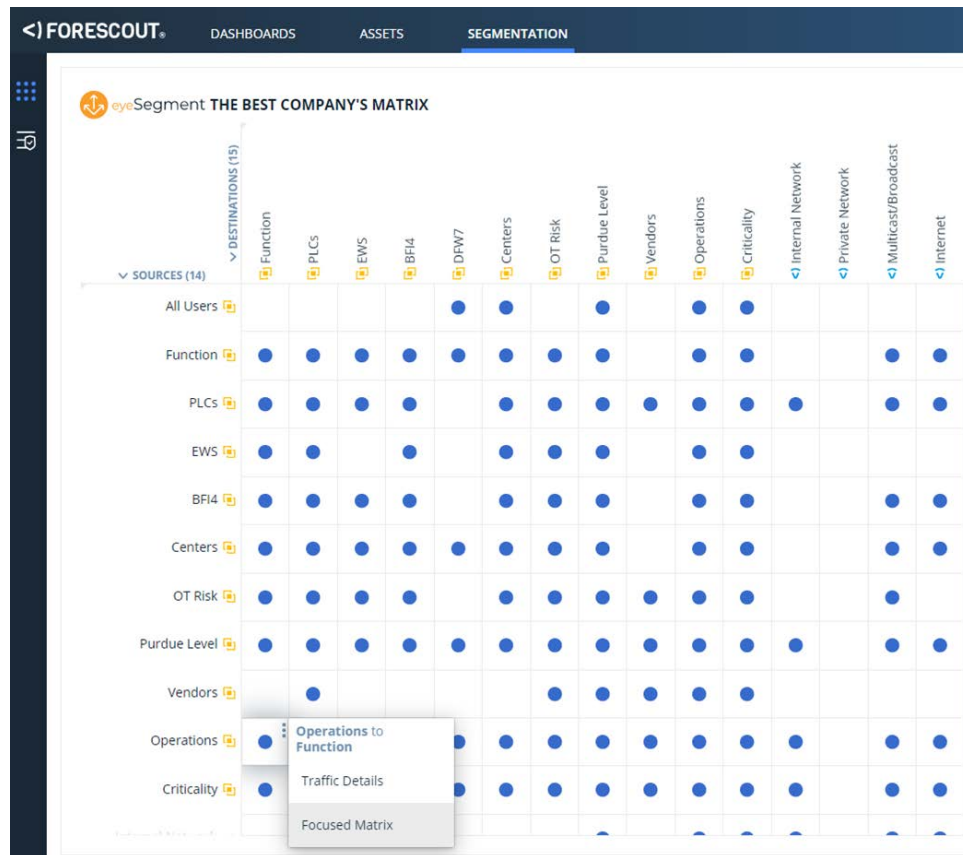
3. Now the user wants to focus on traffic between those sub-groups and the **Function** Destination zone. The Destination zone is expanded, showing its next-level sub-groups as individual Destination zones. All other Destination zones are removed from the matrix. The Source zones are unchanged.



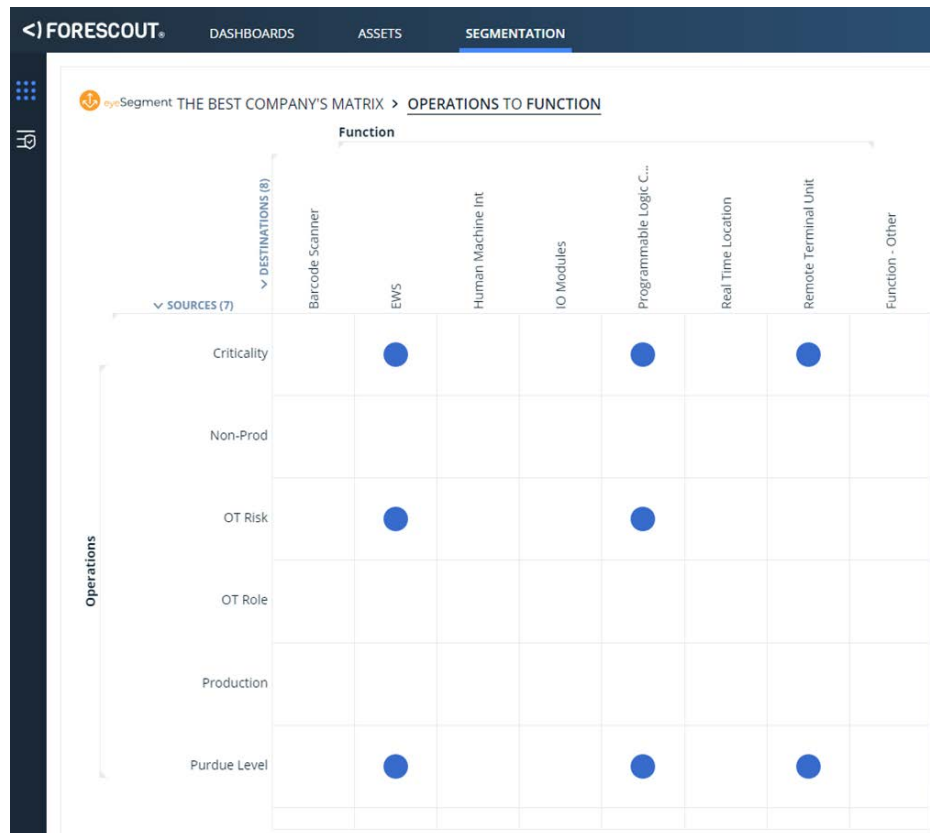
Focus on a Cell

To generate a focused matrix from a single cell:

1. In the matrix, hover over the cell of the specific Source and Destination zones, and select **Focused Matrix**.




The cell's Source and Destination zones are expanded, showing their next-level sub-groups as individual Source and Destination zones. No other Source and Destination zones are displayed in this focused matrix.



View and Export Traffic Details

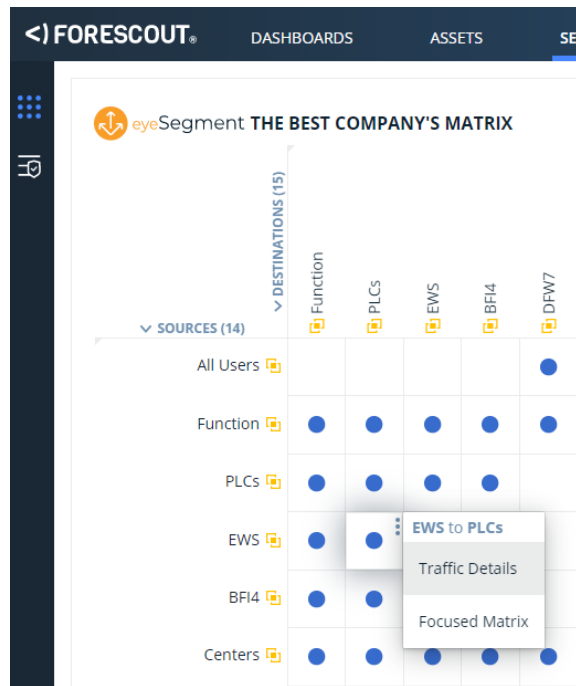
For each traffic icon, you can view the sub-groups, services, Source and Destination IP addresses, and the number of occurrences of the traffic within the defined time range. Use this information to help decide which groups to add to the matrix or to a filter.

Select the **Find & Filter** button to add or change filter criteria.

 You can view up to 1,000 entries. If your traffic of interest is not displayed, add filter criteria to display less traffic that is not of interest and focus on only specific traffic.

To view and export details of a specific traffic pattern:

1. In the matrix, hover over the matrix cell of the specific Source and Destination zone, and select **Traffic Details**.



2. If one or both of the selected zones contains sub-groups, the detected traffic is shown as a nested structure. A color indicates the level of each sub-group for which traffic was detected. If lower-level sub-groups exist but the Source or Destination device is not a member of any of them, the device is listed under the name of the lowest level group it is in, followed by '- Other'.

The screenshot shows the 'SEGMENTATION' dashboard for 'THE BEST COMPANY'S MATRIX'. The table displays traffic segments with the following columns: SOURCE ZONE, DESTINATION ZONE, OCCURRENCES, STARTING FROM, and LAST UPDATE. A legend at the bottom indicates traffic levels from 0 to 4.

SOURCE ZONE	DESTINATION ZONE	OCCURRENCES	STARTING FROM	LAST UPDATE
■ Criticality	(8 connections)	1	Thu May 14 10:02:57	Thu May 21 01:27:22
■ OT Risk	(2 connections)	1	Thu May 14 10:03:21	Thu May 21 01:35:57
■ High CVSS				
	■ EWS	2.3k	Thu May 14 16:08:11	Thu May 21 01:35:57
	■ Programmable Logi...	170	Thu May 14 10:03:21	Thu May 14 15:48:31
■ Purdue Level	(10 connections)	1	Thu May 14 10:02:57	Thu May 21 01:27:22
■ Purdue Level 1				
	■ EWS	502	Thu May 14 16:37:11	Thu May 21 01:27:22
	■ Programmable Logi...	9.3k	Thu May 14 16:36:31	Thu May 21 01:26:32
	■ Remote Terminal Unit	66	Thu May 14 16:43:08	Thu May 14 16:43:08
■ Purdue Level 2				
	■ Programmable Logi...	540		
	■ Remote Terminal Unit	230		

Legend: ■ Level 0 ■ Level 1 ■ Level 2 ■ Level 3 ■ Level 4

To see traffic by service for nested structures, select the Occurrences value of the Source and Destination zone traffic.

3. Additional options are available when traffic originates or ends at an IP address included in the [Internal Network](#) zone. These internal network IP addresses are not in another user-defined zone in the matrix.
 - Select **Other Zones** to view these IP addresses in their groups that you have not included as matrix zones. IP addresses in your internal network but not in any defined group are listed as *Not in any group*.

SOURCE ZONE	DESTINATION ZONE	OCCURRENCES	STARTING FROM	LAST UPDATE
Criticality	(6 connections)	1	Wed May 13 13:17:52	Thu May 21 01:27:17
Importance 2				
All Zones				
Dimensions				
All Locations				
All Locations - Other		2	Wed May 13 13:17:52	Wed May 13 13:19:12
Taxonomy				
Networks				
10.0.0.0		2	Wed May 13 13:17:52	Wed May 13 13:19:12
11.0.0.0		260	Thu May 14 10:06:32	Thu May 21 01:27:17
Unclassified		2	Wed May 13 13:17:52	Wed May 13 13:19:12
Not in any group		2		

Legend: Level 0 Level 1 Level 2 Level 3 Level 4

4. If neither of the selected zones is a nested structure, the detected traffic is listed by service. The services are grouped into port ranges of 1,000. Select port range named **All** to see a table of all the services.

In the example below, service details are shown for traffic originating from devices in the *EWS* zone and ending at devices in the *PLCs* zone. The **Traffic Violations** box indicates that the Traffic Violations option was selected in the matrix, and the traffic shown violated a simulated policy rule.

The screenshot shows the ForeScout Segmentation dashboard. The breadcrumb trail is 'THE BEST COMPANY'S MATRIX > EWS TO PLCS TRAFFIC BY SERVICE'. The interface includes a 'FIND & FILTER' button, a 'TRAFFIC VIOLATIONS' indicator, an 'ADD TO POLICY' dropdown, and an 'EXPORT TO CSV' button. A table displays traffic data with columns for Port Ranges, Services, Occurrences, Starting From, and Last Update. The '0 - 1024' port range is selected, showing 19 occurrences of netbios-ns/137 (UDP) traffic, with a starting time of Wed Jul 08 20:02:31 and a last update of Thu Jul 09 17:34:19.

PORT RANGES	SERVICES	OCCURRENCES	STARTING FROM	LAST UPDATE
ALL (22)	<input type="checkbox"/> netbios-ns/137 (UDP)	19	Wed Jul 08 20:02:31	Thu Jul 09 17:34:19
0 - 1024 (19)				
41000 - 41999 (2)				
42000 - 42999 (1)				

The port-to-protocol service mapping is based on standard static Linux mapping. When Medigate or SilentDefense reports traffic data, their Deep-Packet Inspection (DPI) techniques provide inspected protocol values that are more accurate than the standard mapping.

- To download a CSV file containing details about all the traffic for the traffic pattern represented in the *Traffic by Service* window, select **Export to CSV**. Traffic that does not meet your applied *Find & Filter* criteria is not exported.

If the *Traffic by Service* page shows only policy rule violations, only the violating traffic is exported.

The traffic details for all ports are exported, regardless of which port range is selected in the table.

For each traffic pattern, the exported file includes:

- Source Zone, including each sub-group
- Source IP address
- Destination Zone, including each sub-group
- Destination IP address
- Port
- Protocol
- Service
- Earliest date and time of this traffic
- Last date and time of this traffic
- Number of connections


The file also includes the following header rows:

- Source Zone of the *Traffic by Service* page that was exported
- An indication that the Source Zone is a group
- Destination Zone of the *Traffic by Service* page that was exported
- An indication that the Destination Zone is a group
- An indication if the contents are Traffic Violations Only or Baseline Traffic
- Details of the *Find & Filter* criteria, if applied

Some Find & Filter criteria are exported in non-standard formats:


- Dates are exported as UTC times.
 - Protocols are exported as protocolId decimal values. For more information, refer to <https://www.iana.org/assignments/protocol-numbers/protocol-numbers.xhtml>.
- File creation date and time, in UTC
 - Name of the user who created the file

The downloaded filename includes the Source and Destination zone names of the exported traffic details, and the UTC file creation date and time.

 You can export up to 100,000 records at a time.

View IP-to-IP Traffic Details

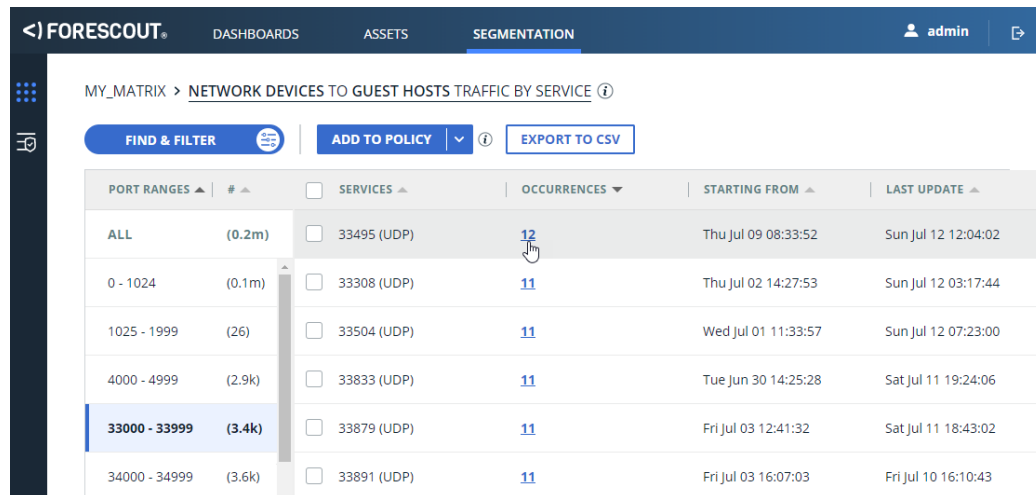
You can view details about the Source and Destination IP addresses in the selected groups that sent or received traffic.

 If more than 1,000 IP addresses in the selected Source or Destination group had traffic, you can view 1,000 addresses:

- that had the most amount of traffic
- that had the least amount of traffic

To view details of IP addresses that sent or received traffic:

1. In the Traffic by Service page, select the Occurrences value of a service used by the Source and Destination zone traffic.

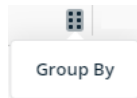


The screenshot shows the FORESCOUT interface with the SEGMENTATION tab selected. The breadcrumb path is MY_MATRIX > NETWORK DEVICES TO GUEST HOSTS TRAFFIC BY SERVICE. There are buttons for FIND & FILTER, ADD TO POLICY, and EXPORT TO CSV. A table lists various services with columns for PORT RANGES, SERVICES, OCCURRENCES, STARTING FROM, and LAST UPDATE. The service 33495 (UDP) is highlighted with 12 occurrences.

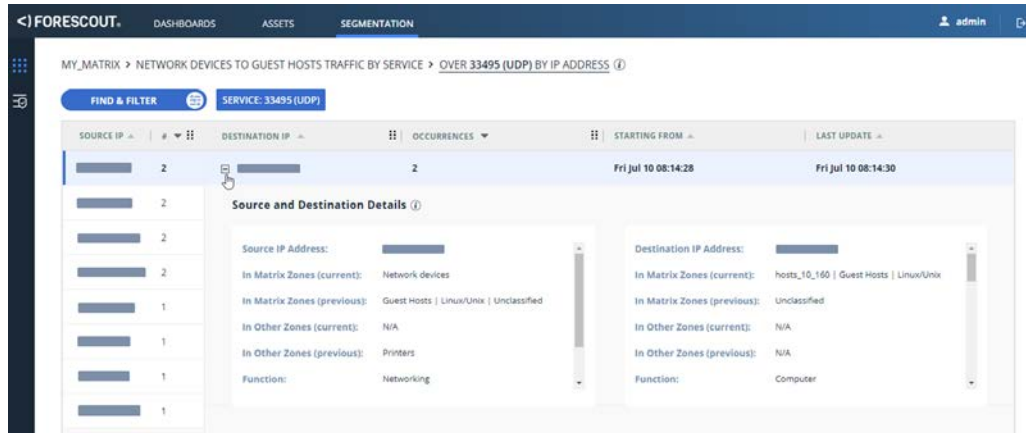
PORT RANGES ▲	# ▲	SERVICES ▲	OCCURRENCES ▼	STARTING FROM ▲	LAST UPDATE ▲
ALL	(0.2m)	<input type="checkbox"/> 33495 (UDP)	12	Thu Jul 09 08:33:52	Sun Jul 12 12:04:02
0 - 1024	(0.1m)	<input type="checkbox"/> 33308 (UDP)	11	Thu Jul 02 14:27:53	Sun Jul 12 03:17:44
1025 - 1999	(26)	<input type="checkbox"/> 33504 (UDP)	11	Wed Jul 01 11:33:57	Sun Jul 12 07:23:00
4000 - 4999	(2.9k)	<input type="checkbox"/> 33833 (UDP)	11	Tue Jun 30 14:25:28	Sat Jul 11 19:24:06
33000 - 33999	(3.4k)	<input type="checkbox"/> 33879 (UDP)	11	Fri Jul 03 12:41:32	Sat Jul 11 18:43:02
34000 - 34999	(3.6k)	<input type="checkbox"/> 33891 (UDP)	11	Fri Jul 03 16:07:03	Fri Jul 10 16:10:43

The traffic details are shown for each IP address within the Source and Destination zones that used the selected service.

2. You can view the IP-to-IP traffic details by Source zone IP address, or by Destination zone IP address. To toggle between these views, select the **Group By** button.



3. Select a row to view details about the Source and Destination devices.



The details include:

- All the matrix zones the device is currently a member of
- All the matrix zones the device is not currently a member of, but was a member of within the last 90 days, and so its traffic might be included in these zones
- All the ForeScout policy groups not shown in the matrix that the device is currently a member of
- All the ForeScout policy groups not shown in the matrix that the device is not currently a member of, but was a member of within the last 90 days
- Function property value
- Vendor and Model property value
- Operating Systems property value
- Other property values if relevant, such as MAC address, open ports, DNS name, user


Delete Traffic

You can permanently delete some or all the traffic data used for the matrix. You might want to do this when:


- some of the traffic shown is not accurate because devices were misclassified and assigned to the wrong zone
- a group used in the matrix becomes divided into multiple groups

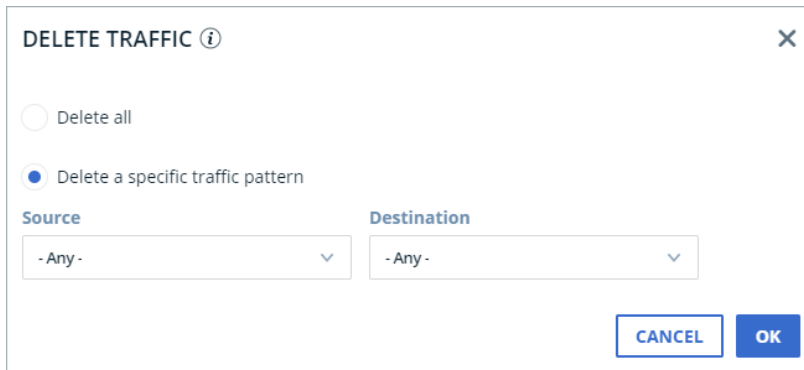
To use this feature, you might need to have additional permissions configured for you at the ForeScout Console.

Traffic collected previously is deleted, but traffic collected after running the command is displayed as regular traffic. It is recommended to complete all group adjustments before you delete the traffic so that all subsequent traffic is aligned with its correct groups.

 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, see the *Data Security Schedule for Customer Network Data in the Forescout Cloud Service* at <https://www.forescout.com/company/legal/data-security-schedule/>.

To permanently delete traffic data:


1. On the eyeSegment Matrix page, select the menu icon , and select **Delete Traffic**.
2. To permanently delete all the accumulated traffic data and clear the matrix, select **Delete all**.
3. To permanently delete only specific traffic data, select **Delete a specific traffic pattern**, and select the traffic pattern to be deleted.



The dialog box titled "DELETE TRAFFIC" with an information icon and a close button (X). It contains two radio buttons: "Delete all" (unselected) and "Delete a specific traffic pattern" (selected). Below the radio buttons are two dropdown menus labeled "Source" and "Destination", both currently showing "- Any -". At the bottom right are "CANCEL" and "OK" buttons.

4. Confirm that you want to delete the traffic data.


The delete process might take several seconds. A new delete request cannot be initiated until the previous delete process is finished.

 If an error message indicates that not all of the traffic was deleted, the remaining traffic continues to be shown in the matrix. Try later to delete the remaining traffic that you intended to delete so that the matrix accurately reflects the traffic in the stated time period.


Ignore Traffic of Specific Devices

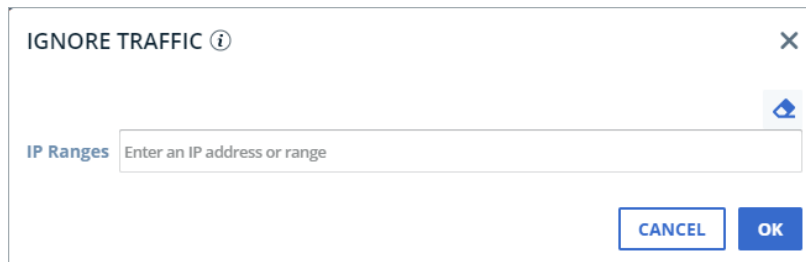
You can stop the collection of traffic data for specific devices. You might want to do this when the traffic between those devices and all other devices is already well managed.

Traffic saved earlier for these devices is not deleted or cleared from the matrix. Consider creating groups of only these devices so that you can use the [Delete Traffic](#) option to permanently delete from the matrix all traffic data previously collected for the group.

 *To use this feature, you might need to have additional permissions configured for you at the Forescout Console.*

To stop collecting traffic data of specific devices:

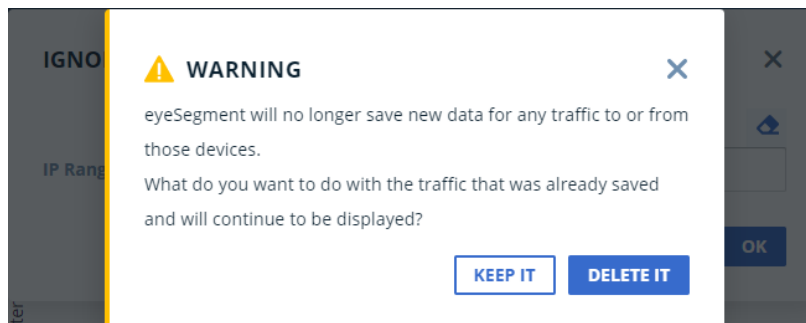
1. On the eyeSegment Matrix page, select the menu icon , and select **Ignore Traffic**.

A dialog box titled "IGNORE TRAFFIC" with an information icon. It contains a text input field labeled "IP Ranges" with the placeholder text "Enter an IP address or range". Below the input field are two buttons: "CANCEL" and "OK".

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

 *Do not enter a subnet mask.*

3. Select **OK**. A warning message informs you that future traffic for those devices will be ignored, but traffic that was already saved will continue to be included in the matrix.

A warning dialog box with a yellow warning triangle icon and the title "WARNING". The text inside says: "eyeSegment will no longer save new data for any traffic to or from those devices. What do you want to do with the traffic that was already saved and will continue to be displayed?". At the bottom are two buttons: "KEEP IT" and "DELETE IT".


4. Do one of the following:
 - To continue displaying the traffic saved earlier, select **Keep It**.

- To open the [Delete Traffic](#) window where you can delete saved traffic, select **Delete It**.

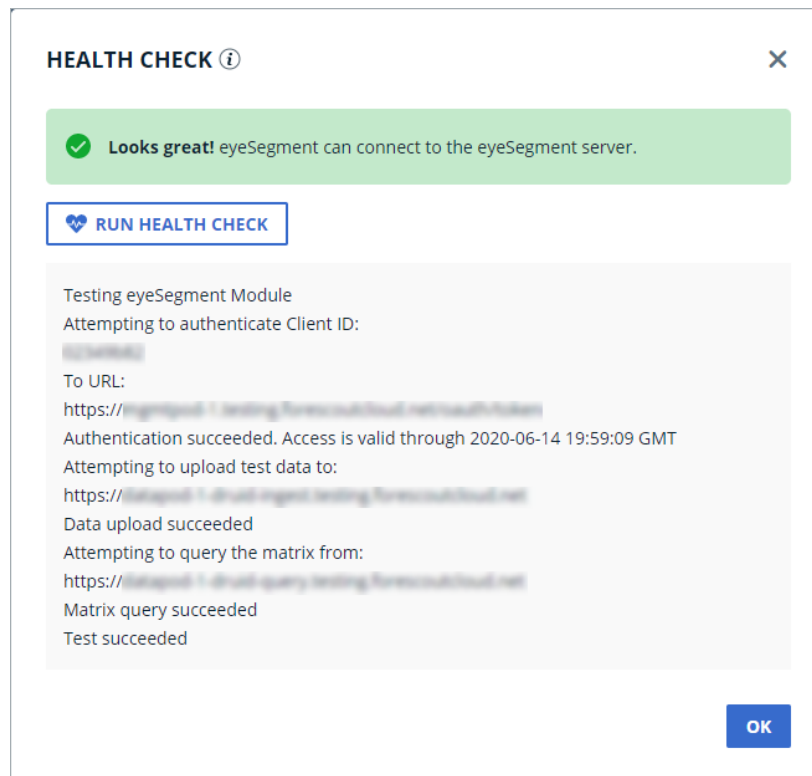
Run a Health Check

Run a health check to confirm that traffic data can be uploaded to the eyeSegment server.


To run a health check:

1. On the eyeSegment Matrix page, select the menu icon , and select **Health Check**.
2. Select the **Run Health Check** button.

 *The health check might run for several seconds.*




3. If the test fails, use the log to determine the problem.

 *If your cloud authentication credentials are invalid, provide valid credentials in the Cloud Uploader configuration. Refer to the Cloud Uploader Configuration Guide for more information.*




About the eyeSegment Policy

An eyeSegment policy is a set of rules. Each rule applies to traffic from a specific Source zone to a specific Destination zone. The rule and its exceptions determine which traffic is *allowed* and which is *denied*. Use this feature to define different actions for individual sub-groups and services.

By default, all traffic is allowed.


 *In this version, rules that deny traffic cannot actually block traffic. They can be used to display suspicious traffic in the matrix and also to send a notification when this traffic is detected.*

Policy rules can include any of the following as Source and Destination zones:

- Specific groups and sub-groups defined in your Forescout configuration.
- The virtual zone named  [Private Network](#) that includes all the devices not within Forescout's internal network but that are in the company's private network.
- The virtual zone named  Multicast/Broadcast that includes multicast and broadcast address ranges.
- The virtual zone named  [Internet](#) that includes all the devices not within the company's private network.
- The virtual zone named - **Any** - that includes all devices.

If an existing rule manages the traffic between a Source zone and a Destination zone, another rule cannot be created for the same two zones.

Policy rules cannot include the following as a Source or Destination zone:

- The virtual zone named  [Internal Network](#).
- A hierarchical group name followed by '- Other' which includes all members of that group that are not members of any of its lower-level sub-groups.

What You Need to Know about This Version

In this version:

- The status of a rule can be set to either **Draft** or **Simulation**.
- If you enable **Notification** for a simulated rule's, device properties are set whenever the rule is violated. See [Send Notifications](#).
- The eyeSegment policy is for simulation purposes only.
- The policy cannot actually deny traffic.

About Simulated Rules

When the rule status is *Simulation* and the rule action is *Deny*, a simulated traffic violation is triggered when both of the following occur:

- A device in the rule's Source zone sends traffic to a device in the rule's Destination zone.

and

- The traffic pattern is not included in a rule exception.

When the rule status is *Simulation* and an exception's action is *Deny*, a simulated traffic violation is triggered when both of the following occur:

- A device in the rule's Source zone sends traffic to a device in the rule's Destination zone.

and

- The traffic pattern is included in the rule exception.

To set device properties whenever the rule is violated, enable **Notification**. See [Send Notifications](#).

To visualize the violations on the eyeSegment Matrix page, select **Traffic Violations** in the [Matrix Visualization Settings](#).

Send Notifications

Device properties can be set whenever a device is the source or destination of denied traffic in a simulated rule.

Notification



If **Notification** is selected in the eyeSegment policy rule, and a simulated traffic violation occurs:


- On the device that sent the denied traffic:
 - In the *Traffic Was Denied from This Client* property, the policy adds the name of the rule that denied the traffic.
 - In the *Server Groups to Which Traffic Was Denied* property, the policy adds the name of lowest-level Forescout policy group in the rule, including exceptions, to which the destination IP address belongs.
If the only Destination zone in the rule and its exceptions is one of the [virtual zones](#), the virtual zone is added to this property.
- On the device that received the denied traffic:
 - In the *Traffic Was Denied to This Server* property, the policy adds the name of the rule that denied the traffic.
 - In the *Client Groups from Which Traffic Was Denied* property, the policy adds the name of lowest-level Forescout policy group in the rule, including exceptions, to which the source IP address belongs.
If the only Source zone in the rule and its exceptions is one of the [virtual zones](#), the virtual zone is added to this property.

You can use these properties to write Forescout policies for handling devices that send or receive denied traffic.



For more information about using these properties, refer to the *eyeSegment Module Configuration Guide*. See [Additional Forescout Documentation](#) for information on how to access this guide.

Visualize the eyeSegment Policy in the Matrix

You can visualize your eyeSegment policy rules in the matrix. This helps you ensure that each network connection of interest is managed by a rule.

 *To help you visualize the implications of your eyeSegment policy, Forescout recommends that your matrix include all the zones used in your policy rules.*


All traffic is evaluated by your eyeSegment policy.

- Traffic denied by an eyeSegment policy rule is shown in the matrix as a *Traffic Violation* .
- A conflict occurs when a zone is included in two different rules. This can happen when - **Any** - is selected as a zone in one of the rules. Hover over the *Conflict* icon  to identify which rules are in conflict.

Create eyeSegment Policy Rules

There are two ways to create eyeSegment policy rules:

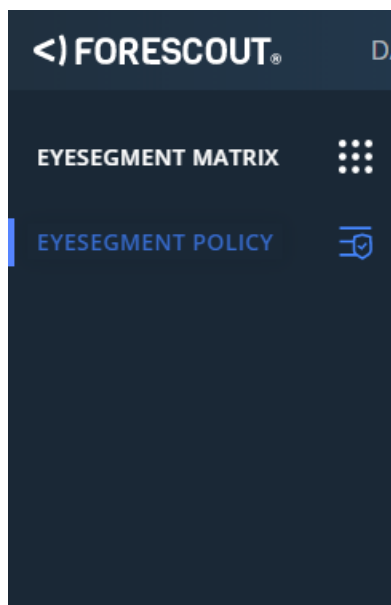
- [Manually Create Policy Rules](#)
- [Automatically Create Policy Rules](#)

 *To manage the eyeSegment policy, you might need to have additional permissions configured for you at the Forescout Console.*

Manually Create Policy Rules

To manually create an eyeSegment policy rule:

1. Hover over the side navigator, and select **eyeSegment Policy**.




2. Select **Add Rule**.
3. To configure the rule and its exceptions, see [Configure Policy Rules](#).
4. To return to the matrix, hover over the side navigator, and select **eyeSegment Matrix**.

Automatically Create Policy Rules

You can automatically create an eyeSegment policy rule in Draft status from a *Traffic* or *Traffic by Service* page. The rule allows or denies all traffic from the Source zone to the Destination zone except for the traffic patterns you select. If a rule already exists for that traffic, the rule is updated with the selected exceptions.

- On a *Traffic by Service* page, the rule adds as exceptions all the traffic that uses any of the selected services.
- On a *Traffic* page, the rule adds as exceptions all selected traffic patterns using any service.
- If *Find & Filter* criteria are applied, they are automatically included in the rule exceptions.


 *The date range filter is not included in rule exceptions.*


To automatically create a rule and exceptions for specific traffic patterns, select the sub-groups and services to be the rule exceptions.

 *No changes are made to your eyeSegment policy until you select **Save**.*

To create an eyeSegment policy rule with just a few clicks:

1. [View and Export Traffic Details](#) of the traffic pattern to be included in the rule.
2. Select the checkbox of each service or traffic pattern for which traffic is to be an exception to your rule.

 *You can select up to 50 services or traffic patterns as exceptions each time.*

3. From the **Add to Policy** dropdown menu, select one of the following:
 - **Deny All Except Selected:** The rule denies all traffic from the Source zone to the Destination zone except for the traffic patterns you select.
 - **Allow All Except Selected:** The rule allows all traffic from the Source zone to the Destination zone except for the traffic patterns you select.
-  *If a rule for these zones already exists, the selected patterns are added to its list of exceptions.*
4. Select **Show Me the Rule**.
 - If this traffic did not have a rule, a new rule having a default name is displayed.
 - If a rule already exists for this traffic, the existing rule is displayed.


The service or traffic patterns you selected are displayed as exceptions to the rule.

5. To edit the rule and its exceptions, see [Configure Policy Rules](#).

Edit or Delete Policy Rules

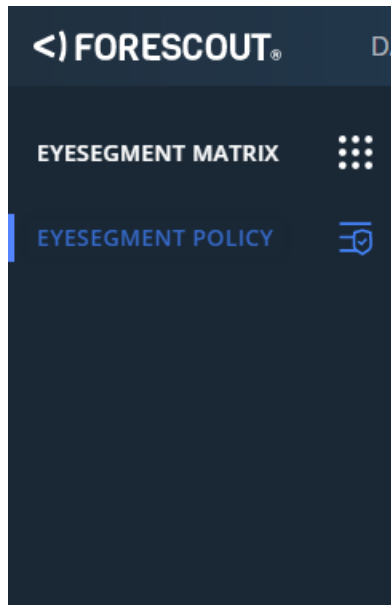
You can edit one eyeSegment policy rule at a time. You can delete multiple rules at a time.

If you edit or delete a rule that was in Simulation status, all its previously detected simulated traffic violations are cleared from the matrix.

 If you cannot delete a rule, see [eyeSegment Policy Rules Cannot Be Deleted in the Considerations and Troubleshooting section](#).

To edit or delete an eyeSegment policy rule:


1. Hover over the side navigator, and select **eyeSegment Policy**.

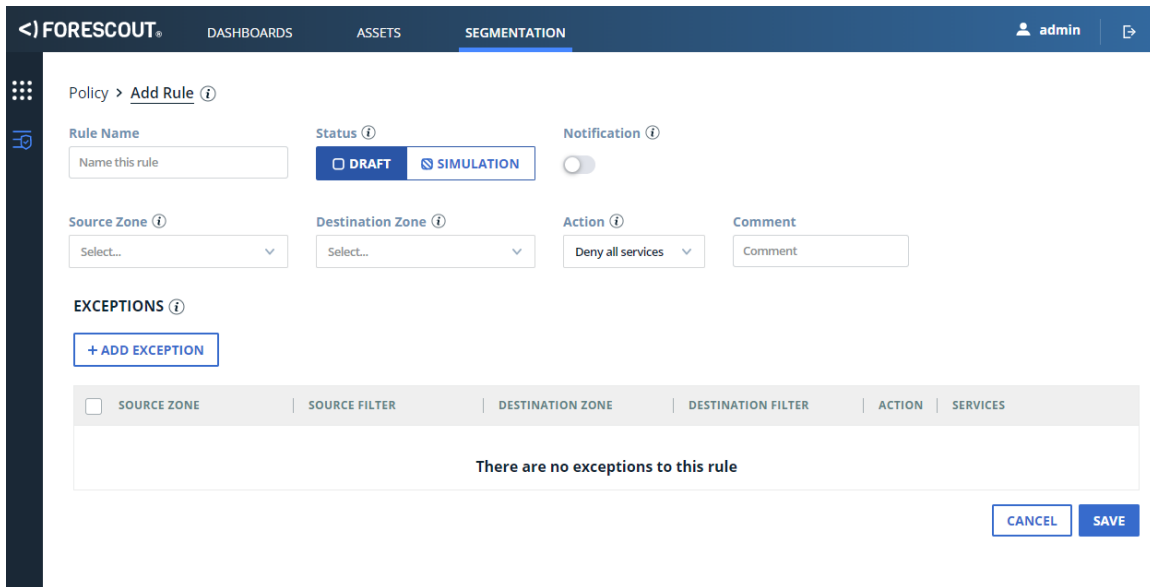


2. To delete one or more rules, select the rules' checkboxes, and select **Delete**.
3. To edit a rule and its exceptions, select the rule's checkbox, and select **Edit Rule**. See [Configure Policy Rules](#).
4. To return to the Matrix page, hover over the side navigator, and select **eyeSegment Matrix**.

Configure Policy Rules

You can change eyeSegment policy rule fields at any time.

 If you save changes to a rule that was in Simulation status, all its previously detected simulated traffic violations are cleared from the matrix.



To configure an eyeSegment policy rule:

1. Name the rule.
 - Rule names are displayed in the eyeSegment Policy page.
 - When a rule in Simulation status with Notification denies traffic, the rule name is written to a device property on both the client and the server.
2. Select a Source Zone and a Destination Zone. The rule will manage all traffic that originates at an IP address in the selected Source zone and ends at an IP address in the selected Destination zone.

 *Note:*



- A selected zone includes also all IP addresses in its sub-groups.
- The zone named - **Any** - includes all IP addresses.
- If either of the rule zones is not included in your matrix, a pop-up message asks if you'd like to add it to the matrix. Adding the zone enables you to visualize the rule and its violations in the matrix.


3. Do one of the following:
 - To deny all traffic between these zones, with possible exceptions of specific traffic patterns, select **Deny all services** in the Action field.
 - To allow all traffic between these zones, with possible exceptions of specific traffic patterns, select **Allow all services** in the Action field.

 To add exceptions for specific traffic patterns, see [Add Rule Exceptions](#).

When *Policy Visualization* is selected in the [Matrix Visualization Settings](#), you can see an indication that the traffic between these zones is defined as *Deny* or *Allow*.

4. In the Status field, do one of the following:
 - If you are not yet interested in seeing simulated traffic violations of this rule, select **Draft**.
 - To see the rule's violations simulated in the matrix, select **Simulation**.

 *Device properties are only set when the simulated rule is violated and when **Notification** is enabled.*
5. To update device properties whenever the device is the source or destination of traffic denied by this rule, select **Notification**. See [Send Notifications](#). A rule for which **Notification** is selected is marked by a bell .

 *This setting is not available when the rule status is Draft.*

6. To delete an exception, select it, and select **Delete**.


Add Rule Exceptions

You can add exceptions to eyeSegment policy rules. Exceptions that meet all the following conditions override the rule:

- The traffic originates at an IP address that is in the exception's Source Zone and also in all of the exception's Source Filter zones.
- The traffic ends at an IP address that is in the exception's Destination Zone and also in all of the exception's Destination Filter zones.
- The traffic uses one of the exception's Services.

To add an exception:

1. In the *Add Rule* or *Edit Rule* page, select + **Add Exception**.
2. In the exception's Source Zone and Destination Zone fields, select the same zones as, or sub-groups of, the zones in the rule.

 *A selected zone includes also all IP addresses in its sub-groups.*
3. Optionally select other groups as Source or Destination filters.
4. In the exception's Service field, select **All** for the exception to apply to traffic on all services, or enter a list of specific services on which the exception applies.
5. Select **OK** for the exception to be added to the Exceptions table.

Considerations and Troubleshooting

Consider the following when using eyeSegment:

- [Forescout Web Client User Security](#)
- [Very Little Traffic Data in the Matrix](#)
- [Very Little Traffic Data for a Group](#)

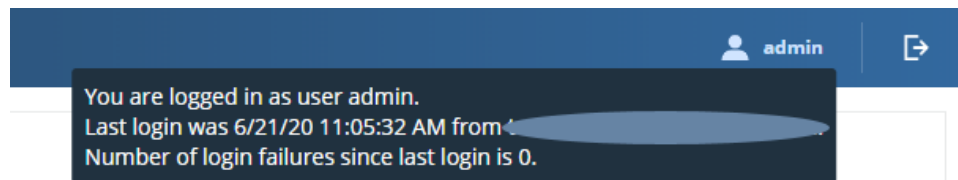
- [eyeSegment Policy Rules Cannot Be Deleted](#)
- [Groups Cannot Be Deleted at the Console](#)

Other issues are described in the Release Notes.

Forescout Web Client User Security

You can hover the mouse over your user name to see the following session information for your account:

- Your user name
- The time and IP address of your previous successful login
- The number of your recent, consecutive login attempts that failed



If you suspect this information is incorrect, report it to your security officer.

Very Little Traffic Data in the Matrix

When the eyeSegment Module is started, Appliances begin to report their detected traffic for each group defined in the Console.

Data is not available for any traffic detected:

- before the module was started
- before all traffic data was deleted

As time passes, more traffic data will be reported and shown.

If you suspect that no traffic is being reported, [Run a Health Check](#).

Very Little Traffic Data for a Group

The traffic data of network devices that are not part of any group is saved in the [Internal Network](#) zone.

- The eyeSegment module begins to save reported traffic data for a specific group after the group is created. Earlier traffic is not associated with that group.
- The eyeSegment module begins to save reported traffic data for a specific device to its group after the device has been added to the group. Earlier traffic for that device is not associated with that group.

eyeSegment Policy Rules Cannot Be Deleted

When a Forescout policy is created in the Console from the eyeSegment Policy Compliance policy template, the names of your eyeSegment policy rules might be selected in the *Traffic Was Denied from This Client* and *Traffic Was Denied to This Server* conditions. You cannot delete a rule from your eyeSegment policy if the rule name is selected in a policy condition.

Groups Cannot Be Deleted at the Console

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

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

Documentation downloads can be accessed from the [Technical Documentation Page](#), and from 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 Support Portal](#)

 Software downloads are also available from these portals.

To identify your licensing mode:

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

Technical Documentation Page

The Forescout Technical Documentation page provides a link to the searchable, web-based [Documentation Portal](#), as well as links to a wide range of Forescout technical documentation in PDF format.

To access the Technical Documentation page:

- Go to <https://www.Forescout.com/company/technical-documentation/>

Product Updates Portal

The Product Updates Portal provides product and documentation downloads for Forescout platform releases, Base Modules, Content Modules, and eyeExtend Modules. The portal also provides 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 Support Portal

The Downloads page on the Forescout Customer Support Portal provides product and documentation downloads for Forescout platform releases, Base Modules, Content Modules, and eyeExtend Modules. Software and related documentation only appear on the Downloads page if you have a license entitlement for the software.

To access documentation on the Customer Support 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.

To access the Documentation Portal:

- Go to https://updates.forescout.com/support/files/counteract/docs_portal/

Forescout Help Tools

You can access individual documents, as well as the [Documentation Portal](#), directly from the Forescout Console.

Console Help Buttons

- Use context sensitive *Help* buttons to quickly access information about the tasks and topics you are working with in the Console.

Forescout Administration Guide

- Select **Administration Guide** from the **Help** menu.

Plugin Help Files

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

Content Module, eyeSegment Module, and eyeExtend Module Help Files

- After the component is installed, select **Tools > Options > Modules**, select the component, and then select **Help**.

Documentation Portal

- Select **Documentation Portal** from the **Help** menu.