FORESCOUT

Forescout

Forescout eyeSight Administration Guide v9.1.4

Contact Information

Forescout Technologies, Inc.
2400 Dallas Pkwy, Suite 230, Plano, TX 75093
https://www.forescout.com/support-hub/
Toll-Free (US): 1-866-377-8773
Tel (Intl): 1-708-237-6591

About the Documentation

- Refer to the Documentation Portal for additional technical documentation: https://docs.forescout.com/
- Have feedback or questions? Write to us at documentation@forescout.com

Legal Notice

© 2026 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.

Table of Contents

Welcome to Forescout eyeSight v9.1.4 12

Log In to the Forescout Console 21

eyeSight device verification 23
Forescout eyeSight customer verification 23
Last Forescout Console login confirmation 24
Exit the Forescout Console 25

Forgot Your Forescout Console password? 25
Forescout Console access only cliadmin_console user 25

Create the Forescout Console access only cliadmin_console user 26

Work with the Forescout eyeSight Initial Setup Wizard 27

Before running the Forescout eyeSight Initial Setup Wizard 27
Update Forescout eyeSight Initial Setup Wizard settings 28
Set Up an appliance with the Forescout eyeSight Initial Setup Wizard 28

Add Channels. 46
Add Channels dialog box 47

Set up an appliance with Enterprise Manager settings 48

Add eyeSight Appliance Wizard – initial settings. 49
Add eyeSight Appliance Wizard - assign IP addresses 50
Add eyeSight Appliance Wizard – Finish Page 51

Set Up an Enterprise Manager with the Initial Setup Wizard. 51
Set Up an Enterprise Manager with appliance settings. 52

Finish 53

When you are done. 53

Work in the Forescout Console 56

Enable or disable the Forescout Console site map 81
Set up the Forescout Console site map – create site locations 81
Customize display thresholds for Forescout Console site map indicators 83

Customize Forescout Console site map compliant threshold settings. 84
Customize Forescout Console site map cluster size settings. 84
Customize Forescout Console site map cluster grid size settings 85

Forescout Console site map tools 85
Add, remove, and reorganize columns in the Detections pane 88
View the "Best Fit" for columns 90
Sort the columns 90
Export Detections pane data 90
Start actions on selected endpoints. 90
Cancel actions on selected endpoints 91
Add endpoint properties to a list. 92
Additional controls 93

Create policy endpoint exceptions 95

Inventory Discovery rules . . . 96
View and update discovered inventory . . . 97
Detection policies . . . 97
Create lists based on inventory detections . . . 98
Create lists ahead of time . . . 99
View lists and values associated with an asset inventory item . . . 99
Edit and remove lists . . . 99
Use inventory detections to create powerful policies . . . 100
Work with organizational units . . . 100
Work with Forescout Groups . . . 103
Import and export group members . . . 106
Create an ignored IP address list . . . 106
Restricting endpoint inspection . . . 107
Details pane – display more endpoint information . . . 107
Identity Model . . . 110
The Host Details dialog . . . 111
Root cause analysis of endpoint policy match . . . 112
Host Log – investigate endpoint activity . . . 114
Work with the Host Log . . . 116
Work with the Forescout Compliance Center . . . 116

Policy Management . . . 120

Work with Forescout eyeSight policies . . . 121
Quickly access Forescout eyeSight endpoints with troubleshooting issues . . . 127
Stop and start Forescout eyeSight policy Actions . . . 128
The Forescout eyeSight policy manager . . . 128
Create a Forescout eyeSight custom policy . . . 133
Policy naming tips . . . 135
Define policy scope . . . 136
Defining a policy main rule . . . 139
Define Forescout eyeSight policy sub-rules . . . 141
Forescout eyeSight policy main rule advanced options . . . 143
Forescout eyeSight policy sub-rule advanced options . . . 147
Policy preferences . . . 151
Default email settings . . . 161
HTTP login attempts . . . 162
Property lists . . . 163
Categorizing policies . . . 163
Tag sub-rules for dashboard widgets . . . 164
Application issues dashboard tag . . . 164
Policy reports and logs . . . 166
Policy logs . . . 166
Policy safety features . . . 169

Policy templates . . . 178

Create policies using templates – basics . . . 178
Tips for rolling out templates . . . 180
Template structure . . . 180
Windows OS enhanced classification template . . . 181
Primary classification template . . . 181
Classification upgrade impact analysis template . . . 189
Compare classification results . . . 191
Stop the migration classification policy . . . 192
Upgrade the classification version . . . 192
Reclassification template . . . 192
Mobile classification template . . . 200
External device classification template . . . 201
Virtual machine classification template . . . 203
Passive learning mode template . . . 204
Process OS X and Windows endpoints for the NAT / SASE template . . . 206
Corporate/Guest control template . . . 206
Working with guest registration options . . . 209
External disk drive compliance template . . . 211
Overall endpoint compliance template . . . 213
Windows update compliance template . . . 215
Macintosh update compliance template . . . 216
Threats templates . . . 216
Track changes templates . . . 219
New TCP/IP port template . . . 220
Health monitoring templates . . . 220
Health monitoring policies template . . . 221
Appliances policy . . . 223
Appliance load compliance policies . . . 223
Appliance resource utilization policies . . . 223
Appliance policy efficiency policies . . . 224
Plugin health policies . . . 224
Appliance inventory templates . . . 224

Working with policy conditions . . . 226

Working with properties . . . 227
Define a policy condition . . . 227
Detect new vulnerabilities and newly supported vendor applications . . . 229
Define custom conditions . . . 230
Define a comparison condition . . . 231
List of properties by category . . . 233
Defining and managing lists . . . 274
Working with lists . . . 274
Modify lists based on endpoint detections . . . 278
Use your custom lists in policies . . . 279

Working with actions 280
Configure audit trail logging 337
Registration page tab 338
Corporate tab 341
Miscellaneous tab 343
Kill instant messaging 345
Kill peer-to-peer 346
Kill process on Linux and kill process on Macintosh 347
Kill process on Windows 347
Run script on CounterACT 348
Run script on Linux and run script on Macintosh 349
Run script on Windows 351
Set registry key on Windows 353
Start antivirus 354
Start Macintosh updates 355
Start Windows updates 355
Update antivirus 360
Windows self remediation 361

eyeSight Base modules, Content modules, and eyeExtend modules 365
Forescout eyeSight Base modules 365
Content Modules 371
Centralized module management 375
Install a module 375
Plugin configuration management 376
Manage a plugin or component on an individual appliance 376
Check for updates 377
Configure check for updates 378
Roll back to previous module versions 379

Accessing Forescout eyeSight web portals 380
Logging in to Forescout eyeSight web portals 380

Forescout eyeSight dashboards 382
Limit user access to Forescout eyeSight dashboards 383
Forescout eyeSight dashboard layout 384
Forescout eyeSight dashboard prerequisites 386
How to populate Forescout eyeSight dashboards 386
Populate the Forescout eyeSight Health Monitoring dashboard 386
Populate Forescout eyeSight device visibility and compliance dashboards 387
Run the Forescout eyeSight dashboard policies template 388
Out-Of-The-Box (OOTB) Forescout eyeSight dashboards 390
Work with dashboards 403
Add a Forescout eyeSight dashboard to your view 403
Manage Forescout eyeSight dashboards 404
Working with Forescout eyeSight dashboard widgets 406

Add a Forescout eyeSight custom widget . . . 406
Drill down into a Forescout eyeSight widget. . . . 407
Manage Forescout eyeSight widgets . . . 410
Forescout eyeSight widget chart type . . . 411

Assets view . . . 413

Add or remove columns in the Assets view . . . 418
View the details for a device in the Forescout eyeSight Assets view . . . 420
Export Forescout eyeSight device list to CSV file. . . . 422

Generate Forescout eyeSight reports and logs . . . 424

Exporting reports and report event details . . . 437

Assets portal . . . 438

Perform an Assets Portal search . . . 439
Clear events detections. . . . 442

Manage your virtual firewall policy . . . 443

TCP vs. UDP blocking . . . 444
Work with Block and Allow rules . . . 445

Threat protection. . . . 447

Disable the worm slowdown mechanism . . . 455
Customize parameters for each scan type . . . 456
Customize scan recognition criteria. . . . 457
Customize block or monitor response to each bite type . . . 458
Customize bite type values . . . 459
Customize email worm settings . . . 460
Customize email anomaly recognition values . . . 462
Configure the block method . . . 463
Handle service attacks. . . . 464
Set the service attack policy . . . 465
Customize service attack criteria . . . 466
Remove the monitor or block state from a service . . . 468
Manage threat protection mail alert deliveries . . . 469
Manually add an endpoint . . . 470
Managing Manually Added Endpoints . . . 471
Changing the Host State Maintenance Time. . . . 472
Changing the Host State . . . 472
Viewing a History of Manually Added Endpoints and Manual Changes . . . 473
Define the active response range . . . 474
View endpoint activity details . . . 475
Add legitimate traffic rules from the event table. . . . 479
View a summary of event details . . . 479
View event traffic . . . 480

Manage enterprise lockdown alerts . . . 481
Send events to specific appliances . . . 483
Customize the forward all lockdown events policy . . . 483
Legitimate traffic . . . 484
Define legitimate scanning activity – wizard . . . 486
Manually define legitimate scanning applications . . . 487
Manually define removed servers . . . 489
Create customized legitimate traffic rules . . . 490
Define legitimate email traffic . . . 494
Create rules for detected endpoints . . . 495

Threat protection advanced tools . . . 496
Define Mark Rules . . . 497
Define List Rules . . . 500
Define virtual site endpoint Operating System parameters . . . 501
Parse event information displayed in email alerts . . . 502

Manage Forescout eyeSight users . . . 503
Create users and user groups . . . 508
Access to Forescout Console tools permissions . . . 511
Access to Forescout eyeSight network endpoints – scope . . . 514
Default Forescout Console admin user . . . 516
Forescout Console password protection . . . 516
Forescout Console login preferences . . . 519
Forescout Console session handling preferences . . . 520
Forescout Console manual user password change . . . 521
Use Forescout eyeSight smart card authentication . . . 522
Smart card certificate configuration for Forescout eyeSight . . . 523
Smart card advanced settings . . . 524
x.509 digital certificate attributes for Forescout eyeSight . . . 525
Forescout eyeSight and OpenSC . . . 526
Smart card user profile setup . . . 526
External Identity Provider User Authentication . . . 526
Setting Up eyeSight to Work with an External Identity Provider . . . 527
Reset Forescout eyeSight Metadata for an External Identity Provider . . . 529
Monitor Forescout eyeSight user activity . . . 530
View Forescout eyeSight audit trail reports . . . 530

Manage Forescout Licenses . . . 534
Activate a Forescout License . . . 535
Update an Existing License File in the Forescout Console . . . 536
Upload License Requests and Download License Files . . . 537
Deactivate or Revoke a Forescout License . . . 538
Convert a Perpetual License to a Subscription License . . . 539
Receiving license alerts . . . 540

Manage Appliances, Enterprise Managers, and Consoles 541
Define Console Access 542
Multiple Console Logins 543
Define Web Access 544
Disable Web Portals 546
Configure Console Preferences 547
Configure Additional NTP Servers (CLI) 549
Upgrade the Enterprise Manager 550
Upgrade the Console 554
Stop and Start the Enterprise Manager 555
View Forescout Device System Health Information 555
Appliance Capacity 557
Verify the Appliance Fingerprint 558
Update the Appliance Fingerprint 558
Register Appliances with the Enterprise Manager 560
Upgrade one or more Appliances 561
Upgrade the Console 564
Start and Stop Appliances 564
Update Appliance Connection Details 565
Manually Upload the Upgrade File to an Appliance 565
Managing Groups of Appliances 566
Working with Appliance Channel Assignments 568
Add Channels 570
Customize VLAN Tagging Definitions 574
Manually Add a VLAN 576
Console Indicators 577
802.1ad and 802.1QinQ VLAN Tag Termination Traffic 578
Limiting User Access to Appliances 578
Controlling Command-line Access to Devices 579
Enterprise and Appliance Authentication 581

Working with appliance folders 583

Additional Forescout eyeSight options 588
Define endpoint discovery rules 597
Configure a Forescout eyeSight backup server 602
Configure a Forescout eyeSight encryption password 604
Perform a scheduled Forescout eyeSight backup 604
Perform a one - time Forescout eyeSight system backup 606
Back up and restore the Forescout eyeSight site for your appliances 606
Forescout eyeSight backup best practices 607
Localize redirected web pages and messages 607
Display local languages in reports, actions, and other features 608
The Forescout Research program 608

Manage Forescout eyeSight email notifications 610

Property configuration when using TLS to send email alerts/notifications (Option 1) . . 612
Property configuration when using TLS to send email alerts/notifications (Option 2) . . 613

Handle Forescout eyeSight network connectivity failures 615

Remote access to endpoints 616

Use a domain-wide policy 616
Use a Forescout eyeSight administrator group 617
Working with Windows XP SP2 machines 617
Using the security configuration wizard 618
Update group policy objects with new windows firewall settings 618
Test domain credentials 619
Test the credentials on the endpoint using a localhost query 620
Test the credentials in the endpoint using remote query 621
Domain configuration test 621
TCP/IP configuration test 622
Forescout eyeSightport setup test 624
NetBIOS over TCP/IP setup test 624
Services test 624
Shares test 625
Troubleshooting deep inspection 625

Configure HTTP redirection 627

SNMP support and integration 631

Import SNMP Service Settings 632
Export SNMP Service Settings 633
Configure SNMP Views 633
Configure SNMP Users 635
Configure Trap Targets 637
Enable and Disable Forescout eyeSight Traps 637

SNMP MIB for appliances 639

Customizing user interfaces 655

Work with the User Portal Builder 655
The legacy customization tool 655
Create or edit a template 657
Publish a customized template 658
Localize text for HTTP interactions 659

The Certificates pane 660

Import and Configure Trusted Certificates 663
Edit Trusted Certificate Entries 664
Remove Trusted Certificate Entries 666
Generate and Import a Trusted Certificate for Web Portals 666
Import and Configure System Certificates 667

Edit System Certificate Entries 667
Generate a New System Certificate 669
Self Signed Certificates 670
Duplicate System Certificate Entries 670
Export System Certificate Entries 670
Remove System Certificate Entries 670

Security deployment hardening best practices 672
Disable Password Login 675

Regenerating the SSH key 677

Welcome to Forescout eyeSight v9.1.4

Forescout eyeSight (formerly Forescout Platform or CounterAct) is intended for new and experienced users who have logged in to the Console from a Forescout® Enterprise Manager or Appliance. Unless specifically noted, instructions and explanations in the guide refer to both login scenarios.

Refer to in the Forescout eyeSight Installation Guide for information on software installation, post-installation, and other installation procedures for Forescout components, including the Enterprise Manager, Appliance, and Console. However, if you need to upgrade your existing eyeSight to a current release, refer to the Forescout eyeSight Upgrade Guide.

About the Forescout eyeSight

To enhance network security, the eyeSight provides infrastructure and device visibility, policy management, orchestration, and workflow streamlining. The eyeSight provides enterprises with real-time contextual information of devices and users on the network. Policies are defined using this contextual information that helps ensure compliance, remediation, appropriate network access, and streamlining of service operations.

Real-time network visibility

eyeSight eyeSight classifies devices the moment they attempt to access your network. For example:

- Desktops, laptops, and servers
- Mobile devices, such as smartphones, and tablets
- Personal and corporate devices
- On-premises virtual machines and off-premises cloud instances
- Switches, WLAN controllers and access points, devices connecting via VPNs, routers, printers, modems, VoIP phones (including PoE-connected VoIP phones, and devices), WLAN access points, and other network devices
- Peripheral devices, such as USB memory sticks, external disk drives, and webcams
- IoT devices
- Rogue devices

Inspection capabilities resolve an extensive range of information about these devices, for example:

- Desktop and mobile operating system information
- Virtual machine details, for example, VMware Guest Machine health status or Amazon EC2 instance type
- User directory information
- Applications installed and running
- Login and authentication information
- Software patch levels
- Endpoint-connected devices, such as USB drives
- Switch ports to which devices are connected
- Windows registry information

Policy-initiated or manual control

Networks are constantly changing, including the connected device types, software, configurations, compliance requirements, and the internal and external threat landscape. The Console enterprise policies are used to implement the necessary notification, remediation, and restriction controls to secure the network.

Examples of eyeSight product capabilities include:

User Enforcement and Education

- Open trouble tickets
- Send email to users or administrators
- Personalize captive portal messages to notify end users, enforce policy confirmation and allow self-remediation
- Force authentication/password change
- Log-off user, disable user AD account

Application Control and Remediation

- Start/stop applications
- Start/stop peer-to-peer/IM
- Apply updates and patches
- Help ensure antivirus products are up-to-date
- Start/stop processes

Network Restrictions

- Port disable (802.1X, SNMP, CLI)
- VLAN control
- VPN disconnect
- ACL block at switches, firewalls and routers
- Wireless allow/deny
- Quarantine until the device is remediated

Traffic Control

- Virtual firewall
- Update network ACL (switch, router, firewall)

Operating System Control & Remediation

- Patch/hotfix update
- Registry configuration

Device Control

- Disable NIC
- Disable use of peripheral devices

Comprehensive third-party orchestration

eyeSight eyeExtend modules allow information sharing with third-party network, security, mobility and IT management products, allowing for automated workflows, time and cost savings and

enhanced security. This sharing of information can resolve security issues and contain compromised devices. Use the information in this guide to integrate with a variety of third-party systems, for example:

- Advanced Threat Detection systems
- Security Information and Event Management systems
- IT Service Management systems
- Endpoint Protection Platforms/Endpoint Detection and Response systems
- Vulnerability Assessment systems
- Next-Generation Firewall systems
- Almost any third-party product using a web API, SQL or LDAP

When integrating with third-party systems, use the eyeSight tools described in this guide to:

- Trigger third-party remediation and ticketing systems
- Efficiently exchange information with third-party systems
- Mitigate a wide variety of network, security and operational issues
- Extend the network visibility provided by eyeSight eyeSight to third-party systems
- Set up third-party systems to trigger actions on endpoints detected by eyeSight

Integration is carried out by working with eyeSight eyeExtend modules (Extended Modules). See Base Modules, Content Modules, and eyeExtend Modules for details.

On-demand asset intelligence

Use Forescout tools to carry out information sharing and automation among your existing IT security and management systems. These tools help you fix security issues and contain breaches.

View real-time at-a-glance dashboards

The Dashboards view is a web-based information center that provides a real-time overview of the network through both Out-Of-The-Box (OOTB) and user-created dashboard widgets. Dashboards deliver dynamic, at-a-glance information about:

- Device visibility (OOTB)
- Device compliance (OOTB)
- Health monitoring (OOTB)
- Forescout policy data, including custom policies

See Dashboards for more information.

Generate reports

The Reports plugin lets you generate reports showing real-time and trend information about policies, endpoint compliance status, vulnerabilities, device details, assets and network guests. Use reports to keep network administrators, executives, the Help Desk, IT teams, security teams or other enterprise teams well-informed about network activity. Reports can help you understand:

- Long-term network compliance progress and trends
- Immediate security needs
- Compliance with policies
- Status of a specific policy
- Network device statistics

Analyze a real-time network inventory

A live network Asset Inventory view displays current network activity on multiple levels, such as processes and services running, vulnerabilities detected, open ports, or logged in users. Use the Asset Inventory to:

- Broaden your view of the network from endpoint-specific to activity-specific.
- View endpoints that have been detected with specific attributes, whether or not they are policy-compliant.
- Easily track network activity.
- Incorporate inventory detections into policies. For example, if you discover that network guests are running unauthorized processes on your network, create a policy that detects and halts these processes on guest machines.

Work with the assets view

The Assets view, is a web-based search, filter and discovery tool that lets you leverage extensive network and device information collected and correlated by eyeSight products.

eyeSight components

eyeSight devices include Enterprise Manager, Appliance, and Virtual Systems.

Connections between eyeSight devices use fingerprints for verification purposes. When a connection is established, the fingerprints of the two eyeSight devices are compared. If they match, the connection is accepted. This ensures that only trusted eyeSight devices connect with each other.

This includes connections between:

- Enterprise Managers and Appliances
- Enterprise Managers and Recovery Enterprise Managers
- Appliances and other Appliances (Direct Inter-Appliance Communication)

  Refer to the *Enterprise Manager / Appliance Communication Technical Note* for information about Enterprise Manager/Appliance communication.

The appliance

A eyeSight Appliance is a dedicated device that monitors traffic going through your corporate network. It helps protect the network against malicious activity and performs extensive network protection.

Your Appliance should have been installed at your network so that it sees vital network traffic.

To handle malware and intelligent hackers, the Appliance should be set up:

- At the connection point between the Internal Network and the rest of the network. This enables protection of a specific network range against infection and attack attempts initiated from the rest of the network, and network protection against infection attempts generated from a specific network area (for example, contractors segment, which is potentially more dangerous).

- Behind a VPN concentrator, where encrypted VPN channels are decrypted, and malicious traffic enters your network.
- Behind remote access servers, where remote access users enter your network.

To apply an admission control policy, the Appliance should be set up:

- Within broadcast domains, preferably mirroring trunk ports.

To work with the Virtual Firewall, the Appliance should be set up:

- Between segments or VLANs.

Your Appliance may be one of several Appliances included in an Enterprise solution or may be part of a High Availability system. The High Availability feature provides high network uptime utilizing redundancy and automatic recovery.

For more information about the High Availability Pairing feature, refer to the *Forescout eyeSight Resiliency and Recovery User Guide*. For more information about Appliance installation, Appliance specifications and deployment, refer to the *Forescout eyeSight installation Guide*.

The Enterprise Manager

The Enterprise Manager is an aggregation device that communicates with multiple eyeSight Appliances distributed across an enterprise. It manages Appliance activity and policies and collects information about endpoint activity detected at each Appliance. This information can be displayed and reported in the Enterprise Manager.

Your Enterprise Manager may be part of a High Availability system or a remote recovery system. The High Availability feature provides high network uptime utilizing redundancy and automatic recovery. The Recovery Enterprise Manager is used as a remote recovery device for an Enterprise Manager that is no longer functioning due to, for example, a natural disaster or crisis.

Virtual systems

eyeSight virtual devices (Appliances and Enterprise Managers) can be installed and managed in virtual data centers and IT environments. They provide capabilities identical to eyeSight device software installations carried out on dedicated machines.

Refer to the *Forescout eyeSight Installation Guide* for details about installing virtual systems.

Use eyeSight virtual devices to:

- Simplify and ease product distribution and deployment, especially for distributed remote sites.
- Reduce IT costs, space, energy consumption and maintenance by using less hardware.
- Comply with green IT requirements.

Hybrid deployments

Virtual and physical hybrid deployments support.

A physical Enterprise Manager can manage both physical and virtual Appliances, and a virtual Enterprise Manager can manage both physical and virtual Appliances.

Support for endpoints behind NAT/SASE connector

For information about eyeSight - Endpoint Behind NAT/SASE integration and setup, refer to the .

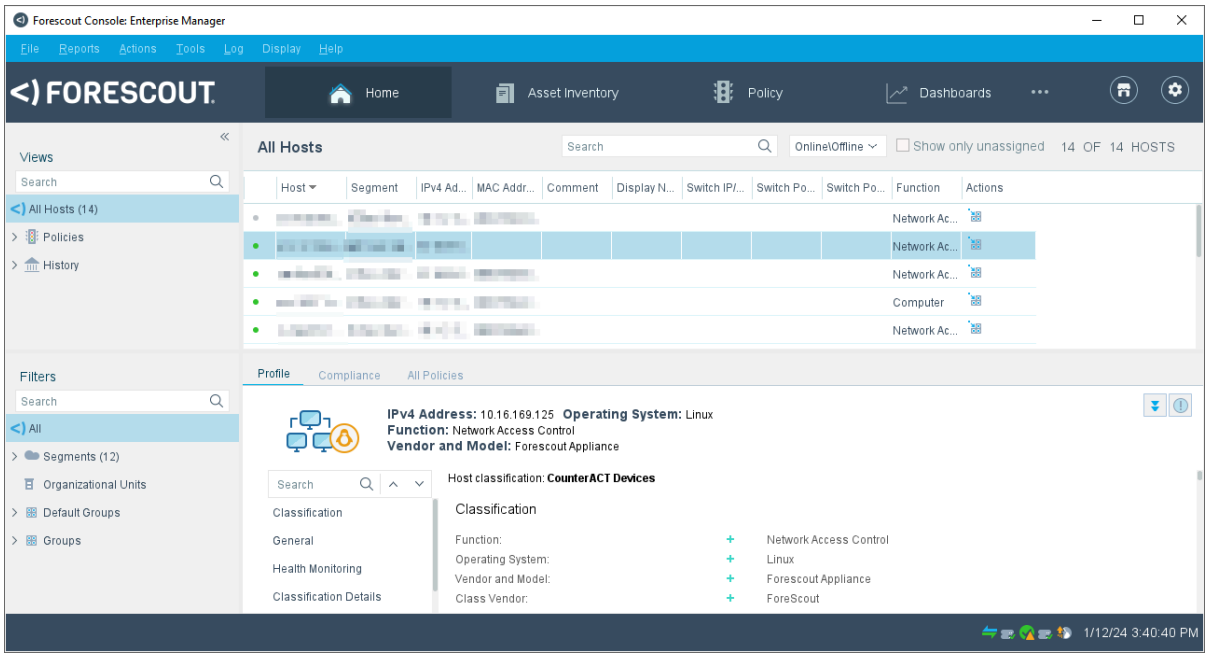
See also the eyeSight Process OS X and Windows Endpoints for NAT/SASE Template

eyeSight User interfaces

eyeSight user interfaces include the Forescout Console and the eyeSight Web Portals.

The Forescout Console

The Forescout Console is the management application used to view important detailed information about endpoints and control them. This information is collected by eyeSight devices.



About the Forescout Console

Detection information is displayed in the Forescout Console, which serves as your unified information, management, and control center.

Key features of the Forescout Console include:

- The Forescout Marketplace is accessible by clicking the Marketplace icon in the upper right-hand corner of the Console.
- An integrated display of endpoints detected by your NAC, Threat Protection, Compliance, and Corporate/Guest Control policies, as well as other endpoints discovered by eyeSight eyeSight.
- Display of extensive endpoint details, such as MAC address, IP address, domain, and NetBIOS machine information; related user information, such as mail addresses and

telephone numbers, as well as the machine block or release status.
- A live network inventory view that displays network activity at multiple levels, for example, processes and services running, detected vulnerabilities, open ports, or logged in users.
- A site map, powered by Google Maps, that provides at-a-glance, real-time corporate and guest status information, compliance levels, security alerts, and more—across offices, cities, countries, and continents.
- Powerful command options that let you manually and automatically remediate, and control detected endpoints and communicate with endpoint users.
- Sophisticated reporting tools let you generate an extensive range of reports that detail and summarize important network activity, asset and inventory information, NAC policy activity, vulnerability scanning and more, as well as the Forescout eyeSight's response to these activities.
- Control tools let you start and stop eyeSight devices and update the configuration defined during installation, for example, the network range protected by Forescout products or the time zone setting. Other control tools let you communicate with your network management application and work with third-party applications.

Forescout eyeSight web portals

Forescout offers additional features that can be accessed via browser-based portals.

Key features of the Forescout Web Portals include:

- Forescout Web Client:
  - Dashboards: Provides a real-time overview of the network and delivers dynamic at-a-glance information about device visibility and compliance. See Dashboards for details.
  - Assets View: Allows you to view, search and filter devices detected by eyeSight eyeSight. See Assets View for details.
  - eyeSegment Application (Segmentation): Allows you to monitor and analyze your physical network traffic from a dynamic zone perspective. Refer to the *eyeSight eyeSegment Application How-to Guide* for details.
- User Portal Builder: Allows you to create, duplicate, preview or export/import customized Guest Management Portal and HTTP pages. See The Forescout User Portal Builder for details.
- Reports Portal: Allows you to generate comprehensive real-time and trend information about policies, vulnerabilities and the network inventory. See Generating Reports and Logs for details.
- Assets Portal: Displays endpoint information, policy violations, login information, User Directory details, organizational mapping details, and endpoint device connections. See Assets Portal for details.

  Note:

  Other portals may be available depending on your license. When running in Certification Compliance mode, the Reports and Assets portals are disabled.

Forescout eyeSight help tools

The Forescout Console provides a range of Help tools to assist first-time users in gaining proficiency and an understanding of the Console.

Help tools also guide veteran users in working with more advanced Forescout Console options. This topic describes the available help tools and how to access them.

Forescout documentation portal

The Forescout Documentation Portal is an intelligent content delivery platform that provides you with a wide range of technical content in one centralized location.

The Forescout Documentation Portal offers unique features that help you fully engage with content:

- Create and share personalized collections of content with My Docs
- Personalize search results to match your preferences
- Watch topics that interest you to get notified when something changes

You can access the portal at: https://docs.forescout.com/

Forescout Console help buttons

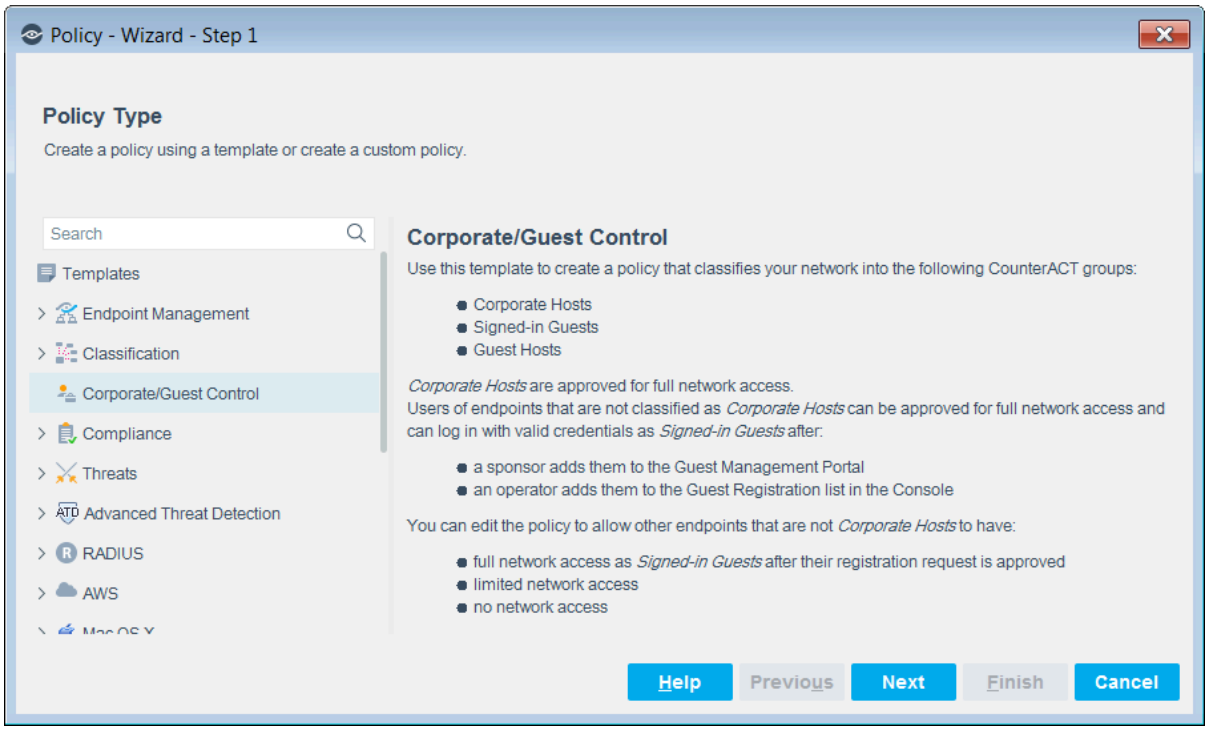
You can quickly access specific information about the tasks and topics by using the Help buttons that appear in Forescout eyeSight dialog boxes, panes, and wizard panes.

Forescout eyeSight Administration Guide help

Select Help > Administration Guide to open the *Forescout eyeSight Administration Guide*.

Forescout Console feature dialog box descriptions

Forescout dialog boxes are designed to automatically display helpful descriptions about various Forescout Console features. For example:



Forescout Console on-screen troubleshooting

Two types of on-screen troubleshooting are available.

Troubleshooting messages

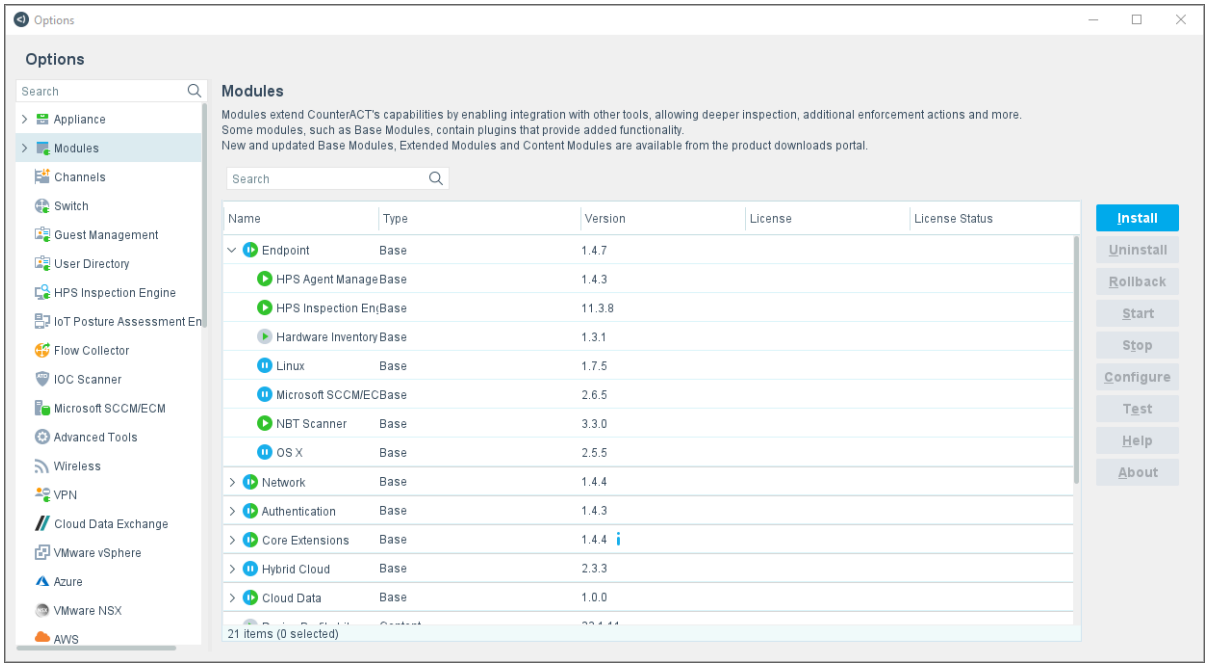
Troubleshooting messages about various issues, failed actions, and other errors can be viewed in the Detections pane for a selected endpoint. Information is also available about resolving these issues. To view troubleshooting tips in the Details pane, select the information icon at the top right corner of the pane, or select the Details link in any tab.

Troubleshooting endpoint policy matches

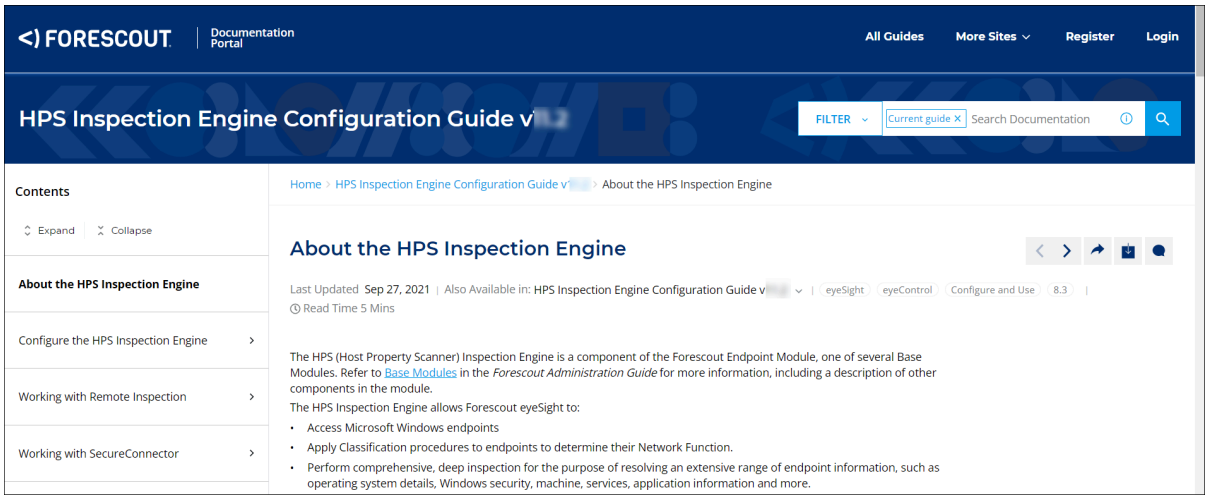
You can quickly troubleshoot an endpoint policy match by viewing member-of-group assignments per policy. This information is presented in a diagram accessed from the tab for each endpoint detected. This is useful if you want to investigate why a certain action, such as Assign to VLAN, was applied to an endpoint. See Root Cause Analysis of Endpoint Policy Match for details.

Plugin/module configuration help

When configuring a eyeSight component, access its configuration guide (Help) directly from the Console Modules pane. Select a plugin or a module and then select Help. Doing so, opens the Forescout Documentation Portal in a web browser page that displays the requested component configuration guide.



For example, selecting Endpoint > HPS Inspection Engine, and then selecting Help, presents the following in a web browser page:



Log In to the Forescout Console

You can manage eyeSight devices via the Forescout Console after the device IP address/FQDN and user login credentials that you provide are verified. Make sure that you have this information before attempting to log in.

Note:
It is not recommended to run the Forescout Console using the Windows 10 built-in administrator account, as it prevents the use of certain Console functionality.

To log in:

1. Select Start > Forescout > Console.

2. Enter the eyeSight device IP address or FQDN in the IP/Name field.
3. From the Login Method drop-down, select a login method:
    - Password for standard authentication
    - Smart Card for authentication using a connected Smart Card

    Note:
    If the Smart Card contains more than one certificate, select the certificate for this eyeSight device.
4. If you selected Password, enter the Console User Name and Password, and skip to Step 6.
5. If you selected Smart Card:
    a. Select the PIN Prompt By method from the drop-down menu:
        - **Smart Card Middleware:** Select when your system uses activClient middleware. You will be prompted to provide a PIN to access the certificates for this Smart Card. If your system uses OpenSC middleware, and you select Smart Card Middleware as your PIN prompt method, the login will fail.

- **Forescout Console:** Select when your system uses OpenSC middleware. You will be prompted to provide a PIN to access the certificates for this Smart Card. If your system uses activClient middleware, and you select Forescout Console as the PIN prompt method, you will be prompted to provide the PIN twice, and then the login process will proceed.

b. If the Dll Location is empty, enter the location where the Smart Card driver is installed on the computer. To use OpenSC, select the `opensc_pkcs11.dll` located in `installdirectory\OpenSC\x86` or `installdirectory\OpenSC\x64`. See OpenSC for more information.
c. If there are multiple Smart Cards connected to the Smart Card reader, the Select a Smart Card window opens after you click Log In. Select the desired Smart Card, and then click OK.
d. If there are multiple certificates associated with the Smart Card, the Select a Certificate window opens. Select the appropriate certificate, and then click OK.

Note:
It is recommended to log on once as the admin after installing the Console to automatically update the JRE before allowing Smart Card authentication.

6. Select Remember this address and user name to automatically fill in this information when you next attempt to log in.
7. Select Log In.

Note:
A window may open displaying terms and conditions. To continue working, read and accept the terms. The login process continues.

8. If two-factor authentication is required, complete the Security Verification requirements and then select Verify.

eyeSight device verification

How to connect to a secured eyeSight device when you log into the Console for the first time.

When logging in to the Console for the first time, you are prompted to verify that you are connecting to a trusted eyeSight device. To do this, compare the output of a eyeSight CLI command with the string that appears in the dialog box. This ensures that you are logging in to a secured Forescout component with protected Console credentials.

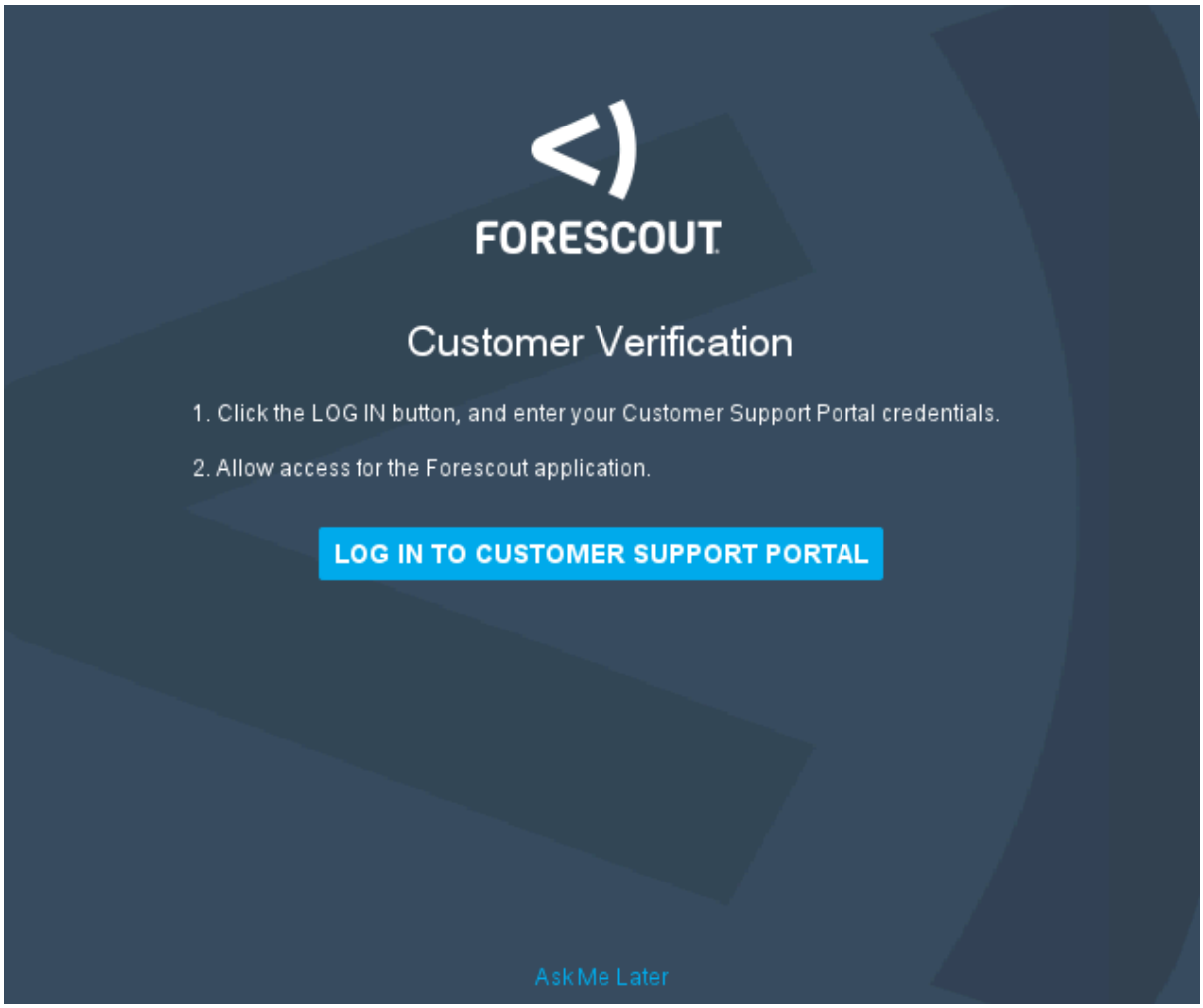
Select Yes to proceed with login only after you have followed the instructions and completed the verification process.

To verify the device:

1. Log in to the eyeSight device through the command-line interface (CLI).
2. Run the command `fingerprintkey`. (In the Bash shell, run `fstool key` instead. Refer to the *Forescout eyeSight CLI Commands Reference Guide* for more information).
3. Verify that the output of the command matches the value displayed in the Login dialog box, and select Yes.

Forescout eyeSight customer verification

If customer verification has not yet been completed, you might be prompted to complete the customer verification process.



To verify the customer:

1. If you do not know your customer credentials for the Forescout Customer Support Portal, or if there is no internet connectivity, select Ask Me Later.
2. Select the LOG IN button. The Customer Support Portal opens.
3. Enter your Customer Support Portal credentials.
   Note:
   These are not the credentials you use to log into the Console.
4. In the Allow Access window, select Allow to allow the eyeSight to securely send endpoint and system information from Appliances in your deployment to The Forescout Research Program. This program helps Forescout improve the security platform effectiveness in the long term.
5. You can log out of the Customer Support Portal.

Last Forescout Console login confirmation

When the Forescout Login dialog box opens, review the following last login information for your account:

- The user name and IP address of your current login session
- The time and IP address of this user's previous successful login

- The number of this user's recent, consecutive login attempts that failed

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

Exit the Forescout Console

When you exit the Console, eyeSight continues to protect your network. System and user events that occurred during logout can be viewed. See Generating Reports and Logs for details.

To exit the Console, select File>Exit.

Forgot Your Forescout Console password?

What to do if you forget your password.

Contact your System Administrator or another user authorized to change your password.

Reset a Forescout Console admin password

Only the admin user has permissions to change the admin password at the Forescout Console. If the admin password is forgotten, it must be updated by a user with `cliadmin` privileges using the `fstool passwd --reset` command.

Forescout Console access only cliadmin_console user

The Forescout Console access only `cliadmin_console` user can be used to recover locked out users.

Since all local CLI users are subject to authentication lockout, it could lead to a situation where all users, including `cliadmin`, are locked out of the system. The `cliadmin_console` user is not subject to authentication lockout and can be used to recover other users or admins that are locked out. The `cliadmin_console` user has the following unique characteristics:

- To utilize this feature, the `cliadmin` user manually creates the Console access only `cliadmin_console` user.
- Once created, no one can delete the `cliadmin_console` user.
- The `cliadmin_console` user's privileges cannot be changed, although its password can.
- The `cliadmin_console` user cannot remotely log in to the Enterprise Manager or Appliance via SSH.
- The `cliadmin_console` user can only log in to the Enterprise Manager or Appliance via the Console as a local user.

Create the Forescout Console access only cliadmin_console user

To create the `cliadmin_console` user:

1. Log in to the Appliance CLI as cliadmin.
2. Run the following command: `fstool user add-console-cliadmin`
3. Enter the password for `cliadmin`.
4. When prompted, enter a password for the `cliadmin_console` user.
   The following message is displayed:

   ```
   User cliadmin_console was successfully added
   ```

Work with the Forescout eyeSight Initial Setup Wizard

The Initial Setup Wizard guides you through important configuration steps to ensure that eyeSight devices are set up quickly and efficiently. The wizard opens automatically when you log in to eyeSight for the first time.

In the Initial Setup Wizard:

1. Review the Before You Begin section.
2. Log in to the Console. See Log In to the Console.
3. Run the Initial Setup Wizard. See Set Up an Appliance with the Initial Setup Wizard.
4. Review the When You Are Done section for information regarding additional basic setup tasks.

Before running the Forescout eyeSight Initial Setup Wizard

Before accessing the Forescout eyeSight Initial Setup Wizard, prepare information about the eyeSight device that you need to configure:

Prepare the following information about the device:

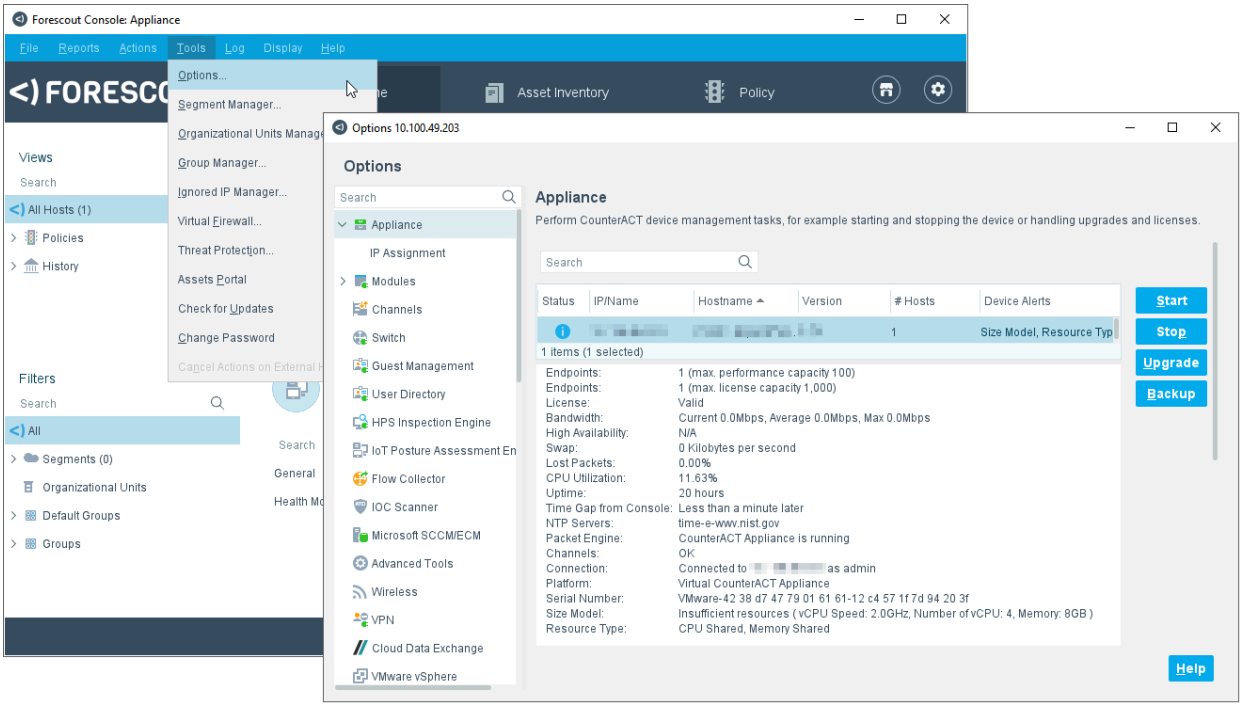
- NTP server address used by your organization.
- Internal mail relay IP address. This allows delivery of email alerts if SMTP traffic is not allowed from the Appliance.
- Forescout Administrator's email address.
- Monitor and response interfaces assignments defined in the Data Center. The monitor interface tracks traffic going through your network. The response interface is used to protect against malicious activity, carrying out Virtual Firewall blocking and HTTP redirection. This information is not required for Enterprise Manager setup.
- For segments or VLANs with no DHCP, the network segment or VLANs to which the monitoring interface is directly connected and a permanent IP address to be used by Forescout products at each such VLAN. This information is not required for Enterprise Manager setup.
- IP address ranges that the Appliance will protect (all the internal addresses, including unused addresses).
- User Directory account information and the User Directory server IP address.
- Domain credentials, including domain administrative account name and password.
- Authentication servers so that Forescout eyeControl can analyze which endpoints have successfully authenticated.
- Core switch IP address, vendor, and SNMP parameters.
- IP address ranges of endpoints known to be sensitive to network probing.

  This information may be tested before it is saved by the wizard at each stage of the setup. A verification message is displayed, indicating if the settings are valid.

Update Forescout eyeSight Initial Setup Wizard settings

The Initial Setup Wizard has options that you can modify.

Most of the options defined in the Initial Setup Wizard can be modified from the Forescout Console Options window (Tools > Options).



Set Up an appliance with the Forescout eyeSight Initial Setup Wizard

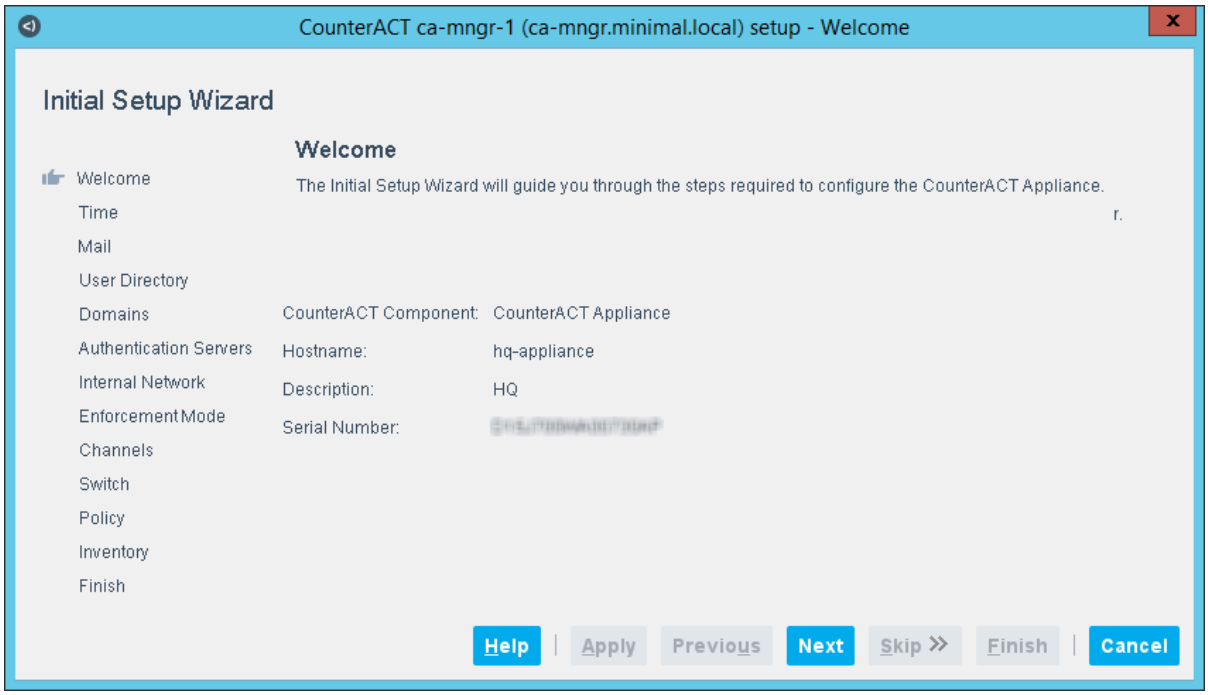
When you log in to the Forescout Console for the first time, the Initial Setup wizard appears.

Forescout eyeSight Initial Setup Wizard – Welcome

The Welcome pane is the first pane in the Initial Setup Wizard for a eyeSight component..

The Welcome pane displays the eyeSight component to which you logged in, as well as information you defined during the installation in the Data Center. More Appliance information can be viewed in the Forescout Options window.

Select Next to start the Initial Setup Wizard.



Forescout eyeSight Initial Setup Wizard – License (Virtual Systems Only, Per-Appliance Licensing Mode)

The License pane of the Initial Setup Wizard appears only for a eyeSight virtual system operating in Per-Appliance Licensing

The virtual license feature is designed to meet the needs of users working in Virtual IT environments, including environments that require a proxy server. These features ensure that such users are working with authorized, secure, and protected licenses.

Note:
Refer to the *Forescout eyeSight Installation Guide* for information about installing Forescout virtual systems.

In the License pane, you can install the virtual demo license provided by your Forescout representative by email. This license is valid for 30 days from the time it was generated by the Forescout representative. When you install the license, the license expiration date is indicated. You must request and install a permanent license before this period expires. See Virtual Licenses for details.

You will be contacted via email regarding the license expiration date and any license violations. In addition, license alerts, violations, status and troubleshooting information can be accessed from the Appliance, Details pane. See View License Alerts for details.

Virtual licenses are authenticated daily by the Forescout License Server (at https://license2.forescout.com). Licenses that cannot be authenticated for a month are revoked and significant Forescout functionality stops. See Virtual Licenses for information about working with the License Server.

When working with the initial demo license, you can select any license file for any device, provided that a specific license file is installed on one device only. (If you use the same license file for more

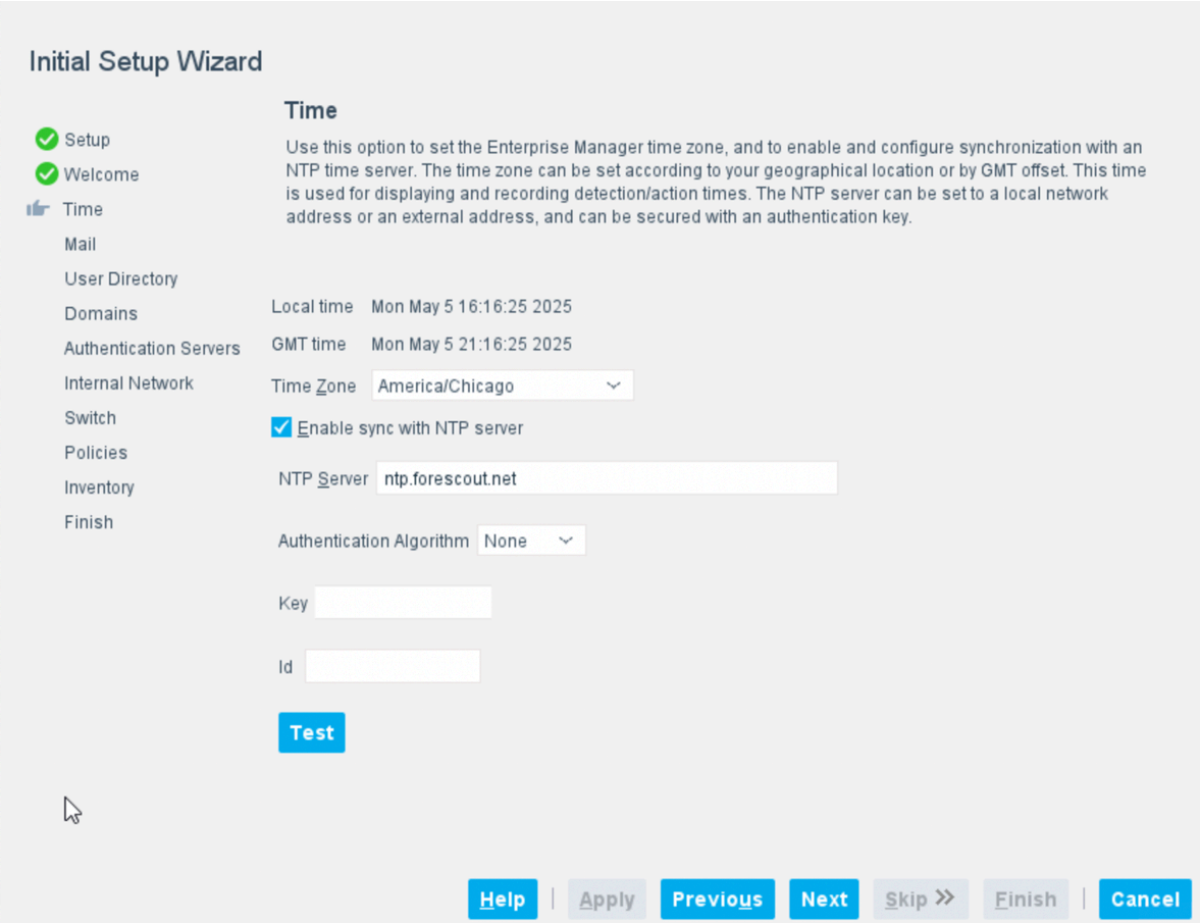
than one device, the license may be revoked. Moreover, you will be unable to add an Appliance to the Enterprise Manager if an Appliance with the same license is already connected.) You can rename the file if required. Extended demo licenses and permanent licenses are intended for a specific device.

Install License	Browse to and select the license file and then select OK. The Install License from File dialog box opens. Select the device and then select Install. A dialog box displays information about the start and end date for installing the license, as well as other license information. If the End User License Agreement opens, accept it.

Forescout eyeSight Initial Setup Wizard – Time

Use the Time pane of the Initial Setup Wizard for time zone NTP time server synchronization settings.

Note:
The NTP time server settings can be modified after the initial setup by selecting Tools > Options > General > Time in the Console. See Configure NTP Server Synchronization.



Time Zone	Set the time zone according to your geographical location or by GMT offset. The default value is the time zone of the Appliance. This time zone is used when displaying and recording detection times in the Console.
Enable sync with NTP server	Enables synchronizing the system clock with an NTP time server. When enabled, lets you set NTP server addresses, and to enter their authentication key strings (SHA-1). Enabled by default.
NTP Server	eyeSight devices require NTP connectivity (port 123 UDP) to an NTP server. Enter an NTP server that your organization connects to or use the eyeSight default server (`ntp.forescout.net`). In the Key field, enter the SHA1 key string used for authentication of the NTP server connection. (Optional but recommended). Select Test to test the availability of the NTP server. If the test fails, contact your IT professional.

You can add additional NTP servers after installation is complete. See Configure NTP Server Synchronization.

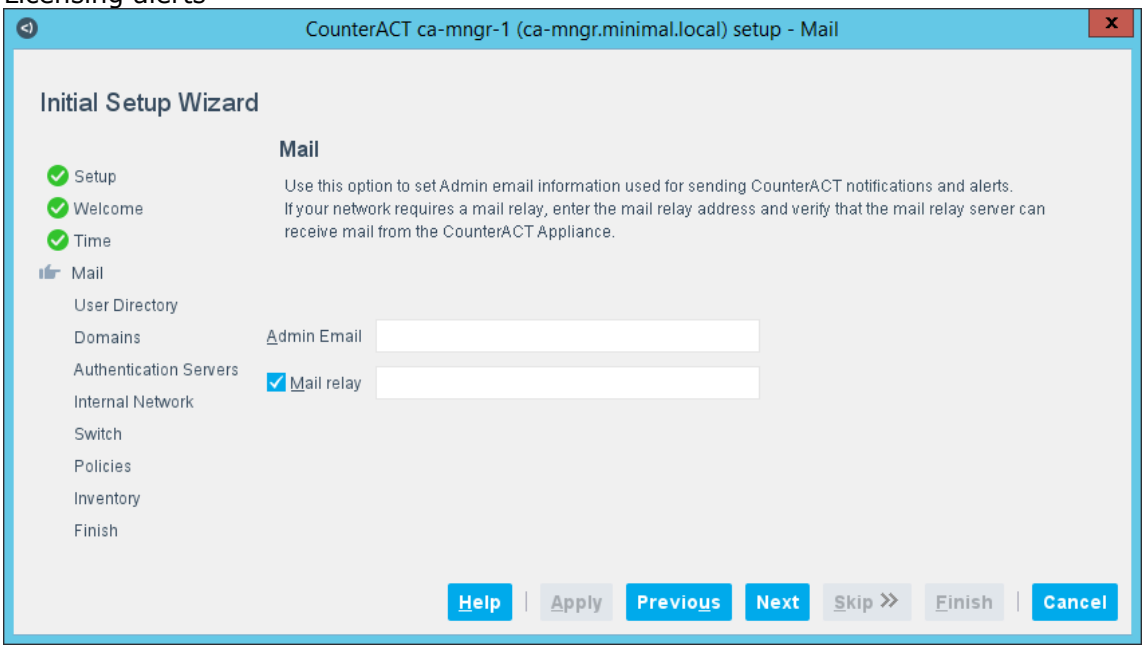
You can define NTP servers for individual Appliances, see Configure Additional NTP Servers

Forescout eyeSight Initial Setup Wizard – Mail

In the Mail pane, you can define the Mail relay and the Admin email addresses.

eyeSight eyeSight generates email messages for:

- Policy and Threat Protection alerts
- Scheduled reports
- Critical system operation alerts
- Licensing alerts



Admin Email (Required)

Forescout Administrator email address(es) or another address that should receive the email alerts / notifications, which are generated by eyeSight eyeSight alerts. Separate multiple addresses by commas, spaces or semicolons.

Example 1: admin@company.com

Example 2: admin@company.com, deputy@company.com

You can sign these emails using a digital certificate, as specified by the

	Secure / Multipurpose Internet Mail Extensions (S / MIME) standard. See Signing Emails with an S/MIME Certificate for details.
Mail Relay	The internal mail relay IP address to allow delivery of email alerts if SMTP traffic (port 25) is not allowed from the Forescout platform to the Internet. This must be the fully qualified host name. For example, mail-relay.example.com. If you enter an incorrect address you will not receive alerts.

You can update all the options that the eyeSight SMTP mail server uses to send its email alerts/notifications, including using SMTP user name / password authentication with TLS (secure communication). See Managing Email Notifications.

Forescout eyeSight Initial Setup Wizard – User Directory

Use the User Directory pane of the Initial Setup Wizard to define the credentials for a User Directory server.

You can define User Directory credentials to validate network authentication and resolve user details. For example, endpoint User Directory display name, department name, or email address.

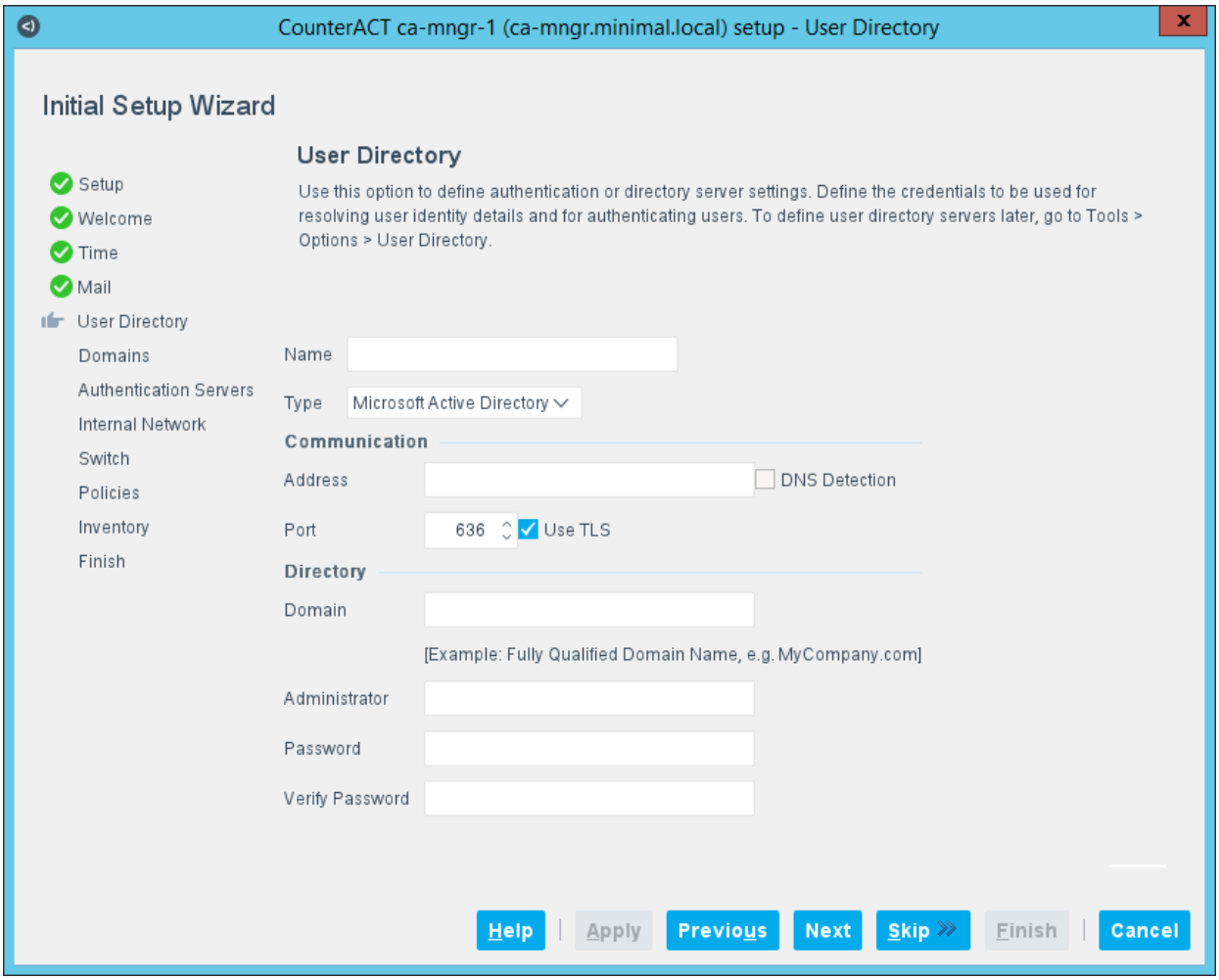
You can define various types of User Directory servers. The following user directory and authentication servers are supported:

- Microsoft Active Directory
- Novell eDirectory
- Oracle Directory
- IBM Lotus Notes
- OpenLDAP Server
- RADIUS
- TACACS

You can work with more than one server type simultaneously. For example, if your organization uses Microsoft Active Directory for retrieving user details and a RADIUS server for verifying authentication, you can configure the plugin to work with both these server types.

Note:
You cannot configure RADIUS or TACACS authentication servers in the Initial Setup Wizard.

You can define additional User Directory servers from the Forescout Console Options window by selecting User Directory, and then selecting Add.



Setup requires a User Directory server that can be queried to validate authentication and obtain details regarding users at detected endpoints. Configure the following settings in the User Directory pane:

Name	Enter the hostname of the server. *Note: This value cannot be edited later.*
Type	Select a server type: Microsoft Active Directory Novell eDirectory Oracle Directory

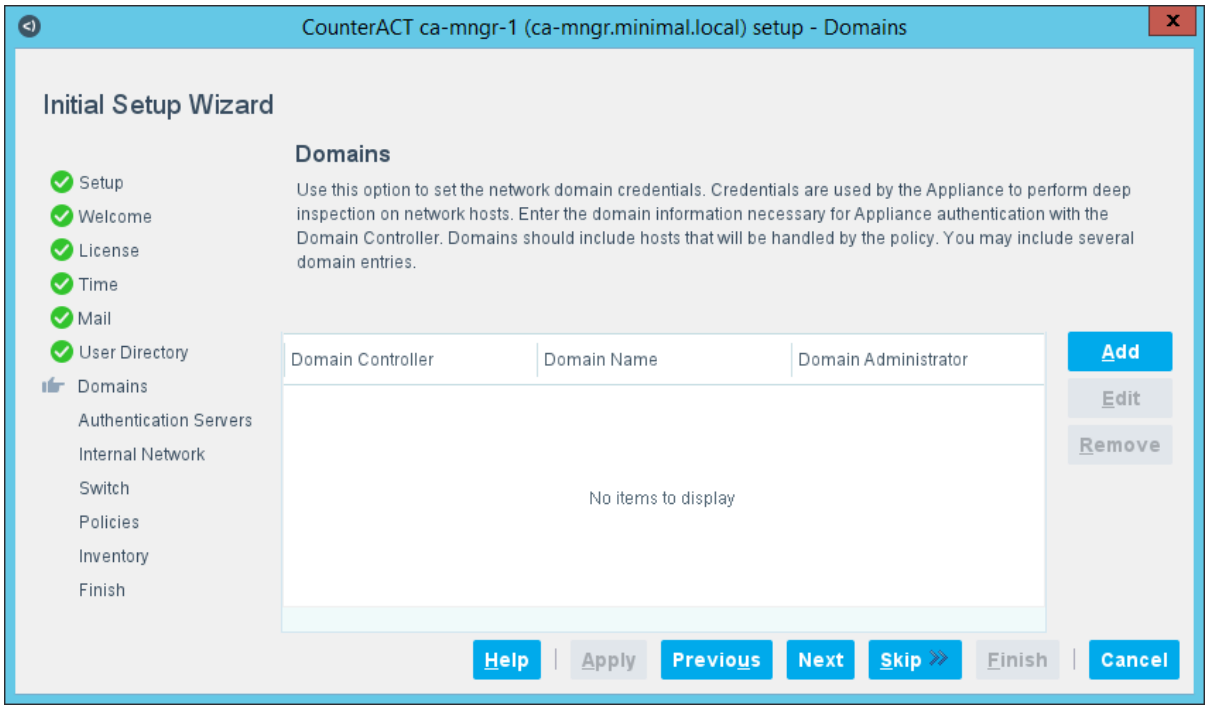
	IBM Lotus Notes OpenLDAP Server **Note:** This value cannot be edited later.
Address/DNS Detection	Do one of the following: Enter the remote address of the server, such as an IP address, an FQDN address string, or an IPv6 address string. For server types other than Microsoft Active Directory, this is the only option. Select DNS Detection to instruct the eyeSight to learn directory servers based on the domain name configured in the Directory section, Domain field. This option applies to Microsoft Active Directory servers only. For more information, refer to the *User Directory Plugin Configuration Guide*.
Port	Enter the server port in the Port field. The default port for servers used as directories to retrieve user information is 636.
Use TLS	For some server types, you can instruct the eyeSight to use TLS to encrypt communication with the User Directory server. By default, Use TLS is enabled. Ensure that TLS communication is supported and enabled on servers used as directories to retrieve user information. The User Directory Plugin can communicate with servers that support TLS 1.1 or TLS 1.2. It cannot communicate with servers that support TLS 1.0 only.

After User Directory server setup, you can view and edit the existing User Directory server configuration by selecting Tools > Options > User Directory in the Console. User details and authentication status are displayed in the Detections pane. For more information about User Directory server setup, refer to the *User Directory Plugin Configuration Guide*. .

Forescout eyeSight Initial Setup Wizard – Domains

Use the Domain Credentials pane of the Initial Setup Wizard to set up network domain credentials that the Appliance uses to perform deep inspection on endpoints.

In the Domains pane, enter the domain information necessary for the Appliance to authenticate with the Domain Controller. Domains should include endpoints that are handled by your policies. You may include several domain entries.



In the Domains pane, select Add, and define the following:

Domain Controller	The Domain Controller IP address. This information is used to test password validity and provide defaults for the authentication servers defined later.
Domain Name	The domain name. The domain should include all endpoints that you want to inspect via the policy. Endpoints in this domain must also be in the Internal Network.
User	The domain administrator name for this domain.
Password	The domain administrator password for this domain.

Note:
Additional domain options let you fine-tune certain inspection process definitions a perform tests. Refer to Configure the HPS Inspection Engine in the HPS IE Configuration Guide.

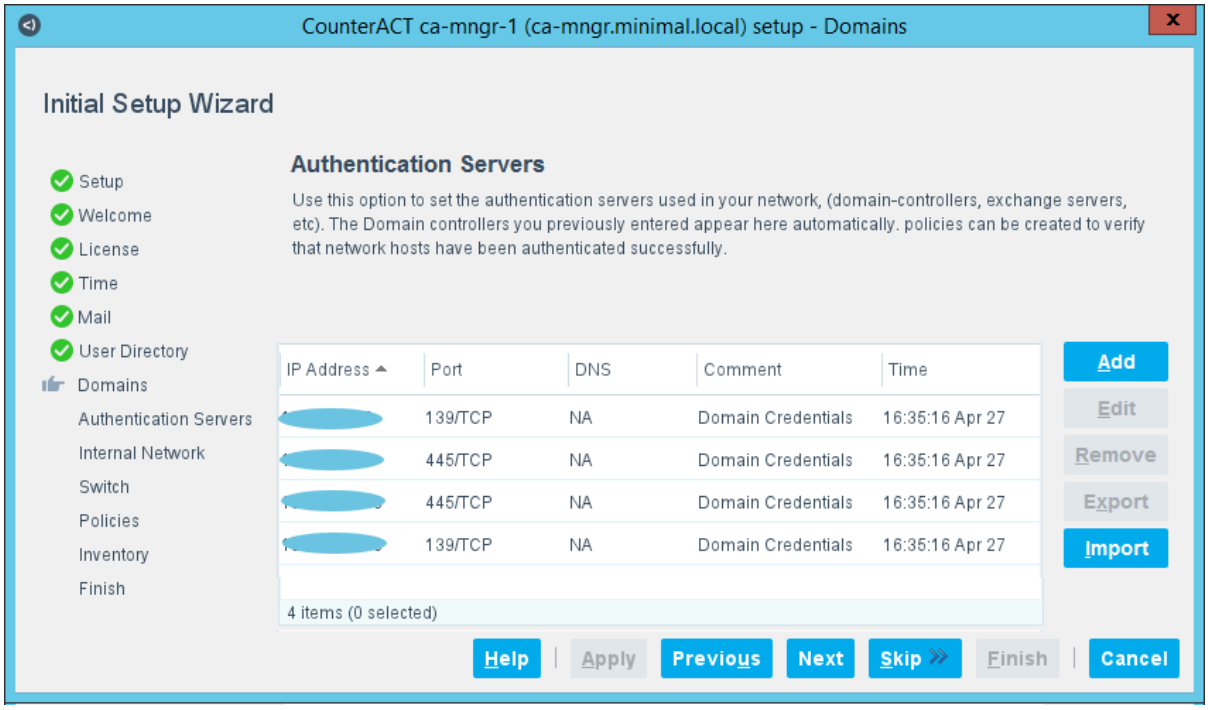
If the verification test fails, you may need to perform troubleshooting tasks. See Remote Access to Endpoints for details.

Forescout eyeSight Initial Setup Wizard – Authentication Servers

Use the Authentication Servers pane in the Initial Setup Wizard to define your authentication servers.

Policies can be created to verify that endpoints have authenticated successfully.

In the Authentication Servers pane, define the authentication servers used in your network (such as domain controllers or exchange servers). Any previously entered domain controllers appear here automatically.



In the Authentication Servers pane, select Add, and define authentication servers.

The following authentication services are supported:

- HTTP (80/TCP)
- Telnet (23/TCP)
- NetBIOS-SSN (139/TCP)
- Microsoft-DS (445/TCP)
- Microsoft-MAPI (135/TCP)
- FTP (21/TCP)
- IMAP(143/TCP)
- POP3(110/TCP)
- rlogin (513/TCP)

Forescout eyeSight Initial Setup Wizard – Internal Network

Use the Internal Network pane in the Initial Setup Wizard to define your network segments or IP ranges.

The Internal Network is a set of network segments or IP ranges that defines your network in the eyeSight. When eyeSight eyeSight detects endpoints with IP addresses within the Internal Network, they are assumed to be in your network.

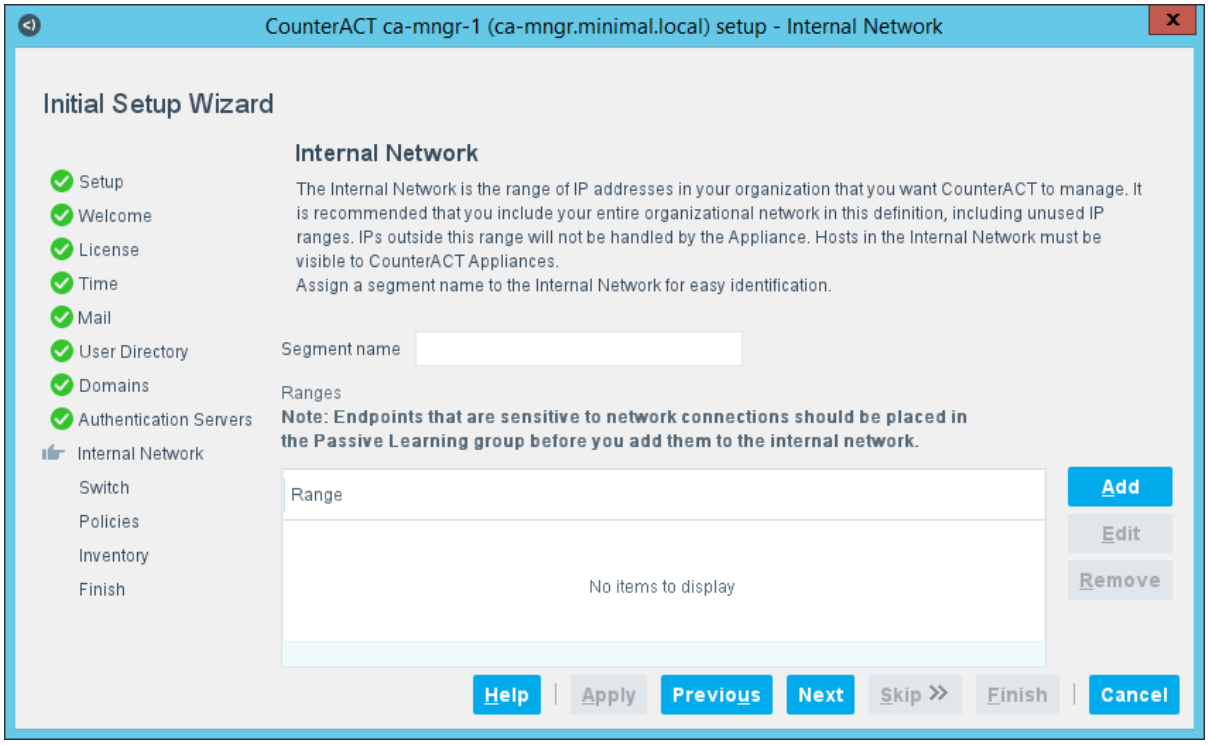
The Internal Network defines the extent of eyeSight management activity. For example, when a Forescout policy scope is defined as "All IPs," the policy is applied to all IP addresses in the

Internal Network. Network segments that are part of your physical network, but are not included in the Internal Network definition, are not managed by Forescout products. In addition, endpoints in the Internal Network must be visible to Forescout Appliances.

The Internal Network is defined in the Console as a set of named IP ranges. Typically, these ranges correspond to logical segments of your network.

Several Forescout tools use these Internal Network segments. For example, you use these segments to assign sectors of your network to Appliances, to define the scope of a policy, and to define the active response range for Threat Protection features.

Segments you define during setup can be fine-tuned to more closely represent the structure of your corporate network, and you can add additional segments later. See Working with Forescout Segments for details.



In the Internal Network pane, select Add to define IP ranges or subnets. The Segment name field is mandatory.

Forescout eyeSight Initial Setup Wizard – Enforcement Mode

Use the Enforcement Mode pane in the Initial Setup Wizard to monitor network traffic.

Full Enforcement	Select this enforcement mode to enable complete functionality
Partial Enforcement	When this enforcement mode is selected, the Appliance can fully monitor network traffic, but has limited ability to respond to it. The Threat Protection, HTTP Actions, and Virtual Firewall options are disabled. This mode is recommended for evaluation purposes only.

	The Partial Enforcement Mode icon is displayed on the status bar if your system is set to this mode.
NAT Detection	Enable this option to detect devices behind NAT (Network Address Translation) servers.
Auto Discovery	When this option is selected eyeSight, eyeSight resolves and displays endpoint properties, such as NetBIOS names, Nmap and domain information. See Endpoint Discovery Rules for details.

Forescout eyeSight Initial Setup Wizard – Channels

Use the Channels pane in the Initial Setup Wizard to define the channel monitor-response interface pairs that the Appliance needs to protect your network.

A channel defines a pair of interfaces used by the Appliance to protect your network.

In general, one interface monitors traffic going through the network (monitor interface). The other interface generates traffic back into the network (response interface). Response traffic is used to:

- Protect against self-propagating malware, worms and hackers.
- Carry out Virtual Firewall blocking.
- Perform policy actions. These actions may include, for example, redirecting web browsers or blocking access to the Internet.

A single interface may also be used as both the monitoring and the response interface.

The monitoring and response interfaces and the appropriate physical connections in the Data Center should be defined when installing the Appliance and connecting it to the network switch. If the definition is later changed, an Appliance reboot is required.

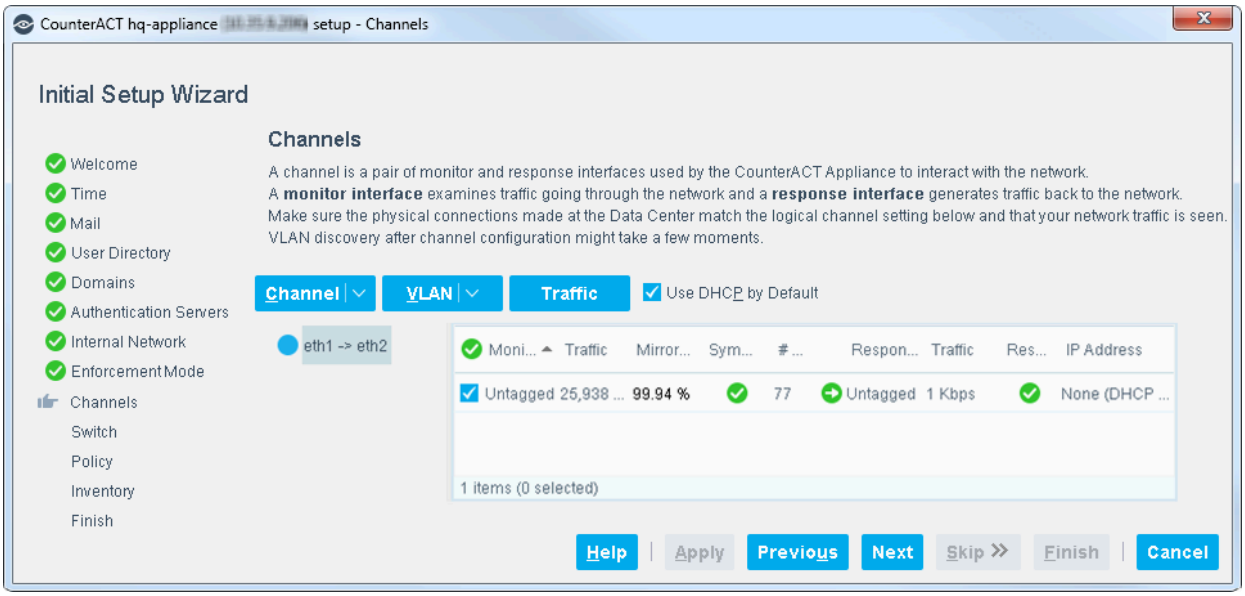
For optimal performance, we recommend to:

- Configure one or two 10G monitor ports in each physical Appliance that monitors traffic.
- When an Appliance uses more than two monitor ports:
  - Ensure that an even number of monitor ports is used.
  - Do not mix interface types, such as a 1Gb network adapter together with a 10Gb network adapter.

For additional performance optimization recommendations, refer to the *Packet Engine Configuration Guide*.

Completing interface assignments made in the Data Center

If you change the monitoring interface assignment in the Channels pane, you must go back to the Data Center and readjust the physical interface connections so that they match.



If your network architecture is set up to work with VLANs, the Appliance automatically detects them. These VLANs are listed in the Channels pane.

Status Indicators

An indicator is displayed on the Console status bar if:

- There is a connectivity problem on an enabled VLAN or interface.
- No channels are enabled.
- A new VLAN is discovered by the Appliance.

Note:
A tooltip provides details about the event.

The Channels pane contains the following options:

Enabled	Activates the channel configuration. Select this option for each VLAN that you want to activate. Monitoring and response activity do not take place until you select Apply from the Channels pane.

Monitor Interface Information

Monitor VLAN	Displays all VLAN IDs discovered for the selected monitor interface. If you defined a channel that works with an IP layer, that VLAN is displayed as IP LAYER.

Traffic	Displays total VLAN traffic detected on the monitor interface.
Mirrored Traffic	Displays the percentage of mirrored traffic from the total VLAN traffic.
Symmetric	Indicates whether the interfaces passed the Symmetric Traffic test. The test verifies that the Appliance can see symmetric traffic on the monitoring interfaces. That is, for every TCP conversation, both incoming and outgoing traffic is visible. If this condition is detected, traffic received on the channel is ignored until the condition has cleared. The test runs continually. If the test fails, you can review related troubleshooting information at the bottom of the Channels pane.
# Hosts	Displays the total number of endpoints monitored on the VLAN.

Response Interface Information

Response VLAN	Displays all VLAN IDs discovered for the selected response interface.
Traffic	Displays total VLAN traffic detected on the response interface.
Response	Indicates whether the Response Traffic test succeeded on the VLAN. The test verifies that the Appliance successfully sends response traffic to the network. The test runs continually. If the test fails, you can review related troubleshooting information at the bottom of the Channels pane.
IP Address	Displays the DHCP address used by the Appliance for response traffic. By default, the IP address is acquired through DHCP. If the DHCP is not successful, the eyeSight cannot respond to ARP requests. In this case, manually define the address. Addresses are defined per VLAN, if required. See Manually Add a VLAN for details.

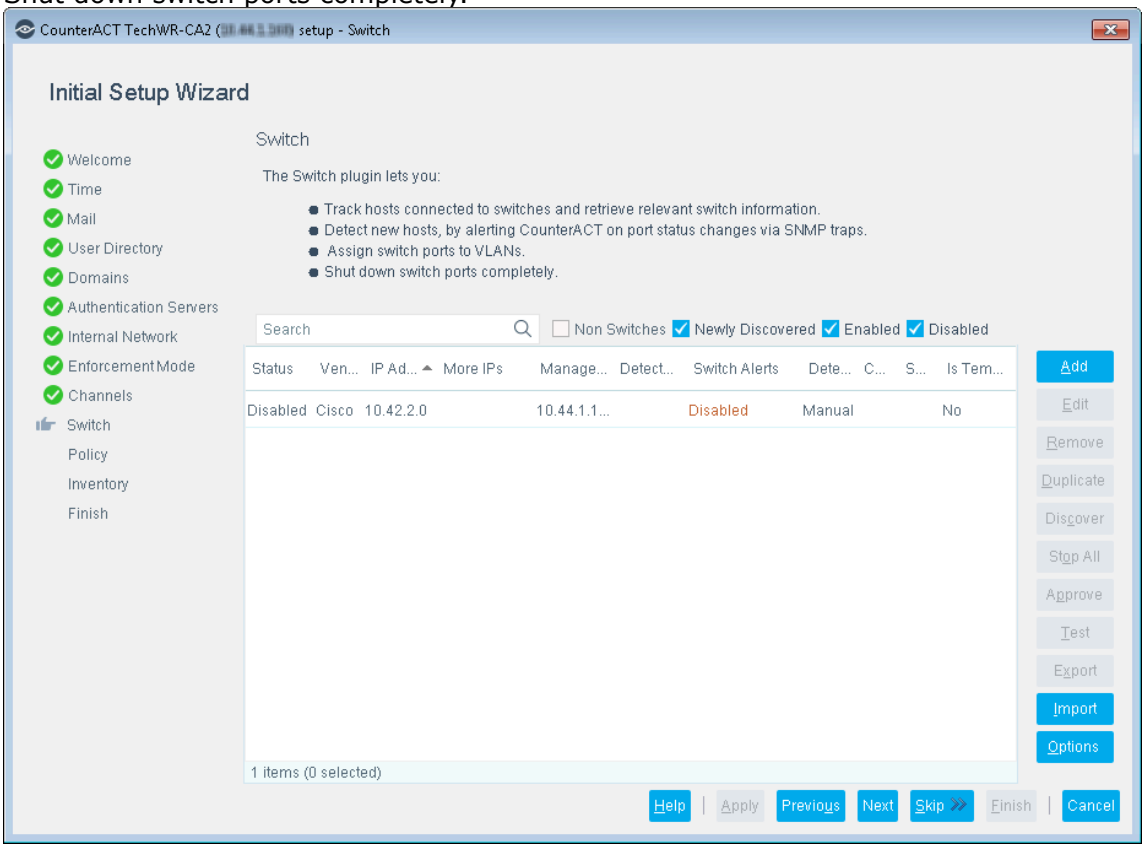
Use DHCP by Default	Select this option if a DHCP address is used by the eyeSight for monitored traffic. Clear this option to manually configure the IP address.

Initial Setup Wizard – Switch

Use the Switch pane in the Initial Setup Wizard to configure the switches that the Switch Plugin manages.

For switches managed by the Switch Plugin, use eyeSight switch tools to:

- Track the location of endpoints connected to network switches and retrieve relevant switch information. For example, users can view the switch IP address and switch port to which endpoints are connected.
- Detect new endpoints on the network, by alerting the Forescout eyeSight about port status changes via SNMP traps.
- Assign switch ports to VLANs, allowing you to set up dynamic, role-based VLAN assignment policies or quarantined VLANs.
- Use ACLs to open or close network zones, services, or protocols on specific endpoints at the switch.
- Block endpoints based on IP addresses or MAC addresses.
- Shut down switch ports completely.



In the Switch pane, you can configure a switch that exists in your network by selecting Add, and completing the Add Switch wizard.

You can configure the switch to add other switches in your network in two ways:

- Auto-discover additional switches: Switches of certain vendors (Cisco, HP, Brocade/ Foundry, Enterasys and Nortel) can auto-discover neighboring switches of any of these vendors. Discovered switches inherit basic attributes of the switch that detected them. All permissions and ACL configurations in discovered switches are disabled
- Use the switch configuration as a template for other switches: When an unmanaged switch (that is, a switch that is not managed by the Switch Plugin) sends an SNMP trap and the community string of the unmanaged switch matches the community string of this switch, then all the settings of this switch (except its IP address) are applied to the unmanaged switch. Switches detected in this manner are automatically added in the Console.

  You can also add additional switches here, and then select Switch in the Console Options window to edit switch configurations and use additional Switch Plugin features.

Note:
You will need to complete the configuration of auto-discovered switches including (recommended) enabling auto-discovery (so that their neighbors can also be auto-discovered) and then enabling these switches.

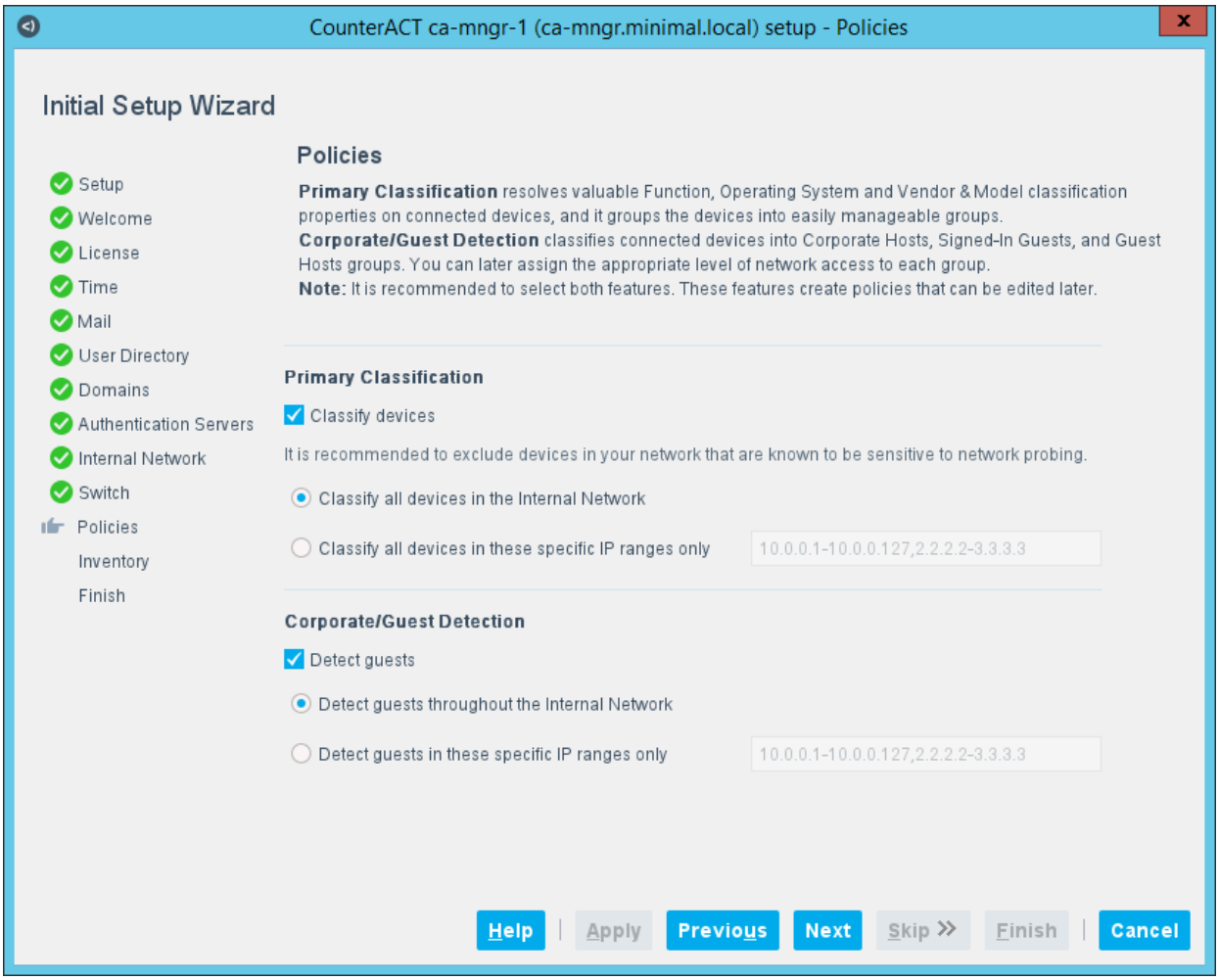
Note:
Refer to the *Switch Plugin Configuration Guide* for information about additional switch configuration features.

Initial Setup Wizard – Policies

Use the Policies pane of the Initial Setup Wizard to classify endpoints into easily manageable groups of network assets and corporate/guest users.

Network asset classification is carried out by a eyeSight Primary Classification policy. Corporate/ guest user classification is carried out by a Corporate/Guest Control policy. These policies are created using core policy templates.

Note:
After registering with an Enterprise Manager, many Appliance policy settings are automatically replaced with the Enterprise Manager settings. See CounterACT Device Management Overview for details.



How classification works

A proprietary algorithm is used to compare the properties of endpoints with the properties of pre-defined device classification profiles, each composed of properties and corresponding values. When the classification algorithm detects that certain endpoint properties match a given profile, the endpoint is classified appropriately. For example, the profile defined for Apple iPad considers a set of properties that includes the HTTP banner, the NIC vendor, and Nmap scan results.

Classify Devices	Select this option to enable Primary Classification, which resolves function, operating system, vendor, and model classification properties on connected devices, and groups the devices into the following easily manageable groups.
Detect Guests	Select this option to enable Corporate/Guest control policies and related groups.

Initial Setup Wizard – Inventory

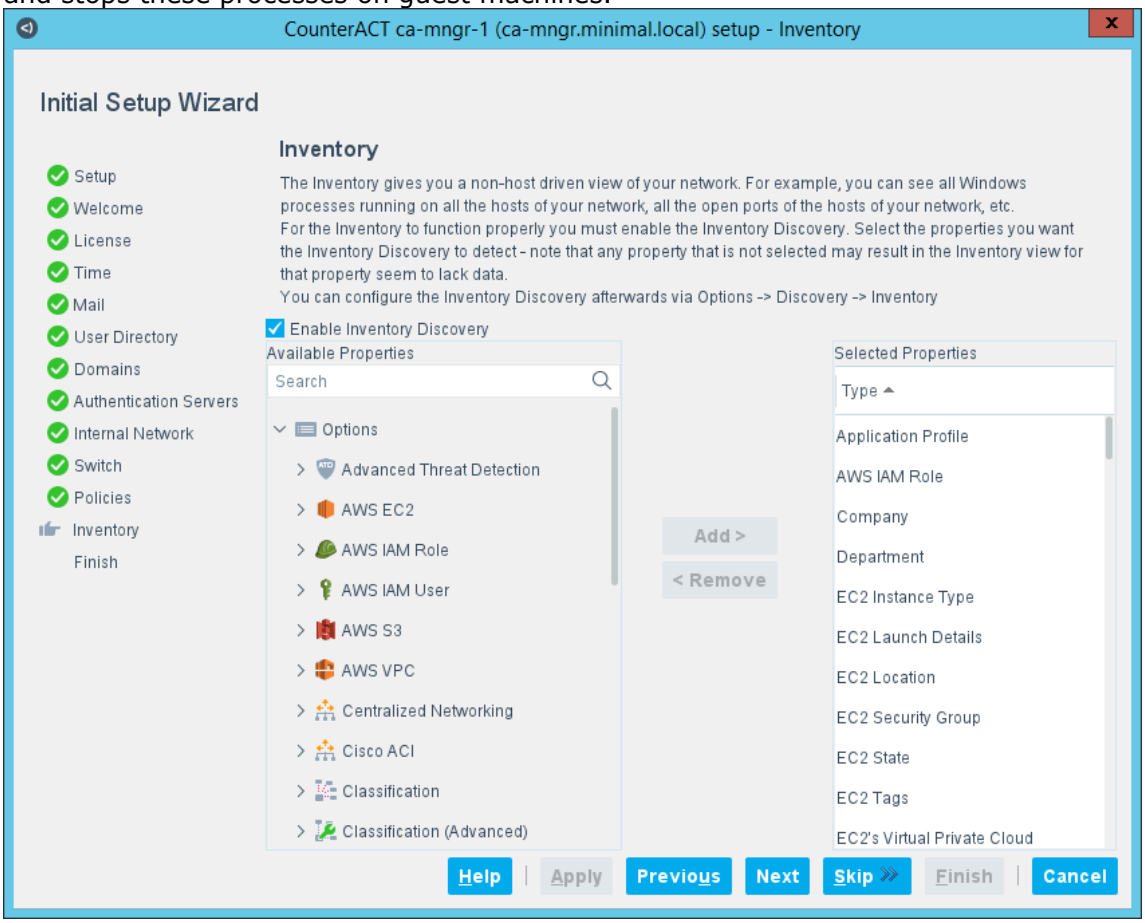
Use the Inventory pane in the Initial Setup Wizard to select the network activities to include in the

Asset Inventory. The Asset Inventory presents a live display of network activity in the Console, for example, running processes and services, detected vulnerabilities, open ports, and logged in users.

See also Working with Asset Inventory Detections for details about the inventory, or select Help in this pane.

Use the Asset Inventory to:

- Broaden your view of the network from endpoint-specific to activity-specific.
- View endpoints that have been detected with specific attributes whether or not they are policy-compliant.
- Easily track network activity.
- Incorporate inventory detections into policies. For example, if you discover that network guests are running unauthorized processes on your network, create a policy that detects and stops these processes on guest machines.

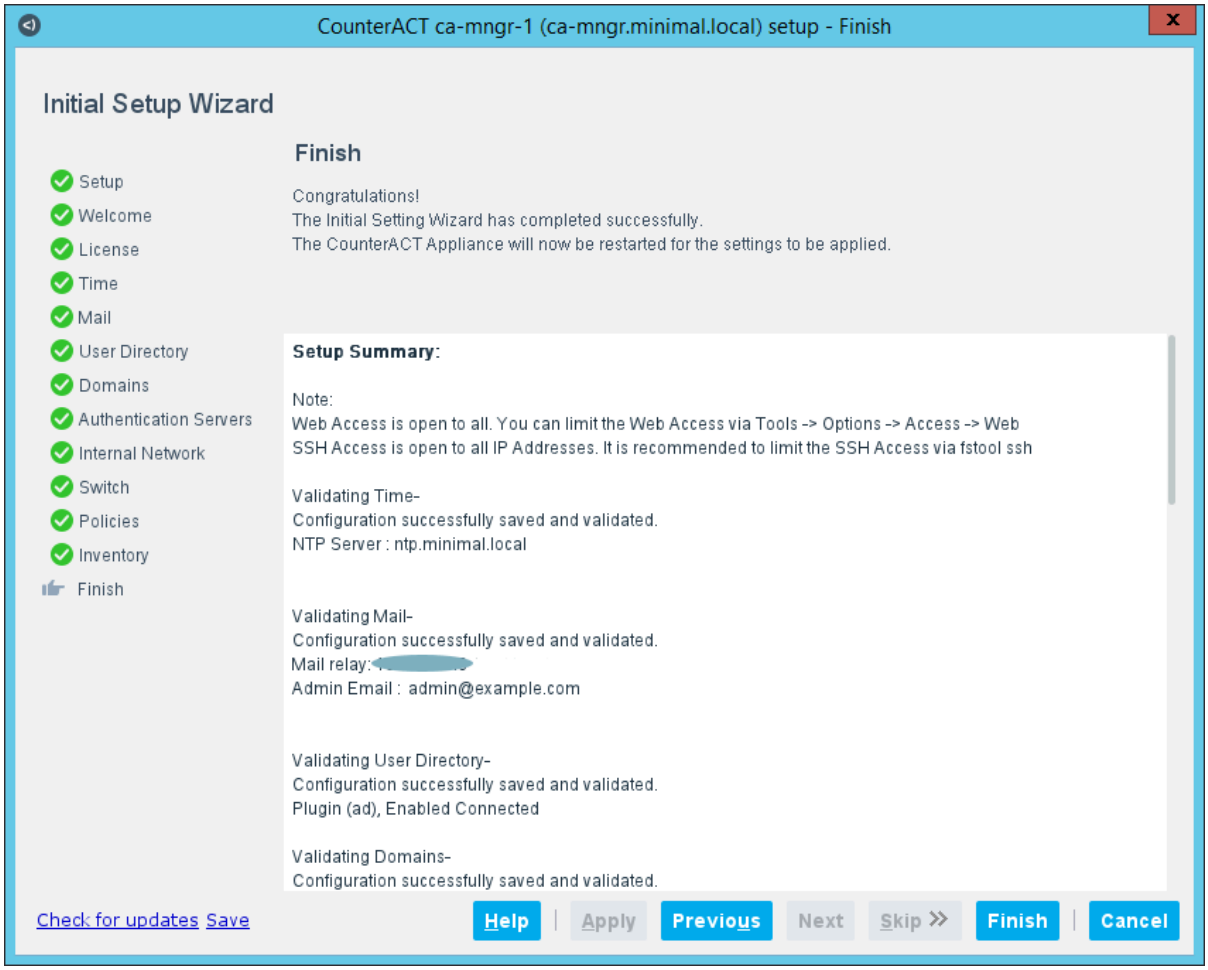


Note:
External Devices Connected and Microsoft Vulnerabilities are excluded from the default Inventory rules. Discovery of these properties may generate extensive network traffic. You can include them by updating the Inventory rules. See How the Asset Inventory Is Learned for details.

Note:
Open ports can also be displayed in the Asset Inventory. This information can be displayed by creating a policy that includes the Open Ports property.

Initial Setup Wizard – Finish

The Finish pane of the Initial Setup Wizard appears when you have successfully completed the Wizard. Review the summary / change settings before you select Finish.



The Finish pane displays a summary of all the wizard definitions. If you select Cancel, all the information in the wizard is deleted. You can update this information from the Console Options window.

Check for Updates	Enable this option to automatically update your system with the most current versions of all installed eyeSight plugins/modules. See Check for Updates for details.

Add Channels

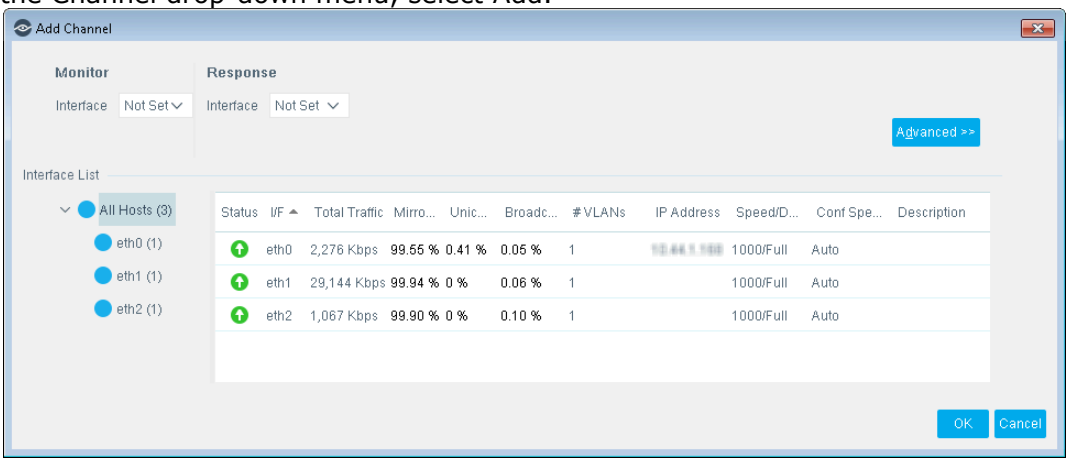
A channel defines a pair of monitor-response interfaces that Appliances need to protect your network. Add the channels that match Appliance interface connections to detect and respond to traffic on network interfaces.

You must define channel definitions that match Appliance interface connections to detect and

respond to traffic on network interfaces.

To add channels that match Appliance interface connections to detect and respond to traffic on network interfaces:

1. From the Channel drop-down menu, select Add.



   The interfaces detected on your Appliance appear in the Interface List. Every few seconds, traffic is captured on the selected interface and is broken down into the different VLANs.
2. Review the interfaces and related information to verify that traffic is detected on the interfaces that you connected to in the Data Center, for example, if traffic is actually mirrored. If you change the monitoring interface assignment here because no traffic is detected (or for any other reason), you must go back to the Data Center and adjust the physical interface connections. Troubleshooting information is displayed at the bottom of the dialog box if traffic detection is exceptionally low or high.
3. From the Monitor drop-down menu, select the interface connected in the Data Center.
4. From the Response drop-down menu, select the interface connected in the Data Center.
5. You can select Advanced to modify VLAN tagging definitions. See Customize VLAN Tagging Definitions for details.
6. Select OK. The Channels pane displays the defined channel setup.
7. Select Apply. Symmetric and Response tests are performed. If the tests fail, you can review related troubleshooting information at the bottom of the dialog box.

Add Channels dialog box

The Add Channel dialog box contains the following options:

Interface	The interface name.
Total Traffic	The total VLAN traffic monitored by the interface.
Broadcast	The percentage of broadcast traffic detected on the VLAN.
Mirrored	The percentage of total traffic not broadcast and not directed at the Appliance.

	This information indicates whether the device is monitoring traffic. A value of less than 20% indicates that the switch was not correctly configured. Under most circumstances, the mirrored traffic percentage should be very high on all but relatively quiet VLANs. A quiet VLAN shows a high percentage of broadcast traffic.
Unicast	The percentage of traffic sent to and from the Ethernet address on the interface.

Set up an appliance with Enterprise Manager settings

You can import the settings of an Enterprise Manager to the new Appliances that the Enterprise Manager will manage. This saves you the trouble of redefining configuration values and ensures uniform configuration.

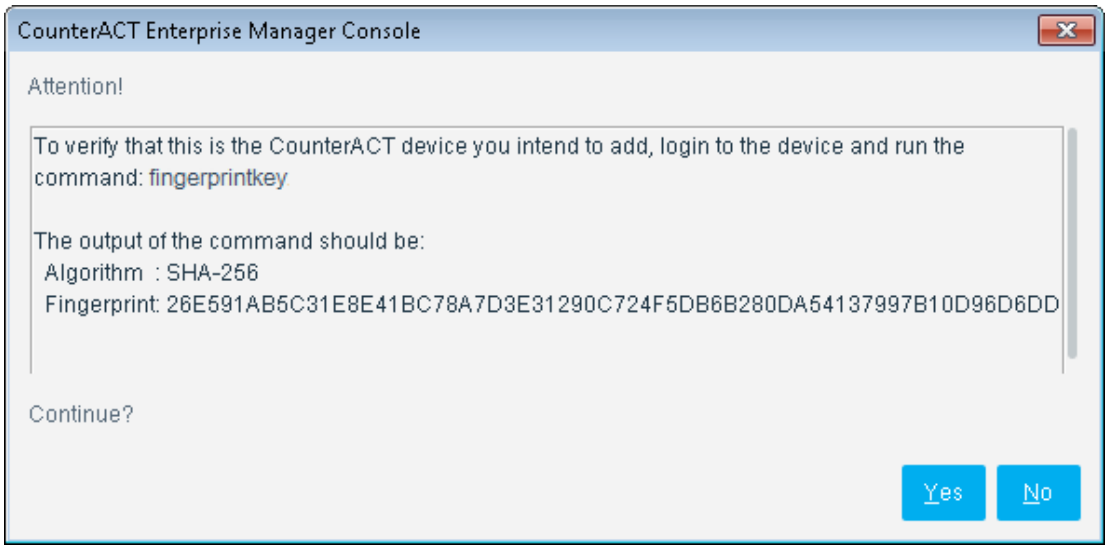
In addition to the Enterprise Manager Wizard settings, plugin versions are synchronized, and the following Enterprise Manager definitions are imported:

- HPS Inspection Engine and Switch Plugin definitions
- Policy and Group definitions
- Virtual Firewall settings
- Policy preferences
- Host Discovery settings
- IP addresses allowed access to the Assets Portal and Console

This option also registers the Appliance with the Enterprise Manager. When Enterprise Manager settings are changed, the settings are applied to the Appliance as well. See Managing Appliances, Enterprise Managers, and Consoles for more information about eyeSight device management.

To set up an Appliance:

1. Log in to the Enterprise Manager via the Console. See Log In to the Console.
2. Select Tools > Options > CounterACT Devices > Add.
3. Enter configuration values and select OK until a connection is made to the Appliance. Messages indicate that the components are connecting and that the Appliance is being registered with the Enterprise Manager.
4. You are prompted to verify that the eyeSight Appliance public key signature is valid.



5. To verify, log in to the eyeSight Appliance through the command-line interface (CLI). Run the command `fingerprintkey`. (In the Bash shell, run `fstool key`. Refer to the *eyeSight CLI Commands Reference Guide* for more information.)
6. Verify that the output of the command matches the value displayed in the Forescout dialog box and select Yes.
7. You are prompted to complete the wizard with Appliance-specific definitions. These include:
    - Initial Setup Wizard – Enforcement Mode (See the description in Set Up an Appliance with the Initial Setup Wizard.)
    - Initial Setup Wizard – Channels (See the description in Set Up an Appliance with the Initial Setup Wizard.)
    - Assign IP addresses
    - Run Appliance Script
8. A summary of all the wizard definitions is displayed. Select Save to save the configuration to an external file.

Add eyeSight Appliance Wizard – initial settings

Enter / accept the basic settings for an Appliance in the Appliance Wizard.

IP/Name	The IP address or DNS name of the Appliance.
Port	The default port is 13000. It is not recommended to change this value.
User Name/ Password	The Admin password created during the Appliance installation in the Data Center.
Appliances	TBS

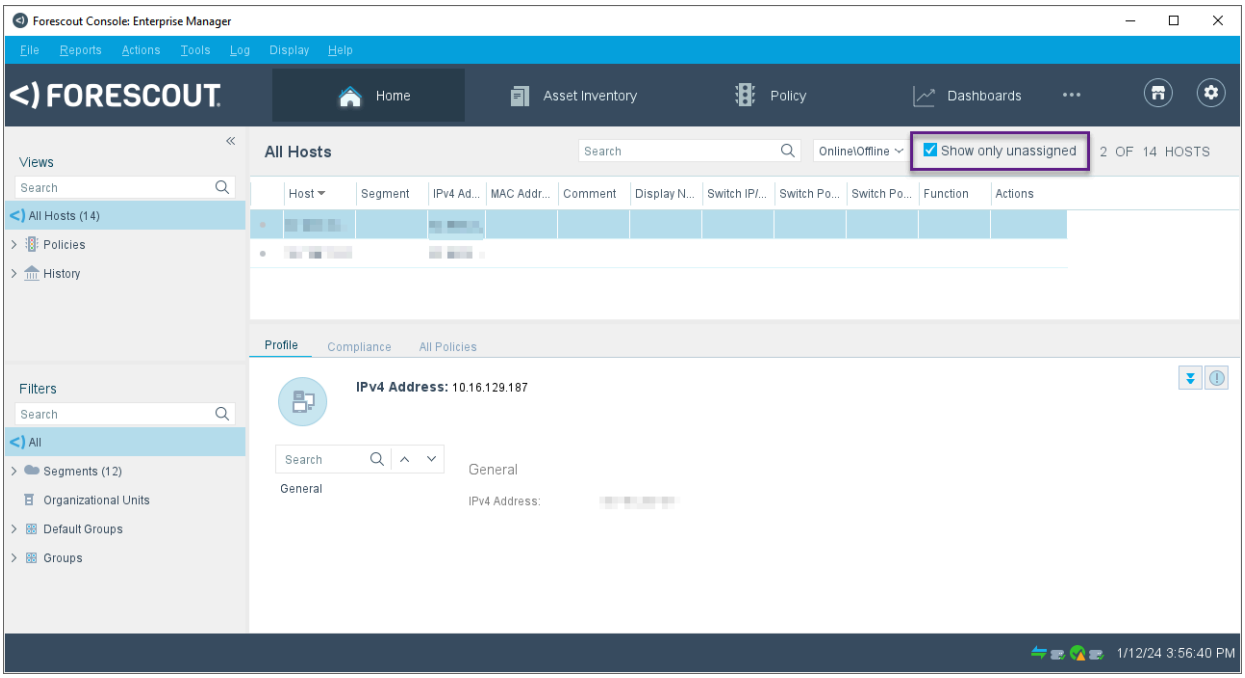
Add eyeSight Appliance Wizard - assign IP addresses

Assign IP Addresses to your Appliance in the Appliance Wizard. It is recommended to assign all endpoints in your Internal Network to eyeSight devices.

Define assignments so that the Appliance manages endpoints that are physically close or manages IP address ranges of the broadcast domains it is tapping in to. Unassigned endpoints can be viewed in the Detections pane by selecting Show only Unassigned.

Distributing the work load among various Appliances:

- Improves performance
- Improves robustness and responsiveness
- Prevents the Enterprise Manager from being a single point of failure if the Enterprise Manager temporarily disconnects



The window includes the Appliance that you are adding as well as other Appliances. Edit as required. All endpoints in your Internal Network should be assigned to an Appliance. Assignments must be unique to each Appliance.

By default, IP address ranges or segments cannot overlap between Appliances. If your network is configured with overlapping IP Addresses, refer to Working with Overlapping IP Addresses in the *Overlapping IP Addresses How-to Guide*.

Unassigned endpoints can be viewed in the Detections pane by selecting Show Only Unassigned.

Editing is only available if you are logged in to the Console via the Enterprise Manager.

You can later view and edit assignments for all Appliances and display unassigned IP addresses. See Working with Appliance Folders for details.

Add eyeSight Appliance Wizard – Finish Page

You can enable the Check for Updates option in the Finish page of the Appliance Wizard.

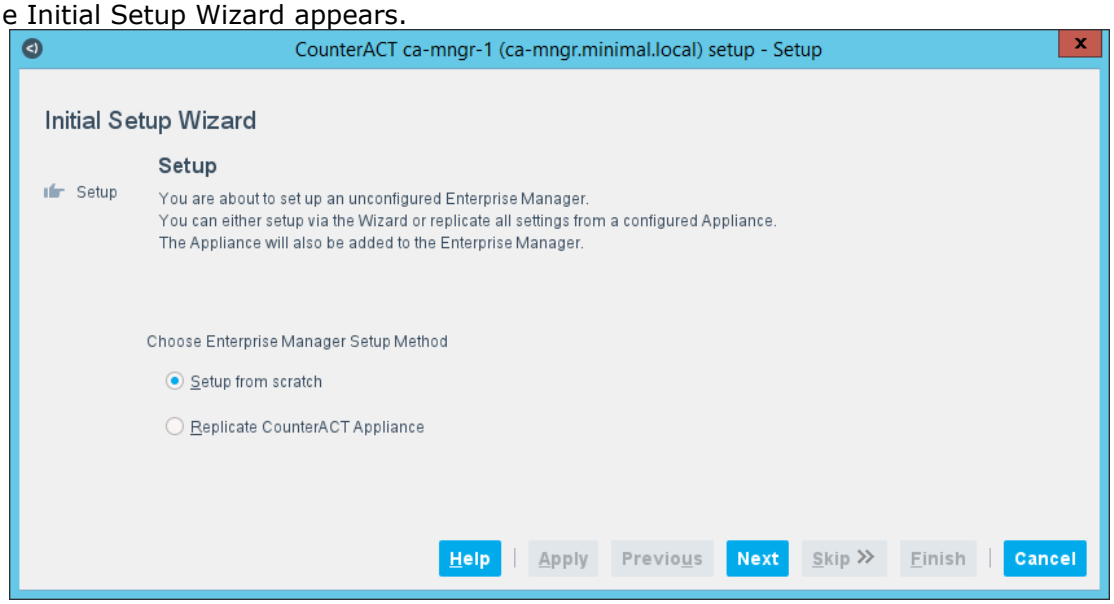
Check for Updates	Enable this option to automatically update your system with the most current versions of all installed plugins/modules. See Check for Updates for details.

Set Up an Enterprise Manager with the Initial Setup Wizard

You set up an Enterprise Manager with the Initial Setup Wizard.

To perform the initial setup for an Enterprise Manager:

1. Log in to the Enterprise Manager via the Console. See Log In to the Forescout Console. The Initial Setup Wizard appears.



2. Select Setup from scratch to run the Initial Setup Wizard for the Enterprise Manager. You are prompted to enter the following information:
   - Appliance time zone and NTP Server settings
   - Mail relay and admin email addresses
   - User Directory account information and the server IP address
   - Domain credentials including domain administrative account name and password
   - Authentication servers used to verify that endpoints have been authenticated successfully
   - Internal Network
   - Switch Information
   - Classification and Guest Control Policies
   - Inventory

   See Set Up an Appliance with the Initial Setup Wizard for information about the Initial Setup Wizard.

Set Up an Enterprise Manager with appliance settings

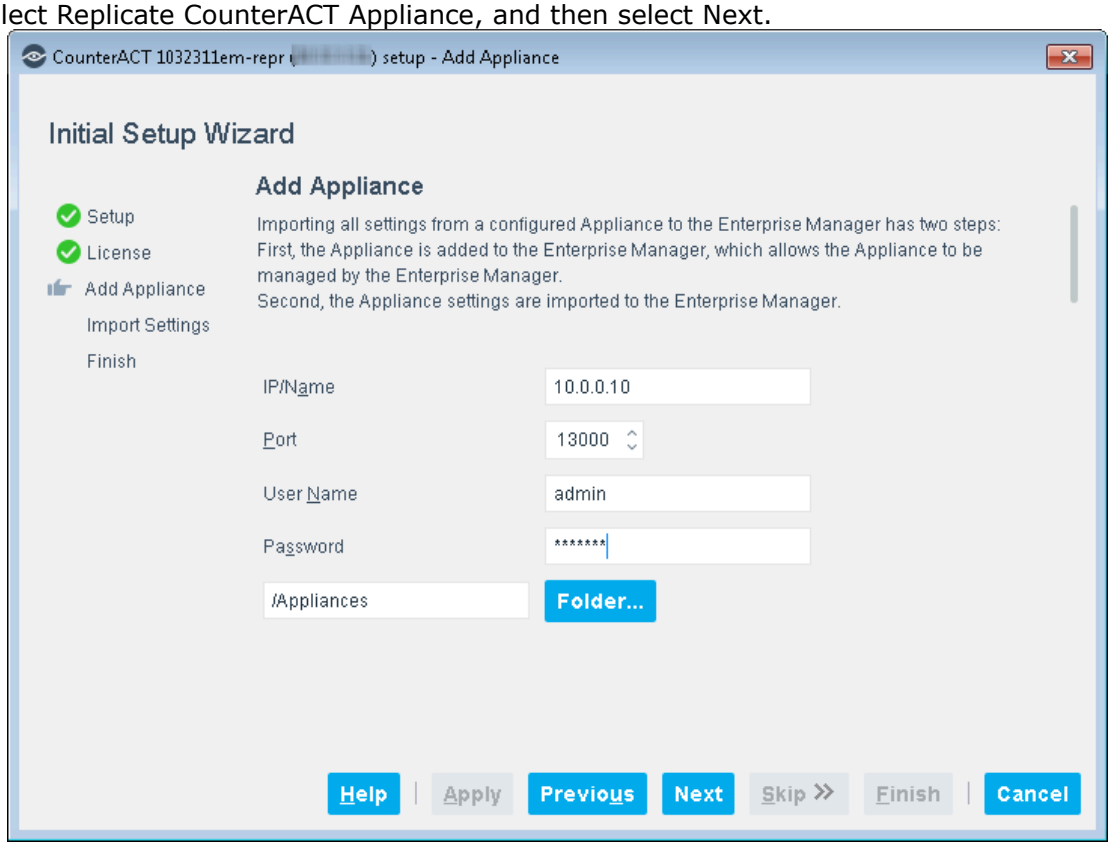
Use this option to replicate settings from a configured Appliance to an Enterprise Manager, and to register the Appliance with the Enterprise Manager.

When you use this option, plugin versions are synchronized, and the following definitions are imported to the Enterprise Manager from the Appliance.

- HPS Inspection Engine and Switch Plugin definitions
- Policy and Group definitions
- Virtual Firewall settings
- Policy preferences
- Host Discovery settings
- IP addresses allowed to connect to the Assets Portal and the eyeSight device
- Internal Network
- Legitimate Traffic rules

To replicate settings:

1. Log in to the Enterprise Manager via the Console. See Log In to the Forescout Console. The Initial Setup pane opens.
2. Select Replicate CounterACT Appliance, and then select Next.



3. In the Add Appliance pane, enter the Appliance IP address. The default port is 13000. It is recommended to keep this value.
4. Enter the Admin password created during the Appliance installation in the Data Center.
5. Select Next. Messages indicate that the components are connecting, and that the Appliance is being registered with the Enterprise Manager.
6. Select Next. You are prompted to verify that the eyeSight Appliance public key is valid.

Finish

A summary of all the wizard definitions is displayed. If you select Cancel, all the information in the wizard is deleted and the Appliance is removed. You can update this information from the Options window.

Select Check for Updates to automatically update your system with the most current versions of all installed plugins/modules.

Plugins and modules significantly broaden eyeSight capabilities. For example, the Switch Plugin lets you track the location of endpoints connected to network switches and retrieve relevant switch information, detect new endpoints on the network, assign switch ports to VLANs, or shut down switch ports completely. See Base Modules, Content Modules, and eyeExtend Modules for more information about this and other plugins.

Select Save to save the configuration to an external file.

When you are done

Perform these procedures after you complete basic setup.

Review Forescout Console and Assets Portal access assignments

By default, Forescout Console and Assets Portal access is available to all users with IP addresses in the Internal Network. To change these defaults, refer to:

- Define Forescout Console Access
- Accessing the Assets Portal

Set up segments

Network Segments are used create a visual representation of your organizational structure, for example, specific departments. After you define segments, you can display endpoints in the Detections pane per segment and configure your policy scope and other Forescout features using segments.

For example, you can view vulnerable endpoints detected in your sales department, malicious endpoints detected by R&D, or network policy violations in the finance department. The segment names that you assign also appear in the Detections pane, Segment column when endpoints are detected. The segments also appear for other features. For example, when creating an accounting segment, the defined range is available when using the VA tool (that is, a user wants to scan accounting), or the Virtual Firewall Policy (that is, accounting cannot use FTP).

See Working with Forescout Segments for details.

Set up segment properties

Segment properties examine the network segment in which an endpoint resides.

Use these properties to create policies that apply actions to endpoints on a particular network segment. These properties are located in the Device Information group of the Properties tree. See Device Information Propertiesu for a description of each property.

Set up ignored IP addresses

You can define endpoints that should be ignored by all policy and Discovery rules, for example, a set of servers to exclude from policy inspection. Endpoints that you add to this group are inspected by Threat Protection and Virtual Firewall policies. See Creating an Ignored IP Address Listi for details.

Review, run and edit pre-defined template policies

eyeSight templates are predefined policies that help you:

- Quickly create important, widely used policies based on predefined policy parameters.
- Automatically group network devices into categories that can be used to apply policies.
- More easily control endpoints and guide users to compliance.
- More easily and quickly implement Forescout product capabilities.
- Roll out your policies more safely by applying conditions and actions that have been used and tested.
- Pinpoint any infractions to your security system more quickly.

Predefined actions are instructions about how to handle endpoints. They are generally disabled by default. You should only enable actions after testing and fine-tuning the policy. See Policy Templatesr

Set up HTTP redirection for policies

HTTP actions let you redirect endpoint web sessions and replace them with important messages or tasks.

For example, you can redirect a user web session and replace it with a notification page, or with a page that forces the network user to authenticate. To use these features, you may need to perform preliminary redirection procedures. Note the following:

- HTTP actions require that the Appliance sees traffic going to the web.
- HTTP redirection requires proper injection setup. See Configure HTTP Redirection for details.
- If your organization uses a proxy for web connection, you must define the proxy ports to be used. See Policy Preferences for details.
- An option is available to redirect user Intranet sessions. See Defining HTTP Redirect Exceptions and Configure HTTP Redirection for details.
- To disable HTTP redirection, see Disable Web Portals.

Set up a threat protection policy and define legitimate traffic for threat protection policies

Your Threat Protection Policy lets you define how eyeSight eyeControl handles malware, worms and other malicious endpoints that attempt to infect your network. See Threat Protection for more information.

You may also need to ignore legitimate scanning activity detected by eyeControl, for example, when you are performing vulnerability assessments, when traffic is generated by legitimate email servers, or for any other business requirement that compels you to grant full access to specific addresses. You should do this to facilitate legitimate traffic and avoid blocking important traffic.

Install the CyberArk Credential Provider on eyeSight devices

Specific eyeSight components, currently the HPS Inspection Engine and the Switch Plugin, can query the CyberArk Enterprise Password Vault in order to retrieve login credentials from the vault. To perform their queries, the components use the CyberArk Credential Provider that must be installed on the eyeSight device (Enterprise Manager or Appliance) on which these components run.

The eyeExtend for CyberArk Module supplies the eyeSight with the CyberArk Credential Provider. For the procedure to install the CyberArk Credential Provider on eyeSight devices and, as necessary, to configure the eyeExtend for CyberArk Module for credential retrieval, refer to Configure the CyberArk Module for Credential Retrieval in the *eyeSight eyeExtend CyberArk Configuration Guide*.

Review Asset Inventory items and create lists

The Asset Inventory presents a live display of network activity at multiple levels, for example, running processes and services, detected vulnerabilities, open ports, and logged in users.

Use the Asset Inventory to:

- Broaden your view of the network from endpoint-specific to activity-specific.
- View endpoints that have been detected with specific attributes whether or not they are policy-compliant.
- Easily track network activity and elements.
- Incorporate inventory detections into policies using customized authorized and unauthorized Lists. You can use the inventory to discover network guests running unauthorized processes on your network; create an unauthorized processes list and incorporate that list in a policy that detects and halts these processes on guest machines. For example, create an Unauthorized Processes Running list and use that list in a policy with the Kill Process action on endpoints that run the process.

See also Working with Asset Inventory Detections and Create Lists Based on Inventory Detections.

Set up map locations

The site map, powered by Google Maps, provides at-a-glance, real-time corporate site status, compliance level, alerts and more — across offices, cities, countries and continents.

You can toggle from a detail-oriented endpoint view to a broader birds-eye view to keep track of endpoints deployed at sites across the globe.

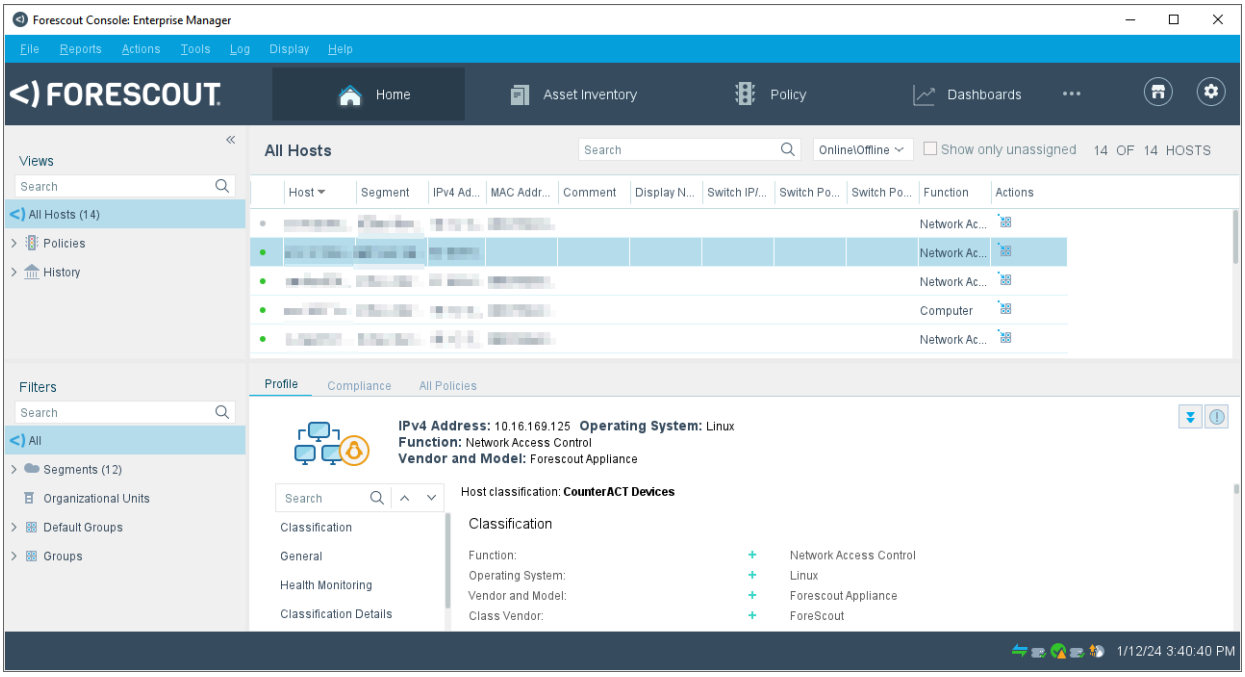
See Set Up the Map – Create Site Locations for details.

Work in the Forescout Console

The Forescout Console is the management application used for viewing information about endpoints and devices.

From the Forescout Console, you can view NAC compliance status, malicious intrusions, vulnerable endpoints, and real-time network inventories. In addition, the Console offers an extensive range of tools to analyze and manage these endpoints.

For the eyeSight Web Client, see Log In to the Forescout Console.



Forescout Console components

The following sections describe the key components of the Forescout Console window:

Title bar

The title bar displays the following information:

- eyeSight device IP address or host name.
- Login user name.
- eyeSight device connection status with the Console.
- Under certain circumstances, a user may have limited Scope access. Limited Scope access means that users cannot see or control many feature configurations in defined ranges and segments.

Under certain circumstances, a user may have limited Scope access. Limited Scope access means that users cannot see or control many feature configurations in defined ranges and segments. See Access to Network Endpoints – Scope for details.

Menu bar

The menu bar displays the Console menu options.

You can select More Space or Less Space in the Display menu to adjust the line spacing in the Console display.

Toolbar – Console views

Toolbar items provide quick access to important information and tools.

Endpoints detected on the network

To open the Home view, select the Home tab:

The Home view displays:

- Extensive real-time information about endpoints detected on your network, for example, endpoint details learned by eyeSight eyeSight, information about endpoint policy status, and eyeSight actions applied to endpoints. See Working with Forescout Detections for details.
- The Forescout site map. The map, powered by Google®, provides at-a-glance, real-time information about endpoints across offices, cities, countries, and continents. See Working in the Site Map for details.

  Adjust the view for viewing preferences by using the toggle arrow on the edge of the Forescout Console pane.

Asset Inventory

The Asset Inventory presents a live display of network activity at multiple levels, for example, running processes and services, detected vulnerabilities, open ports, and logged in users.

To open the Asset Inventory view, select the Asset Inventory tab:

Use the Asset Inventory to:

- Broaden your view of the network from endpoint-specific to activity-specific.
- View endpoints that have been detected with specific attributes, whether or not they are policy-compliant.
- Easily track network activity and elements.
- Incorporate inventory detections into policies. For example, if you discover that network guests are running unauthorized processes on your network, you can create a policy that detects and halts these processes on guest machines.

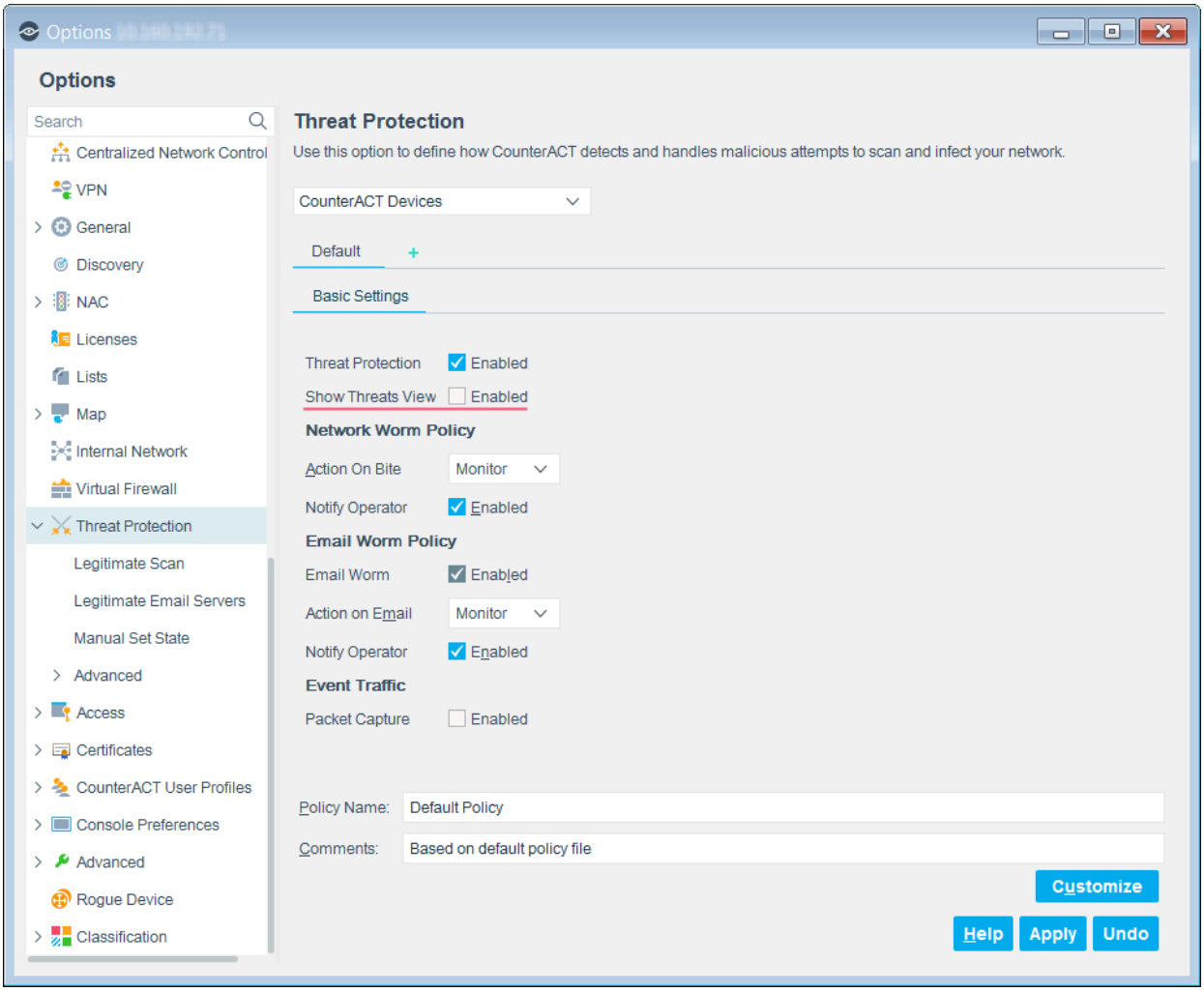
For details, see Working with Asset Inventory Detections.

Threats

Threats view displays endpoints detected via Threat Protection policies. Create and edit Threat Protection Policies from this view. See Threat Protection for details. The Threats tab can be shown

or hidden.

To show or hide the Threat Protection tab, select Tools > Options > Threat Protection, and then enable or disable the Show Threats View option.



Customize the Threats View

Adjust the view for viewing preferences via the toggle arrows on the edge of the Forescout Console pane.

Policy management view

Use the tools in the Policy view to create, edit and manage policies.

To open the Policy Management view, select the Policy Management tab:

Dashboards (and Assets view)

Access the Dashboards (and Assets) view of the eyeSight Web Client. See Logging In to Forescout Web Portals for more information.

Dashboards display dynamic, at-a-glance information about:

- Device visibility
- Device compliance
- Health monitoring
- Forescout policy data, including custom policies

See Dashboards and Assets View for more information about these tools.

Assets portal, reports portal, and user portal builder

You can access the Assets Portal, Reports Portal and the User Portal Builder from the Forescout Console toolbar by clicking the ellipsis icon .

Note:
Users with an eyeSegment license can access Segmentation (eyeSegment application) from the toolbar.

Ellipsis Icon

Access these options from the ellipsis drop-down menu:

Assets Portal, a web-based search and discovery tool that lets you leverage extensive network information regarding network assets. See Assets Portal for details.

Reports, to generate web-based reports. See Reports. For a full description of these reports, refer to the *Reports Plugin Configuration Guide*. .

User Portal Builder, a web-based portal for customizing the appearance of the Guest Management Portal, and web login pages for the HTTP Notification and HTTP Login. See The Forescout User Portal Builder for details.

Note:
Users with an eyeSegment license can access Segmentation (eyeSegment application), to analyze and manage their physical network traffic from a dynamic zone perspective. Refer to the *eyeSegment Application How-to Guide* for details

Marketplace Icon

Click the Marketplace icon to go to the Forescout Marketplace at marketplace.forescout.com to take advantage of all integrations from Forescout, our partners, the wider community, and third-party applications.

Options Icon

Use the Optionsp window to define a wide range of system parameters and update parameters configured during the Appliance installation and initial setup.

Status bar

The status bar may display the following information:

Channel Connectivity Indicator

The Channel Connectivity Indicator is displayed if:

There is a connectivity problem on one of the enabled channels.

No channels are enabled.

A new channel is discovered.

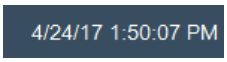
Forescout eyeSight continually searches for traffic on channels defined in the Channel Configuration dialog box. A tooltip indicates which event occurred.

Alarm Indicator (Malicious Hosts Only)

The alarm indicator flashes when new endpoint activity is detected. By default, the alarm blinks for two minutes each time a high severity event is detected.

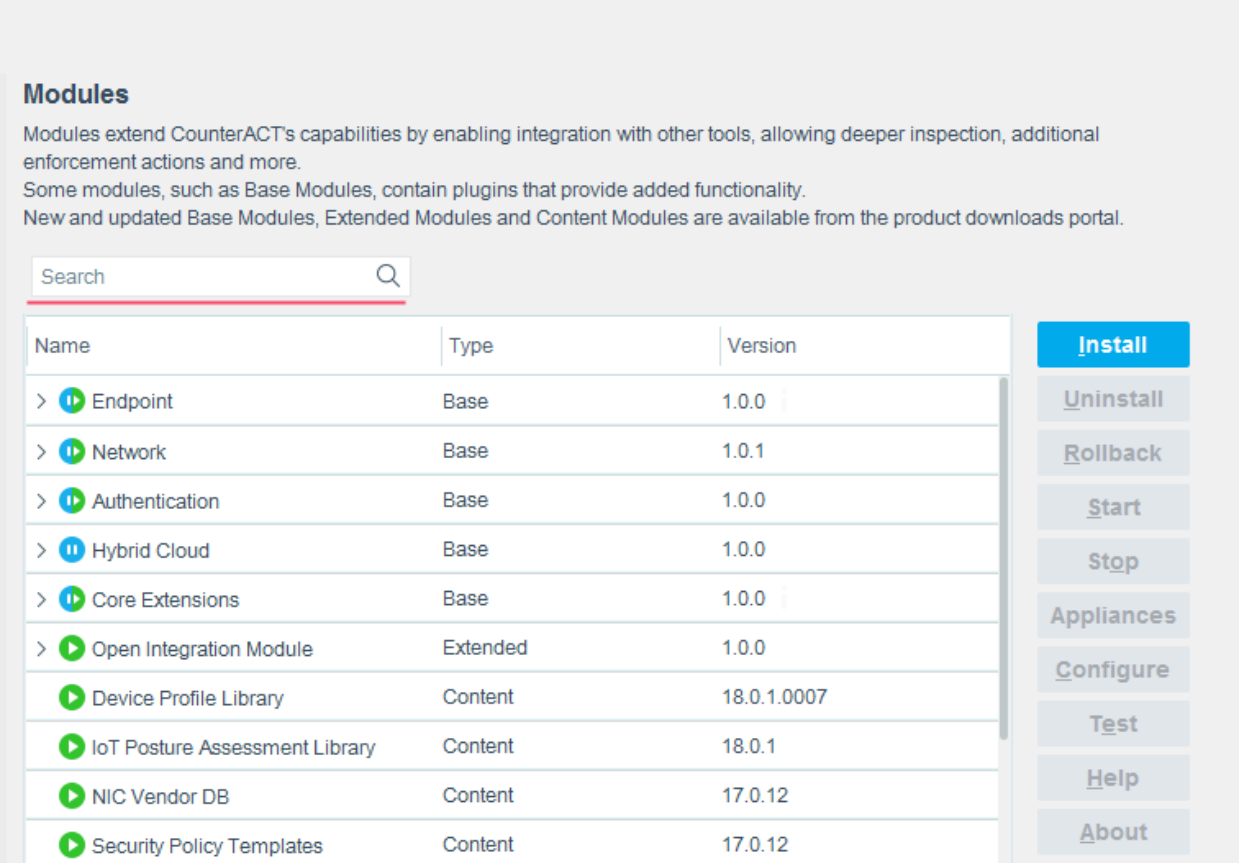
Service Attack Indicator

The service attack indicator blinks when Forescout products detect a service attack. The indicator blinks until the service attack is viewed in the Current Service Attack dialog box. See Handling Service Attacks for details.

Connection Status Indicator	Indicates the connection status between Appliances and the Enterprise Manager. If an Appliance is disconnected, the red X mark is displayed. If a VMware VM is running as a shared resource, the blue I is shown.
Enforcement Mode	If you set the system to the Partial Enforcement mode, the Enforcement indicator is displayed. The Partial Enforcement mode lets you monitor network traffic but limits your ability to respond to it. Specifically, the Threat Protection, HTTP Actions, and Virtual Firewall options are disabled. This mode is recommended for evaluation purposes only. See Set the Enforcement Mode for details. If the indicator reads High Activity Mode, Forescout products are responding to an extensive amount of traffic.
Updates	Indicates the availability of new updates of installed plugins and modules, based on detected versions installed on your eyeSight devices. Select the icon to view and install newer versions. See Base Modules, Content Modules, and eyeExtend Modules for details.
High Availability Cluster Status	Indicates the status of a High Availability pair. Refer to the *Forescout eyeSight Resiliency Solutions User Guide*. for more information about High Availability.
Date and Time Indicator 	Indicates the current date and time according to your local time zone setting.

Search in the Forescout Console

Use the search tool to quickly access information from the Forescout Console, for example, in the Views pane, Detections pane, or the Modules pane. Items that match the search text appear as you type.



Where relevant, collapsed folders expand if the search item you entered is found in the folder. Some search bars can be hidden or displayed by clicking the pane header, for example, the Filters pane.

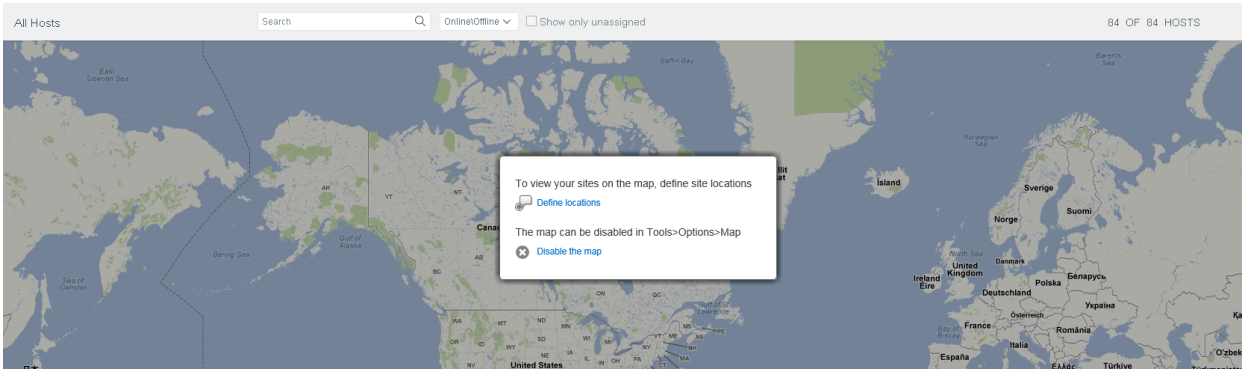
Wildcard Searches

You can use the following wildcard characters in Forescout Console searches:

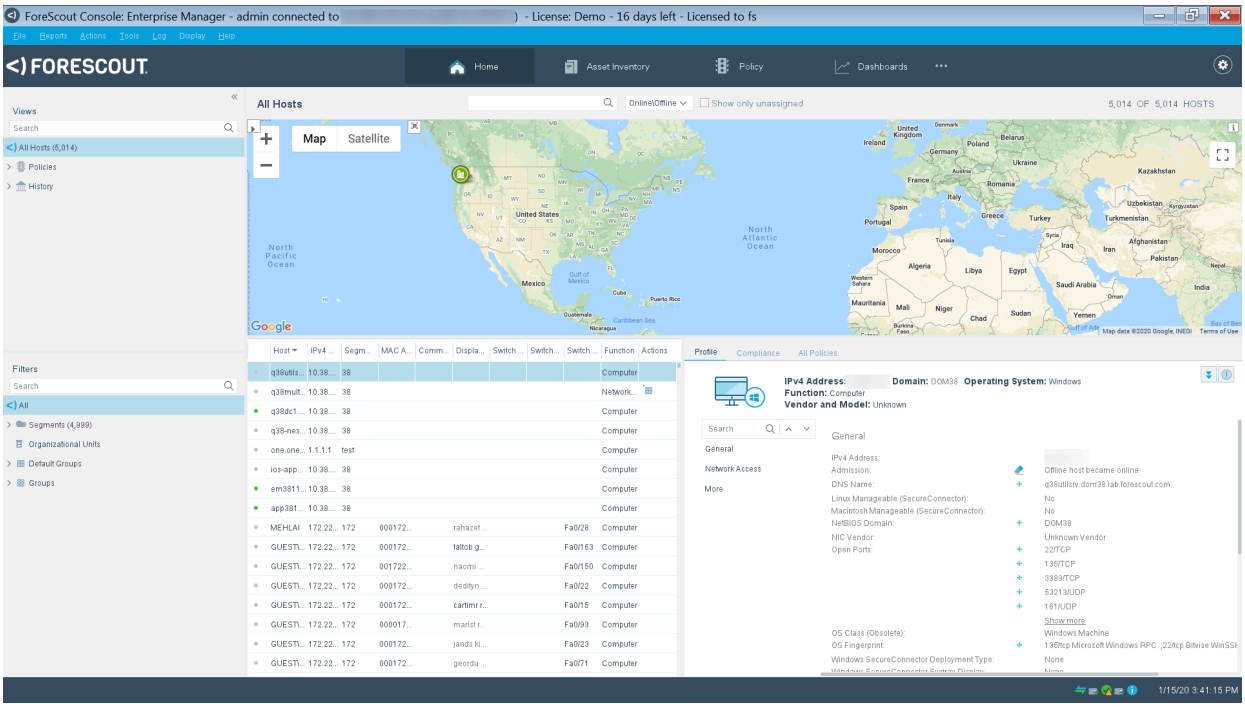
- * (asterisk). Matches any string, including an empty string, and including symbols. You can use the asterisk (*) anywhere in a string.
- ? (question mark). Matches one single character, including symbols.
- \ (backslash). Used as an escape character to protect a subsequent special character (*,? ,\). For example, typing "\?" will search for a question mark (?) symbol.

Work in the Forescout Console site map

The Forescout Console site map, powered by Google®, provides at-a-glance, real-time information about endpoints across offices, cities, countries, and continents. You can toggle between a Satellite view and a Map view.



Endpoint information is displayed in the panes below the site map.



Use the map to get high-level status information for each site, such as:

- Total number of devices
- Non-compliant devices
- Unmanaged devices
- Devices without policies deployed
- Blocked devices
- Malicious devices
- Number of online and offline devices
- Number of corporate and guest devices Browser Requirements: The map runs on Internet Explorer 11.

Work with detections

The Console Home tab displays important details about endpoints detected by eyeSight policies. This information can include:

- Device information, for example, IP addresses, MAC addresses, DNS host name or NetBIOS host name
- Guest and compliance status
- Switch related information, for example, the switch port to which the endpoint is connected
- Endpoint and user identity information, for example, User Directory user name, email address, department
- Information related to actions taken at the endpoint and notifications sent to network users

  Note:

  If you installed plugins/modules, related information also appears. For example, if you installed the VPN Concentrator Plugin, VPN user information is displayed.

  The information displayed in the Detections pane varies depending on the selected Home view. See Home Views.

Deriving unique endpoints from observed addresses

eyeSight learns the IP and MAC addresses of endpoints and network nodes in the following ways:

- By auditing network traffic
- By polling switches, controllers, domain controllers, and other network nodes
- When optional plugins are installed that use additional information sources, such as flow protocols

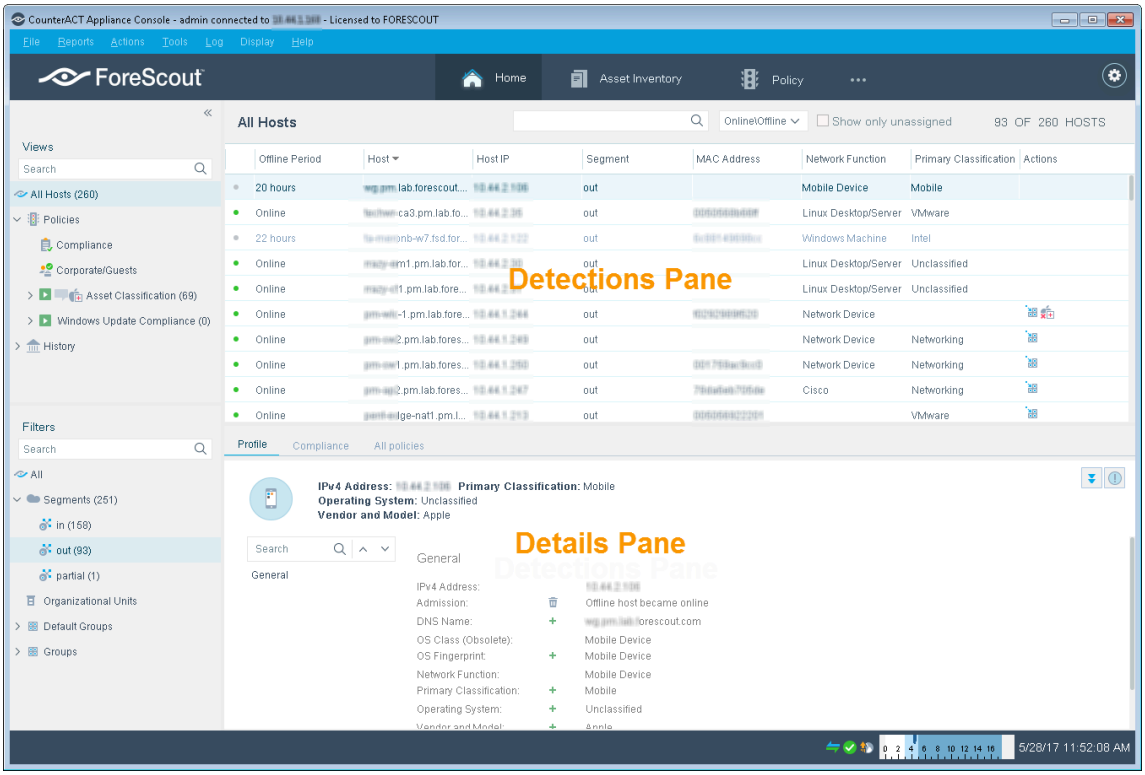
  eyeSight analyzes this information to identify unique endpoints, and to correlate IP and MAC addresses to each endpoint.

- eyeSight data correlation logic uses only IPv4 addresses to identify unique endpoints. IPv6 addresses are not used to identify endpoints.
- When no IPv4 address correlates to a unique MAC address, eyeSight lists this MAC-only endpoint with a placeholder IPv4 address in Console views.

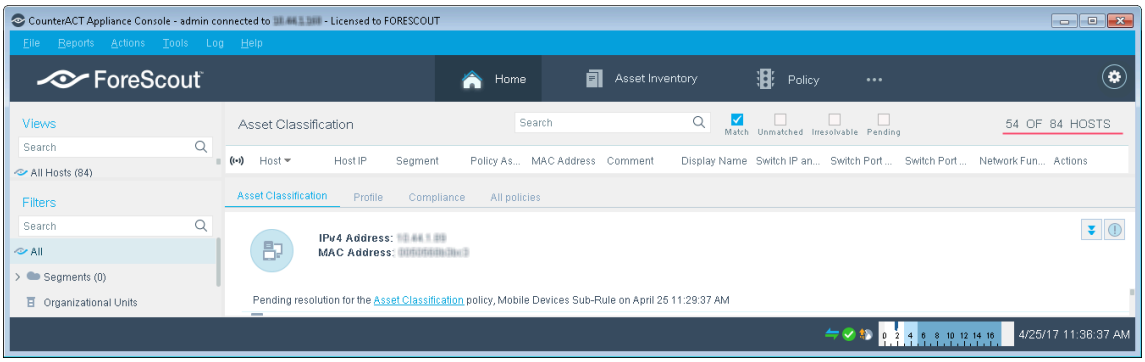
  This discovery and correlation logic is unchanged when IPv6 addressable endpoints are supported.

- Dual-stack endpoints are detected and displayed by their IPv4 addresses.
- IPv6-only endpoints are detected by their MAC addresses, and displayed using a placeholder IPv4 address (as is done for MAC-only endpoints without an IPv4 address).

  For Console settings to enable detection of MAC-only and IPv6-only endpoints, see Work with Hosts without IPv4 Addresses.

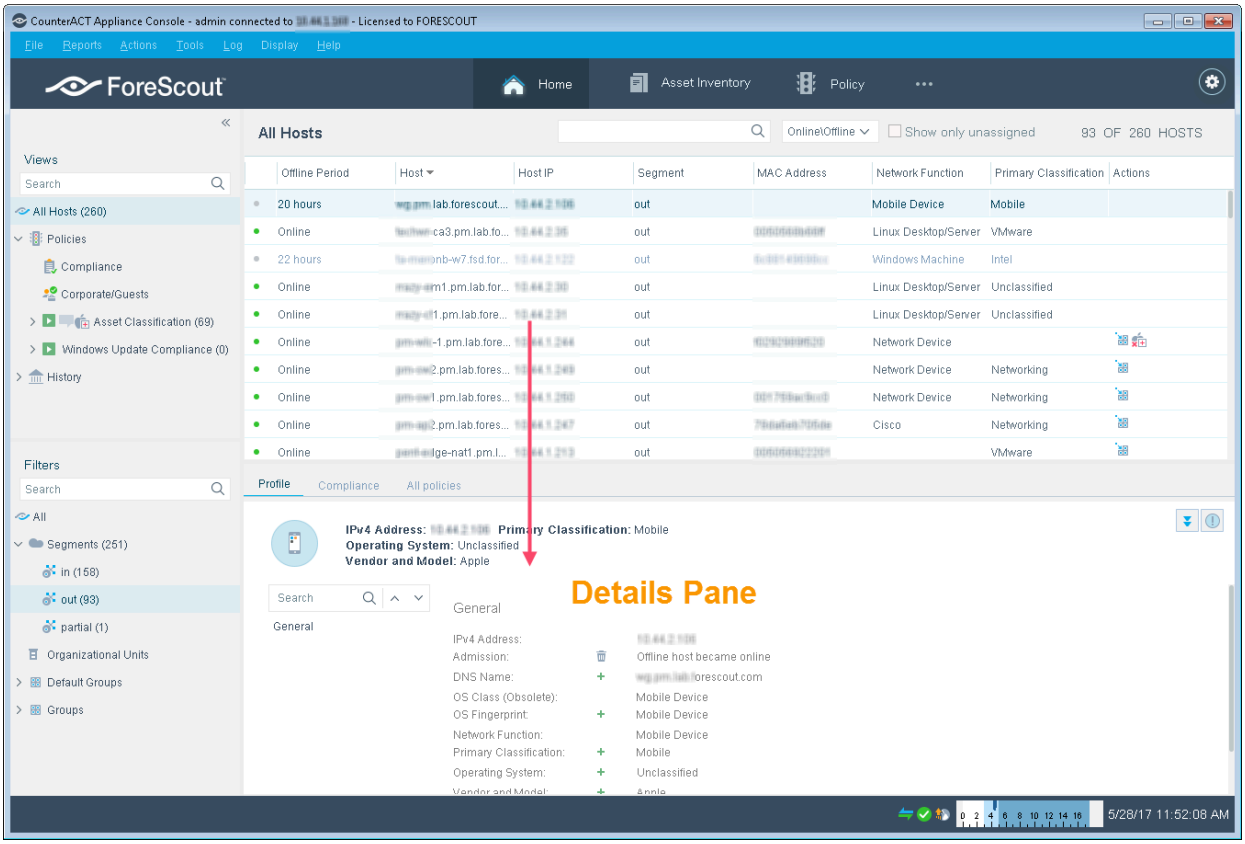


The Hosts indicator at the top right corner of the Detections pane displays the total number of endpoints detected for the folder or sub-folder you select. When there are a large amount of endpoints and it takes a long time to load the information to the Console, this indicator is updated to Showing X of X and displays the number of endpoints currently loaded out of the total detected.



About the Forescout Console details pane

When you select an endpoint in the Detections pane, extensive details appear in the Details pane.



Forescout Console home views

The information displayed in the Detections pane varies depending on the selected Home view.

Forescout Console All Hosts view

The All Hosts view

displays all endpoints that eyeSight eyeSight detects. This includes endpoints that are not part of a particular policy.

Policy view

The Policy view

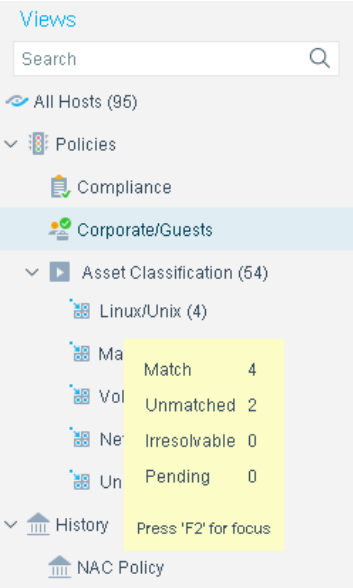
displays endpoints detected as a result of policies created in the Policy Manager. Important detection statistics are provided. For example:

- The policy that the endpoint matched and when it was detected
- Machine information such as the IP address, MAC address, NetBIOS name and DNS name
- Actions taken at the endpoint, for example, if the endpoint was blocked or if access was prevented to the Internet
- User Directory information
- Automated notifications sent to endpoint users
- Information about endpoints that do not match the policy; endpoints that have been released from policy sanctions and endpoints that are pending inspection

Real-time policy status summary

You can view a real-time status summary for each policy. Policy status summaries are automatically updated in real time as the endpoint status changes.

Note:
Hold your cursor over a policy folder to view the summary information.



Compliance view

The Compliance view

displays endpoints that were detected in policies categorized as Compliance policies. By default, these include policies generated from Compliance templates.

Compliance categorization can also be configured in the Policy Manager.

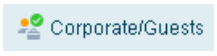
Use this view to see information about the overall compliance status of endpoints included in such policies.

Select a specific endpoint to view a compliance summary for Compliance policies that inspected the endpoint.

The Compliance column entry in the Detections pane indicates whether the endpoint is overall compliant. If an endpoint is inspected by several compliance policies and is not compliant in one, the endpoint is not compliant.

More specific compliance information is shown in the Details pane > Compliance tab, in the Forescout Compliance Center section. This information includes policy names, compliance issues, actions taken, remediation and last update time and the Status. If the Status indicates NA, the endpoint was not in the policy scope.

Corporate/guests view

The Corporate/Guests view 

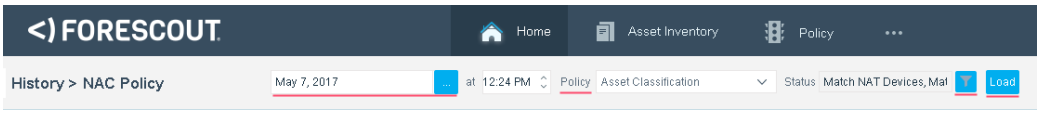
displays endpoints that were detected in policies categorized as Guest policies, including policies generated from the Corporate/Guest Control template. Categorization is performed in the Policy Manager. .

This view displays information about the overall corporate or guest status of endpoints included in such policies.

History view

The History view

displays a filtered snapshot of detection and action information from a previous period. You can view information about malicious endpoints, Service Attacks, and policy detections. When you select a History view, a set of filters are displayed at the top of the Detections pane.

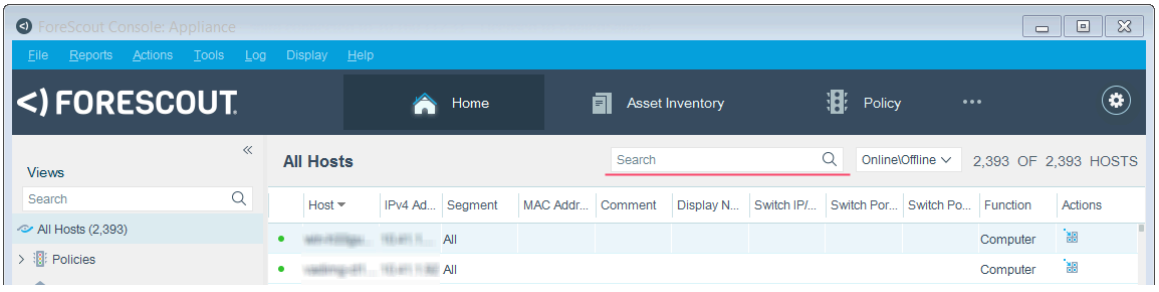


Work in the Detections pane

You can perform a variety of tasks from the Detections pane.

Track endpoints using the Detections pane filter

Use the Detections pane filter to quickly track endpoints of specific interest to you. Endpoints that meet the filter requirements appear as you type.



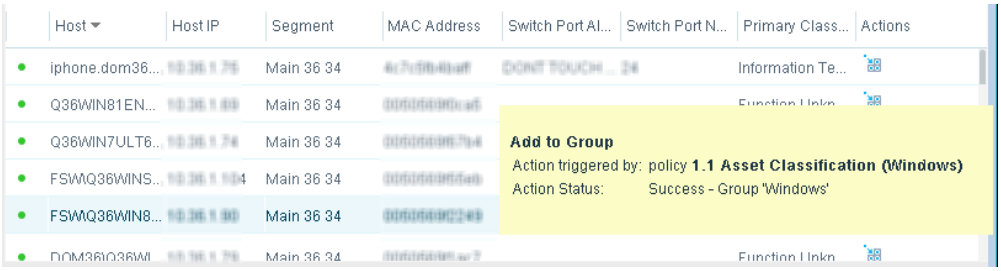
Note:
The filter applies to all endpoints, but information may not appear if it is contained in hidden columns. Be sure to display columns that may contain relevant details.

Note:
Restrict comma-separated search patterns in the Detections pane filter to no more than 20 patterns at a time. Searches query each column of each Host listed in the Detections pane, and extensive searches can lead to delays or service restarts. Search more effectively and

reduce search times by narrowing searches using the Segments, Policies, and Group filters.

View table tooltip information

When you hover over an item in the table, a tooltip displays information regarding that item. For example, if you hold your cursor over the Action field, a tooltip displays detailed information regarding the action. Important troubleshooting information may be included. For example, an entry indicating that the endpoint has not been assigned to an Appliance and as a result is not monitored. For easier reading, select F2 to freeze the tooltip.



Configure the Detections pane columns

Default columns appear in the Detections pane with basic endpoint property details, actions taken at endpoints, and related information. The information varies according to the selected Home view. For each view, default information is displayed.

You can set change the layout and content of the columns in several ways.

Control endpoints from the Detections pane

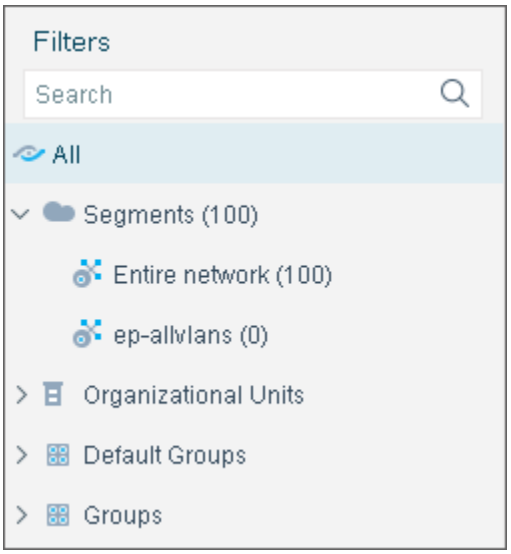
Various options are available for controlling endpoints from the Detections pane. For example, you can:

- Start and cancel Forescout actions on selected endpoints
- Create endpoint exceptions
- Recheck endpoint status
- Clear property detections
- Add a customized comment about the endpoint
- Add the endpoint properties to a policy list

Work in the filters pane

The Filters pane provides tools that let you organize endpoints into logical categories, and then view them in the Detections pane per category.

This is important, for example, when managing networks with extensive detections.



Several filter categories can be created:

Work with asset inventory detections

Select the Asset Inventory tab to view a live display of network activity at multiple levels, for example, running processes and services, detected vulnerabilities, open ports, and logged in users.

Use the Asset Inventory to:

- Broaden your view of the network from endpoint-specific to activity-specific.
- View endpoints that have been detected with specific attributes, whether or not they are policy-compliant.
- Easily track network activity and elements.
- Incorporate inventory detections into policies (black and white lists). For example, if you discover that network guests are running unauthorized processes on your network, create a policy that detects and halts these processes on guest machines.

The Asset Inventory is organized according to the following categories of network activity:

- Classification
- Microsoft Vulnerabilities detected
- Classification (Advanced)
- External Devices connected
- Users
- Applications Installed
- Guest Registration
- Switches integrated with the Forescout eyeSight
- User Directory
- Switch
- Open Ports
- Certain Windows, Linux and Macintosh activity and elements
- Geolocation

You can maximize smooth tracking of this activity by customizing the inventory categories into sub-categories. For example, you may discover via the Asset Inventory that your network is working with a variety of authorized and unauthorized processes. If this is the case, you could

create lists of authorized and unauthorized processes under the Process Running property folder or lists of Switch IP addresses per VLAN under the Switch folder.

Inventories only show endpoints that are currently online.

Asset Inventory activities are queried and refreshed every 23 hours. The refresh frequency can be modified from the Inventory Discovery rule. See Endpoint Discovery Rules for details.

Note:
On a managed Appliance (connected to the Enterprise Manager), the Asset Inventory information is read-only, i.e., you cannot create, edit or remove lists.

Inventory Discoveries vs. Policy Discoveries

Working with policies lets you query specific endpoints to discover what network activities they are carrying out, and to control them. The Asset Inventory provides an additional view of your network by presenting an overall cross-section of key network activities. This means, for example, instead of running a policy to verify that certain processes are or are not running on your network, you can instantly view all processes running in the Asset Inventory view.

How the Asset Inventory is learned

The properties listed in the Asset Inventory view are learned using the following Forescout tools:

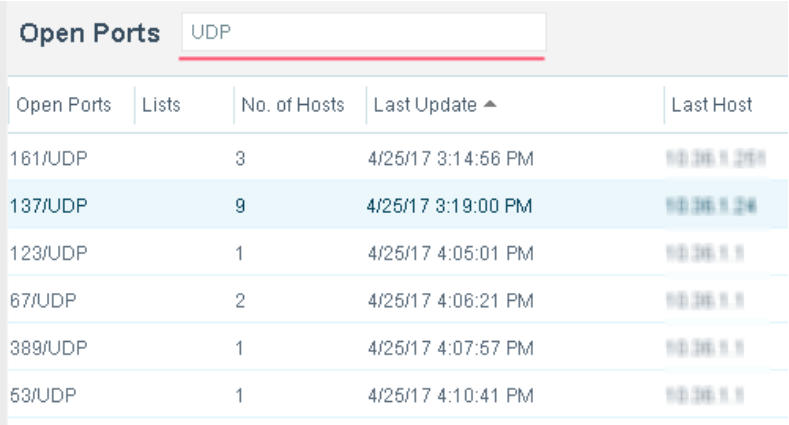
- Inventory Discovery Rules
- Detection Policies

Note:
Certain inventory items may be learned passively by eyeSight eyeSight. This happens when the Appliance is installed and starts monitoring your network. However, this information may only be gathered from part of your network. It is recommended not to rely solely on this information when working with the Asset Inventory.

Filter the asset inventory view

The following options are available for filtering the Asset Inventory view.

Use the Search tool to filter the Asset Inventory display. The filter is applied automatically as you type, with the matching Asset Inventory items immediately shown in the Asset Inventory view. For example, display all open UDP ports by typing in UDP in the filter field.



You can customize the Asset Inventory. For example, you may discover via the Asset Inventory that your network is working with a variety of authorized and unauthorized applications. In this case, you could create lists that itemize authorized and unauthorized applications under the Windows Applications Installed property folder or lists of Switch IP addresses per VLAN under the Switch folder. After you create lists, you can filter the Asset Inventory view according to those lists.

See Use Lists to Customize the Asset Inventory for details.

Asset inventory panes

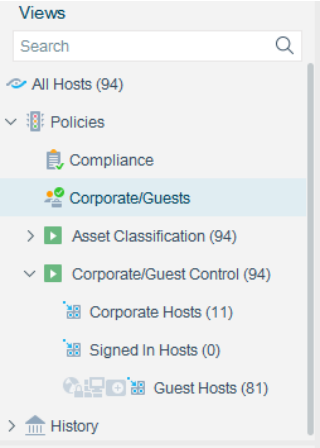
The Asset Inventory is divided into the following areas:

- The Views Pane lists inventory categories based on endpoint properties and property lists that you create.
- The Detections Pane lists information about the inventory property category selected in the Views pane. For example, the number of endpoints running a specific process.
- The Hosts Pane displays all endpoints that are detected with the selected inventory item. For example, the endpoint IP address, MAC address, connected switch port, or User Directory name.

Inventories only show information detected at online endpoints.

Views pane

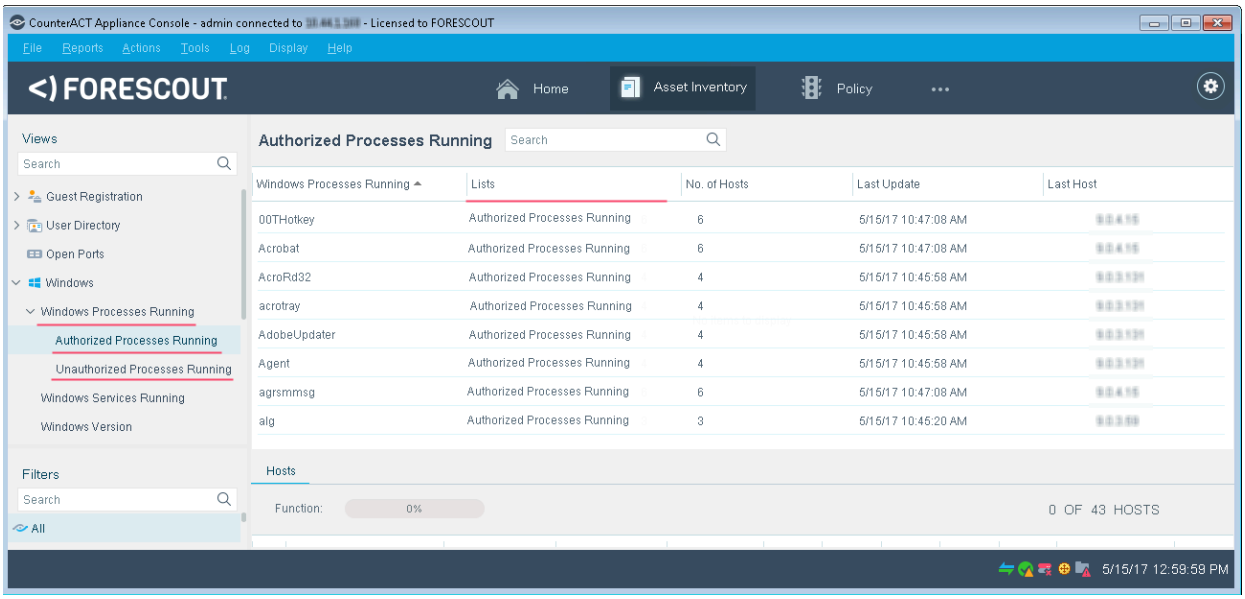
The Views pane shows the Asset Inventory items that you can view.



If plugins or eyeExtend modules (Extended Modules) are installed, other items might be displayed, such as:

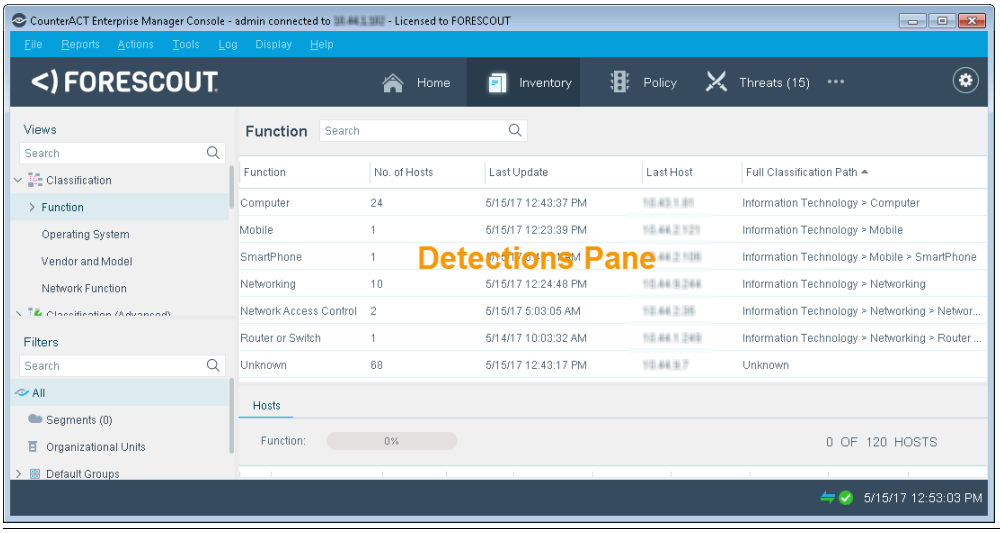
- Classification Properties
- Guest Registration
- Windows machines
- Function
- User Directory
- Microsoft Vulnerabilities detected
- Operating System
- Open Ports
- Services Running
- Vendor and Model
- Windows Applications Installed
- Switches integrated with the eyeSight
- Network Function
- External Devices connected
- Macintosh machines
- Advanced Classification Properties
- Linux machines
- Software Updates Missing
- Suggested Function
- Logged-in users
- Applications Installed
- Suggested Operating System
- Operating system versions running
- Users
- Processes Running

You can create lists for each of the property categories shown in the view. For example, create an Unauthorized Processes Running List under the Processes Running category, and add all unauthorized processes detected at your network to it.



Detections pane

The Detections pane displays information about the property selected in the Views pane. Previously, the Detection pane read and showed only limited columns, resulting in missing data. Now, it reads all the columns and shows limited columns that were shown previously; however, you can add or remove additional columns for the selected view category.

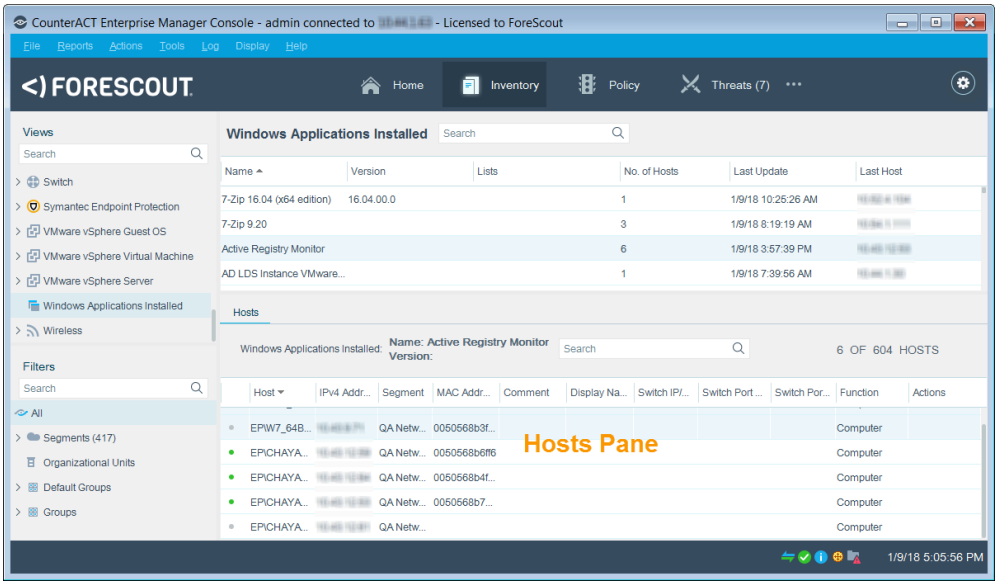


Inventory Property	(for example, Processes Running) The property selected in the Views pane. Information in this column includes all the values for the related property. For example, if you select the Process Running property, this column shows all the processes currently running.
No. of Hosts	The number of endpoints currently detected with the selected property. For

	example, the number of endpoints running a process; the number of endpoints detected at switch IP address; the number of endpoints detected with vulnerabilities or the number of endpoints logged in as Windows users.
Last Update	The last date and time when the detection was made.
Last Host	The last endpoint where the activity was detected.
Lists	The lists to which the live inventory property was assigned. For example, the iexplore.exe process may be part of the White listed Server Processes list and the White listed Endpoint Processes list. See Use Lists to Customize the Asset Inventory for more information about creating lists.

Hosts pane

The Hosts pane displays the endpoints that have been detected for the Asset Inventory item selected. Previously, you would see missing data for several hardware properties; however, data for all properties can now be viewed. Use the tools available when working with endpoint detections to handle these endpoints. For example, you can assign actions to endpoints or drill down to get more detailed endpoint information. Use the search tool at the top of the pane to filter endpoints. See Control Endpoints from the Detections pane for details.



Use lists to customize the asset inventory

The Asset Inventory automatically detects a wide range of network activity that you can organize into logical categories. For example, you may discover via the Asset Inventory that your network is working with a variety of authorized and unauthorized processes. If this is the case, you can create Lists of authorized and unauthorized processes under the Process Running property folder or lists of Switch IP addresses per VLAN under the Switch folder.

Working with inventory lists enables more customized, smoother tracking of network activity.

You can use lists when working with policies. For example, create a policy that tracks and stops machines running unauthorized processes. See Defining and Managing Lists for details.

Work with eyeSight segments

Segments are named groups of IP addresses. Use segments to represent your network in the Console in a way that reflects your organizational structure.

Note:
The segments discussed here are related to the IP subnets that define your network environment but may not exactly parallel your network's IP structure. The segments discussed here are internal Forescout definitions used to specify sub-sections of your network within the Console.

Note:
From eyeSight Version 8.4, the Forescout Admin (REST) API provides you with automatic configuration capabilities for managing deployments on the eyeSight, where network entities, such as the segment tree and default groups ranges, can change on a daily basis. The Admin API allows you to integrate third-party network management IPAM (IP Address Management) tools, such as Infoblox and BlueCat, and ensures that segments defined on the eyeSight are synchronized with their latest IPAM database definitions. For more information, see Work with the Forescout Admin API in the *Admin API Plugin Configuration Guide*.

Segments let you organize endpoints into logical categories within Forescout. For example, you can define segments for Sales or Finance departments in your organization. Sub-segments can also be created: Create a Sales category and, under that, Local Sales and International Sales categories.

The segments you create appear in the Filters pane of the Console.

After you define segments, you can use them to:

- Filter the Detections pane. For example, display endpoints in the Sales department that match a specific policy.
- Specify IP addresses for Forescout features. For example, use predefined segments to specify the scope of a policy, antivirus tool, or Virtual Firewall.
- Work with the site Map. For example, create a location called NYC-HQ, New York and then assign the respective segments in the NYC-HQ office network to this location. See Set Up the Map – Create Site Locations for details.
- Create reports based on segments, for example, Compliance trends per segment. See Generating Reports and Logs for details.

When you work with segments:

- Modifying an existing segment changes the IP addresses that are referenced by the segment wherever it is used in eyeSight. For example, the scope of policies may change, or the Appliance that handles certain IP addresses may change.

- You can use the Audit Trails reports to search for information about users who have modified segment definitions.
- One set of segments is shared among all eyeSights

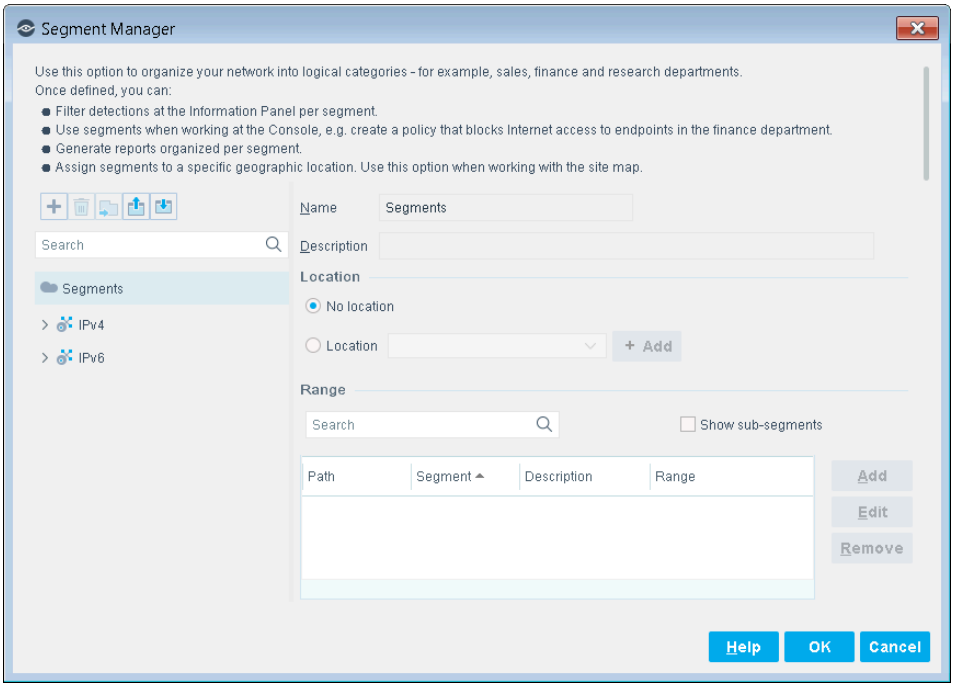
Work with the Segments Manager

To view / manage segments in the Segments Manager do one of the following:

- Right-click the Segment node in the Filters pane in the Console and select Segment Manager.
- Select Segment Manager from the Tools menu to open the Segment Manager.

The left pane shows the Segments tree. Use the search tool in this pane to find existing segments.

The right pane shows information for the selected segment. The table lists IP addresses assigned to the segment. Select Show sub-segments to show IP addresses that this segment inherits from its children. Use the search tool to look for a specific IP address in this segment's scope.



- For each segment, the table lists the following information:
  - The full Path to the segment
  - The Segment name
  - The segment Description
  - The Range of IP addresses associated with this segment
- You can modify the segment tree in the following ways:

	Add a segment. You are prompted to name the new segment and specify its location in the segment tree. The new segment is created as a child of the selected node.
	Delete the selected segment. Forescout products may still manage the

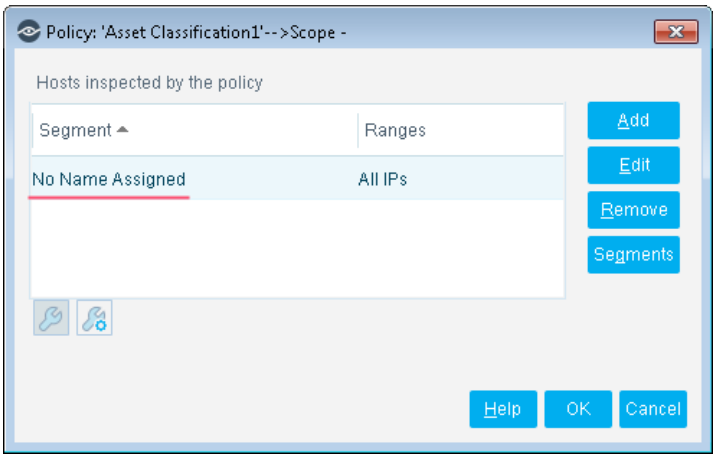
	IP addresses associated with the segment. See Remove Segments from the Tree.
	Move the selected segment and its children to another location in the tree. The selected segment is moved under the new parent node that you specify. You can also drag and drop nodes of the tree. Moving segments in the hierarchy can change the IP addresses they contribute to parent segments. This can change the IP addresses that are referenced by the parent segment.
	Select Export to save segment definitions of the selected node and its children to a file. Select Import to create a new branch at the selected node based on definitions in a file. Segment definitions are expressed in a structured XML file, or in a CSV file that lists each segment definition. You can also right-click a node in the segment tree and select Export or Import.

In the right pane, you can edit definitions for the selected segment. For example, select Add to assign IP addresses to the segment.

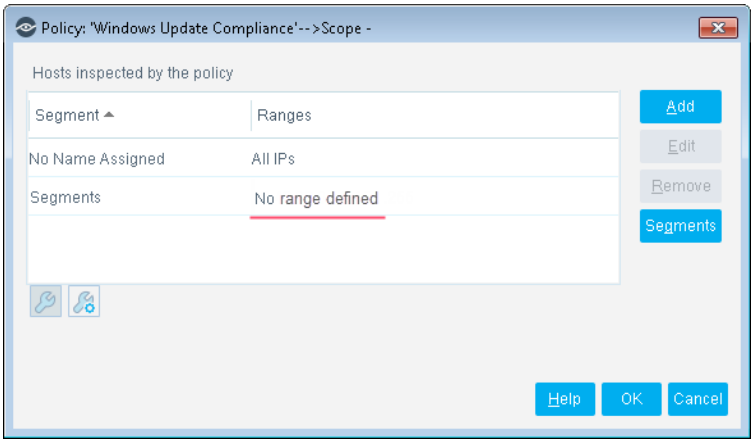
Remove segments from the tree

Removing segments from the Segment tree only deletes the segment name. If you have already assigned IP addresses to this segment, Forescout products still handle endpoints with those IP addresses.

However, references to the segment in policies and other areas of the Console indicate that no segment name is assigned.



Conversely, if you remove IP assignments from the Ranges area, those IP addresses are no longer included in the segment.



If only empty segments are assigned to a failover cluster, and you want to remove one of the segments, you must first remove it from all failover cluster folder assignments before you remove it from the Segment tree. See Working with Appliance Folders and the *Forescout eyeSight Resiliency and Recovery Solutions User Guide* for more information.

File formats for importing and exporting the segment tree

You can export or import the entire segment tree or a specific segment. You may want to export segments if you are doing extensive editing and additions and want to use an external tool. You can also use the exported file as a template that reflects the file format required for importing.

Segment data (segment names and address ranges) is imported or exported in two file formats: XML or CSV.

A typical CSV file has the following format:

```
Segment ID,Parent Segment ID,Current Segment ID,Segment
Name,From,To,Segment Description
0,-1,0,Segments,,,
```

```
1,0,3921800411724927309,internal
network,10.160.50.1,10.160.50.120,
```

After the header line, each segment is as a line of the file, with the following fields:

Segment ID	A numerical ID assigned to each segment. This value must be unique in the segment tree.
Parent Segment ID	The parent ID of each segment. Each segment must have a parent. The parent ID for the root segment is –1.
Segment Name	A name assigned to the segment. This name is displayed in the Filters pane and Information table.
From/To	IP address range of the segment. If there are several ranges within the segment, those ranges must have the same segment ID, parent ID, and name.

Common spreadsheet applications can be used to edit CSV files, as shown below.

A	B	C	D	E
Segment ID	Parent Segment ID	Segment Name	From	To
0	-1	Source Network	1.0.0.0	223.255.255.255
1	0	Finance	10.0.0.0	10.0.2.255
2	0	Engineering	10.0.5.0	10.0.7.255
3	2	Development	10.0.5.0	10.0.5.255
4	2	QA	10.0.6.0	10.0.6.255
5	0	Administration	10.0.3.0	10.0.4.255

The same simple tree shown in CSV format is shown below in XML format.

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
GROUP DESCRIPTION="" NAME="Segments" SEGMENT_ID="0"
UPGRADE_PERFORMED="true">
    <GROUP DESCRIPTION="" NAME="internal network"
SEGMENT_ID="3921800411724927309" UPGRADE_PERFORMED="true">
        <RANGES RANGE="10.160.50.1-10.160.50.120"/>
    </GROUP>
</GROUP>
```

The `<GROUP>` element is used to define segments, and can be nested to show tree structure. The segment name, description, and unique numerical ID are represented by attributes of the `<GROUP>` element.

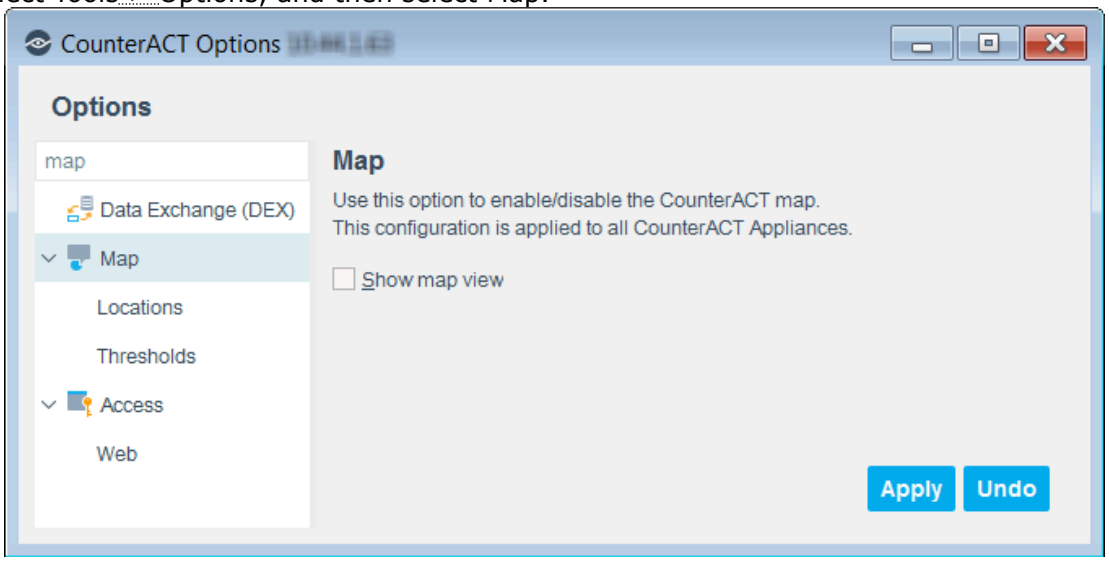
The `<RANGE>` element is used to define IP addresses in the segment.

Enable or disable the Forescout Console site map

You can enable or disable the Forescout Console site Map. This configuration is applied to all Appliances.

To enable or disable the site map:

1. Select Tools > Options, and then select Map.



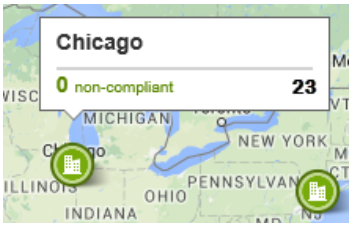
2. Select or clear Show map view.
3. Select Apply.

Set up the Forescout Console site map – create site locations

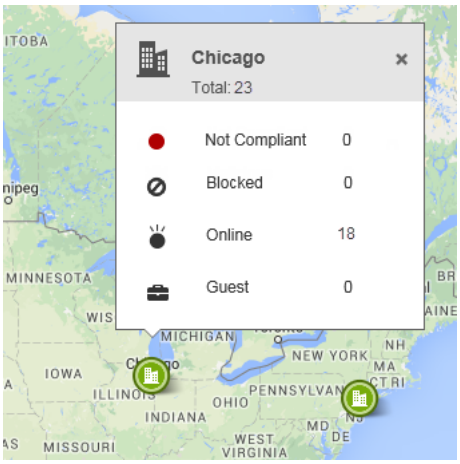
To work with the site map, you must create map locations. Map locations comprise specific geographic locations that are assigned to segments. For example, create a NYC HQ location and assign segments located in the New York office network to this location.

Each map location is represented on the map by a location indicator. .The indicator size is based on the number of detections at the site, i.e., when there are more detections, the site indicator is larger.

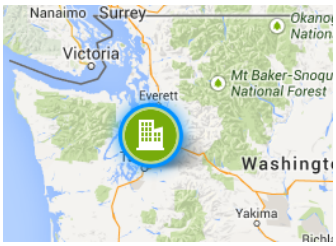
After locations are created, the map displays information about detections at each site when you position your cursor over a site.



Click a location to view detailed site information. For example:



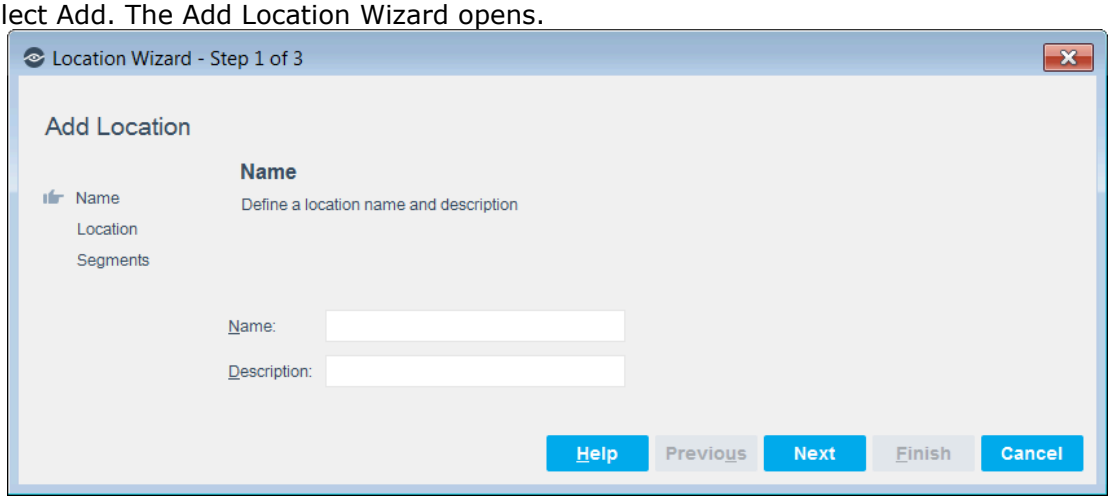
When you double-click a site, the endpoints at that site are displayed in the Detections pane below the map. A blue ring around the icon indicates that the site is selected. Clicking anywhere on the map to deselect the site.



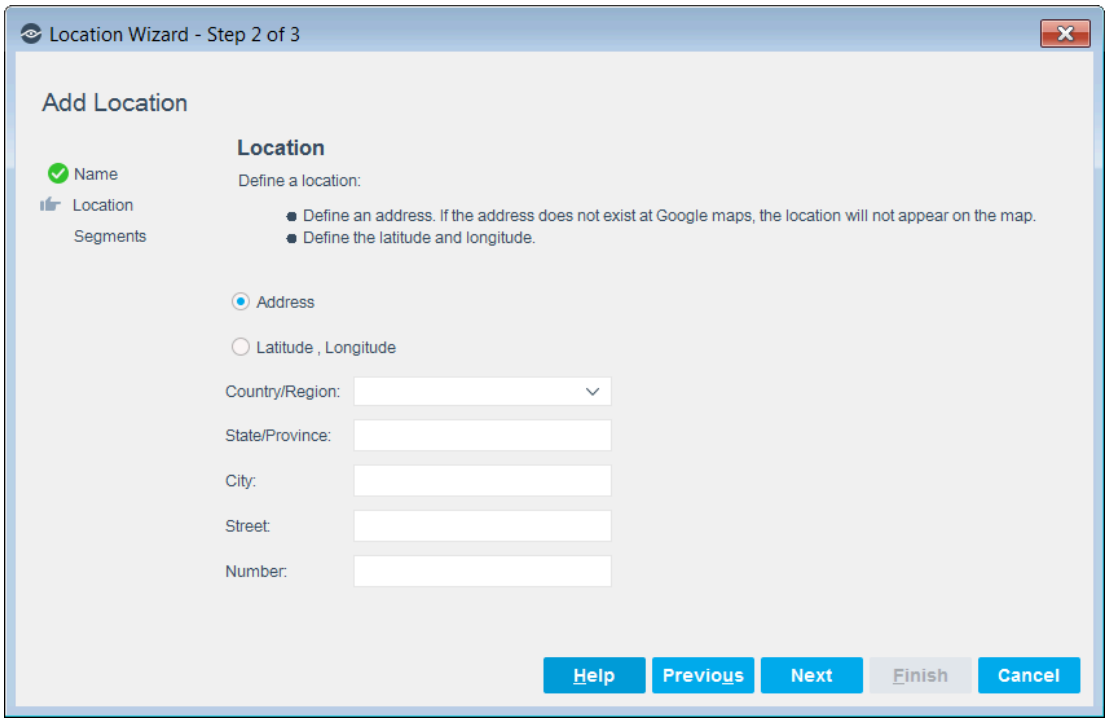
Note:
You can also assign segments to locations from the Segment Manager.

To define locations:

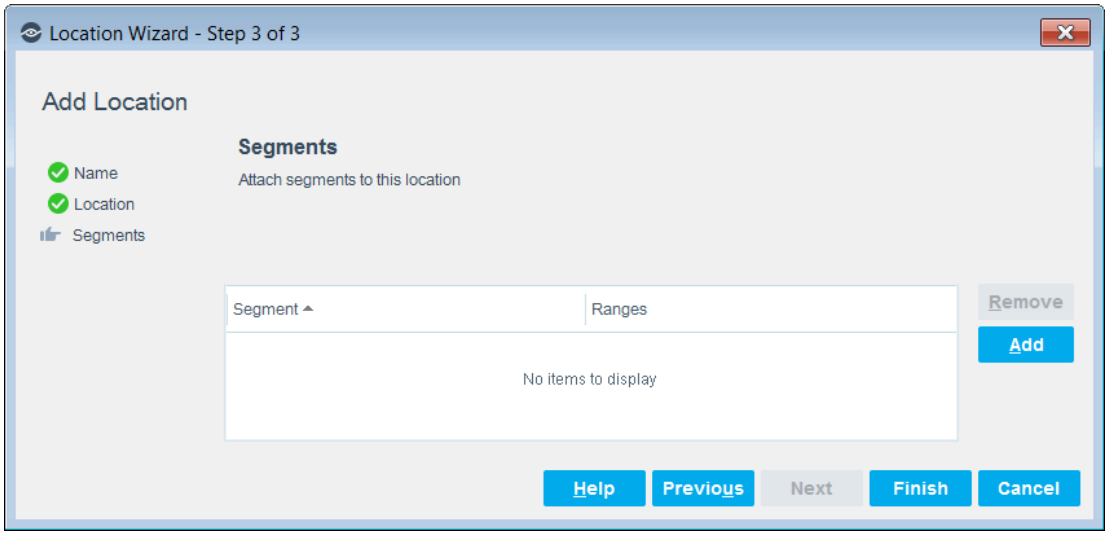
1. Select Tools > Options.
2. Select Map , and then select Locations. The Locations pane appears.
3. Select Add. The Add Location Wizard opens.



4. Enter a location name and description. Select Next.



5. Define a location:
    - Define an address. If the address you enter is not maintained by Google Maps, the location will not appear on the map.
    - Define the latitude and longitude.
6. Select Next.



7. Select Add. The Segment selection dialog box opens.
8. Select the segments that you want to associate with this geographical location.
9. Select OK. The location appears in the Locations pane.

Customize display thresholds for Forescout Console site map indicators

The following options are available for customizing display thresholds for map indicators:

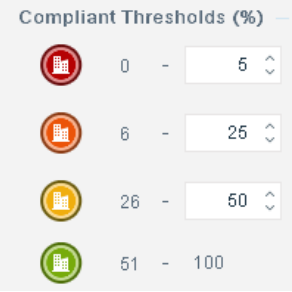
- Customize Compliant Threshold Settings
- Customize Cluster Size Settings
- Customize Cluster Grid Size Settingss

Customize Forescout Console site map compliant threshold settings

Customize the Compliant Thresholds (%) settings to adjust the color of location icons according to the percentage of compliant endpoints. Different colored icons are displayed on the map when the percentage of endpoints detected for a certain category is exceeded. For example, set the map to display a red, Critical icon for a site when between 0% and 5% of endpoints are compliant.

To customize:

1. Select Tools > Options.
2. Select Thresholds from the Maps folder. The Thresholds pane appears.



3. Define the compliance display thresholds.

Customize Forescout Console site map cluster size settings

Customize the Cluster Size settings to adjust the size of onsite and offsite location icons on the map. Larger icons are displayed for sites with a greater number of endpoints. For example, set the map to display a larger icon when there are between 10 and 50 endpoints at an onsite location and a smaller icon when there are less than 10 endpoints.

To customize:

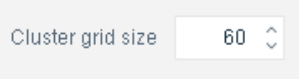
1. Select Tools > Options.
2. Select Thresholds from the Maps folder. The Thresholds pane appears.

3. Adjust the Cluster Size ranges to define the icon sizes.

Customize Forescout Console site map cluster grid size settings

The Cluster grid size field in the Forescout Console site map determines how nearby offsite locations are clustered together at differing zoom levels.

The Forescout Console site map uses grid-based clustering to divide the map into squares of a certain size. When viewing the map from a higher zoom level, geographically close, offsite endpoint locations are grouped together and only one offsite indicator is displayed. When you zoom in, you see each distinct location.



The larger the number, the more offsite locations that are geographically close to one another will be clustered together at higher zoom levels. See View Grid-Based Clustering of Endpoints for details.

To customize:

1. Select Tools > Options menu.
2. Select Thresholds from the Maps folder. The Thresholds pane appears.
3. Adjust the Cluster grid size value.

Forescout Console site map tools

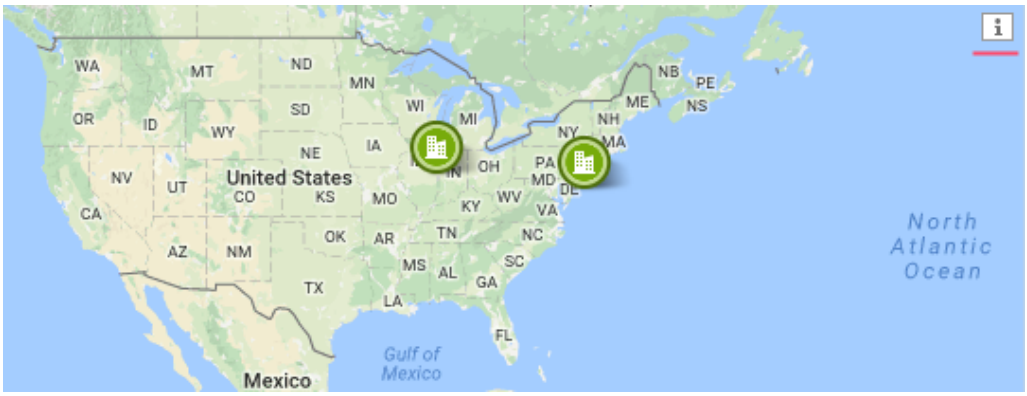
Use map tools to:

- Access the Map Legend
- View Grid-Based Clustering of Endpoints
- View Site-Specific Statistics
- Filter Map Display
- Display Information about Endpoints Not Assigned to a Location

See Enable or Disable the Map to view the map.

Access the Forescout Console site map legend

Select the Information icon to display the map legend.



Note:

m The Externally Managed Devices item in the legend serves as the groundwork for future support of offsite endpoint management.

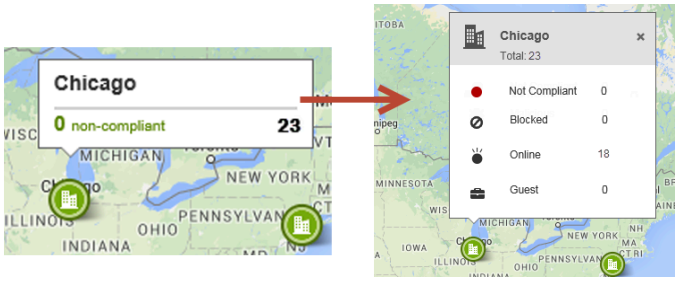
View grid-based clustering of endpoints on the Forescout Console site map

The Forescout Console site map uses grid-based clustering to divide the map into squares of a certain size. When viewing the map from a higher zoom level, geographically close endpoint locations are grouped together and only one indicator is displayed. When you zoom in, you see each distinct location.

The Cluster grid size field determines how locations are clustered. See Customize Cluster Grid Size Settings for details.

View site-specific statistics on the Forescout Console site map

Select a site indicator to open a site form detailing the total number of endpoints detected and the number of endpoints detected at a site for specific categories. For example, you can view endpoints that were detected as non-compliant, malicious, or blocked.

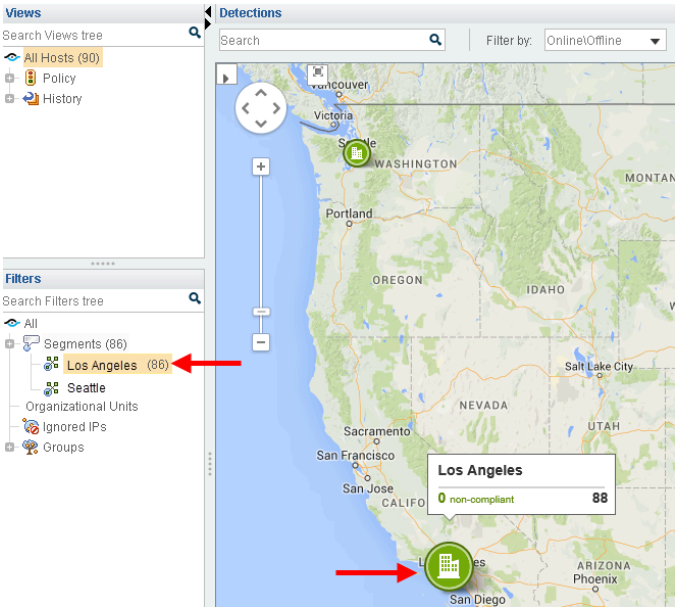


Filter the Forescout Console site map display

A set of powerful filtering tools let you quickly view items that interest you.

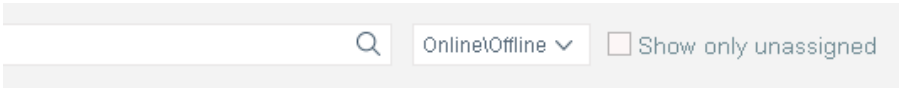
Group, segment and policy searches

These search options focus the map display based on location or segments and groups that you select in the Filters pane.



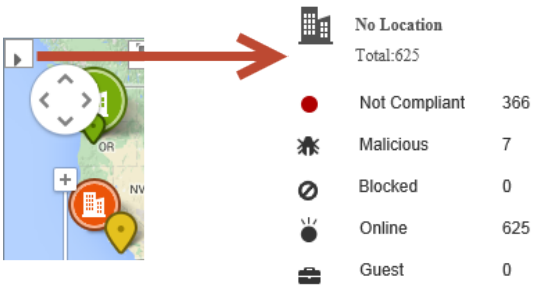
Filter by online/offline/unassigned endpoints

The default map filter lets you filter by online/offline or unassigned endpoints.



Display information about endpoints not assigned to a location on the Forescout Console site map

You can easily view information about endpoints that have not been assigned to a location. Site locations are defined in Tools > Options > Maps > Locations. Select the No Location indicator to learn about these endpoints.



Add, remove, and reorganize columns in the Detections pane

Default columns appear in the Detections pane with basic endpoint property information. Additional information can be displayed by adding other columns. You can also remove columns if

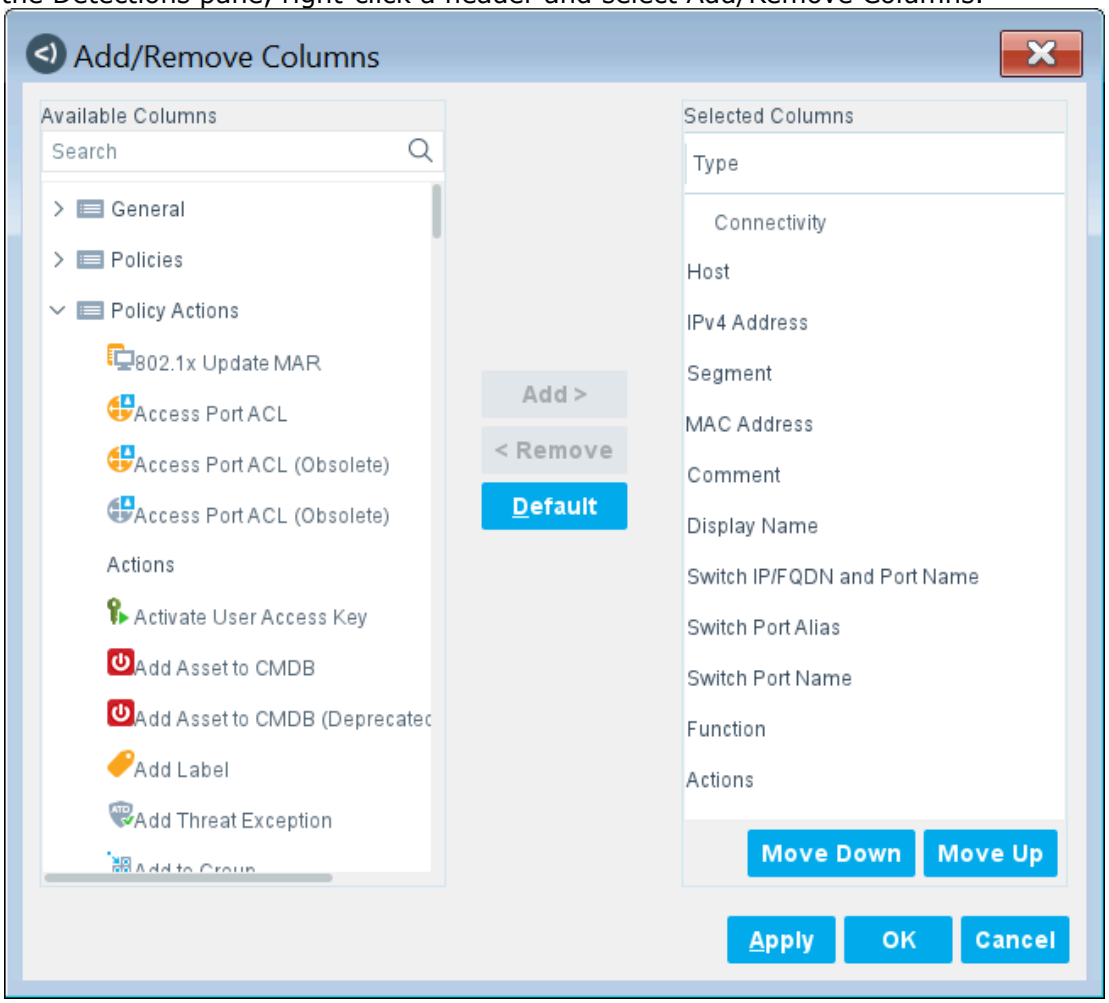
your screen becomes too busy.

Note:
The Host and Host IP columns are based on IPv4 and MAC information. When IPv6 addressable endpoints are supported in your environment, use the procedure described here to add columns for IPv6-related properties. See Device Information Properties. For Console settings to enable detection of MAC-only and IPv6-only endpoints, see Work with Hosts without IPv4 Addresses .

Note:
To remove columns directly from the Detections pane, right-click a column and select Remove Column.

To add, remove, and reorganize columns:

1. In the Detections pane, right-click a header and select Add/Remove Columns.



2. In the Available Columns list, select the columns that you want to add and then select Add.
3. In the Selected Columns list, select the columns that you want to remove and then select Remove.
4. The first column in the Selected Columns list is displayed in the leftmost position in the Detections pane. Use the Move Down and Move Up options to reorder the columns.
5. Select OK.

View the "Best Fit" for columns

You can improve the readability of the Detections pane by working with the Best Fit Column option. This feature automatically adjusts the selected column width to best display the column text. Right-click a column title and select Best Fit Column, or double-click the separator line in between columns.

Sort the columns

The columns can be sorted in ascending or descending alphabetical, chronological, or numerical order, as appropriate for each column. Click a column header to sort the table content according to its values. A triangle at the top of the column indicates the sorting order (downward for descending, upward for ascending).

Export Detections pane data

You can export Detections pane data or sections of it to a CSV file.

To export data:

1. Select Export Current Table from the Reports menu, or right-click an endpoint and select Export Table.
2. Complete the following fields:

File name	The name of the export file. Select Browse to navigate to the location where you want to save the file.
File type	The format in which data is exported.
Selected rows only	Select this option to only export data for the rows you selected in the table.
Displayed columns only	Select this option to only export data columns shown in the table.

3. Select OK.

Start actions on selected endpoints

You can perform actions on endpoints displayed in the Detections pane. For example:

- Send email, balloon messages or HTTP messages to operators, administrators and network users
- Block or quarantine endpoints to a VLAN
- Prevent access to the Internet
- Kill a process, peer-to-peer application, or instant messaging application
- Force authentication to the network

See Working with Actions for details about all actions.

To start an action:

1. Right-click an endpoint in the Detections pane.
2. Select an action category and sub-category, and then select an action.

Note:
If you installed plugins or modules, related actions are available. For example, if you installed the VPN Concentrator Plugin, VPN related actions are included.

Cancel actions on selected endpoints

You can manually cancel actions currently carried out on detected endpoints. The action remains canceled until it is unmatched from a policy and then re-matched, or until it is removed from a policy definition or stopped. You can select several endpoints and cancel actions simultaneously.

To cancel actions, right-click the endpoint in the Detections pane, and then select Cancel Actions.

Can all action types be canceled?

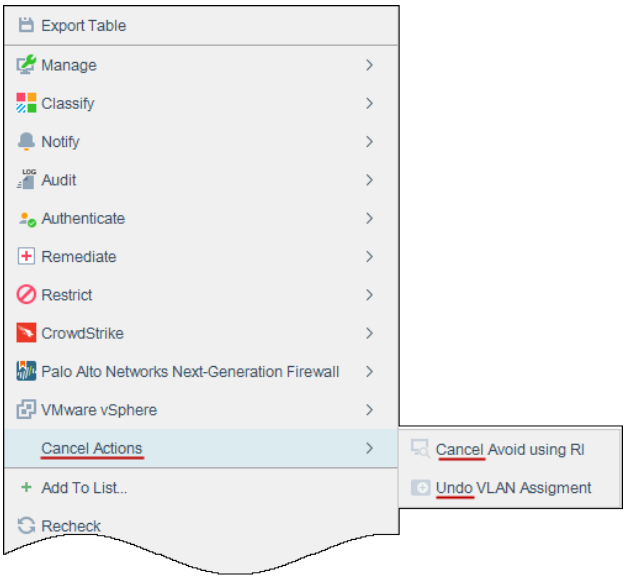
Only continuous actions can be manually canceled. Continuous actions have continued impact on the endpoint. For example, the Assign to VLAN action keeps endpoints in a specific VLAN.

Note:
An exception to this is the Add to Group action.

One-time actions have temporary impact on the endpoint until they are carried out again, for example, the Send Email action or the HTTP redirection action. One-time actions cannot be manually canceled once they are carried out. If you incorporated an action in an Action Schedule, you can perform the manual cancel on a one-time action.

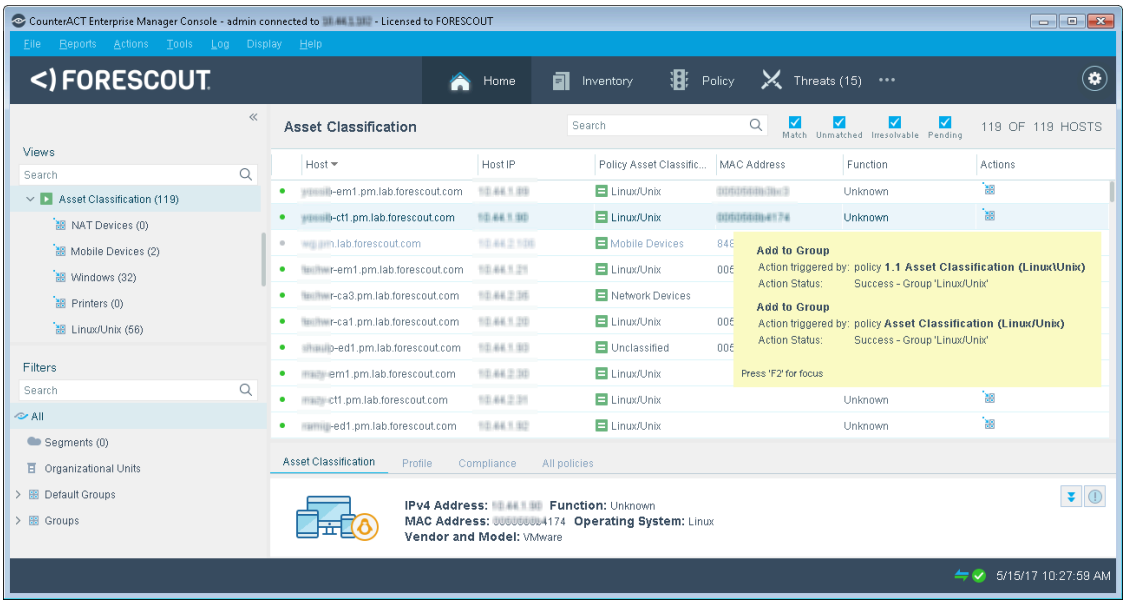
How do you know if an action can be canceled?

Right-click the endpoint in the Detections pane, and check to see if the action appears when you select Cancel Actions.



How do I know how an action was applied?

The Action tooltip displays information about how the action was applied or stopped.



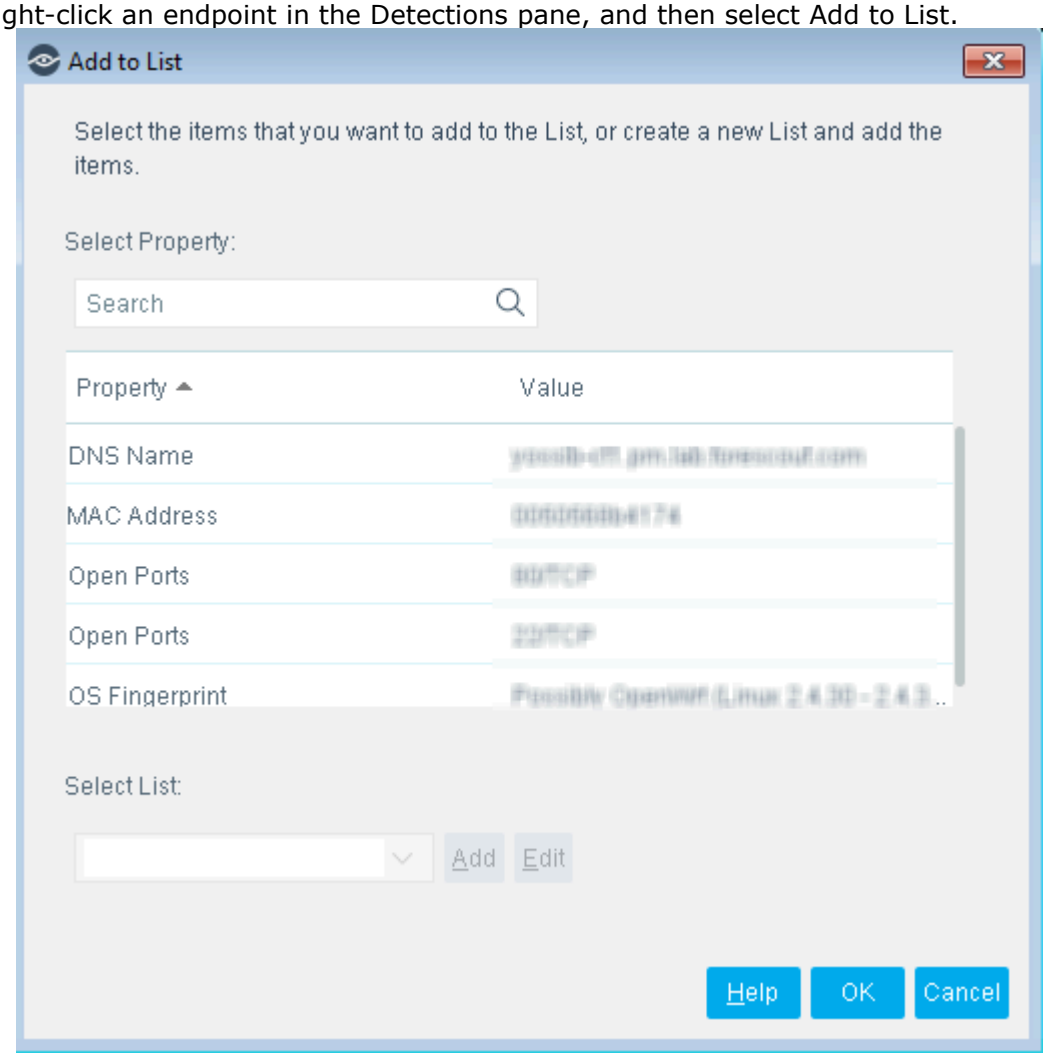
Add endpoint properties to a list

You can select an endpoint and add the properties detected on it to a property List. For example, a list of services or MAC addresses.

Use Lists to create powerful policies. For example, add a prohibited service to a service blacklist and then create a policy that uses the list to detect the service at endpoints.

To add endpoint properties:

1. Right-click an endpoint in the Detections pane, and then select Add to List.



2. Select the properties that you want to add to the list.
3. Select a list in which to add the properties or create a new list.
4. Select OK.

Additional controls

Additional controls are also available from the Detections pane.

Exception	Excludes selected endpoints from policy inspection. See Create Policy Endpoint Exceptions for details.
Delete	Releases the endpoint from any action taken. If the endpoint is detected and at the next recheck matches the policy, the action is applied again.
Recheck	Rechecks the endpoint for policy detections. Options are available to recheck a single endpoint for a particular policy or recheck the endpoint for all

policies. You can also recheck multiple endpoints simultaneously.

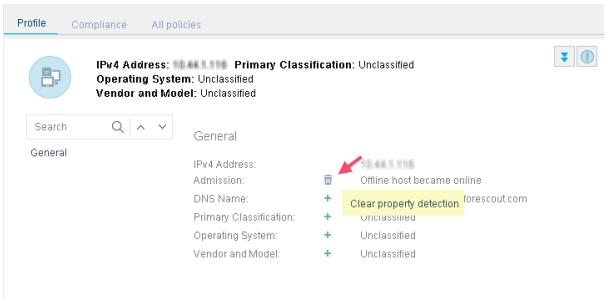
Clear Detection

Clear Event property detections, for example, admission or authentication login events.

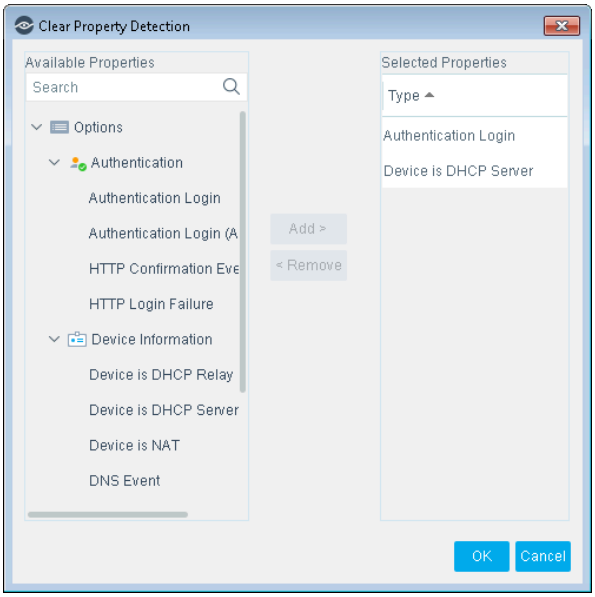
This action cancels any actions assigned to the endpoint as a result of the detection. You may need to clear event detections for troubleshooting purposes.

Two options are available for clearing detections:

- Clear a single event from the Console Details pane > Profile tab.
- Clear several events by right-clicking an endpoint, selecting Clear Detection, and then selecting the events that you want to clear.



- Clear several events by right-clicking an endpoint, selecting Clear Detection, and then selecting the events that you want to clear.



	The dialog box displays all endpoint events, regardless of whether they were detected on the endpoint. The Event Viewer and Audit Trail maintain information about cleared events. See Generating Reports and Logs for details. Events can also be cleared from the Assets Portal. See Assets Portal for details.
Comment	Makes endpoint management easier with user-defined comments. Create a comment by right-clicking an endpoint or group of endpoints, and then use the search box to look for endpoints with the comment text or create a policy that detects endpoints based on your comment. Special characters such as `~!@#$%^&=*()+[]\;'/{}|:"? are not allowed in the comment field and are removed if entered. The comment is retained for the life of the endpoint in the Console. Use the Device Information > Comment property to create a policy that detects endpoints with a comment. See Device Information Properties for details.

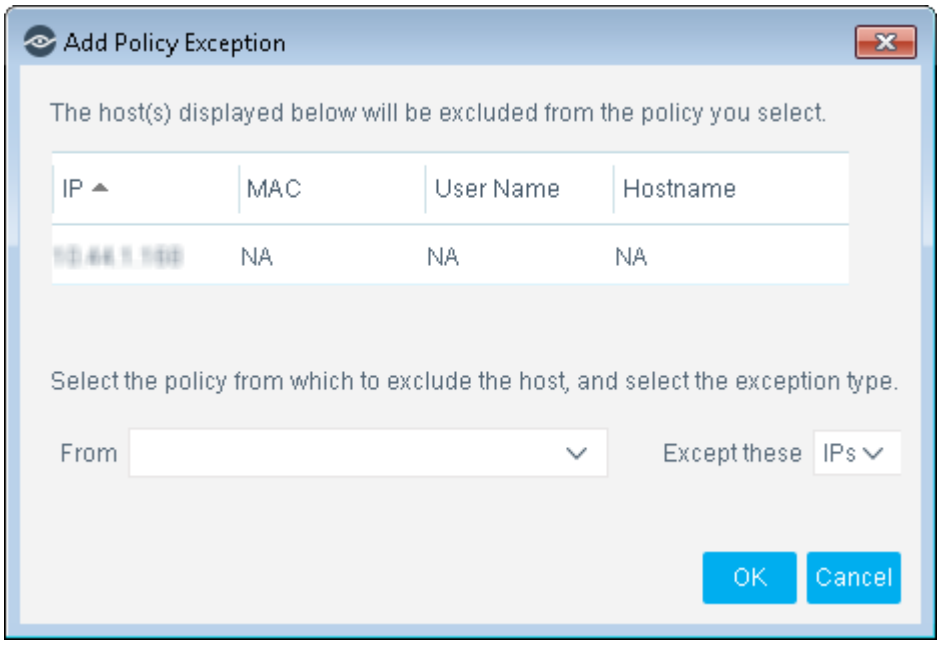
Create policy endpoint exceptions

You can select endpoints in the Detections pane and exempt them from further inspection for the policy that detected them. The exceptions that you create here are added to the policy's Exceptions parameters.

If you add an endpoint as an exception while it is blocked or redirected, that endpoint is immediately released.

To create exceptions:

1. In the Detections pane, right-click an endpoint or group of endpoints and select Exceptions > Add Policy Exception. The selected endpoints are listed in the Add Policy Exception dialog box.



2. Select a policy or sub-rule from which to exclude the endpoint and define the exception type.
3. From the Except these drop-down menu, select the type of identifier to use in applying the exception. Options may include the IP address, host name, and MAC address or user name of the endpoint. Select the identifier that is least likely to change.
4. Select OK. The specified endpoints are exempt from further inspection for this policy. Blocking actions taken are released. Non-blocking actions, such as Add to Group, Send email, and one-time HTTP actions are not stopped.

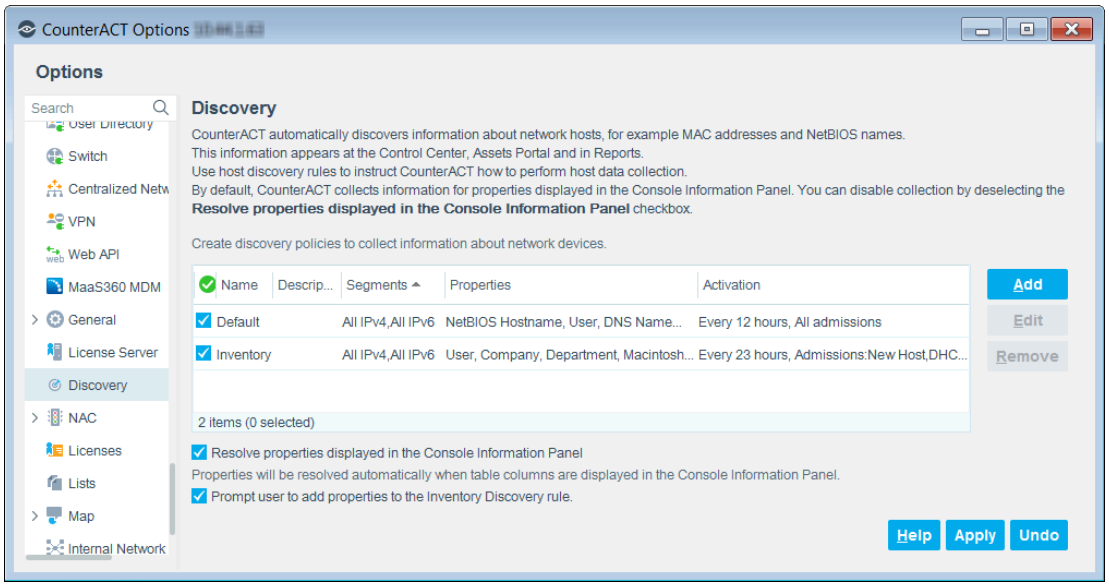
Inventory Discovery rules

Inventory Discovery, defined in the Discovery manager, instructs eyeSight eyeSight to discover the properties that you see in the Asset Inventory.

Note:
To ensure that these properties are discovered and displayed, you must enable Inventory Discovery.

To enable Inventory Discovery:

1. Select Tools > Options, and then select Discovery.



2. Enable the rules by selecting the Inventory checkbox.
3. Select Apply, and then select Close.

Note:

External Devices Connected and Microsoft Vulnerabilities are excluded from the Inventory rules by default. Discovery of these properties may generate extensive network traffic. You can include them, however, by updating the Inventory Discovery rules.

Note:

Open Ports can also be displayed in the inventory. This information is displayed by creating a policy that includes the Open Ports property. It is not learned from Inventory Discovery.

View and update discovered inventory

You can update inventory properties discovered, as well as IP address ranges included in the discovery, and the discovery activation frequency. The policy name cannot be edited.

To update the discovered inventory:

1. Select the Inventory entry from the Discovery manager, and then select Edit.
2. The Discovery Wizard opens. See Endpoint Discovery Rules for details about working with the wizard. If you clear a property in the Inventory Discovery rule but select it in another discovery rule, that property is included in the Asset Inventory. For example, if you clear the Windows Applications Installed option in the Inventory Discovery rule, but select it in another discovery rule, installed applications are displayed in the Asset Inventory view.

Note:

The user Audit Trails log displays changes made to the Inventory Discovery rule. See Monitoring User Activity for details about this log.

Detection policies

Inventory properties can also be discovered via your policies. For example, if you run a policy that detects running processes, the detected processes will appear in the Asset Inventory. Specifically, if you want to discover and display open ports in the Asset Inventory, you should

create a policy that detects these ports.

Create lists based on inventory detections

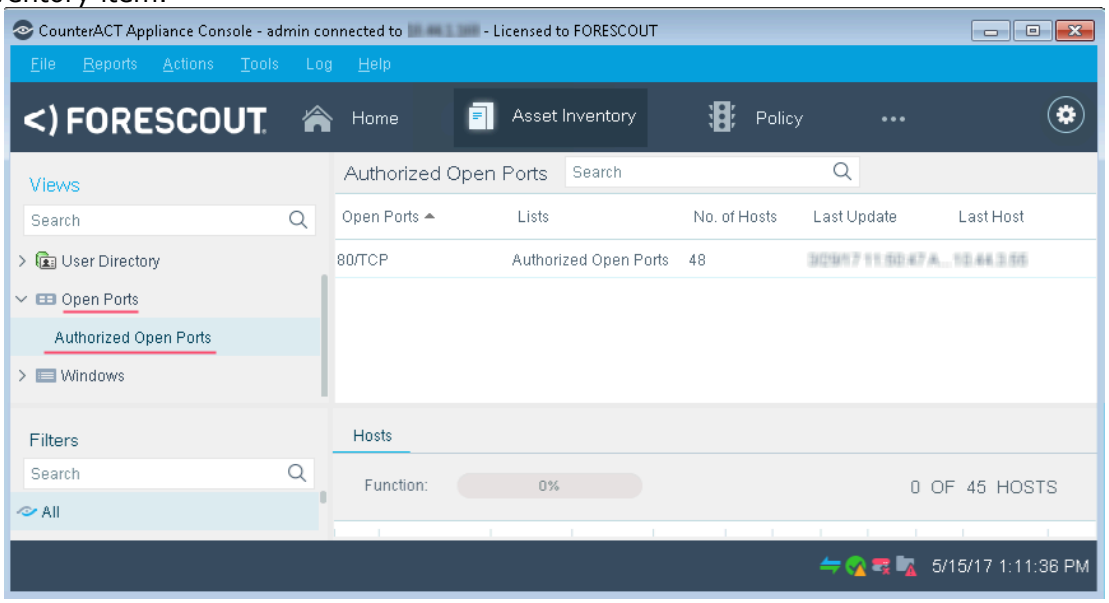
Create lists based on Inventory detections – for example, if you see that eyeSight eyeSight detected extensive authorized and unauthorized open ports, select the authorized ports and add them to an Authorized Open Ports list and then select the unauthorized ports and add them to an Unauthorized Open Ports list. You can create new lists or add the property values to an already existing list.

To create lists based on inventory detections:

1. Select an Asset Inventory category in the Views pane, for example, Open Ports.
2. Right-click one or more endpoints in the Detections pane, and then select Add to List.
3. Specify the following information for the list.

Select Property	The list indexes selected values of this property.
Select List	The name of the list. To append the property values of the selected endpoints to an existing list, select it from the drop-down. Select Add to define a new list. To modify an existing list, select it, then select Edit.

4. Select OK. The list is displayed in the Views pane when you select the parent Asset Inventory item.



Create lists ahead of time

You can create inventory lists for items that your network has not yet detected. This is useful if you know ahead of time that you want to be able to easily track specific types of activity or elements.

For example, if you do not want to work with specific open ports on your network. In this case, you may want to create blacklists of open ports. When endpoints start working with these ports, they will appear in the Detections pane > Lists column. Information about endpoints working with these ports is included in the Hosts Pane.

To create lists for a property:

1. Right-click a property folder in the Views pane, and then select Add List.
2. Specify the following information for the list:

List Name	The name of the list.
Description	This description is displayed in the Lists pane.
Values	A comma-separated list of index values for the property tracked by the list.

3. Select OK. The values you specified appear in the Asset Inventory under the folder that you created when they are detected on the network.

   The list and all the values that you entered can be viewed in the Lists pane.

View lists and values associated with an asset inventory item

You can view all lists and values that are associated with an Asset Inventory item. This information includes items that were manually added, as well as previously detected items that are currently offline.

To view lists, right-click an Asset Inventory folder and select View Lists. The Lists pane opens with all lists related to this item.

Edit and remove lists

Use the tools described here to edit and remove Lists. Changes affect both the Asset Inventory view and the Lists shown in the List pane.

You cannot remove lists that are currently used in policies. Such lists can be edited, but the changes may immediately affect the policy behavior.

- To remove a list, right-click a list in an Asset Inventory folder, and then select Remove List. Then select OK.

- To edit a list, right-click a list in an Asset Inventory folder and select Edit List. The List dialog box opens, showing all the values for the list. Edit as required, and then select OK.

Use inventory detections to create powerful policies

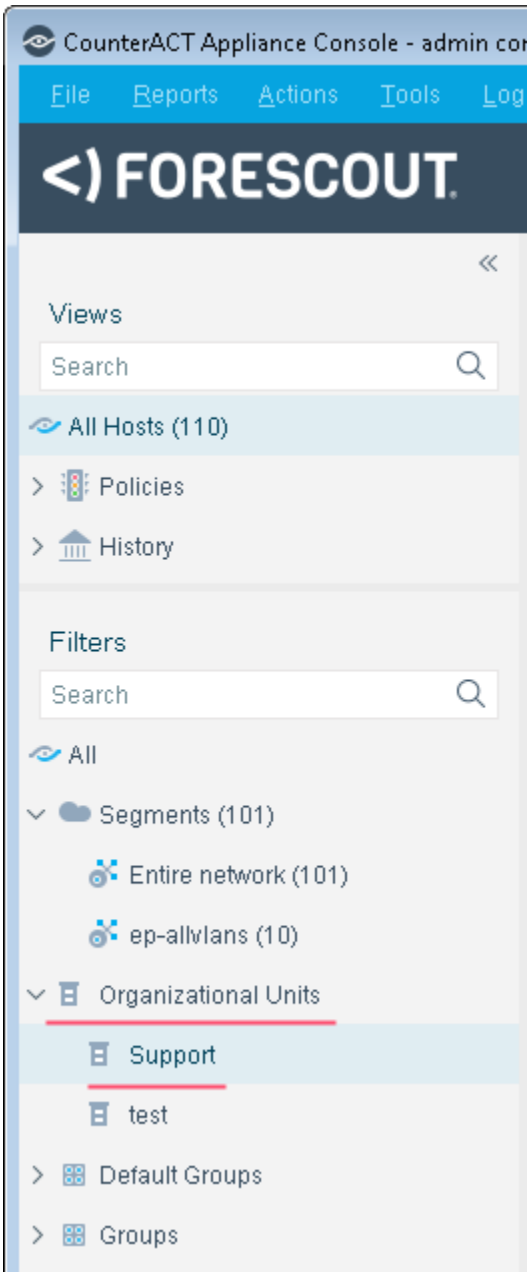
Incorporate inventory data into your policies. Specifically, use inventory items to create property *lists*, and incorporate lists into policy conditions by following these guidelines:

1. View activities displayed in the Asset Inventory of interest to you, for example, unauthorized services running.
2. Add the activity to a current list or create a new list. See Defining and Managing Lists for details.
3. Add the list to your policy and define the appropriate action. For example, create a policy that finds unauthorized services running and use the Send Email action to notify your IT team. See Use Your Custom Lists for details.

Work with organizational units

An organizational unit reflects a group of Forescout segments that have something in common. For example, the East, West and Central Management segments can be organized within the Management Organizational Unit.

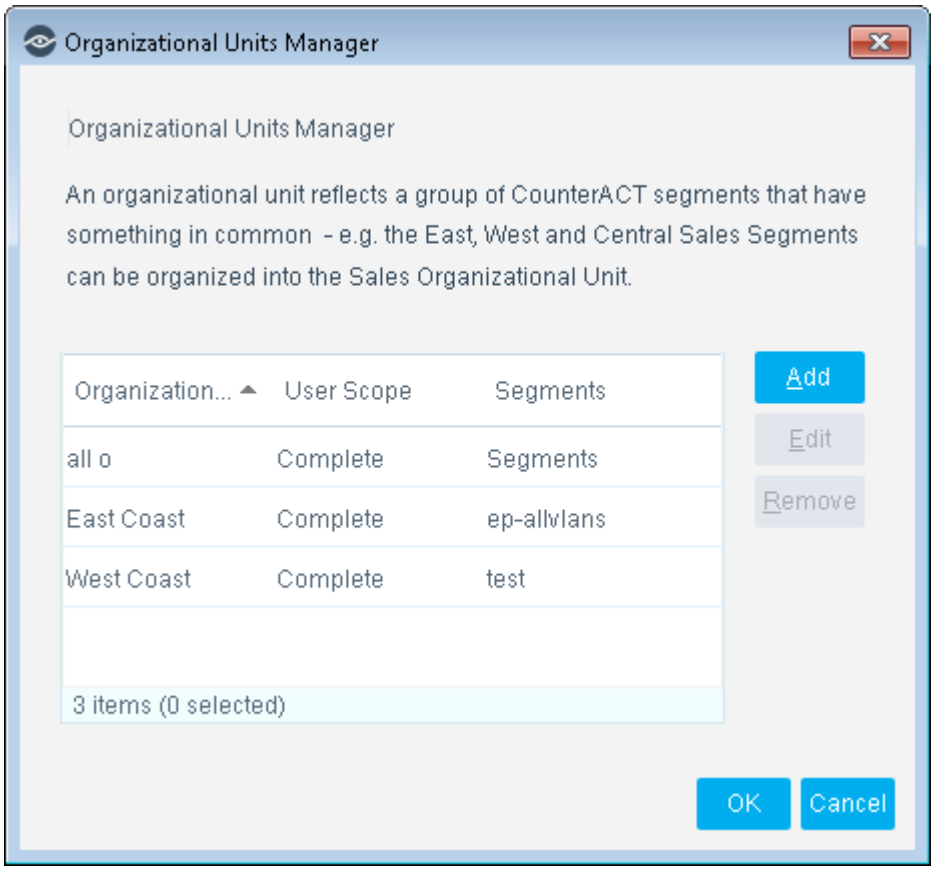
You can filter the view in the Detections pane according to a specific organizational unit. This makes it easier for you to locate problematic network areas.



You can add organizational units to reflect the structure of your organization.

To work with organizational units:

1. Right-click Organizational Units in the Filters pane, and then select Organizational Units Manager.



2. In the Organizational Units Manager:
   - Select Add to define a new organizational unit.
   - Select an existing organizational unit, then select Edit or Remove.
3. When you add or edit an organizational unit, specify the following information.

Name	The name of the organizational unit.
Description	A short description of this organizational unit.
Segments	The segments that are included in the organizational unit. When you Add a new organizational unit, open the tree and select segments. When you Edit an existing organizational unit, segments in the organizational unit are highlighted. Press the <Ctrl> key and select segments you want to include in the organizational unit.

4. Select OK. The Organizational Unit appears in the Filterso pane.

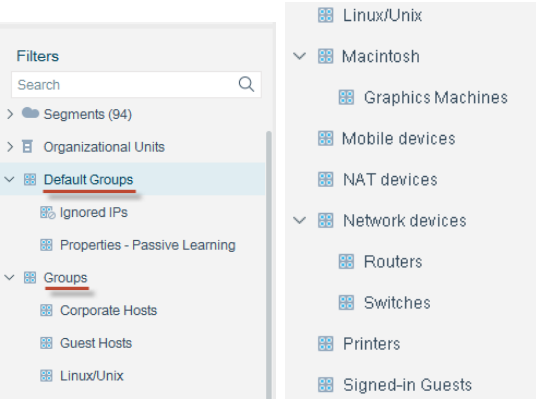
Work with Forescout Groups

A group is a collection of endpoints with something in common, for example, endpoints that run Windows operating systems or guest endpoints. Groups help you view and manage detections.

After you define groups and add endpoints to them, you can use the groups when specifying the scope of a policy. For example, if you create a Windows group, this definition is available when defining the scope or condition of a policy.

Groups are displayed in the Filters section of the Navigation pane.

The Console provides some default groups. For example, classification and corporate/guest groups may have been automatically created when your Console was set up. See Initial Setup Wizard – Policies for details. In addition, optional plugins and policy templates may create groups.



Groups exist in a hierarchy, with sub-groups inside parent groups. All endpoints in the sub-groups are included in the parent group.

Note:
For policy evaluation purposes, endpoints that belong to child groups are not members of the parent group by default; they are sub-members. Policies must check both the parent and child groups to see the endpoints within a child group.

To add endpoints to a group:

- Specify the MAC or IP addresses in Group Manager.
- Use the Add to Group action in a policy, or apply it from the Console's right-click menu.

When a group is used, for example, when a policy is evaluated that uses the group in its Scope definition, endpoints that currently have addresses in these ranges or lists are included in the group. Endpoints may not be included in the group later if their IP addresses change.

The Audit Trail reports provide information about users who have modified group definitions.

Not all users have access to the Group features. See Access to Console Tools – On-premises Permissions for details.

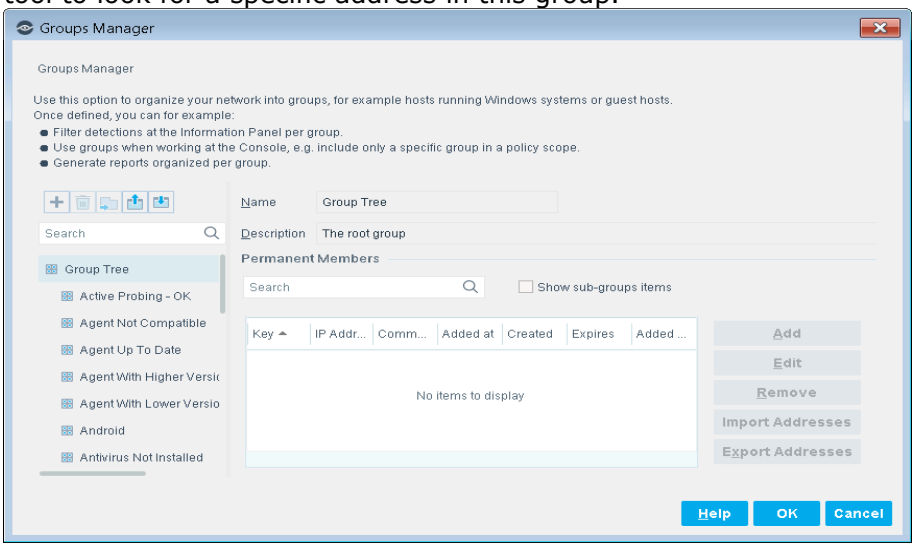
Work with the Group Manager

To view and manage groups in the Group Manager, do one of the following:

- Right-click a group node in the Filters pane in the Console and select Group Manager.
- Select Tools > Group Manager.

The Group Manager displays details for the selected node:

- The left pane shows the Group tree. Use the search tool in this pane to find existing groups.
- The right pane shows information for the selected group. The Permanent Members table lists IP addresses that are permanently assigned to the group. Select Show sub-group items to show MAC/IP addresses that this group inherits from its children. Use the search tool to look for a specific address in this group.



You can modify the group tree in the following ways:

	Add a group. You are prompted to name the new group and specify its location in the tree. The new group is created as a child of the selected node.
	Delete the selected group. If the group is used in a policy, you are informed, and the deletion is not allowed.
	Move the selected group and its children to another location in the tree. The selected group is moved under the new parent node that you specify. You can also drag and drop nodes of the tree. Moving groups in the tree can change the IP/MAC addresses they contribute to parent groups. This can change the endpoints that are referenced by the parent group.

	Select Export to save group definitions of the selected node and its children to a file. Select Import to create a new branch at the selected node based on definitions in a file. Group definitions are expressed in a structured XML file. You can also right-click a node in the Groups tree and select Export or Import

In the right pane, the table lists the following information for endpoints assigned to the group:

Key	The value by which the endpoint is associated with the group (IP address or MAC address) eyeSight eyeSight detects groups association based in this value.
IP Address	Displays the IP address if available. In the case of an address range, this field is blank.
Comment	The Comment text specified when the endpoint was added.
Added At	The timestamp of when the endpoint was added or the last time it was edited.
Created	Whether the endpoint was added manually or automatically using a policy.
Added By	The name of the Forescout user or policy that added the member.
Expires	Indicates whether the endpoint was added by a policy with the Expires when host no longer matches policy option, and is automatically removed from the group when it no longer meets the policy condition.

To add endpoints or ranges to the group, select Add. Specify endpoints in one of the following ways:

IP Range or Subnet	An IP address, address range, or subnet to include in the group.

MAC Addresses	A MAC address block definition to include in the group.

Import and export group members

You can use the Groups Manager to add or remove individual endpoints, or to define ranges of MAC/IP addresses that are included in the group. You can also import and export lists of group members.

To export group member details:

1. In the Groups Manager dialog box, right-click an entry in the table and select Export. An Export dialog box opens.
2. Choose the file location.
3. Choose a file format (CSV or PDF).
4. If you create a PDF file, you can set the title that appears in the file header.
5. Use the checkboxes to select the information that is exported. To import group member details:
6. In the Groups Manager dialog box, select a group. The table shows endpoints or MAC/IP addresses assigned to the group.
7. Select Import Addresses. The Import Group Members box opens.
8. Browse to a text file with IP/MAC addresses. Select Import. The addresses are added to the group.

Create an ignored IP address list

You can define endpoints that should be ignored by all Policies and Discovery rules, for example, a set of network servers that should not be included in inspection.

Note:
From eyeSight Version 8.4, the Forescout Admin (REST) API provides you with automatic configuration capabilities for managing deployments on the eyeSight, where network entities, such as the segment tree and default groups ranges, can change on a daily basis. The Admin API allows you to integrate third-party network management IPAM (IP Address Management) tools, such as Infoblox and BlueCat, and ensures that segments defined on the eyeSight are synchronized with their latest IPAM database definitions. For more information, see Work with the Forescout Admin API in the *Admin API Plugin Configuration Guide*.

To ignore endpoints for specific policies, create policy exceptions or narrow the policy scope.

Endpoints added to this group are included in Threat Protection and Virtual Firewall policy inspections.

You can filter the view in the Filters pane according to ignored IP addresses.

The following options are available for creating ignored IP addresses:

- Add individual endpoints or import lists of endpoints using the Ignored IP Manager. See Import and Export Group Members.
- By using the Add to Group feature. See Add to Group for details.

Restricting endpoint inspection

Forescout products use both passive and active methods to inspect and manage endpoints:

- Passive methods learn endpoint information from network devices, monitored traffic, or other data sources in your environment.
- Active methods include probing the endpoint for open ports, running Nmap against the endpoint, or any other attempt to establish a network connection to the endpoint.

Some devices, such as critical OT/IoT devices, can be adversely affected if eyeSight eyeSight repeatedly connects to resolve properties or run Nmap scans. This is referred to as active scanning. Assign these endpoints to the Properties - Passive Learning group to limit active scanning of specified endpoints or IP ranges. Forescout eyeSight never contacts endpoints in this group to resolve properties, even for policy evaluation. Properties that can be learned passively may be resolved for endpoints in this group, depending on available information.

Note:
When you assign an endpoint to the Properties – Passive Learning group based on its MAC address, Forescout eyeSight may apply active scan processes when it first detects the endpoint's IP address on the network, until it discovers the endpoint's MAC address.

Note:
Properties that cannot be learned passively, but require active scanning, will remain Irresolvable for endpoints in this group. This can impact policy evaluation. Review how Irresolvable conditions are handled in key policies that manage these endpoints.

Note:
From eyeSight Version 8.4, the Forescout Admin (REST) API provides you with automatic configuration capabilities for managing deployments on the eyeSight, where network entities, such as the segment tree and default groups ranges, can change on a daily basis. The Admin API allows you to integrate third-party network management IPAM (IP Address Management) tools, such as Infoblox and BlueCat, and ensures that segments defined on the eyeSight are synchronized with their latest IPAM database definitions. For more information, see Work with the Forescout Admin API in the *Admin API Plugin Configuration Guide*.

Note:
Since SecureConnector relies on a connection maintained from the endpoint to the eyeSight, properties resolved using SecureConnector continue to be resolved for these endpoints.

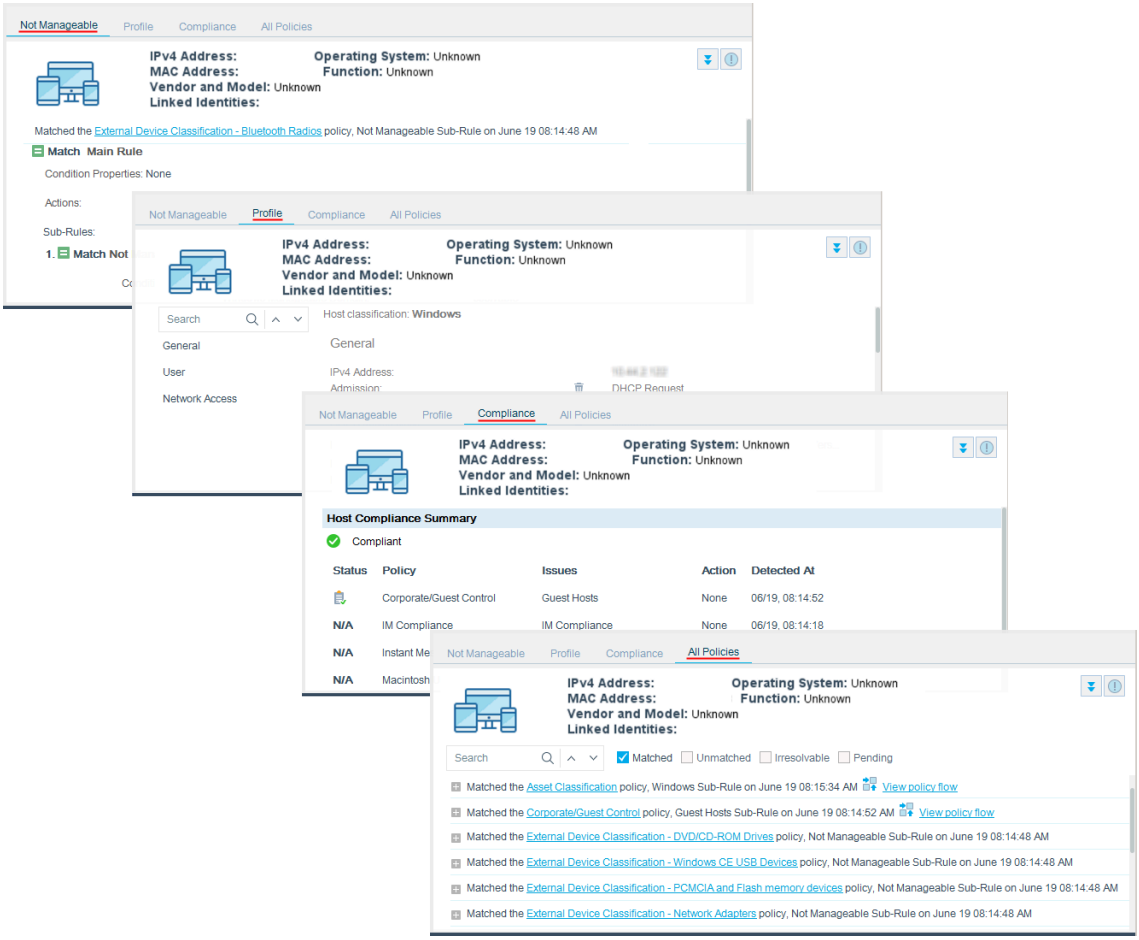
The following options are available for restricting inspection of endpoints:

- Add individual endpoints or import lists of endpoints using the Properties - Passive Learning group manager. See Import and Export Group Members.
- Apply the Add to Group action to endpoints that match policy conditions. See Add to Group for details.

If you are not sure which devices may be adversely impacted by active scanning, you can use the Passive Learning Mode template to discover and handle them. See Passive Learning Mode Template for details.

Details pane – display more endpoint information

The Details pane displays an extensive range of information about the endpoint selected in the Detections pane.



The following categories of information are available:

- Information about specific policies: Review matched and unmatched details or review information about why the endpoint was not inspected by a policy. This information is available when a policy is selected in the Views pane.
- Profile information: Review specific details about endpoint properties, for example, device identity information, switch information, Active Directory information.
- Compliance Information: Review a summary of endpoints' compliance status. The Forescout Compliance Center summarizes endpoints that comply or do not comply with policies that you have created. A single line indicates whether the endpoint is compliant. This line is followed by a table with a row for each compliance policy that includes the policy status, name, compliance issues, actions taken, original detection date, and last update time. To display the Forescout Compliance Center, you must categorize your policy as a Compliance policy in the Policy Manager. See Categorizing Policies for details.
- All policies information: Review matched and unmatched details for all the policies by which an endpoint was inspected, or review information about why the endpoint was not inspected in those policies. Select the View policy flow links to view a root cause analysis of each policy match. See Root Cause Analysis of Endpoint Policy Match.

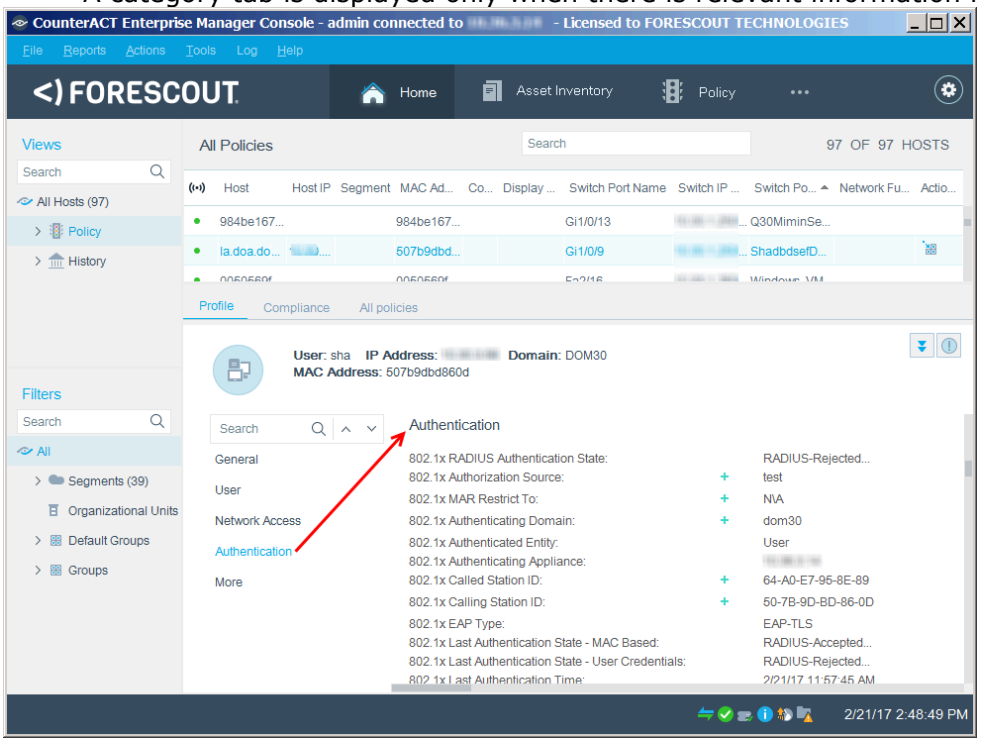
Note:
The "Linked Identities" field in the details pane appears only when an asset has a linked identity. If an asset has no links, this field will not be present.

Details pane tools

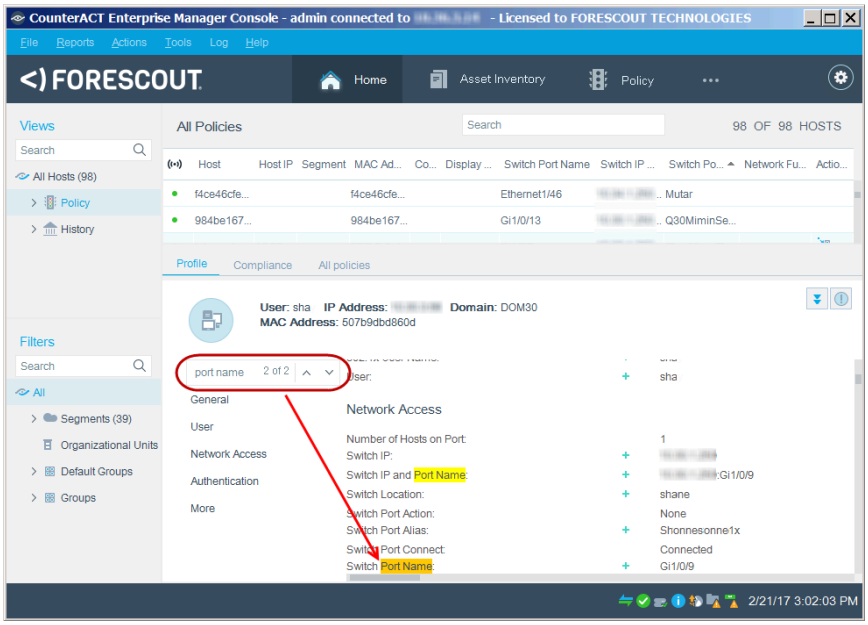
To toggle between details and summary, select (Show all details) from the pane.

Host attributes displayed in the Profile tab are arranged into logical categories. You can easily navigate between the different categories by selecting the category tabs at the left side of the pane.

Note:
A category tab is displayed only when there is relevant information for the selected host.

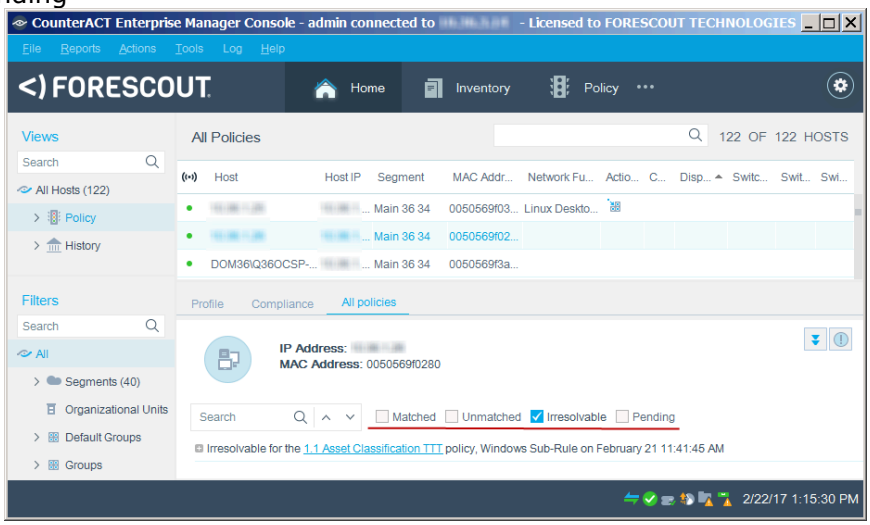


Use the Search option in the Profile tab and the All Policies tab to locate specific information. You can step through search results.



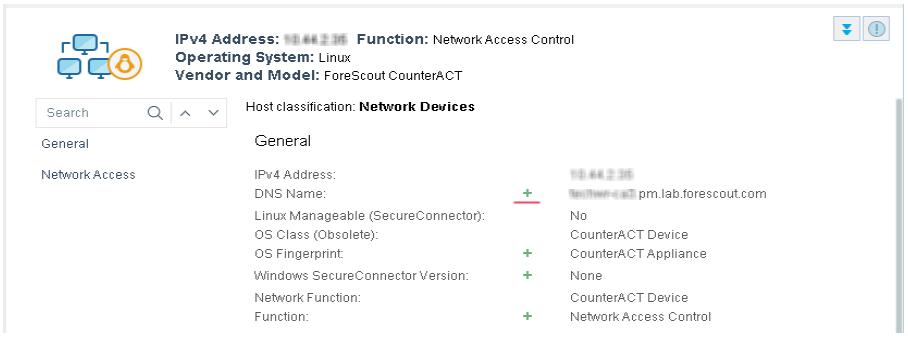
You can match the status of policy evaluation for the endpoint, such as:

- Matched
- Unmatched
- Irresolvable
- Pending



View troubleshooting information by selecting (Show troubleshooting messages). See Troubleshooting Messages for details.

Add a property to a List by selecting + in the Details pane.



Identity Model

Forescout detects when assets belong to the same host. This is important because different network interfaces, such as various IP or MAC addresses, might actually be from the same device. When Forescout identifies that assets are part of the same host, it links them together in a process called "linking and syncing."

Linking and syncing

Once assets are linked, their host properties are shared and synchronized. This means any new host property learned by one asset is automatically updated to its linked assets, providing a cohesive view of the network.

Assets are linked based on specific identifiers, each associated with a particular plugin and version:

Property	Plugin	Version Introduced
EC2 Instance ID	AWS	2.3.6
SCCM/ECM GUID	Microsoft SCCM/ECM	2.6.7
Intune Device ID	HPS Inspection Engine	11.3.13

If assets resolve the same value for an identifier, they are linked. Even if the required plugin version is not available, linking will still occur if both assets are managed by the same appliance.

Viewing linked assets

You can view linked assets by checking the host details of an asset, where a new field called "Linked Identities" is available.

Note:
The "Linked Identities" field in the details pane appears only when an asset has a linked identity. If an asset has no links, this field will not be present.

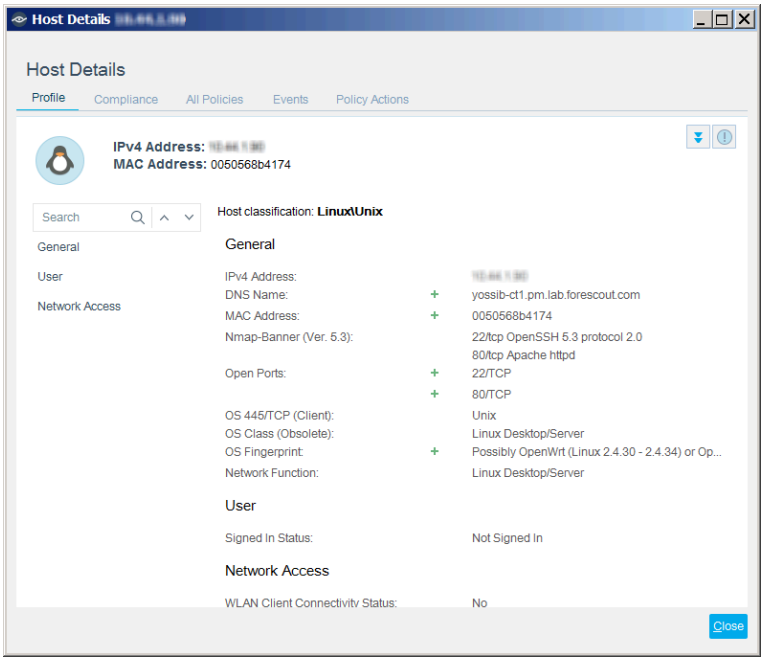
The Host Details dialog

The Host Details dialog box provides information about policy detections, endpoint properties, and details about actions carried out on detected endpoints. While you can view some of this information from the Console, the Host Details dialog box provides more details.

To view endpoint details, double-click the endpoint in the Detections pane. The Host Details dialog box appears.

Note:
To conserve space, host properties with unresolved, empty, or null values for this endpoint are not displayed.

Note:
Information in the Policy Actions tab can be exported. See Policy Action Log for details.

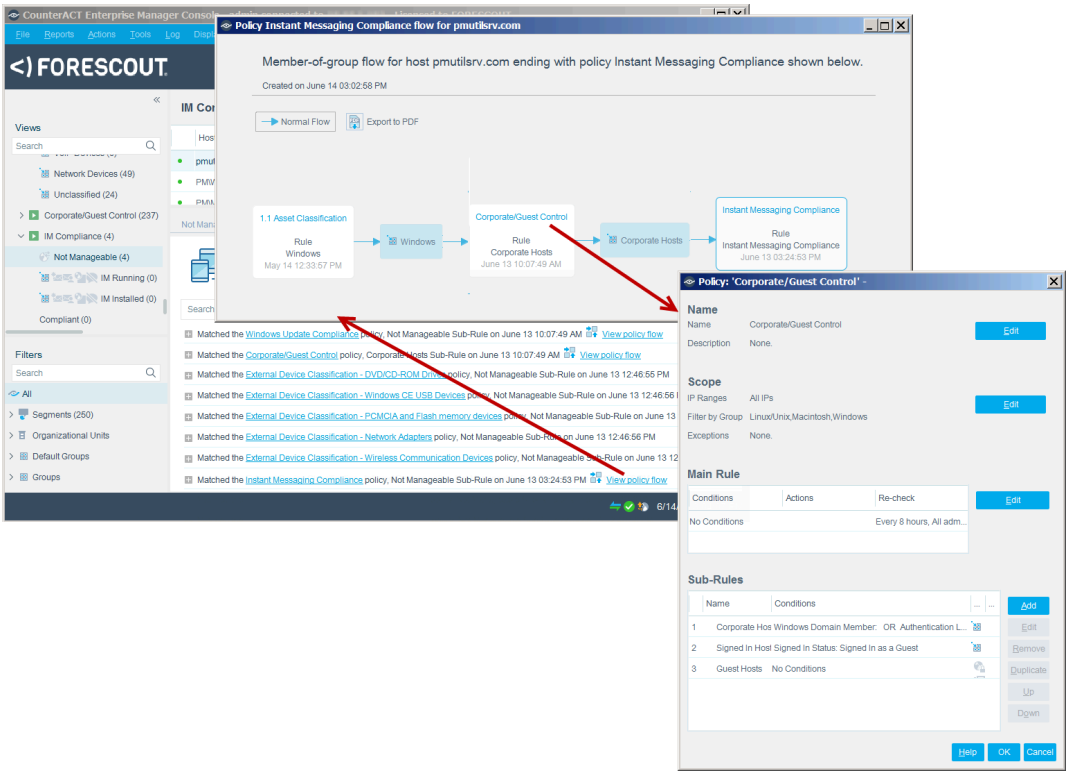


Root cause analysis of endpoint policy match

Quickly troubleshoot why a policy was run on a specific endpoint. This is useful if you want to investigate why a certain action, such as Assign to VLAN, was applied to a specific endpoint.

Quickly troubleshoot why a policy was run on a specific endpoint. This is useful if you want to investigate why a certain action, such as Assign to VLAN, was applied to a specific endpoint. The policy flow diagram shows the flow of policies by which the endpoint was added to a group by the preceding policy and is a member of a group that is a condition for the next policy.

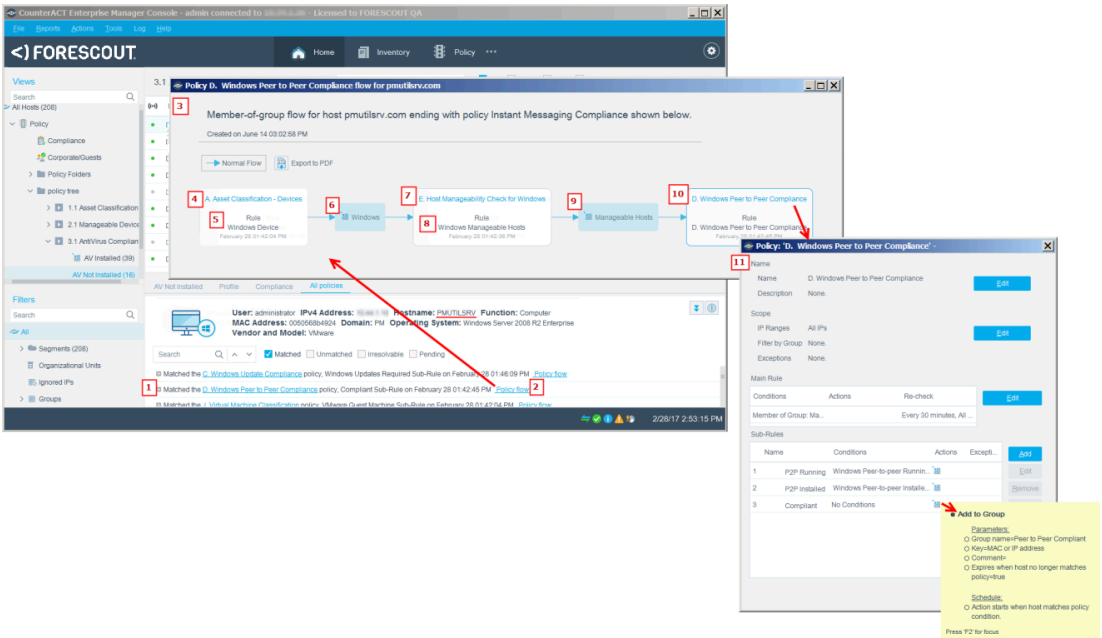
The policy flow diagram is accessed from the endpoint's specific policy tab or All Policies tab. You can double-click any policy in the diagram to view its details.



Policy flows are displayed only for policies that meet at least one of the following conditions:

- The policy was run due to the endpoint's membership in a group.
- The policy resulted in endpoint membership in a group.

For your convenience, the diagram can be saved in PDF format.



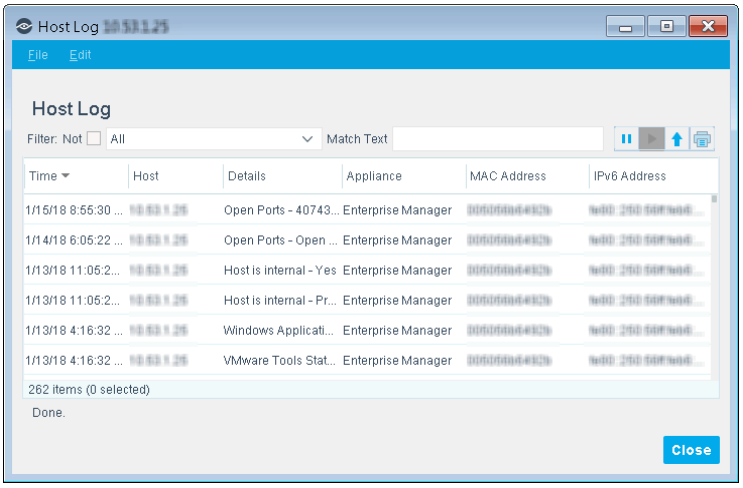
In the following example policy flow:

1. The All Policies tab indicates that host PMUTILSRV matched policy D. Windows Peer to Peer Compliance.
2. To see which group memberships triggered that policy to be run on that endpoint, select the Policy flow link.
3. A dialog box opens displaying the policies that put that endpoint into the group that triggered policy D. Windows Peer to Peer Compliance.
4. The first policy in the endpoint policy flow is A. Asset Classification – Devices.
5. This policy detected that the endpoint matched the Windows Device policy rule.
6. The resulting action added the endpoint to the group Windows.
7. Then policy E. Host Manageability Check for Windows was run because the endpoint was a member of the group named Windows.
8. This policy detected that the endpoint matched the Windows Manageable Hosts policy rule.
9. The resulting action added the endpoint to the group Manageable Hosts.
10. The final policy in the flow, D. Windows Peer to Peer Compliance, was run because the endpoint was a member of the group Manageable Hosts.
11. To view or edit the details of any of the policies in the policy flow, select the policy name link.

Host Log – investigate endpoint activity

Use the Host Log to investigate the activity of specific endpoints, and display information about how Forescout products handled those endpoints. The log displays information about endpoints as they are detected and is continuously updated.

You can display endpoints from a specific time period and IP address range. In addition, filter tools are available to limit the log display, for example, to specific policies or sub-rules. An option is also available to export the Log to an XML file.



The following information is available for each entry:

Appliance	The device that detected the event.
Details	The details of the event.

Host	The IPv4 address of the host.
IPv6 Address	The IPv6 address of the host.
MAC Address	The MAC address of the detected endpoint.
Non MAC host ID	[Not used in this version.]
Status	The status of the operations that have taken place. For example, if a policy action is complete, the status is OK.
Time	The time the event occurred.
Type/Name	The type of event. Use the filter option to control which event types are displayed. The name is basic information about the type.

The following filter options are available:

All	All log events.
Malicious	The sources detected via the Malicious Source Policy.
Only Changes	New, changed, or rechecked properties regarding the selected IP address ranges.
Policy	The name of the Network Integrity policy or sub-policy.
Property	Changes to Network Integrity Policy properties, for example, when authentication changes status.
System	Important Forescout system events, including Console/Enterprise Manager initialization time, Appliance status, plugin/module status (running or stopped), and changes in Appliance IP Assignments to Network Integrity Policies. Use the Event Viewer to review more detailed system event information. See Work with System Event Logs.

Work with the Host Log

To work with the Host Log:

1. Right-click an endpoint from the Detections pane, and then select Information>Host Log.
2. Enter a time range and then select OK.
3. (Optional) To modify the displayed information, click in the table header to add or remove columns.
4. To export this log data or sections of it to a CSV file:
   a. (Optional) Select rows to export.
   b. Select File>Export in the Export Table dialog.
   c. Complete the following fields:

File name	The name of the export file. Select Browse to navigate to the location where you want to save the file.
File type	The format in which data is exported.
Selected rows only	Select this option to only export data for the rows you selected in the table.
Displayed columns only	Select this option to only export data columns shown in the table.

   d. Select OK.

Work with the Forescout Compliance Center

The Forescout Compliance Center is an endpoint web-based compliance wizard used for the purpose of:

- Letting users log in.
- Bringing endpoints to network compliance.
- Informing users of their compliance level with respect to your corporate security policies.
- Offering users instructions for performing self-remediation by following links that you provide.

  Note:
  For the Forescout Compliance Center to be effective, the endpoint user must have SecureConnector installed on the endpoint device accessing the network. See Start SecureConnector / Stop SecureConnector for information about installing SecureConnector.

  Note:
  The Forescout Compliance Center is not accessible when HTTP Redirection is disabled. For more information, see Disable Web Portals .

The Forescout Compliance Center dialog box is displayed until the endpoint has successfully logged in and is compliant with selected policies.

Users can also manually open the compliance wizard from their endpoint to view their

compliance status.

Customize page design

The design of the Forescout Compliance Center may be customized. In addition to customizing the look and feel of the page (adding logos, images and text), you can also create a separate design for endpoints that are compliant and another design for endpoints that are not compliant. See Customizing HTTP Pages.

Using the Compliance Center vs. policies

The tasks carried out via the Host Compliance Center dialog box can also be carried out using policies. When using policies, many of the activities displayed in the Security Center are hidden from the endpoint user. For example, SecureConnector can be installed remotely and antivirus updates or compliance violations can be remediated without endpoint user interaction.

You should consider using the dialog box when you want to offload the task of maintaining compliance from your IT team, educate your users regarding security requirements at your organization, and force them to bring their machines into compliance. This may be useful, for example, at universities or organizations where guests may be required to self-remediate.

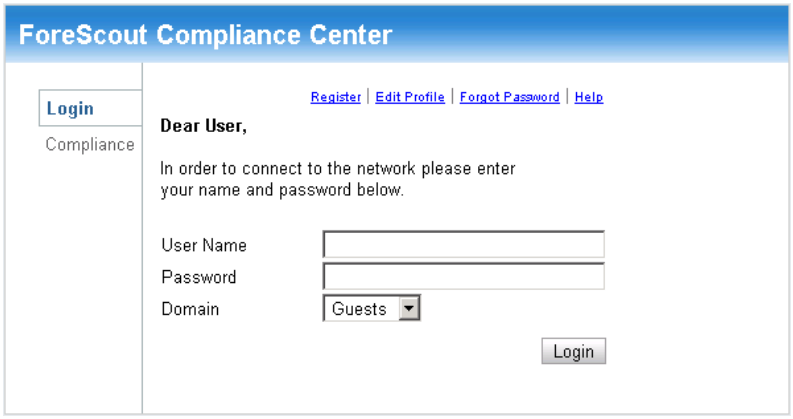
What endpoint users see

Users can access the Compliance Center from endpoints that run SecureConnector.

Hold the cursor over the Forescout icon in the system tray to view that endpoint's compliance status.

If there is noncompliance at the endpoint, Forescout eyeSight notifies the user. On the Windows Notification Bar at the bottom of the window, the Forescout icon is displayed as red. Placing the cursor over the icon, the endpoint details are displayed. For example:

Right-click the icon to open the Forescout Compliance Center dialog box. The Login tab prompts users to enter their login credentials to sign into your network. See the HTTP Login action for more information about when the Login tab is activated.



After users successfully sign in, the Compliance tab opens.

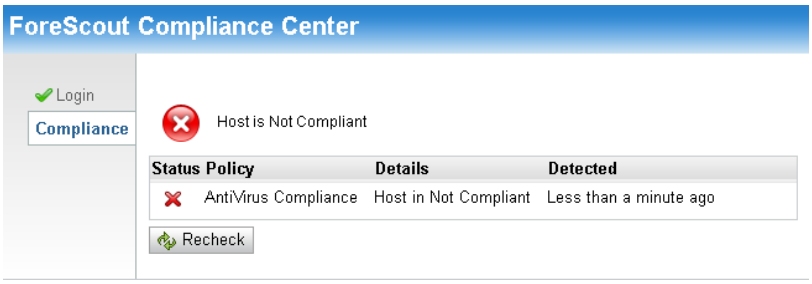
The Compliance tab:

- Assists you in downloading and installing SecureConnector.
- Assists you in achieving network compliance.

You can add comments to this tab by using the HTTP Notification action. Messages entered using these actions are also displayed in the tab.

Achieve Compliance

The Compliance tab displays the endpoint compliance status.



If there is any noncompliance with any policy, Host is Not Compliant is displayed. This indication refers to all policies that you run on the endpoint which are categorized as Compliance in the Policy Manager, as well as default Compliance template policies.

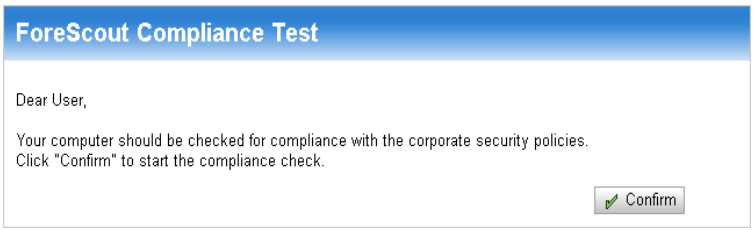
In addition, the Compliance tab can be used to display messages and links prompting noncompliant endpoints to become compliant by taking action, for example, by clicking a link that redirects end users to a site where they can download the latest antivirus application or to install patches.

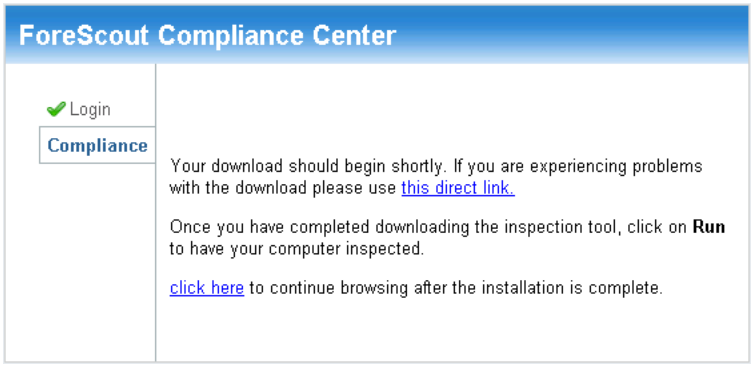
Users can select Recheck to verify their compliance status. All categorized policies are rechecked against the GUI Policy Editor options. Categorization is configured in the Policy Manager.

If the endpoint meets all the requirements of each of these policies, it is compliant, and Host is Compliant is displayed.

Install SecureConnector

If the endpoint is not managed by SecureConnector, the wizard prompts you to download and run SecureConnector. The following pages are displayed:





Policy Management

Forescout policies let you automate and simplify the intricate and time-consuming tasks involved in dealing with a multitude of events, users, vendors and devices; continuously changing downloads and patches; new vulnerabilities; extensive compliance requirements, and more. For example, policies can be used to:

- Pinpoint and quarantine endpoints that are working without antivirus software or that are not properly patched.
- Limit the network access available to guests and consultants.
- Enable automated detection of endpoints that are missing required Microsoft Service Packs and provide self-remediation tools.
- Verify that all mission critical servers are hardened according to the server hardening policy.
- Run scheduled vulnerability checks and automatic repair and protection mechanisms.
- Automatically discover and quarantine rogue wireless access points.
- Create admission control policies to determine who can access the network and under what conditions.
- Display important policy results in the *Dashboards* view, a web-based center that delivers dynamic at-a-glance information about network compliance, threats and guests.

Policies let you define instructions for automatically identifying, analyzing, and responding to a broad range of network activity for the purpose of bringing endpoints into policy compliance.

Specifically, you use policies to initiate endpoint inspection, specify conditions under which Forescout products should respond to endpoints, and define actions to perform at endpoints that match or do not match the policy requirements. You can define policies as simple as identifying missing laptops or more complex policies that control network access and VLAN assignment based on the organizational structure.

Note:
In addition to creating your own policies, you can also use policy templates – out-of-the-box templates that help you quickly create important policies based on predefined policy parameters. See Policy Templates for details.

How policies are structured

Policies are composed of the following elements:

- A unique policy name.
- A policy scope, for example, the endpoints that you want to inspect.
- Policy Conditions: Instructions to Forescout eyeSight regarding what properties to look for on endpoints. For example, detect endpoints running Windows XP and an outdated Symantec Antivirus application.
- Policy Actions: Measures to take at endpoints, if those properties or condition are either met or not met, for example, halt peer-to-peer applications, block Internet access, or notify endpoint users.

About templates for policy creation

The Console is delivered with ready-to-use templates. Using them helps you quickly create

commonly used policies.

About custom policy creation

Carry out extensive, deep inspection on endpoints by creating your own customized policies. Use the custom feature to create policies not covered by templates. See Create a Custom Policy.

Working with policy results

After running a policy, you can view detection information in the Home view, Detections pane. You can also manage policies from this location. See Control Endpoints from the Detections Pane for details.

Broaden the Scope – Plugins and eyeExtend Modules

The eyeSight platform is delivered with predefined policy detection criteria and actions. You can broaden the scope of these parameters, however, by integrating items that better correspond to your organizational and networking environment. This is accomplished by utilizing plugins and eyeExtend modules. For example, the Forescout eyeExtend for McAfee ePolicy Orchestrator lets you integrate with McAfee ePO, access related information, synchronize with related servers, and more.

See Base Modules, Content Modules, and eyeExtend Modules and refer to the relevant configuration guide for details.

Work with Forescout eyeSight policies

This topic describes basic information you need to know when working with policies and templates.

Note:
If registered with an Enterprise Manager, many Appliance policy settings are automatically replaced with the Enterprise Manager settings. See CounterACT Device Management Overview for details.

When Are Forescout eyeSight policies run?

By default, endpoints are inspected by policies every eight hours and on any admission event – a network event that indicates the admission of an endpoint into the network. For example, when it physically connects to a switch port, when its IP address changes, or when it sends out a DHCP request. For more information, see Admission-Based Activation in .Main Rule Advanced Options

You can define Scheduled Rechecks for a policy or for a specific sub-rule of the policy. For more information, see how to update a Policy Recheck in Main Rule Advanced Options and Sub-Rule Advanced Options.

Event Driven Monitoring

When SecureConnector is installed on an endpoint, it continuously monitors some host properties and reports changes in these properties. This triggers re-evaluation of all policies that include the changed host property. Event driven monitoring significantly reduces network traffic, provides the

most updated information without waiting for scheduled policy rechecks, and allows timely response to changes at the endpoint.

View detected endpoints in the Forescout Console

In the Views pane of Home view, open the Policies folder to view information about endpoints inspected by a policy. For example:

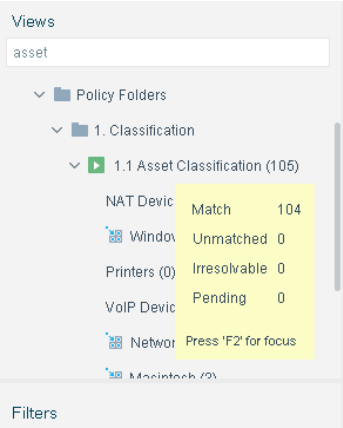
- Endpoints that match or do not match the policy, and the detection time.
- Actions taken at the endpoint. For example, if the endpoint was blocked or if access was prevented to the Internet.
- User directory information.
- Switch related information.

  Select a policy. The Detections pane lists relevant endpoint information.

  Endpoints appear in the policy-specific view until:

- Evaluation of the policy for the endpoint yields a different result.
- You remove the endpoint. Right-click the endpoint and select Delete.
- The policy is cleared. Right-click the policy and select Clear.

You can view a real-time compliance status summary for each policy. Policy status summaries are automatically updated in real time as the endpoint status changes. In the Views pane, move your cursor over a policy or right-click a policy and select Show Summary.



View detection information per group or segment

You can display detections associated with a specific network segment or group.

Groups are endpoints that have something in common – for example, endpoints that run Windows. Groups are defined by users or automatically created via policies. See Working with Forescout Groups for details.

Segments are network subdivisions created by users, for example, a finance department or East coast regional office. See Working with Forescout Segments for details.

Select a Segment or Group filter from the Filters pane of the Console. Endpoints associated with the group or segment are listed in the Detections pane.

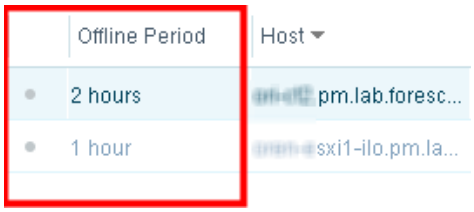
View detection information by endpoint status

In addition to viewing endpoints that match your policies, you can also view information about other endpoints detected, for example, endpoints that do not match a policy. These endpoints can be managed similarly.

To view detection information by endpoint status, select one of the following options:

Match	Endpoints that match the conditions defined in the policy.
Unmatched	Endpoints that do not match the conditions defined in the policy.
Pending	Endpoints in queue for inspection, according to policy activation definitions: According to the next scheduled inspection When an admission event is detected When the policy is manually run
Irresolvable	These endpoints were inspected, but Forescout eyeSight did not receive enough information to verify whether they matched the policy conditions. The endpoints are re-inspected according to activation definitions.
Online\Offline	Toggle between viewing only endpoints that are online or viewing both online and offline machines. The Detections pane includes a Connectivity column, which contains icons indicating the online or offline status of the endpoint. A tooltip provides details about when the endpoint was last seen. Offline endpoints are previously detected endpoints that are no longer connected to the network. If an endpoint is connected to a network switch that is managed by the Switch Plugin, Forescout eyeSight can discover that the endpoint is offline up to one minute after disconnection from the network. (default value) This time period can be changed in the Switch Advanced Settings dialog box, of the Switch Plugin. Use the Read – MACs connected to switch port and port properties (MAC address table) option. For more information, refer to the *Switch Plugin Configuration Guide*.

If an endpoint is not connected to a managed switch, eyeSight can discover that the endpoint is disconnected up to one hour after disconnection. You can change this time period. See Inactivity Timeout in Time settings for details.



To view this column:

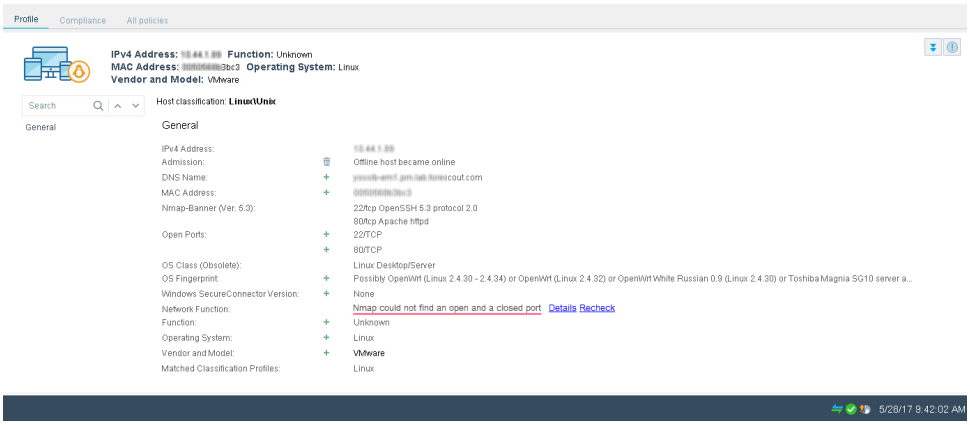
Right-click a column header and select Add/Remove columns. Select Offline Period from the dialog box that opens.

Show Only Unassigned

Displays endpoints that have not been assigned to an Appliance. Each endpoint in your network must be assigned to an Appliance. See Working with Appliance Folders for details.

Troubleshooting Forescout Console messages

Messages about irresolvable issues, failed actions, and other errors can be displayed in the Forescout Console. You can also open linked troubleshooting pages that offer suggestions for handling these issues.



To view troubleshooting messages:

- Select (Show troubleshooting messages), located at the top right corner of the Details pane, to toggle display of troubleshooting messages.
- In the Details pane, review the relevant troubleshooting information. Select the Detailsm link that appears after the text. The link may appear in any tab. A window opens with troubleshooting tips.

Using Forescout eyeSight groups

A group is a collection of endpoints with something in common, such as endpoints that run Windows or network guests. An endpoint can belong to any number of groups.

Organizing your endpoints into groups makes it easier to manage and analyze policies. For example, there is no need for a rule to detect operating system types or user types. These groups can be defined once and reused for various policies. Fewer rules mean simpler policies that are easier to prepare, monitor, and track.

In policies, groups can be used:

- To filter the scope of endpoints inspected by the policy.
- To define endpoints excluded from the policy (exceptions).
- As a policy condition: Automatically apply policies to predefined groups. For example, define a policy with the condition that endpoints are members of both the Windows group and the Norton Antivirus Installed group. The policy can then check whether the antivirus application is running and enable it if necessary. The Member of Group property is found in the Device Information property category.
- As a policy action: Automatically add endpoints to predefined groups based on certain conditions. For example, define policies that use the Nmap-OS Class property and the Add to Group action to organize your endpoints into groups called Windows, Linux, Macintosh, and Other.

An additional option automatically removes the endpoints from the group when the condition is no longer met. This keeps the group membership constantly updated. Consider the example where a policy places all endpoints with connected USB mass storage devices into a group called USB Attached. If someone removes the USB device from the endpoint, the policy automatically removes the endpoint from the USB Attached group.

Basic Forescout eyeSight policy rollout tips

Smart policies let you reliably and automatically handle an extensive range of network events and tasks. To make maximum use of a policy, you should define policies carefully. Do not create ineffective rules, for example:

- Conditions that can never occur.

  For example, when the activation mechanism is a new service and the condition for the service is 80/TCP and 139/ TCP.

- Actions that are not relevant to the condition.

  For example, assigning self-remediation actions for vulnerabilities on endpoints that were not inspected for vulnerabilities.

- Policies that are difficult to maintain.

  For example, if you create a rule that blocks endpoints that are missing antivirus installations, you should include an action that notifies the system administrator when such endpoints are detected.

- Policies that are too dynamic.

Groups, segments, and property lists may affect policies in such a way that the status of endpoints can be unintentionally changed. Verify that you do not set up overly complex policies using these features. Keep policies simple, and make sure that you have a clear idea of what kind of endpoints appear in each group, segment, and property list.

- Plan ahead when creating policies.

  Before you create a policy in the Console, decide upon general goals, reduce them to requirements, and then translate them into policies. For example, the goal 'control access of non-corporate users and devices to the network' can be broken down into the following requirements and policies:

  - Requirement 1: Restrict visitor access in conference rooms.

    Policy 1: In conference rooms, automatically limit access to non-corporate users (visitors), allowing them limited network access only while allowing full corporate network access to corporate employees.

  - Requirement 2: Restrict visitor access to the production network.

    Policy 2: When physically attempting to connect to the production network, non-authenticated users are denied access.

  - Requirement 3: Track down and remove rogue Wireless Access Points (WAP).

    Policy 3: Wireless Access Points are prohibited across all offices, including remote branches. Any discovered WAP must be automatically disconnected from the network.

- Test Your Policy

  You may want to create a policy and then test it before you start taking any action at endpoints in your network. You can do this by creating policies but not assigning any actions or by creating actions and disabling or enabling them during the testing period.

Forescout eyeSight policy priorities

The following hierarchies, from highest to lowest, are applied when an endpoint is detected as a result of different policies:

- Virtual Firewall – Allow Rule
- Threat Protection Policy – Threat Protection Blocked (host, port) and Virtual Firewall – Block Rule
- Group Definition – Authentication Servers (allow)
- Policy – Virtual Firewall Block
- Manually Block

How Forescout eyeSight handles endpoint identity changes

Policy detection mechanisms efficiently handle endpoint identity changes to ensure proper, transparent support in instances of IP address changes.

- Assigning a new IP to a detected host

Policy detection mechanisms recognize the reassignment of IP addresses on a specific endpoint via the endpoint MAC address or VPN user name. When such detections occur, all actions for the detected endpoint are transferred to the new IP address and canceled on the older address, thereby protecting the correct machine. The new IP address is updated in the Detections pane.

- IP transferred from one machine to another

  Under certain circumstances, a specific IP address detected on one machine is later discovered on a second machine. In such cases, all actions are released from the original machine, and no actions are applied to the second machine. However, Forescout eyeSight eyeSight activates Admission-based inspection for the IP address.

The following message is displayed in the Host Log when these changes occur:

```
IP Change: IP Changed from ...
```

You can customize the mechanism by which Forescout eyeSight recognizes and handles endpoint identity changes. For example, endpoint identity change can also be calculated for changing NetBIOS host names that are associated with specific IP addresses. See Policy Preferences for details.

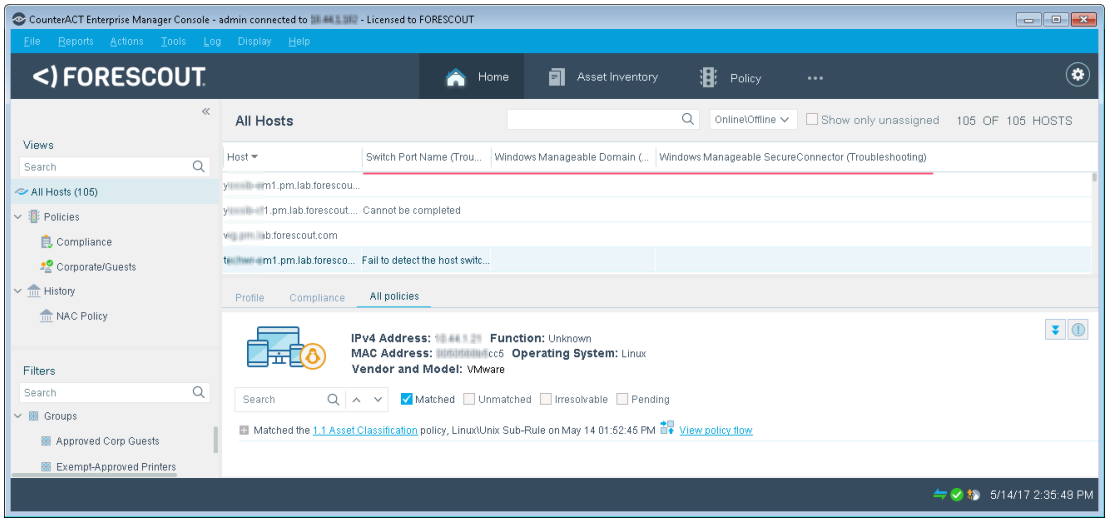
Stop a Forescout eyeSight policy from the appliance

If required, you can use the `fstool nphalt` command to stop the policy through the command-line interface (CLI). Using this tool stops the detection mechanism, releases blocked endpoints, and "undoes" other actions. You may need to use this tool if you cannot access your Forescout Consolep but need to stop the policy.

Quickly access Forescout eyeSight endpoints with troubleshooting issues

You can easily filter the Detections pane to display only those endpoints with troubleshooting issues.

1. Right-click a Detections pane column, and then select Add/Remove Columns.
2. In the Add/Remove columns dialog box, enter troubleshooting in the search field. Select the troubleshooting related columns you want to display.
3. Select OK. Filter and sort based on these columns to identify endpoints with troubleshooting issues.



Stop and start Forescout eyeSight policy Actions

You can stop and start specific actions that are applied by policy rules.

When you stop an action:

- Actions currently affecting endpoints are stopped.
- From now on, actions are not applied to endpoints that match the policy condition.

You may need to stop actions to test a policy before enforcing sanctions, i.e., only detect endpoints that match a policy.

When you stop or start actions for main policies, related sub-policy actions are also stopped or started.

One-time actions, such as email and HTTP redirection, can only be stopped if they are defined in Actions schedules.

To tell whether an action is stopped:

- Look at the action icon: Action icons are grayed out if stopped.
- Check the Start or Stop Rule Actions dialog box: Select the policy or sub-policy, and then select Stop Policy Actions or Start Policy Actions to see the stopped and started actions.

To stop or start an action:

1. In the Views pane of Home view, right-click a policy or sub-rule in the Policies folder, and then select Stop Policy Actions or Start Policy Actions. The Stop Action or Start Action dialog box opens.
2. Select the actions you want to stop or start.

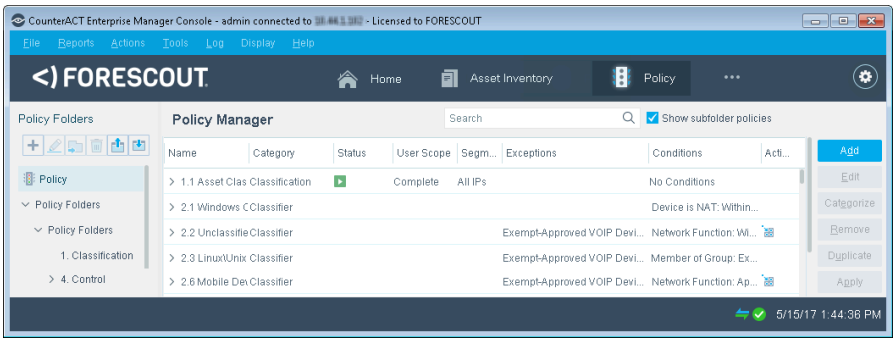
   Note:

   You can also edit the action definitions here.

The Forescout eyeSight policy manager

Define and manage policies from the Forescout eyeSight Policy Manager. Select the Policy tab to

work with the Policy Manager.



The following information can be displayed in the Policy Manager for each policy:

> (show sub-rules)	Toggle display of a policy's sub-rules.
Name	The name assigned to the policy.
Status	Indicates whether the Forescout eyeSight detection mechanism is paused or running. When paused, new detection events are ignored.
Category	The category assigned to the policy.
Dashboard Tags	The dashboard tag applied to a policy sub-rule. See Tag Sub-Rules for Dashboard Widgets for details.
Description	The policy description.
Conditions	The properties inspected on endpoints, i.e., specific OS systems, antivirus updates, registry information, etc.
Scope	The endpoints that are inspected for this policy.
Actions	Measures taken at the endpoint if it matches the policy.
Recheck	The conditions under which to recheck endpoints that match the policy. Specifically, you can define: How often endpoints are rechecked after they match a policy.

	Under what conditions to carry out the recheck.
Groups	Forescout groups included in the policy inspection. See Working with Forescout Groups for details.
Segments	The range of IP addresses to be inspected for the policy. See Define Policy Scope for details.
Exceptions	The range of IP addresses excluded from policy inspection.
User Scope	The range of endpoints a Forescout operator can view and work with. Complete: Indicates that the policy scope is within the user scope and the policy can be edited. Partial: Partial access is available. The policy can only be viewed. None: No access is available. The policy can only be viewed. See Access to Network Endpoints – Scope.
Path	The path to the policy (in the Policy Folders pane of the Policy Manager).

The Policy Manager provides the following tools:

Add	Create a new policy.
Edit	Edit an existing policy. You can also right-click a policy or sub-rule in the Policy Manager and select Quick Edit.
Remove	Remove a policy.
Duplicate	Duplicate a policy, and then edit as required.
Categorize	Categorize policies to help you organize and view them in the Policy Manager. For example, display only those policies labeled as Compliance policies. In addition, a Compliance folder and Corporate/Guests folder in the Views pane of the Console displays all policies according to their category.

	These categories are also used by: Forescout Compliance Center Dashboards (Device Compliance widgets) Site Map Compliance Status property Corporate/Guest Status property See Categorizing Policies for details.
Dashboard Tag	Apply dashboard tags to policy sub-rules to display matched devices in relevant Dashboard widgets. See Tag Sub-Rules for Dashboard Widgets for details.
Move to	Assign a policy to a folder. Folders are used to organize policies into logical groups for easier navigation and management in the Policy Manager. For example, create East Coast Finance and West Coast Finance folders and place the appropriate policies in those folders. These folders also appear in the Views pane in the Console. See Manage Policy Folders for details.
Stop	Stop the policy activation. When stopped, the detection mechanism is halted. Actions carried out on endpoints previously detected are maintained.
Start	Start the policy activation.
Export	Export policies of interest. Policies are exported as XML files.
Custom	Create custom reusable policy conditions. Select Custom from the Tools menu. See Authentication Properties for details.
Generate Policy Report	Generate a report listing all your policies and policy definitions.

	Select Policies Summary Report from the Reports menu.
Apply	Apply changes you made in Policy Manager. You must select Apply to save changes, for example, new policies you created.

Manage policy folders

Use the Policy Folders pane to organize your policies into logical folders for easier navigation and management. These folders appear in the Views pane of Home view.

The following tools are available in the Policy Folders pane:

>	Toggle display of the contents of a node in the Policy Folders tree.
	Add a folder as a child of the selected node. You can also right-click a node and select New Policy Folder.
	Delete the selected node. If you create and then delete a folder, any policies in the folder will also be deleted.
	Move the selected node its children to another location in the tree. The selected node is moved under the new parent node that you specify. You can also drag and drop nodes of the tree.
	Select Export to save segment definitions of the selected node and its children to a file. Select Import to create a new branch at the selected node based on definitions in a file. Segment definitions are expressed in a structured XML file, or in a CSV file that lists each segment definition. You can also right-click a node in the segment tree and select Export or Import.
	Select the Import icon from the Policy Folders pane or right-click in the Policy

Folders pane and select Import. Complete the fields in the Import Policy Folder dialog box, where:

- Target Node is the destination.
- Import Mode is the method used to import the policy folder, either as a sub-folder of the folder in the original location (Add folder to the target) or as a sub-folder of the target itself (Add folder content to the target).
- File name is the name of the policy to import.

By default, policies are imported as XML files.

If you import a policy that refers to groups not defined on the Appliance, these groups are automatically created however the groups will not contain any members.

If you import a policy with a segment that does not exist, you receive a warning message and the policy is imported without the segment.

When policy conditions or actions include login credentials for network devices, servers, or services, the exported policies are encrypted. When you export these policies, you are prompted for a password that is used to encrypt the exported file. When you import these properties, you are prompted for the password.

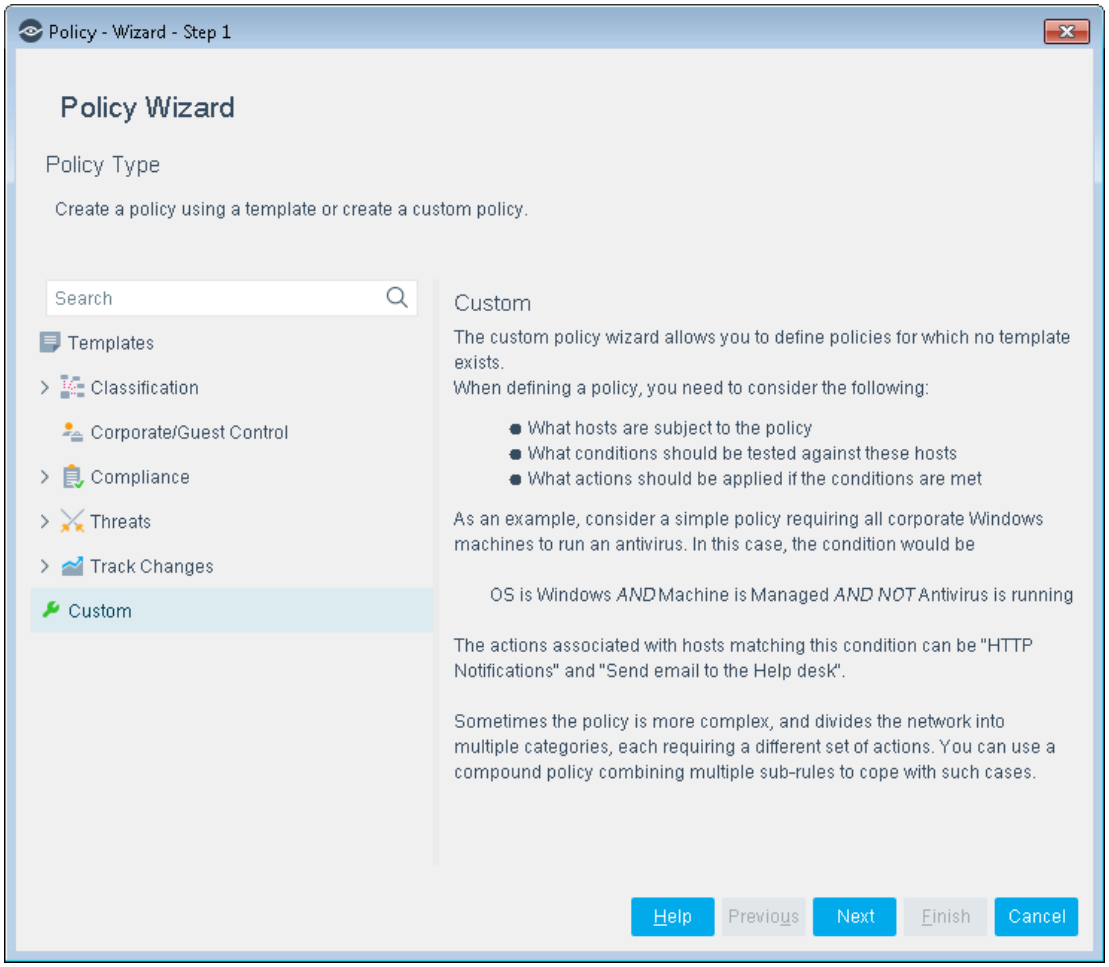
Create a Forescout eyeSight custom policy

You can create a Forescout eyeSight custom policy to deal with issues not covered in the policy templates. Custom policy tools provide you with an extensive range of options for detecting and handling endpoints.

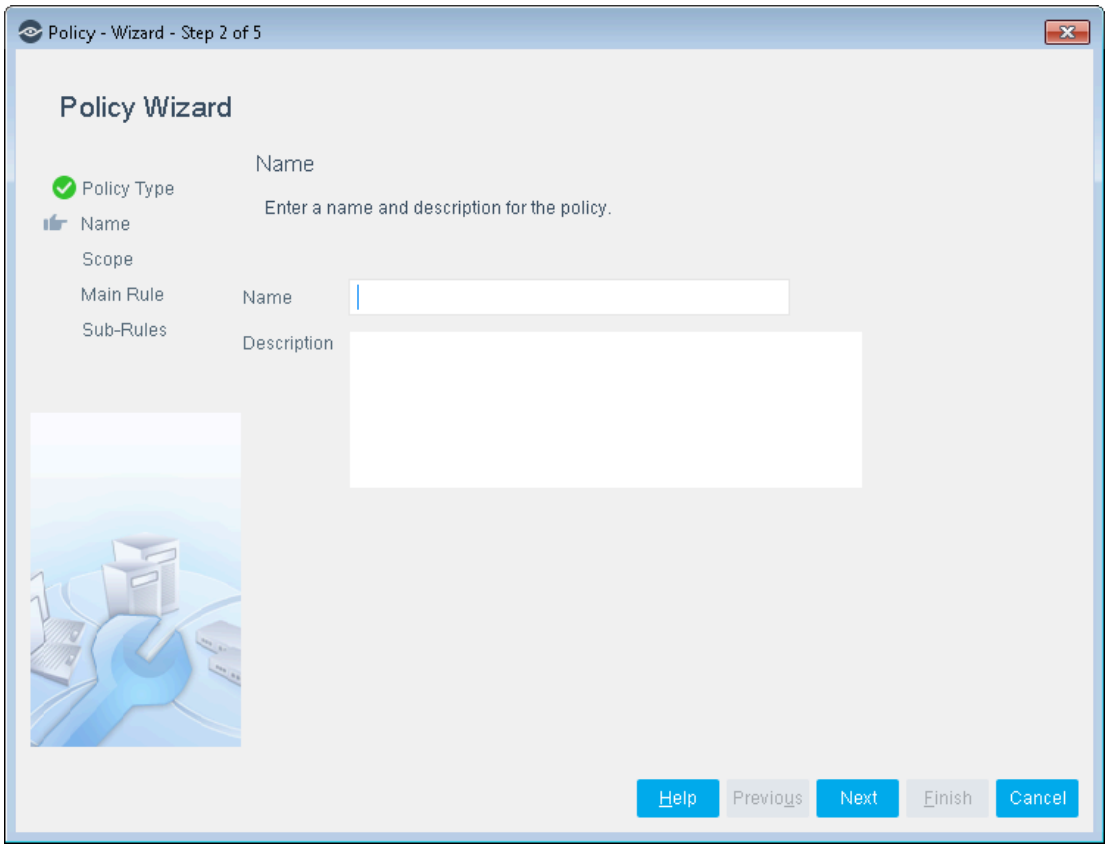
After the policy is created, it is displayed in the Policy Manager. To run the policy, select Apply from the Policy Manager.

To create a policy:

1. Select the Policy tab. The Policy Manager opens.
2. Select Add from the Policy Manager. The Policy Wizard opens.
3. Select Custom.



4. Select Next.



5. Define a unique policy name and useful policy description. Policy names appear in the Policy Manager, the Views pane, Reports and in other features. Precise names make working with policies and reports more efficient. See Policy Naming Tips for guidelines about creating effective names.
6. Select Next. The Scope pane opens. Define a general range of endpoints to be inspected for this policy. See Define Policy Scope.
7. Select Next. The Main Rule pane opens. See Defining a Policy Main Rule.
8. Select Next. The Sub-Rules dialog box opens. Use this dialog box to review and update Main Rule definitions and advanced policy settings, as well as to define sub-rules. See Defining Policy Sub-Rules.
9. Review the sub-rule conditions and actions, and then select Finish.

Policy naming tips

Policy names need to clearly reflect what the policy does. For example, do not use a generic name such as Antivirus.

In this example, use a more descriptive name that indicates that your policy is checking antivirus updates and which vendors are authorized.

You should avoid having another policy with a similar name. In addition, ensure that the name indicates whether the policy criteria must be met or not met.

Examples:

Name	Improved Name
Antivirus S	Symantec Antivirus Not Updated at Seattle Site
Antivirus S/M/I	Symantec/McAfee Antivirus is Not Installed at Seattle Site
P2P	Inform, then Restrict Web Access on Peer-to-Peer Detections n

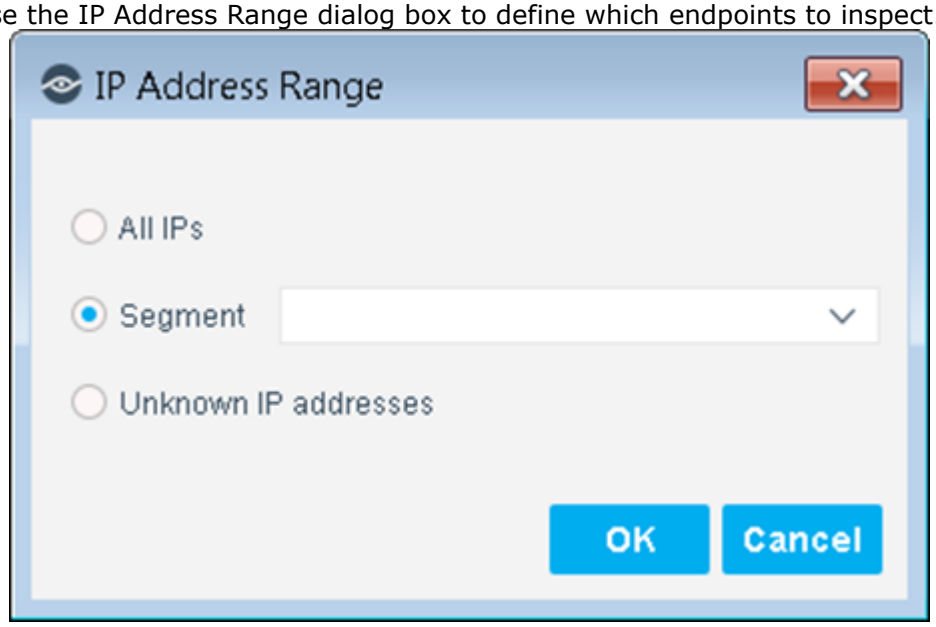
Define policy scope

Define a general range of endpoints for this policy to inspect. You can filter this range by:

- Including only certain Forescout groups, such as endpoints that run Windows. Use this option to pinpoint endpoint inspection.
- Excluding devices or users that should be ignored when using a policy, for example, VIP users running Windows.

To define policy scope:

1. Use the IP Address Range dialog box to define which endpoints to inspect.



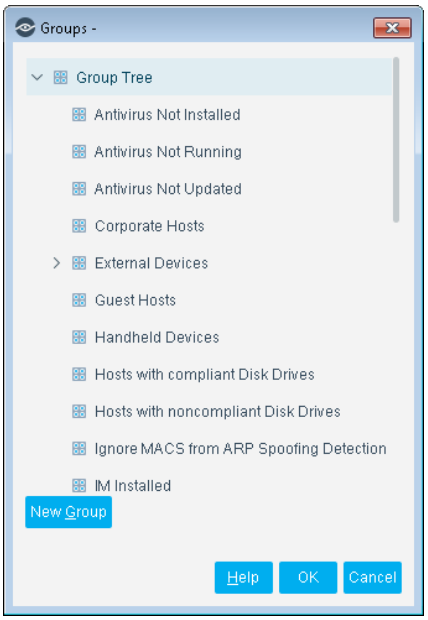
The following options are available:

- All IPs: Include all IP addresses in the Internal Network.
- Segment: Select a previously defined segment of the network. To specify multiple segments, select OK or Cancel to close this dialog box, and then select Segments from the Scope pane.
- Unknown IP addresses: Apply the policy to endpoints whose IP addresses are not known. Endpoint detection is based on the endpoint MAC address.

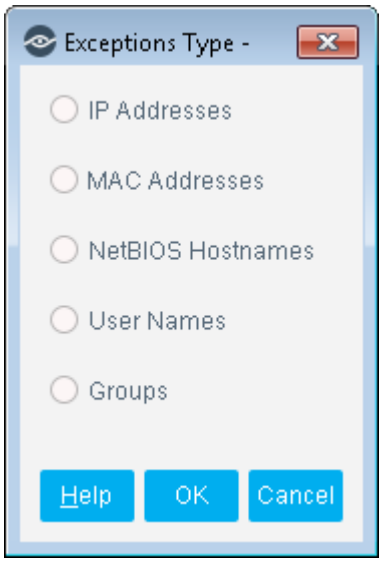
For more information about the detection of MAC-only endpoints, see Work with Hosts without IPv4 Addresses.

2. Select OK.
3. Select Advanced to fine-tune the scope. Two options are available:
    - Only include some Forescout groups in the inspection. If you select several groups, and an endpoint is detected in at least one, that endpoint is included in the policy inspection.
    - Select Add from the Filter by Group area to include only specified Forescout groups in the inspection. These groups must be part of the Internal Range.

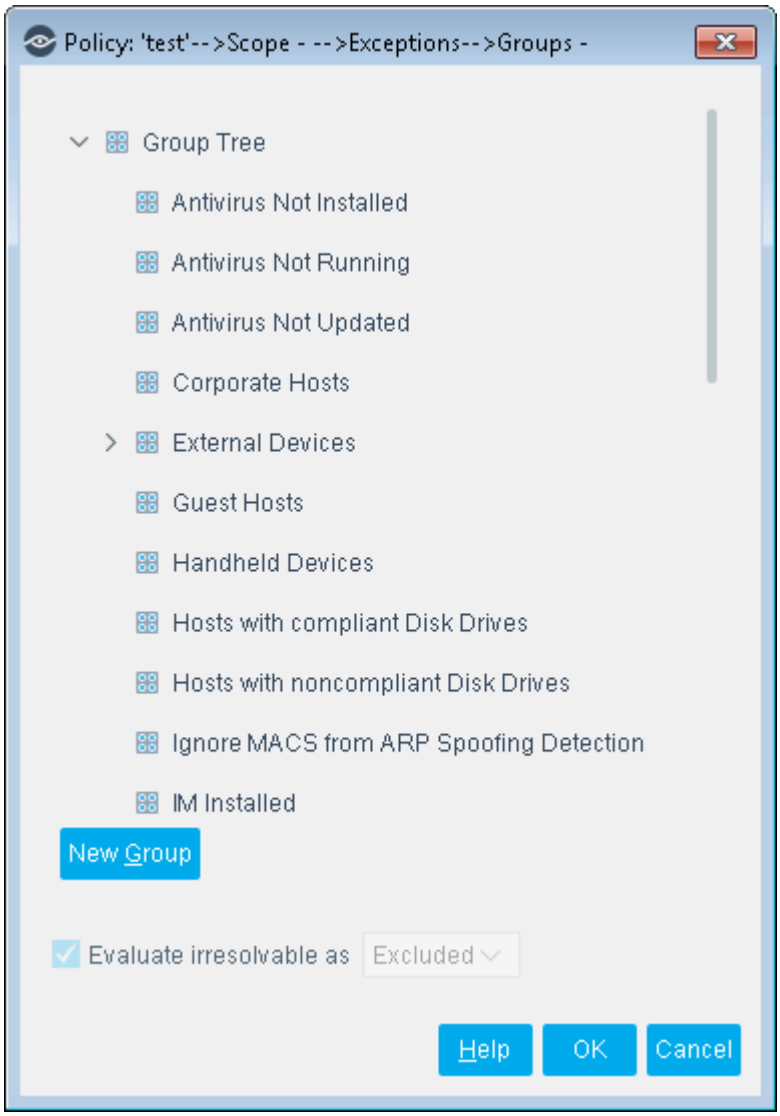
      The Groups dialog box opens.



4. Select a group.
5. Select OK. To create more groups, select New Group.
6. Exclude endpoints from inspection. For example, ignore groups of VIP users when conducting inspections.
7. Select Add from the Exceptions area, to exclude endpoints from inspection. For example, ignore groups of VIP users from inspections. The Exception Type dialog box opens.



8. Select an exception type and then select OK. An Exception dialog box opens. Exception dialog boxes vary depending on the selected exception. In general, you can define a specific exception value, for example, enter a specific user name or use a Property Value List (a user-defined list of property values, such as a list of user names).



9. Select OK.
10. Select the Evaluate Irresolvable As checkbox to define how Forescout eyeSight evaluates the endpoint if the exception value cannot be resolved, for example, if eyeSight does not know the user name. Either include the endpoint as an exception, exclude the endpoint as an exception, or mark the endpoint as Irresolvable for the policy.
11. After defining each exception, select OK.
12. Select Next. The Main Rulep pane opens.

Defining a policy main rule

Endpoints that match the Main Rule are included in the policy inspection. Endpoints that do not match this rule are not inspected for this policy.

A Main Rule consists of:

- A condition: A set of properties that is queried when evaluating endpoints. For example, Windows XP machines without up-to-date Symantec Antivirus installations.
- Actions: Measures taken at endpoints. For example, provide automatic remediation at endpoints without up-to-date Symantec Antivirus installations.

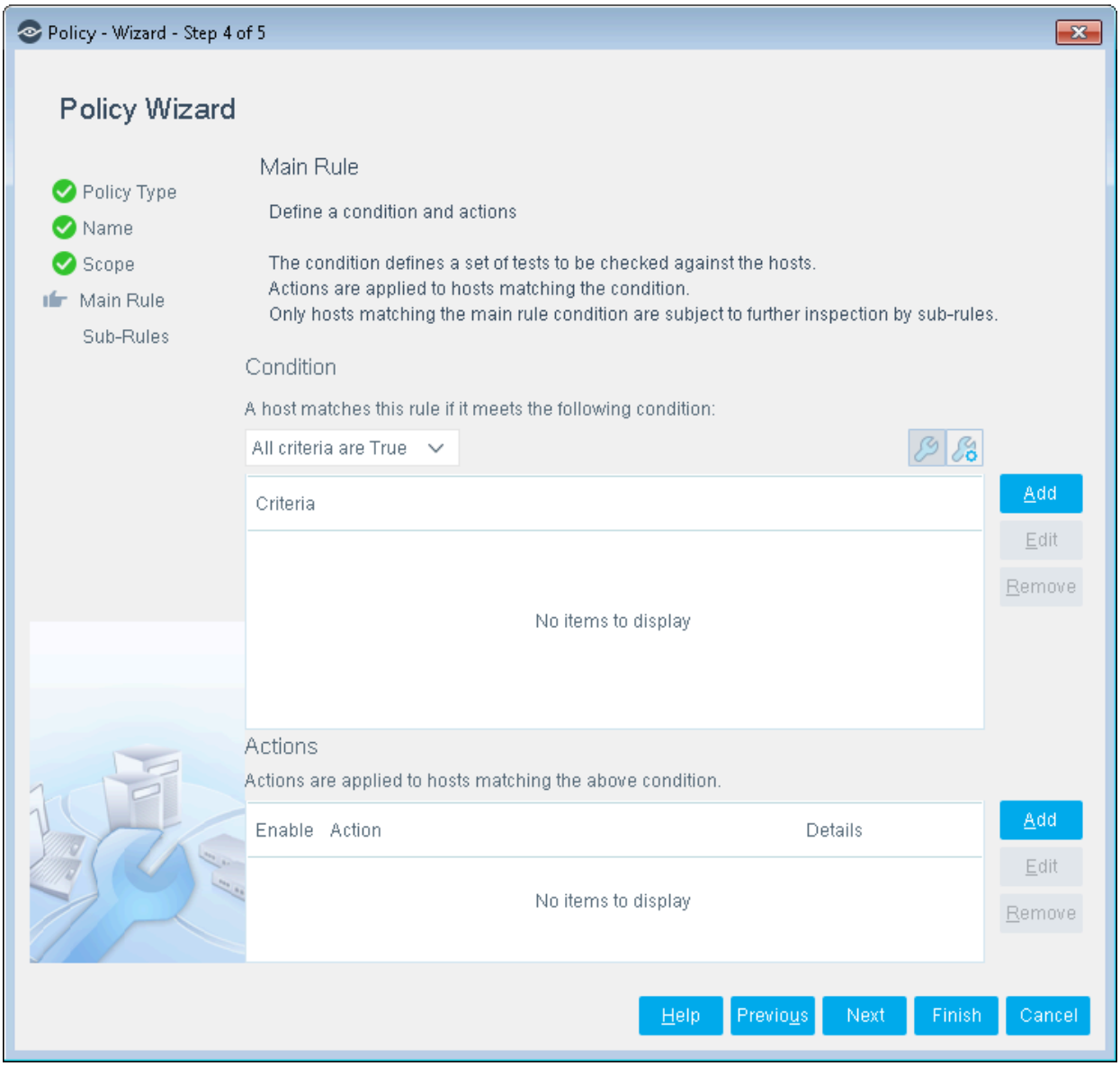
We recommend to define conditions and actions in Main Rules when the policy deals with a single policy purpose or problem and solution. For example, consider a policy requiring all corporate Windows machines to run an antivirus application. In this case, the Main Rule includes:

- Condition: Operating system is Windows AND Machine is Managed AND NOT running an antivirus.
- Action: Send HTTP notifications to end users and Send email to the Help Desk.

Some policies, however, are designed to accomplish more, and contain more than one problem and solution. For example:

- Communicate with users who have installed peer-to-peer applications:
- If users are part of the IT or Development departments, then list peer-to-peer applications detected and advise users to uninstall.
- If users are part of any other department, then send them email asking them to contact the IT department to assist them in uninstalling and notify IT which endpoints are not compliant.

For these use cases, use policy sub-rules to create multiple conditions and related actions. See Defining Policy Sub-Rules for details.



To define Main Rule conditions and actions:

1. Select Add from the Condition or Actions area of the Main Rule dialog box as required. See Working with Policy Conditions and Working with Actions for details about conditions and actions.
2. When you are done, select Next. The Sub-Rulesp dialog box opens. Use the dialog box to review and update Main Rule definitions and advanced policy settings, and then define sub-rules.

Define Forescout eyeSight policy sub-rules

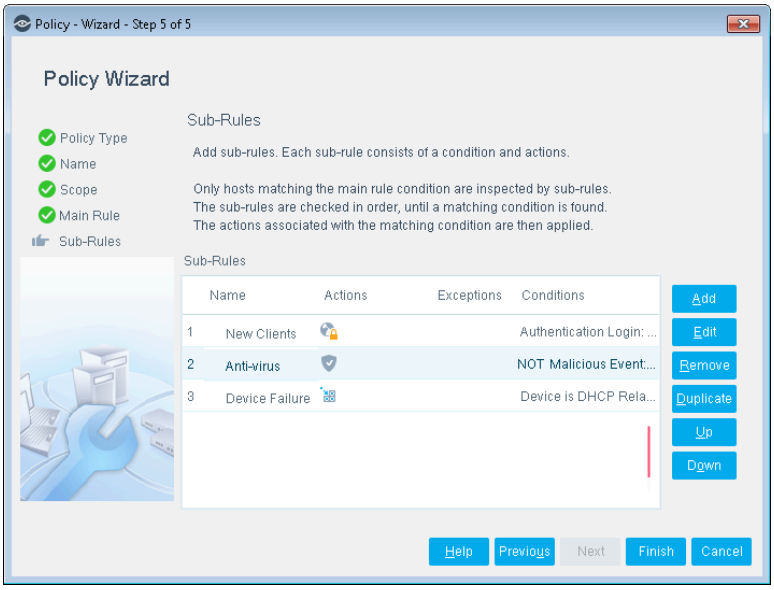
Sub-rules can be used to automatically follow up on endpoints after initial detection and handling. Creating sub-rules lets you streamline separate detection and actions into one automated sequence.

Sub-rules consist of the following elements:

- Name and description
- Conditions and actions
- Exceptions
- Recheck instructions

The order of sub-rules is important. Sub-rules are evaluated in the order in which they appear until the endpoint matches a rule. When an endpoint matches a rule's condition, that rule's actions are applied to the endpoint and evaluation of the policy ends for that endpoint. Later sub-rules of the policy are not evaluated for the endpoint.

You can create sub-rules and then modify their hierarchy in the Sub-Rules dialog box.



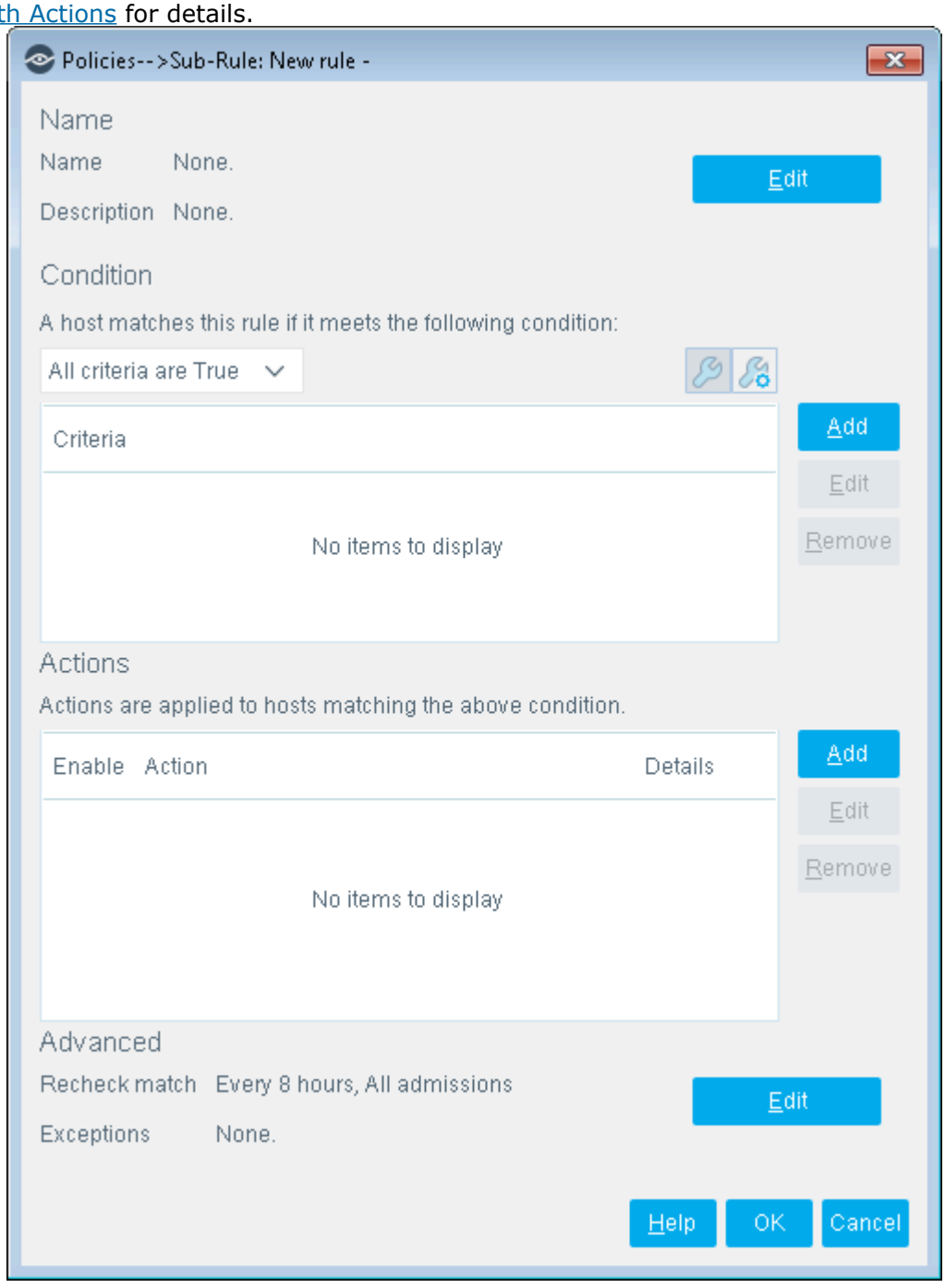
For example, use a sequence of sub-rules to implement the following policy logic:

- Assign endpoints to different VLANs based on their security compliance:
  - If non-corporate endpoints are detected, block access to the production network, but allow limited network Internet access.
  - If corporate unmatched endpoints are detected, but are VIP users, then remediate in a separate VLAN, but do not block access.
  - If corporate endpoints are unmatched, then remediate in a separate VLAN and block access to the production network until remediation is complete.
- Communicate with users who have installed peer-to-peer applications:
  - If users are part of the IT or Development departments, then list peer-to-peer applications detected and advise users to uninstall.
  - If users are part of any other department, then send them email asking them to contact the IT department to assist them in uninstalling, and notify IT which endpoints are not compliant.

To define a sub-rule name and description:

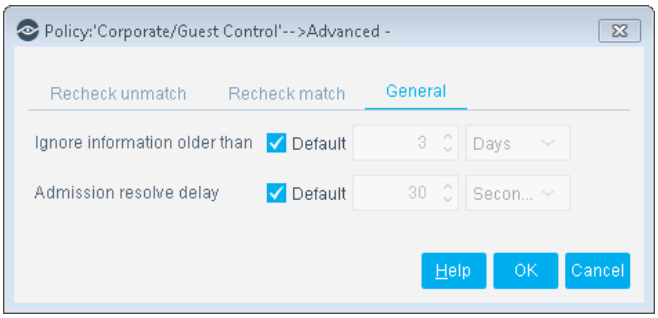
1. Select Add from the Sub-Rules dialog box.
2. Enter a unique policy name and description.
3. Select OK. The name is displayed in the New Sub-Rule dialog box . Use the dialog box to define sub-rule conditions and actions. See Working with Policy Conditions and Working

with Actions for details.



Forescout eyeSight policy main rule advanced options

Right-click a Main Rule in the Policy Manager, and then select Quick Edit > Advanced.



Update a Policy Recheck for Unmatched and Matched Endpoints

By default, both matched endpoints and unmatched endpoints are rechecked every eight hours, and on any admission event. An admission event is a network event that indicates the admission of an endpoint into the network, such as when it physically connects to a switch port. A complete list of admission events is described below.

Recheck tools let you define:

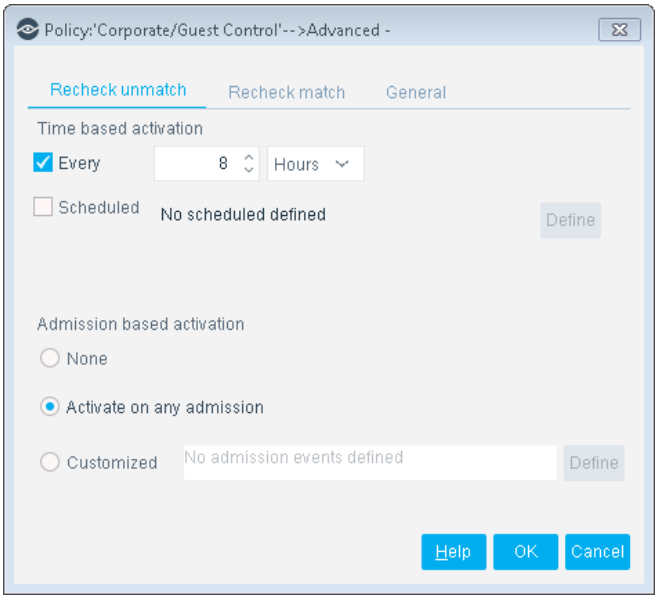
- How often endpoints that match a policy are rechecked
- Under what conditions to perform recheck

You can update the default setting for matched and unmatched hosts, for example, to initiate inspection according to a set schedule. You can also configure several recheck settings to work simultaneously, for example, when a host IP address changes every five hours.

Separate settings can be defined for hosts that either match or do not match a policy.

To define rule recheck settings:

1. Right-click a Main Rule from the Policy Manager, and then select Quick Edit > Advanced.
2. Select the Recheck unmatch or Recheck match tab.



Time Based Activation

The policy is run at a certain time and date. The default is every eight hours. The following options are available:

Every	Select this option to run a policy at specific intervals, i.e., per seconds, minutes, hours or days. This is recommended, for example, if you want to check that a web or email service is consistently running, or if you need to verify the integrity of any other mission critical service in your network.
Scheduled	Define a schedule for running the policy.

Admission-Based Activation

The following options are available:

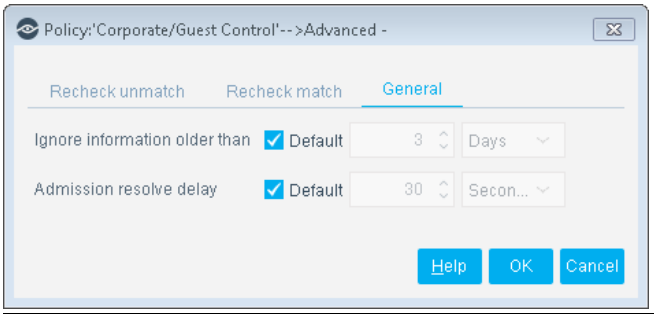
None	Do not inspect on the basis of an admission event.
Activate on any admission	Run the policy when any of the following admission events occur: New IP: By default, endpoints are considered new if not previously detected on your network within a 30-day period. For example, if an IP address was detected on the first of the month, and then detected again 31 days later, the detection will initiate the activation. The default time period can be changed. See Policy Preferences for details. IP Address Change Switch Port Change DHCP Request Authentication via the *HTTP Login* action Log in to an authentication server SecureConnector connection If you have installed plugins or modules, additional admission events types may be available. For example, the New Wireless Host Connected Events option is available if you installed the Wireless Plugin.

Customized	Admission-based inspection. Select Define to customize the admission values.

Note:
A delay exists between the detection of network admission events and the onset of the policy evaluation. When an endpoint boots, the IP address is assigned rather quickly, before most of its services have loaded. Waiting 30 seconds (default delay time) increases the chances that the policy evaluation starts when more details could be learned about the endpoint (after all services have loaded). You can update the delay default time. See Policy Preferences for details.

Handle Forescout eyeSight policy dated information – General tab

To define how dated information is handled, right-click a rule from the Policy Manager, and then select Quick Edit > Advanced, and then select the General tab.



Ignore information older than	The time information should be stored and used for evaluation. The value set here overrides global settings for this policy. For example, you can define a schedule that evaluates the policy every two days, but only use information one day old for evaluation.
Admission resolve delay	Delay policy evaluation for newly discovered endpoints. This enables all services to load on a newly booted endpoint before policy evaluation. This delay is applied only after a New Host admission event. It does not influence policy evaluation after other admission events. This delay applies only to properties resolved by directly examining the endpoint. It does not impact properties that are learned from other sources. The value you set here applies only to this policy, and overrides the global Network Admission Resolve Delay setting (Options > NAC > Time Settings).

Set and Increment Forescout eyeSight policy counters

This topic describes properties and actions to set and evaluate counters in policies. Policies can

trigger actions based on counters assigned and incremented previously by other policies. This lets you use endpoint history in policies.

For example, if an endpoint repeatedly installs pluggable memory devices, you can initiate actions on the endpoint after this behavior is repeated several times. Use counters to take into account hot-swap memory, and identify problematic repeat users.

When using counters in policies:

- Counters are incremented when:
  - The endpoint meets the conditions of the policy, and the counter is initialized.
  - Host properties change. The policy examines the endpoint and finds that it no longer satisfies the policy.
  - Host properties change again. The policy examines the endpoint again and finds that it satisfies the policy. The counter is incremented.

  This is how Forescout eyeSight evaluates other policy conditions. However, counter values are retained even when the endpoint no longer satisfies the conditions of the policy.

  Note:
  Counters are maintained per endpoint. The same counter can have a different value for each endpoint.

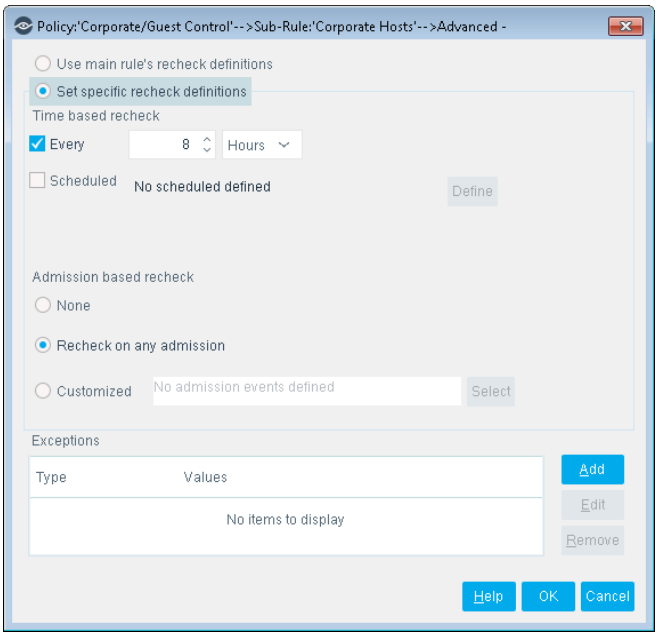
  Use properties and actions related to counters as follows:

- When you create a policy rule that defines a new counter, use only the Set Counter action.
- A policy rule that increments an existing counter must use both the Counter property and the Set Counter action:
  - The rule contains a condition that uses the Counter property to verify the presence of the counter for an endpoint. Enable the Evaluate irresolvable criteria as True option when the Counter property is used to verify the presence of a new counter.
  - Then the rule uses the Set Counter action to increment the counter on endpoints that match the condition.

Forescout eyeSight policy sub-rule advanced options

Right-click a Sub-Rule from the Policy Manager, and then select Quick Edit > Advanced.

The Advanced Sub-Rule dialog box opens for the selected sub-rule.



Inherit Main Rule Recheck Definitions

Automatically apply main rule recheck definitions to all sub-policies, instead of defining the recheck value for each sub-rule.

To use main rule definitions:

- Select Use main rule recheck definitions.

Sub-Rule Recheck Policy. Sub-rule Recheck tools let you define:

- How often endpoints are rechecked.
- Under what conditions to perform a recheck.

By default, endpoints are rechecked every eight hours, and on any admission event.

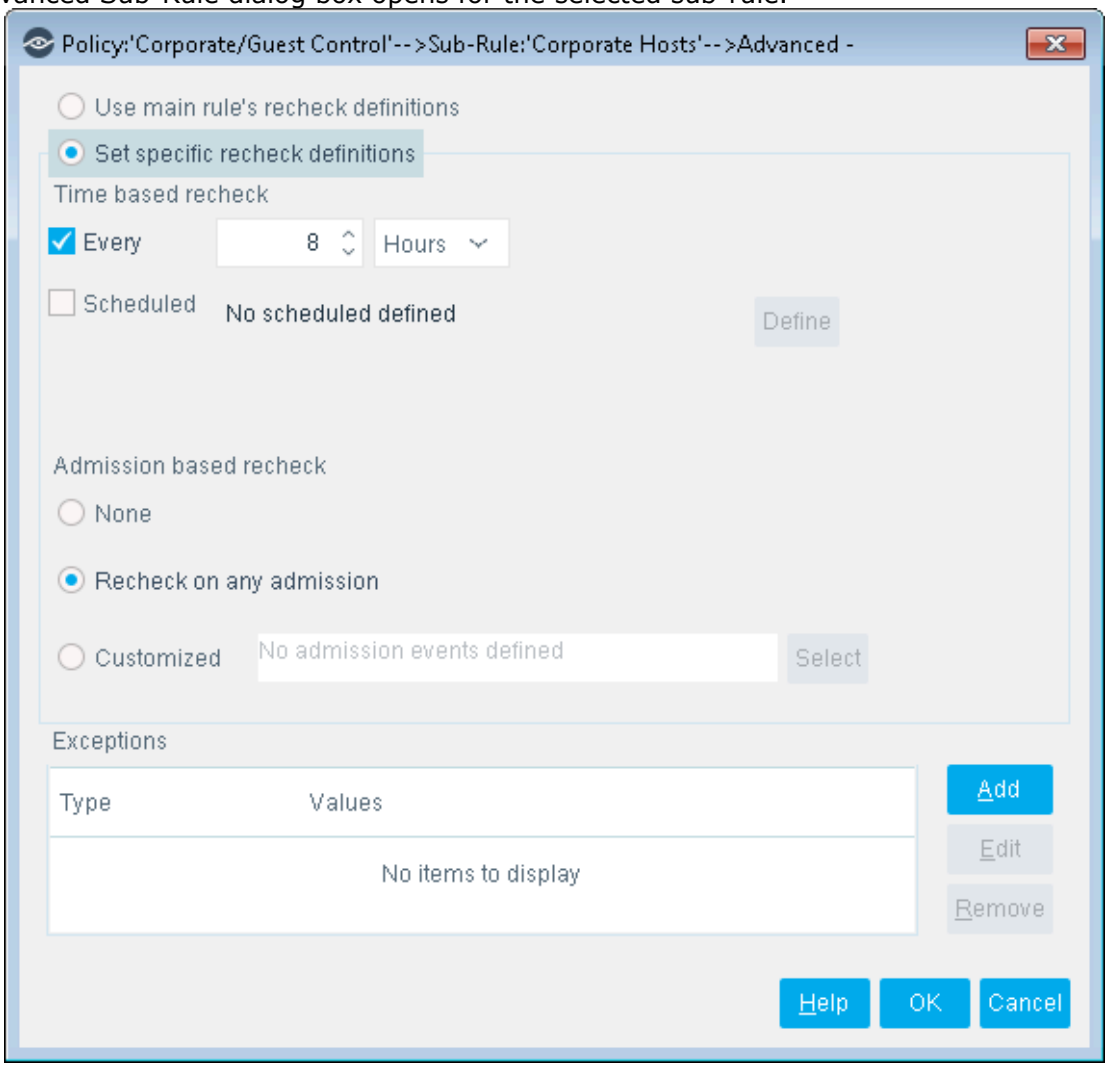
1. Right-click a sub-rule from the Policy Manager and select Quick Edit > Advanced . The Advanced Sub-Rule dialog box opens for the selected sub-rule.
2. See Update a Policy Recheck for Unmatched and Matched Endpoints for details. Define Sub-Rule Exceptions

   Use exceptions to exclude specific endpoints from inspection. In a sub-rule, exceptions may be used, for example, as follows:

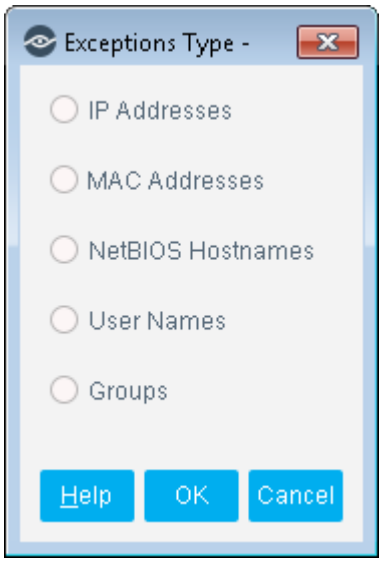
   - Scope
     - Windows hosts
   - Sub-Rule 1
     - Condition: Vulnerable to MS-08-xxx
     - Action: Browser Notification
     - Exception: Windows Servers
   - Sub-Rule 2
     - Condition: Symantec AntiVirus not installed
     - Action: Browser Notification
     - Exception: none

In this case, Windows servers are not subject to the first sub-rule, but are tested for the others.

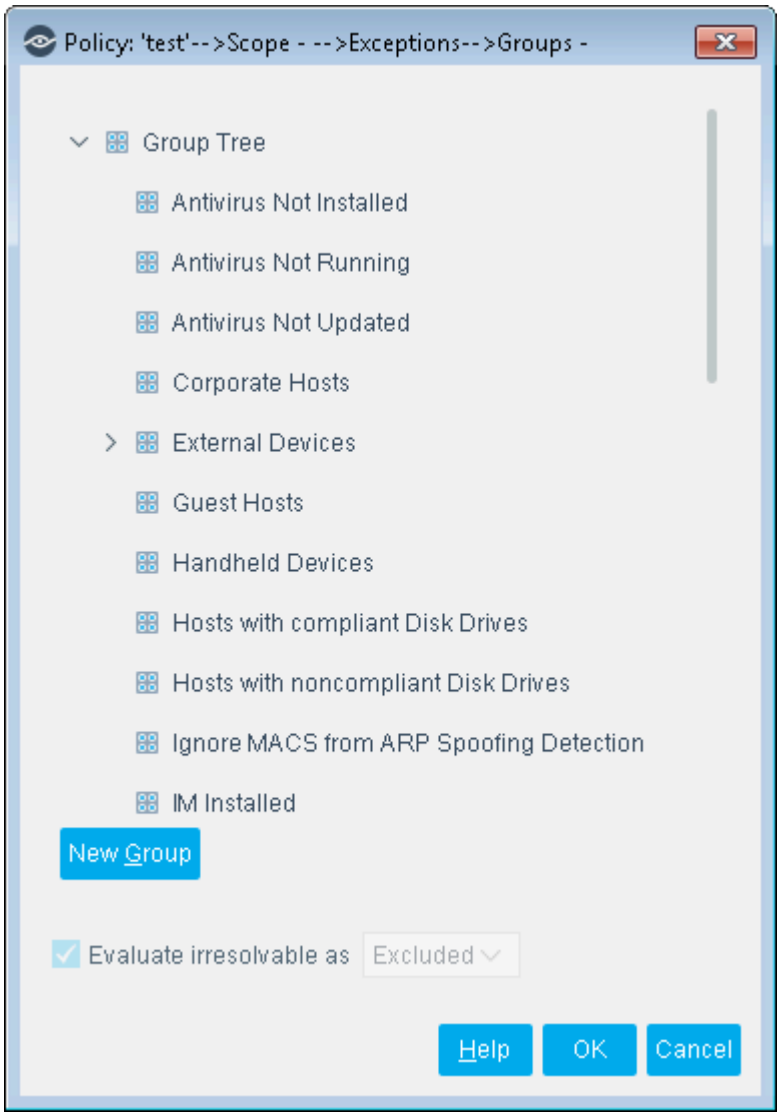
3. Right-click a sub-rule from the Policy Manager and select Quick Edit > Advanced. The Advanced Sub-Rule dialog box opens for the selected sub-rule.



4. In the Exceptions section, select Add.



5. Select an exception type and then select OK. An Exception dialog box opens. This dialog box varies depending on the selected exception. In general, you can define a specific exception value (for example, a specific user name) or use a user-defined List of property values (for example, user names). See Defining and Managing Lists for details.



6. Select OK.
7. Select the Evaluate Irresolvable As checkbox to define how Forescout eyeSight evaluates the endpoint if the exception value cannot be resolved, for example, if eyeSight does not know the user name. Either include the endpoint as an exception, exclude the endpoint as an exception, or mark the endpoint as Irresolvable for the policy.
8. After defining each exception, select OK.

Policy preferences

The preferences set here are applied to all connected Appliances. Preferences cannot be set individually for each Appliance.

To access the NAC options select Tools > Options, and then select NAC.

Defining authentication servers

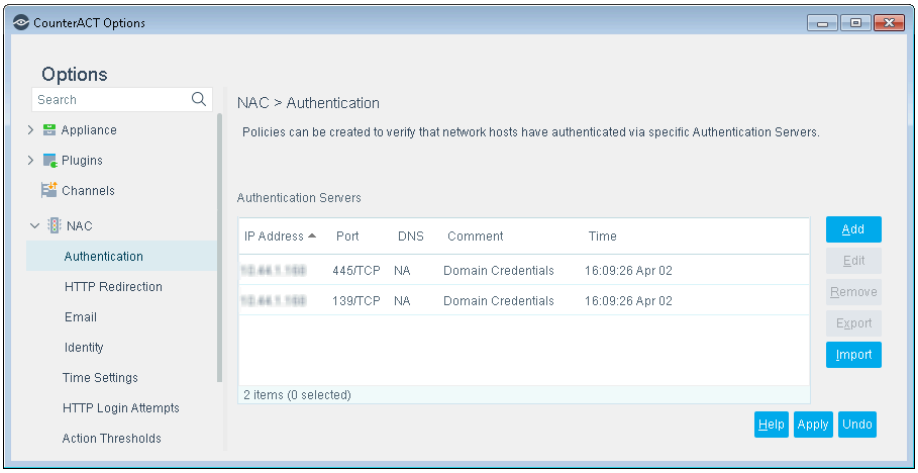
Policies can be created to verify network users have been authenticated via specific authentication

servers.

The following authentication servers are supported:

- HTTP (80/TCP)
- Telnet (23/TCP)
- NetBIOS-SSN (139/TCP)
- Microsoft-DS (445/TCP)
- Microsoft-MAPI (135/TCP)
- FTP (21/TCP)
- IMAP(143/TCP)
- POP3(110/TCP)
- rlogin (513/TCP)

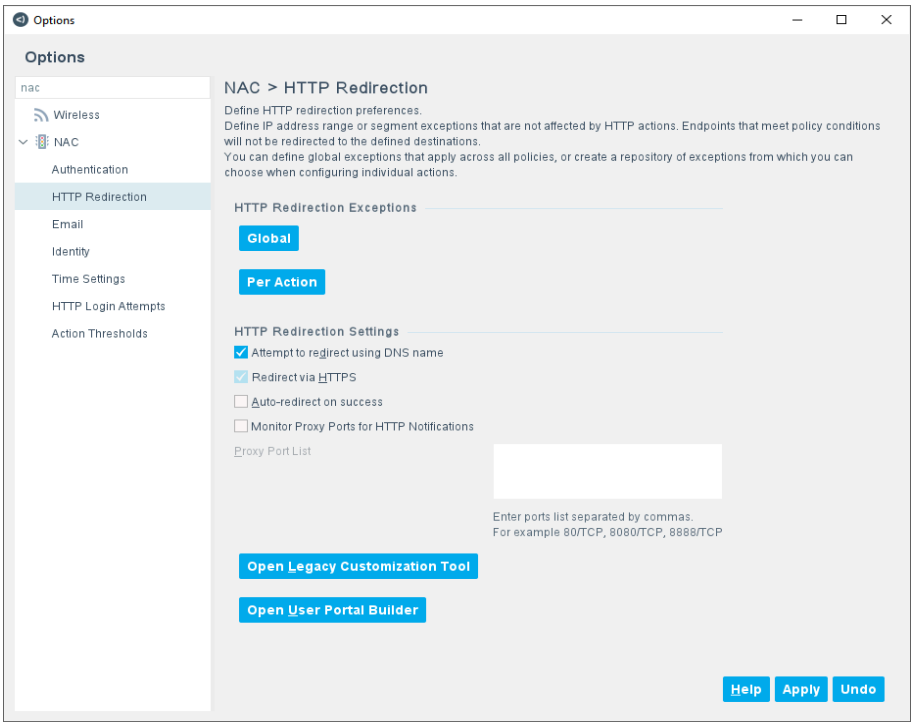
After you configure authentication servers, they are automatically deployed. These servers are automatically opened and added as Virtual Firewall rules. View these rules in the Firewall Policy pane.



HTTP Redirection options

Each Appliance can support up to 200 hijack actions per minute.

Several options are available for handling HTTP traffic from Tools > Options > NAC > HTTP Redirection.



Defining HTTP Redirect exceptions

You may need to refrain from redirecting business essential Internet sites or refrain from blocking access to important files on the Internet. This can be performed by creating HTTP redirect exceptions.

By default, user web sessions going to the Internet and Intranet are redirected. An option is available to only handle Internet traffic. See Redirecting Web and Intranet Sessions.

You can define exceptions in two ways:

- Global URL Exceptions. Global URL exceptions that apply for all actions.
- IP Address Exceptions per Action. IP address exceptions that can be applied to individual actions.

Global URL Exceptions

Endpoint users who browse to URLs in this list are not redirected by Forescout eyeControl even when an HTTP action is applied to the endpoint.

A number of URL strings are included in the list of global HTTP redirection exceptions by default. These strings are included to prevent endpoint users from receiving browser errors related to various issues, such as proxy servers, certificate revocation, and captive portals. These strings can be edited or removed.

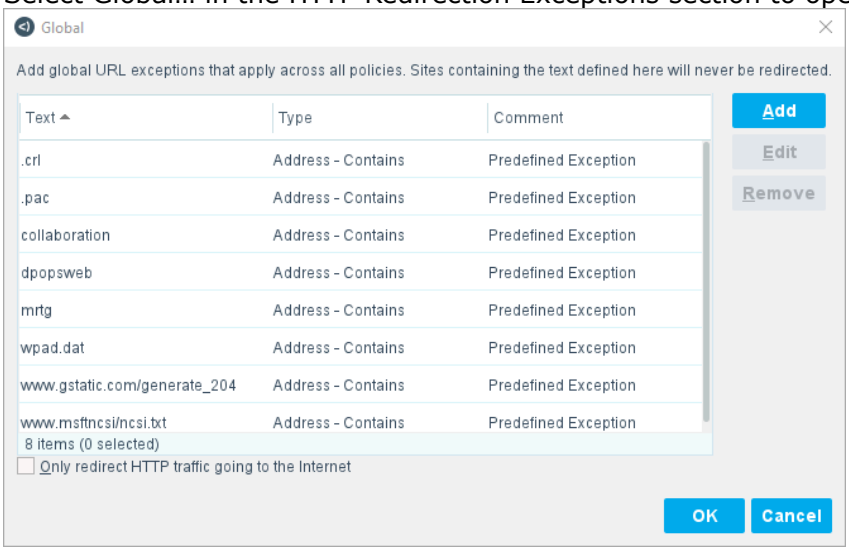
By default, the following URLs are never redirected:

- windowsupdate.microsoft.com
- windowsupdate.com
- update.microsoft.com
- updates.microsoft.com

- exchange

This enables access to Microsoft Windows Update servers and prevents redirection of the Exchange server when used via the web interface. These URLs cannot be seen or edited by the user.

1. Select Tools > Options > NAC > HTTP Redirection.
2. Select Global... in the HTTP Redirection Exceptions section to open the Global dialog box.



3. Select Add.
4. In the New URL Text dialog box, select an option from the Look in URL drop-down menu.
   - Filename
   - Address
5. Select Contains or Exact.
6. In the Text field, enter the URL address or filename to search for.
7. Select OK

Note:
If the address contains one string from the defined list, the user is not redirected.

Redirecting web and Intranet sessions

By default, all user sessions are redirected regardless of whether the traffic goes to the Internet or to the Intranet. An option is available to redirect Internet traffic only.

- In the Global dialog box, select Only redirect HTTP traffic going to the Internet. User sessions to the Intranet are not redirected.

IP address exceptions per action

Configuring HTTP Redirection Exceptions per action lets you define IP address ranges or segments that are not affected by a specific HTTP action. For example, create a policy that displays a customized message in end user web browsers using the HTTP Notification action, except for endpoint IP addresses between 192.168.10.15 and 192.168.10.30.

Add IP address ranges or segments to a repository of HTTP exceptions that can later be applied to individual actions.

This feature applies to the following HTTP actions:

HTTP Localhost Login

HTTP Login

HTTP Notification

HTTP Redirection to URL

Start SecureConnector

Windows Self Remediation

You can add an HTTP Redirection exception per action in the following ways:

- Add an Exception to the Repository
- Apply an Exception to an Action

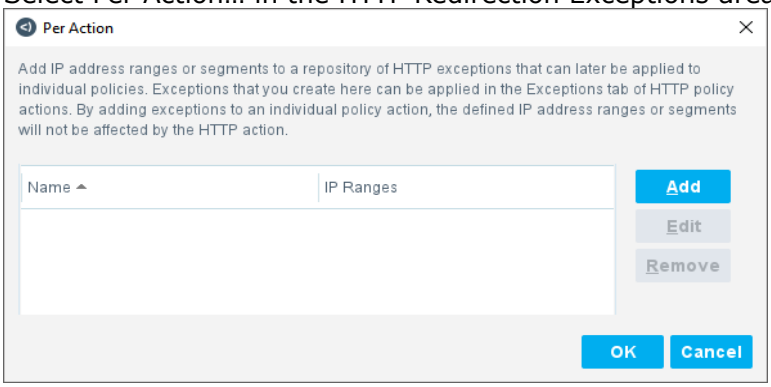
Note:
If you want to apply global HTTP exceptions to all network users, you can work with Global URL Exceptions.

When multiple HTTP actions, each containing HTTP Redirection Exceptions, are simultaneously applied to an endpoint, only the exceptions for the first HTTP action received by Forescout eyeControl are applied. Additional HTTP Redirection Exceptions are only applied when there are no other HTTP actions applied to the endpoint.

Add an exception to the repository

Exceptions that you create in the repository can be applied in the Exceptions tab of HTTP actions.

1. Select Tools > Options > NAC > HTTP Redirection.
2. Select Per Action... in the HTTP Redirection Exceptions area.



3. Select Add.
4. Enter a name for the exception in the Add IP Range dialog box.
5. Select Add to add an IP address range or segment, and then select OK.
6. Select OK in the Add IP Range dialog box.
7. Select OK in the Per Action dialog box.

Apply an exception to an action

1. In the relevant HTTP action configuration, navigate to the Exceptions tab.
2. Select Add. In the dialog box that opens, Select the name of the HTTP exception from the Select IP Range drop-down menu, and select OK. The exception is displayed in the Exceptions table.

Redirect using web server DNS name

When Forescout eyeControl redirects a browser to the captive web server, it can either use the web server IP address or its DNS name. Using the DNS name is recommended when using encrypted HTTPS transactions. The web server can have a certificate installed, avoiding the browser warning when interacting over HTTPS with an uncertified web server. For the DNS option to work properly, the endpoints must resolve this name using their defined DNS servers.

1. Select Tools > Options > NAC > HTTP Redirection.
2. Select Attempt redirect using the DNS name to redirect using the DNS name.

Global redirect via HTTPS

Redirect via HTTPS is selected by default and cannot be changed.

Redirected traffic includes information sent to network users via the HTTP actions, as well as authentication credentials sent back to the Appliance. For example, when you use the HTTP Localhost Login action, authentication credentials are sent back to the Appliance using the method that you defined.

If you transmit via HTTPS, network users see a security alert in their web browser when they attempt to access the web. The alert indicates that the site's security certificate was not signed by a known Certificate Authority (CA). (A default self-signed certificate is installed during product installation). You can generate a known CA Security Certificate to avoid this situation. See Generating and Importing a Trusted Web Server Certificate and HTTP Redirection for details.

Skip HTTP redirect confirmation message

You can instruct Forescout eyeControl to not display the confirmation message that appears by default at the endpoint after the HTTP action is successfully completed. When this happens, endpoint users are automatically redirected to the page they originally browsed to.

1. Select Tools > Options > NAC > HTTP Redirection.
2. In the HTTP Redirection Settings area, select Auto-redirect on success.

Defining proxy ports for HTTP notification

If your organization is configured to access the web through a proxy, you must enable the ports.

1. In the HTTP pane, select Monitor Proxy Ports for HTTP Notifications.
2. Enter the ports in the Proxy Ports List field. Use the following format: 80/TCP, 8080/TCP, 8888/TCP.
3. Select Applyr.

Customize HTTP pages

Redirected web pages are generated by eyeSight users to interact with endpoints when specific actions are performed. At the endpoint, a default or customized web page replaces the page otherwise displayed. The content inside the page is configured when defining policy actions. See Working with Actions for details.

Use the User Portal Builder when customizing the web pages displayed by the following eyeSight eyeControl actions:

- HTTP Login
- HTTP Notification

For more information, see The Forescout User Portal Builder.

When you upgrade from versions earlier than 8.0.0, customizations created using the legacy Forescout Customization Tool are preserved for these interfaces and are upgraded to the User Portal Builder. However, customization files that are configured manually and then copied to the Forescout file system in versions earlier than 8.0.0 are not available after upgrade. Use the User Portal Builder to recreate these customizations.

Use the legacy Customization Tool when customizing the web pages displayed by the following Forescout actions:

- HTTP Localhost Login
- Start SecureConnector
- Start Macintosh Updates
- Start Windows Updates
- Windows Self Remediation
- Compliance Center

For more information, see The Legacy Customization Tool.

When you upgrade from versions earlier than 8.0.0, all customizations for these interfaces are upgraded.

Email preferences

The Send Email action automatically delivers email to administrators when a policy is matched. If there is extensive activity as a result of your policy, the recipients may receive an overwhelming number of emails.

The following tools are available to help you manage email deliveries:

- Define the maximum number of email alerts delivered per day (from midnight)
- Define the maximum number of events that are listed in each email

For example, you can define that you only want to deliver five emails per day, and that each email will contain up to 50 events. The limits defined apply to each email recipient, and for both the Send Email and Send email to host actions.

Customizing endpoint identity change thresholds and detection mechanisms

IP addresses associated with a specific MAC address may change frequently. This may happen, for example, if several VPN users receive different IP addresses for the same MAC address. eyeSight eyeSight ignores these changes for the purpose of rechecking the same endpoints and carrying out actions on them.

By default, IP address changes are ignored when up to 20 changes occur within a 5-minute period on the same MAC address.

Before the threshold is passed:

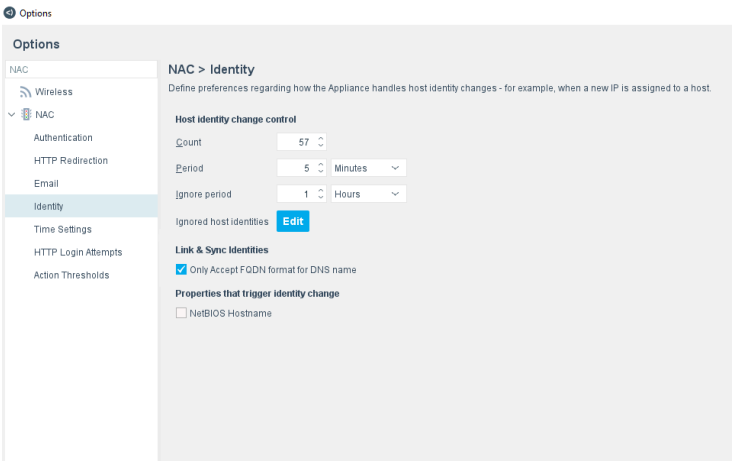
- All actions are released from the original IP address and no actions are applied to the new IP address when the change occurs.
- However, eyeSight eyeSight activates the Admission based activation option for the IP address

  The detection is displayed in the Detections pane with the same MAC addresses and the most current IP address detected.

After the threshold has passed: If there is an IP address change after the threshold has passed:

- The MAC address is ignored as a mechanism for identifying the endpoints in any policy.
- The MAC is automatically added to a list of ignored addresses which can be modified manually by adding or deleting MAC addresses as needed.
- All new detections on the MAC are displayed individually per IP address.

Select Tools > Options > NAC > Identity. Use the options in this pane to update the default IP address threshold. You can also apply the ignore mechanism and threshold definitions to NetBIOS host name changes detected on the same IP address.

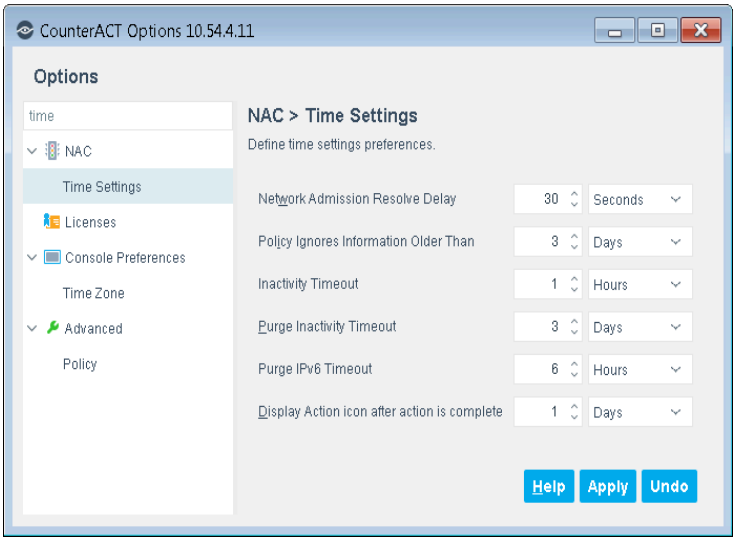


Count	The number of IP address changes that can occur before the threshold is passed.
Period	The time period during which identity changes can occur before the threshold is passed.

Ignore period	Endpoint identity change will be ignored for this period.
Ignored host identities	The MAC addresses that are ignored during detection. The threshold for IP address changes on this MAC has been passed. The MAC is automatically added to a list of ignored addresses. You can edit and remove MAC addresses from the list.
Link & Sync Identities	If selected, Forescout links and synchronizes assets that share an identical strong identifier (for example, hostnames in their Fully Qualified Domain Names). • When you select Enable Link & Sync Identities, Forescout links assets that share the same identity and synchronizes sharable properties across those records. These properties are copied between the synchronized hosts and become part of the host data in all platforms. • For endpoints with both wired and wireless connections, access policies evaluate each interface separately. The shared information applies at the operating system level, not at the user level. If you clear the option, the records remain separate, and policies may apply differently to each interface.
NetBIOS Hostname	Apply the ignore mechanism and threshold definitions to NetBIOS names that change on the same IP address.

Time settings

Select Tools > Options > NAC > Time Settings to set the time settings.



Network Admission	A delay time between the detection of network admission events and the onset of the policy evaluation. This delay increases the chances that the rule

Resolve Delay	evaluation will start when more details can be learned on the endpoint (after all services have loaded). You can also set this value per policy. See Update the Network Admission Resolve Delay in Main Rule Advanced Options for details.
Policy Ignores Information Older Than	A time period that Forescout eyeSight does not see traffic at previously detected endpoints. Endpoints listed in a policy that are inactive beyond the time set here are no longer rechecked. Inspection begins again only when the endpoint in rediscovered as a result of the activation settings defined. The default Inactivity Timeout is defined in the Policy Preferences dialog box. The value there is applied to all Appliances until changed specifically, per policy, here.
Inactivity Timeout	After initial detection, endpoints in your network may disconnect from the network, that is, go offline. For endpoints that are not connected to a switch managed by the Switch Plugin, the Inactivity Timeout option is used to resolve offline status. This is the time period that endpoints should be disconnected from the network in order for Forescout eyeSight to resolve them as offline. The minimal (and default) offline setting is one hour. This parameter applies to policy endpoints as well as other endpoint detections. Endpoints that are offline beyond the time set here can be hidden from the Home view, Detections pane. This lets you view and work exclusively with online endpoints. If endpoints are connected to a switch that is managed by the Switch Plugin, by default Forescout eyeSight detects offline status within one minute. Refer to the *Switch Plugin Configuration Guide* for information about changing this one-minute default setting.
Purge Inactivity Timeout	After initial detection, endpoints in your network may disconnect from the network – become inactive for a lengthy period. The Purge Inactivity Timeout refers to a specific time period that Forescout eyeSight does not see traffic at endpoints that it previously discovered. This includes policy endpoints as well as other endpoint detections. Endpoints that are inactive beyond the time set here are cleared from the database. For example, those endpoints no longer appear in the Detections pane, Host Details dialog box, Policy Log, in reports, or in the History view.
Purge IPv6 Timeout	This setting determines how long Forescout eyeSight associates an IPv6 address with an endpoint. This timeout is measured from the time eyeSight learns the IPv6 address. If eyeSight does not detect this address or its

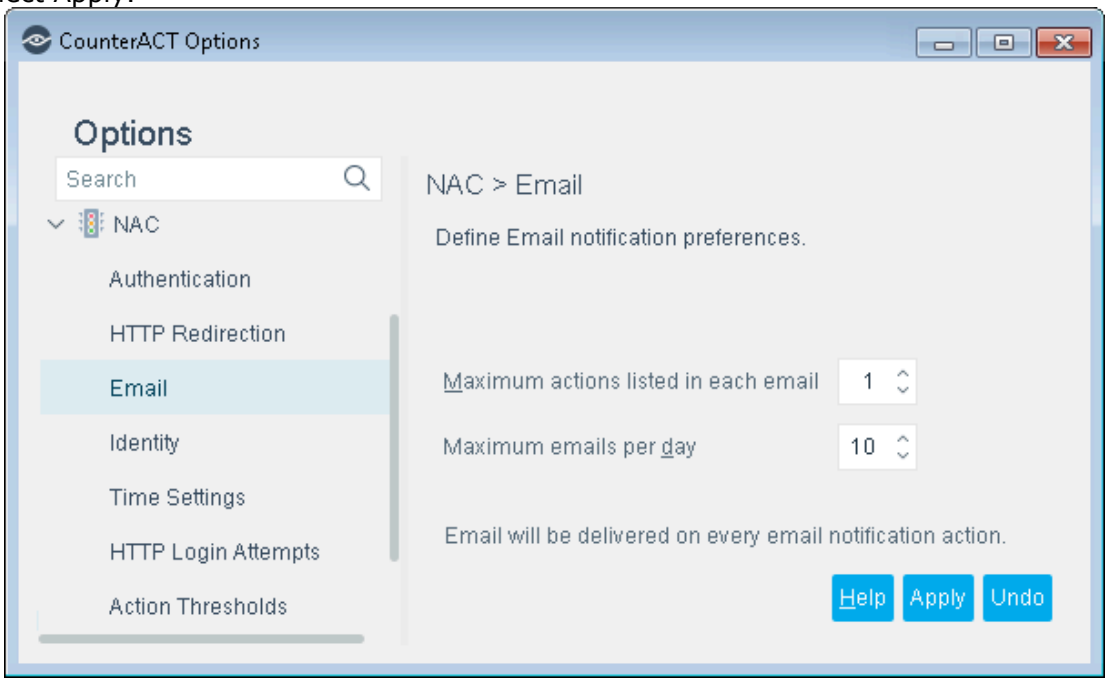
	related MAC address in the network during the time period specified: It no longer associates the address with the endpoint. This address no longer appears in the IPv6 Address host property for the endpoint. If the endpoint has no other IP or MAC address, it is purged completely.
Display Action Icon after Action Is Complete	The time period that the Console displays an Action icon after a one-time action is complete.

Default email settings

By default, up to 10 emails can be sent within 24 hours, and one message is displayed in each email. For example, if there is activity early in the day and 10 emails are sent by 2:00 PM, you will not receive emails about events that occurred during the rest of the day.

After the maximum number of emails has been sent, a warning email is delivered stating that the email delivery threshold has been reached and that you will receive no more email alerts until midnight. At midnight, an email is sent summarizing events that were not delivered.

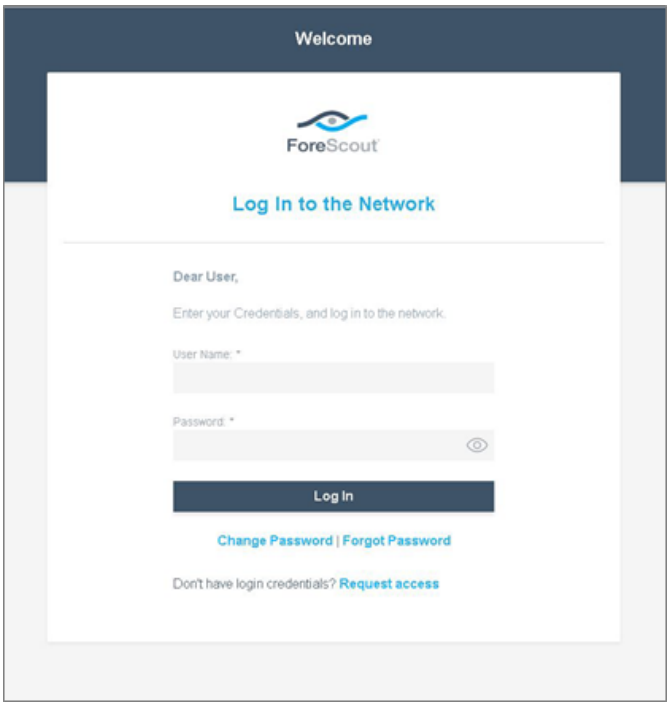
1. Select Tools > Options > NAC > Email.
2. Set the Maximum actions listed in each email. For example, to receive an email alert each time an events occurs, enter 1 in the Maximum actions listed in each email field.
3. Set the Maximum emails per day.
4. Select Apply.



You can sign these emails using a digital certificate, as specified by the Secure/ Multipurpose Internet Mail Extensions (S/MIME) standard. See Signing Emails with an S/MIME Certificate for details.

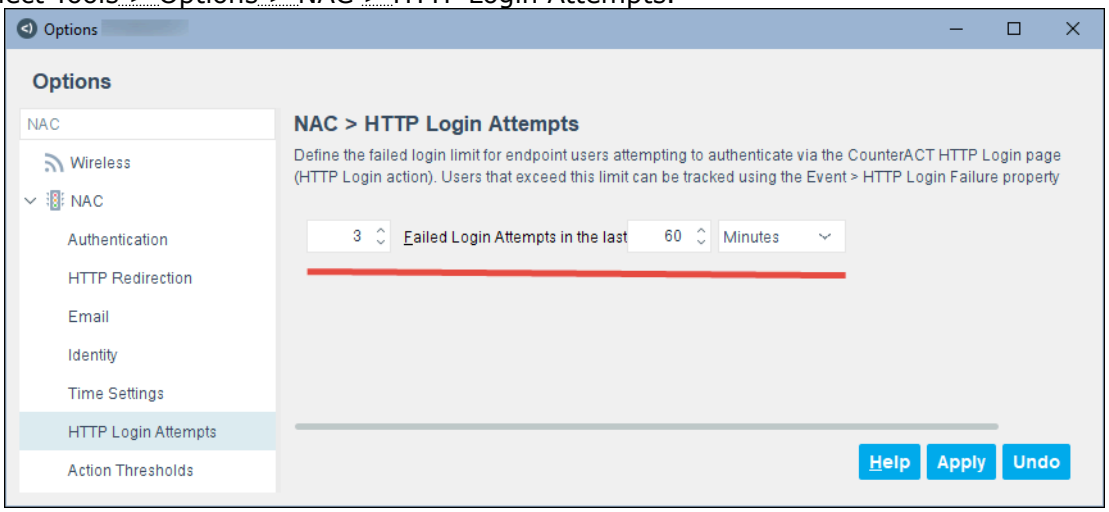
HTTP login attempts

Define a failed login limit for endpoint users attempting to log in via the HTTP Login page. This page is triggered via the HTTP Login action.



You can define the number of failed login attempts that occurs within a specific time frame. Users who exceed this limit can be detected using the HTTP Login Failure property. In addition, you can follow up with users who exceeded the limit by creating useful policy actions, for example, notifying the IT team or preventing user access to the production network.

1. Select Tools > Options > NAC > HTTP Login Attempts.



2. Set the number of failed login attempts and the time within which failed login attempts must occur in order for a login failure attempt to be detected.
3. Select Apply.

Property lists

Lists contain endpoint properties and related values, for example, a list of domain user names, or a list of DNS names, or of processes that you want to prohibit on your network. Each List is associated with a single endpoint property and can contain multiple related values.

Using lists speeds up and streamlines the policy creation process.

For example, if you discovered that network guests are running unauthorized processes on your network, create a list of these processes, and then incorporate them into a policy that will detect and halt them. You can manually create lists or create lists based on Inventory detections and policy detections. See Defining and Managing Listsl for details.

Categorizing policies

Assign policies to policy categories to:

- Help you organize and view policies in the Policy Manager. For example, display only policies that have been labeled as Compliance policies.
- Include categorized policies in the Compliance folder and Corporate/Guests folder in the Views pane of the Console. See Home Views.
- Include categorized policies in the Forescout Compliance Center. See Working with the Forescout Compliance Center.
- Display categorized policies in the Site Map. See Working in the Site Map.
- The Compliance Status and Corporate/Guest Status properties. See Device Information Properties.

By default, these include policies generated from Classification, Compliance and Corporate/Guest Control templates.

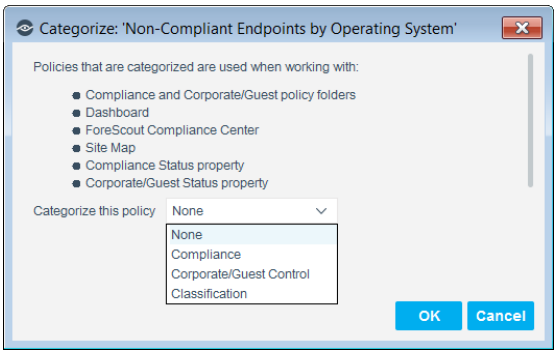
This section describes how to categorize other policies as either Classification, Compliance or Corporate/Guest.

Follow these guidelines:

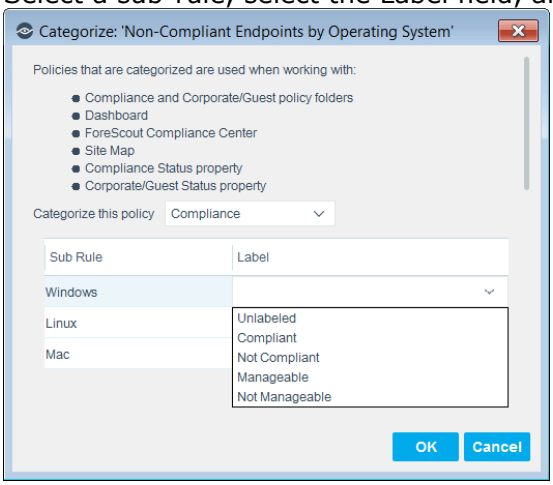
1. Create a policy for which you need to view results in a dashboard.
2. Categorize the policy as either Classification, Compliance, or Corporate / Guest.
3. Label endpoints that match the policy sub-rules as follows:

Sample Categorization and Labeling – Running Vital File on Windows Endpoint Policy

1. Create a policy. In this example, the policy name is Non-Compliant Endpoints by Operating System.
2. Select Categorize.



3. Select Compliance from the Categorize this policy drop-down menu.
4. Select a sub-rule, select the Label field, and then select Compliant.



Endpoints that match this sub-rule are calculated as compliant.

5. Select Unlabeled if you do not need results to be calculated for endpoints that match the sub-rule.

Tag sub-rules for dashboard widgets

Apply dashboard tags to policy sub-rules to display matched devices in relevant Dashboard widgets.

The following tag is available:

- Application Issues Dashboard Tags

Application issues dashboard tag

Applying this tag to relevant policy sub-rules will include matched devices in the Applications – Top 5 Reasons for Noncompliance Widget.

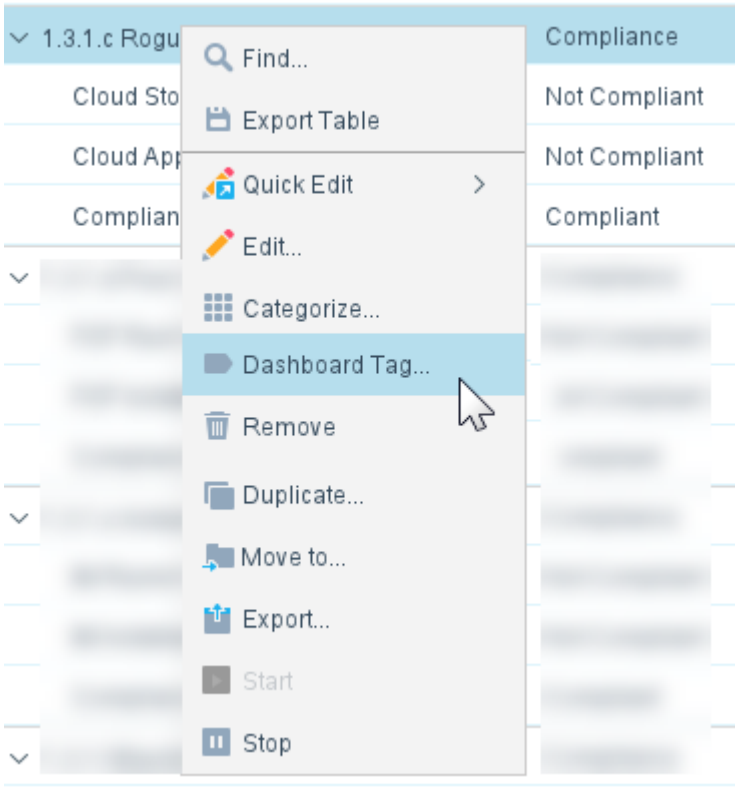
By default, this widget displays devices matched to policies created from relevant compliance templates. To include additional devices not detected by these templates, tag sub-rules related to application issues that you want displayed in the widget with the Application Issues tag.

This tag can only be applied to sub-rules in Compliance policies that are labeled as *Not Compliant*.

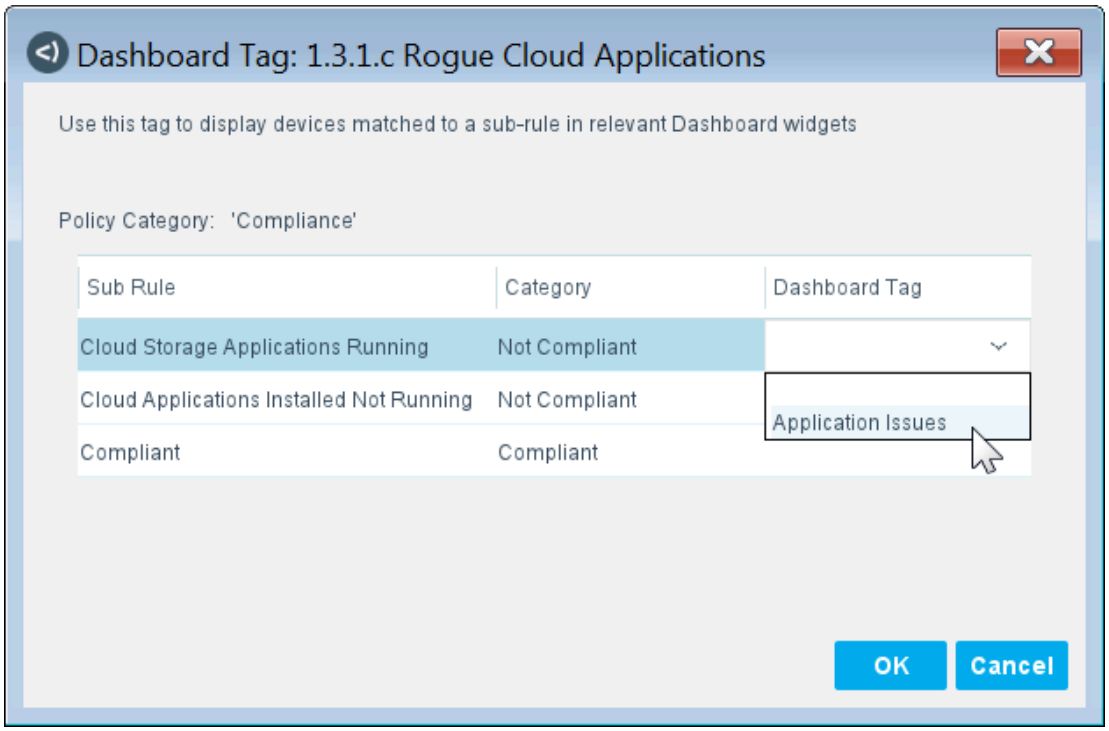
See Categorizing Policies for details.

To tag a sub-rule:

1. In the Policy Manager, navigate to the required Compliance policy. See Categorizing Policies for details.
2. Right-click the policy, and then select Dashboard Tag….



3. Select the relevant sub-rule/s (categorized as Not Compliant), and then select Application Issues from the drop-down menu in the Dashboard Tag column.



To remove the tag, deselect Application Issues by selecting the blank entry in the drop-down menu.

4. Select OK.

Policy reports and logs

You can use the Reports Portal to generate reports. See Reports Portal.

To generate a report listing your policies and policy definitions, select Reports>Policies Summary Reportl from the main menu.

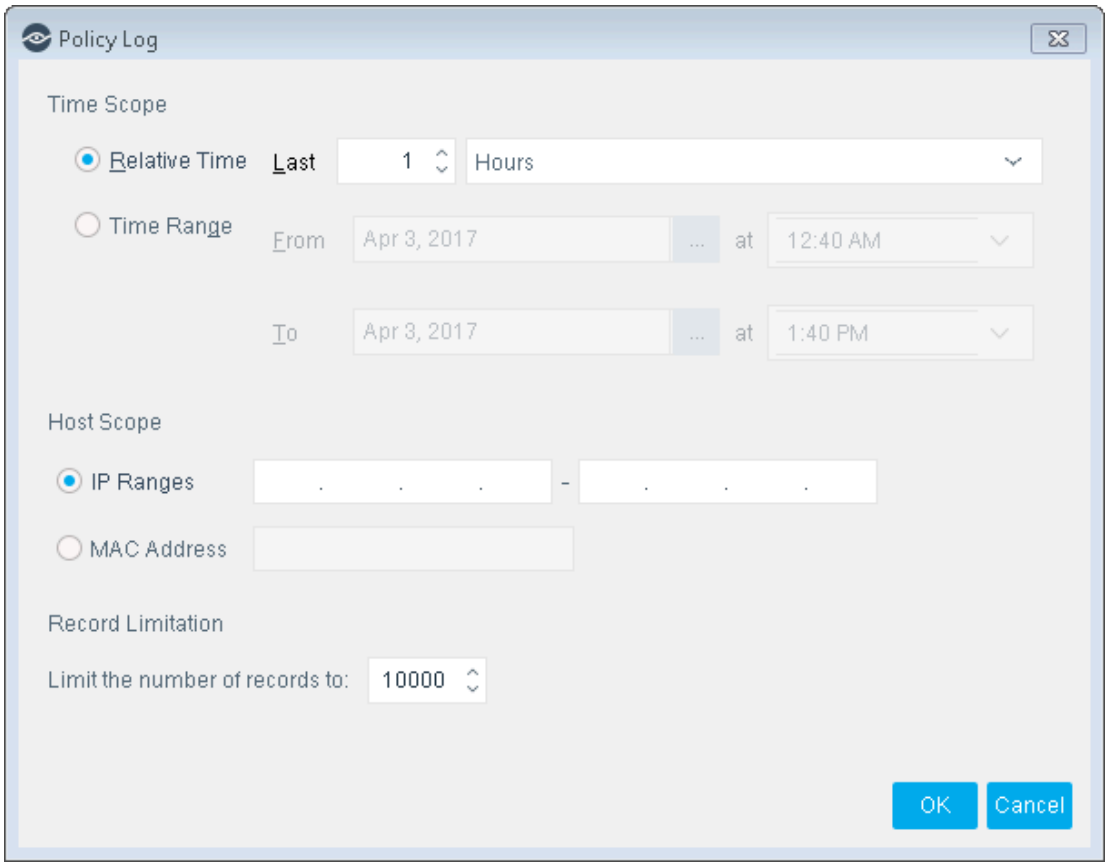
Policy logs

Use the Policy Log to investigate the activity of specific endpoints, and display information about how those endpoints are handled. The log displays information about endpoints as they are detected and is continuously updated.

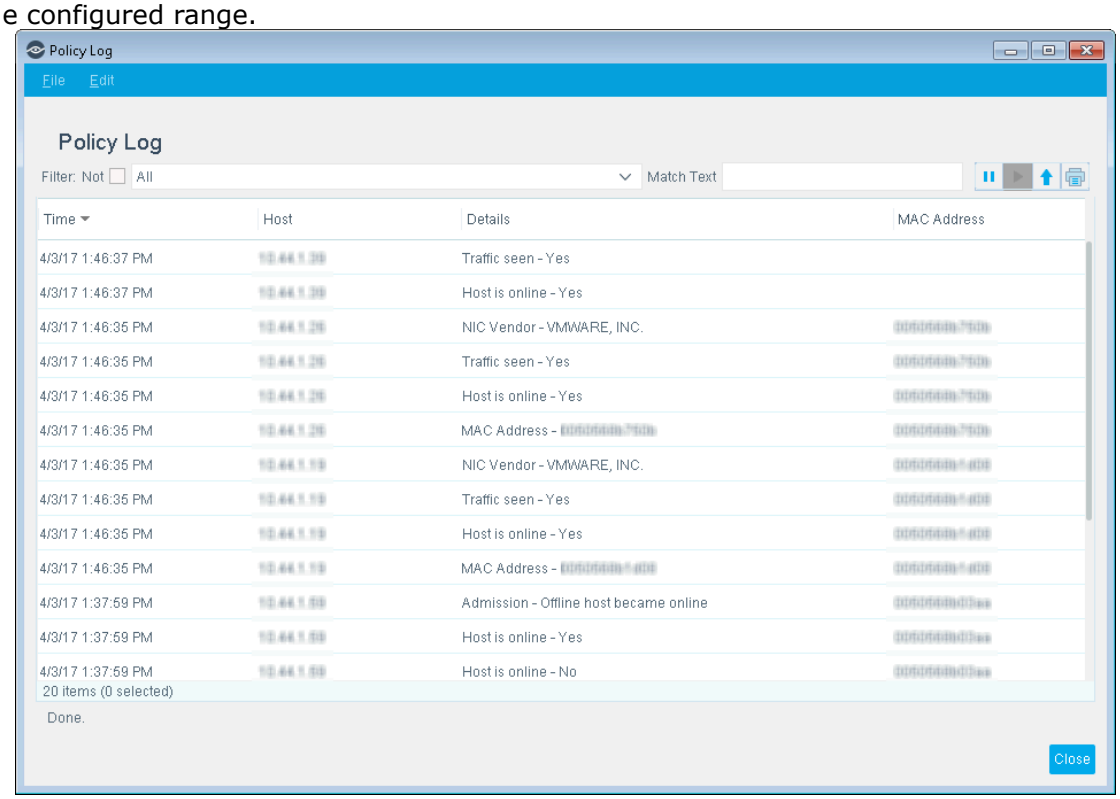
You can display endpoints from a specific time period and IP address range. In addition, filter tools are available to limit the log display, for example, to specific policies or sub-rules. An option is also available to export the Log to an XML file.

To work with policy logs:

1. Select Log > Policy Log.



2. Define a time scope and address range and select OK. A Log dialog box opens according to the configured range.



The following information is available:

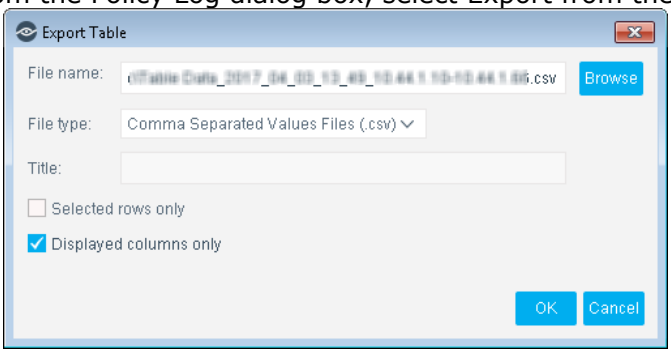
Time	The time the event occurred.
Host	The IP address of the detected endpoint.
Type/Name	The type of event. Use the Filter option to control which event types are displayed. The name is basic information about the type.
Details	Event details.
Status	The status of the operations taken place. For example, if a policy action is complete, the status is OK.
Origin	The device that detected the event.
MAC Address	The MAC address of the detected endpoint.

The following filter options are available:

All	Display all log events.	
Log	Displays detections, action execution, and additional information.	
Threat Protection	Displays endpoints detected via the Threat Protection Policy.	
	Only Changes	Displays new, changed, or rechecked property that was learned regarding to the selected IP address ranges.
Policy	The name of the policy or sub-policy.	
Property	Changes to the status of policy properties. For example, the Authentication, Signed In Status property changed from Not Signed In to Signed In as a Guest.	
System	Important system events, including Console initialization time, Appliance status, plugin and module status, and changes in Appliance IP address assignments.	

Use the Event Viewer to review more detailed system event information. See Work with System Event Logs for details.

3. To export log data:
   a. From the Policy Log dialog box, select Export from the File menu.



   b. Browse to the location for saving the file.
   c. Configure the export options.

Displayed columns only	Do not export information in hidden columns of the table.
Selected rows only	If you selected rows before export, only these rows are included in the export file.

   d. Select OK.

Policy safety features

Several safety features are available to help ensure that your policies efficiently handle endpoints.

Working with action thresholds

An action threshold is the maximum percentage of endpoints that can be controlled by a specific action type defined at a single device. By working with thresholds, you gain more control over how many endpoints are simultaneously restricted in one way or another..

In some scenarios, policy enforcement requires blocking or restricting network devices and users. Action thresholds are designed to automatically implement safeguards when rolling out such sanctions across your network. Consider a situation in which you defined multiple policies that utilize a blocking action, for example, the Virtual Firewall or Switch Block action. In a situation where an extensive number of endpoints match these policies, you may block more endpoints than you anticipate.

How Action thresholds work

1. Forescout products set default thresholds for an action type.
2. Forescout products put actions on-hold for endpoints that are detected after the threshold is passed.
3. An On-hold indicator blinks on the Console status bar. Manual approval is required to

cancel the on-hold status and carry out the actions.
4. Select the indicator to access the Action Threshold dialog box, where you can, for example, change the threshold or stop the device. Additional options are also available.
5. When the situation is remediated and the blocking limit falls below the threshold, you can cancel the on-hold status and continue to block or remediate.
6. You can also manually select endpoints and cancel on-hold status.

You can also create threshold policy exceptions, i.e., policies that you want to exclude from action threshold calculations. For example, you can exclude all thresholds when working with policies that handle outside contractors.

How On-hold thresholds are calculated

Thresholds for each action type are calculated per device, based on the number of endpoints assigned to the device.

To enforce on-hold status, the following must occur:

- A threshold percentage must be exceeded. See for details.
- The number of endpoints with an action assigned to them must be equal to or more than the minimal number of endpoints Forescout eyeSight is instructed to detect before calculating the threshold. By default, this number is ten.

Using the default, if the total number of endpoints assigned to a device is 500, and the default threshold for the Switch Block action is 2%, then the threshold limit is passed after 2% of the endpoints on the device (or 10 endpoints in this example) are blocked via the switch. At this point, the action is put on-hold for new endpoints detected.

Actions covered and threshold percentages

The following table lists actions covered by thresholds and the default threshold values.

Action	Default Threshold
Switch Block	2%
Assign to VLAN	2%
Virtual Firewall	2%
HTTP Notification	20%
HTTP Redirection to URL	20%
Send Email	2% during one minute

Action	Default Threshold
VPN Block	1%
WLAN Block	1%
Kill Process on Windows	2%
Add to Blocking Exceptions list	2%
ACL	2%
Disable External Device	2%

How do I know when a threshold violation occurred?

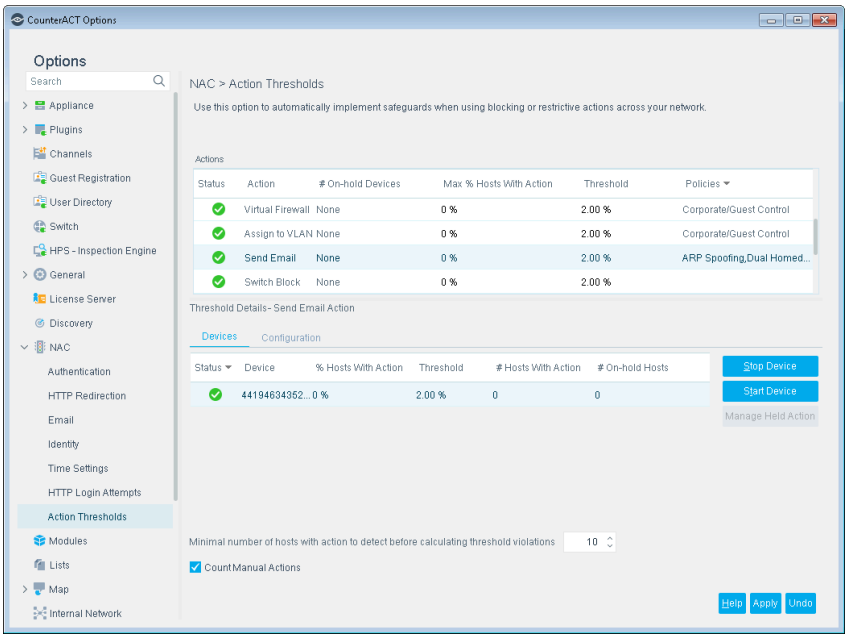
The action threshold indicator flashes if a threshold violation occurred.

You can select the icon to open the Action Threshold dialog box for details. At that point the indicator will remain on the status bar, but will not flash.

A tooltip gives you information about the on-hold status.

Configure action thresholds

Select Tools > Options > NAC > Action Thresholds.



The Actions area lists all the actions defined in your enterprise and provides related information.

Status

The on-hold status of the action. If the action is put on hold at one device, the overall status is considered On-hold.

A green check-mark means that the action is not on-hold at any device. A blue icon indicates that it is On-hold.

Action

The action being handled.

 # On-hold Devices

The number of devices that are working with an on-hold action.

Max % Hosts With Action

The highest percentage of endpoints covered by an action at a specific device, in relation to all enterprise devices. For example, 20% of all endpoints at a specific device have been assigned this action, and this is the highest percentage at all devices.

Use the value to get a better understating of how to configure your threshold for a particular action. Using this example, if 20% is the maximum value but the default threshold is at 2%, you may want to adjust the threshold.

Threshold

The current on-hold threshold for the action.

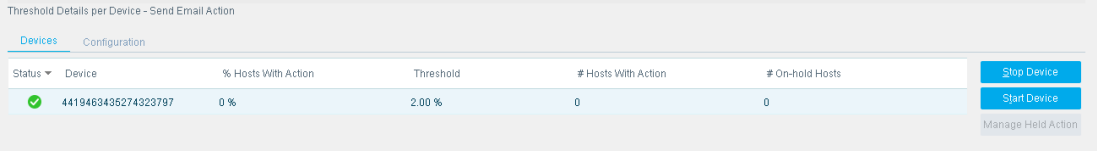
Policies

Policies that include this action.

Select an action from this section and review detailed threshold information in the Threshold Details area. This section displays threshold information for the action you select in the Actions area, for example, the current number of endpoints On-hold at a specific device for the Virtual Firewall action. You can also use the tools in this section to:

- Change the default threshold.
- Create threshold policy exceptions; policies to exclude from action threshold calculations. For example, exclude all policies that handle organizational visitors.
- Configure thresholds if you are working in small environments.
- Start or stop a device.
- Cancel the On-Hold mechanism.
- Include or exclude endpoints that were manually assigned an action.

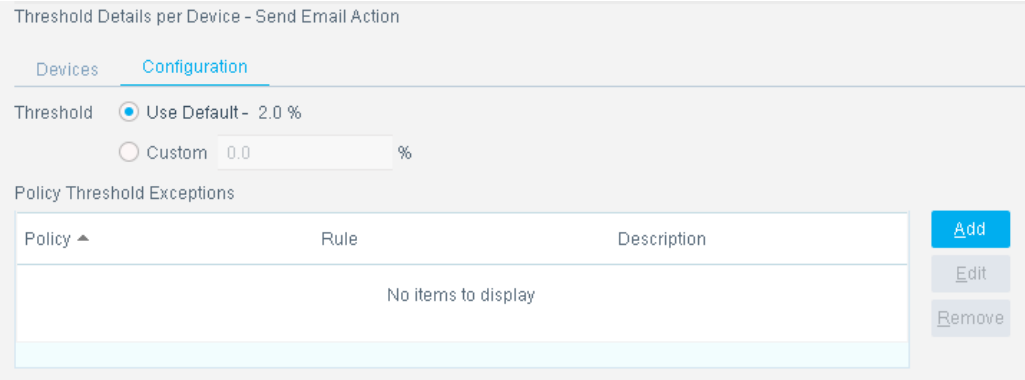
The Devices tab describes threshold information for an action you select in the Actions area, for example, the current number of endpoints on hold at a specific device for the Send Email action.



Status	The On-hold status for the action on the selected device. A green check-mark means that the action is not On-hold at this device. A blue icon indicates that it is.
Device	The device IP address.
Threshold	The current threshold for this action. The threshold is identical on all devices and varies by default per action.
% Hosts With Action	The percentage of endpoints on the device that are targeted for the action selected in the Actions section. Some actions may be carried out, while others may be on-hold because of a threshold violation.
# Hosts With Action	The total number of endpoints on the device to which the action applies. Endpoints detected by policies that are configured as threshold exceptions are not counted.
# On-hold Hosts	The number of endpoints on the device that are not being controlled by the action because of a threshold violation – On-hold.
Stop Device	When you stop a device, all activity on endpoints is halted. You may decide to do this if the action is causing unexpected results.

Manage Held Action	Define how to handle a held action on previously detected endpoints. Options: • Perform the action. • Cancel the action. The action remains canceled until it is either deleted or unmatched to a policy and then matched. • Leave the action on-hold. After releasing the on-hold mechanism, you can continue blocking or restricting newly detected endpoints.

Use the Configuration tab of the Thresholds pane to change the default configuration for the threshold and to create threshold policy exceptions – policies that you want to exclude from action threshold calculations. For example, exclude all policies that handle organizational visitors. You can exclude an entire policy or a specific rule. Threshold values that contain fractions are rounded to the nearest whole number.



Minimal number of hosts	The minimum number of endpoints that are counted for an action before enforcing a threshold. For example, wait until 20 endpoints are detected with a certain action before calculating the threshold. This setting applies to all devices. The calculation is done by each device separately. The default setting is 10 endpoints. In small enterprises with fewer endpoints, the default threshold may be initiated too soon. For example, if the threshold is 1% and less than 100 endpoints are assigned to the device, then the first action will bypass the threshold. Conversely, in large organizations, the threshold may need to be lowered.
Count Manual Actions	By default, endpoints that were manually assigned actions are included in the endpoint count. To exclude these endpoints, clear this option.

Managing actions on-hold on a specific device

If too many actions are not being carried out, you can take the following actions to release the On-hold mechanism on previously detected endpoints.

- Increase the action threshold in the Configuration tab from the Options > NAC > Actions Thresholds pane.
- Stop the relevant policies.
- Increase the minimum number of endpoints to detect.
- Add the relevant policies to the Policy Threshold Exceptions list in the Configuration tab from Tools > Options > NAC > Actions Thresholds.
- Apply the Manage Held Action option to selected devices.

Approve actions on a specific endpoints

You can release the On-hold status for specific endpoints and approve the action.

1. In the Detections pane, click the Actions column header, and look for the hourglass icon. This icon indicates endpoints that are On-hold or Pending. The first set of endpoints is On-hold.
2. Right-click the endpoint, and then select Approve Actions. Select the action that you want to release from On-hold.

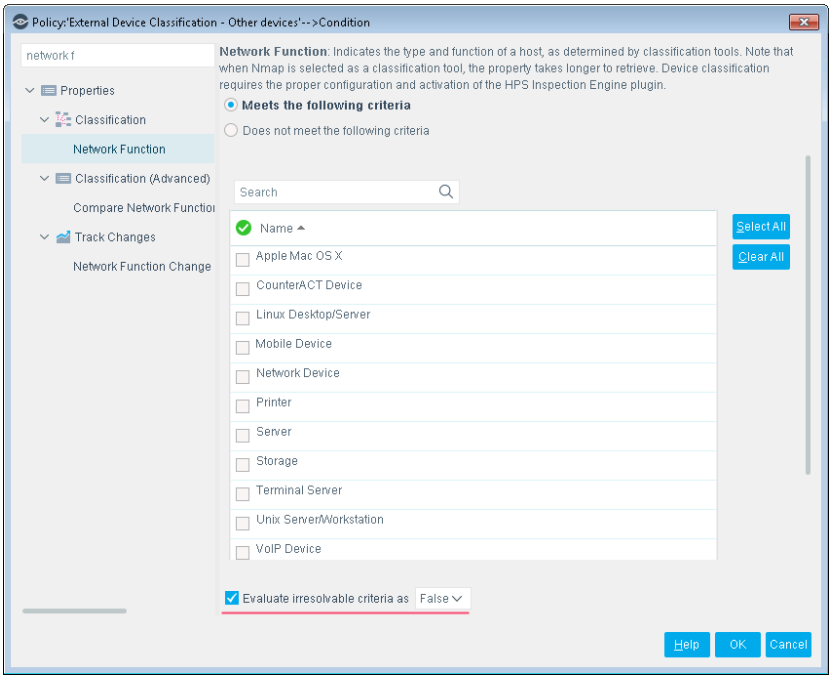
Handling irresolvable criteria

In some situations, eyeSight eyeSight cannot properly resolve endpoint property criteria. Such criteria are considered irresolvable criteria.

Property criteria can have a status of Irresolvable for one of two reasons:

- eyeSight eyeSight failed to resolve the criteria.
- A system error caused eyeSight eyeSight not to respond to the resolve request (for example, a plugin is not running or experienced a timeout).

Many properties provide an option for handling irresolvable criteria. If eyeSight eyeSight cannot verify a property, you can choose how to resolve that endpoint.



You can instruct eyeSight eyeSight to handle irresolvable criteria as follows:

True	Treat the endpoint as if it matches the criteria defined for the property.
False	Treat the endpoint as if it does not match the criteria defined for the property.

If you do not select the Evaluate irresolvable criteria as option, the criteria is handled as irresolvable and the endpoint does not undergo further analysis. The endpoint is not checked to see if it matches additional condition criteria

By default, all irresolvable criteria are evaluated according to the user-defined settings configured in the property (Evaluate irresolvable criteria as True/False).

However, when criteria are irresolvable due to a system error, you can change this default setting. Because this status did not stem from an actual failure to resolve, but rather from of an error, this resolution can be considered imprecise. As a result, you can override any user-defined settings and continue to evaluate such criteria as irresolvable. The endpoint does not undergo further analysis and is not checked against additional condition criteria.

To access this setting, select Tools > Options > Advanced Policy.

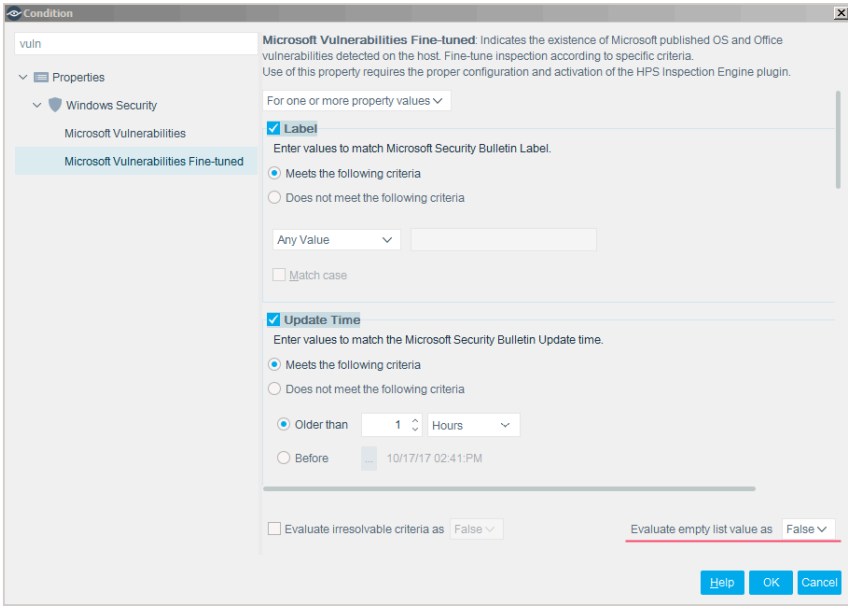
Evaluate criteria that is irresolvable due to a system error	Determines how to handle irresolvable criteria that are not caused by a failure to resolve the property. • Always as Irresolvable - continue to evaluate Irresolvable criteria as such when the evaluation was caused by a system error. • According to user-defined settings per property -irresolvable criteria are evaluated according to the user-defined settings configured in the property.

Handling criteria defined as empty lists

Properties supply information learned on an endpoint to evaluation criteria. If a property is normally populated with information that is not present on an endpoint, eyeSight eyeSight evaluates the property as an empty list for that endpoint. You can choose to evaluate the properties as True or False in this case.

For example, the Microsoft Vulnerabilities Fine-tuned property is used to report and evaluate the Microsoft vulnerabilities on an endpoint. If the endpoint has no Microsoft vulnerabilities, no content is returned for the property, and a criteria based on this property cannot be evaluated.

Evaluate empty list value as	Determines how to resolve criteria when an endpoint does not contain information reported by a property.


Condition
vuln
Properties
Windows Security
Microsoft Vulnerabilities
Microsoft Vulnerabilities Fine-tuned
Microsoft Vulnerabilities Fine-tuned: Indicates the existence of Microsoft published OS and Office vulnerabilities detected on the host. Fine-tune inspection according to specific criteria.
Use of this property requires the proper configuration and activation of the HPS Inspection Engine plugin.
For one or more property values
Label
Enter values to match Microsoft Security Bulletin Label.
Meets the following criteria
Does not meet the following criteria
Any Value
Match case
Update Time
Enter values to match the Microsoft Security Bulletin Update time.
Meets the following criteria
Does not meet the following criteria
Older than
1
Hours
Before
10/17/17 02:41:PM
Evaluate irresolvable criteria as
False
Evaluate empty list value as
False
Help
OK
Cancel

Policy templates

Policy templates are predefined policies that help you:

- Quickly create important, widely used policies based on predefined policy parameters.
- Automatically group network devices into categories that can be used to apply policies.
- More easily control endpoints and guide users to compliance.
- More easily and quickly implement Forescout product capabilities.
- Roll out your policies more safely by applying conditions and actions that have been used and tested.
- Pinpoint any infractions to your security system more quickly.

Create policies using templates – basics

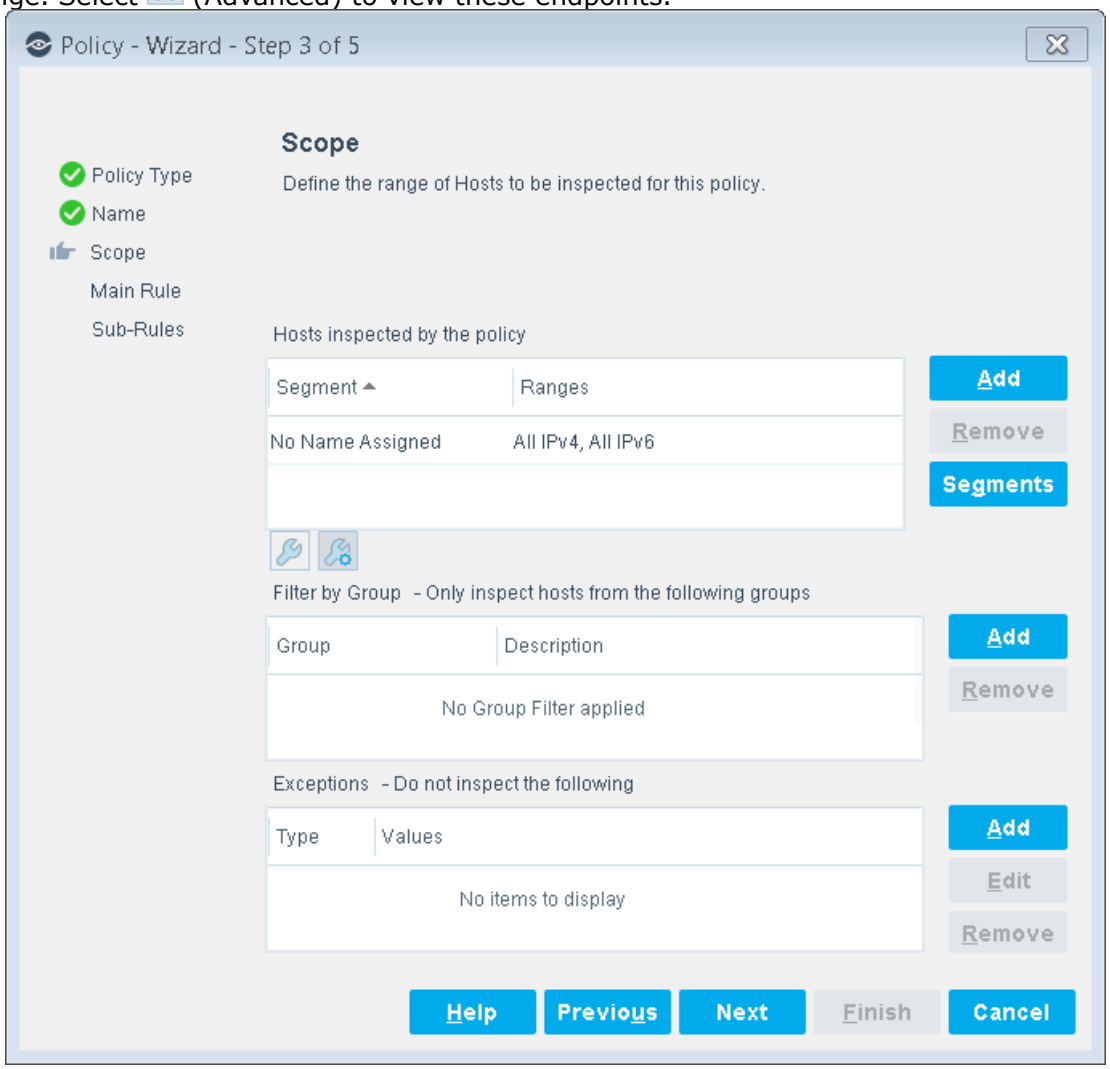
The following table provides a brief description of available Forescout policy templates.

Category	Description
Classification	Create policies that detect network devices according to these categories. Discovered endpoints are placed in Groups that are displayed in the Console, Filters pane.
Corporate/ Guest Control	Create a policy that detects and classifies your network into the following Forescout groups: Corporate endpoints Signed-in guests Guest Hosts (unauthorized endpoints) You can define the policy so that unauthorized endpoints are prompted to sign in with valid credentials or register to the network as guests by providing identity information. Options are also available to allow unauthorized endpoints to skip the registration process and enter the network with limited access.
Compliance	Generate compliance policies, understand the compliance level at your network, guide users to compliance and remediate endpoints.
Threats	Detect and remediate threats to your network by enforcing policies against a range of widely used techniques.
Track Changes	Track Changes host properties, which report a change in the value of a reference property.

Note:
If you installed plugins or modules, related templates may also be available. See Base Modules, Content Modules, and eyeExtend Modules for details.

To create policies from templates:

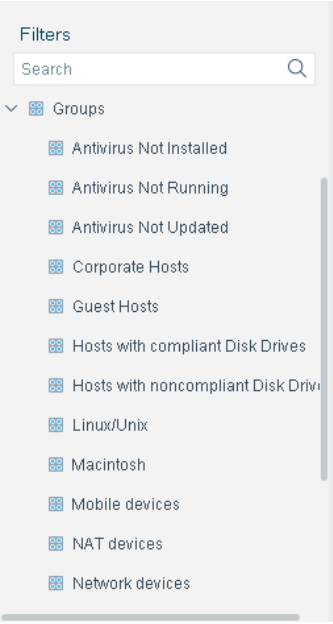
1. Select the Policy tab. The Policy Manager opens.
2. Select Add. The Policy Wizard opens.
3. Select a policy template. The Primary Classification and Corporate/Guest Control policies may have been run during the initial Console setup. If not, run the Primary Classification policy wizard to create device classification groups, and then the Corporate/Guest Control policy wizard, before defining other policies.
4. Select Next.
5. In the Scope pane, enter the IP address ranges or segments to inspect. Some templates are predefined with specific endpoints that should be either included or excluded from the range. Select (Advanced) to view these endpoints.



6. Review the remaining template pages to understand how the template is defined, and provide any undefined parameters.
7. The policy is displayed in the Policy Manager. Select Apply to run it. (Predefined actions are disabled by default.)
8. Verify that the policy results are reasonable for your network. If not reasonable, fine-tune the policy as needed. See Tips for Rolling Out Templates.
9. When you are satisfied with the policy results, run the policy again and, if necessary, enable predefined actions. See Start Actions on Selected Endpoints.

Tips for rolling out templates

To create policies that classify the network into Groups, use the Primary Classification template to create device classification Groups, and then the Corporate/Guest Control template. The groups created by these policies are prerequisites for other policies. As a result, it is important to run and fine-tune these policies first. If you installed the Forescout platform from scratch, then the Primary Classification and the Corporate/Guest Control policies may have been run during initial setup. The created groups should appear in the Console, Filters pane. If you have not run these policies and are working with other templates, you are prompted to create the relevant groups before continuing.



Consider the following when rolling out any policy template or custom policy:

- Do not enable policy actions when first running policies. First, verify that the policy pinpoints the right users and devices, and verify that there were a reasonable number of discoveries.
- Rather than rolling out several policies at the same time, consider working as follows:
  - Deploy one policy.
  - Review and fine-tune the policy.
  - Roll out another policy.
- Initially, avoid rolling out a policy across all enterprise sites. Consider rolling out policies one site at a time, even if the policies will eventually be deployed across the enterprise. Handle the roll-out this way because many sites operate under unique work procedures with site-specific requirements.

Template structure

Templates are predefined to streamline the process of creating policies. Policy templates are built as follows:

- Policy name (there is a predefined default name) and an optional description.
- Policy scope, for example, the endpoints that you want to inspect (filtered for certain

templates).
- Instructions regarding what endpoint properties to look for (conditions). For example, find Windows endpoints that are running peer-to-peer applications (predefined when using templates).
- Instructions regarding measures to take at endpoints, if conditions are met, actions. For example, send email to the IT department when non-corporate installations are found (predefined when using templates). Template actions are disabled by default.

For more information about these policy elements, see Create a Custom Policy.

Detections and actions resulting from the template policies appear in the Home view, and can be managed from there.

Windows OS enhanced classification template

Use this template to retrieve detailed Windows OS information from managed devices in order to assess their risk scoring handling priorities. This policy considers the actual hotfixes already installed on the devices, to improve the accuracy of the risk scores for the devices.

To create a policy:

1. Select Add from the Policy Manager and expand the Classification folder.
2. Select Windows OS Enhanced Classification.
3. Select Next, and complete the policy creation wizard.

Policy Sub-Rule

The sub-rule for this template is matched for the following conditions:

- Windows Hotfix Installed: Indicates the existence of a security update on the host. Use of this property requires the proper configuration and activation of the HPS Inspection Engine. Use of this property requires the proper configuration and activation of the HPS Inspection Engine.
- Windows Version Fine-tuned: Indicates the specific version of Windows running on the host.

Primary classification template

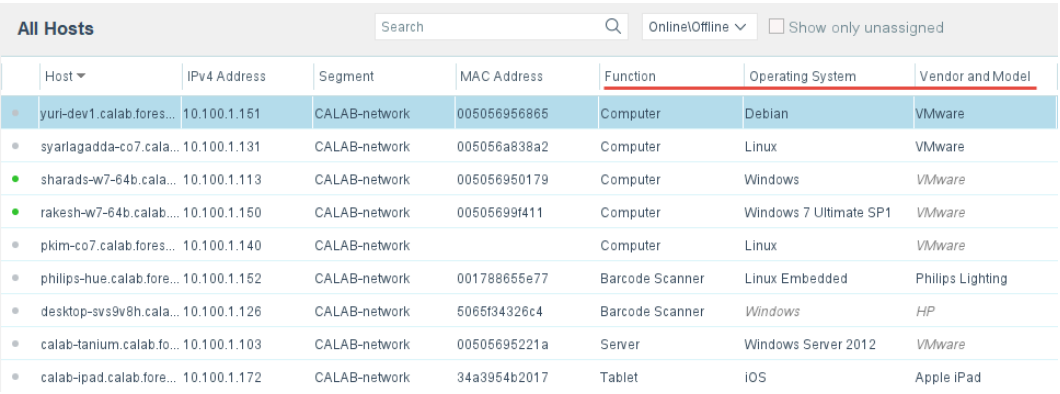
Classification is an objective assessment of what a device is, from a functionality, operating system, manufacturer, and model point of view. eyeSight eyeSight uses all the data discovered about each device to intelligently figure out what the device is.

The Primary Classification policy template, a feature of the Device Classification Engine, uses a vast array of information provided by various eyeSight components to determine the function, operating system, vendor, and model of each endpoint. The policy template then uses this classification information as conditions for sub-rules to broadly classify the endpoints.

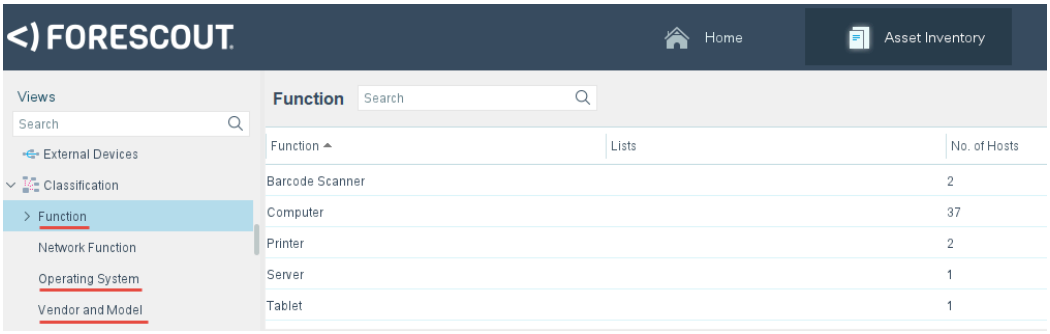
Classification Enabled by Default

Forescout eyeSight automatically discovers classification properties: Function, Operating System, and Vendor and Model,, accessed through Tools > Options > Discovery > Inventory, prior to configuring or running the Primary Classification policy template. See Working with Asset Inventory Detections for more information.

Data for classification properties is added to endpoints in the All Hosts pane.



Classification properties are added to the Classification folder of the Asset Inventory.



Replacing Asset Classification Policies

Upgraded versions of Forescout might include legacy Asset Classification policies that provide limited information about endpoints. To take advantage of more precise classification profiles, it is recommended to create and run Primary Classification policies.

The Primary Classification policy provides more comprehensive classification in your environment than legacy Asset Classification policies. To use it as your primary classification policy, ensure that the Add to Group actions are enabled in the Primary Classification policy, and use the Policy Manager to stop your Asset Classification policies.

Template classification groups

Policies created based on the Primary Classification template can create Forescout groups for various device categories, and automatically place each endpoint in the appropriate device group.

eyeSight devices are placed in their own groups.

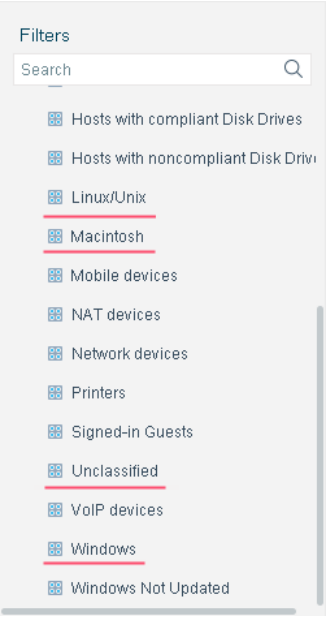
If a device does not meet the criteria for any group or if eyeSight cannot evaluate the endpoint, it is placed in an Unclassified group. The operator may then choose to manually classify the device. See Use an Action to Assign a Classification.

Note:
Legacy Asset Classification policies include all eyeSight devices and network storage devices in the Network devices group.

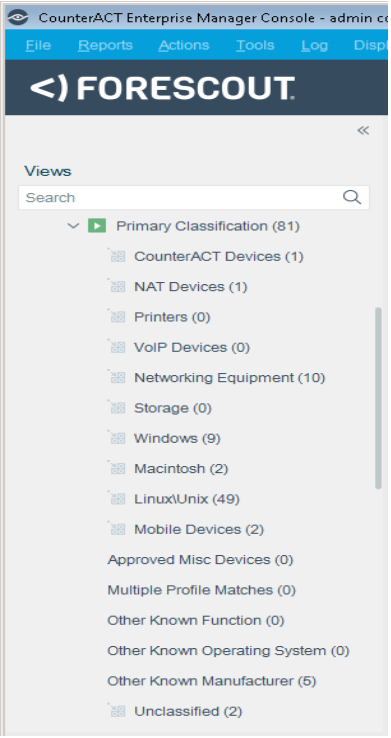
Note:

The Primary Classification template includes a sub-rule that indicates if a member of the Exempt-Approved Misc Devices group does not meet the criteria for a classification category. It is recommended to add to this group all the endpoints that eyeSight does not classify, but that you know about and specifically do not want to fall into the Unclassified group.

Groups created by this policy are used when running policies created by other templates. Organizing your endpoints into groups makes it easier to create and manage other policies and track policy results. These groups appear in the Groups tree in the Console Home tab, Filters pane. When you select a group, associated endpoints appear in the Console, Detections pane.



In addition, a sub-rule is created for each group type. You can view each policy's sub-rules under Policies in the Console Home tab, Views pane.



When a Primary Classification policy is run, the following endpoint classification properties are resolved:

- Function
- Operating System
- Vendor and Model
- Suggested Function – Indicates all the Function property values that matched this endpoint's profile if there were multiple matches
- Suggested Operating System – Indicates all the Operating System property values that matched this endpoint's profile if there were multiple matches
- Function Classified By – Indicates if the Function property value was determined by the Device Classification Engine or was set by an action
- Operating System Classification Update – Indicates if the Operating System property value was determined by the Device Classification Engine or was set by an action

Note:

c These properties are not resolved by legacy Asset Classification policies.

Create a primary classification policy

This topic describes how to use the Primary Classification template to create a policy.

Before you create the policy:

- Consider which endpoints you want to inspect. The policy does not handle endpoints outside of the Internal Network.
- Ensure that a Primary Classification policy using the Add to Group actions is run before any other policy.

  To create a policy, select Add from the Policy Manager, and expand the Classification folder.

Then select Primary Classification and complete the policy creation wizard.

Classification Policy Scope

Classification policies use both passive and active methods to classify endpoints. Active methods include probing the endpoint to check for a small range of open ports, running Nmap against the endpoint, and attempting to connect using WMI, SMB and/or RRP (depending on your HPS Inspection Engine configuration). To fully benefit from classification, it is recommended to run a classification policy on your entire network. However, if there are endpoints in your network that are known to be sensitive to network probing, it is recommended to exclude these endpoints when creating Primary Classification policies. For details about excluding sensitive endpoints, see Restricting Endpoint Inspection.

Note:
The Primary Classification policy template can resolve classification properties for endpoints even when their IP addresses are unknown.

Device Classification Using a Primary Classification Policy

A Primary Classification policy includes sub-rules for devices found in most environments. It is recommended to enhance the policy by adding additional sub-rules above the Approved Misc Devices sub-rule for devices that are particular to your environment.

A Primary Classification policy attempts to resolve the following classification properties for each connected endpoint:

- Function
- Operating System
- Vendor and Model

When a classification policy cannot match the endpoint to a specific profile in the Device Profile Library:

- If multiple profiles match the endpoint, the property is resolved as the most specific value in the Device Profile Library that is common to all the matching profiles. For example, if Windows Server 2008 Enterprise RTM and Windows Server 2008 Enterprise SP2 operating system profiles both match the endpoint, the Operating System property is resolved as Windows Server 2008 Enterprise.
- If there is no common value among all the matching profiles, the property is resolved as Multiple Suggestions.
- If no profiles in the Device Profile Library match the endpoint, the property is resolved as Unknown.

How Discovered Devices Are Handled – Policy Actions

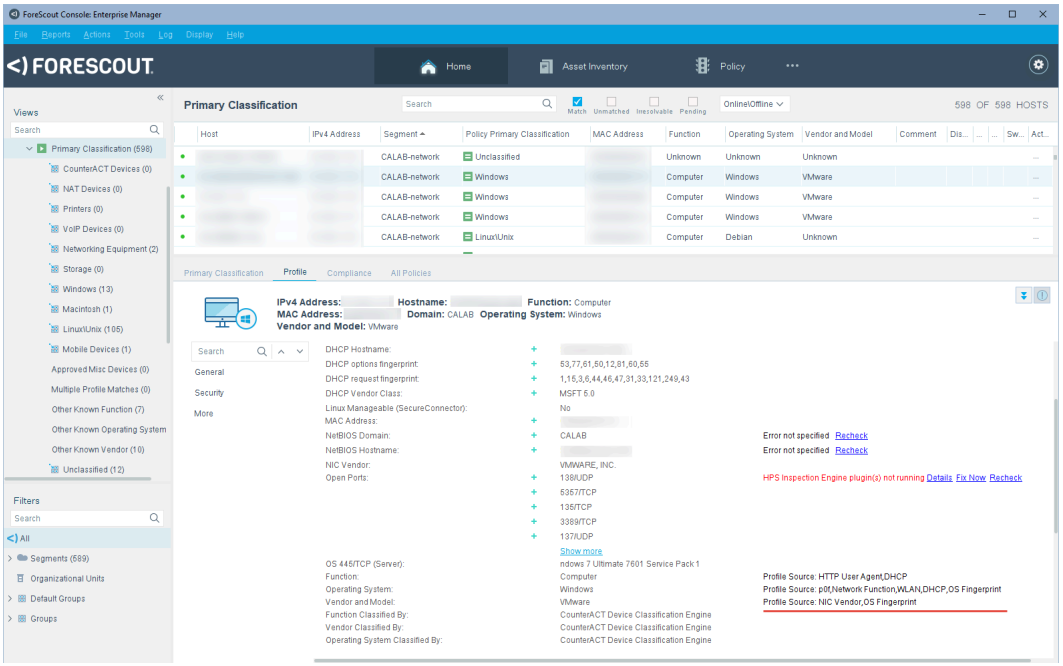
This policy adds each endpoint to a Forescout group according to the device category. These Add to Group actions are enabled by default.

Note:
To avoid possible conflicts with legacy Asset Classification policies, it is recommended to use the Policy Manager to stop all Asset Classification policies used in earlier versions of eyeSight, and to run only Primary Classification policies.

When the Add to Group actions are enabled, endpoints are removed from groups if Forescout eyeSight discovers, during policy recheck, that the device function or type has changed, or if the policy has been stopped.

How an endpoint was classified

To view information about how the Primary Classification template and the Device Classification Engine classified an endpoint, select the Show troubleshooting messages icon in the Profile tab of the Details pane.



The Profile Sources are displayed to the right of the Function, Operating System, and Vendor and Model fields. This is the list of labels of the host properties in the matched fingerprints for that endpoint.eIf all or some of the host properties and the corresponding values of an endpoint match the condition of a fingerprint defined by the Device Profile Library, the fingerprint matches for that endpoint. There can be multiple matched fingerprints for an endpoint.All the labels of the host properties defined in the matched fingerprints are displayed, including those properties that were not used in the matching process.

Use an action to assign a classification

You can use the Classify actions to override an endpoint classification property set by a Primary Classification policy. Changing a property value may cause the endpoint to match a different policy sub-rule when your classification policy is run again. If the Add to Group actions are enabled in your classification policy, the endpoint is added to the appropriate group.

It is useful to manually assign a classification in the following situations:

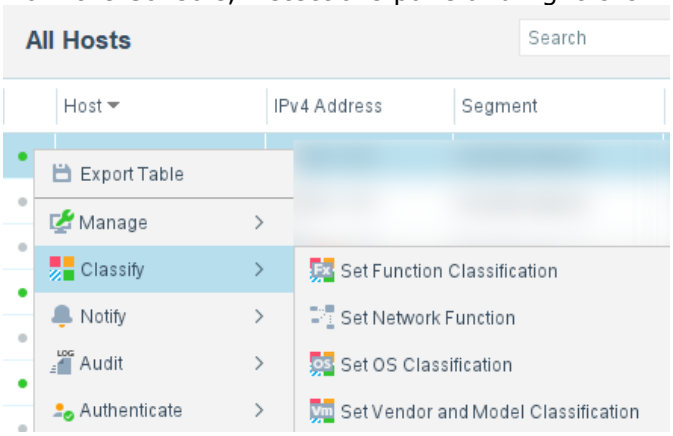
- The classification resolved by eyeSight eyeSight is not correct or eyeSight eyeSight was not able to resolve a classification.
- You are able to refine the device's classification. For example, eyeSight resolved the device Function property as a Healthcare, but you know it's actually an X-Ray device.
- The endpoint was excluded from the range of endpoints to be classified due to its sensitivity to probing

You can use the Cancel Actions action to easily revert your manual classification assignments to those set by your classification policy.

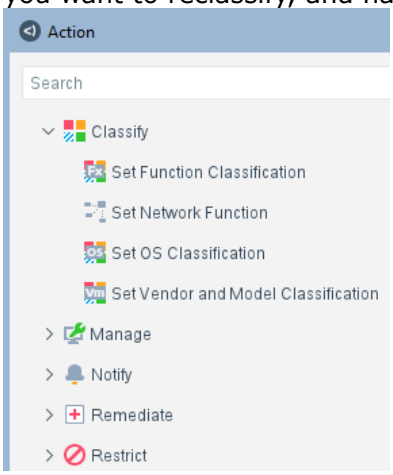
After a Set Function Classification, Set OS Classification, or Set Vendor and Model Classification action is used to change a property value, the new value causes the endpoint to match a different sub-rule in the Primary Classification policy. If the Add to Group policy actions are enabled, the endpoint is added to the appropriate group.

To use Actions to classify devices, do one of the following:

- To manually classify one or more endpoints, select the endpoints that you want to classify from the Console, Detections pane and right-click.

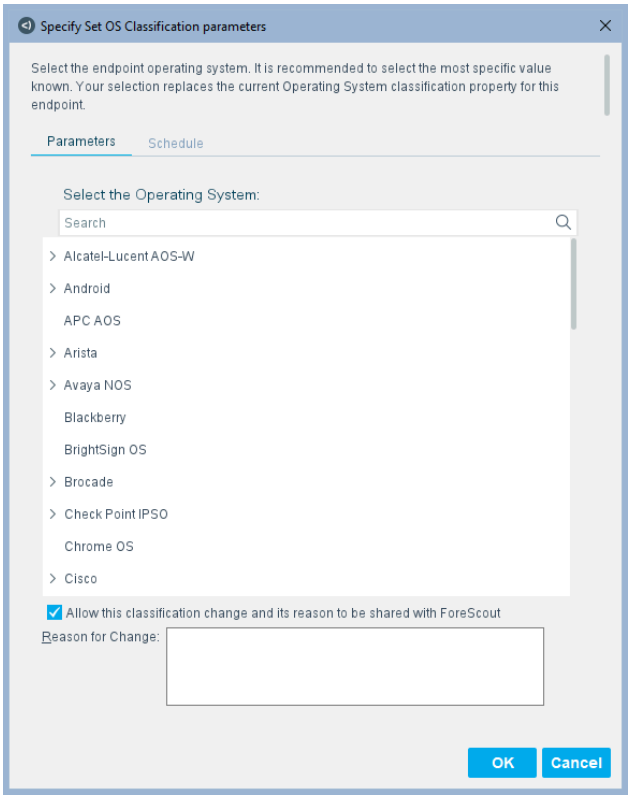


- To reclassify endpoints using a policy, set the policy conditions to detect the endpoints that you want to reclassify, and navigate to the Actions tree from the Policy Actions dialog box.

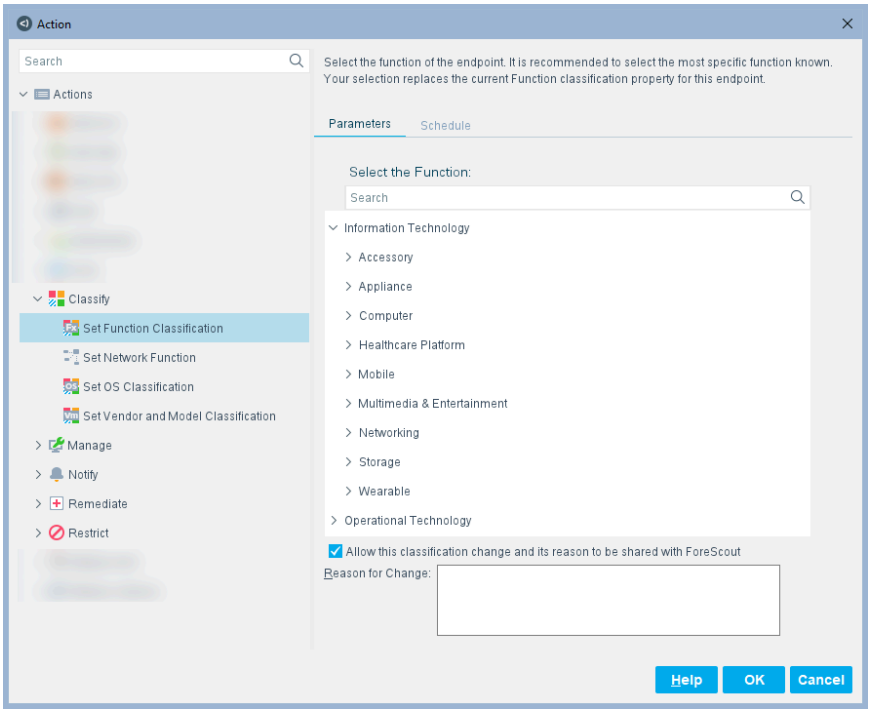


- Expand the Classify folder, and select the classification property to be set:
  - Set Function Classification
  - Set Network Function
  - Set OS Classification
  - Set Vendor and Model Classification

    From an endpoint:



From a policy:



- Select the appropriate property value.
- If you agree to provide the Forescout Research Program with information about the change, select the checkbox, and enter:
    - The reason why the selected classification is appropriate for this endpoint

- The ideal classification for this endpoint, if it is not in the classification list

Note:
Your changes are shared with The Forescout Research Program if you did not opt out of the program.

Your feedback is sent to Forescout to help provide better classification services.

Fine-tune the classification mechanism

Several methods are used for retrieving classification information, for example, Nmap tools, domain credentials, information resolved on devices managed by SecureConnector, or switches configured to work with the eyeSight.

Nmap tools are used if other mechanisms are unable to resolve the endpoint classification.

You can fine-tune the Nmap classification.

Note:
You can prevent Nmap fingerprinting of endpoints that are sensitive to network traffic. See Restricting Endpoint Inspection .

To fine-tune Nmap classification, select Tools > Options > HPS Inspection Engine. Select the Classification tab and update Nmap settings as required. Refer to the HPS Inspection Engine Configuration Guide for more details.

Classification upgrade impact analysis template

Note:
This template is only relevant to eyeSight users who have upgraded to this release from an earlier release.

If HPS Inspection Engine in your environment is currently configured to use Classification version 2, it is strongly recommended to upgrade to version 3. Version 3 uses a newer version of Nmap to improve the underlying classification capabilities of eyeSight. This upgrade changes how the Network Function property is resolved during endpoint classification.

The Classification Upgrade Impact Analysis policy template lets you examine the possible impact of upgrading eyeSight Classification tools, including changes in how endpoints are handled by Asset Classification policies.

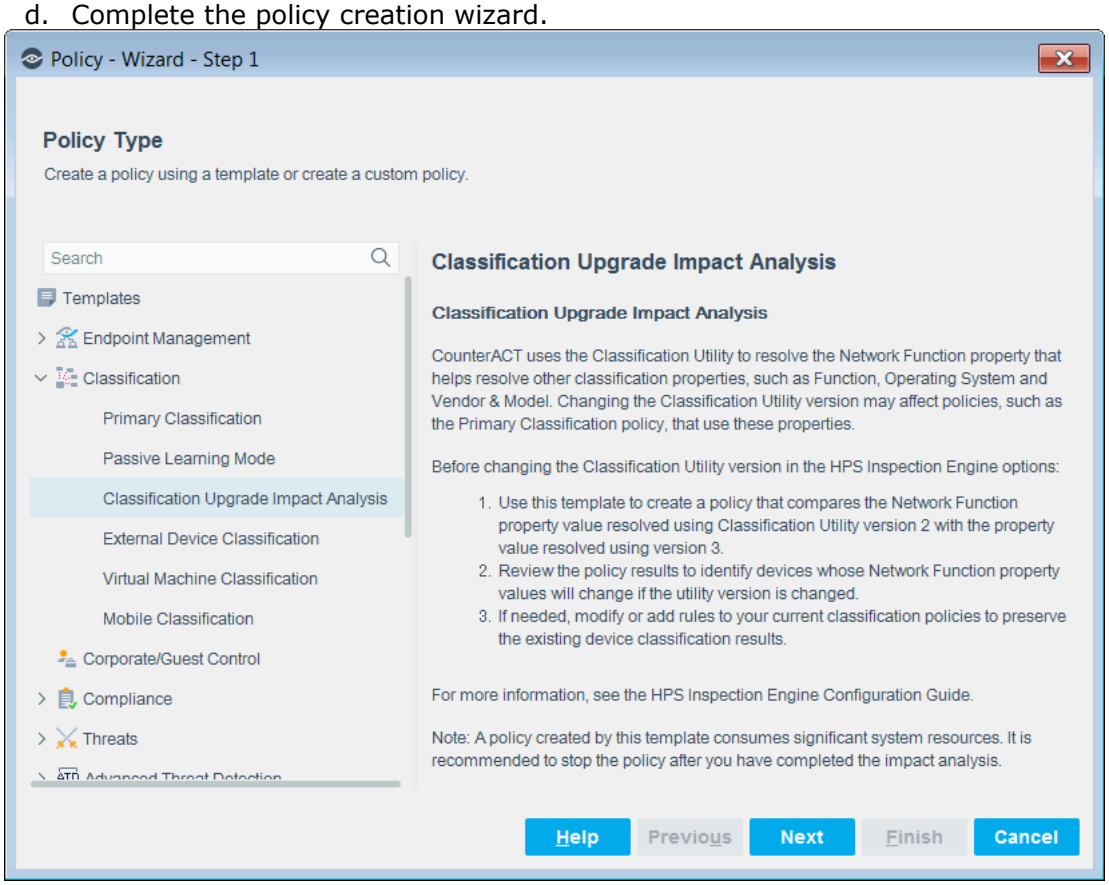
When you change the set of classification methods used by eyeSight, there may be significant changes in the results of the plugin's classification processes. These changes are evident when some endpoints receive new values for the Network Function and OS Fingerprint properties and can strongly influence how classification policies evaluate endpoints.

The Classification Upgrade Impact Analysis template lets you examine the impact of changing eyeSight from Classification version 2 to Classification version 3.

Before you change the Classification version, we highly recommend to follow this procedure:

1. Create a policy based on this template, to detect endpoints for which the new and old classification methods yield different results.:
    a. Select Add from the Policy Manager.

b. Open the Classification folder.
c. Select Classification Upgrade Impact Analysis.
d. Complete the policy creation wizard.



Note:
The Unknown IP addresses option is not applicable to this template. This policy is applicable only to endpoints with IP addresses.

2. Carefully analyze the endpoints which are classified differently by the two classification versions, especially these cases:
   - Endpoints classified correctly by classification version 2, but not classified at all under version 3
   - Endpoints classified correctly by classification version 2, but classified incorrectly under classification version 3
3. Decide how to handle changes in classification results. If necessary, adjust existing classification policies to ensure that all endpoints are correctly classified by classification version 3. You may need to create rules that use the Classify action to apply a desired classification to some endpoints. You may also find that many endpoints which were not accurately classified by classification version 2 are now handled correctly by the improved capabilities of classification version 3. In these cases, you may be able to remove sub-rules that you inserted to correct automatic classification, simplifying classification policies.

Prerequisites

- Classification version 2 is currently configured.
- Consider which endpoints you want to inspect. The policy does not handle endpoints outside of the Internal Network.

How Devices Are Classified and Compared – Policy Conditions

You can learn more about how the classification comparison is carried out by viewing policy conditions.

Sub-Rule Result	Description
Versions 2 and 3 Differently Classified	The results for classification version 2 and 3 are different. Review the differences and manually assign a classification, if required. See Use an Action to Assign a Classification. This is optional.
Version 2 Classified and Version 3 Unclassified	eyeSight did not classify the asset using classification version 3. These assets were previously classified using version 2. Manually assign a classification if the number of unclassified devices is minimal. See Use an Action to Assign a Classification. This is optional. If there are an extensive number of unclassified devices, contact your Forescout representative.
Version 2 Unclassified and Version 3 Classified	eyeSight classified the asset using classification version 3. These assets were previously unclassified.
Versions Identically Classified	The results for classification version 2 and 3 are identical.
Both Versions are Unclassified	eyeSight did not classify the asset in either version. Manually assign a classification if the number of unclassified devices is minimal. See Use an Action to Assign a Classification. This is optional. If you there are an extensive number of unclassified devices, contact your Forescout representative.
Version 2 Unclassified – Offline Hosts	eyeSight classified the assets in version 2. In version 3, they are unclassified because the assets are offline.

Compare classification results

After running the Classification Upgrade Impact Analysis policy from the Policy Manager, you can compare classification results between versions 1 and 2. Classification version 2 delivers more accurate results. Migration from version 1 to version 2, however, may change some classifications.

To compare results:

1. Select the Console Home tab.
2. From the Views pane, navigate to the Classification Upgrade Impact Analysis policy.

3. Select a sub-rule from the Migration Classification policy in the Views pane. Information about endpoints inspected in the sub-rule appears in the Detections pane.
4. Select an endpoint. Endpoint details appear in the Details pane.
5. Select the tab with the related sub-rule.
6. Expand the folder with the rule. Details about the comparison appear.
7. Review the details.
8. Use an action to manually classify the device, if required. See Use an Action to Assign a Classification.

Stop the migration classification policy

The Classification Upgrade Impact Analysis policy uses system resources that are not needed after you have reviewed results and made manual assignments where required. When you have completed these tasks, stop the migration policy in Policy Manager.

Upgrade the classification version

You are ready to upgrade the Classification tools used by eyeSight after completing the following:

1. Run the Classification Upgrade Impact Analysis template.
2. Compare results and, where required, use an action to manually classify the device. See Use an Action to Assign a Classification.
3. Stop the Classification Upgrade Impact Analysis policy.

   The upgrade affects your Asset Classification policy and any other policy that uses classified assets. Refer to the HPS Inspection Engine Configuration Guide for details.

Reclassification template

Use the Reclassification template to create a policy to reclassify properties on devices connected to your network, following classification. You can use this template to correct incorrect classifications and classify unclassified devices.

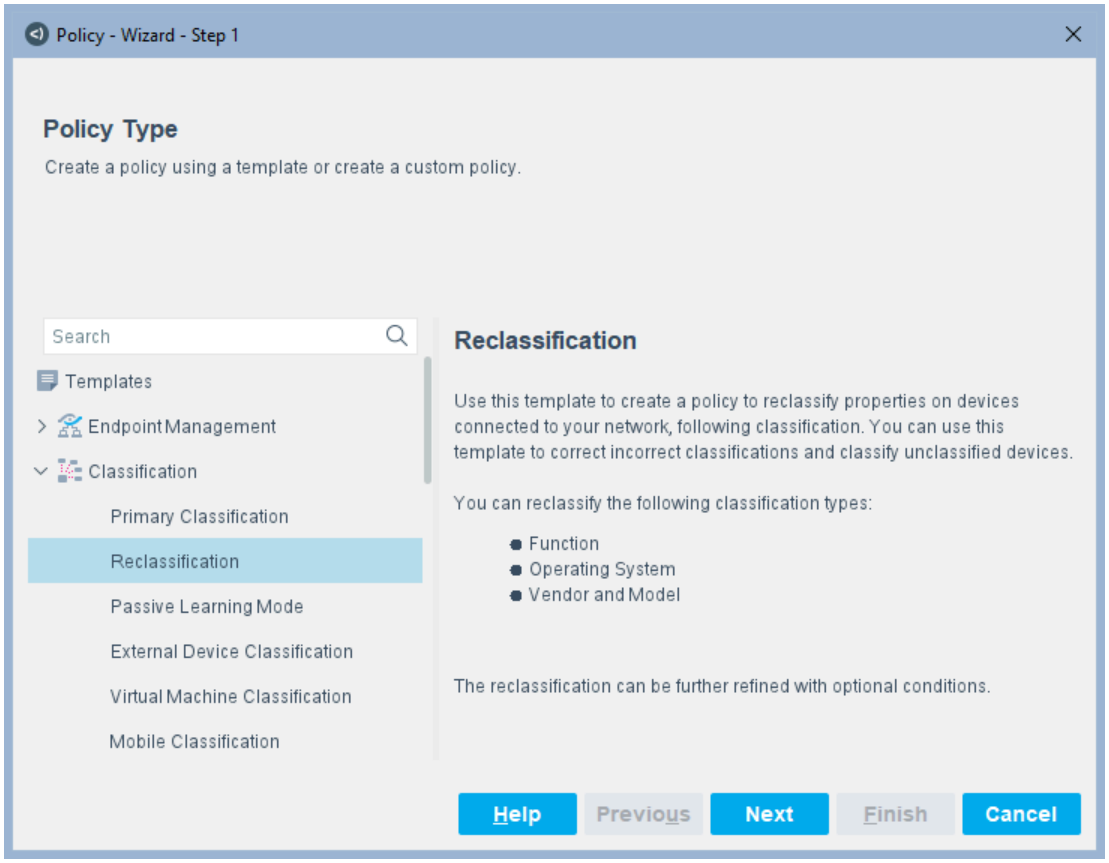
You can reclassify the following classification types:

- Function
- Operating System
- Vendor and Model

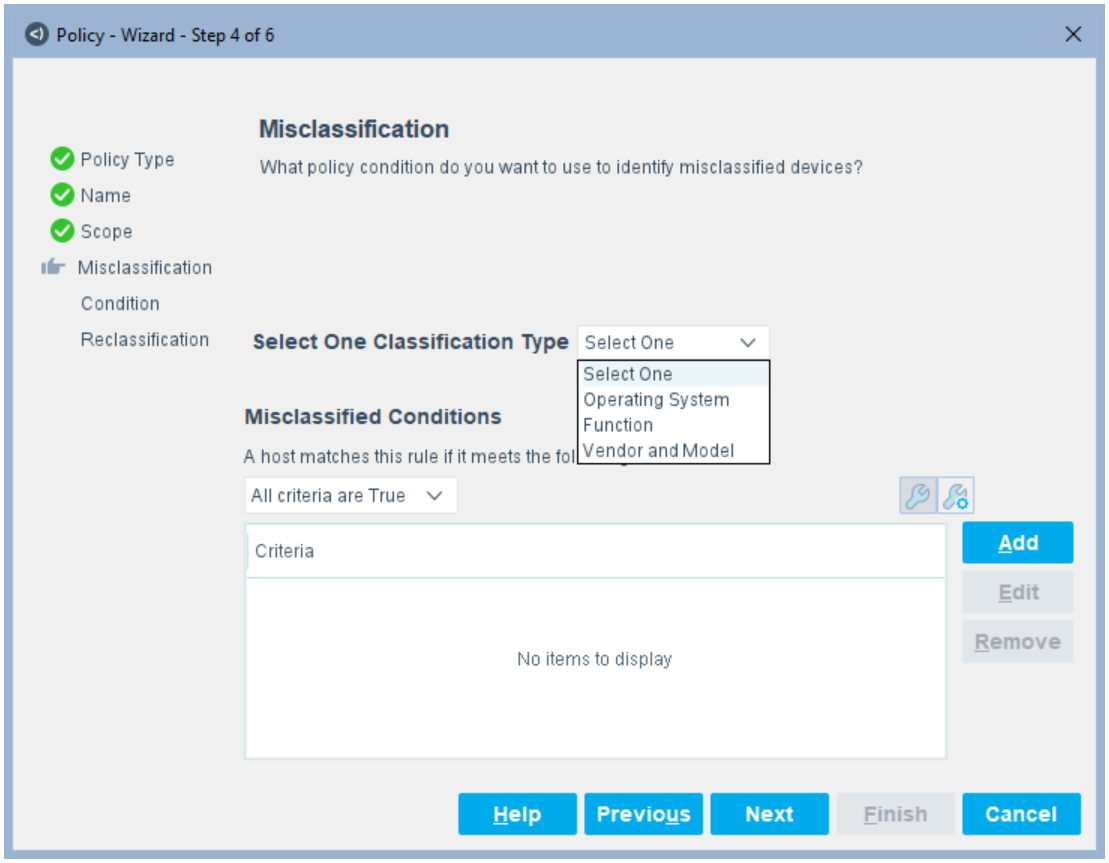
The reclassification can be further refined with optional conditions.

To create a reclassification policy:

1. Select Add from the Policy Manager.
2. Expand the Classification folder and select Reclassification.
3. Complete the policy creation wizard.



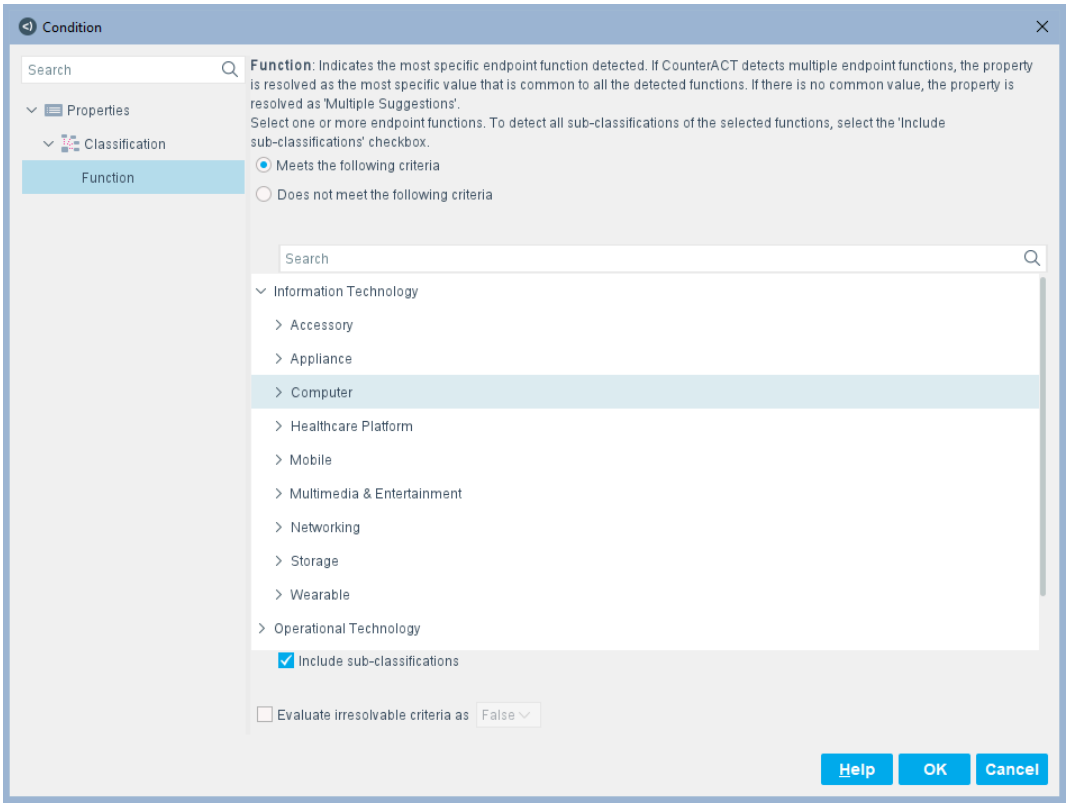
4. Select Next from the Scope dialog. The Misclassification pane opens. On this pane, you will select the misclassified classification type and the condition that is misclassified.



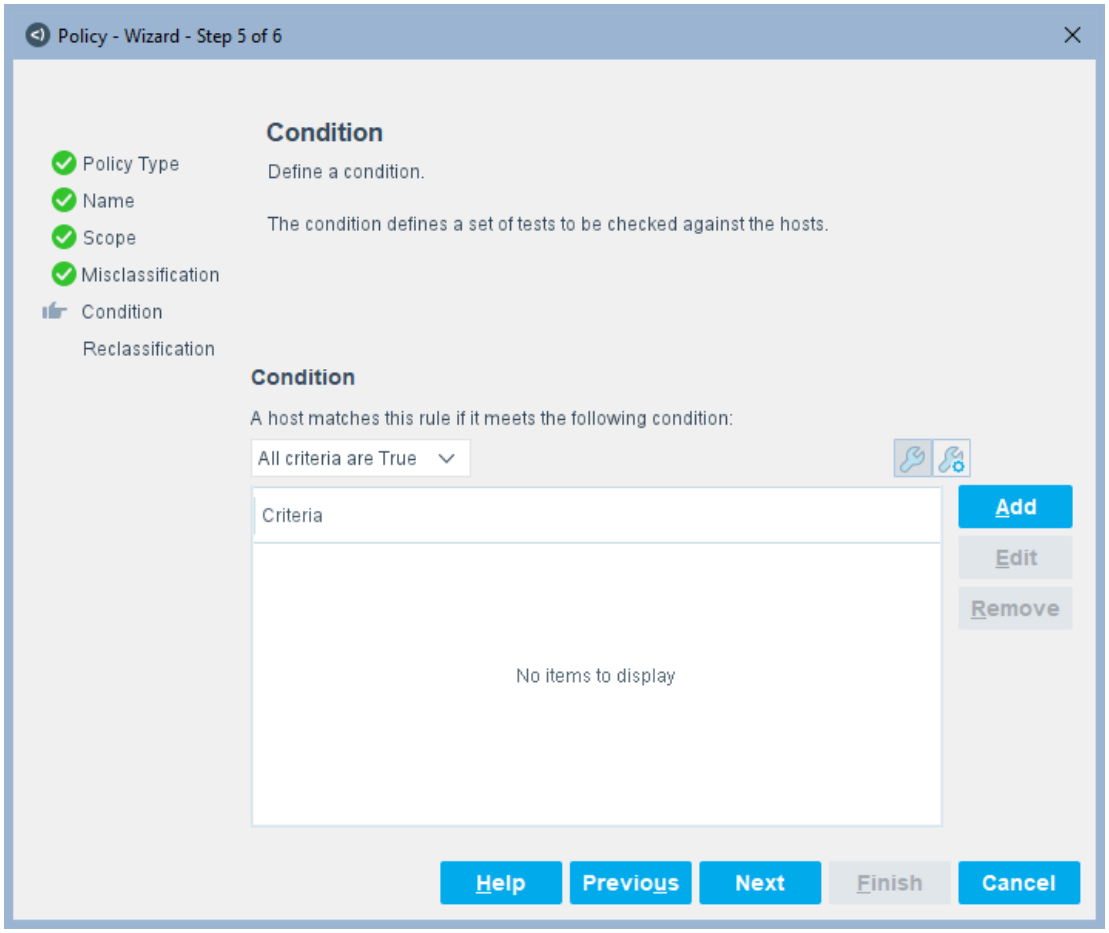
5. Select one classification type from the drop-down menu:
    - Operating System
    - Function
    - Vendor and Model

    For example, if the host function is classified as Computer instead of Gaming, select the type as Function.

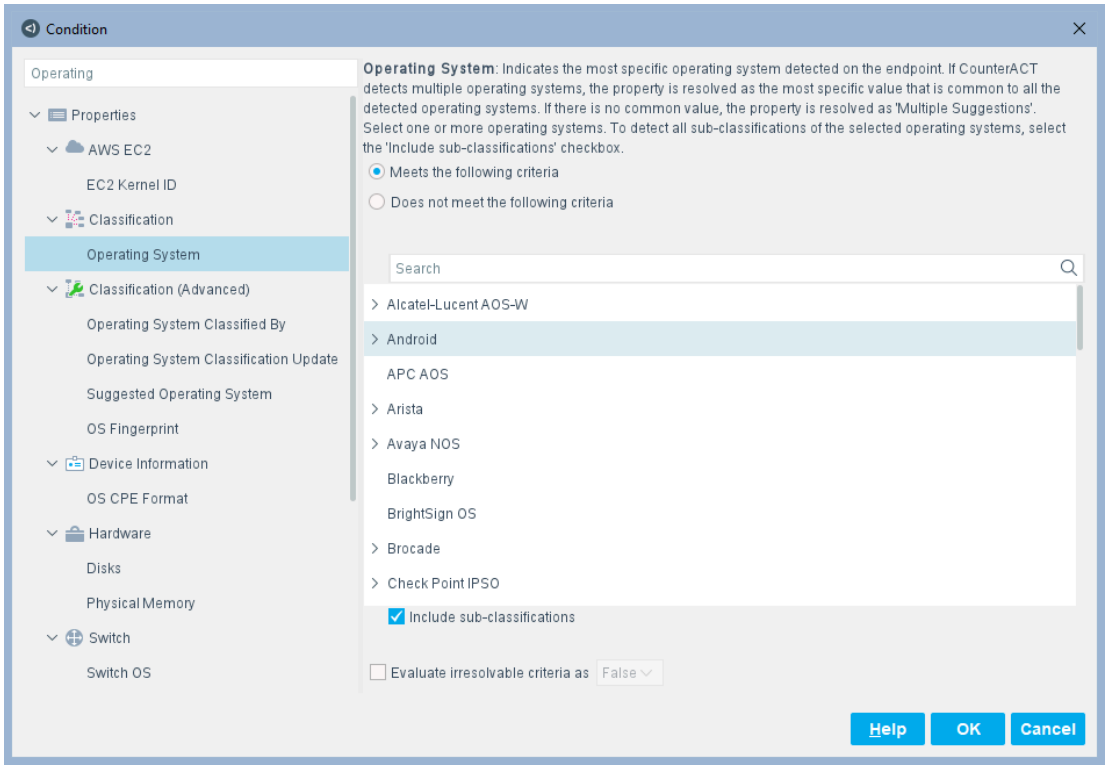
    Then select Add to add a condition. The selected classification type determines the properties that are displayed in the Condition dialog box.



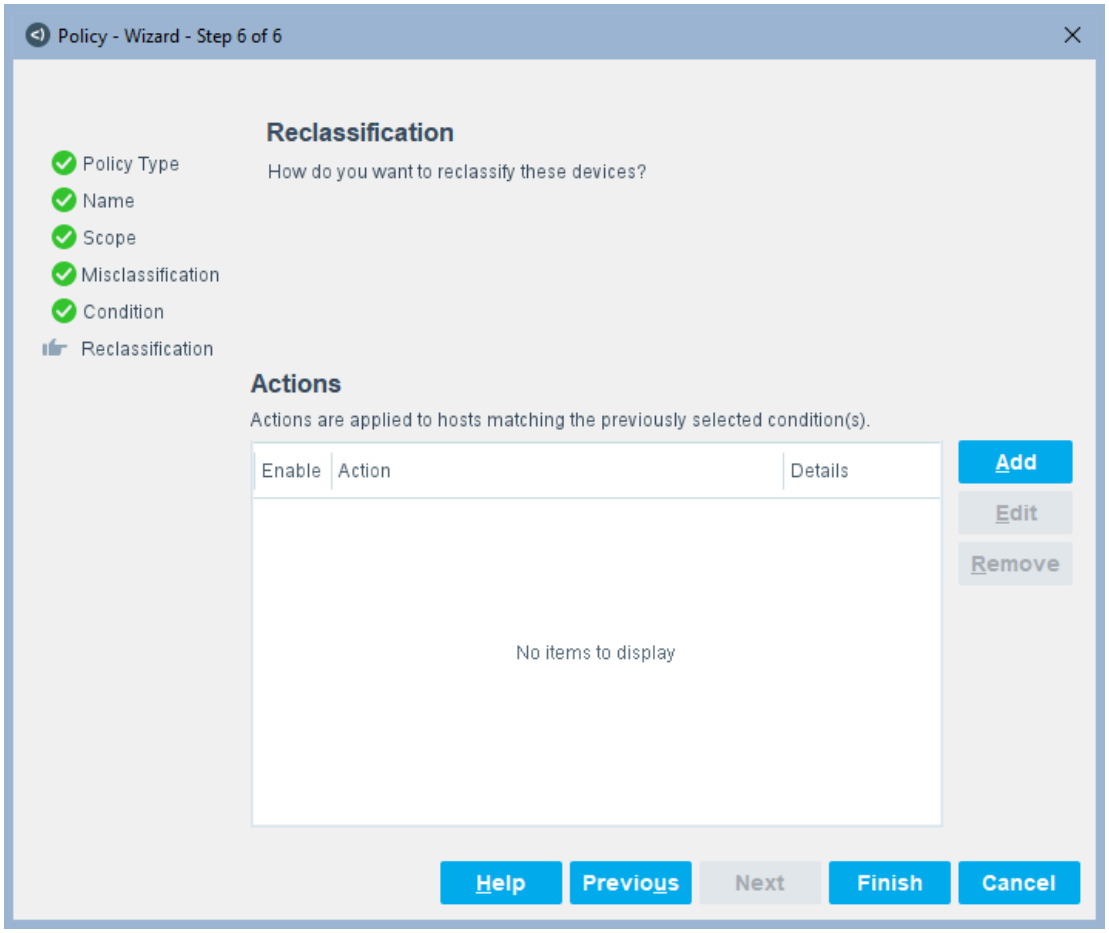
6. Select the condition. For example, if the host function is classified as Computer instead of Gaming, select the misclassified condition as Function > Computer. Select OK.
7. In the Misclassification pane, select Next.



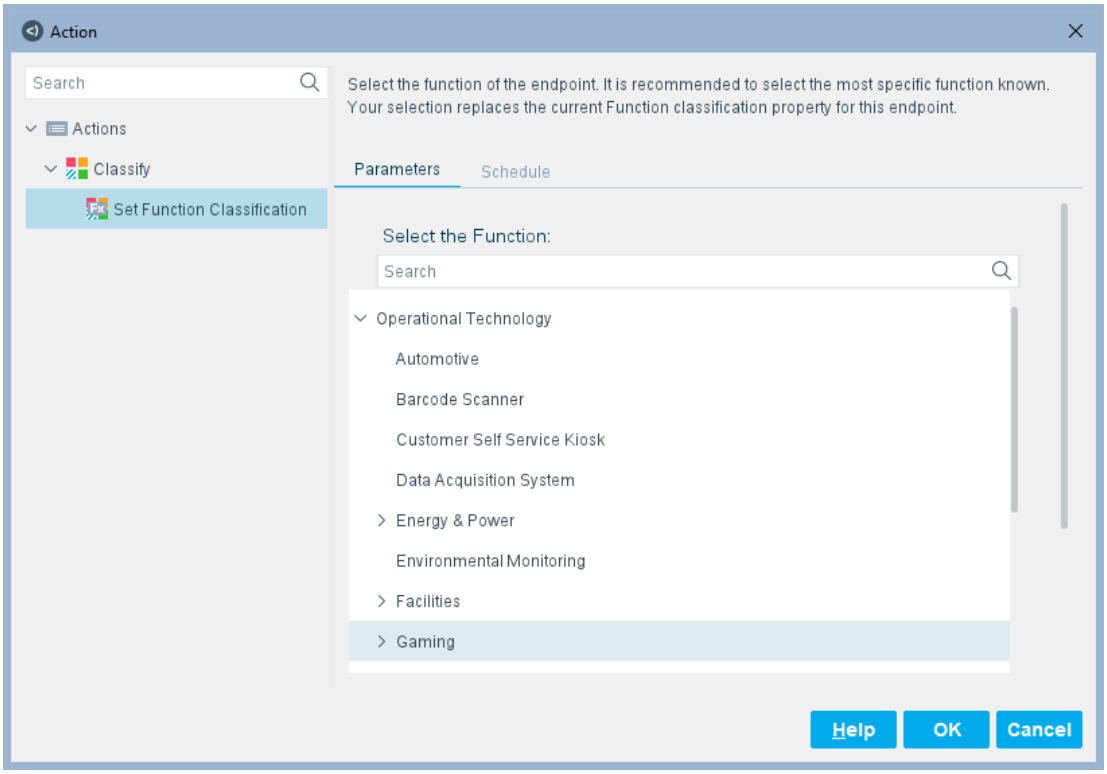
8. (Optional) To filter out hosts, you can add any other conditions, in addition to the misclassified condition. This further refines the classification. Select Add. To skip this step, select Next.



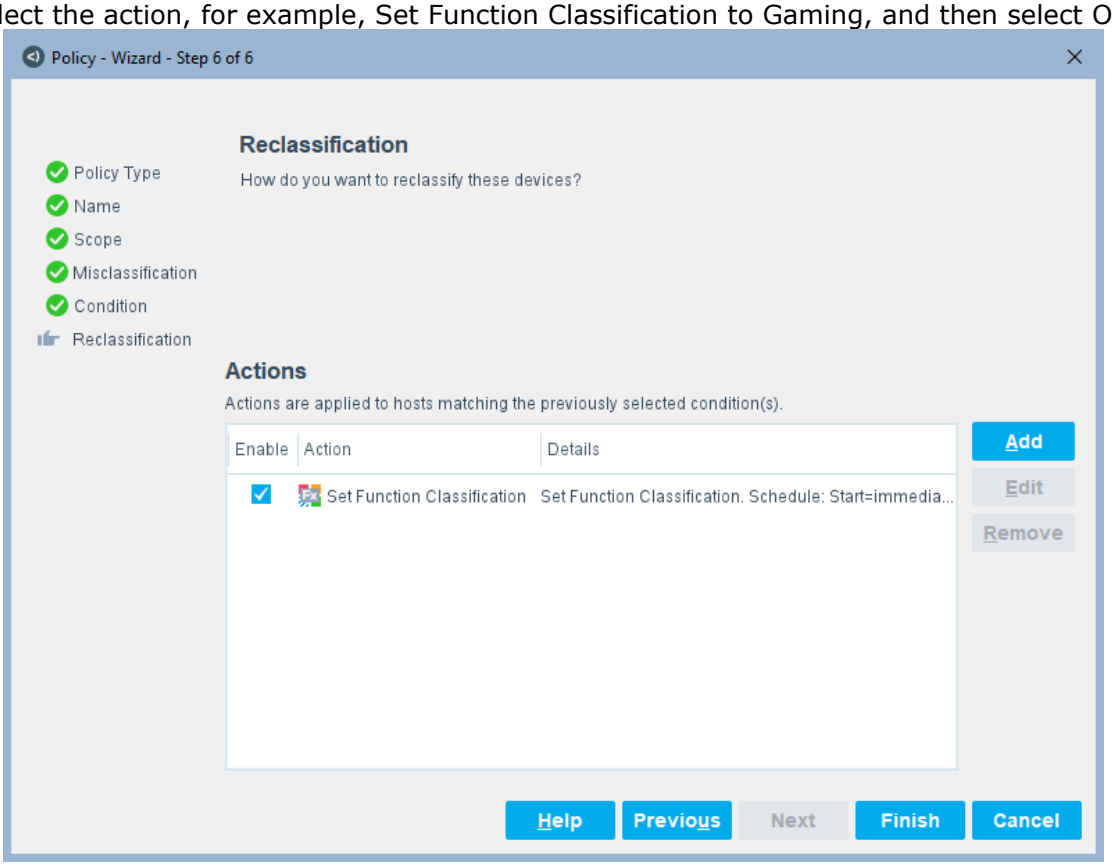
9. Select the condition and then select OK.
10. Select Next.



11. Select Add to select the action to which to set the classification type. The selected classification type determines the properties that are displayed in the Action dialog box.



12. Select the action, for example, Set Function Classification to Gaming, and then select OK.

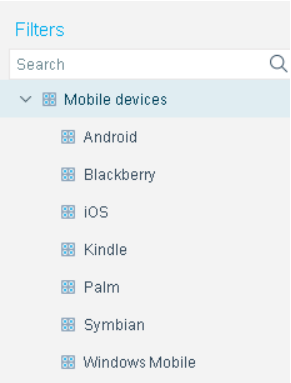


13. Select Finish.

Mobile classification template

This template creates a policy that classifies devices in the Mobile asset group.

When you create and run a policy based on this template, related vendor/protocol sub-groups automatically appear under the Mobile devices group in the Filters pane. When you select a sub-group, its members appear in the Detections pane, where you can view information about them.



Prerequisites

It is recommended to use the Mobile Classification policy template in environments running an Asset Classification policy.

Note:
When using Primary Classification policies, the Function property identifies mobile devices, and Mobile Classification policies are not needed. To act on specific types of mobile devices, it is recommended to use the Operating System and Function property conditions in compliance and control policies.

- Run an Asset Classification policy or Primary Classification policy with the Add to Group actions enabled before running this policy template. This is required because the classification policies create device groups, including the Mobile devices group, on which the Mobile Classification template is based.
- Consider which endpoints you want to inspect. The policy does not handle endpoints outside of the Internal Network.

To create a policy:

1. Select Add from the Policy Manager.
2. Open the Classification folder and select Mobile Classification.
3. Complete the policy creation wizard.

How Forescout eyeSight Detects Mobile Devices – Policy Conditions

eyeSight eyeSight classifies mobile devices by using the following classification properties:

- iOS: Operating System – iOS
- Amazon Fire:
  - Operating System – Android > Amazon Fire OS
  - Vendor and Model – Amazon > Amazon Kindle
- Android: Operating System – Android

- Windows Mobile: Operating System – Windows > Windows Mobile
- Blackberry:
    - Operating System – Blackberry
    - NIC Vendor - RIM
- Symbian: Operating System – Symbian
- Palm: Operating System – Palm OS
- Other: No Conditions

How Discovered Devices Are Handled – Policy Actions

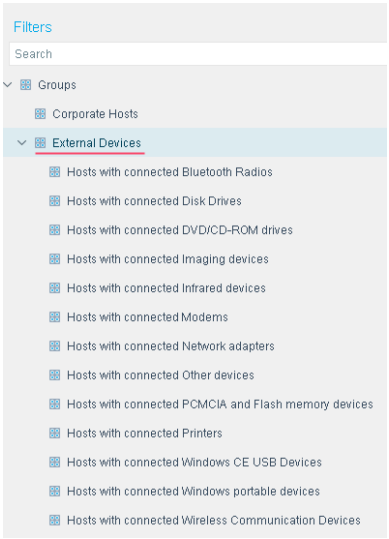
By default, the policy creates Sub-groups according to the mobile device categories. This action is enabled by default.

Endpoints are removed from groups if eyeSight eyeSight discovers, during policy recheck, that the device function or type has changed.

External device classification template

This template creates a policy that detects external devices connected to Windows endpoints.

The policy creates a Forescout External Devices group that includes a sub-group for each external device class that you instruct eyeSight eyeSight to detect. These sub-groups automatically appear under the Groups tree in the Console, Filters pane.



In addition, a policy is created for each group type. You can view these policies in the Policies > External Devices folder in the Views pane.

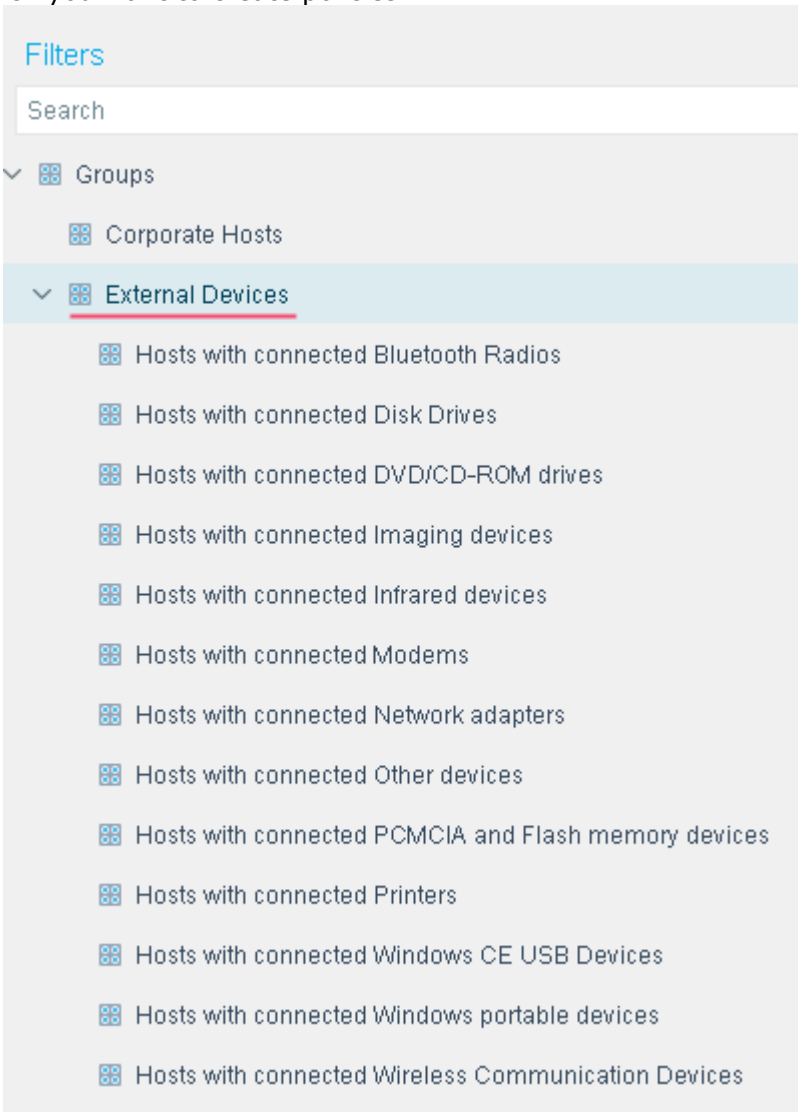
Prerequisites

- Consider which endpoints you want to inspect. The policy does not handle endpoints outside of the Internal Network.
- Run a policy created by this template before running most other policies:
    - External Device groups are used when working with the other templates. The External Device template was most likely run during initial Appliance setup. Check the Filters pane to verify that your endpoints have been classified.
    - Organizing your endpoints into groups makes it easier to create and manage other

policies and easier to track policy results.

To create a policy:

1. Select Add from the Policy Manager.
2. Open the Classification folder and select External Device Classification.
3. Select Next and continue to complete the policy creation wizard.
4. The External Device Classification pane opens. Select the types of external devices for which you want to create policies.



5. Select Next and then select Finish.

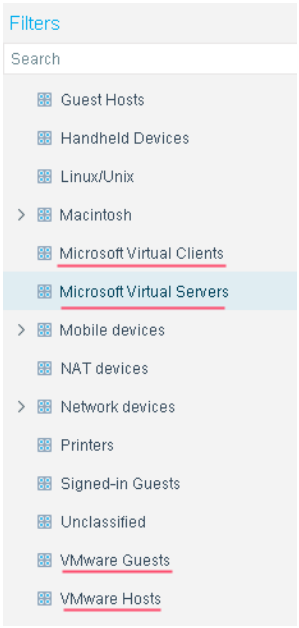
How Discovered Devices Are Handled – Policy Actions

By default, devices that are discovered are added to a sub-group named by device types. This action is enabled by default. Endpoints are removed from groups if eyeSight eyeSight discovers, during policy recheck, that the device function or type has changed. See Update a Policy Recheck for Unmatched and Matched Endpoints in Forescout eyeSight policy main rule advanced options.

Virtual machine classification template

This template creates a policy that detects virtual machines (VMs) in your network.

The policy organizes virtual machines into VMware Guests, VMware Hosts, Microsoft Virtual Clients, Microsoft Virtual Servers and Others groups. These groups are displayed in the Console, Filters pane.



To create a policy:

1. Select Add from the Policy Manager.
2. Open the Classification folder and select Virtual Machine Classification.
3. Select Next and complete the policy creation wizard.

How Forescout eyeSight Detects Virtual Machines – Policy Conditions

VM activity is detected by eyeSight eyeSight in several ways:

- If a VMware guest or host machine is found. VMware guests are detected if the value of device interfaces starts with VMware Accelerated and if the NIC vendor uses VM in their name. VMware host machines are detected if the device interfaces are identified as a VMware Virtual Ethernet adapter for vmnet.
- If a Microsoft virtual client or server is found. Virtual clients are detected if the NIC vendor is Microsoft Corp. Virtual servers are found if the service running is displayed in the list of Microsoft's virtual services.

How Virtual Machines Are Handled – Policy Actions

Detected virtual machines are added to the appropriate Virtual Machine group. This action is enabled by default. Clear the checkbox to disable it.

Passive learning mode template

Passive Learning mode restricts eyeSight eyeSight from probing endpoints in order to learn information about them. Use this mode in environments that may contain sensitive endpoints controlling real-time operational processes where active probing may harm or cause shutdowns in the system. This kind of probing is referred to as active probing.

Note:
If you know which devices on your network may be adversely impacted by active probing, assign these endpoints to the Properties - Passive Learning group to limit eyeSight active inspection of them. eyeSight never contacts endpoints in this group to resolve properties, even for policy evaluation. See Restricting Endpoint Inspection for details.

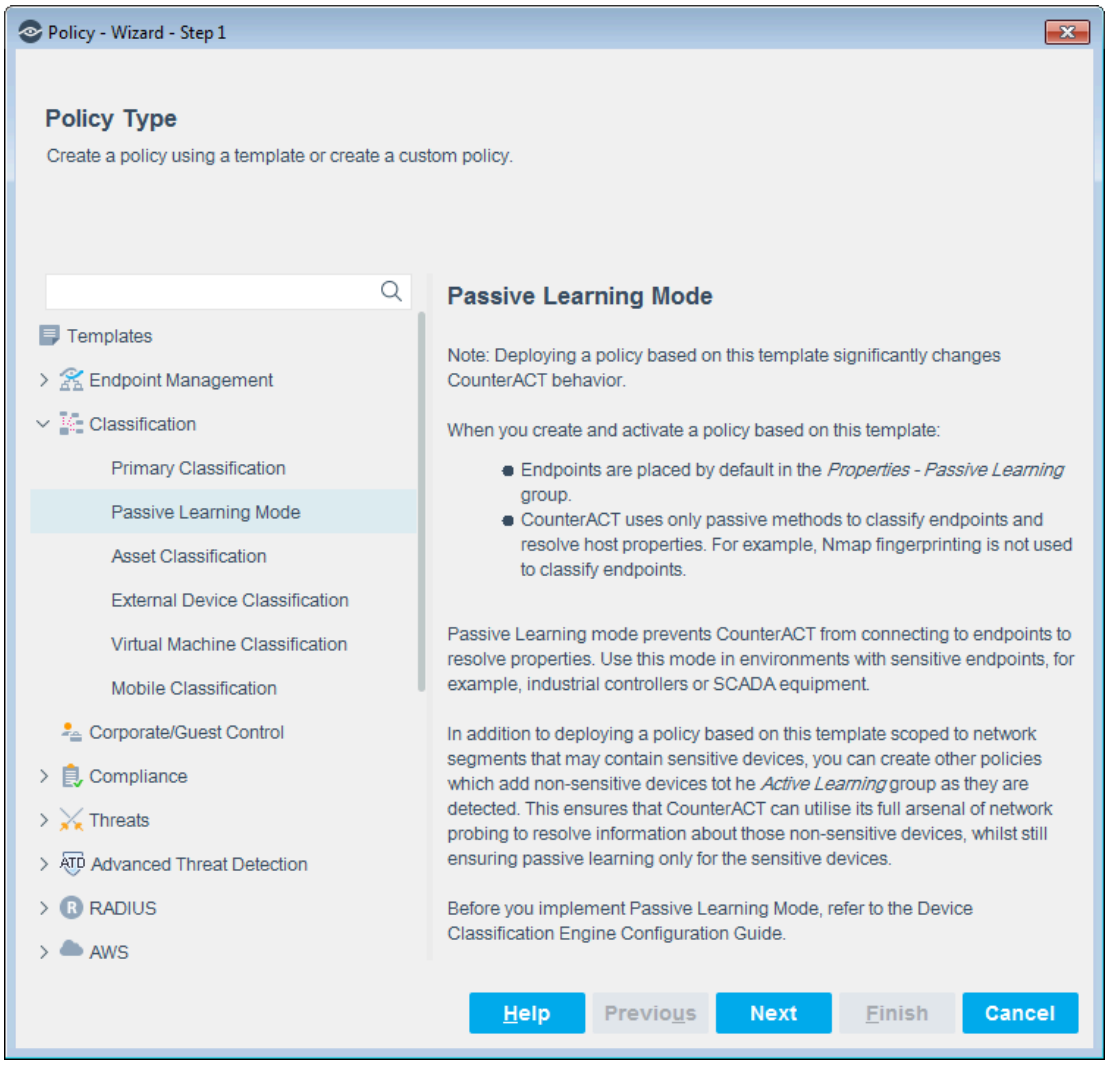
Deploying a policy based on this template significantly changes eyeSight behavior. When you create and activate a policy based on this template:

- Endpoints are placed by default in the Properties - Passive Learning group.
- eyeSight eyeSight uses only passive methods to classify endpoints and resolve host properties. For example, Nmap fingerprinting is not used to classify endpoints.

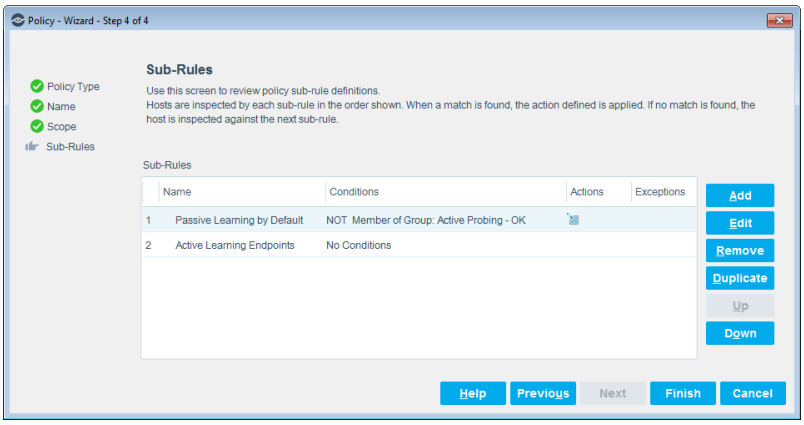
In addition to deploying a policy based on this default template and scoped to network segments that contain sensitive devices, you can create an additional custom policy to add non-sensitive devices to the Active Probing - OK group as they are detected (or add them to the group manually). This lets you focus Passive Learning on sensitive devices only. The Active Probing - OK group is created and added to the list of Groups when you create a new policy using the Passive Learning Mode template.

To create a policy:

1. Select Add from the Policy Manager and expand the Classification folder.
2. Select Passive Learning Mode.
3. Select Next and complete the policy creation wizard.



Passive Learning Sub-Rules



- Rule 1: Passive Learning by Default

This rule ensures that all endpoints that are not specifically added to the Active Probing - OK group by other policies, are added to the Properties - Passive Learning group. The effect of this rule is to

make Passive Learning the default behavior of eyeSight eyeSight.

- Rule 2: Active Probing - OK Endpoints

Endpoints that are added to the Active Probing - OK group by other policies match this sub-rule and are therefore removed from the Properties - Passive Learning group.

Process OS X and Windows endpoints for the NAT / SASE template

Use this template to create a policy for OS X and Windows endpoints, which deletes an on-premises endpoint before admission on connection behind NAT / SASE.

For Endpoint behind NAT / SASE integration recommendations with regards to this template, see Set up Policies in the Endpoint Visibility Behind NAT / SASE How-To Guide.

To create a policy based on the Endpoints Behind NAT/SASE template:

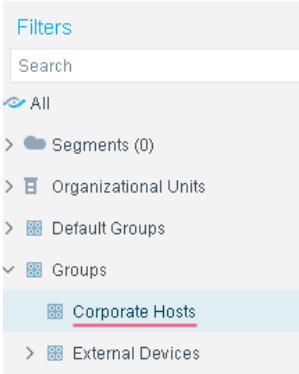
1. Select Add from the Policy Manager.
2. Select Endpoint Behind NAT/SASE Policy Templates > Process OS X and Windows Endpoints for NAT/SASE
3. In the Name pane, edit the name, if required, and add a description.
4. Select Next.
5. In the Scope pane, select All IPs to include all IP addresses in the Internal Network, and then select OK.
6. Select Next.
7. In the Main Rule pane, Conditions area, the SecureConnector NAT/SASE IP host properties and the Delete Host action appear.
    - SecureConnector NAT/SASE IP: Indicates visibility for endpoints that are hidden behind NAT/SASE IP addresses. You do not need to add a specific IP in this property to see all the endpoints behind NAT/SASE. You only need to add a specific IP to filter for a specific location. For example, when the NAT IP is part of the EMEA location Endpoints Behind NAT/SASE vendor IP.
    - Delete Host action: If the user moves from office to remote or vice versa, the template deletes the physical IP so that Forescout can discover the NAT/SASE IP.
8. Select Next, then Finish.

Corporate/Guest control template

Use this template to create a policy that:

- Organizes endpoints into Corporate Hosts, Signed-in Guests and Guest Hosts groups
- Allows users at unauthorized endpoints to register as guests
- Enforces network restrictions on users at unauthorized endpoints

After a policy based on this template is run, endpoints are automatically classified into Corporate Hosts, Signed-in Guests, and Guest Hosts groups. The groups appear in the Filters pane in the Console, under the Groups node.



Deploy the policy created by this template as follows:

1. Use the template to create a policy that classifies your network into Corporate Hosts, Signed-in Guests and Guest Hosts groups, and set up options for handling guests. Options for handling guests are disabled by default. You should set these up when working with the template, but only activate them after completing stages 2 to 4. See Working with Guest Registration Options.
2. Review the groups generated by the policy to verify that they accurately reflect your network. These groups appear in the Filters pane > Groups folder in the Console.
3. Enable the policy actions provided in the template. See Activate Policy Actions. Prerequisites.
    - Consider which endpoints you want to inspect, specifically segments in which guests may connect to the network. The template does not handle endpoints outside of the Internal Network.
    - The Corporate/Guest Control policy does not apply to printers and network devices, which are detected and classified by a Primary Classification policy. Verify that you have run and fine-tuned a Primary Classification policy.
    - Verify that the Primary Classification policy is applied to the network segment or IP address range on which you want to apply the Corporate/Guest Control policy.

    To create a policy:

4. Select Add from the Policy Manager.
5. Select Corporate/Guest Control.
6. Select Next. The Name pane opens.
7. Edit the name if required and add a description. See Policy Naming Tips.
8. Select Next and continue the policy creation wizard.
9. In the Guests pane, configure settings for handling guest endpoints.

Show a Login page link where guests can register for full network access as Signed-in Guests	When this option is enabled, unauthorized users not yet registered as guests must request network access using the Guest Registration form in a web browser. When this option is cleared, guest registration must be initiated by a sponsor in the Guest Management Portal or by a Forescout operator in the Guest Management Pane. See Pre-Registration and Guest Registration Management
Network access	Users are automatically granted network access after they provide

requests are automatically approved	registration information.
Guests must be approved by the sponsor...	When this option is enabled, the registration information submitted by the guest must be approved by designated corporate contacts, called sponsors, before the guest is granted network access. If the guest does not specify sponsors, the registration information is sent to the emails you define for this option. Sponsor emails you specify here must be defined in the Guest Management, Sponsors tab. See Create Sponsors.
Allow guests to skip login and have limited access only	When this option is enabled, guests can opt out of registration.

10. Select Next and complete the policy creation wizard.

Activate Policy Actions

The HTTP Login action launches the Guest Registration form and other web pages or emails used for the guest registration process. By default, this action is disabled. The template is designed this way so that you can run and fine-tune the policy before you activate the corporate login and guest registration process.

In addition, the template provides the Assign to VLAN action and the Virtual Firewall action to restrict access for unauthorized endpoints. These actions are also disabled by default.

After you have tested and approved the behavior of the policy, edit relevant sub-rules to activate these actions.

If you use the Assign to VLAN action to quarantine guest hosts:

- The guest VLAN must be included in the IP address scope of this policy.
- This VLAN must be defined on all switches on which guest hosts can be found.

How endpoints are Detected – Policy Conditions

Note:
By default, only the Add to Group actions are enabled. Run and fine-tune your policy before you activate the corporate login and guest registration processes.

If at least one of the following criteria is met, the endpoint is added to the Corporate Hosts group. Hosts that do not meet any of these criteria are added to the Signed-in Guests group or the Guest Hosts group.

- The Endpoint Recently Authenticated to an Approved Authentication Server

This criterion verifies that the endpoint authenticated with an approved authentication server within the last four weeks.

Review the authentication servers defined in the Console at Options>NAC> Authentication.

Note:
If authentication values change after the policy is defined, authentication credentials in the policy must be updated manually. You can update these credentials via a property List which is automatically generated with the template.

- The Endpoint Is Currently Signed In as a Domain User

This criterion verifies that the endpoint is signed in as a domain user.

Hosts not categorized as Corporate Hosts are evaluated to see if they are Signed-in Guests. A Signed-in Guest is a non-corporate user who received a valid user name and password and logged in using those credentials. This sub-rule evaluates if the endpoint meets one of the following criteria:

- The user is currently signed-in to your network as a Signed-in Guest
- The user successfully logged in as a Signed-in Guest via the HTTP Login action within the last 12 hours
- The user is approved based on their Guest Registration status

Endpoints that do not meet the criteria for Corporate Hosts or Signed-in Guests are classified as Guest Hosts, and users at these endpoints are called guests. These may include, for example, visiting professionals, contractors or university students, or corporate members using personal devices that are not currently known to eyeSight eyeSight.

How Endpoints Are Handled

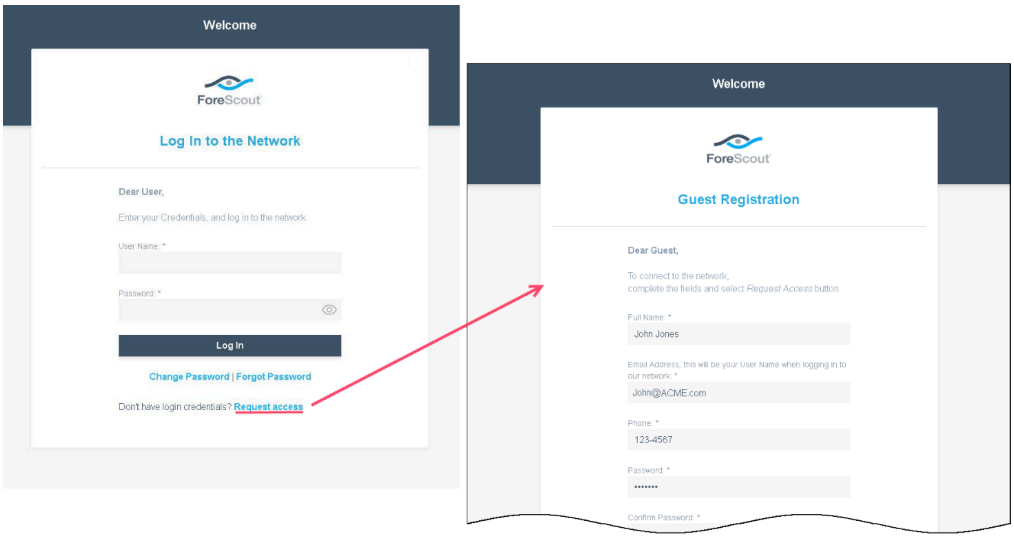
Corporate users and Signed-In guests receive access based on their credentials.

Guest Hosts are directed to the interaction you specify. See Working with Guest Registration Options

Working with guest registration options

When guest registration is enabled, unauthorized users are presented with a Login page where they can choose how to proceed. The page appears when the user attempts to access the corporate network and remains until login succeeds, is skipped or if the endpoint is released via the Console or the Assets Portal.

The Login page prompts users to either sign in using received credentials, or complete a registration form with identity information. This provides you with registration information for each guest, such as contact details and the name of the individual who invited the guest to the network. This guest identity information is stored on a guest server (the Appliance) and can be viewed by a sponsor in the Guest Management Portal or by a Forescout operator in the Guest Management Pane. See Pre-Registration and Guest Registration Management.



The following are examples of ways to handle unauthorized users:

Automatically approve guest registrations

You may want to do this if you anticipate many guests and do not have the resources to accept or reject each one, but do want to keep track of who registered. Select Network access requests are automatically approved in the Guests pane of the Policy Wizard. Guests fill out a registration form with identity information, including an email address. Guests log in using their email address as their user name, together with a password that they defined during registration.

Require email approval by an authorized corporate sponsor

For guests to be approved by authorized individuals, called *sponsors*, in your organization, select Guests must be approved by the sponsor... field and clear the Allow guests to skip login and have limited access only field. In addition to the sponsor named by each guest, you can define additional pre-defined sponsors for guests by typing the email addresses of these sponsors in the field. Email addresses must be comma-separated. There is no limit to the number of sponsors that you can list, and only one must grant approval. After approval, guests are sent a password that is automatically generated. When guests log in to the network, their credentials are checked against the approved credentials. Refer to the Guest Management Portal for Sponsors or information about adding guests. for information about adding guests.

Allow network access to pre-approved guests only

To define pre-approved guests:

- Sponsors can add pre-approved guests in the Guest Management Portal. Login credentials are generated and sent to these guests.
- Operators can define identity information and login credentials for pre-approved guests at the Console. It is the responsibility of your organization to forward the credentials to the guests.

No other guests are authorized to log in to your network. To use this option, clear Show a Login page link where guests can register for full network access as Signed-in Guests, and clear Allow guests to skip login and have limited access only. See Pre-Registration and Guest Registration Management for information about manually adding guests.

Always allow guests limited access only

There are no login requirements for limited access, and all unauthenticated users enter the network with limited access only. Unauthorized guests cannot request full network access. To use this option, clear Show a Login page link where guests can register for full network access as Logged in Guests, and select Allow guests to skip login and have limited access only.

Let users enter the network with limited access or request full access

Allow unauthorized users to either register to receive login credentials, or skip login and enter the network with limited network access. To use this option, select Show a Login page link where guests can register for full network access as Logged in Guests and select Allow guests to skip login and have limited access only.

External disk drive compliance template

This template lets you analyze your network's compliance level for external disk drives connected to Windows endpoints. The policy categorizes endpoints with connected drives into compliant and noncompliant groups that can be viewed in the Home view, Compliance folder.

Compliant external disk drives should be authorized disk drives, i.e., drives that you allow on your network. Disk drives are identified by their ID.

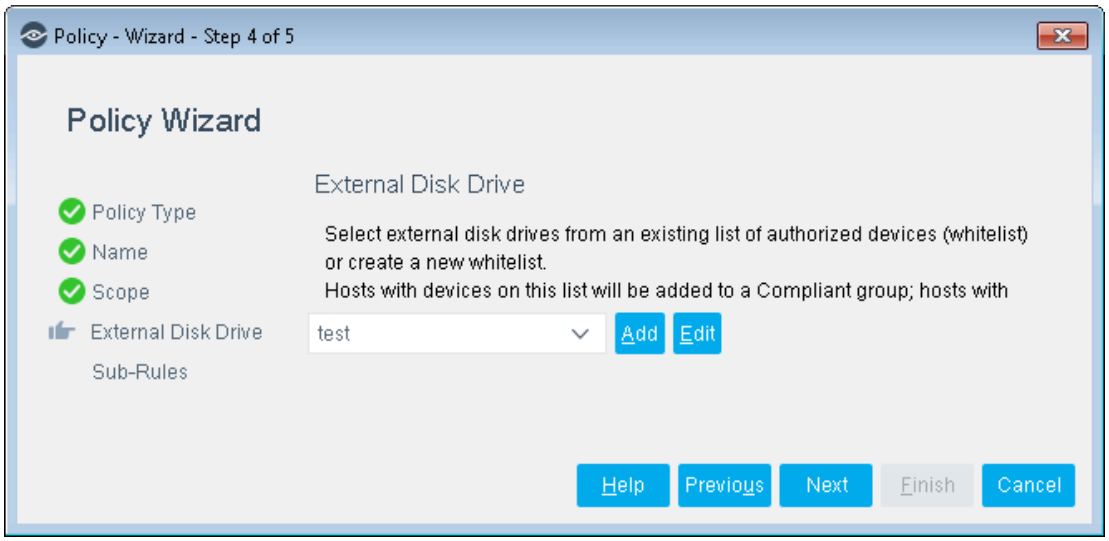
In addition, policy actions can be used to guide endpoint users to compliance, to automatically disable external disk drives that are not compliant, or shut down endpoints with unauthorized disk drives.

Prerequisites

- Consider which endpoints you want to inspect. eyeSight eyeSight does not handle endpoints outside the Internal Network.
- Verify that you have run and fine-tuned policies created from a Primary Classification template and a Corporate/Guest Control template. The External Disk Drive Compliance template applies only to corporate, Windows endpoints. These groups are automatically included in the scope.
- Verify that the HPS Inspection Engine is configured with credentials that allow it to remotely inspect corporate Windows endpoints. This may require using the Windows Group Policy to allow access from all Appliances to port 445/TCP on domain endpoint devices.

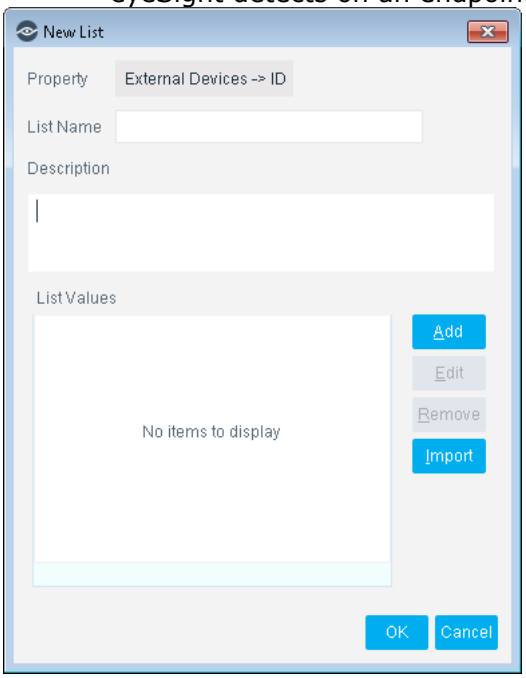
To create a policy:

1. Select the Policy tab. The Policy Manager opens.
2. Select Add.
3. Select the Compliance folder.
4. Select the External Disk Drive Compliance template.
5. Select Next and continue the policy creation wizard.
6. The External Disk Drive pane opens.



Specify a whitelist of authorized external disk drives.

- Select a list you created from the Asset Inventory or by using the List option. The list is based on the External Device Disk IDs group. See Working with Asset Inventory Detections and Defining and Managing Lists for details.
- To create a new List, select Add.
  - The property External Devices > ID indicates that eyeSight eyeSight looks for external disk drives based on their ID number.
  - When you add list values, it is important to type the exact device ID, including spaces. This field is case-sensitive.. This value is what eyeSight detects on an endpoint.



7. Select Next.to complete the policy creation wizard.

Detect External Disk Drives – Policy Sub-Rules

The policy finds endpoints that have external disk drives connected, whether the drives are

authorized or not.

How Endpoints Are Handled – Policy Actions

Policy actions determine how to respond to endpoints that have noncompliant disk drives connected.

- Add to Group: This action is enabled by default.
  - Endpoints using authorized drives are placed in the Hosts with compliant Disk Drives group.
  - Endpoints using unauthorized drives are placed in the Hosts with noncompliant Disk Drives group.
- HTTP Notification: Notify users that a noncompliant disk drive has been detected on their endpoints through their browsers, and to prompt them to disconnect such a drive. This action is disabled by default.
- Set Registry Key on Windows: Set the registry key to disable endpoints with noncompliant disk drives. This is disabled by default.
- Disable External Device: Automatically disable noncompliant disk drives. This is disabled by default.

When an external device is detected by eyeSight eyeSight, it may not automatically appear in your whitelist. If this happens it is recommended to add it to the list. For more information about how to add newly detected external devices to the list, see Defining and Managing Lists and Working with Asset Inventory Detections.

Overall endpoint compliance template

This template lets you analyze the compliance level at your network for commonly used Windows compliance policies, for example, users who have installed peer-to-peer applications or endpoints having out-of-date antivirus applications. The policy categorizes noncompliant endpoints into noncompliant Groups that can be viewed in the Home view > Compliance folder. In addition, policy actions can be used to let you guide endpoint users to compliance without disrupting their productivity.

Note:
Macintosh Update Compliance is not handled by the Overall Endpoint Compliance template since it is not a Windows policy. Use the Macintosh Update Compliance template to create an individual policy.

Prerequisites

- Consider which endpoints you want to inspect. eyeSight eyeSight does not handle endpoints outside the Internal Network.
- Verify that you have run and fine-tuned policies created from a Primary Classification template and a Corporate/Guest Control template. The Overall Endpoint Compliance template applies only to corporate, Windows endpoints. These groups are automatically included in the scope. To view them, run the policy and then use the edit tools to view the policy Main Rule.
- This policy only examines Windows endpoints that are manageable using domain credentials or SecureConnector. Verify that the HPS Inspection Engine is configured with credentials that allow it to remotely inspect corporate Windows endpoints. This may require using Windows Group Policy to allow access from all Appliances to port 445/TCP on domain endpoint devices.

To create a policy:

1. Select Add from the Policy Manager.
2. Select the Compliance folder.
3. Select the Overall Endpoint Compliance template.
4. Select Next and continue the policy creation wizard.
5. The Required Applications pane opens. Specify the applications that must be present on endpoints.

Personal firewall	Check for vendors/products defined in the Personal Firewall property.
Antivirus	Check for vendors/products defined in the Antivirus Installed and the Antivirus Running properties. See Windows security properties Antivirus Running properties.
Updated within the last	This test uses the Antivirus Update Date property. See Windows security properties. When an endpoint has the value Irresolvable for this property, the policy rule evaluates the endpoint as Compliant.
Windows Updates	This test uses the Windows Vulnerabilities property.

6. Select Next. The Restricted Applications pane opens. Specify the applications that must not be present on endpoints.

Instant Messaging	Check for vendors/products defined in the Windows Instant Messaging Installed and the Windows Instant Messaging Running properties.
Peer-to-Peer	Check for vendors/products defined in the Windows P2P Installed and the Windows P2P Running properties.

7. Select Next and complete the policy creation wizard. A separate compliance policy is created for each of the Required or Restricted Applications you selected.

   The Windows Applications Content Module updates the applications detected and reported by these properties. Refer to the *Windows Applications Configuration Guide* for more information.

How Noncompliant Devices Are Handled – Policy Actions

The following actions are provided by the template to handle non-compliant endpoints:

- Add to Group: the action is enabled by default. The following groups are populated:
  - Antivirus Not Installed, Antivirus Not Running or Antivirus Not Updated
  - Personal FW Inactive
  - Windows Not Updated

    - P2P Installed, P2P Running
    - IM Installed, IM Running
- Email notification is sent to the Forescout operator. The generic message can be modified from the template Sub-Rule dialog box. The action is disabled by default.
- Email and web notification is sent to noncompliant users, indicating that their computers are not running a corporate antivirus application. The generic message can be modified from the template Sub-Rule dialog box. The action is disabled by default.

In addition, the following remediation actions are available for some applications:

- Stopped antivirus applications are automatically restarted. The action is disabled by default.
- Microsoft Updates can be remediated using the Start Windows Updates action or the Windows Self Remediation action.

If there is noncompliance at the endpoint, the Forescout icon is displayed in red on the Windows Notification Bar at the bottom of the window. Hold your cursor over the icon to display the endpoint details.

Windows update compliance template

This policy detects hosts that are not updated with the latest Microsoft-published vulnerability patches, and creates a Windows Not Updated group.

In addition, optional remediation actions, disabled by default, can be used to:

- Install SecureConnector to manage Windows machines.
- Allow endpoint users to remediate from the desktop.
- Allow automatic remediation.

Prerequisites

- Verify that you have run and fine-tuned policies created from a Primary Classification template and a Corporate/Guest Control template. Detected endpoints must already be categorized into Windows, Macintosh, and Corporate Hosts groups.
- Endpoints must be manageable using domain credentials or SecureConnector. The template verifies which endpoints are manageable and which are not.

To create a policy:

1. Select Add from the Policy Manager.
2. Select the Compliance folder, and then select Windows Update Compliance.
3. Select Next and complete the policy creation wizard.

How Endpoints are Detected and Handled

The policy template provides four sub-rules.

- Not Manageable: The Start SecureConnector action installs SecureConnector to make

endpoints manageable by eyeSightt eyeSight. This action is disabled by default.
- Waiting for Reboot: Windows updates were successfully downloaded and installed. The endpoint must reboot to complete the update process. The template provides no remediation actions.
- Windows Updates Required: Windows endpoints have not been updated with the most current Windows updates. This sub-rule provides three actions.
    - The endpoint is added to the Windows Not Updated group for processing. This action is enabled by default.
    - The Start Windows Updates action can update the endpoints and inform the end user. This action is disabled by default.
    - The Windows Self Remediation sends the user links to the updates and patches that must be installed to resolve discovered vulnerabilities. This action is disabled by default.
- Compliant: The endpoint does not require any security or vulnerability update. It is not added to any additional group and no actions are performed.

Macintosh update compliance template

This template lets you verify that endpoints have installed the most current Macintosh software updates.

Prerequisites

- Verify that you have run and fine-tuned policies created from a Primary Classification template and a Corporate/Guest Control template. Detected endpoints must be categorized into Windows, Macintosh, and Corporate Hosts groups.
- Endpoints must be manageable. The template verifies which endpoints are manageable and which are not. See Start SecureConnector / Stop SecureConnector for details.

To create a policy:

1. Select Add from the Policy Manager.
2. Select the Compliance folder, and then select Macintosh Update Compliance.
3. Select Next and complete the policy creation wizard.

How Endpoints are Detected and Handled

The policy finds endpoints that have not been updated with the most current Macintosh updates. The template provides the following actions.

- Send Email: You can deliver email notification to network users indicating that specific security and other updates are missing on their machines. This action is disabled by default.
- Start Macintosh Update: You can automatically send an update link to the endpoint. This action is disabled by default.

Threats templates

Threats templates let you detect an extensive range of malicious threats that can compromise the security of your network. You can decide which endpoints to inspect, and apply policy conditions and actions through the templates to neutralize malicious threats.

There are no prerequisites for any of the Threats templates.

Malicious hosts template

Use this template to create a policy that tracks malicious network activity, for example, worm infections or malware propagation attempts. It can be used to enhance automatic Threat Protection Policy actions, which are limited to blocking traffic.

How Endpoints are Detected and Handled

Malicious endpoint activity is detected using Active Response technology, an innovative, patented technology created by Forescout Technologies that effectively mitigates human attackers, worms and other self-propagating malware. Active Response technology accurately pinpoints and halts threats at the earliest stages of the infection process. See Threat Protection for details.

The policy conditions instruct eyeSight eyeSight to detect a wide range of scan, bite and email anomaly events. If an endpoint has triggered one of these events, eyeSight evaluates it as malicious.

Template actions determine how to respond to endpoints that are malicious.

- Send Email: A predefined action lets you send email to the Forescout Administrator indicating that a malicious event was detected at an endpoint. The email provides information about the endpoint, for example, the IP address, the logged in user, and User Directory information. You must provide an email address recipient. This action is disabled by default.
- HTTP Notification: A predefined action lets you deliver browser notification to the end user, indicating that malicious activity has been detected. This action is disabled by default.

ARP spoofing template

Use this template to create a policy to track and remediate attempts to maliciously direct network traffic.

ARP spoofing is a technique used to attack an Ethernet network that may allow an attacker to sniff data frames on a Local Area Network (LAN), modify the traffic, or completely stop it. The aim is to associate the attacker’s MAC address with the IP address of another node so that any traffic meant for that IP address is mistakenly sent to the attacker instead. The attacker could then choose to forward the traffic to the actual default gateway (passive sniffing) or modify the data before forwarding it.

Refer to the *Port Mirroring Technical Note* for more information about configuring your environment to detect ARP spoofing.

How Endpoints are Detected and Handled

ARP spoofing activity is detected by tracking whether the number of different MAC addresses for a specific IP address exceeds the number specified in the criterion. Generally, this number is one. The template conditions instruct eyeSight eyeSight to indicate if the number of MAC addresses reported for an IP address over a specific time period exceeds a certain limit. You can define the number of MAC addresses and the time period.

Enable actions provided by the template to resolve endpoints on which ARP Spoofing activities have been detected.

- Send Email : A predefined action lets you send email to the Forescout administrator

indicating that an ARP Spoofing activity was detected at an endpoint. The email provides information about the endpoint, for example, the IP address, the logged in user, and User Directory information. You must provide an email address recipient. This action is disabled by default.

Impersonation template

This template lets you track impersonation activity on your network. Impersonation is a technique used by an unauthorized individual masquerading as someone who is authorized, for the purpose of gaining access to data on your network.

How Endpoints are Detected and Handled

Impersonation activity is detected by tracking a change in the Nmap-Network Function of the endpoint.

Enable actions provided by the template to resolve endpoints on which impersonation activities have been detected.

- Send Email: A predefined action lets you send an email to the Forescout Administrator indicating that an impersonation activity was detected at an endpoint. The email provides information about the endpoint, for example, the IP address, the logged in user, and User Directory information. You must provide an email address recipient. This action is disabled by default.

Dual homed template

Use this template to create a policy that tracks threats from dual-homed Windows endpoints – endpoints that are assigned more than one IP address or use network adapters that act as a bridge between trusted and untrusted networks on endpoints.

In such cases, a separate address can be used to connect to different networks. This information may be important because endpoints connected to more than one network can be used as routers to transmit malicious traffic. Endpoints connected to both wireless and land networks can also create back doors for hackers and worms.

The policy template actions let you notify security teams when dual-homed endpoints are detected.

If endpoints are managed by SecureConnector, you can disable network adapters that act as a bridge between trusted and untrusted networks. All connections are disabled, except for the connection used by SecureConnector. Disabled adapters are re-enabled when SecureConnector disconnects from the trusted network. The actions are disabled by default.

How dual-homed threats are detected

Threats from dual-homed endpoints are detected in the following ways:

- SecureConnector Manageable Sub-Rule
- Detect Windows endpoints managed by SecureConnector. These endpoints have at least one network adapter connected to the host, used for the SecureConnector connection to the Appliance.
- Detect one or more additional enabled network adapters.

- Verify that the additional adapter is not already disabled by SecureConnector or used by SecureConnector to connect to the Appliance.

Hosts that meet these criteria are considered dual-homed. You can manage these endpoints by notifying your IT or Security team or disabling the network adapter not used by SecureConnector. Hosts that meet these criteria are considered dual-homed. You .an manage these endpoints by notifying your IT or Security team or disabling the network adapter not used by SecureConnector..

- Domain Manageable Sub-Rule
- Detect Windows endpoints managed remotely, i.e., if eyeSight eyeSight has access to the endpoint remote registry and file system, and is not managed by SecureConnector as well.
- Detect endpoints with more than one IP address. Endpoints associated with more than one IP address are considered dual-homed.

Note:
You can fine-tune the template policy by defining the IP addresses that are to be ignored when calculating using the Number of IP Addresses property. For details refer to the *HPS Inspection Engine Configuration Guide* .

If endpoints meet these criteria they are considered dual-homed.

How threats to dual-homed hosts are handled

Template actions determine how to respond to endpoints on which threats to a dual-homed network have been detected. Dual-homed endpoints can be handled in two ways; depending on how the dual-homed endpoint is managed.

- Send Email: A predefined action lets you send an email to the Forescout Administrator indicating that a threat to a dual-homed network was detected at an endpoint. The email provides information about the endpoint, for example, the IP address, the logged in user, and User Directory information. You must provide an email address recipient. This action is disabled by default.
- Disable Dual Homed: A predefined action lets you disable network adapters that act as a bridge between trusted and untrusted networks on endpoints managed by SecureConnector. All connections are disabled, except for the connection used by SecureConnector. Disabled adapters are re-enabled when SecureConnector disconnects from the trusted network. This action is disabled by default.

To further control these endpoints, you can disable the network adapter and use the Start SecureConnector action to manage the endpoints with SecureConnector. When this happens, the endpoints are automatically detected by the SecureConnector Manageable Sub-Rule.

Track changes templates

These templates are based on Track Changes host properties, which report a change in the value of a reference property.

For example:

- Application Change
- Hostname Change
- Operating System Change
- Shared Folder Change

- Switch Change
- User Change
- Windows Service Change

Note:
For details about using the New TCP/IP Port template, see New TCP/IP Port Template .

Under certain circumstances, such changes may be indicative of malicious activity or security breaches. These policies can be used, for example, to alert you if an application version has been altered or a new application has been introduced into your network.

There are no prerequisites for any of the Track Changes templates.

New TCP/IP port template

The New TCP/IP Port template lets you track the addition of new TCP/IP ports to your network. The Transmission Control Protocol (TCP) is one of the core protocols of the Internet Protocol suite, and is often referred to as TCP/IP. A new TCP/IP port can be particularly threatening to the security of your network because TCP provides a communication service between an application program and the Internet Protocol (IP) when an application sends a large chunk of data across the Internet using IP.

Note:
There are no prerequisites for using this template.

To create a policy:

1. Select Add from the Policy Manager.
2. Select the Track Changes folder, and then select New TCP/IP Port.
3. Select Next and complete the policy creation wizard.
4. Review the policy conditions and actions, and select Finish.

How Endpoints are Detected and Handled

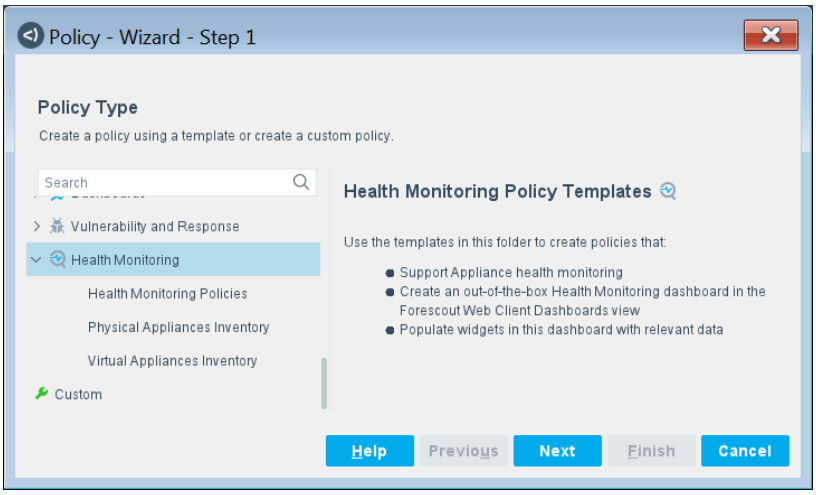
Forescout eyeSight detects endpoints with new TCP/IP ports when port status changes between opened and closed.

There are no default actions for the New TCP/IP Port template

Health monitoring templates

Use the Health Monitoring Policies Template and Appliance Inventory Templates to create health monitoring policies, enable the Health Monitoring Dashboard and populate specific widgets in the dashboard.

After you run the Health Monitoring Policies Template, the Health Monitoring Dashboard will be available to add to your Dashboards view. See Add a Dashboard to Your View for details.



Health monitoring policies template

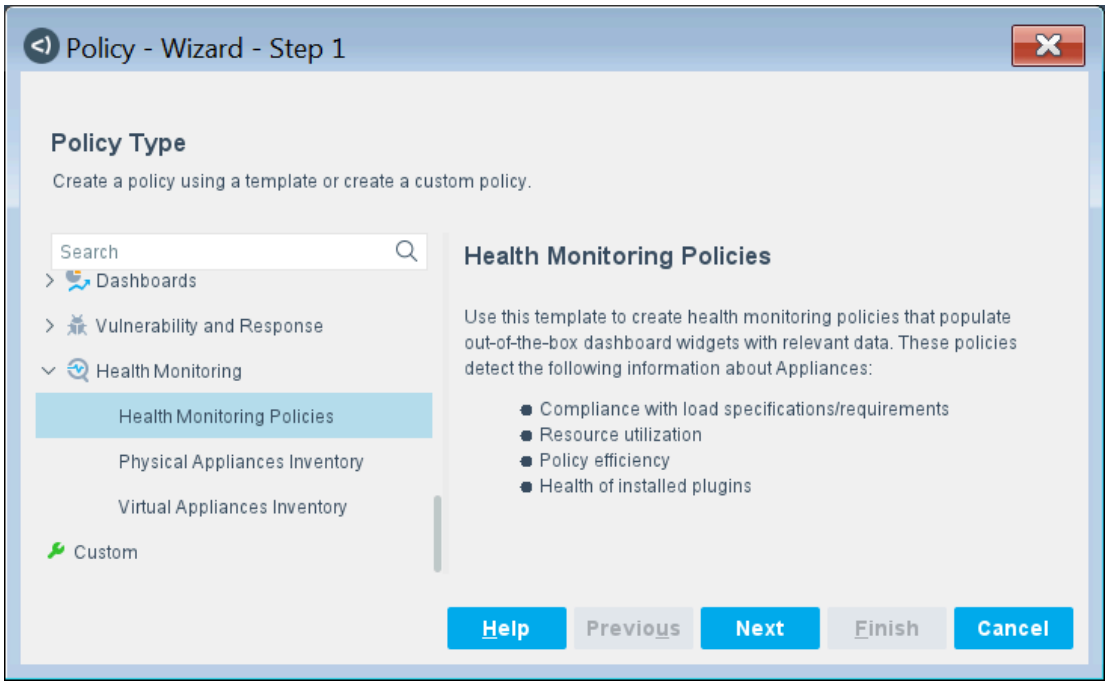
Use the templates in this folder to create policies that:support Appliance health monitoring, to create an out-of-the-box Health Monitoring dashboard in the eyeSight Web Client Dashboards view, and to populate widgets in this dashboard with relevant data.

Run this template to create the following policies:

- Appliances Policy
- Appliance Load Compliance Policies
- Appliance Resource Utilization Policies
- Appliance Policy Efficiency Policies
- Plugin Health Policies

To run the template:

1. Log in to the Console and select the Policy tab.
2. (Recommended) Create a new folder to hold the default Health Monitoring policies.
3. Select the folder and select Add from the Policy Manager. The Policy Wizard opens.
4. Expand the Health Monitoring folder and select Health Monitoring Policies.



5. Select Next. The Health Monitoring Policies pane opens, displaying a summary of the policies that have been activated.

6. Select Finish.

7. Select Apply to save the policy settings.

Appliances policy

This policy detects Forescout devices that are functioning as Appliances and adds them to the Appliances group. This group is then used in the main rule of the other policies created by the Health Monitoring Policies template to filter for Appliances only.

Appliance load compliance policies

This pair of Health Monitoring policies analyzes and identifies Appliances as compliant or noncompliant with Forescout load specification guidelines.

The Forescout Licensing and Sizing Guide specifies the Forescout load specification guidelines.

These policies identify whether Appliance specifications are more or less than the amounts recommended by Forescout.

- Appliance Load Compliance Analysis Policy: Analyzes Appliance performance and compares it with Forescout specifications. Each specification is a separate sub-rule in the policy.

  Appliances that do not meet any one of the minimum specifications are added to the Appliances - Overloaded group, which is used by the Appliance Load Compliance policy to identify Appliances as either compliant or not compliant with load specifications.

  This policy's sub-rules use Health Monitoring – Load Specification Compliance properties .

- Appliance Load Compliance Policy: Identifies Appliances as either compliant or noncompliant with Forescout load specifications, based on the detailed analysis performed by the Appliance Load Compliance Analysis policy.

  This policy populates the Appliance Load Compliance Widget in the Health Monitoring dashboard.

Appliance resource utilization policies

This pair of policies analyzes and identifies Appliances as having either normal or high resource utilization.

These policies identify how effectively Appliances actually utilize their resources, irrespective of whether Appliance specifications are found compliant by Appliance Load Compliance Policies.

- Appliance Resource Utilization Analysis Policy. This policy analyzes various factors related to Appliance resource utilization and determines whether they are within an acceptable range, based on testing performed by Forescout. For example, factors like CPU usage, disk latency, packet loss, and others. Each factor is a separate sub-rule in the policy.

  Appliances that do not fall into the acceptable range for any one of the factors are added to the Appliances - High Resource Utilization group, which is used by the Appliance Resource Utilization policy to identify Appliances as having either or normal resource consumption.

  This policy's sub-rules use Health Monitoring – Resource Utilization properties.

- Appliance Resource Utilization Policy. This policy identifies Appliances as having either normal or high resource utilization, based on the detailed analysis performed by the Appliance Resource Utilization Analysis policy.

  This policy populates the Appliance Resource Utilization widget in the Health Monitoring dashboard.

Appliance policy efficiency policies

This pair of policies analyzes and identifies Appliances as having either optimal or sub-optimal policy efficiency.

- Appliance Policy Efficiency Analysis Policy. This policy analyzes various factors related to how effective policies are performing in your deployment. For example, the average rate that requests to resolve endpoint properties are made per minute. Each factor is a separate sub-rule in the policy.

  Appliances that do not fall into the acceptable range (based on testing performed by Forescout) for any one of the factors are added to the Appliances – Sub-Optimal Policy Efficiency group, which is used by the Appliance Policy Efficiency policy to identify Appliances as having either optimal or sub-optimal policy efficiency.

  This policy populates the Appliance Policy Efficiency Analysis Widget in the Health Monitoring dashboard.

  This policy's sub-rules uses Health Monitoring – Policy Efficiency properties.

- Appliance Policy Efficiency Policyp

Plugin health policies

This pair of policies analyzes and identifies Appliances as having either degraded or optimal plugin health.

- Plugin Health Analysis Policy. This policy analyzes various negative factors related to the overall health of plugins installed in the Forescout deployment. For example, whether a plugin crashed or stalled sometime in the last 30 minutes. Each factor is a separate sub-rule in the policy.

  If an event occurs indicating poor plugin health, the Appliance is added to the Degraded Plugin Health group, which is used by the Plugin Health policy to identify Appliances as having either degraded or optimal plugin health.

  This policy populates the Plugin Health Analysis Widget in the Health Monitoring dashboard.

  This policy's sub-rules uses Health Monitoring Plugin Health properties.

- Plugin Health Policyh. This policy identifies Appliances as having either degraded or optimal plugin health, based on the detailed analysis performed by the Plugin Health Analysis policy.

Appliance inventory templates

Run the following Appliance Inventory policy templates to create physical and virtual Appliance inventory policies and populate specific widgets in the dashboard.

- Physical Appliances Inventory Template. Populates the Physical Appliance Inventory Widget in the Health Monitoring Dashboard.
- Virtual Appliances Inventory Template. Populates the Virtual Appliance Inventory Widget in the Health Monitoring Dashboard.

To run an Appliance inventory template:

1. Log in to the Console, and select the Policy tab.
2. (Recommended) Create a new folder to hold the default Health Monitoring policies.
3. Select the folder, and then select Add from the Policy Manager. The Policy Wizard opens.
4. Expand the Health Monitoring folder, and select either:
    - Physical Appliances Inventory
    - Virtual Appliances Inventory
5. Select Next, and complete the policy creation wizard.

Working with policy conditions

A policy condition is a set of endpoint property criteria combined with Boolean logic operators.

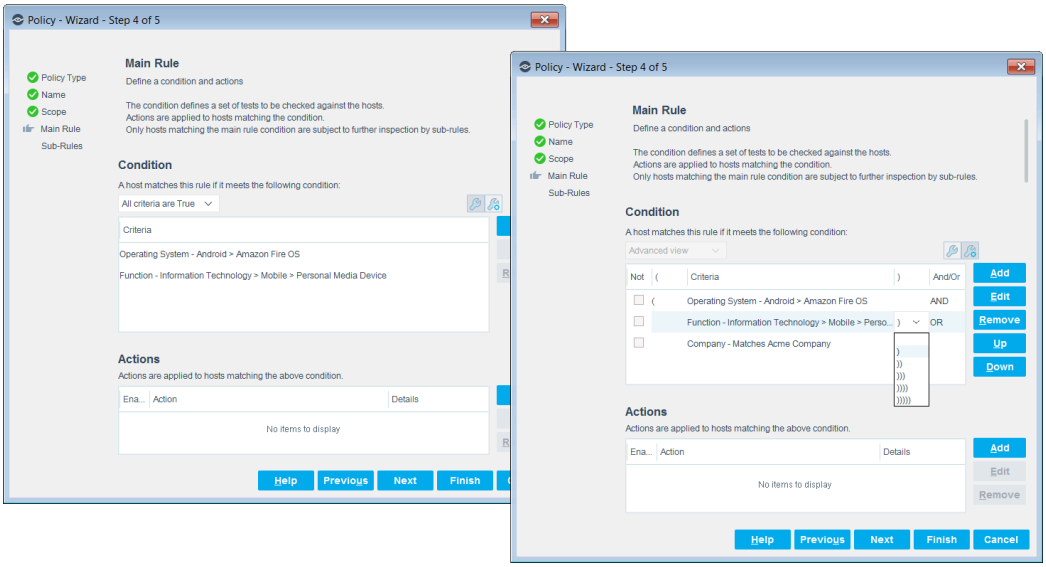
For example:

- Match certain values of the Windows Version property to detect endpoints running Windows XP

  AND

- Match values of the AntiVirus Running property that indicate Symantec AntiVirus is present on the endpoint.

Typically actions that are applied to endpoints match a condition. Each condition-action pair defines a rule or sub-rule of the policy.



Properties

Each criterion of a policy condition examines the value of a property to detect endpoints.

A property is an attribute detected on the endpoint and reported to Forescout. Forescout eyeSight supports an extensive range of endpoint and network device properties.

Most properties report information learned by traffic monitoring or fingerprinting and inspection of endpoints.

Some properties return endpoint or network device information from other platforms in your network.

Some properties run scripts. The result of the script is the property value.

Content Modules and eyeExtend modules, provide additional properties. For example, if you install the Forescout eyeExtend for McAfee ePolicy Orchestrator, properties specific to that McAfee product

are available.

Conditions and Criteria

To control the condition statement logic, select (Advanced) in the policy rule Condition area. You can click the column immediately before or after a criterion to add parentheses, and you can select the And/Or column to change the default Boolean logic.

Conditions may include several criteria, i.e., several sets of Boolean endpoint properties. Each condition provides an option to specify which criteria must be met in order for the endpoint to match the policy.

Condition Shortcuts

- Create and reuse *Custom conditions* in any of your policies. Using Custom conditions saves you time when you create policies and prevents you from making mistakes when defining the condition. See Authentication Properties for details.
- Create and use *Lists* of property values in any of your policies. These are user-defined lists of property values, for example, a list of user names or a list of domain names. Using Lists saves you time when you create policies and prevents you from making mistakes when entering values. For example, a list of switch IP addresses that you may need to use repeatedly when defining different policies. See Defining and Managing Lists for details.

Irresolvable Criteria

In some situations, Forescout eyeSight cannot properly resolve endpoint property criteria. Many properties provide an option for handling such irresolvable criteria. If Forescout eyeSight cannot verify a property, you can choose how to treat that endpoint. See Handling Irresolvable Criteria for details.

Working with properties

Forescout Appliances must regularly query endpoints to keep property values up to date. This can generate significant network traffic. Forescout provides several methods for minimizing traffic:

- In general, endpoints are polled for property values only when a policy that includes the property is evaluated. Defining the time interval at which policies are evaluated and rechecked influences the frequency at which endpoints are queried.
- When SecureConnector is used on endpoints, event driven monitoring can be enabled. SecureConnector proactively sends updates to the HPS Inspection Engine only when it detects a change in an endpoint property. This eliminates blind polling by Forescout Appliances, and significantly reduces redundant network traffic.

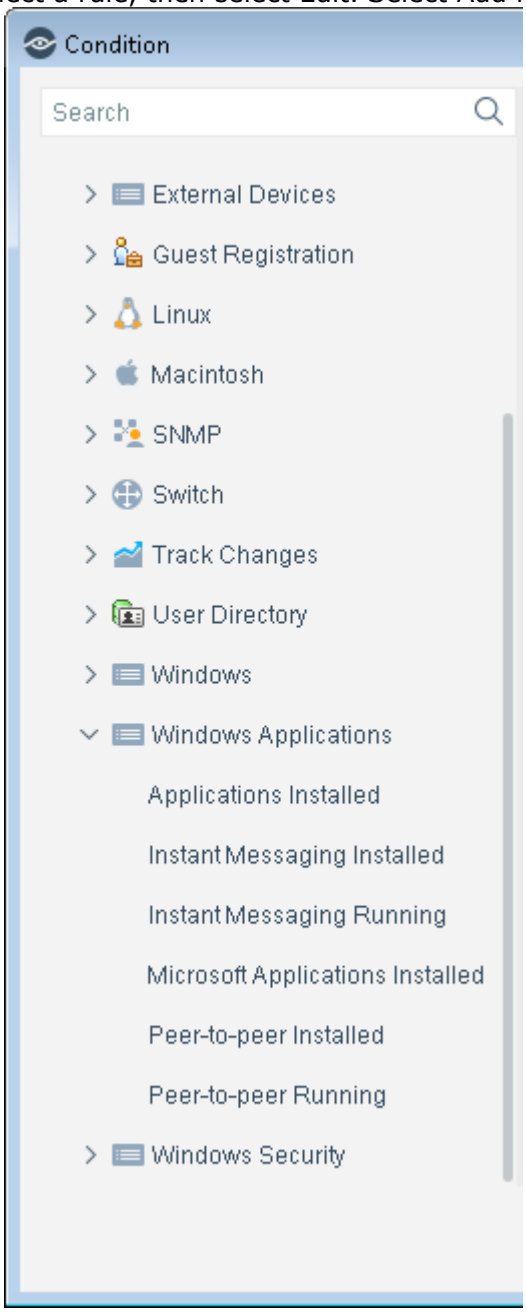
Define a policy condition

You can define the properties to be detected on an endpoint as part of a condition definition. To use a comparison condition when you Add/Edit a policy, select a rule and edit its condition. Select the Comparison folder in the Properties tree as you would to define a new condition.

List of Properties by Category for a list of available properties.

To define properties:

1. In Policy view:
    - Add a policy and navigate to the pages of the wizard that show Main and sub-rule definitions.
    - Edit a policy.
2. Select a rule, then select Edit. Select Add from the Condition area of the dialog box.



3. Select a property type in the Select Property section and define the a matching criteria for this property's value. Use matching expression options to define matching criteria for a property's value. Common matching expressions include:
    - Contains
    - Starts or Ends with
    - Greater than
    - Matches
    - Matches expression

- In List (See Defining and Managing Lists)
- Any Value

4. Select OK. The Conditions dialog box reopens.
5. Repeat this procedure to define several criteria in the rule condition. You may decide that a match is acceptable:
   - If all criteria are true.
   - If one criterion is true.
   - If all criteria are false.
   - If one criterion is false.

Detect new vulnerabilities and newly supported vendor applications

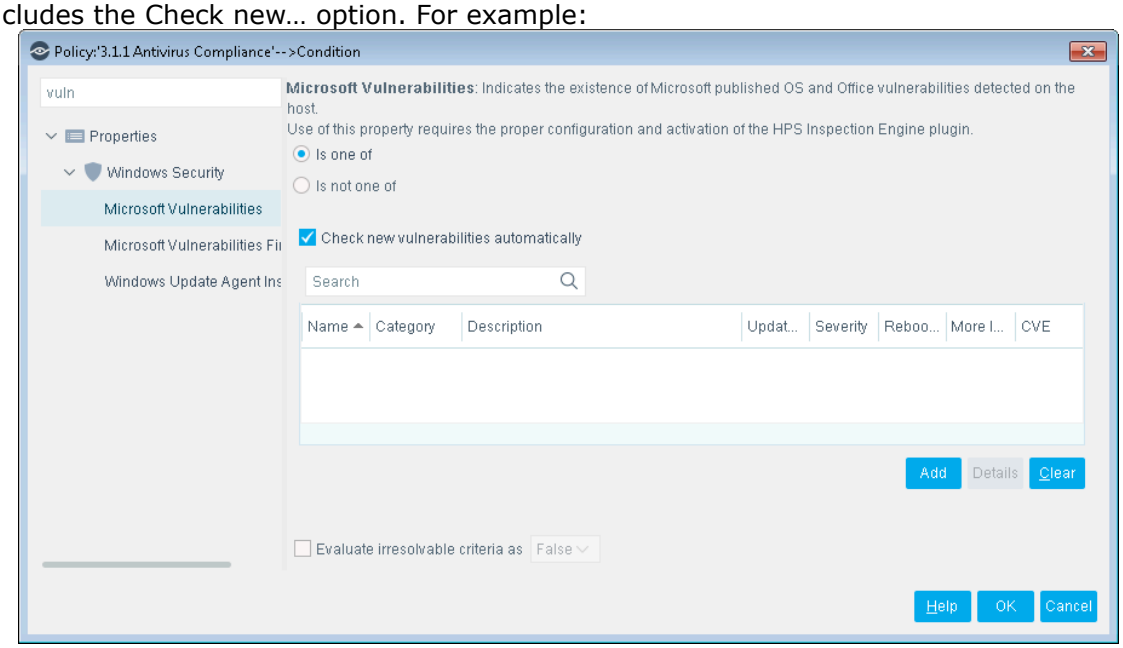
You can choose to automatically detect new Microsoft vulnerabilities and newly supported vendor applications on your network endpoints.

For example:

- When working with the Windows Applications > Cloud Storage Installed property in your policies, automatically detect any Cloud storage applications of newly supported vendors.
- When working with the Windows Security > Microsoft Vulnerabilities property in your policies, automatically detect new Microsoft published OS and Office vulnerabilities.

To detect new vulnerabilities and supported application vendors:

1. Verify that you have installed the most current Windows Applications Plugin and the Windows Vulnerability DB. Refer to the relevant Forescout portal for information about new application and vulnerability detection support.
2. Select the Microsoft Vulnerabilities property or a Windows application property that includes the Check new… option. For example:



3. Select Check new vulnerabilities automatically.
4. Select OK. Refer to the *Windows Applications Configuration Guide* for a complete list of supported vendors. Select Tools > Options > Modules, select Windows Applications, and then select Help.

Define custom conditions

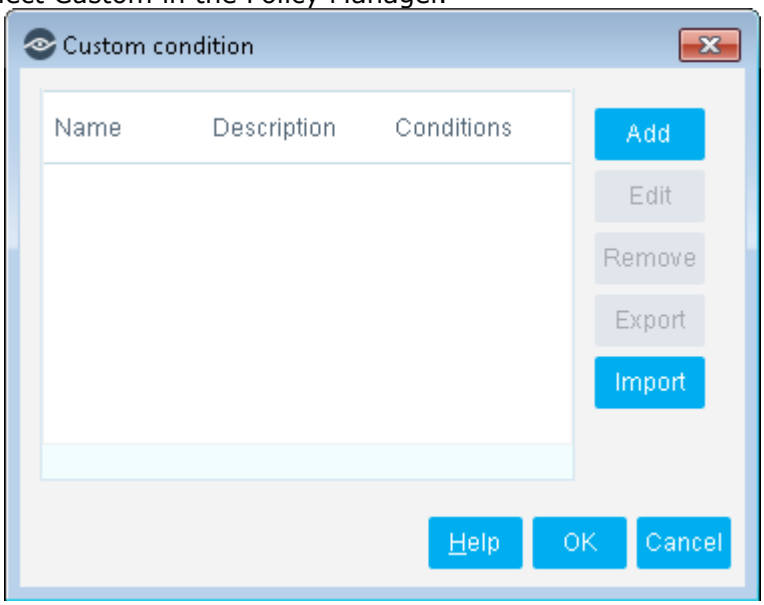
You can create custom conditions independent of a policy, and reuse them in several policies. This saves you the trouble of redefining complex conditions.

Conditions can be imported and exported as XML files.

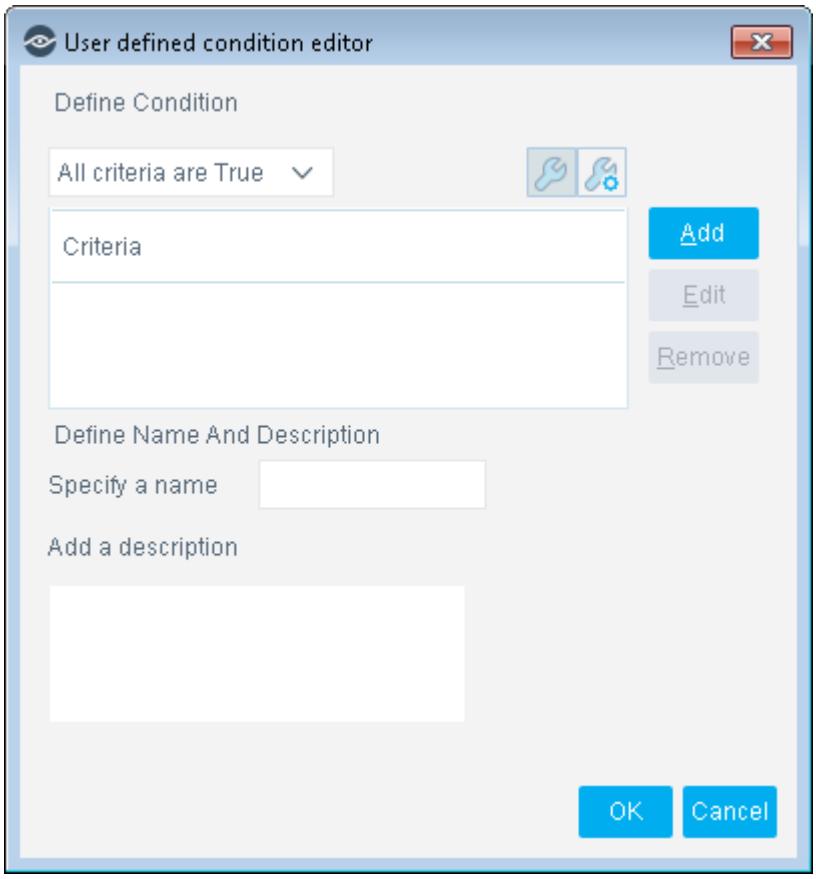
Note:
You cannot define a custom condition when you use the policy creation wizard to Add/Edit a policy.

To create custom conditions:

1. Select Custom in the Policy Manager.



2. Select Add. The User defined condition editor opens.



3. Select Add.
4. Define properties as required and select OK.
5. Define a name and description for the condition and select OK. The Condition is displayed in the Custom Condition dialog box. Use this dialog box to manage your created conditions.

   To use custom conditions when you Add/Edit a policy, select a rule and edit its condition. Select the Custom folder in the Properties tree as you would to define a new condition.

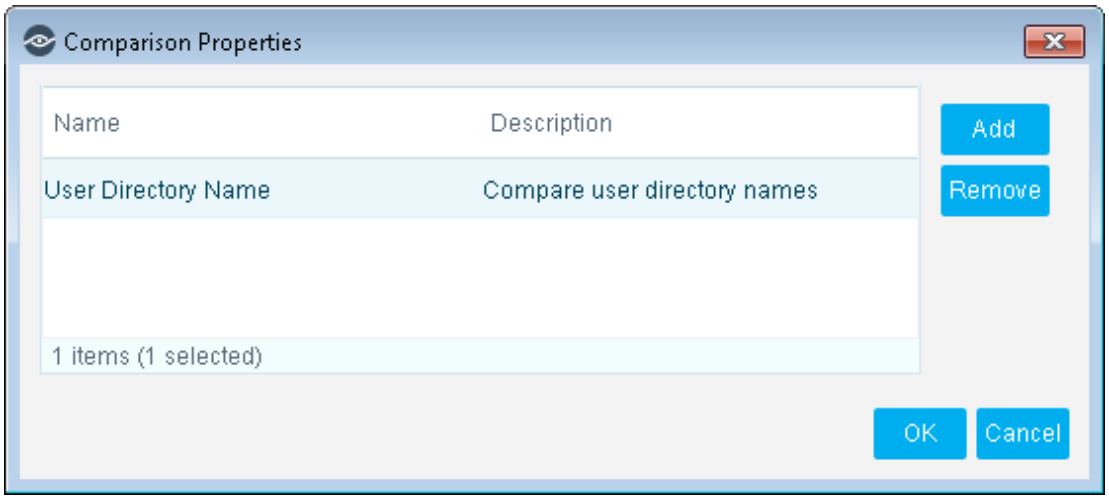
Define a comparison condition

You can create a property that indicates differences between two property values.

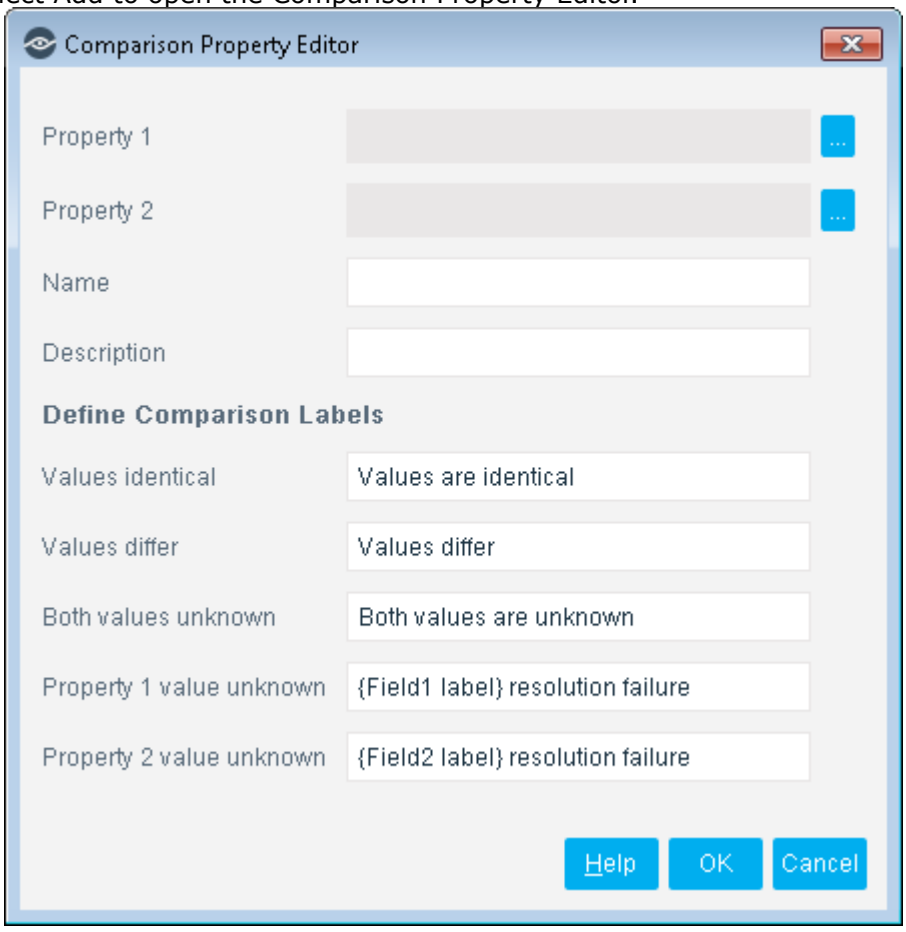
For example, create a new property called Compare User Directory Names, and compare User Directory > LDAP User Name with User Directory > Display Name. The comparison results will indicate whether the values are identical, differ or if either of the values is unknown. Results appear in the Profiles tab for the policy where the property was used.

To create a comparison condition:

1. Select Comparison in the Policy Manager.



2. Select Add to open the Comparison Property Editor.



3. Define the Property:
    a. In the Property 1 field, select the first property for comparison.
    b. In the Property 2 field, select the second property for comparison.
    c. In the Name field, enter the name of the new property.
    d. In the Description field, enter a description of the property.
4. Customize the names of the property comparison results. For example, change the Values Identical result label to User Directory Names Identical.
5. Select OK. The new property appears in the Comparison Properties dialog box.
6. Select OK. To use a comparison condition when you Add/Edit a policy, select a rule and

edit its condition. Select the Comparison folder in the Properties tree as you would to define a new condition.

List of properties by category

This topic describes properties that are available by default in a typical eyeSight deployment. Some properties may not be available depending on the details of your Forescout configuration. Some properties may not be available, or remain unpopulated with data if certain device types are not present in your network.

Authentication properties

Authenticated by Certificate	Indicates whether a certificate-based authentication process for the endpoint was successful. If a certificate for this feature is not found on the endpoint, this property returns the value No.
Authentication Certificate Expiration	Indicates the value of the Valid To field of the certificate installed on the endpoint for certificate-based authentication.
Authentication Certificate Issuer	Indicates the value of the Issuer field of the certificate installed on the endpoint for certificate-based authentication.
Authentication Certificate Root CA Subject	Indicates the value of the Subject field of the certificate installed on the endpoint for certificate-based authentication.
Authentication Certificate Serial Number	Indicates the value of the Serial Number field of the certificate installed on the endpoint for certificate-based authentication.
Authentication Certificate Status	Indicates the state of the certificate installed on the endpoint for certificate-based authentication, and any verification errors for the certificate. For example, you can use this property to identify endpoints with revoked certificates. If a certificate for this feature is not found on the endpoint, this property returns the value No certificate.
Authentication Certificate Subject	Indicates the value of the Subject field of the certificate installed on the endpoint for certificate-based authentication.
Authentication Certificate Subject Alternate Name	Indicates the value of the Subject Alternate Name field of the certificate installed on the endpoint for certificate-based authentication.

Authentication Login	Indicates whether the endpoint performed any of the following: A successful login to an authentication server. To use this feature you must configure your authentication servers. The following authentication services are supported: HTTP (80/TCP) Telnet (23/TCP) NetBIOS-SSN (139/TCP) Microsoft-DS (445/TCP) Microsoft-MAPI (135/TCP) FTP (21/TCP) IMAP(143/TCP) POP3(110/TCP) rlogin (513/TCP) The user authenticated via the User Directory server as a result of a HTTP Login action. The user authenticated as a guest as a result of a HTTP Login action. See Defining Authentication Servers for details.
Authentication Login (Advanced)	Indicates endpoints that logged in to the network using a specific protocol or against a specific server. Enter the protocol name or the server IP address. Servers referenced here must be defined in the Authentication pane. See

	Defining Authentication Servers for details.
HTTP Confirmation Events	Indicates whether the end user confirmed an HTTP notification message generated by Forescout eyeControl. Confirmation is discovered via the Confirmation Identifier name, defined in the HTTP Notification action. Enter the name of the identifier. If discovered, the user confirmed the message.
HTTP Login Failure	Indicates whether the endpoint exceeded the HTTP login failure threshold defined in Options > NAC > HTTP Login Attempts. The User Directory Plugin must be installed to work with this property.
HTTP Login User	Indicates the name of the last user that performed successful HTTP Login authentication.
Signed In Status	Indicates endpoints that are: Signed-in to the network using a valid domain name. See HTTP Login action for details. Signed-in as guests. Signed-out or never signed in.

Classification properties

Function	Indicates the most specific function in the Device Profile Library that matches the endpoint. For example, Information Technology > Accessory > VoIP > IP Phone. If multiple functions match the endpoint, the property is resolved as the most specific value in the Device Profile Library that is common to all the matching functions. For example, if Gaming Console and SmartTV profiles both match the endpoint, the property is resolved as Multimedia & Entertainment. If there is no common value among all the matching functions, the property is resolved as Multiple Suggestions.

	If no function profiles in the Device Profile Library match the endpoint, the property is resolved as Unknown. Select one or more endpoint functions. To detect all sub-classifications of the selected functions, select the Include sub-classifications checkbox.
Network Function	Indicates the type and function of an endpoint, as determined by various passive and active means, including Nmap. Due to the activation of Nmap, this information may take longer to resolve. Use of this property requires that you configure the HPS Inspection Engine. Refer to the *Network Function Property Algorithm Technical Note*.for details for details.
Operating System	Indicates the most specific operating system in the Device Profile Library that matches the endpoint. For example, Macintosh > OS X 10.11 - El Capitan. If multiple operating systems match the endpoint, the property is resolved as the most specific value in the Device Profile Library that is common to all the matching operating systems. For example, if Windows Server 2008 Enterprise RTM and Windows Server 2008 Enterprise SP2 profiles both match the endpoint, the property is resolved as Windows Server 2008 Enterprise. If there is no common value among all the matching operating systems, the property is resolved as Multiple Suggestions. If no operating system profiles in the Device Profile Library match the endpoint, the property is resolved as Unknown. Select one or more operating systems. To detect all sub-classifications of the selected operating systems, select the Include sub-classifications check box.
Vendor and Model	Indicates the most specific vendor and model in the Device Profile Library that matches the endpoint. For example, Samsung > Samsung Galaxy Tablet > Samsung Galaxy Tablet 10. Select one or more vendors or models. To detect all sub-classifications of the selected vendors and models, select the Include sub-classifications check box.

Advanced classification properties

Service Banner	Indicates the service and version information, as determined by Nmap. Due to the activation of Nmap, this information may take longer to retrieve. Use of this property requires that you configure the HPS Inspection Engine.
Network Function Resolution Method	Indicates the method used to classify the device's Network Function property. The following options are available: Active Banner Active Fingerprint Managed (Network Device or Endpoint) Manual Classification Passive Banner Passive Fingerprint
HTTP User Agent	Indicates Learned HTTP User Agent Banner (from portal and Packet Engine).
Function Classified By	Indicates whether the Function classification property was determined by the Device Classification Engine, or was set by an action.
Operating System Classified By	Indicates whether the Operating System classification property was determined by the Device Classification Engine, or was set by an action.
Function Classification Update	Indicates whether a Function classification change is pending for this device due to a Device Profile Library upgrade. You can apply all pending classification changes in the Tools > Options > Device Profile Library window.
Operating System Classification Update	Indicates whether an Operating System classification change is pending for this device due to a Device Profile Library upgrade. You can apply all pending classification changes in the Tools > Options > Device Profile Library window.

Vendor and Model Classification Update	Indicates whether a Vendor and Model classification change is pending for this device due to a Device Profile Library upgrade. You can apply all pending classification changes in the Tools > Options > Device Profile Library window.
Suggested Function	If there are multiple candidates for the endpoint's Function classification, this property indicates all the profiles in the Device Profile Library that match this endpoint. These values are considered less accurate than the resolved Function property value, possibly due to conflicting choices. If the Function property has been changed by a policy or manual action, this property indicates the endpoint's Function classification set by the Device Classification Engine.
Suggested Operating System	If there are multiple candidates for the endpoint's Operating System classification, this property indicates all the profiles in the Device Profile Library that match this endpoint. These values are considered less accurate than the resolved Operating System property value, possibly due to conflicting choices. If the Operating System property has been changed by a policy or manual action, this property indicates the endpoint's Operating System classification set by the Device Classification Engine.
OS Fingerprint	Indicates the type of the operating system running on the endpoint, as determined by Nmap. Use this property instead of OS Class for classification of unlisted and unknown OS names. Due to the activation of Nmap, this information may take longer to retrieve. Use of this property requires that you configure the HPS Inspection Engine.
Compare OS Fingerprint to (Classification Version 2)	Indicates the difference between current OS Fingerprint and OS Fingerprint Classification Version 2. The following options are available: Both failed OS Fingerprint resolution failure OS Fingerprint (Classification Version 2) resolution failure Values are identical Values differ
Compare OS	Indicates the difference between current OS Fingerprint and OS Fingerprint

Fingerprint to (Classification Version 3)	Classification Version 3. The following options are available: Both failed OS Fingerprint resolution failure OS Fingerprint (Classification Version 3) resolution failure Values are identical Values differ
Compare Network Function To (Classification Version 2)	Indicates the difference between current Network Function and Network Classification Version 2. The following options are available: Both failed Network Function resolution failure Network Function (Classification Version 2) resolution failure Values are identical Values differ
Compare Network Function To (Classification Version 3)	Indicates the difference between current Network Function and Network Classification Version 3. The following options are available: Both failed Network Function resolution failure Network Function (Classification Version 3) resolution failure Values are identical

	Values differ

Device information properties

Access IP	Indicates the endpoint IP address that Forescout eyeSight used the last time it connected successfully to the endpoint.
Assigned Label	Labels mark and group endpoints based on properties or other evaluated values. Policies can apply further management logic based on labels assigned by a previous policy. This lets you construct complex policy behaviors that track endpoint history. This condition compares a text string to the labels assigned to the endpoint. The text string you specify is compared to each of the labels assigned to the endpoint. You can specify various matching logic options, such as partial string matching. You can apply time constraints to the condition. Forescout eyeSight matches only endpoints that satisfy the matching condition during the specified time period.
Comment	Indicates devices that contain device Comment text defined by the Forescout user. (Right-click an endpoint in the Detections pane to add a comment. The comment is retained for the life of the endpoint in the Console.) Special characters such as `~!@#$%^&=*()+[]\;'/{}|:"? are not allowed in the comment field and are removed if entered.
Compliance Status	Indicates the endpoint status based on policies categorized as Compliance policies.
Corporate / Guest Status	Indicates the endpoint status based on policies categorized as Corporate/ Guest Control policies.
Counter	Compares the value of a counter to a numerical value. Name: The name of an existing counter.

	Counter: Value(s) that the condition compares to the current value of the counter. You can specify a single value, a list of values, or a range of values. Note: Enable the Evaluate irresolvable criteria as True option when the Counter property is used to verify the presence of a newly created counter.
Forescout Script Result	Runs a script or command on the Appliance, and examines the result. Forescout eyeSight evaluates the script or command for each endpoint that matches previous conditions of the policy. This result is compared to the specified values and matching logic of the condition. Ignore Failed Script Result – Enter true to ignore any partial output received by eyeSight before the session failed. The property is evaluated as Irresolvable. Enter false to preserve output from the failed session in the property, and use that output to evaluate the condition. **Note:** If you are running a script to retrieve a value that includes the endpoint's IP address, the script should not include the {IP} tag, as Forescout eyeSight automatically appends the IP address to the list of arguments passed to the script.
Device Interfaces	Detects endpoints with specific device interface information. This information may be part of the interface name, vendor and MAC address. Use of this property requires the proper configuration and activation of the HPS Inspection Engine.
Device is DHCP Relay	Indicates whether endpoints are running DHCP Relay services. Use of this property requires the proper configuration and activation of the HPS Inspection Engine.
Device is DHCP Server	Indicates whether endpoints are DHCP servers. Use of this property requires the proper configuration and activation of the HPS Inspection Engine.
Device is NAT	Indicates whether the endpoint performs a Network Address Translation, potentially hiding other devices behind it. If you have enabled Partial Enforcement mode, this condition will not work.

	See Set the Enforcement Mode for details.
DHCP Server Address	Indicates whether the device IP address was received from a DHCP server. If so the value of the property is the IP address of the DHCP server. In addition to DHCP server properties, such as this one, which are discovered by Forescout eyeSight, additional DHCP host properties are discovered by the DHCP Classifier Plugin. This plugin extracts host information from DHCP messages and uses DHCP fingerprinting to determine the operating system and other host configuration information. For more information, refer to the *DHCP External Classifier Plugin Configuration Guide*.. Select Tools > Options > Modules, select the plugin, and then select Help.
DNS Name	Indicates the endpoint's DNS name.
Host is online	Indicates whether the endpoint is connected to the network.
IPv4 Address	IPv6 Address Indicates one or more IP addresses of an endpoint. Matching criteria include: Any IP address Addresses in a named Forescout Internal Network segment Addresses in a specific IP range or subnet IP addresses that start with, end or match a certain numerical expression Endpoints without a known IPv4 address (endpoints will be detected when Forescout eyeSight discovers their MAC address). For details about working with IPv6 addresses, refer to the *Work with IPV6 Addressable Endpoints How-to Guide*.
Last Known IPv4 Address	Indicates an IPv4 Address that once referred to this endpoint, but was assigned to another endpoint. See Work with Hosts Whose IPv4 Address Is Used by Another Host.

MAC Address	Indicates the MAC address of the endpoint.
Member of Group	Lets you investigate endpoints that are part of a group.
Nested Device ID	The detected ID of a sub-module or controller within an endpoint.
Nested Device Parent IP	The IP address of an endpoint that contains sub-modules or controllers.
NetBIOS Domain	Indicates the NetBIOS Domain to which the endpoint is logged on.
NetBIOS Hostname	Indicates the NetBIOS host name of the endpoint.
Network Adapters	Indicates specific types of network adapters, for example, adapters having a specific device name, MAC address or connection status. Endpoints must be managed by SecureConnector to resolve this property.
NIC Vendor	Indicates the vendor of the NIC, as detected by Forescout eyeSight based on the MAC prefix. The HPS NIC Vendor DB updates vendor information used to resolve this property. eyeSight can automatically add newly supported vendors to a policy condition that you create with this property. For more information about this plugin, select ToolsOptions > Modules, select the plugin, and then select Help.
NIC Vendor Value	Indicates a string value associated with the NIC Vendor. You can create conditions that match several variants of a vendor name, or look for a specific substring in a name. The HPS NIC Vendor DB updates vendor information used to resolve this property. Forescout eyeSight can automatically add newly supported vendors to a policy condition that you create with this property. For more information about this plugin, select Tools > Options > Modules, select the plugin, and then select Help.
Number of IPv4 Addresses	Number of IPv6 Addresses Indicates the number of IP addresses of each type that Forescout eyeSight

	detected for an endpoint. You can specify IPv4 addresses to ignore when calculating the Number of IPv4 Addresses property. For details refer to *Configure Tuning* in the *HPS Inspection Engine Configuration* Guide. The count of IPv6 addresses depends on the Purge IPv6 Timeout defined for inactive IPv6 addresses. There are parallel Track Changes properties.
Open Ports	Indicates the availability of open ports on the endpoint. This is determined by inspecting real-time traffic as well as using Nmap. The condition is considered "true" if any of the listed ports are detected.
OS CPE Format	Indicates the operating system running on the endpoint, in Common Platform Enumeration format. This property is reported by the Windows Applications, Linux, OS X and ARF Reports Plugins. The property contains the CPE 2.3 representation of the operating system bound to a formatted string. You can use Forescout property expression types (For example, Contains, In List, or Matches) to create policy conditions that identify logical parts or substrings of the CPE name string.
Segment Name	Retrieves the *leaf node name* of the network segment on which the endpoint resides. Condition options let you apply string matching criteria to this value.
Segment Path	Retrieves the full pathname of the network segment on which the endpoint resides. Condition options let you apply various string matching criteria to this value.
SMB Relay	Indicates the endpoint may be spoofing session-layer SMB authentication. Forescout eyeSight compares the IP address of the SMB session used by the endpoint to the IP addresses it discovers on the endpoint. If the IP address of the SMB session is not included in the addresses discovered on the endpoint, eyeSight assigns this property the value True and reports a NAT detection event using the Device Is NAT host property. Use this property to improve detection of man-in-the-middle attacks. There is a parallel Track Changes property.

snmpwalk Command Output	OID: Enter the ID. SNMP version: Enter the SNMP version. Community: Enter the community for versions 1/2c. User (V3): Enter the user and password (version 3). Password (V3): Enter the user and password (version 3). Extra snmpwalk options: Include additional snmpwalk options. If you include -x for SNMPv3 privacy, the same password used for authentication is used for privacy. Filter: Include only specific information in the output by piping into a Linux command. Ignore Failed Script Result: Enter true to ignore any partial output received by Forescout eyeSight before the session failed. The property is evaluated as Irresolvable. Enter false to preserve output from the failed session in the property, and use that output to evaluate the condition. **Note:** Enter *UNUSED* in a field if you want Forescout eyeSight to ignore the parameter.
SSH Command Output	SSH Username/SSH Password: Specify credentials used to log in and establish an SSH session on the endpoint. These credentials are not encrypted. SSH Connection Flags (optional): (Optional) Specify additional Open SSH option flags that are applied when the SSH session is established. Command: Enter the command submitted on the endpoint. Pipe session through AWK filter (optional): (Optional) Specify a Linux filter command to filter output before evaluating the condition. When command/session fails, evaluate condition: Select as Irresolvable to

	ignore any partial output when the session fails. The property is evaluated as Irresolvable. Select Based on data received to preserve output from the failed session in the property, and use that output to evaluate the condition. **Note:** Enter *UNUSED* in a field if you want Forescout eyeSight to ignore the parameter.
SSH Command Output (interactive)	SSH Username/SSH Password: Specify credentials used to log in and establish an SSH session on the endpoint. These credentials are not encrypted. SSH Connection Flags (optional): (Optional) Specify additional Open SSH option flags that are applied when the SSH session is established. Interactive Session Script: Enter an alternating series of commands and expected responses, beginning with a command. Each command is on an odd numbered line, each expected response is on an even line. Expected response lines contain regular expressions used to match actual output. Response timeout: The maximum interval, in seconds, that Forescout eyeSight waits after submission of each command for an output response. Login timeout: The maximum interval, in seconds, that Forescout eyeSight waits when it logs in to establish the SSH session. Pipe session through AWK filter (optional): (Optional) Specify a Linux filter command to filter output before evaluating the condition. When command/session fails, evaluate condition - Select as Irresolvable to ignore any partial output when the session fails. The property is evaluated as Irresolvable. Select based on data received to preserve output from the failed session in the property, and use that output to evaluate the condition. After eyeSight establishes an SSH session on the endpoint, it submits the first command listed in the Interactive Session Script field. eyeSight waits for a response, and tests the response output against the expected response in the next line of the script.

	If the actual response output does not match the expected response, or if the session times out without a response, eyeSight ends the interactive session. If the output matches the expected response, eyeSight submits the next command in the session script. eyeSight ends the session after a response is received for the last command, or after the session times out. The property contains a log of all submitted commands and complete actual responses. *Note: Enter *UNUSED* in a field if you want Forescout eyeSight to ignore the parameter*
Traffic seen	Indicates when network traffic was last seen.
URL Content	URL: Enter the path of the URL from which you want to retrieve information. You can use the {ip} tag to specify the endpoint IP address, for example, http://{ip}/info.html User/Password: Enter user credentials if access to the pane requires authentication. Kerberos Domain: Specify a Kerberos (Active Directory) domain if the user is part of a domain. Extra curl options. Set additional curl options (check out 'man curl' on Linux) Filter: Include only specific information in the output by piping into a Linux command. For example, to exclude the text XYZ use `" grep –v "XYZ""` Ignore Failed Script Result: Enter true to ignore any partial output received by Forescout eyeSight before the session failed. The property is evaluated as Irresolvable. Enter false to preserve output from the failed session in the property, and use that output to evaluate the condition. **Note:** Enter *UNUSED* in a field if you want Forescout eyeSight to ignore the parameter.

User	Indicates the domain user name currently logged on to the endpoint. This property is reported by the HPS Inspection Engine and OS X Plugins.

Event properties

ARP Spoofing	Indicates whether the number of different MAC address reported for an IP address exceeds the number specified here. This lets you keep track of the different MAC addresses used by an IP address as advertised by ARP responses. Normally, there should be only one MAC address per IP address. This property lets you detect attempts to maliciously direct network traffic. To work with this condition, the Appliance must monitor ARP traffic, i.e., the broadcast domain where ARP requests are transmitted. Refer to the *Port Mirroring Technical Note* for more information about configuring your environment for detecting ARP spoofing.
Admission	Indicates whether one or more admission events were detected. Admission event types include: New IP: By default, endpoints are considered new if they were not detected at your network within a 30-day period. For example, if an IP was detected on the first of the month, and then detected again 31 days later, the detection initiates the activation. The default time period can be changed. See Policy Preferences for details. IP Address Change Switch Port Change DHCP Request Authentication via the HTTP Login action Log in to an authentication server SecureConnector connection If you have installed plugins/modules, additional admission events types may

	be available. For example, the New Wireless Host Connected Events option is available if you installed the Wireless Plugin.
Malicious Event	Indicates the type of threat protection event to respond to. Parameters selected here are applied in addition to parameters defined in the Threat Protection Policy. See Threat Protection for details.
Miscellaneous Events	Indicates endpoints whose IP address was used by a newly connecting endpoint. This may happen, for example, if the original endpoint was offline for a certain period and the newly connecting endpoint received its IP. When this happens, the original endpoint is displayed in the Console without an IP address until it reconnects.
NetFlow Sessions as Client / NetFlow Sessions as Server	Sessions let you run policies based on real-time identification of network traffic patterns between servers and clients, helping you pinpoint: When sessions are initiated Which protocols are used For example, use this property to ensure compliance of data flow security for audit usage or to track down network users trying to access sensitive protected data, such as credit card information or financial accounts. Indicates which endpoints generated sessions to specific servers using a defined protocol. Sessions as Client: Indicates which endpoints generated sessions to specific servers using a defined protocol. Sessions as Server: Indicates which servers received sessions from specified endpoints using a defined protocol.
Traps Received	Indicates that an SNMP trap was received on the port where the endpoint is connected.

External devices properties

External Devices	Refers to external devices connected to an endpoint by cross-referencing all the device attributes listed below. In order for an endpoint to match the defined condition, all attributes in this list must match. Name: Detects endpoints connected to an external device with a specific device name. ID: Detects endpoints connected to an external device with a specific device ID number. Class: Detects endpoints that are connected to specific external device classes, including: Wireless communication devices Portable devices Windows CE USB devices Printers PCMCIA and Flash memory devices Other devices Network adapters Modems Infrared devices Imaging devices Disk Drives DVD/CD-ROM drives

Bluetooth Radios

Bus Type: Detects the bus on which the external device is connected.

Status: Detects the connection status.

Guest registration properties

Guest Account Approve Date

Indicates when the guest network access was approved.

Guest Approved By

For users allowed network access as guests via the HTTP Login action, this field indicates the email address of the sponsor who approved the network access.

Guest Registration Status

Indicates the status of a guest network access request.

Guest Tags

Indicates the value of the tags assigned by the sponsor to the guest.

See Managing Guest Tags for details.

Guest Registration Information

For users allowed network access as guests via the HTTP Login action, this field indicates the information that was provided when the guest self-registered or was registered by a sponsor or operator:

Guest Account Approve Date

Guest Comment

Guest Company

Guest Contact Person

Guest Contact Person Email

Guest Custom[1-5] form fields

	Guest Email Address
	Guest Full Name
	Guest Location
	Guest Phone Number
	Guest Registration browser user agent
	Guest Registration Date
	Guest Title
	User Name
	You can use any of this information to enforce actions on guests.

Health monitoring properties

The following properties are used to help you monitor Appliance health. These properties are included in policies created by Health Monitoring Templates. Running these templates populates Health Monitoring Dashboard widgets.

Health Monitoring

Forescout Device Models	Indicates the Forescout device model, including 5100 Series and CT Series physical Appliances, and virtual Appliances.

Health Monitoring – Plugin Health

Plugins Health Metrics	Indicates the following health metrics for installed Forescout plugins:
	Name of the Forescout plugin
	Whether the Forescout plugin crashed sometime in the last 30 minutes
	Whether the Forescout plugin stalled sometime in the last 30 minutes

	The maximum number of plugin requests dropped per minute
	The average amount of time, in seconds, that plugin requests are delayed on this Appliance

Health Monitoring – Policy Efficiency

Forescout Device Admission Event Rate	Indicates the average rate of new endpoints being admitted into the network, per minute, and normalized to 100 managed endpoints.
Forescout Device Property Value Change Rate	Indicates the average rate that property values are changing, per minute, and normalized to 100 managed endpoints.
Forescout Device Learn Events Rate	Indicates the average rate that plugins report to eyeSight about new learned properties, per minute, and normalized to 100 managed endpoints.
Forescout Device Resolve Request Rate	Indicates the average rate that requests to resolve endpoint properties are made, per minute, and normalized to 100 managed endpoints.

Health Monitoring – Load Specification Compliance

Forescout Device CPUs	Indicates the number of CPUs in the Forescout device.
Forescout Device 802.1x Authentication Rate	Indicates the number of 802.1x authentications performed by the Forescout device, per second.
Forescout Device HTTP Login Rate	Indicates the number of HTTP logins (captive portal) performed by the Forescout device, per minute.
Forescout Device Switch/WLAN Devices	Indicates the number of switch and wireless LAN devices managed by the Forescout device.
Forescout Device Total Memory (GB)	Indicates the total memory of the Forescout device, in GB.

Forescout Device Traffic Bandwidth (Mb)	Indicates the bandwidth of traffic processed by the Packet Engine, in megabits per second (Mbps).
Forescout Device Packets (Kpps)	Indicates the packets processed by the Packet Engine, in kilo packets per second (kpps).
Forescout Device Hard Drive (GB)	Indicates the Forescout Device hard drive storage, in GB.
Forescout Device Managed Endpoints	Indicates the number of endpoints managed by the Forescout device.

Health Monitoring – Resource Utilization

Forescout Device CPU Usage (%)	Indicates the average percentage of the total CPU usage of the Forescout device.
Forescout Device Global Lock (%)	Indicates the percentage of time that critical resources are locked by a thread in the Forescout system.
Forescout Device Memory Usage (%)	Indicates the percentage of system memory used on the machine.
Forescout Device Packet Loss (%)	Indicates the average amount of packets that are lost, and not processed by the packet engine.
Forescout Device Storage Usage (%)	Indicates the percentage of the hard drive that is being used.
Forescout Device Swaps Average	Indicates the average amount of memory swapped in/out per second.
Forescout Device Resolve Delay	Indicates the average delay in resolving Forescout properties, in seconds.
Virtual Forescout Device CPU Ready (%)	Indicates the average CPU ready % per vCPU (the percentage of time the VM was ready, but could not be scheduled to run on the physical CPU). In general, values under 5% are acceptable. Values 5% and above indicate potential performance issues due to CPU resource contention.

The VMware vSphere Plugin must be configured and running for this property to work.

Virtual Forescout Device Disk Highest Latency

Indicates the highest read or write latency in milliseconds for all disks configured for the VM.

Note:
The VMware vSphere Plugin must be configured and running for this property to work.

Linux properties

Linux Expected Script Result

Use this property to run a command or file that detects certain endpoint attributes, statuses or any other information defined in the script or command. Commands and file can also be used to carry out actions on endpoints.

Enter a command or browse to a file that you want to run. The commands and scripts that you create are automatically saved on all Appliances. All file extensions are supported and can be run.

A Run Script Action is also available.

Linux File Date

Indicates the last modification date and time of a defined file on an endpoint.

Linux File Exists

Indicates whether a specified file exists on an endpoint.

Linux File Size

Indicates the size (in bytes) of a specified file on an endpoint.

Linux Hostname

Indicates the Linux host name.

Linux Manageable (SSH Direct Access)

Indicates whether the endpoint is connected to eyeSight via SSH and is manageable via Remote Inspection.

Linux Manageable (SecureConnector)

Indicates whether the endpoint is connected to eyeSight via SecureConnector.

Linux Processes Running	Indicates the full pathnames of processes running on an endpoint.
Linux SecureConnector Version	Indicates the version of the SecureConnector package running on the endpoint.
Linux User	Indicates all the users logged in to the endpoint. The list of usernames is comma-separated.
Linux Version	Indicates the specific version of Linux running on the endpoint.
OS CPE Format	Indicates the operating system running on the endpoint, in Common Platform Enumeration format. The plugin resolves this general Forescout property for Linux endpoints.
User	This is a general Forescout property. For Linux endpoints, the plugin populates this property with the username of the user currently logged in to the endpoint console. You can query the User Directory based on this value.

Macintosh properties

The OS X Plugin supports the following properties for macOS endpoints.

Macintosh Expected Script Result	Runs a command or file that detects certain endpoint attributes, statuses or any other information defined in the script or command. Commands and file can also be used to carry out actions on endpoints. Enter a command or browse to a file that you want to run. The commands and scripts that you create are automatically saved on all Appliances. All file extensions are supported and can be run. A Run Script action is also available.
Macintosh Applications Installed	Indicates the applications present on an endpoint. For endpoints running OS X 10.8, the Certificate field is not reported.
Macintosh File Date	Indicates the last modification date and time of a defined file on an endpoint.

Macintosh File Exists	Indicates the existence of a specified file on an endpoint.	
	Macintosh File Size	Indicates the size (in bytes) of a specified file on an endpoint.
Macintosh Hostname	Indicates the macOS host name.	
	Macintosh Manageable (SecureConnector)	OSX SecureConnector Connected/Disconnected Indicates whether the endpoint is connected to eyeSight via SecureConnector. OSX SecureConnector Connected/Disconnected is the related Track Changes property.
Macintosh Processes Running	Indicates the processes running on an endpoint.	
	Macintosh SecureConnector Version (OSX Plugin)	Indicates the version of the SecureConnector package running on the endpoint.
Macintosh Software Updates Missing	Indicates macOS security and other updates that are missing on the detected endpoint. To resolve this property on endpoints running OS X 10.8, Forescout eyeSight must use an admin account to access the endpoint.	
Macintosh User	Indicates all the users logged in to the endpoint. The list of usernames is comma-separated.	
Macintosh Version	Indicates the version of macOS running on the endpoint.	
	OS CPE Format	Indicates the operating system running on the endpoint, in Common Platform Enumeration format. The plugin resolves this general Forescout property for macOS endpoints.

OSX SecureConnector Connected/ Disconnected	OSX SecureConnector Connected/Disconnected is the related Track Changes property.
User	This is a general Forescout property. For macOS endpoints, the plugin populates this property with the username of the user currently logged in to the endpoint console. You can query the User Directory based on this value.

Remote inspection properties

The following properties indicate which management services are available on the endpoint that Forescout eyeSight can use to perform Remote Inspection.

MS-RRP Reachable	Indicates whether Forescout eyeSight can use the Remote Registry Protocol for Remote Inspection tasks on the endpoint.
MS-SMB Reachable	Indicates whether Forescout eyeSight can use the SAMBA protocol for Remote Inspection tasks on the endpoint.
MS-WMI Reachable	Indicates whether Forescout eyeSight can use the Windows Management Interface for Remote Inspection tasks on the endpoint. In previous releases, this property was named Windows Manageable Domain by WMI.

These properties do not have an Irresolvable state. When the plugin or module cannot establish connection with the service, the property value is False. Do not use the Evaluate Irresolvable Criteria as option with these properties.

The following corresponding Track Changes policies are listed under the Track Changes folder:

- MS-RRP reachability changed
- MS-SMB reachability changed
- MS-WMI reachability changed

SNMP properties

Use of SNMP properties requires the proper configuration and activation of the HPS Inspection Engine. When entering the following values, use these guidelines:

- For SNMP V1, use: `-v 1 -c <community>`
- For SNMP V2, use: `-v 2 -c <community>`
- For SNMP V3, use: `-v 3 -u <user> -A <password>`

  Use the SNMP Parameters field to enter optional SNMP connection parameters. The following parameters are supported:

Parameter	Description
-p <port>	Specify the port used for SNMP messaging on the server.
-r <retries>	Specify the number of times to retry the request.
-t <seconds>	Specify the timeout period before retrying the request.
-E <engine_ID>	Specify the Context Engine ID for REQUEST messages (SNMP v3 only).
-n <cont_name>	Specify the Context Name (SNMP v3 only).

SNMP-MIB-II ifNumber

Indicates the number of network interfaces (regardless of their current state) present on this system. The collection of this information depends on access parameters (SNMP Parameters) specific to the SNMP version of the inspected endpoint.

In the SNMP-MIB-II ifNumber field, enter the number of interfaces to be detected on the SNMP agent.

SNMP-MIB-II

sysDescription

Indicates a textual description of the entity. This value should include the full name and version identification of the system's hardware type, software operating-system, and networking software. It is mandatory that this only contain printable ASCII characters. The collection of this information depends on access parameters (SNMP Parameters) specific to the SNMP version of the inspected endpoint.

In the SNMP-MIB-II sysDescription field, enter the description that should match the SNMP agent system description. If you are not sure of the name, you can use the regular expression option, and enter wildcard text – for example, ci.* if you want to detect a Cisco switch.

SNMP-MIB-II sysLocation

Indicates the physical location of this node (for example, telephone closet, third floor). The collection of this information depends on access parameters (SNMP Parameters) specific to the SNMP version of the inspected endpoint.

In the SNMP-MIB-II sysLocation field, enter the location that should match the SNMP agent. If you are not sure of the name, you can use

	the regular expression option, and enter wildcard text (.*).
SNMP-MIB-II sysName	Indicates an administratively assigned name for this managed endpoint. By convention, this is the endpoint's fully qualified domain name. The collection of this information depends on access parameters (SNMP Parameters) specific to the SNMP version of the inspected endpoint. In the SNMP-MIB-II sysName field, enter the requested system name to match.
SNMP-MIB-II sysUpTime	Indicates the time since the network management portion of the system was last re-initialized. The collection of this information depends on access parameters (SNMP Parameters) specific to the SNMP version of the inspected endpoint. Use the Older than or Before options to create a condition based on the time the SNMP agent was last turned on.
SNMP-OID	Indicates an OID value, on the SNMP agent. The collection of this information depends on access parameters (SNMP Parameters) specific to the SNMP version of the inspected endpoint. In the SNMP OID field, enter the requested OID value on the endpoint. If the OID query and the SNMP-OID Value match, then the condition is registered.

Switch properties

An extensive range of properties are resolved for Switches that are configured to work with Forescout eyeSight. The section provides an overview of the Switch properties.

Select Options from the Tools menu and then select Switch to configure the Switch Plugin. Select Help for information about configuration and for more information about working with switch properties.

Basic managed switch information

The following properties resolve basic information about a managed switch:

SGT	The Security Group Tag (SGT) assigned to an endpoint. An SGT is a number in the range of 1 - 65,535.

	Endpoints with an assigned SGT are connected to a managed Cisco switch in a Cisco TrustSec domain. When the property is currently included in existing policies and the advanced configuration flag `assign_sgt` is disabled, the property is marked as Obsolete in the relevant policies. For details about this flag, refer to the *Forescout Switch Plugin Configuration Guide*.
Switch Port Configurations	**Note:** For use with Cisco and Arista devices only. The configuration detail of the switch interface to which an endpoint is connected. For this property to be resolvable, the Switch Plugin must be configured to use CLI to learn the endpoints that are connected to the managed switch. For details, refer to the Forescout Switch Plugin Configuration Guide.
Number of Hosts on Port	The number of endpoints connected to a specific port. You can write a condition for this number to instruct the Switch Plugin to detect ports with more than one endpoint (MAC address) if, for example, a hub and a guest computer have been connected together with a company endpoint on a company switch port. Ports connecting between switches are excluded from this calculation.
Switch Hostname	The switch name as defined in the managed switch.
Switch IP/FQDN	Either the IP address or the fully qualified domain name of the switch.
Switch IP/FQDN and Port Name	Either the IP address or the fully qualified domain name of the switch and the port name (the physical Ethernet interface information of the port). The format is `<IP address/FQDN>:<port>`.
Switch Location	The switch location based on the switch MIB.
Switch OS	The operating system of the switch device to which the endpoint is connected.
Switch Port ACL	The name of the ACL applied to the switch port.

Switch Port Action	The action, either Assign to VLAN, Provision VLAN or Switch Block, that is assigned to the switch port.
Switch Port Alias	The description of the port as defined in the switch configuration and modified by the Switch Plugin.
Switch Port Connect	The physical connectivity between the endpoint and the switch port.
Switch Port PoE Connected Device	**Note:** For use with Arista, Brocade, Cisco, Huawei, and Tejas devices only. Description of the PoE device that is connected to the PoE-enabled switch port, as provided by the managed switch. For example, `Cisco IP Phone 6921`. For all other plugin-managed switches, this property displays the value N/A (not available).
Switch Port PoE Power Consumption	**Note:** For use with Arista, Brocade, Cisco, Huawei, and Tejas devices only. Power consumption of the PoE device that is connected to the PoE-enabled switch port, as provided by the managed switch. The power consumption value provided is in milliwatts (mW). For example, 750. When either a non-PoE device or no device is connected to the PoE-enabled switch port, the property value is zero (0). For switch vendors that the plugin does not support switch port PoE, the Console displays the following information for this property: `Vendor is currently not supported for this property`.
Switch Port Name	The hard-coded port name.
Switch Port VLAN	The VLAN associated with the switch port.
Switch Port VLAN Name	The name of the VLAN associated with the switch port.

Switch Port Voice Device	Whether the endpoint connected to the switch port is a VoIP device.
Switch Port Voice VLAN	The switch port VLAN to which the VoIP endpoint is connected.
Switch Vendor	The switch vendor name.
Switch Virtual Interface	Identifies whether the switch interface is a Switch Virtual Interface or not. The property is supported for managed switches only.
Switch VoIP Port	Whether the switch port is a VoIP port.
System Description	Detects the system description information provided by the managed device. System description information is as specified by the network device SNMPv2-MIB property `sysDescr (1.3.6.1.2.1.1.1)`.
Switch Device Vendor and Type	The vendor and the device type of a managed switch device. Examples: Cisco (switch) or Cisco_ASA (firewall). Currently, this property is only available for use in/resolved by a policy that is created using a Vulnerability and Response (VR) policy template.

Network device compliance properties

For any Cisco network device managed by the Switch Plugin, use the following policy properties to create policies that determine network device compliance:

Running Config	**Note:** For use with Cisco devices only. Detects running config information of switches managed by the Switch Plugin, as generated by the `show running-config` command. The Switch Plugin resolves this property for information in the following instances: (a) After plugin start and initially detecting the switch and (b) Whenever running config information changes. Before working with this property, several configuration tasks must be performed.

	As the amount of information provided by the resolved Running Config property can be very extensive, you can filter this information.
Running Config Time	**Note:** For use with Cisco devices only. Contains the timestamp, `MM/DD/YY HH:MM:SS AM/PM`, of the plugin's running config information query of the device.
Interface Table	**Note:** For use with Cisco devices only. Detects the specific interface configuration provided in a device running config for the interface. Per interface, the resolved property provides the following information: Interface Name: The interface name and when available the interface location information. Interface Configuration (raw): The specific, interface configuration, as provided in a device running config.

Track changes properties

Items in this category check whether a property value has changed, for example, if a user name changed. Detecting changes in endpoints is a powerful method of identifying possible attacks or noncompliance.

All these properties exist under other categories, but here these properties check whether the value has changed. For example, the Windows File Size property in the Windows folder detects the size of a file at a specific location. In the Track Changes folder, Forescout eyeSight detects if the file size at that location changed.

Some of the Track Changes properties require the proper configuration and activation of the HPS Inspection Engine.

User directory properties

The following user attributes indicate if the user's account in the User Directory is disabled or expired:

- Account is Disabled
- Account is Expired

The following user attributes may vary depending on the User Directory configuration:

- Common Name, Employee Number, Password Last Set
- Company, Initials, Phone
- Department, Last Name, Street Address
- Display Name, LDAP User Name, Title
- Distinguished Name, Member Of, User Given Name
- Email, Mobile Phone

Windows properties

NetBIOS Membership Type
Indicates whether the endpoint is a domain or workgroup member.

SMB Signing
Indicates support for SMB Signing on the Windows endpoint. Valid values are:

Required: the endpoint requires that all SMB communication is signed.

Enabled: the endpoint supports SMB signing but does not require it.

Disabled: the endpoint does not support SMB signing, even when it is requested by the communicating entity

Windows Active Users
Indicates the username/domain of one or more users currently logged in to a Windows endpoint

Windows Domain Member
Indicates whether the endpoint is a member of any of the domains defined in the HPS Inspection Engine.

Windows Expected Script Result
For use on managed Windows machines only.

Use this property to run a command or file to detect certain endpoint attributes, statuses, or any other information defined in the script or command. Commands and file can also be used to carry out actions on endpoints.

(If you use a file that exists on the endpoint, enter its absolute path).

You can also enter output text that should be matched on the endpoint against the output of the script.

	Use this property, for example, to find users sharing the My Music folder. A script is run by starting a service called `fsprocsvc`. The service does not open any new network connection or generate traffic. Communication is carried out over Microsoft's SMB/RPC (139/TCP or 445/TCP) and authentication is carried out using domain credentials. If there is no request to run a new command within two hours, the service dissolves automatically. Refer to the *HPS Inspection Engine Configuration Guide*. for more information about this service. You can reference the result of the script using a property tag.
Windows File Date	Indicates the date that a specific file was last modified. Use this property, for example, to check that endpoints on the network have a specific file, from a specific date. Examples would be a security configuration file or an antivirus signature file. By using this condition, you can create a policy that enforces existence of the specific file, from a specific date, on every endpoint.
Windows File Exists	Indicates a file name. Use this property, for example, to check that endpoints on the network have a specific file. You can use the following Windows environment variables when you specify a pathname in a condition: %COMMONPROGRAMFILES% %PROGRAMFILES% %TEMP% %HOMEDRIVE% %SYSTEMDRIVE% %USERPROFILE% %HOMEPATH% %SYSTEMROOT% %WINDIR%
Windows File MD5 Signature	Indicates endpoints with specific MD5 signatures.
Windows File Size	Indicates a file name and size (in bytes). Use this property to check that endpoints on the network have a specific file of a specific file size.
Windows File Version	Indicates the version of a defined file on an endpoint.
Windows File Version Comparison	Indicates the existence of a defined file with a version higher than specified.

Windows Is Behind NAT	Indicates whether the endpoint was detected behind a NAT device.
Windows Last Login Event	Indicates the last detected login event on Windows endpoints that are managed by SecureConnector installed as a service. The property is resolved to one of the following values: None: No Login or Logout events have been detected, or the endpoint is not managed by SecureConnector as a service. Login: The most recent Windows Login/Logout Event received by SecureConnector was Login. Logout: The most recent Windows Login/Logout Event received by SecureConnector was Logout.
Windows Logged On	Indicates whether a user is logged in to the endpoint.
Windows Manageable Domain	Indicates whether Forescout eyeSight has access to the endpoint's remote registry and file system. If either criterion is not met, the endpoint is unmanageable. This is typical of endpoints that are foreign to the domain. Irresolvable endpoints are resolved based on their previous recheck status.
Windows Manageable Domain (Current)	Similar to the Windows Manageable Domain property, except that if irresolvable, the status not manageable is applied until the next recheck. This property differs from the Windows Manageable Domain property, which resolves irresolvable endpoints based on their previous recheck status.
Windows Manageable Local	Indicates that Forescout eyeSight either has or does not have access to localhost credentials on the detected machine. These credentials include the local user name, password and domain. When this information is available, the endpoint is manageable and can be inspected.
Windows Manageable SecureConnector	Indicates whether Forescout SecureConnector is running on the endpoint. See Start SecureConnector / Stop SecureConnector for details. When an endpoint with multiple interfaces connects to eyeSight through one

	NIC, only that host (NIC) is reported by this property. When Forescout actions are applied to a dual-homed endpoint, the action is applied to all interfaces of the endpoint, even if another host (NIC) on the same endpoint is managed by SecureConnector. If a blocking action is applied to the endpoint, it may lose access to network services it uses. The Advanced Tools Plugin provides an additional host property that can be used to detect and manage dual-homed endpoints using SecureConnector.
Windows Processes Running	Indicates Windows processes running on inspected endpoints.
Windows Processes Running and User	Indicates a currently active process on a Windows endpoint, and the username/domain of the user that owns the process.
Windows Registry Key Exists	Indicates the existence of a specified Windows registry key. Only the following key roots are available: HKEY_CLASSES_ROOT, HKEY_LOCAL_MACHINE and HKEY_USERS.
Windows Registry Value	Indicates the value of a specified Windows-registry key. Only the following key roots are available: HKEY_CLASSES_ROOT, HKEY_LOCAL_MACHINE and HKEY_USERS. To retrieve the default value of a registry key, end the pathname with a backslash as in this example: `HKEY_LOCAL_MACHINE\HW\DESCRIPTION\System\BIOS\`
Windows Registry Value Exists	Indicates the existence of a value for a specified Windows registry key.
Windows SecureConnector Connection Encryption	Indicates the TLS version used in communications with SecureConnector on Windows.
Windows SecureConnector Deployment Type	Indicates the SecureConnector deployment mode installed on the endpoint.
Windows	Indicates the SecureConnector visible mode installed on

SecureConnector Systray Display	the endpoint.
	Windows Services Installed (Display Name) Identifies the Windows services that are currently installed on a Windows endpoint. The resolved property provides the Display name of each installed Windows service. A Windows service's display name can vary across Windows endpoints, depending upon each machine's OS language. Note: In eyeSight versions prior to 8.3, this property is named Windows Services Installed.
Windows Services Installed (Service Name)	Identifies the Windows services that are currently installed on a Windows endpoint. The resolved property provides the Service name of each installed Windows service. A Windows service's service name is consistent across Windows endpoints because service names are independent of the machine's OS language.
Windows Services Running (Display Name)	Identifies the Windows services that are currently running on a Windows endpoint. The resolved property provides the Display name of each running Windows service. A Windows service's display name can vary across Windows endpoints, depending upon each machine's OS language. Note: In eyeSight versions prior to 8.3, this property is named Windows Services Running.
Windows Services Running (Service Name)	Identifies the Windows services that are currently running on a Windows endpoint. The resolved property provides the Service name of each running Windows service. A Windows service's service name is consistent across Windows endpoints because service names are independent of the machine's OS language.
Windows Shared Folders	Indicates whether a specific folder is currently shared on a Windows endpoint. Use this property, for example, to find network users sharing music folders. The ability to detect shared directories increases network security by helping users stop unwanted data from propagating across the network. This property returns the name of the directory.
Windows Version	Indicates to specific Windows versions detected or missing on the endpoint.

Windows Version CPE Format	Indicates the Windows version running on an endpoint in Common Platform Enumeration format. The property contains the full CPE 2.3 name string, bound to a URI, as follows: `cpe:/<part>:<vendor>:<product>:<version>:<update>:<edition>:<language>:<sw_` Use text matching tools to create policy conditions that match substrings of the CPE name string. The value of this property is duplicated in the more general OS CPE Format host property.
Windows Version Fine-tuned	Indicates the specific version of Windows running on the host.

Windows application properties

The Windows Applications Plugin is used to resolve several properties.

To create policy conditions based on these properties, choose from the list of supported third-party applications. Forescout eyeSight has analyzed the structure, footprint, and related processes of these applications, so the plugin detects them more accurately and inspects them more deeply. New releases of the Windows Applications Plugin add supported applications or enhance support for known applications.

You can choose to automatically add newly supported vendor applications to a policy condition that you create with these properties. See Detect New Vulnerabilities and Newly Supported Vendor Applications for details.

When you define policy rules to handle detected endpoints, remember that the scope of these properties is limited to supported applications—they do not detect or inspect unsupported applications.

For example:

- The Instant Messaging Installed property detects endpoints on which at least one supported messaging application is installed. It does not detect other applications that may be present on the endpoint. When no supported applications are detected on the endpoint, the property resolves to the value *None*, but unsupported messaging applications may be present.
- Similarly, the Hard Drive Encryption State property detects drives/partitions encrypted by supported applications. When no drives are encrypted by supported applications, the property resolves to the value Not Encrypted for each partition on the endpoint, but partitions may be encrypted by unsupported applications.

  Note:
  Use other host properties to create conditions that inspect endpoints and detect files or processes of unsupported applications.

Windows	Indicates which applications are installed on the Windows endpoint via

Applications Installed	Add/Remove Programs. This property resolves the name of the applications, and their version number if available. When you define policies with Windows Applications Installed and select For all property values and Name, all the installed applications must match the Name for the host to match the condition.
Cloud Storage Installed	Indicates that at least one of the following cloud storage applications is installed on the endpoint.
Cloud Storage Running	Indicates that at least one of the following cloud storage applications is running on the endpoint.
Hard Drive Encryption Installed	Indicates the hard drive encryption applications(s) installed on the endpoint.
Hard Drive Encryption State	Indicates whether hard drives on the endpoint are encrypted, and which application, if any, was used to encrypt each drive.
Instant Messaging Installed	Indicates that an instant messaging application is installed on the endpoint.
Instant Messaging Running	Indicates that an instant messaging application is running on the endpoint.
Microsoft Applications installed	Indicates the existence of Microsoft products on the endpoint.
Peer-to-peer Installed	Indicates endpoints that have installed peer-to-peer applications.
Peer-to-peer Running	Indicates endpoints that are running peer-to-peer applications.

Windows security properties

The Windows Applications Plugin updates vendor information used to resolve several of these properties. You can choose to automatically add newly supported vendors to a policy condition that you create with these properties. See Detect New Vulnerabilities and Newly Supported Vendor Applications for details.

Anti-Spyware Installed	Indicates whether Anti-Spyware is installed.	
	Antivirus Installed	Indicates whether an antivirus service is installed.
Antivirus Running	Indicates whether an antivirus service is currently running on the endpoint.	
	Antivirus Update Date	Indicates the date of the last antivirus signature update performed on the endpoint. The antivirus application must be running to be detected. This means an update is installed on any antivirus vendor running on the endpoint.
Windows Hotfix Installed	Indicates the existence of a security update on the endpoint, based on Hotfix ID and caption.	
Intranet WSUS Server	Indicates the host name or IP address of the intranet WSUS server on the endpoint. Use this property when working with the Microsoft Vulnerability properties and the Start Windows Updates action. The server version on the endpoint and the server version installed on the network must match in order for endpoints to be remediated by a WSUS server.	
Microsoft Vulnerabilities	Indicates the existence of published Microsoft operating system and application vulnerabilities on the endpoint. To use this property: The Windows Update Agent must be available on the endpoint. The endpoint must be managed by either Remote Inspection or SecureConnector. Refer to the HPS Inspection Engine Configuration Guide for details. You can automatically add newly supported vulnerabilities to a policy condition that you create with this property. See Detect New Vulnerabilities and Newly Supported Vendor Applications. Use the Windows Self Remediation action to download missing patches to endpoints.	

Microsoft Vulnerabilities Fine-tuned	Indicates the existence of Microsoft published OS and Office vulnerabilities detected on the endpoint. Fine-tune inspection according to specific criteria. The following criteria can be searched: Label Update Time Severity Product CVE An advanced option for the Microsoft Vulnerabilities property lets you improve performance and reduce network bandwidth. Use the option to define the rate to recheck endpoint vulnerabilities on machines where vulnerabilities were already checked and not found. These endpoints will not be rechecked at a rate higher than the rate that you define. If the rate that you define is more frequent than the rate in the Recheck policy, the Recheck policy rate is applied. If you disable this option, the Recheck policy rate is applied.
Personal Firewall	Indicates if a personal firewall has been detected on the endpoint.
Windows Updates Installed – Reboot Required	Indicates if Windows updates were installed, and if the endpoint is waiting for a reboot. Use this property in conjunction with Microsoft Vulnerability Updates to indicate if a reboot of the endpoint is needed to complete the installation of a security update.
Windows Security Center Antivirus Status	Indicates antivirus applications detected on the endpoint by the Windows Security Center, as well as endpoint status.
Windows Update Agent Installed	Indicates whether the Windows Update Agent (WUA) is installed on network endpoints. The agent is required to

resolve the Microsoft Vulnerabilities and Microsoft Vulnerabilities Fine-tuned properties, as well as carry out the Start Windows Updates action.

Defining and managing lists

Lists contain endpoint properties and related values, for example, a list of domain user names or a list of DNS names, or of processes that you want to prohibit on your network. Each List is associated with a single endpoint property and can contain multiple related values. Manually create lists here or create lists based on Inventory detections and policy detections. You can use Lists of property values when defining policies.

Using lists speeds up and streamlines the policy creation and endpoint management process.

For example, create an Unauthorized Processes Running list and use that list in a policy with the Kill Process action on endpoints that are running the process.

You can use this option for any property that consists of free text and for the Device Information > Open Ports property. Other properties, for example, installed software, peer-to-peer applications or properties indicating endpoint manageability, cannot be included in lists.

Note:
The Corporate/Guest Control template automatically generates a list of corporate domains.

The following options are available for creating property lists:

- Working with Lists.
- Modify Lists Based on Endpoint Detections.
- Create lists from properties discovered via the Asset Inventory and policies. See Create Lists Based on Inventory Detections and Add Endpoint Properties to a List for details.

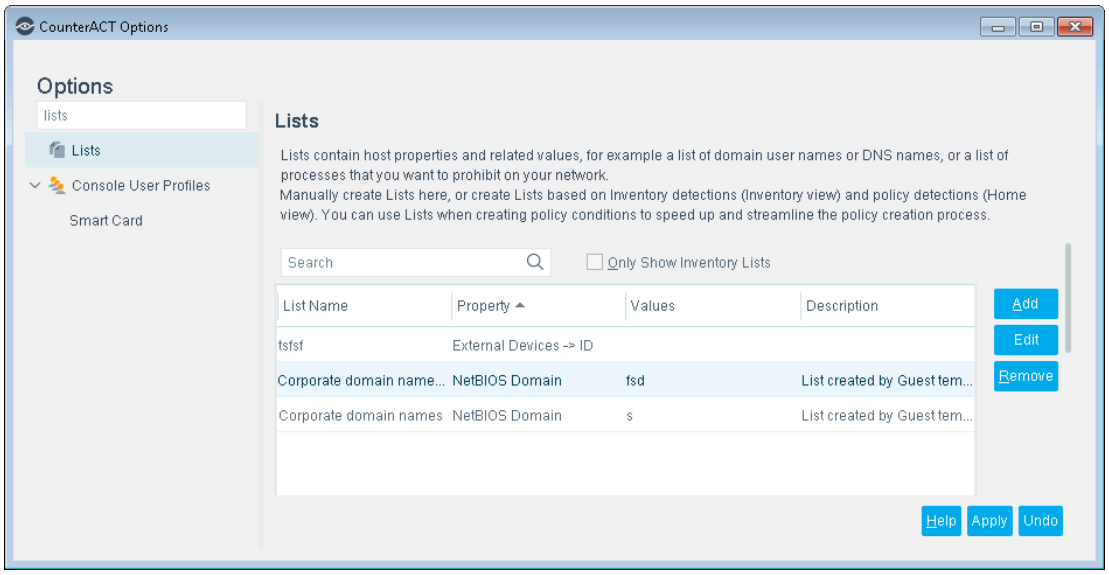
You may have generated lists based on Inventory detections. Select Only Show Inventory Lists in the Lists pane to display only those lists. See Working with Asset Inventory Detection for details.

Working with lists

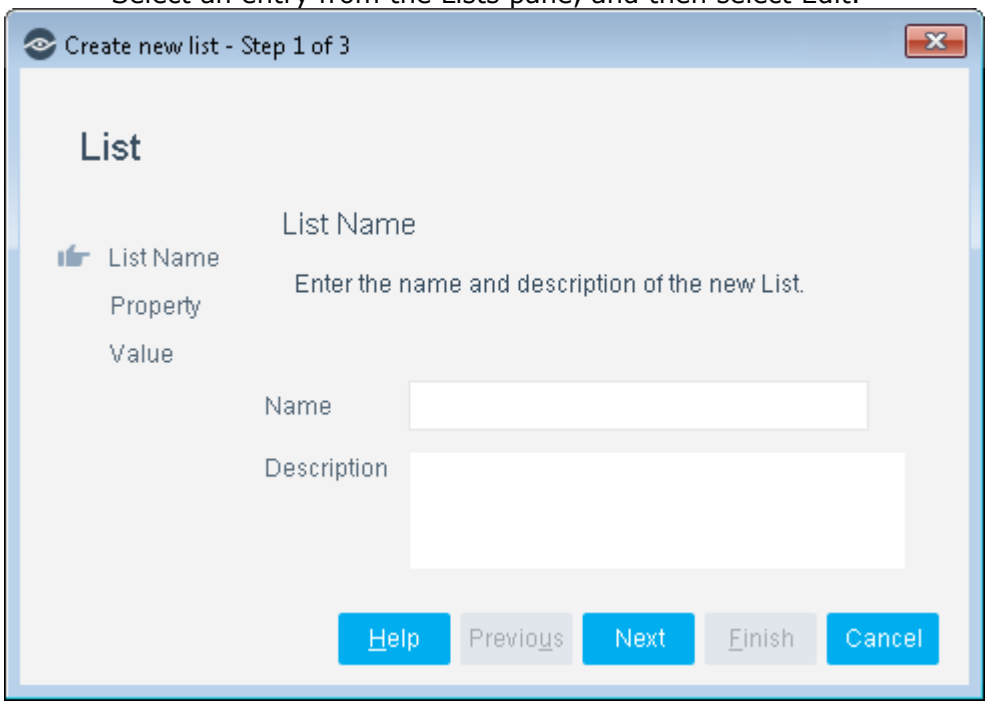
Use the List wizard to generate lists.

To work with lists:

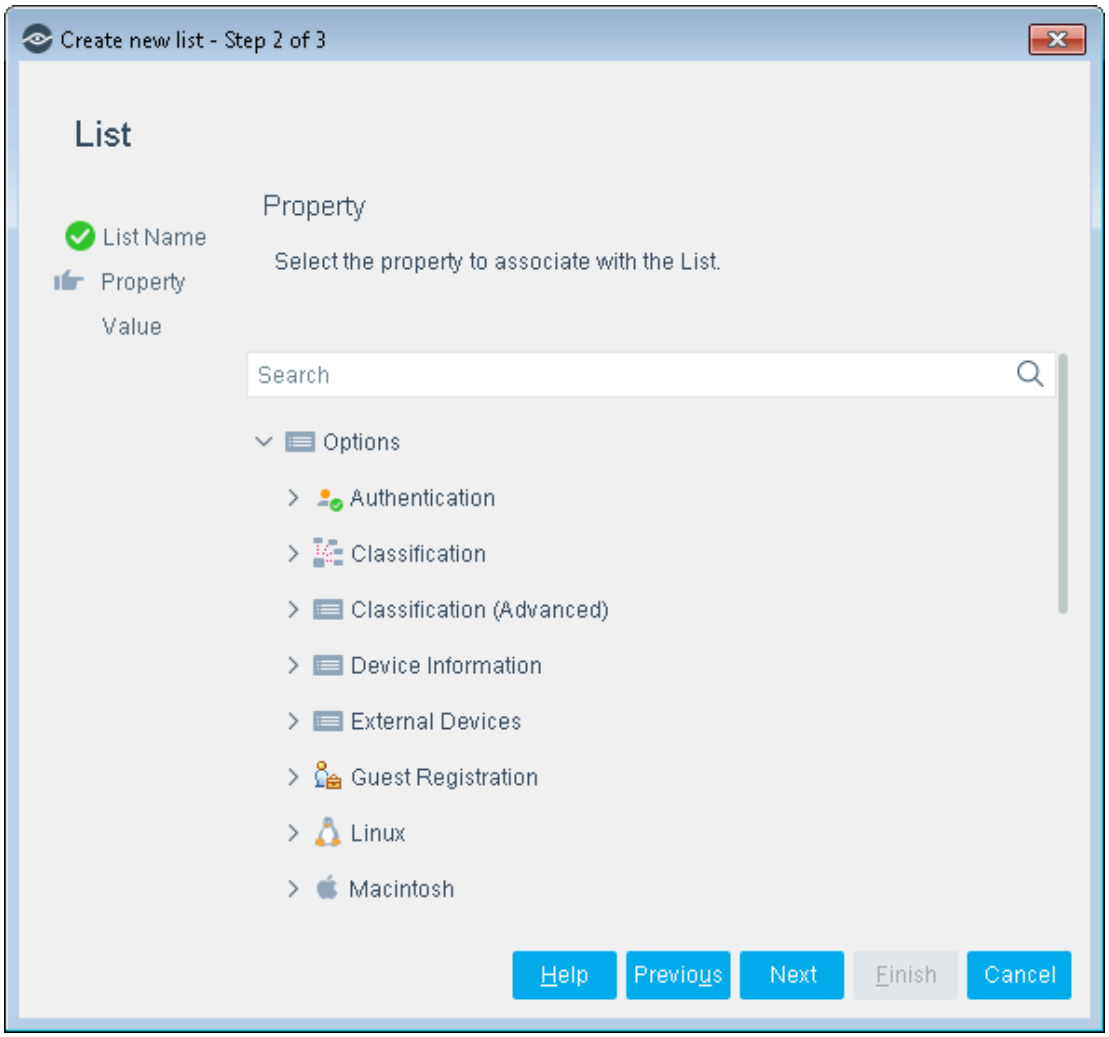
1. Select Tools > Options from the Console, and then select Lists.



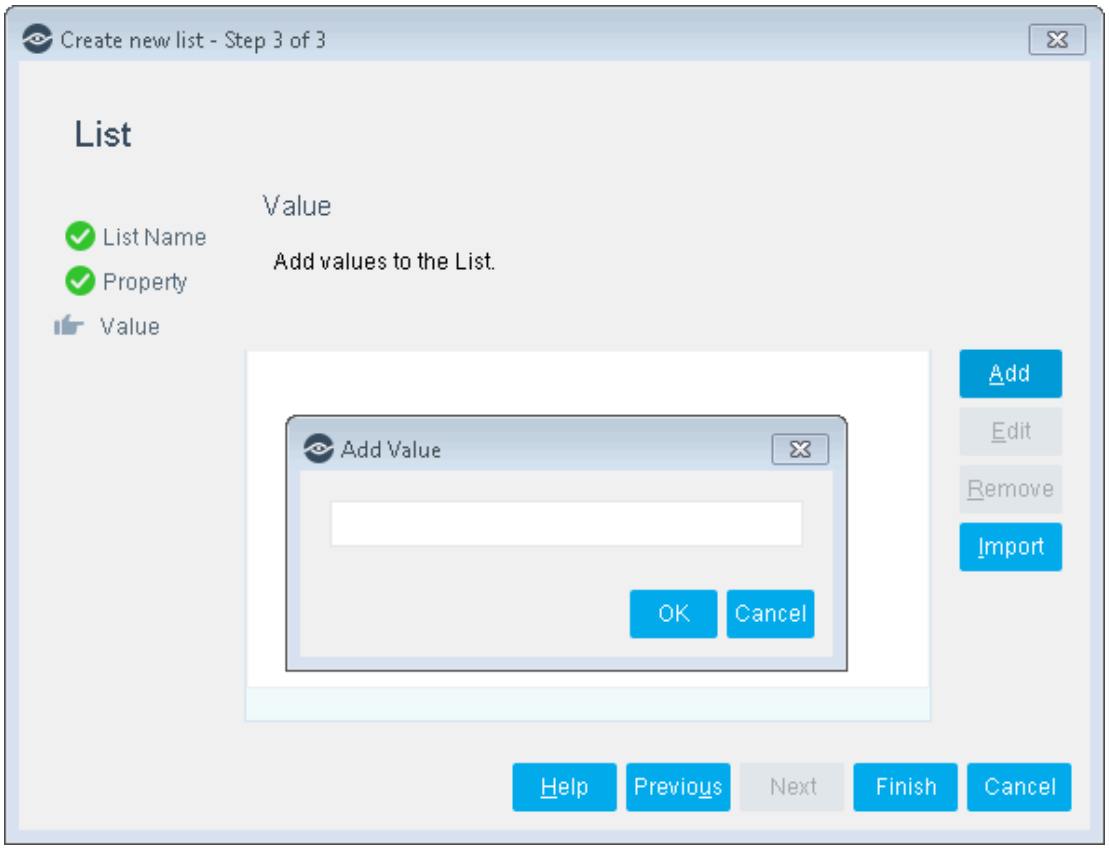
2. To delete a list, select it and select Remove. You cannot remove lists that are used in policies.
3. Do one of the following: The wizard opens in the List Name pane.
    - Select Add.
    - Select an entry from the Lists pane, and then select Edit.



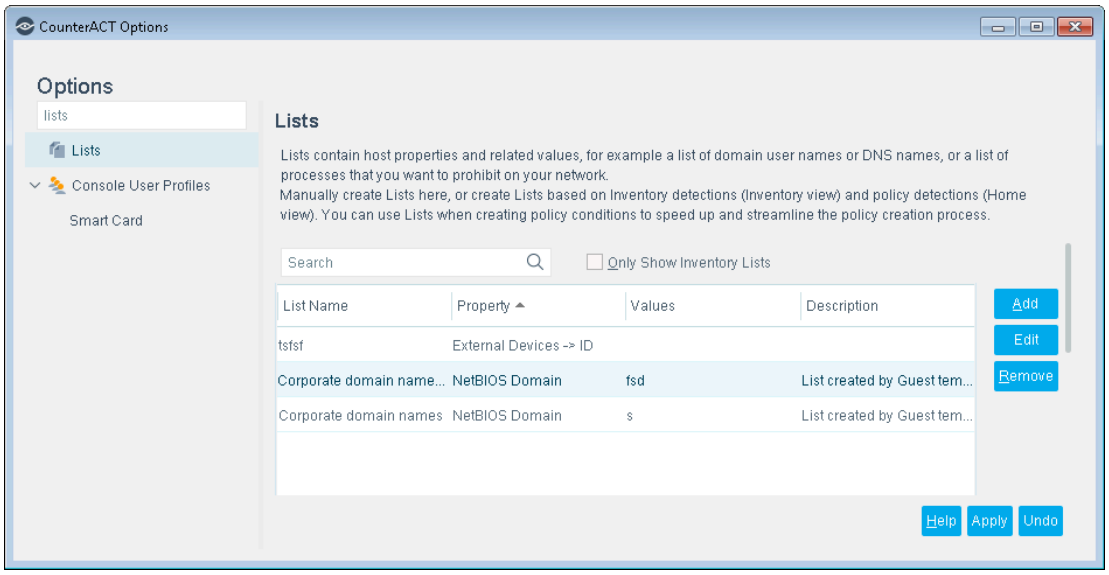
4. Enter a name for your list and add a description.
5. Select Next.



6. Select the property for which to make the list. See Working with Properties for information about the properties shown. You can use this option for any property that consists of free text and for the Device Information > Open Ports property. Other properties, for example, installed software, peer-to-peer applications or properties indicating endpoint manageability, cannot be included in lists.
7. Select Next.



8. Select Add, and then enter a value.
9. Add additional values as required.
10. Edit a value:
    - Select the value. The name is displayed in the free text field.
    - Edit the value. The new value is added to the list.
    - Delete the previous value.
11. Import values from external programs. Type one value per line. A value can contain spaces. Files should be imported in TXT format and must be UTF-8 encoded.
    - Select Import.
    - Navigate to your file and import.
12. Select Finish. Your value list is displayed in the Lists pane.



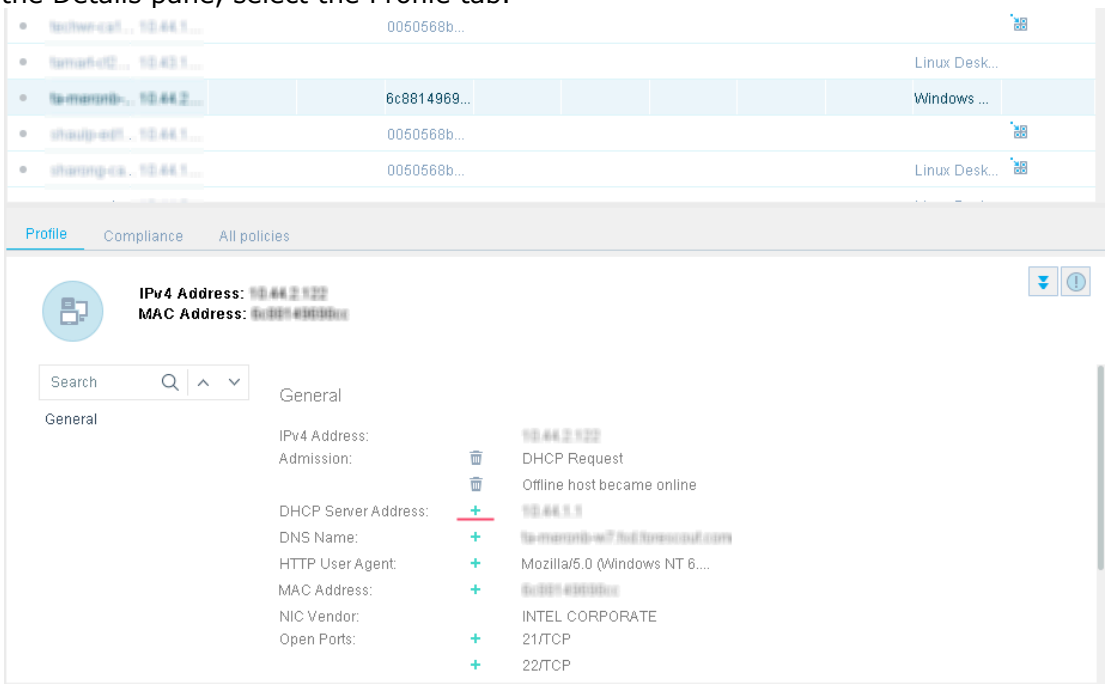
13. Select Apply, and then select Close. Lists you add here appear in the Asset Inventory view, if the list includes properties detected in the network.

Modify lists based on endpoint detections

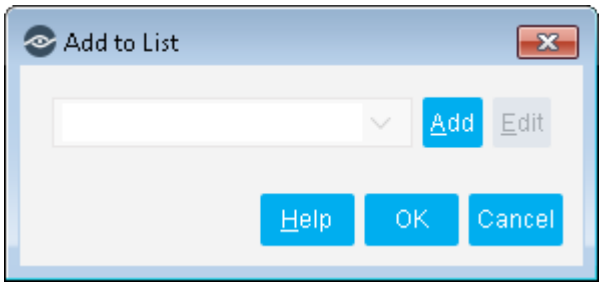
The Home view, Details pane provides information about endpoint properties detected by Forescout products. You can navigate to these properties and automatically assign them to lists or add them to new lists.

To create a list from endpoint detections:

1. Select an endpoint from the Home view, Detections pane.
2. In the Details pane, select the Profile tab.



3. Select ✚ next to the properties shown in the Details pane, Info tab.



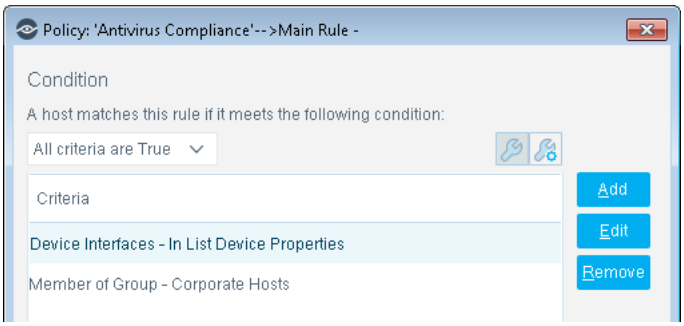
4. Select a list from the drop-down menu, or select Add to add the property to a new list.
5. Select O.c

Use your custom lists in policies

You can use property value Lists when defining policies. Using lists speeds up and streamlines the policy creation process, and minimizes mistakes that can be made when defining policy property values.

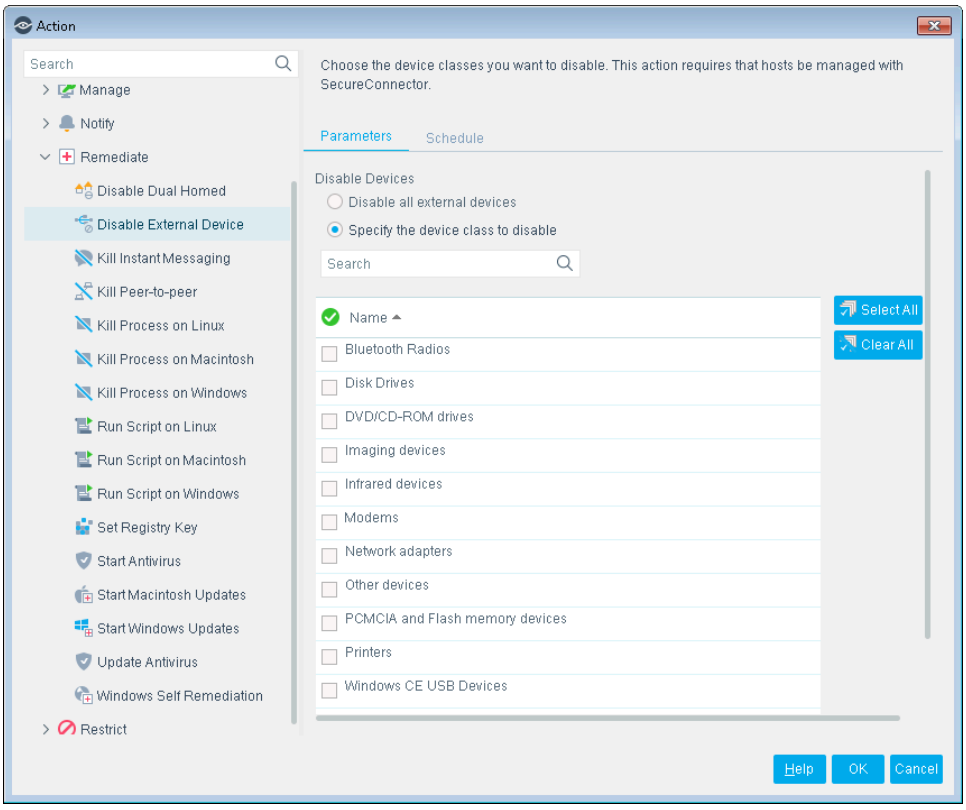
When you define condition criteria based on a property, use the In List matching expression, and specify the list. The list you specify must contain data of the type returned by this property.

You cannot remove lists from Console while they are used in policies.



Working with actions

Actions are measures taken at endpoints, ranging from notices, warnings and alerts to remediation, network and web access restrictions, and complete blocking.



In addition to the actions delivered with your Forescout system, other actions may become available when you install modules and eyeExtend modules. For example, if you are working with the Forescout Wireless Plugin or the Forescout eyeExtend for FireEye HX, actions delivered with these components are available. See Base Modules, Content Modules, and eyeExtend Modules for information about working with plugins and eyeExtend modules. Refer to the related plugin or eyeExtend module Configuration Guide for details about these actions.

Action tools

Enabling and disabling actions

You can create actions for all your policies, and enable and disable them as required. You may need to disable actions, for example, to test your policies and get a sense of network compliance before communicating with network users or taking actions on network devices. Actions can be enabled or disabled from:

- Home view, Detections pane.
- Home view, Views pane. See Stop and Start Policy Actions for details.
- A policy. See Enabling and Disabling Actions for details.

Action schedules

Action schedules can be assigned to each policy action. This lets you control when actions are carried out and for what duration. For example, you can create a policy that warns users not to run peer-to-peer applications and then blocks their Internet access if applications are detected after the warning period. See Action Schedules for details.

Property tags in actions

Property tags can be incorporated in email and HTTP actions. For example, the User Directory mail tag {ad_mail} can be added to an Action notification. This tag is translated to the actual email address of the user logged in to the detected machine. See Property Tags for details.

Action thresholds

Action thresholds automatically implement safeguards when rolling out blocking and restrictive actions.

Action thresholds are designed to automatically implement safeguards when rolling out such sanctions across your network. Consider a situation in which you defined multiple policies that utilize a blocking action, for example, the Virtual Firewall or Switch Block action. In a situation where an extensive number of endpoints match these policies, you may block more endpoints than you anticipated.

An action threshold is the maximum percentage of endpoints that can be controlled by a specific action type defined at a single Appliance. Working with thresholds gives you greater control over how many endpoints are simultaneously restricted in one way or another.

See Working with Action Thresholds for details.

Scripts and interactive actions

Several actions require that Forescout eyeControl run scripts on the endpoint. Refer to the HPS Inspection Engine Configuration Guide. for details about how scripts are run using Remote Inspection or SecureConnector. Select Tools > Options > Modules, select the plugin, and then select Help.

Typically, scripts are run in the background, but actions such as the HTTP Notification and HTTP Login actions initiate end user interaction. Forescout eyeControl can run interactive scripts on Macintosh endpoints running the following shell types:

- sh
- bash
- csh
- tcsh

Evaluate commands and scripts

Unlike other script actions, these properties and actions run scripts and commands on the CounterACT appliance itself, and not on endpoints. In addition, you can use the script result as a policy condition.

To specify a script or command for these properties and actions, do one of the following:

- Enter a script name or command directly in the Command or Script field. To include host properties in the command statement, select Add Tags to insert data tags that resolve to host property values.
- Select the Command or Script drop-down menu to view recently selected scripts and commands.
- Select the ellipsis icon ... to build a library of scripts for this action. Scripts that you add appear in the command or script drop-down menu.

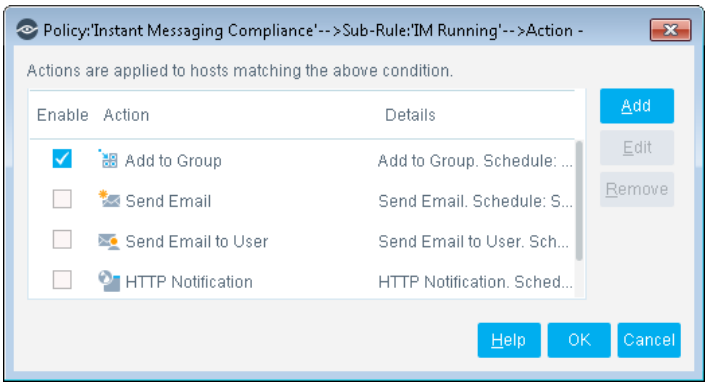
Accessing console actions

Actions can be incorporated into policies and carried out when certain conditions are met. For example, you can create a policy that detects users working with unauthorized instant messaging applications, and use a Forescout actions that kills those applications.

Alternatively, you can manually apply an action on selected endpoints.

Access actions:

- From the Home view, Detections pane.
- When creating and editing a policy. Right-click a policy Main Rule or Sub-Rule from the Policy Manager. Select Quick Edit, and then select Actions. The Policy Action dialog box opens.

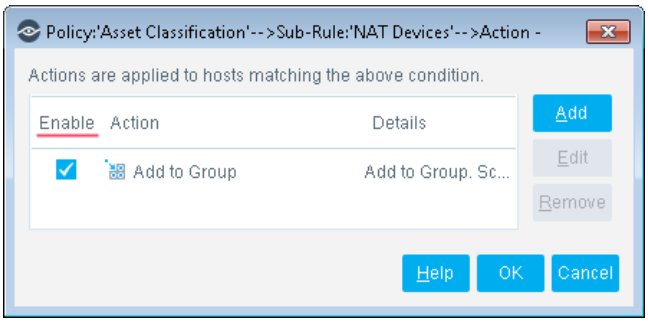


Enable and disable actions in policies

You can create actions for all your policies, and enable and disable them as required. You may need to disable actions, for example, to test your policies and get a sense of network compliance before communicating with network users or taking actions on network devices.

Policies can be enabled or disabled from the:

- Policy wizard: open the policy and edit a rule. Select or clear the checkbox beside the action in the Actions section.
- Home view, Detections pane.
- Home view, Views pane. See Stop and Start Policy Actions for details.



Audit actions

Send message to Syslog action

The Send Message to Syslog action is included by default as an Audit action.

The Send Message to Syslog action is used by the Syslog Plugin to send a message to the Syslog server. This message overrides Syslog Plugin configuration options.

The action exposes the following settings:

Message to Syslog	The message to send to the Syslog server when the policy is triggered.
	Message Identity Free-text field for identifying the Syslog message.
Syslog Server Address	Syslog server IP address.
	Syslog Server Port Syslog UDP port number (default value is 514).
Syslog Facility	Syslog messages facility (default value is local4).
Syslog Priority	Syslog messages priority (default value is info).
Use TLS	Instruct Forescout eyeSight to use TLS to encrypt communication with the Syslog server when the TCP protocol is used (selected in Syslog Server Protocol). Ensure that TLS communication is supported and enabled on the Syslog server.
Soft-fail OCSP requests	When TLS is used, Forescout eyeSight sends an Online Certificate Status Protocol (OCSP) request for the certificate revocation status to check that the Syslog server certificate has not been revoked.

If eyeSight could not receive a response from the OCSP Responder, the certificate is considered valid. By default, hard-fail is applied.

If you specify any of the options for the action, Add Tags is enabled. You can add property tags to the message. The tag is translated to the current information associated with the tag. See Property Tags for details.

Authenticate actions

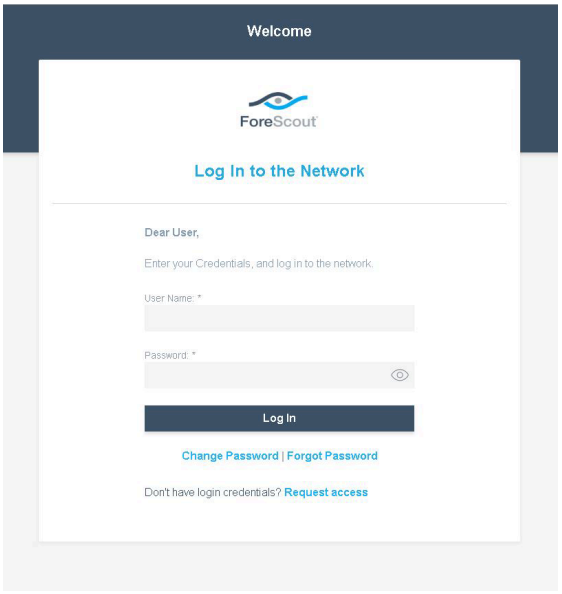
This topic describes actions that control the access of corporate and guest users to a corporate network. These actions are provided by the User Directory Plugin.

- User Directory Management
- Corporate and Guest Management

HTTP login

Use the HTTP Login action to:

- Prompt endpoint users to authenticate or self-register before accessing your network. Users attempting to access the network access the Login pane and must enter valid credentials.

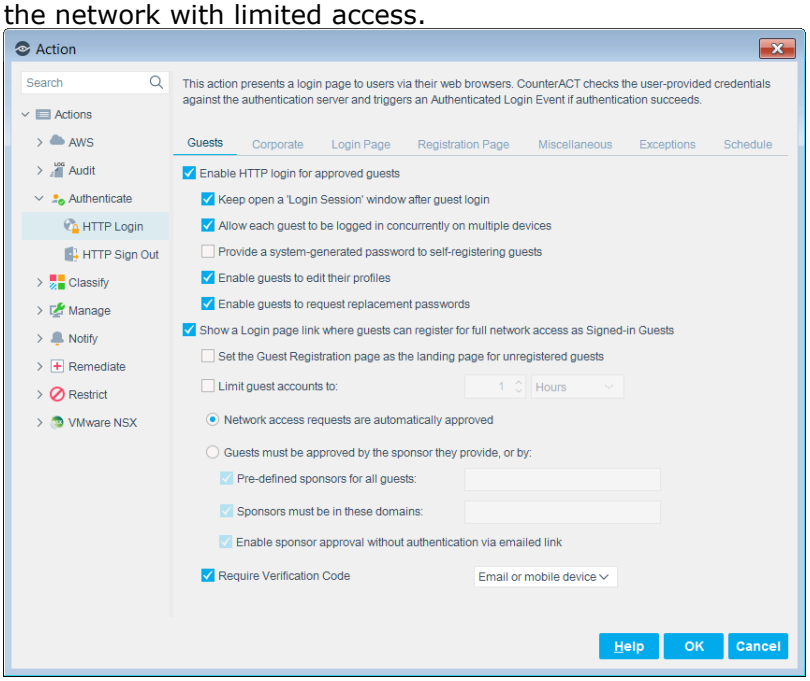


  The action can be configured to handle guest and corporate users. For details, see Handling Guests and Handling Corporate Users.

  Configurable HTTP Login action options let you:

- Define the servers against which the user will authenticate.
- Enable and define a registration process by which unauthorized users can request network access via a web registration form. You may want to enable this if your organization allows visitors to access the network.
- Define login requirements so that users can skip authentication and registration, and enter

the network with limited access.



This action can be used with other policy actions. For example, you can define a policy quarantining all unauthenticated users to an isolated VLAN. If the user logs in properly, the policy's actions are canceled, removing all limitations imposed. In this example, the user is removed from the isolated VLAN and can join the network and browse.

Note:
Web messages and emails used in this action can be changed and localized. See Localize Redirected Web Pages and Messages for details.

Note:
Login failures can be easily tracked. See HTTP Login Attempts for details.

Note:
You can customize the text that the HTTP Login action displays at the user's endpoint. See Customize HTTP Login Action Text for details.

Note:
HTTP Login is disabled whenever HTTP Redirection is disabled. See Disable Web Portals for details.

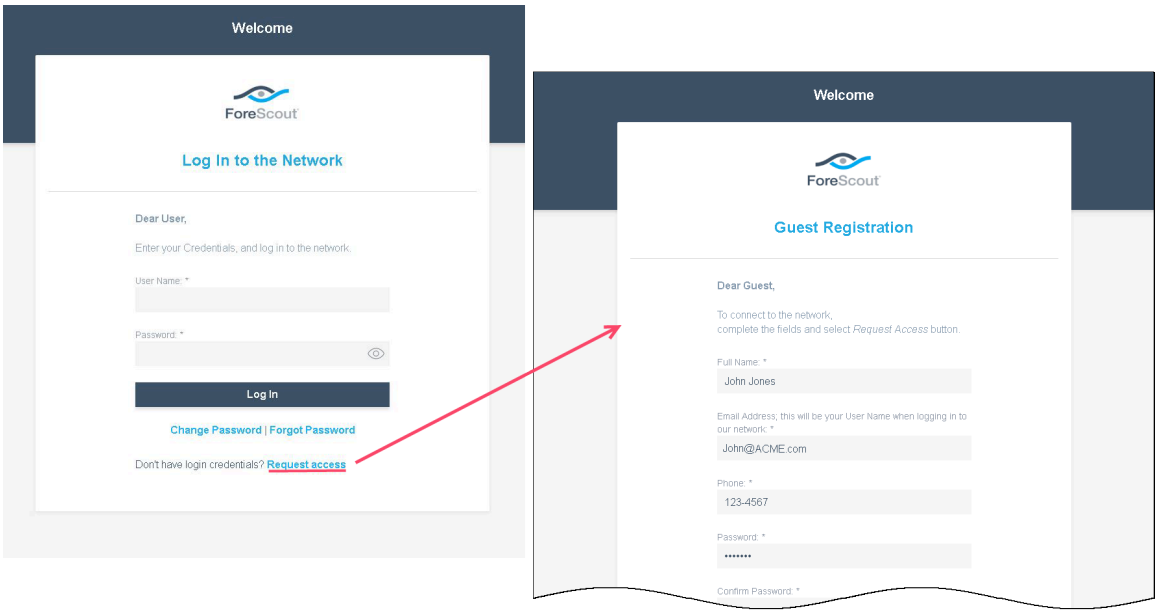
Depending on the endpoint operating system and how the endpoint is managed, this action is implemented by the HPS Inspection Engine, the Linux Plugin, or the OS X Plugin.

Handling Guests

This section describes how to work with the HTTP Login action when handling network guests. For example, you can create policies that deal with visiting professionals or contractors.

Guests are authenticated against the Appliance.

You can define the action so users who do not have authentication credentials can register as guests using a Guest Registration form that is displayed in the user's web browser. In the Login page, guests select Request access to open a Guest Registration page.



Configure the HTTP Login action for guest login on the following tabs:

- Guests Tab: Defines how authentication and registration is performed.
- Registration Page Tab: Defines which information guests must provide in the Guest Registration form.
- Login Page Tab: Defines the text that appears on the Login page.
- Miscellaneous Tab: Defines additional configuration options, such as encryption and compliance.

Handling Corporate Users

Use the Corporate options to enable corporate authentication.

To configure the action for corporate users, use the following tabs:

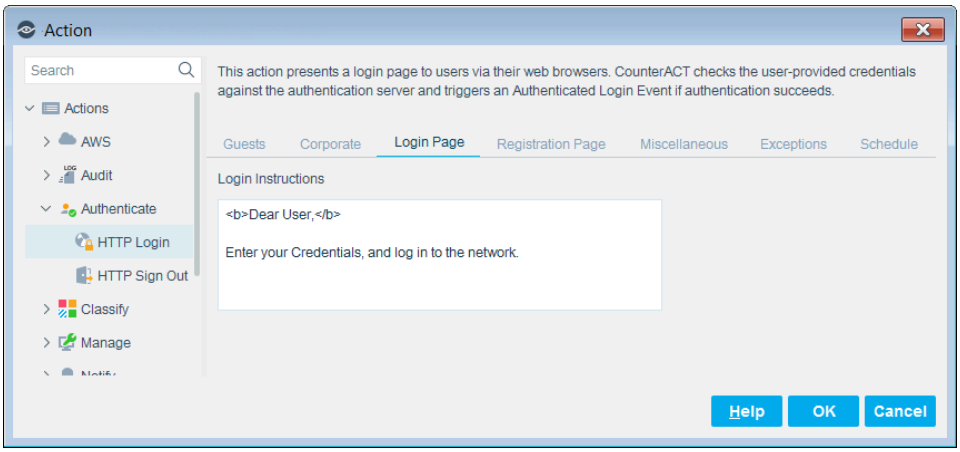
- Corporate Tab: Defines which servers are used for authentication.
- Login Page Tab: Specifies the text that is to appear on the Login page.
- Miscellaneous Tab: Specifies addition configuration options such as encryption and compliance.

Login page tab

The Login Page tab is used to define the content of the Login page that is displayed to both guest and corporate users.

After the user successfully logs in, the Authentication, Signed In Status property is resolved as either Signed In as a Guest, if the user's status is network guest, or Signed In as a Domain User, if the user's status is corporate user.

The User Name entered is used when resolving the Device Information > User Name property. If necessary, you can instruct Forescout eyeControl to use the machine name instead of this name or to use this name when the machine name is not available. Refer to the HPS Inspection Engine Configuration Guide for details.



The following options are available on the Login Page tab:

Login Instructions	Define the Login page message that is presented to both guests and corporate users.

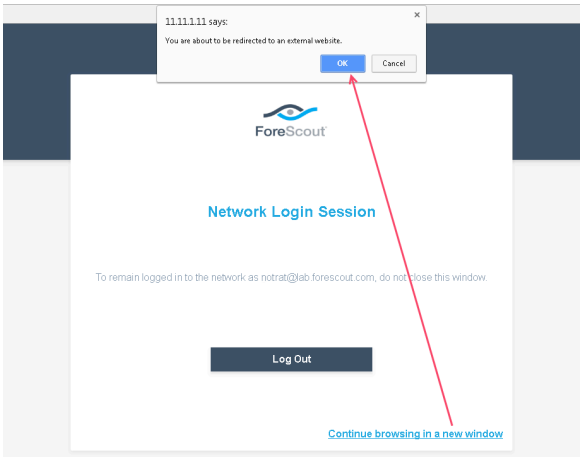
Guests tab

Use the HTTP Login - Guests tab to define guest login session options, as well as a registration strategy.

Guest login session options

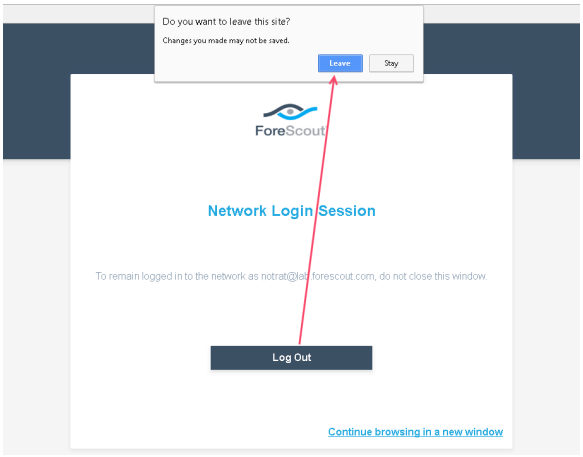
These options let you control the guest login experience.

Enable HTTP login for approved guests	Select this option to enable login for approved guests. Authentication is validated against a Forescout server database after the guest is approved.
Keep open a 'Login Session' window after guest login	Select this option to display a Forescout Login Session window for guests. To browse as a registered guest, the user selects Continue browsing in a new window, and then OK.

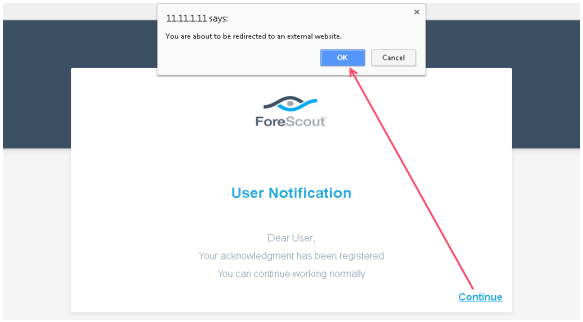


The user must keep the Login Session window open to maintain a network to Internet connection, provided this access was granted in the policy. During this time, the Authentication, Signed In Status property for the endpoint is resolved as Signed In as a Guest.

To leave the network, the user selects Log Out, and then Leave:



If the Keep open a 'Login Session' window after guest login option is not selected, the Forescout Login Session window is not displayed. Instead, a User Notification window is displayed. To browse as a registered guest, the user selects Continue and then OK. The Authentication, Signed In Status property for the endpoint is resolved as Not Signed In.



Allow each guest to be logged in concurrently on multiple endpoints	You can control the number of devices a single guest can log in to concurrently. Select this option to allow multiple logins. If this option is not selected, a second login by the same user closes the first session on the original computer.
Provide a system-generated password to self-registering guests	Select this option to generate a password for the guest to use to log in. This option is relevant only when a guest registers for network access using a Guest Registration form. When this option is selected: Guests are not prompted to define their own passwords in the Guest Registration form. When the guest is approved, a password is generated for the guest to use in the Password field of the Login page. A system-generated password is provided in an email that is sent to the guest. System-generated passwords adhere to the password policy rules that are defined in the Guest Registration pane's Password Policy tab.
Enable guests to edit their profiles	Select this option to display the Edit Profile link on the Login page that is presented to guest users. Selecting this link displays the Edit Profile page, where guests can edit information that they initially provided when registering using the Guest Registration form.
Enable guests to request replacement	Select this option to display the Forgot Password link in the Login page for guest users. Selecting this link displays the Forgot Password page, where approved guests can request a new password for login.

passwords

Guest registration options

The following guest registration options are available:

Show a Login page link where guests can register for full network access as Signed-in Guests	Enables not-yet-approved guests to self-register. If all guests must be pre-approved for network access, clear this checkbox. For details, see Enable Guest Registration.	
	Set the Guest Registration page as the landing page for unregistered guests	Prompts the unregistered guest to complete the Guest Registration form. For details, see Enable Guest Registration.
Limit guest accounts to	To set a maximum time for guests to request network access, select Limit guest accounts to and enter a time limit. When unspecified, the maximum network access approval period defaults to 8 hours. In the Guest Management Portal, sponsors can set a specific limit to the network access of their self-registering guests. When the time period elapses, the guest account expires, and the guest is required to register again.	
Network access requests are automatically approved	Allows guests to be automatically approved after submitting a Guest Registration form. For details, see Allow Automatic Approval of Registered Guests.	
	Guests must be approved by the sponsor they provide or by	Requires that guests be explicitly approved by an individual in your organization. This can be a named corporate sponsor or predefined sponsors can be used for all guests. If you select this option, select one or more of the following: • Pre-defined sponsors for all guests • Sponsors must be in these domains • Enable sponsor approval without authentication via email For details, see Sponsor Approval of Guests.
Require Verification Code	If selected, eyeSight eyeControl sends a one-time verification code to the guest email address or mobile phone number entered in the registration form, and then requires the guest to enter the code before logging in. For details, see Work with Verification Codes.	

Allow only pre-approved guests

If all guests must be pre-approved for network access, clear the Show a Login page link where guests can register for full network access as Signed-in Guests check box. Information about pre-approved guests is saved on the Appliance. When pre-approved guests log in to your network, their credentials are checked against this information. Pre-approved guests can be added by:

- A sponsor in the Guest Management Portal.
- A Forescout operator in the Guest Management Pane. It is the responsibility of your organization to forward login credentials to these pre-approved guests. The eyeSight does not do this.

Allow Automatic Approval of Registered Guests

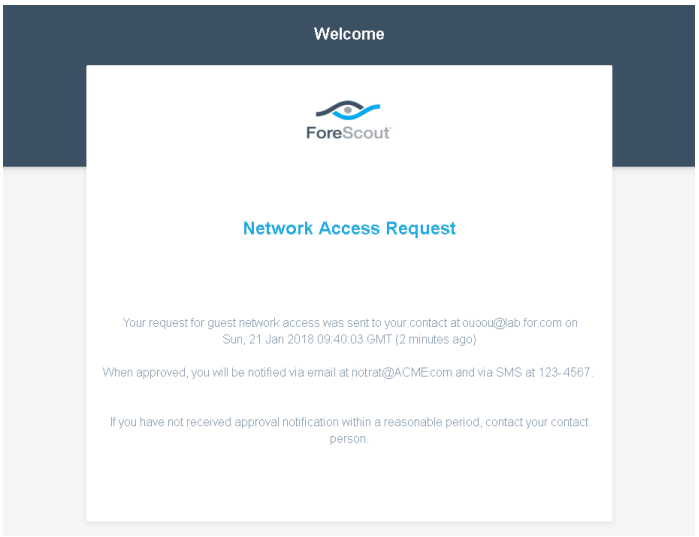
For guests to be automatically approved after submitting a Guest Registration form, select the Network access requests are automatically approved option. You may want to do this if you anticipate many guests and do not have the resources to accept or reject each one, but do want to keep track of who is registered. Approved guests are displayed in the following locations:

- In the Guest Management Portal where sponsors can view the registered guests that specified them as their corporate contact.
- In the Guest Management Pane, select Options from the Tools menu and then navigate to and select Guest Registration to display the Registered Guests tab and view the registered guest entries.

Sponsor Approval of Guests

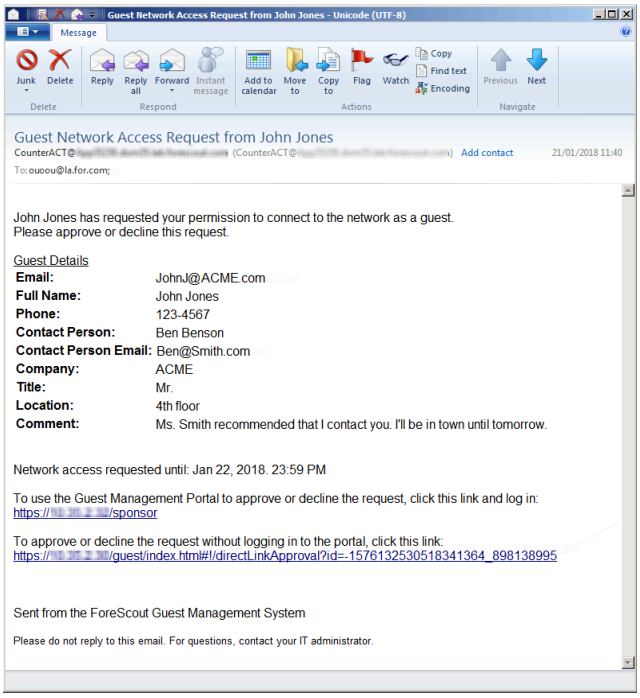
If you require that guests be explicitly approved by an individual in your organization – a corporate *sponsor* – select the Guests must be approved by the sponsor... option. The sponsor specified by the guest on the Guest Registration form receives a notification email that includes a link to the corporate Guest Management Portal. After logging in to the portal, sponsors can approve or decline network access to guests awaiting approval.

Before sponsor approval is completed, a notification page indicates that a network access request has been sent to the contact. The guest receives an email notification once access is approved.

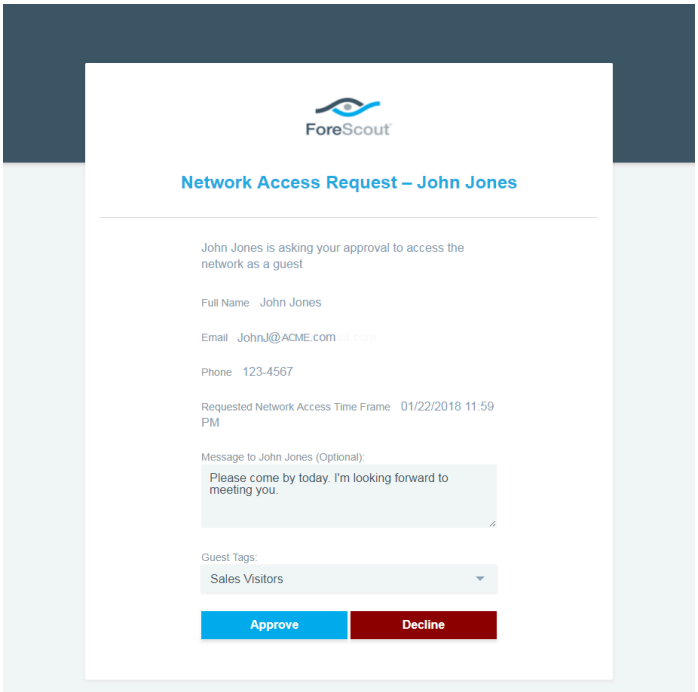


Enable Sponsor Approval without Authentication via Emailed link

The guest registration request notification email that is sent to sponsors always includes a link to the corporate Guest Management Portal. Select Enable Sponsor Approval without Authentication via Emailed link to include an additional link in the notification email to a Network Access Request page containing the specific guest registration request.



- The first link opens the Login page of the Guest Management Portal, where a sponsor can log in and administer all their guest registration requests.
- If the Forescout user selected the Enable sponsor approval without authentication via emailed link option in the Guests tab of the HTTP Login action, then a second link is included. This link opens a Network Access Request page, where the sponsor can approve or decline the network access request of the specific guest.



This option is useful if:

- You do not want to require sponsors to log in to the Guest Management Portal to approve guest registration requests.
- Sponsors are temporarily unable to access the Guest Management Portal.
- Your organization does not employ an Active Directory server to verify the credentials of its personnel. (Logging in to the Guest Management Portal requires Active Directory verification of user domain credentials).

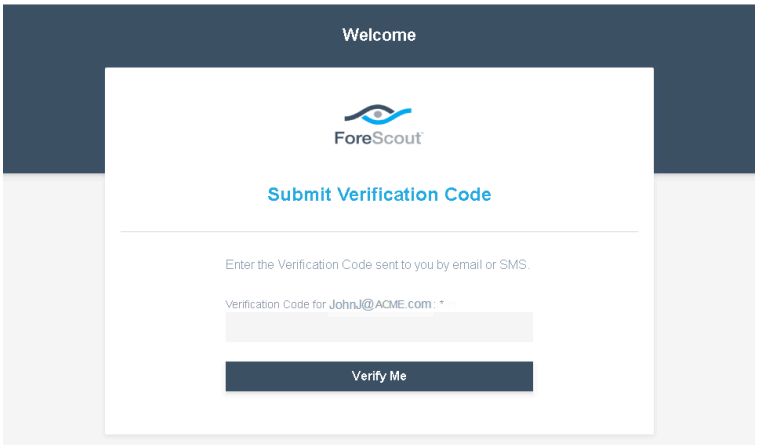
Use of this option maintains backward compatibility with HTTP Login action functionality of previous versions.

Note:
If Enable sponsor approval without authentication via emailed link is selected, it is recommended to select Sponsors must be in these domains to ensure that only corporate employees receive the emailed link.

Pre-defined sponsors for all guests	Select this option to provide a comma-separated list of emails of corporate sponsors. In addition to the primary sponsor named by each guest in the Contact Person and the Contact Person Email fields of the Guest Registration form, these sponsors will also receive guest registration notifications.

Work with Verification Codes

Verification codes are used when working with the HTTP Login action that requires guests to register before the Guest Registration request is processed. Use this feature to verify that the email address or phone number entered by the guest in the registration form is valid. eyeSight eyeControl sends a one-time verification code to the guest email address or mobile phone number that they entered in their registration form, and then requires the guest to enter the code before logging in.



Verification codes are automatically generated and validated by eyeSight eyeControl.

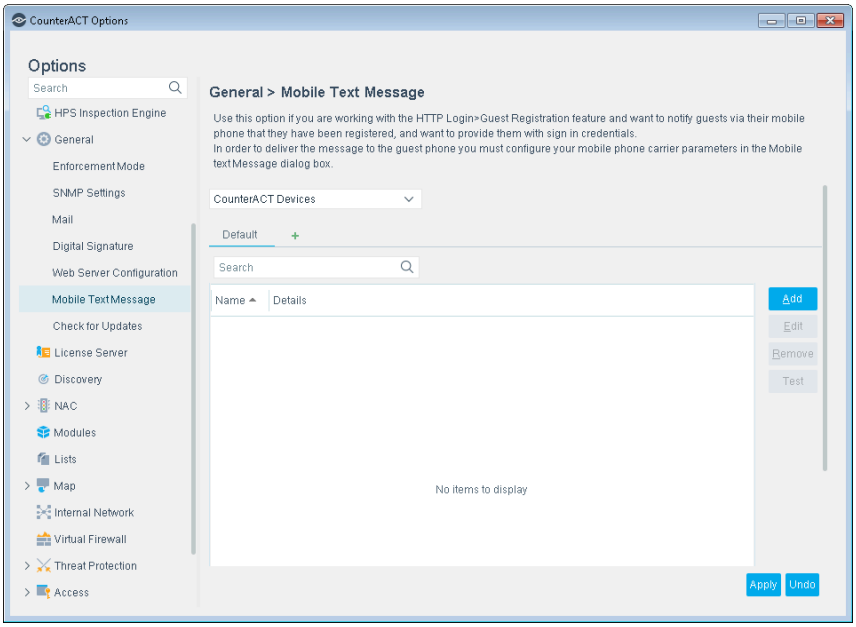
To work with verification codes:

1. Select Require Verification Code on the Guests tab.
2. From the drop-down menu, select whether the verification code is to be sent via email only, via mobile phone only, or via both email and mobile phone. The email message includes a customized message. The mobile text message includes only the verification code.

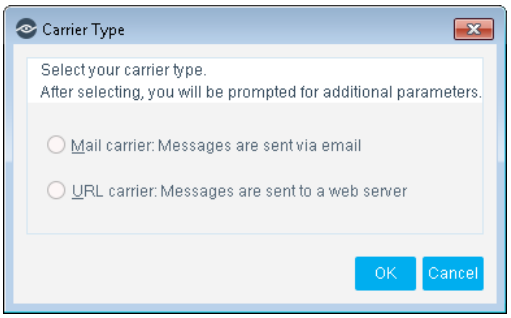
To send a verification code to a mobile device, you must define how the message is submitted to the mobile carrier.

To define text messaging through a mobile carrier:

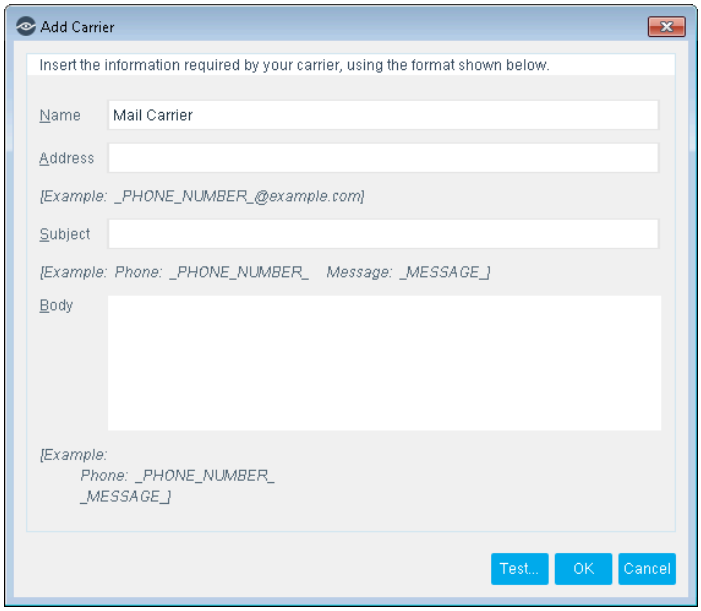
1. Select Tools > Options from the Console menu, and then select General > Mobile Text Message.



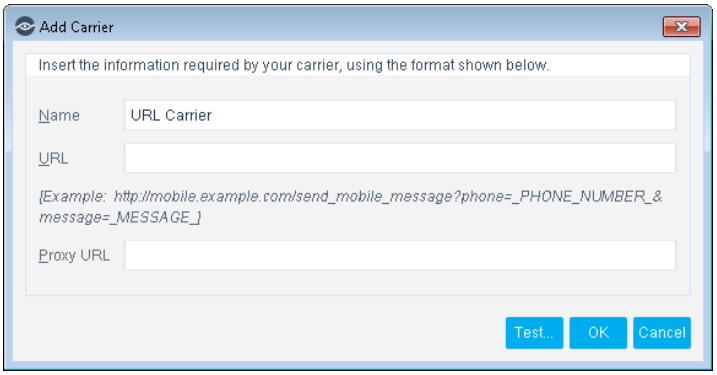
1. Select Add.



1. Select Mail Carrier to send text message requests to a carrier in email format or select URL Carrier to send text message requests to a carrier in a URL string.
2. Select OK.
3. In the Add Carrier dialog box, enter a name that identifies this carrier in the Name field. In the other fields of the dialog box, enter string patterns that define the format used to submit message requests.
    - For message requests in email format, the fields correspond to the Address, Subject, and Message fields of an email message.



- For message requests in URL format, a single URL field is used to submit the message request. In addition, an optional Proxy URL field lets you specify an alternative URL.



In these fields, use the following parameters as placeholders for values that are inserted into the request:

- _PHONE_NUMBER_ is the target phone number for the text message. For example, for guest registration this is the phone number submitted by the guest.
- _MESSAGE_ is message text inserted in the request. For example, for guest registration this is the registration code.

1. Select Test to send a sample message request using the defined format. Enter values for the _PHONE_NUMBER_ and _MESSAGE_ parameters, and select OK to submit the message request. Confirm receipt of the test message on the target mobile device.
2. In the Add Carrier dialog box, select OK. The carrier is added to the list in the Mobile Text Message pane.

Viewing Registered Guests

Approved guests can be viewed in the Guest Management Portal and in the Guest Management Pane.

Working with Guest Tags

Use guest tags to categorize guests into groups, for example, Limited Access guests and Full Access guests or Building A guests and Building B guests.

You can create policies that evaluate guests for their guest tag assignments. For example, create a policy that detects Building A-tagged guests and assigns them to a specific VLAN or allows them minimum network access.

See Managing Guest Tags for details.

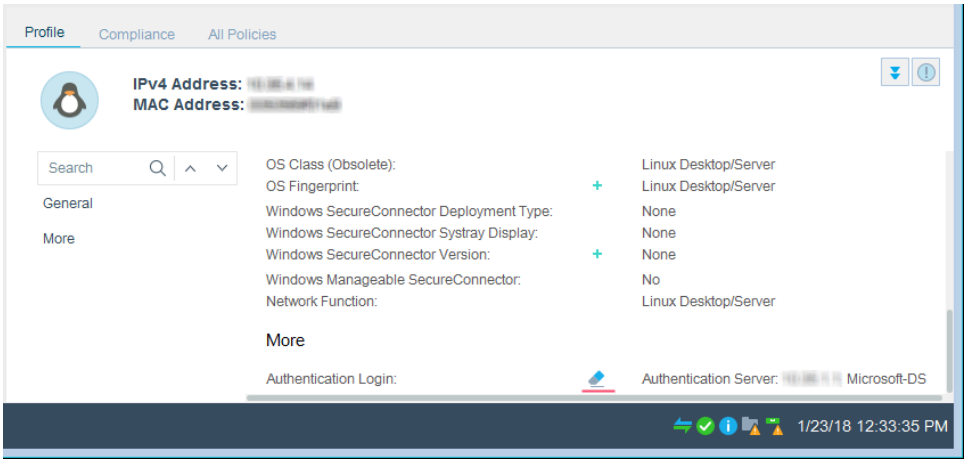
HTTP sign out

The HTTP Sign Out action signs out detected endpoints that meet the following criteria:

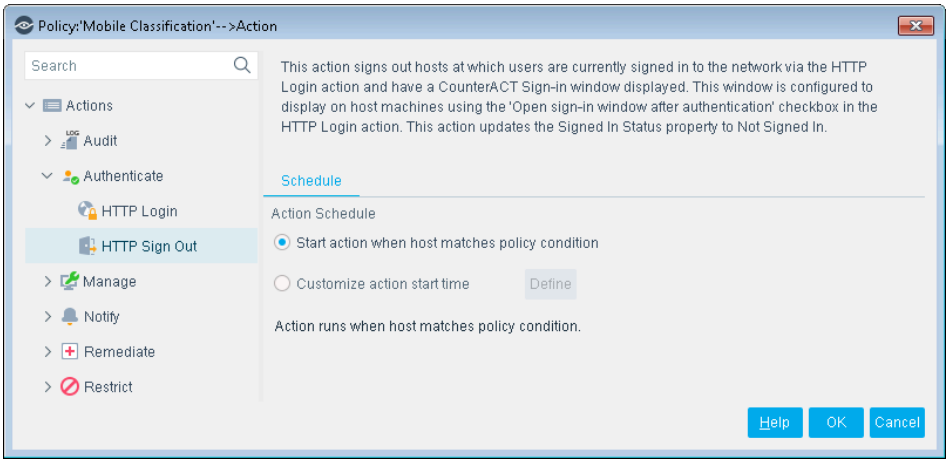
- The endpoint user is currently signed in to the network via the HTTP Login action.
- The endpoint displays a Forescout Login Session window.
- The Signed In Status condition is tested to resolve the endpoint's login status.

Note:

Corporate/Guest Control policies created using the template provided in eyeSight version 8.0 and above do not test the Signed In Status condition. If the HTTP Sign Out action is run, it has no effect on the endpoint's HTTP Login status. To sign out these endpoints, go to the endpoint's Profile tab, and select the eraser icon before the Authentication Login property.



Use the action, for example, in a policy that requires users to re-authenticate following a specific event, such as a Link Down Trap (Trap Received property).



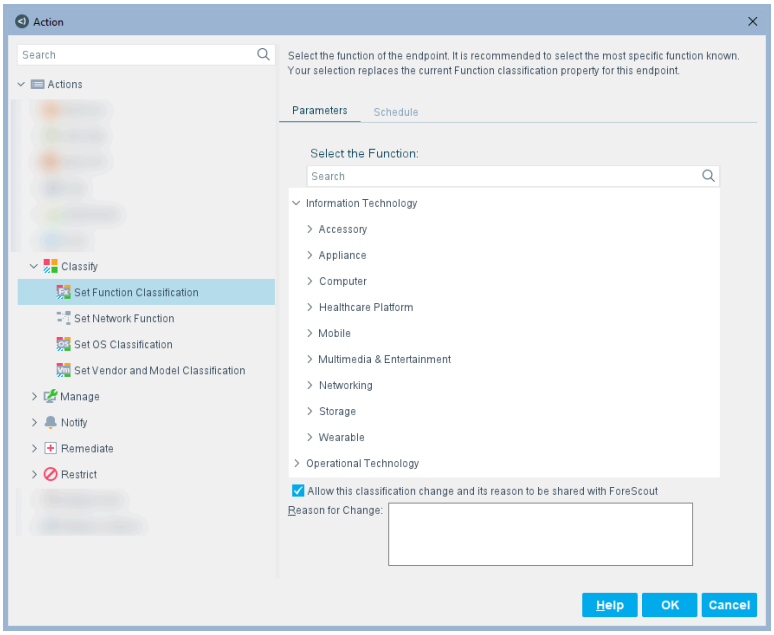
The HTTP Sign Out action updates the Authentication, Signed In Status property of the detected endpoint to Not Signed In.

Depending on the endpoint operating system, and how the endpoint is managed, this action can be implemented by the HPS Inspection Engine, the Linux Plugin, or the OS X Plugin.

Classify actions

Set function classification

The Set Function Classification action lets you override a Function property value set by eyeSight eyeSight.



This is useful in the following situations:

- The classification resolved by eyeSight eyeSight is not correct or eyeSight eyeSight was not able to classify the endpoint based on its function.
- You are able to refine the device's classification. For example, eyeSight classified the device function as Healthcare, but you know it is actually an X-Ray device.
- The endpoint was excluded from the range of endpoints to be classified due to its sensitivity to probing.

If the Primary Classification template was deployed with the Add to Group actions enabled, the classified device is added to the related classification group. See Primary Classification Template for details.

If you agree to provide the Forescout Research Program with information about the change, select the checkbox, and enter:

- The reason why the selected classification is appropriate for this endpoint
- The ideal classification for this endpoint, if it is not in the classification list

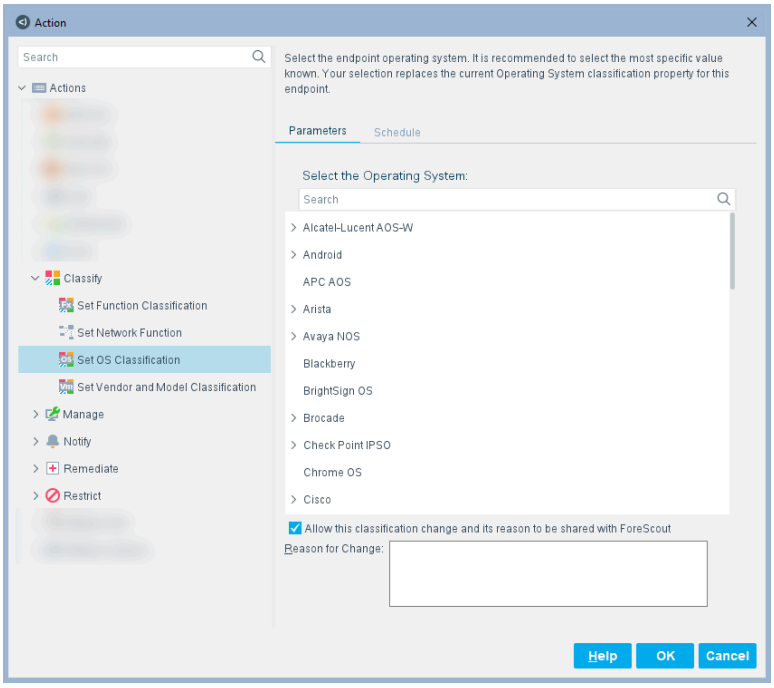
Your feedback is sent to Forescout to help provide better classification services.

Note:
Your changes are shared with The Forescout Research Program if you did not opt out of the program.

You can easily reset a manual classification assignment to that set by the Device Classification Engine by selecting Revert to Suggested Function Classification from the Cancel Actions drop-down.

Set OS classification

This action lets you override an Operating System property value set by eyeSight eyeSight.



This is useful in the following situations:

- The classification resolved by eyeSight eyeSight is not correct or eyeSight eyeSight was not able to classify the endpoint based on its operating system.
- You are able to refine the device's classification. For example, eyeSight eyeSight classified the operating system as Macintosh, but you know it is actually macOS 10.12 - Sierra.
- The endpoint was excluded from the range of endpoints to be classified due to its sensitivity to probing.

If the Primary Classification template was deployed with the Add to Group actions enabled, the classified device is added to the related classification group. See Primary Classification Template for details.

If you agree to provide the Forescout Research Program with information about the change, select the checkbox, and enter

- The reason why the selected classification is appropriate for this endpoint
- The ideal classification for this endpoint, if it is not in the classification list

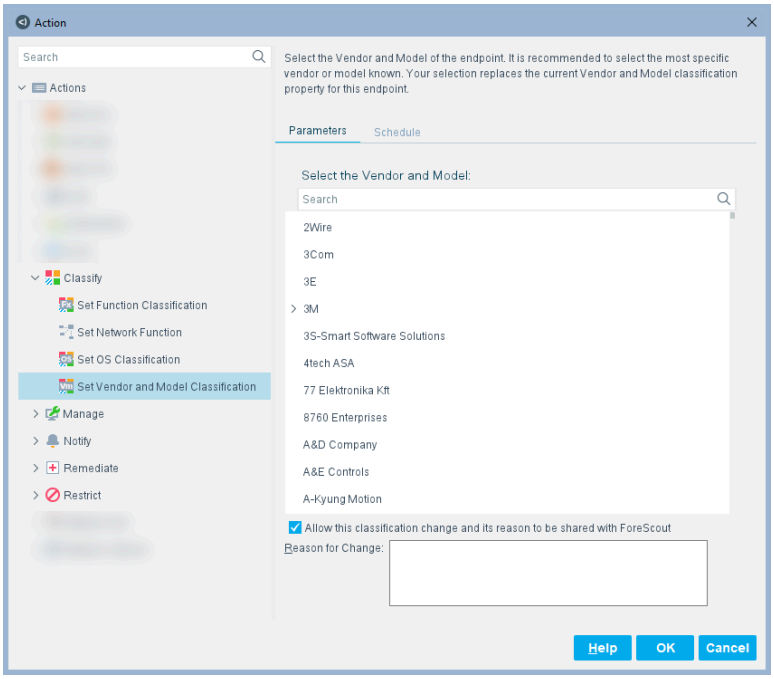
Your feedback is sent to Forescout to help provide better classification services.

Note:
Your changes are shared with The Forescout Research Program if you did not opt out of the program.

You can easily reset a manual classification assignment to that set by the Device Classification Engine by selecting Revert to Suggested Operating System Classification from the Cancel Actions drop-down menu.

Set vendor and model classification

This action lets you override a Vendor and Model property value set by eyeSight eyeSight.



This is useful in the following situations:

- The classification resolved by eyeSight eyeSight is not correct or eyeSight eyeSight was not able to classify the endpoint based on its vendor and model.
- You are able to refine the device's classification. For example, eyeSight eyeSight classified the vendor and model for the host as Apple, but you know it is actually Apple TV.
- The endpoint was excluded from the range of endpoints to be classified due to its sensitivity to probing.

If the Primary Classification template was deployed with the Add to Group actions enabled, the classified device is added to the related classification group. See Primary Classification Template for details.

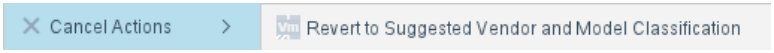
If you agree to provide the Forescout Research Program with information about the change, select the checkbox, and enter:

- The reason why the selected classification is appropriate for this endpoint
- The ideal classification for this endpoint, if it is not in the classification list

Your feedback is sent to Forescout to help provide better classification services.

Note:
Your changes are shared with The Forescout Research Program if you did not opt out of the program.

You can easily reset a manual classification assignment to that set by the Device Classification Engine by selecting Revert to Suggested Vendor and Model Classification from the Cancel Actions drop-down menu.

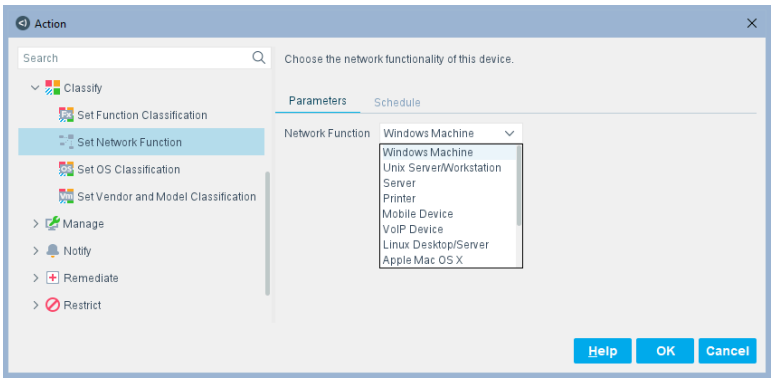


Set network function

This action lets you manually set a Network Function property value. This property is relevant only in environments running a legacy Asset Classification policy.

Note:
Primary Classification policies do not use the Network Function property.

After a device is classified using its Network Function property value, it is added to the related Asset Classification group, provided that the Asset Classification policy template was deployed.



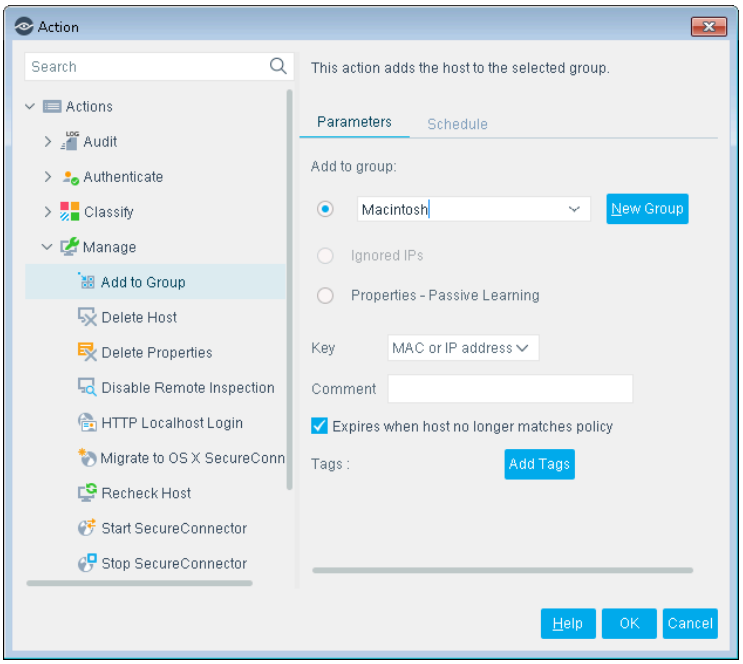
You can easily reset a manual classification assignment to that set by the Device Classification Engine by selecting Cancel Manual Network Function Classification from the Cancel Actions drop-down menu.

Manage actions

This section describes actions that manage endpoints.

Add to group

A group is a collection of IP addresses that has something in common. For example, a group may contain endpoints that are printers. Use the Add to Group action to place endpoints that match a policy condition into a group.



Specify the group to which endpoints are added:

- To add endpoints to an existing group, select the first option and do one of the following:
  - Type the group name in the search field to locate it in the group tree.
  - Drop-down the group tree and navigate to the group.
- To create a new group and add the endpoint to it, select New Group. Specify a Name and Description, and indicate the new group's location in the tree.
- Select Ignored IPs to add endpoints to the Ignored IPs group; endpoints in this group are ignored by NAC and Discovery policies. See Creating an Ignored IP Address List.
- Select Properties - Passive Learning to add endpoints to the Properties - Passive Learning group; Forescout eyeSight never contacts endpoints in this group to resolve properties, even for policy evaluation. See Restricting Endpoint Inspection for details.

Specify additional action options

- Select Expires when host no longer matches policy if you want the endpoint to be removed from the group when it no longer matches the policy condition. When this option is cleared, you must manually remove endpoints from the group using Groups Manager. See Working with Forescout Groups.

  Note:

  When the action adds endpoints to the *Ignored IPs* group, policies ignore members of this group, and Expires when host no longer matches policy is unavailable. When the action adds endpoints to the *Properties-Passive Learning* group, policies are evaluated for the endpoint based on passively learned information or third-party data sources.
- Specify the Key, the value by which each endpoint is associated with the group. Forescout eyeSight detects group association based on this value.

  Note:

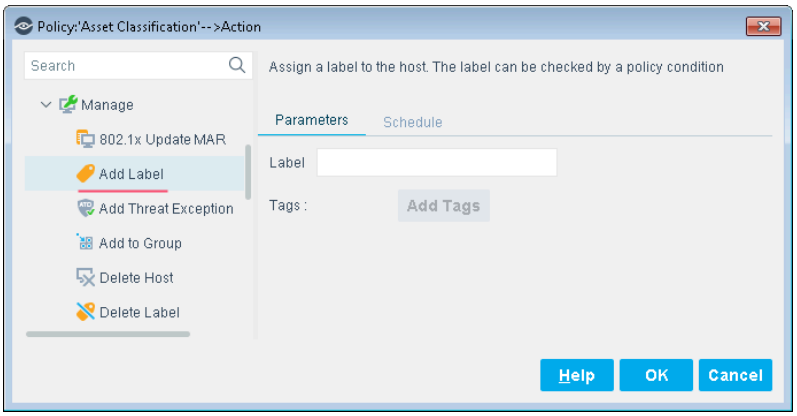
  Although you can use an IPv6 address as the Key value when you use Group Manager, the Add to Group action only supports IPv4 addresses. To support IPv6-only endpoints, specify the MAC address as the Key.

Add label

Labels mark and group endpoints based on properties or other evaluated values. Policies can apply further management logic based on labels assigned by a previous policy. This lets you construct complex policy behaviors that track endpoint history.

This action requires that the Advanced Tools Plugin is running.

The Add Label action assigns a text label to endpoints that match the conditions of the policy. This action is located in the Manage group of the Actions tree.

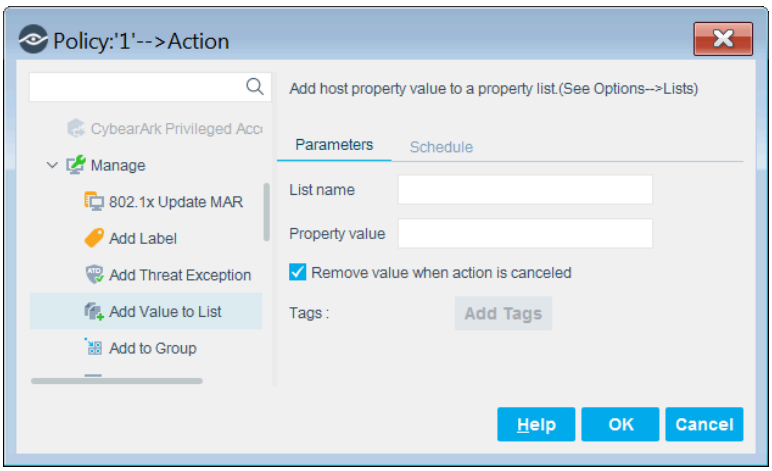


In the Label field, define the label text. The label can combine static text strings and endpoint-specific information. Select Add Tags to insert data tags that resolve to host property values. Labels are listed with other endpoint details in Home and Asset Inventory views.

Add value to list

This action requires that the Advanced Tools Plugin is running.

Use the Add Value to List action to place property values that match a policy condition into a list. For example, place all logged-in users of hosts at which a malicious event was detected by eyeSight eyeSight into a Malicious Users list. You can then use this list to define a policy that performs a restrict action on other hosts where the user logged-in to.



In the List name field, enter the name of the list that you want to add the property value to. The list name you enter must match the name of a previously defined list.

In the Property value field, use tags to define endpoint-specific property values. Select Add Tags to insert data tags that resolve to host property values.

Select the Remove value when action is canceled option to remove the value from the list when the action is canceled (i.e. when the host no longer matches the policy rule).

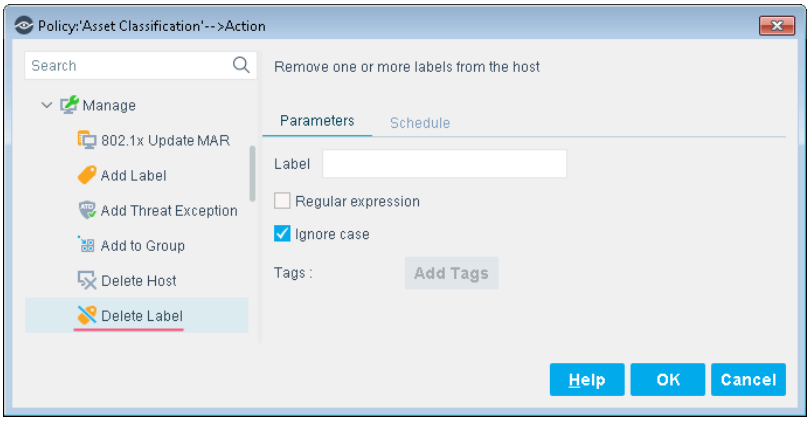
See Defining and Managing Lists for more information about lists.

Delete label

Labels mark and group endpoints based on properties or other evaluated values.

This action requires that the Advanced Tools Plugin is running.

The Delete Label action removes a text label from endpoints that match the conditions of the policy. This action is located in the Manage group of the Actions tree.



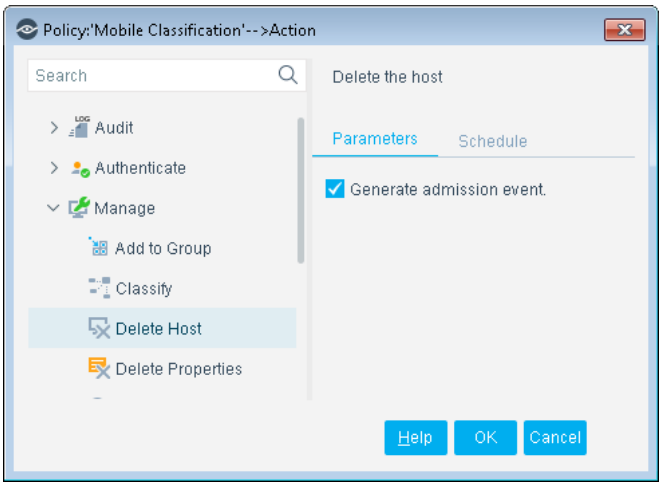
In the Label field, define the label text. The label can combine static text strings and endpoint-specific information. Select Add Tags to insert data tags that resolve to host property values.

To delete several labels, enter a string using wildcard characters and then select Regular expression. All partially matched labels are deleted.

Select Ignore case to match label strings regardless of the use of uppercase or lowercase letters.

Delete host

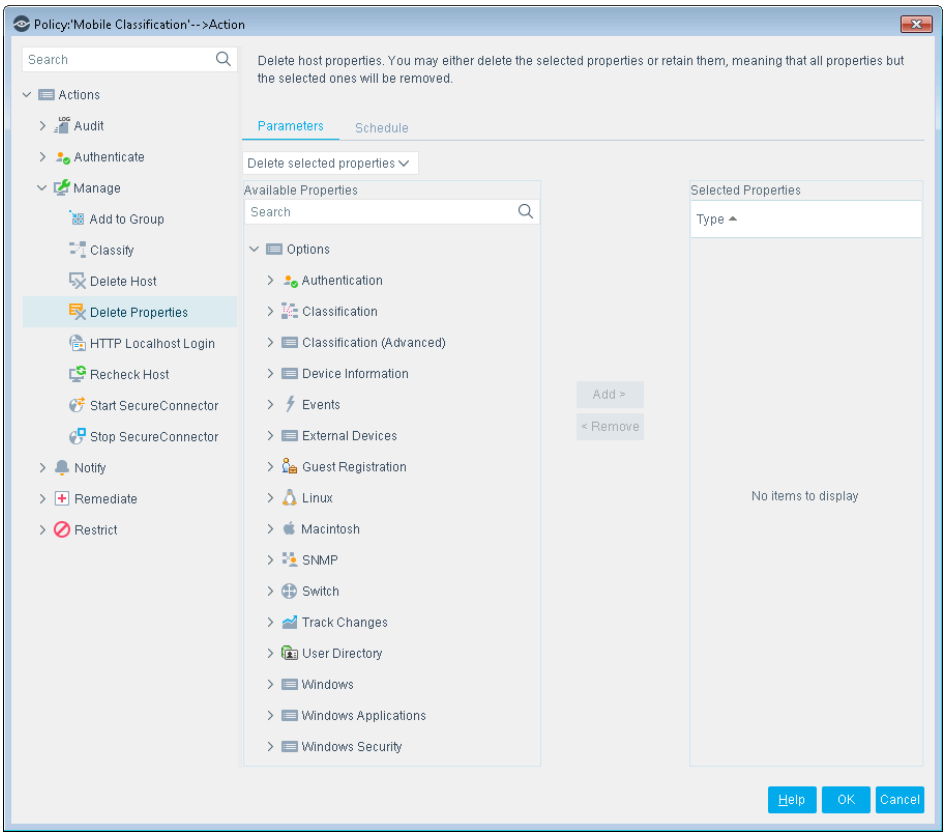
This action lets you instruct eyeSight eyeSight to delete endpoints detected in a policy. Select Generate admission event to rediscover endpoints immediately after they are deleted. When you clear the checkbox, endpoints are rediscovered after they generate traffic.



Delete properties

The Delete Properties action lets you instruct eyeSight eyeSight to clear all detections made on endpoints. Clearing cancels any actions assigned to the endpoints as a result of the detection.

Select Generate admission event to reevaluate the endpoint immediately after the detections are cleared. When you clear the checkbox, properties are evaluated after an endpoint generates traffic.

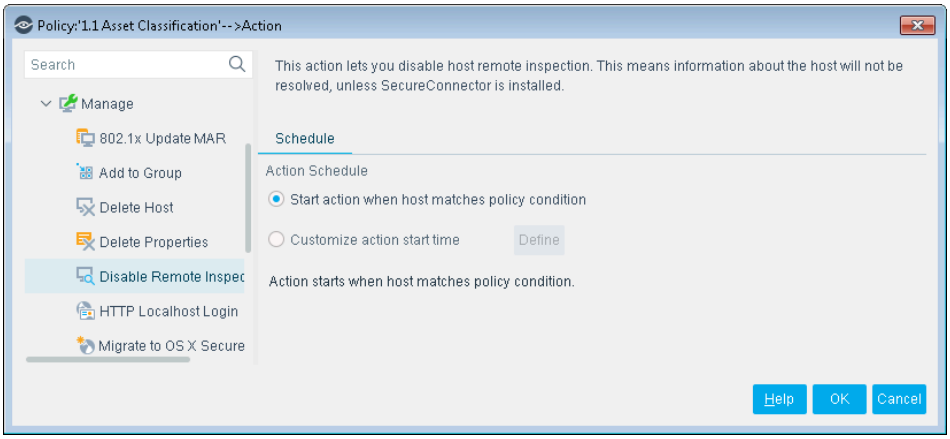


Disable remote inspection

The Delete Remote Inspection action instructs eyeSight eyeSight not to resolve host properties for the endpoint using Remote Inspection. Actions are still applied to the endpoint. This action is maintained as long as the endpoint matches the conditions of the policy rule, or until the action is manually canceled for the endpoint.

This action may be useful in situations where administrators want to minimize traffic and deep inspection of sensitive computers at sensitive times. For example, Forescout administrators can use this action to support end users on trading floors or in process control environments that require minimal endpoint traffic and CPU overhead during periods of peak activity. Deep endpoint inspection can be performed using remote inspection during downtime periods.

Endpoints managed using SecureConnector are not affected by this action.



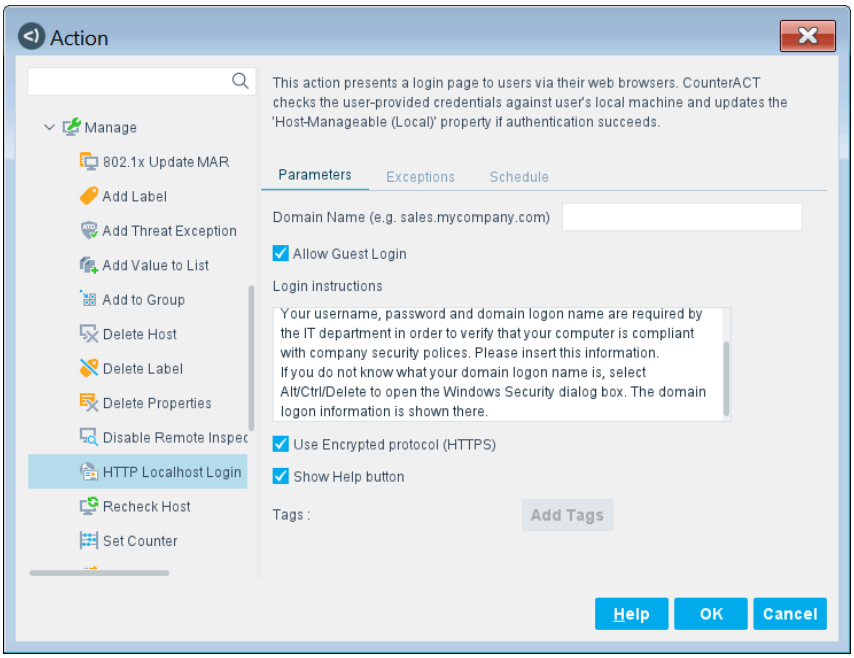
HTTP localhost login

Use the HTTP Localhost Login action to detect unmanageable guest endpoints, and allow users at the endpoints to authenticate. After the endpoints are authenticated, they can be included in all policy inspections

You may need to inspect guest machines that are not part of the network domain, ensure that they comply with corporate policies, and enforce network restrictions that are not in compliance. These endpoints are referred to as unmanageable hosts and can be included in your policy.

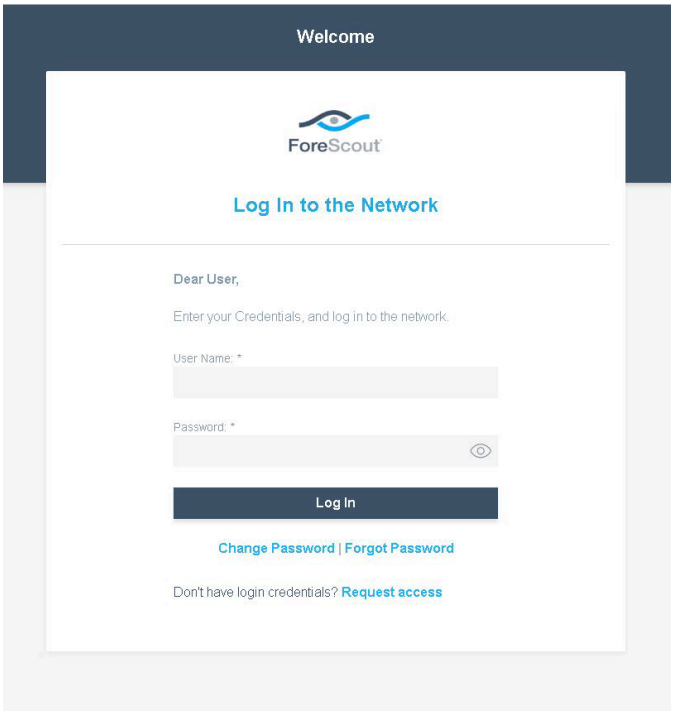
If you are using Flexx licensing, ensure that you have a valid eyeSight eyeControl license to use this action. Refer to About Flexx Licenses in the *Forescout eyeSight Flexx Licensing How-to Guide* for more information about managing licenses.

Note:
HTTP Localhost Login is disabled whenever HTTP Redirection is disabled. For more information, see Disable Web Portals .



Users at unmanageable endpoints are presented with an HTTP Login page when they attempt to access the web, and must provide their local login credentials to gain web access. If you have assigned other actions to the policy and the authentication is successful, all the policy's actions are canceled, removing all the limitations imposed.

If you think login credentials might not be available to users and do not want to limit their access, you can allow guest login to the web by selecting Allow Guest Login. When selected, the Login page includes a guest link option. You may want to do this, for example, when the guest user does not authenticate and is blocked from your network, but allowed web access.



The network user is prompted with a Login page on each attempt to access the web, until:

- The user successfully logs in.
- The endpoint is released via the Home view, Detections pane or Assets Portal.
- The guest login option is selected (when enabled).

It is recommended to select Use Encrypted protocol (HTTPS) to send the redirected page via HTTPS. To send it via the non-encrypted HTTP protocol, clear the Use Encrypted protocol (HTTPS) option. See Transmitting Actions via HTTPS for details.

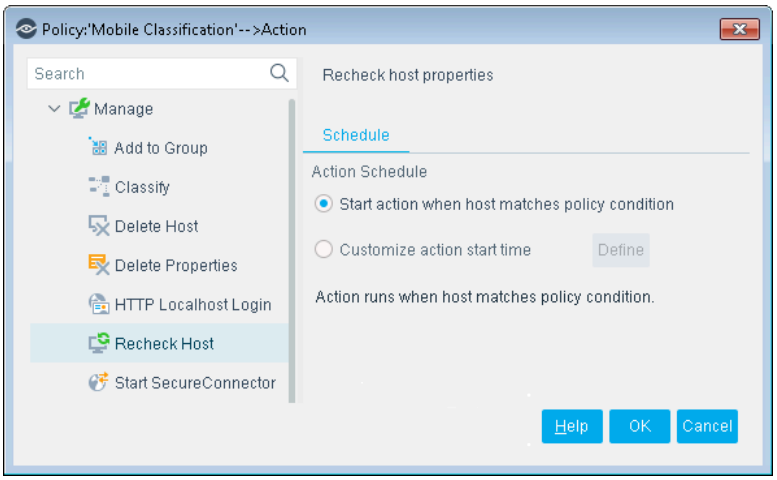
When using this action, you should configure the following condition properties. Use the ANDvalue between both properties:

- Windows>Manageable Domain>Does not meet the following criteria
- Windows>Manageable Local>Does not meet the following criteria

Depending on the endpoint operating system and how the endpoint is managed, this action is implemented by the HPS Inspection Engine, the Linux Plugin, or the OS X Plugin.

Recheck host

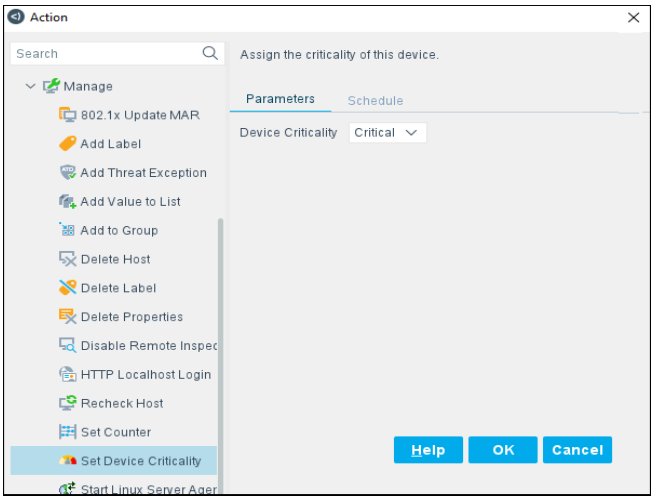
Use the Recheck Host action to recheck endpoints against conditions defined in a policy.



Set device criticality

The Set Device Criticality action lets you optionally assign device criticality according to the configuration of the device in your environment.

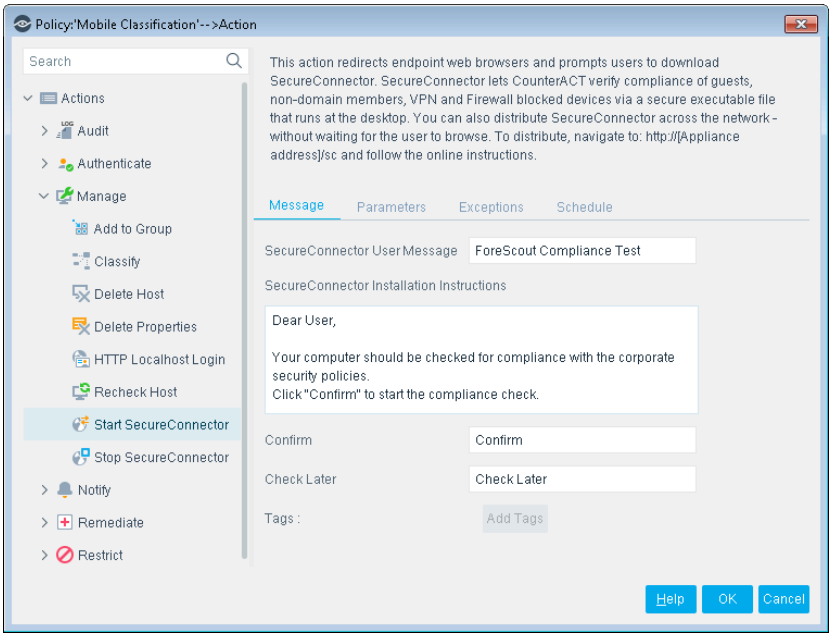
For example, assign device criticality according to device function, network segment, or device group.



Start SecureConnector / Stop SecureConnector

The Start SecureConnector and Stop SecureConnector actions let you install or stop Forescout's SecureConnector, a light footprint executable that runs on the endpoint. SecureConnector makes endpoints manageable and performs or optimizes certain actions.

For details about how SecureConnector works, supported operating systems, and installation methods other than the ones described here, refer to About the HPS Inspection Engine in the *HPS Inspection Engine Configuration Guide*.



Making Endpoints Manageable

Use SecureConnector to access unmanageable endpoints and make them manageable for deep inspection.

In general, Windows endpoints are unmanageable if their remote registry and file system cannot be accessed by Forescout eyeSight. Similarly, Linux and OS X endpoints are unmanageable if they

cannot be accessed using SSH direct access.

Typically this occurs when:

- Endpoints are not part of the domain, or are guests on the network
- Domain credentials do not work or are not available
- Endpoints browse to VPNs or wireless networks

Use the following properties to detect endpoints that cannot be managed without SecureConnector:

- For Windows endpoints (supported by the HPS Inspection Engine):
  - Windows Manageable Domain
  - Windows Manageable Domain (Current)
  - Windows Manageable Local
- For Linux endpoints (supported by the Linux Plugin):
  - Linux Manageable (SSH Direct Access)
- For OS X endpoints (supported by the OSX Plugin):
  - Macintosh Manageable (SSH Direct Access)

After you install SecureConnector, use the following properties to confirm that Forescout eyeSight accesses and manages an endpoint using SecureConnector:

- For Windows endpoints (supported by the HPS Inspection Engine):
  - Windows Manageable SecureConnector
  - Windows Manageable SecureConnector (via any interface)
- For Linux endpoints (supported by the Linux Plugin):
  - Linux Manageable (SecureConnector)
- For OSX endpoints (supported by the OSX Plugin):
  - Macintosh Manageable (SecureConnector)

Performing or Optimizing Certain Actions

When Windows endpoints are managed by SecureConnector, the local SecureConnector instance optimizes implementation of the following actions:

- Assign to VLAN action (required)
- Disable External Device action (required)
- Send Balloon Notification action (required)
- Disable Dual Homed action (required)
- Kill Process , *Kill Instant Messaging* , and Kill Peer-to-peer actions.

For example, some of these actions detect and stop specific Windows processes. On Windows endpoints that have SecureConnector installed, the process is killed more frequently.

To use the local SecureConnector instance for some of these actions, optional configuration settings must be enabled when you configure the HPS Inspection Engine. For details, refer to Configure the HPS Inspection Engine in the *HPS Inspection Engine Configuration Guide*.

Interactive vs. Background Installation Methods

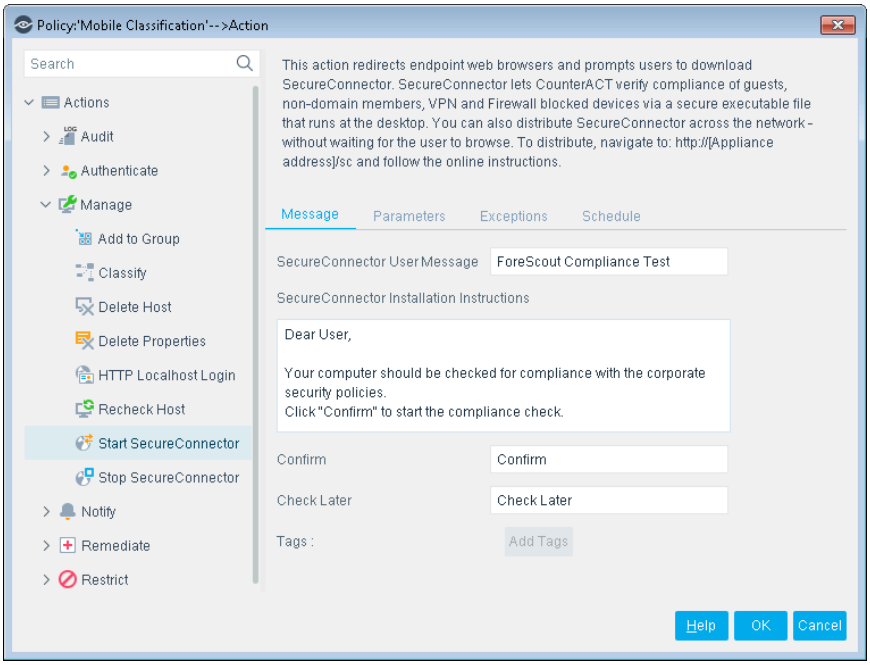
The Start SecureConnector action directs unmanaged endpoints to a web page at which end users interactively install SecureConnector. This web page is disabled whenever HTTP Redirection is disabled. For more information see Disable Web Portals.

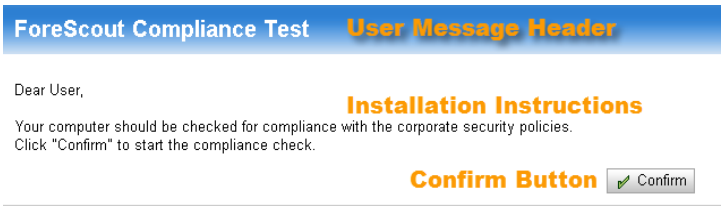
Alternatively, there are non-interactive ways to download and install SecureConnector on endpoints in the background. For example:

- On endpoints that are manageable using Remote Inspection, you can use the Remote Installation option of the action to install SecureConnector using a background script.
- To support automated deployment independent of Forescout policies, you can generate SecureConnector installer packages. Use your environment's endpoint management/utility tools to distribute and run these installers.

Message Tab

Use this tab to customize the notification page that is displayed to the end user. The message is displayed when the installation method chosen from the Parameters Tab is either HTTP Installation at the endpoint or Both.



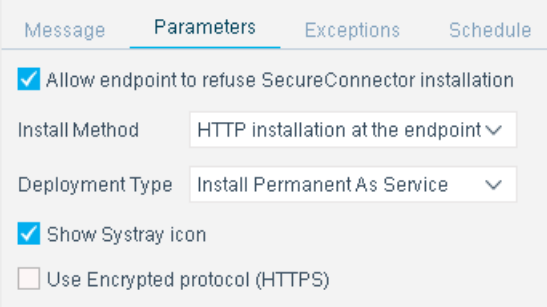


SecureConnector User Message	Text displayed as the page header.
SecureConnector Installation Instructions	Body text of the message.
Confirm	Text displayed on the Confirm button. When users select this button,

	SecureConnector installation proceeds immediately.
Check Later	Text displayed on the Check Later button. When users select this button, SecureConnector installation is deferred. This button is only displayed when the Allow endpoint to refuse SecureConnector installation option in the Parameters tab is enabled.

Parameters Tab

Use this tab to define Start SecureConnector installation and deployment parameters.



Allow endpoint to refuse SecureConnector installation	Allow users to the skip the installation by selecting the Check Later button. This option is only applicable if Install Method is set to HTTP Installation at the endpoint or Both .
Install Method	The following installation methods are available: HTTP Installation at the endpoint: Install at the endpoint via the end user's web browser. When endpoint users browse the Internet they are redirected to a page that prompts them to download SecureConnector. The page can be customized. See Localize Redirected Web Pages and Messages for details. Remote installation: Perform remote installation on manageable endpoints using domain credentials. Forescout eyeSight uses a script when this option is selected. Both: Both methods are activated simultaneously. If a remote installation succeeds, HTTP installation is halted.
Deployment Type	The following deployments types are available: Install Dissolvable: Configure SecureConnector to close at reboot or disconnection from the network, leaving no footprints. If SecureConnector is

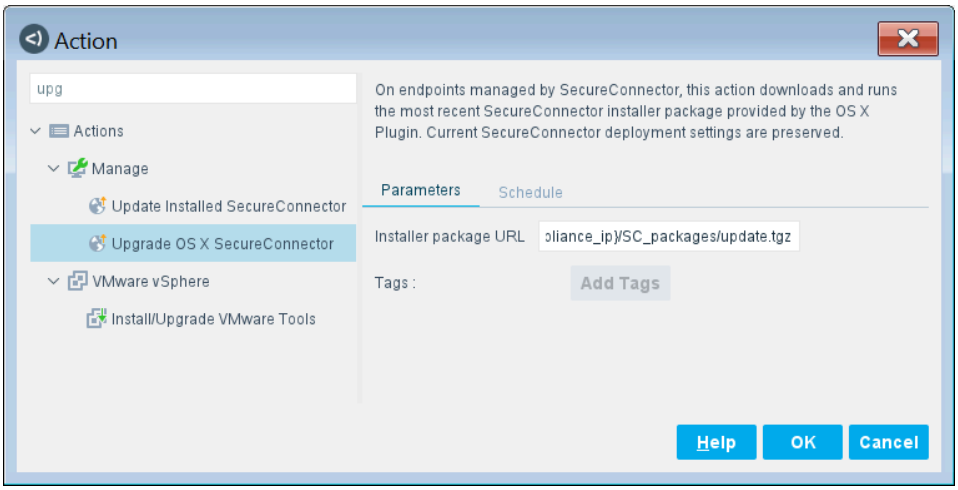
	not installed via the Dissolvable mode, it can be removed using the uninstall option on the endpoint. Install Permanent as Service Install Permanent as Application (Windows only)Install SecureConnector permanently on the endpoint as a user application or a root-level service. Installing SecureConnector as a Service provides the following advantages: Enhanced SecureConnector performance, especially when working with interactive actions such as Run Script on Windows. SecureConnector can be run before login and after logout. Refer to About the HPS Inspection Engine in the *HPS Inspection Engine Configuration Guide*. for details. On Windows endpoints, the Install as Application option installs SecureConnector as an application under the currently logged in user. When no user is logged in, SecureConnector is not installed.
Show Systray icon	Show the Forescout icon on the endpoint after SecureConnector is installed.
Use Encrypted protocol (HTTPS)	Send the redirection page via HTTPS. See Transmitting Actions via HTTPS for details.

Upgrade OS X SecureConnector

Unlike other plugins that support SecureConnector for Windows and Linux endpoints, the OS X plugin does not automatically update SecureConnector on endpoints when you install a new release of the plugin. Use this action to update SecureConnector on Mac OS X endpoints after you upgrade the OS X Plugin.

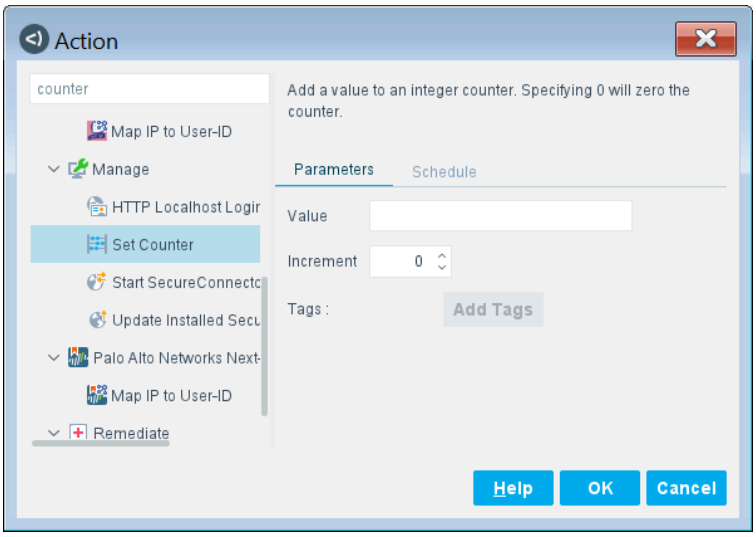
This action updates the SecureConnector package running on a Mac OS X endpoint. Deployment type (permanent/dissolvable) and menu bar visibility options are preserved during upgrade.

In the Installer package URL field, specify a valid network path to the update.tgz archive that is used to update endpoints. By default, this field points to the file that the OS X Plugin places on each Appliance. If you copy this archive to a content distribution network or server, specify the full network path to this new location. For details, refer to About the OS X Plugin in the *OS X Plugin Configuration Guide*.



Set counter

This action creates or increments a counter. This action is located in the Manage group of the Actions tree.



Use the following fields to define an action that creates a new counter or increments an existing counter.

Value	A text label for the counter. Because counters are maintained for each endpoint, this label can combine static text strings and endpoint-specific information to yield an endpoint-specific label. Select Add Tags to insert data tags that resolve to host property values.
Increment	The numerical value added to the existing value of the counter. The counter is incremented for an endpoint each time that endpoint matches the conditions of the rule.

To reset an existing counter to zero, specify 0 in this field.

When you create a policy that defines a new counter, use only the Set Counter action. A policy that increments an existing counter must use both the Counter property and the Set Counter action. See Set and Increment Counters for details.

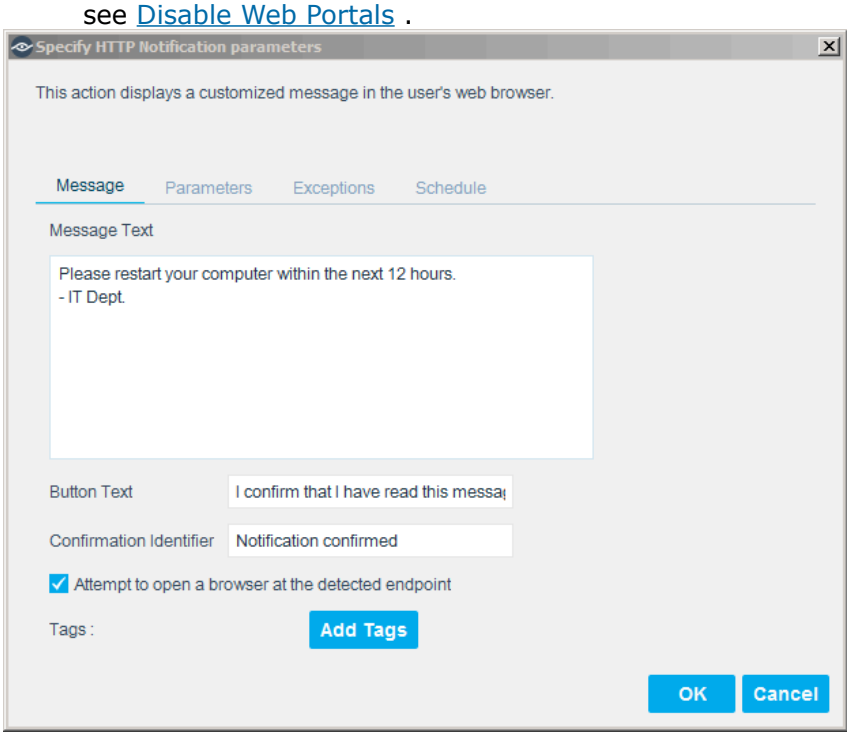
Notify actions

This topic describes actions used for communicating with endpoint users.

HTTP notification

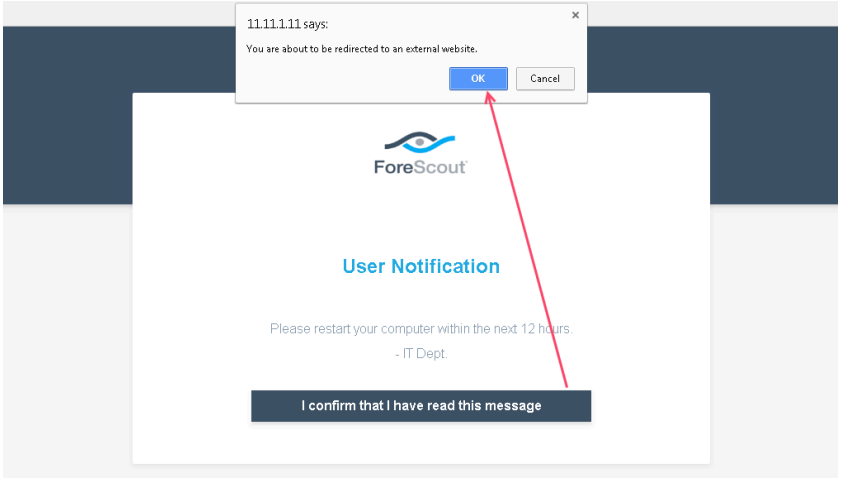
The user's web session is redirected when attempting to access the web. The user is presented with a message that you compose.

Note:
HTTP Notification is disabled whenever HTTP Redirection is disabled. For more information, see Disable Web Portals .



Web sessions are redirected until:

- The user confirms reading the message. See Parameters Tab for more information. After confirmation, a pop-up message informs users that they are being redirected to an external website.



- The endpoint is released via the Home view, Detections pane or Assets Portal.

Message Tab

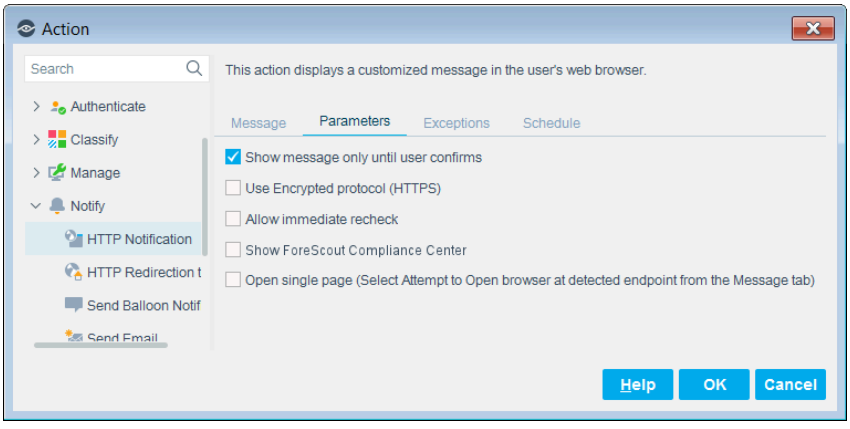
Enter the message that you want the user to read.

You can receive information regarding end user confirmation of browser notification messages. To discover which users have confirmed, add a confirmation string to the Button text field and create a policy with the new HTTP Confirmation Events Property.

By default, the user's session is redirected when the user attempts to access the web. However, you can define the action to automatically open a browser at the endpoint, instead of waiting for the user to browse. This ensures that the message gets to the user faster. Select Attempt to open a browser at the detected endpoint. (This option is not available for Windows 2000 and Windows 2003 server machines, and only works on managed machines.) eyeSight eyeSight uses a script when this option is selected. Refer to About the HPS Inspection Engine in the *HPS Inspection Engine Configuration Guide* for details about how scripts work.

You can also customize the height and width of the notification page and open the notification page as an Explorer dialog box, rather than displaying it using the default web browser. For details, refer to the *HPS Inspection Engine Configuration Guide* .

Parameters Tab



- To allow the endpoint user to only confirm the message once, select Show message only until user confirms.

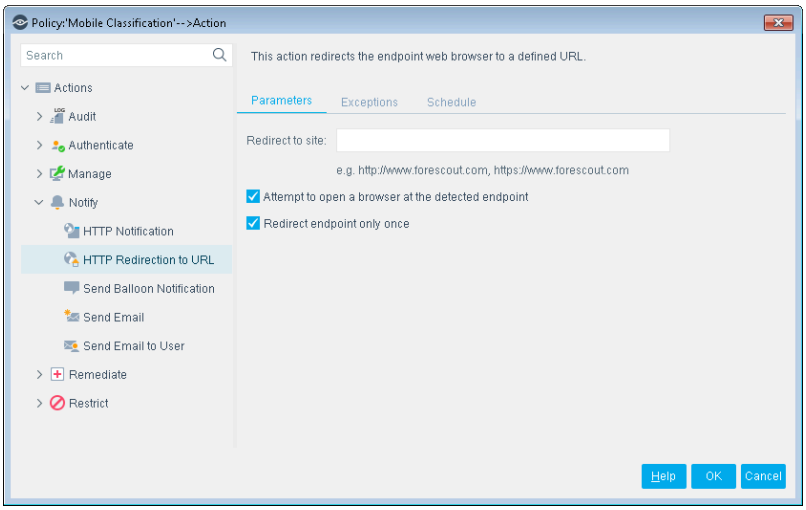
- To send the redirected page via HTTPS, select Use Encrypted protocol (HTTPS). See Transmitting Actions via HTTPS for details.
- Endpoints users can run a policy recheck directly from the notification page by selecting Allow immediate recheck. This allows endpoints to verify compliance status in between defined rechecks. On-demand rechecks at the endpoint enable faster overall network compliance and increase productivity. You can hide this option by clearing Allow immediate recheck.
- Select Show ForeScout Compliance Center to display the Login page at the endpoint. If the endpoint has been assigned compliance policies, they will also appear in the wizard. See Working with the Forescout Compliance Center for details.
- Select Open single page to only redirect the first web browser tab, allowing the user to continue browsing in other tabs. Verify that Attempt to open a browser at the detected endpoint is selected on the Message tab.

HTTP redirection to URL

The user's web session is redirected to a specific web page. You can combine this action with the HTTP Notification action, redirect the endpoint web session to a specific site and add a customized message.

If you are using Flexx licensing, ensure that you have a valid license to use this action. Refer to About Flexx Licenses in the *Forescout eyeSight Flexx Licensing How-to Guide* for more information about managing licenses.

Note:
HTTP Redirection to URL is disabled whenever HTTP Redirection is disabled. For more information, see Disable Web Portals .



HTTP Redirection to URL

By default, the user's session is redirected when the user attempts to access the web. However, you can define the action to automatically open a browser at the endpoint, instead of waiting for the user to browse. This ensures that the message gets to the user faster. Select Attempt to open a browser at the detected endpoint. (This option is not available for Windows 2000 and Windows 2003 server machines, and only works on managed machines.) Forescout eyeControl uses a script when this option is selected. Refer to the *HPS Inspection Engine Configuration Guide*. for details about how scripts work.

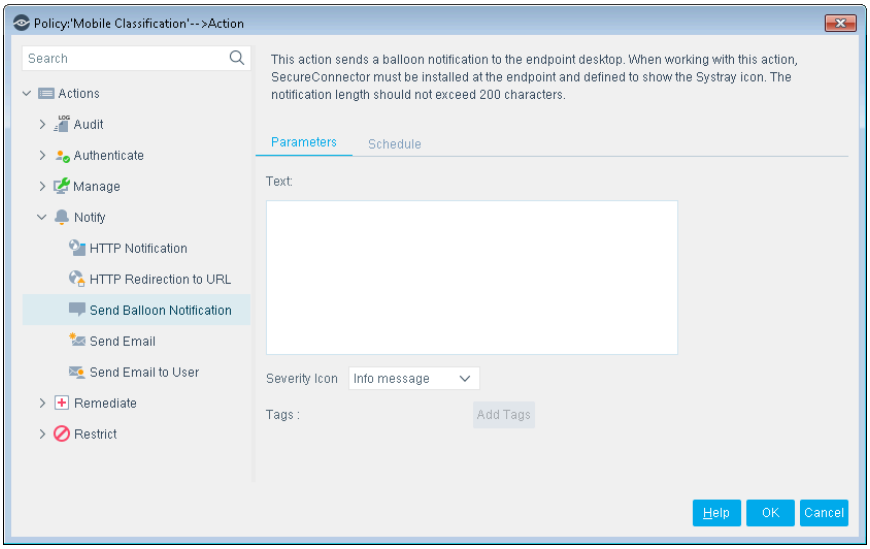
By default, the action is only applied one time during the match period. The first time the end user enters a URL in the web browser, the endpoint is redirected to the URL configured in the action. You can configure this action to continuously apply to endpoints that match the policy rule by clearing the Redirect endpoint only once checkbox. As a result, the endpoint is always redirected to the URL configured in the action within the match period.

Send balloon notification

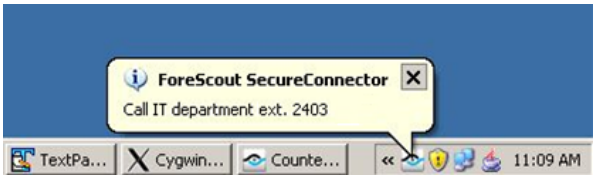
Use this action to send a balloon message to the detected endpoint. Use of this feature requires that the endpoint be connected via SecureConnector.

Users can type messages of up to 200 characters and indicate whether the message should appear with an Error, Warning or Information icon.

Note:
The character limit may vary slightly in certain languages.



Balloon messages are displayed in the endpoint system tray.

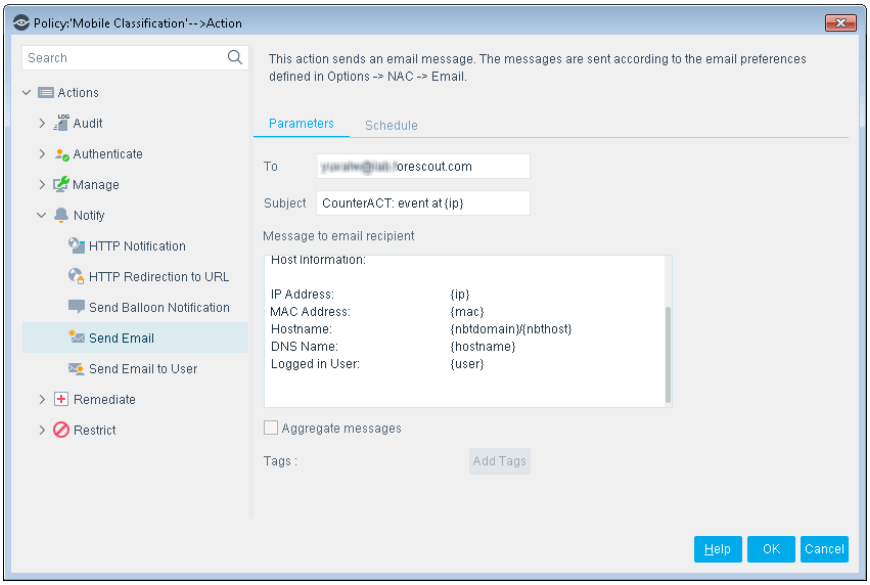


Send email

Send an email notification to the administrator or to other addresses. Basic information about the endpoint is displayed by default in the email message. Add additional text as required. When composing the message, you can insert any number of property tags. For example, if you enter {ip}, the IP address at which the events were detected is automatically inserted into the message. See Property Tags for details.

Select Aggregate messages to help you manage email deliveries. When selected, the values set for Policy Email Preferences are applied to this action. Specifically, these preferences define:

- The maximum number of email alerts delivered per day (from midnight)
- The maximum number of events that are listed in each email

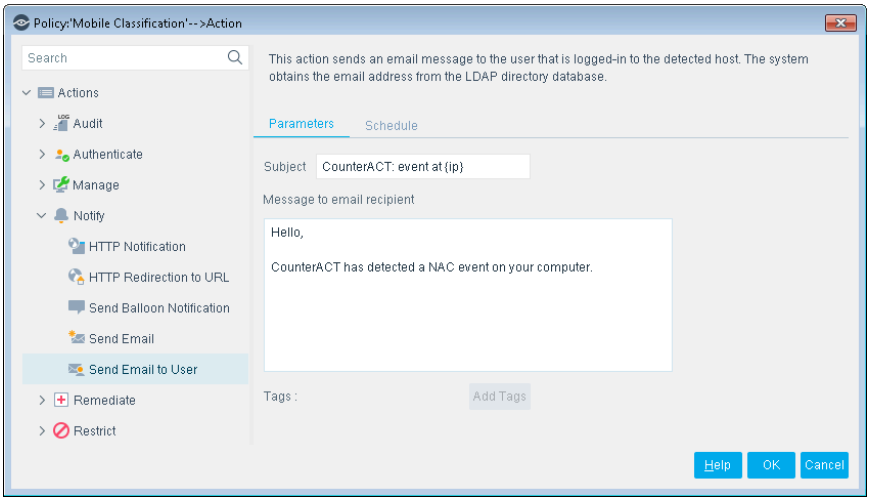


You can sign these emails using a digital certificate, as specified by the Secure/Multipurpose Internet Mail Extensions (S/MIME) standard. See Signing Emails with an S/MIME Certificate for details.

See Policy Preferences for details.

Send email to user

This action sends an email message to the User Directory, User Mail Address that is registered with the detected endpoint.



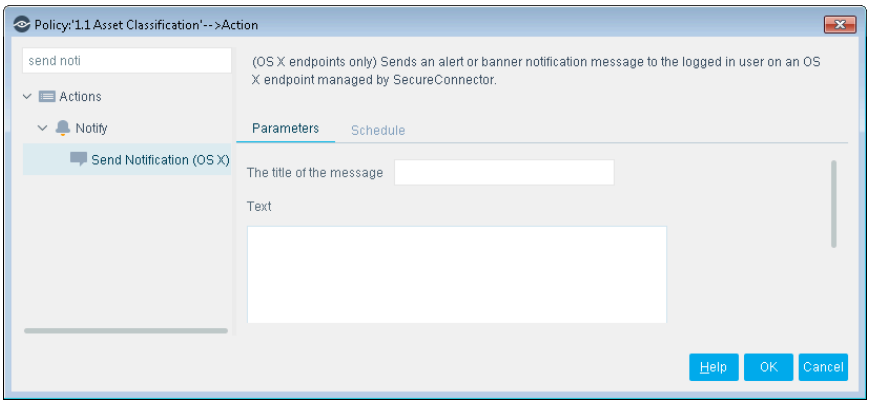
Basic information about the endpoint is displayed by default in the email message. Add additional text as required. When composing the message, you can insert any number of property tags. For example, if you enter `{ip}`, the IP address at which the event was detected is automatically inserted into the message. See Property Tags for details.

You can sign these emails using a digital certificate, as specified by the Secure/Multipurpose Internet Mail Extensions (S/MIME) standard. See Signing Emails with an S/MIME Certificate for details.

Send notification OS X action

This action sends an alert or banner notification message to an OS X endpoint managed by SecureConnector. The Notification Center of the user currently logged in to the endpoint handles the message. This action parallels the Send Balloon Notification action for Windows endpoints. You can use property tags to include endpoint-specific property values in the notification. See Property Tags for details.

Banner notifications appear briefly on screen. Alerts persist on screen until the user interacts with them.



Remediate actions

Remediation actions help you remediate endpoint vulnerabilities.

If you are using Flexx licensing, ensure that you have a valid eyeSight eyeControl license to use these actions. Refer to About Flexx Licenses in the *Forescout eyeSight Flexx Licensing How-to Guide* for more information about managing licenses.

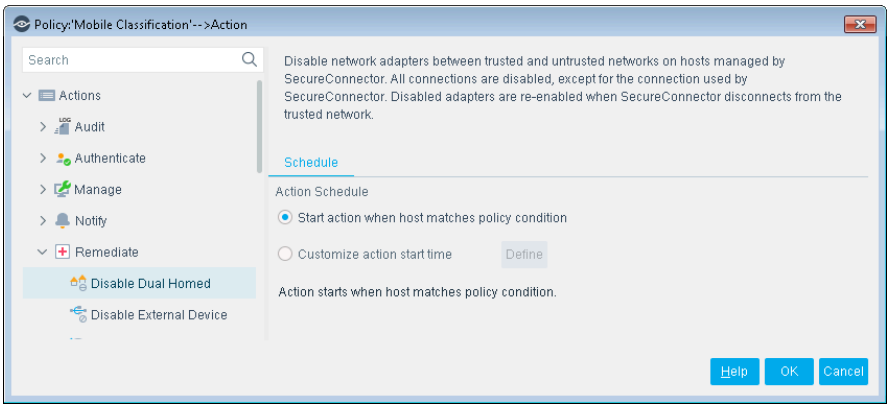
Note:
The Expedite IP Discovery action is an exception, and does not require an eyeControl license.

Disable adapters on dual homed devices (Disable Dual Homed) - Windows only

This action disables network adapters that act as a bridge between trusted and untrusted networks on endpoints managed by SecureConnector.

All connections are disabled, except for the connection used by SecureConnector. Disabled adapters are re-enabled when SecureConnector disconnects from the trusted network.

Note:
This action applies only to endpoints managed by SecureConnector.

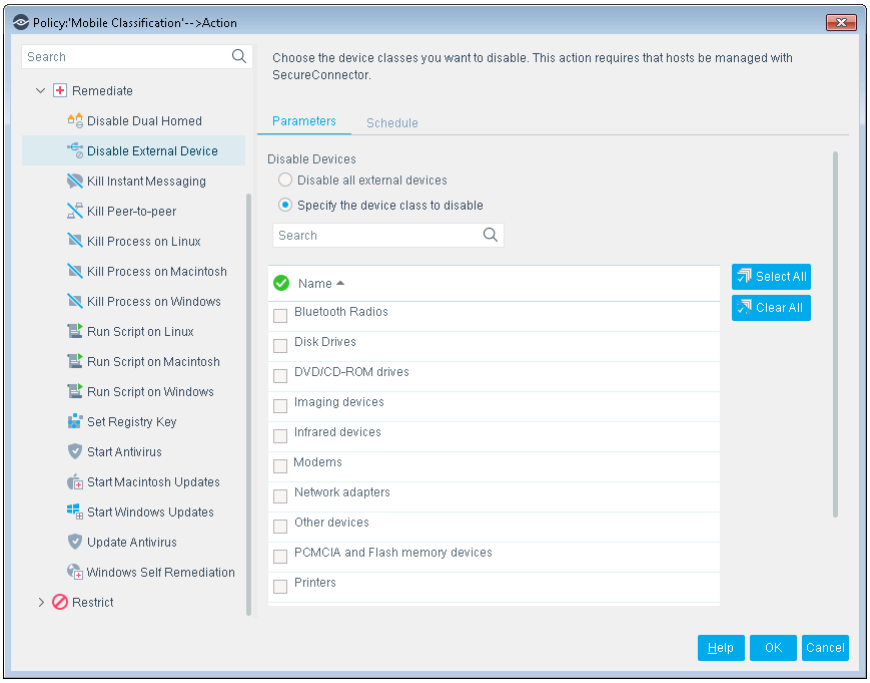


Disable external devices

The Disable External Devices action disables external devices connected to Windows endpoints, for example, USB mass storage devices, modems, printers, cameras, NIC cards, PCMCIA, CD/DVD, gaming, and smartphones.

The devices remain blocked until the action is canceled, even if the device is inserted, removed and later reinserted. This action requires that endpoints be managed with SecureConnector, and requires the proper configuration and activation of the HPS Inspection Engine. Use the External Devices property when working with the action.

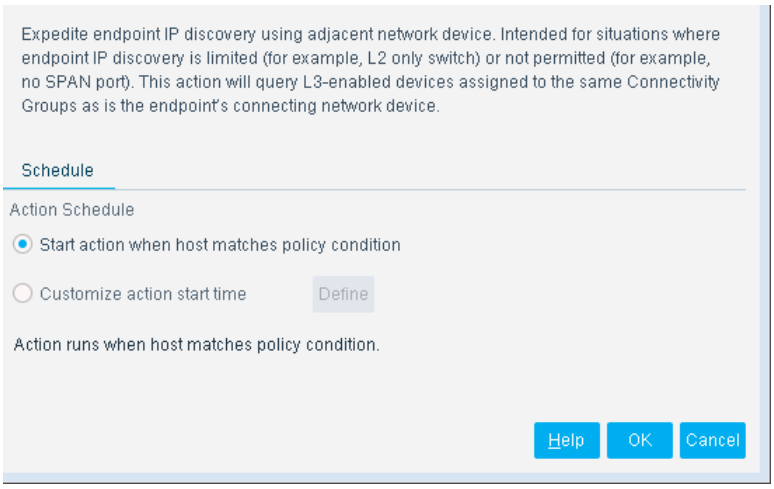
This action requires that endpoints be managed with SecureConnector. You can automatically install SecureConnector when deploying this action. Select Tools > Options, select HPS Inspection Engine and then select the SecureConnector tab.



Expedite IP discovery

The Expedite IP Discovery action is a remediate action provided by the Switch Plugin. Use this action to address situations of delayed endpoint IP discovery.

The action expedites the resolution of endpoint IP addresses (IP discovery resolve requests) by the Switch Plugin querying the ARP table of designated, adjacent, L3-enabled network devices.

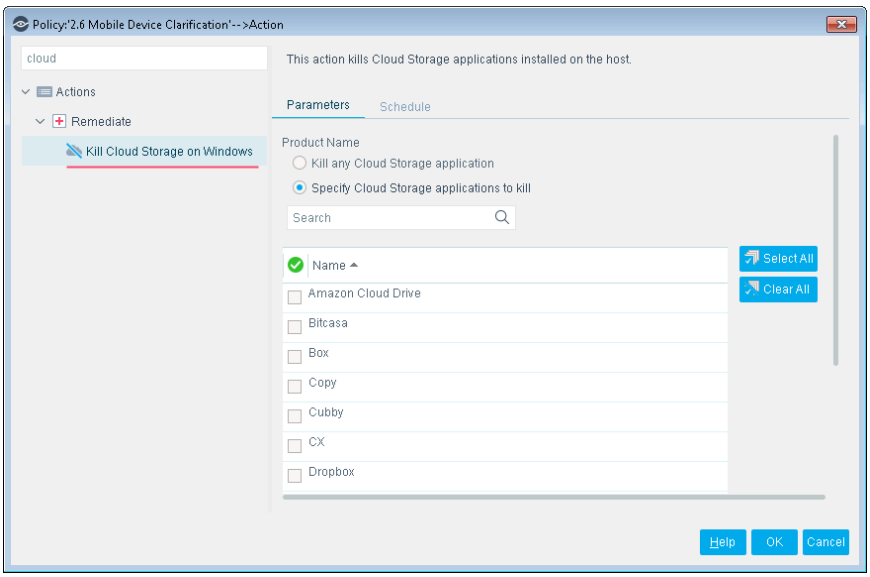


For details about this action, including the symptoms and root causes of delayed endpoint IP discovery, refer to Expedite IP Discovery in the *Switch Plugin Configuration* Guide.

Kill Cloud Storage on Windows

The Kill Cloud Storage on Windows action halts specified cloud storage applications that are running on Windows endpoints.

By default, the application is killed once a minute. If the endpoint has SecureConnector installed it is killed once a second.



To increase the kill frequency, you can automatically install SecureConnector on endpoints when this action is applied to them. When you configure the HPS Inspection Engine, select the Automatically run SecureConnector on Windows endpoints to increase frequency of Kill Process, Kill IM and P2P actions checkbox.

Refer to About the HPS Inspection Engine in the *HPS Inspection Engine Configuration Guide* for details about SecureConnector configuration. Select Tools > Options > Modules, then select the plugin, and then select Help.

Note:
Forescout eyeControl uses a script on the endpoint to apply this action if the endpoint is managed via domain credentials (Windows Manageable (Domain) is True). Refer to the *HPS Inspection Engine Configuration Guide* for details about scripts.

The Windows Applications Plugin provides updates to the applications supported by this action. Refer to the *Windows Applications Configuration Guide* for more information about the module. Select Tools > Options > Modules, then select Windows Applications, and then select Help.

Restrict actions

Restrict actions are used to restrict endpoint access to the network and Internet .

If you are using Flexx licensing, ensure that you have a valid Forescout eyeControl license to use these actions. Refer to About Flexx Licenses in the *Forescout eyeSight Flexx Licensing How-to Guide* for more information about managing licenses.

Switch restrict actions

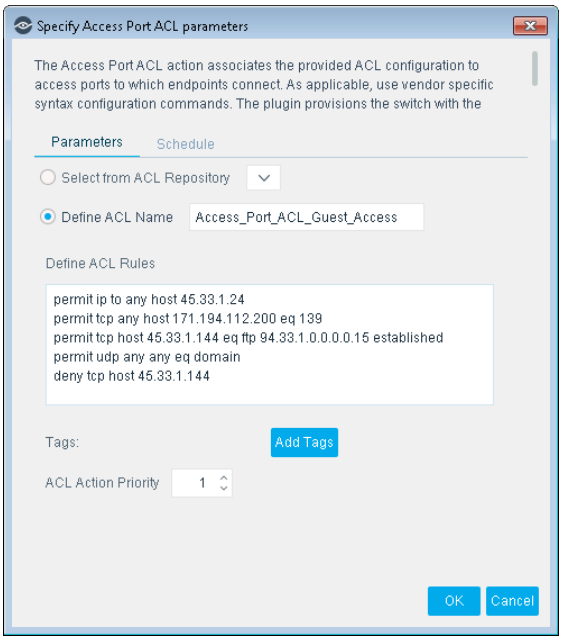
The Switch Plugin provides the following restrict actions:

For details about these actions, refer to the *Switch Plugin Reference Guide*.

Access port ACL

Use the Access Port ACL action to define an ACL that addresses one or more than one access control scenario, which is then applied to an endpoint’s switch access port. Access control scenarios are typically role or classification driven, for example, registered guest or compliance, and not endpoint IP specific.

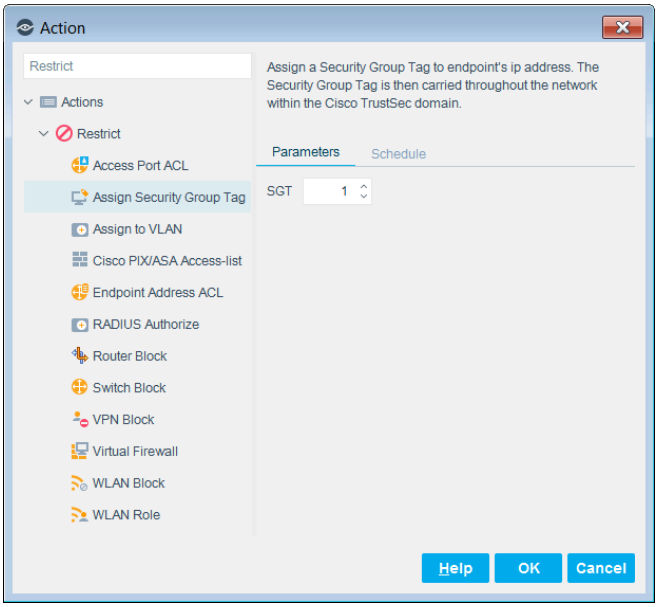
For example, implement an ACL action that denies corporate network access to guests but permits Internet access, regardless of endpoint IP address (no IP address dependency).



In the ACL configuration, take advantage of the full set of switch capabilities. Forescout eyeControl does not inspect and does not alter the provided content; the plugin's role is one of delivery vehicle to provision a network switch.

Assign security group tag

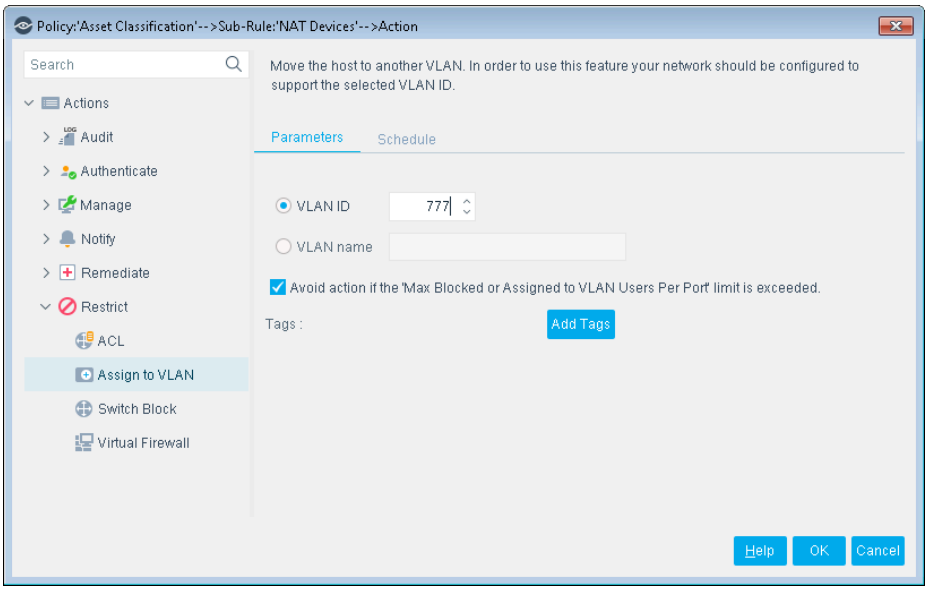
Use the Assign Security Group Tag action to assign a Security Group Tag (SGT) to detected endpoints. For this action to be available in the Console, you must enable the advanced configuration flag `assign_sgt`, which is disabled by default. Endpoints with an assigned SGT are connected to a managed Cisco switch in a Cisco TrustSec domain. An SGT is a number in the range of 1–65,535.



Assign to VLAN

Use the Assign to VLAN action to assign endpoints to a VLAN, rather than turning off their switch ports.

This enables secured remote connection to endpoints for the purpose of deploying patches, but prevents the propagation of unwanted traffic to other sections of the network.



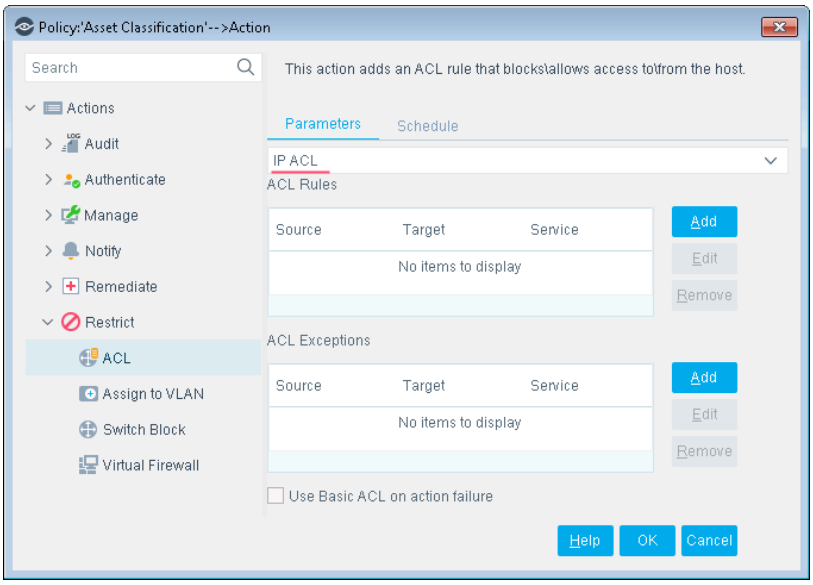
The Assign to VLAN action is not supported for the VoIP device if there is a VoIP device between the switch and the endpoint (a VoIP port with a connected VoIP phone and a connected PC behind the phone).

In this scenario, the Assign to VLAN action is supported for the endpoint, when specific Forescout/ Switch Plugin requirements are fulfilled.

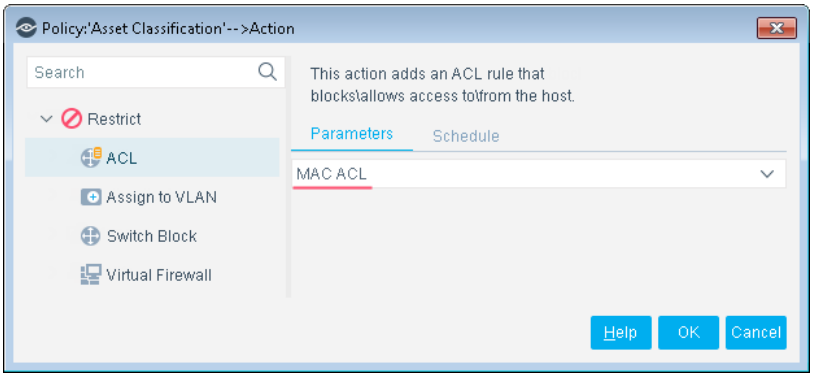
Endpoint address ACL

Use the Endpoint Address ACL action to define and apply any of the following, connected endpoint handling:

- IP ACL: Instruct a switch to close (ACL rule) or to open (ACL exception) network zones, services or protocols to traffic to or from specific, endpoint IP addresses connected to the switch.

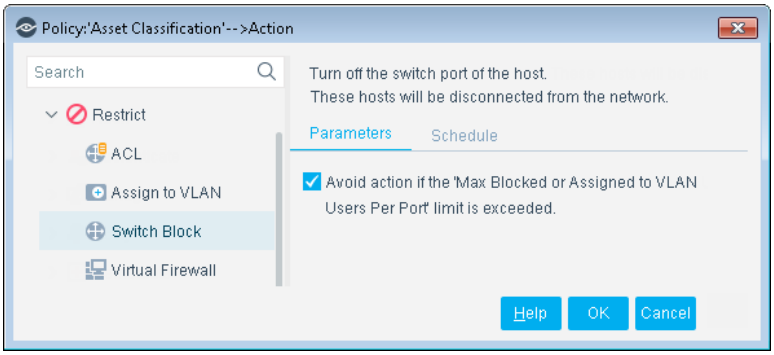


- MAC ACL: Instruct a switch to block all traffic sent from the affected, endpoint MAC address.



Switch block

Use the Switch Block action to completely isolate endpoints from your network by turning off their switch port and preventing endpoints from communicating with the network. This is an extreme action that should be used with care.



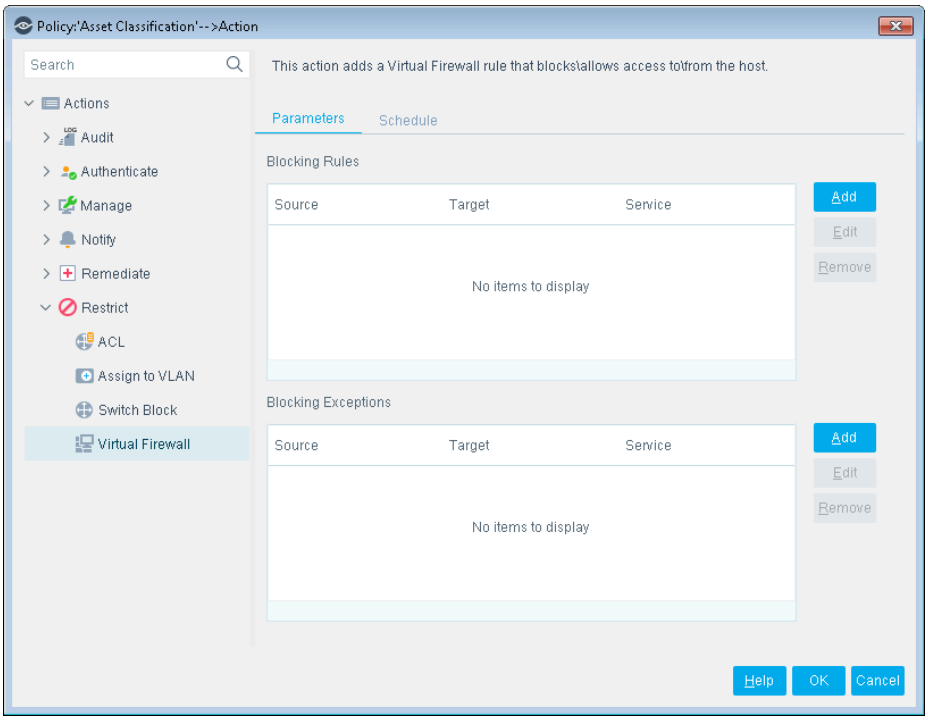
If there is a VoIP device between the switch and the endpoint, that is, a VoIP port with a connected VoIP phone and a connected PC behind the phone, the Switch Block action is supported for the endpoint, when the blocking of VoIP ports is globally enabled in the Switch Plugin for all

managed switches.

Virtual firewall

The Virtual Firewall action lets you block access to and from detected Windows endpoints. The action also provides an option to define blocking exceptions. For example, when you define a range of addresses to block, but want to allow traffic to and from IT administrator endpoints or VIP endpoints.

You can configure your system to use the Virtual Firewall action to block endpoints connecting through a proxy server from accessing HTTPS pages when a redirect action is also used. See Blocking HTTPS via Proxy Server.



Endpoints detected via a policy and blocked with the Virtual Firewall, appear in the Virtual Firewall pane, but for display purposes only. Manage these endpoints via the Home view, Detections pane.

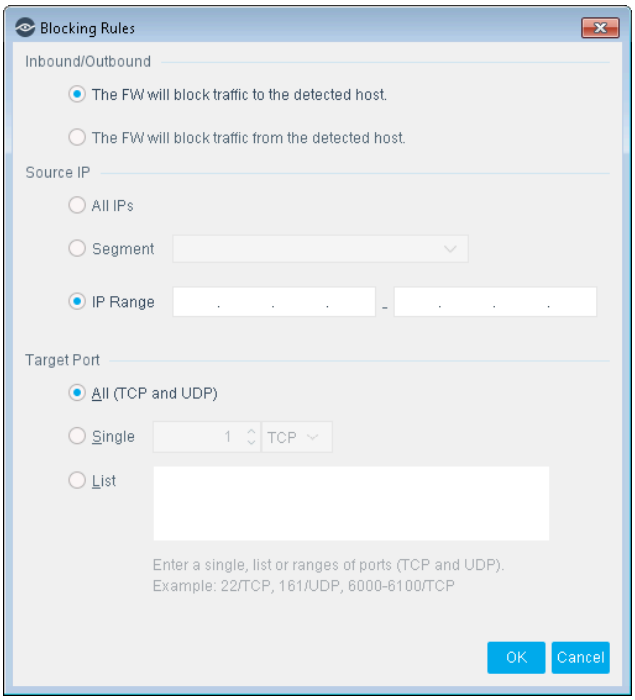
Rules created directly via the Virtual Firewall pane take precedence over policies created here.

Creating a blocking rule

This rule lets you block traffic to or from the detected endpoint.

To block traffic:

1. In the Blocking Rules section, select Add.
2. Select The FW will block traffic to the detected host to block inbound traffic to detected endpoints on specified services.



3. In the Source IP section, define the endpoints that are prevented from communicating with the detected endpoint.
4. In the Target Port section, define the services on the detected endpoint that are blocked.
5. Select OK.

The new rule appears in the Blocking Rules list. You can edit or remove rules by selecting Edit or Remove, as required.

To block traffic from the detected endpoint:

1. In the Blocking Rules section, select Add.
2. Select The FW will block traffic from the detected host. This lets you block outbound traffic from detected endpoints to specific services on other endpoints.
3. In the Target Port, section. define the endpoints that are prevented from receiving traffic
4. Select OK.

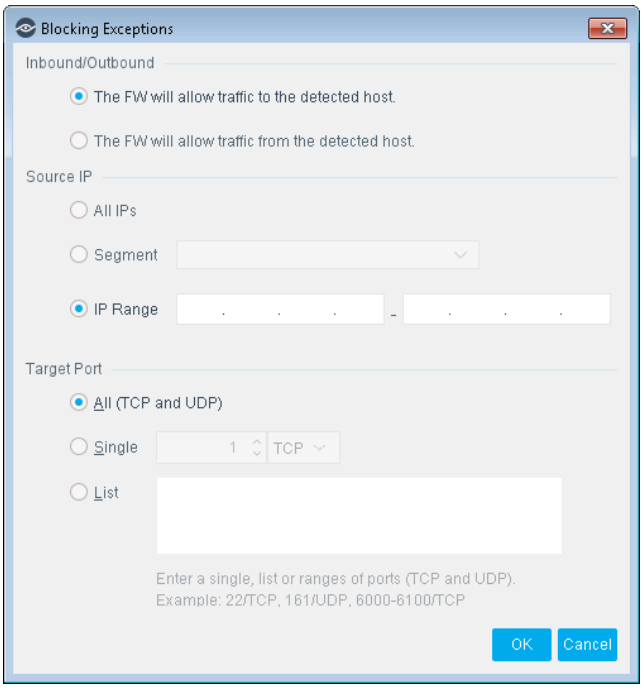
The new rule appears in the Blocking Rules list. You can edit or remove rules by selecting Edit or Remove, as required.

Creating exceptions

You can define exceptions to the blocking rules created. This enables the continuous flow of traffic to or from detected endpoints. For example, when you define a range of addresses to block, but want to allow traffic to and from IT administrator endpoints or VIP endpoints.

To create rule exceptions:

1. In the Blocking Exceptions section, select Add.



2. Select The FW will allow traffic to the detected host to allow inbound traffic to detected endpoints.
3. In the Source IP section, define the endpoints that are allowed to communicate with the detected endpoints.
4. In the Target Port section, define the services on the detected endpoints that are allowed.
5. Select

   The new rule appears in the Blocking Exceptions list. You can edit or remove rules by selecting Edit or Remove as required.

To allow traffic from the detected endpoint:

1. In the Blocking Exceptions section, select Add.
2. Select The FW will allow traffic from the detected host to allow outbound traffic from the detected endpoints.
3. In the Target IP section, define the endpoints that are allowed to receive traffic from the detected endpoint.
4. In the Target Port section, define the services on the endpoints that are allowed.
5. Select OK.

The new rule appears in the Blocking Exceptions list. You can edit or remove rules by selecting Edit or Remove as required.

Blocking HTTPS via proxy server

By default, the Virtual Firewall action does not block endpoints connecting through a proxy server from accessing HTTPS pages when a redirect action is also used.

To allow this action to block such endpoints, you must modify the system setup and settings as described below.

Setup

To set up your system to block endpoints connected via proxy servers:

1. Select Options > NAC > HTTP Redirection > Monitor Proxy Ports for HTTP Notifications and configure the proxy port.
2. Verify that the IP address of the proxy server is within the range of the Internal Network (Options > Internal Network).
3. If you want to apply the HTTP Notification action to HTTP traffic, clear the Show message only until user confirms option in the Parameters tab of the action. HTTPS traffic will not be redirected by this action.
4. Verify that the defined proxy service is not configured as an Authentication Server (Options > NAC > Authentication).

Enable/Disable

After your system is set up properly, perform the following to block endpoints connecting through a proxy server from accessing HTTPS pages when a redirect action is also used.

To enable the Virtual Firewall action:

1. Run the following commands:

   ```
   fstool set_property engine.conf.params.blockOutgoingSessionInHijack 8

   fstool service restart
   ```

2. Configure and run the relevant policy/policies, including the Virtual Firewall action and any relevant HTTP action/s

To disable the Virtual Firewall action:

- Run the following commands:

```
fstool set_property engine.conf.params.blockOutgoingSessionInHijack 0

fstool service restart
```

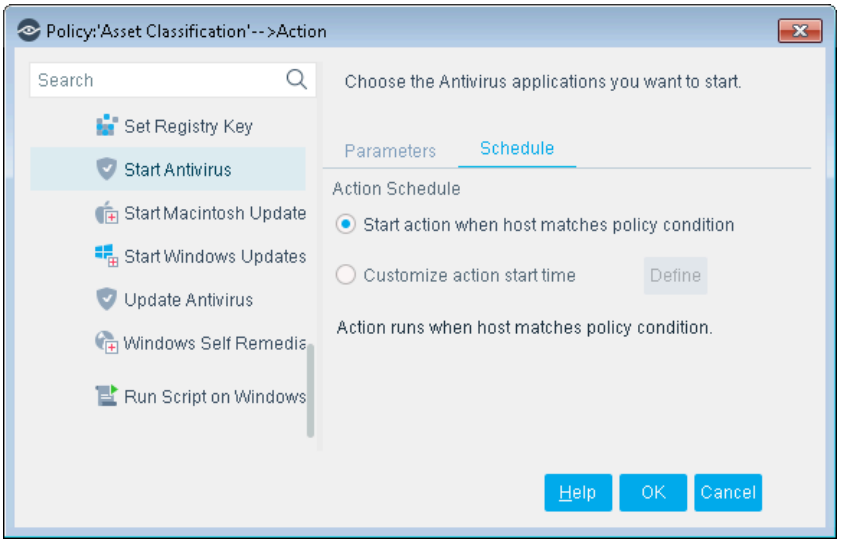
More action tools

Action schedules

By default, actions are carried out when eyeSight eyeSight detects that the endpoint matches the policy. Alternatively, action schedules can be assigned to each action. This lets you to control when actions are carried out and for what duration. For example, you can create a policy with an action that sends email to noncompliant users three times a week or for two weeks. When the endpoint complies with the policy, the email will no longer be sent.

Schedules are especially useful when you need to escalate sanctions on noncompliant endpoints. For example, create a policy that warns users not to run peer-to-peer applications and then blocks their Internet access if applications are detected after the warning period.

To create an action schedule, open the policy wizard, select a rule, and open an action for editing. Select the Schedule tab.



Property tags

Property tags can be used to insert endpoint property values in condition or action definition fields. For example, important endpoint or User Directory information can be added to email messages, and endpoint identifiers can be added to comments and labels.

Note:
If the information cannot be resolved, the message displays the tag code rather than the resolved information.

To use a property tag when you configure a Condition or Action, select a text field. Select Add Tags and insert a tag with data relevant to the field.

When the text field is evaluated, the tag is replaced by the actual property value of the endpoint.

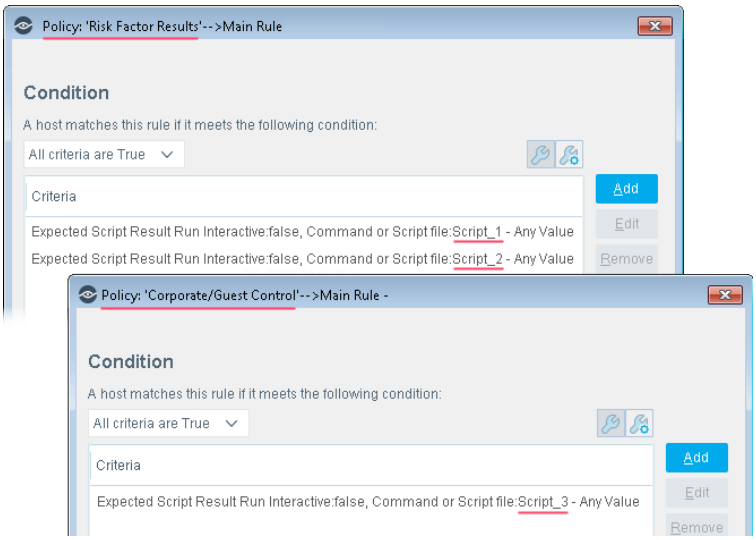
Property Tags for Script-Based Host Properties

One special type of property tag references the value of host properties that are resolved by running a script or command on an endpoint. When you create a policy condition using one of the

following properties, a property tag is generated that lets you include the host property value in action definition fields:

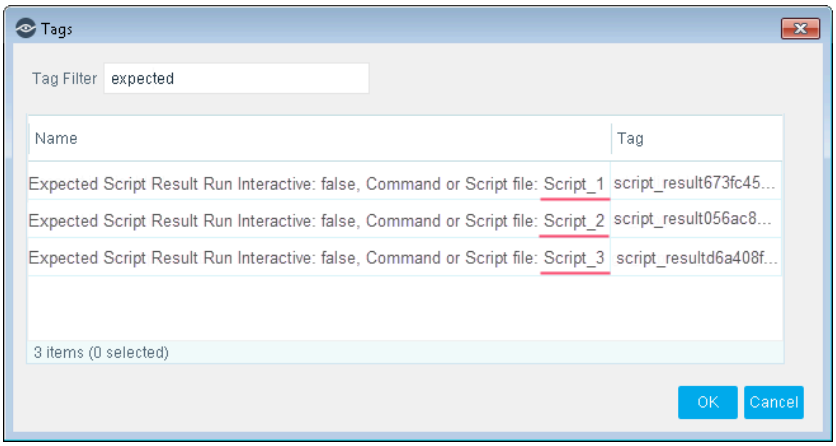
- Windows Expected Script Result
- Linux Expected Script Result
- Macintosh Expected Script Result
- Windows Registry Key Exists
- Windows Registry Key Value

In the following example, two different policies use the Expected Script Result host property to evaluate scripts on an endpoint.



When eyeSight eyeSight evaluates these conditions, it generates and maintains a separate value for each instance of the host property.

eyeSight eyeSight automatically generates property tags that let you reference these values. This tag is retained as long as the related condition is present in active policies.



Action icon display tool

You can choose a time-period in which to display an Action icon after a one-time action is

complete. For example:

- After an email action is performed.
- After network users confirm reading redirected pages.
- After users perform redirecting tasks.

  See Display Action Icon after Action Is Complete for details.

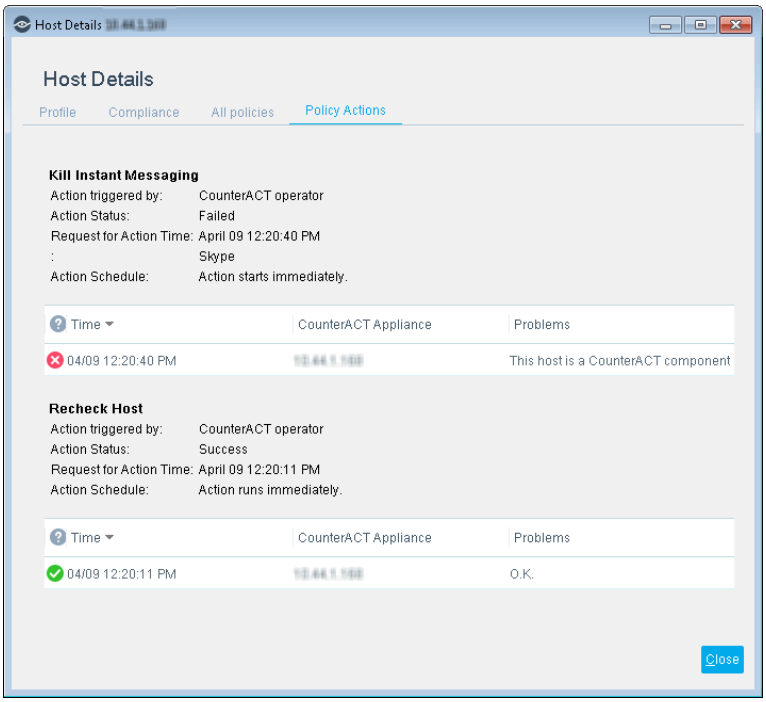
Policy action log

The Host Details dialog box provides specific information about actions carried out on detected endpoints. You can view this information from the Console as soon as the endpoint has been detected via the policy. The information displayed provides more details than presented in the Home view, Detections pane. The dialog box lists the current actions and important related information, such as:

- Details entered in notification actions
- The Appliance that carried out the action
- The time the actions were carried out
- Information indicating the action status

An option is also available to export the log.

To view the Actions log, double-click an endpoint from the Home view, Detections pane. The Host Details dialog box opens. Select the Policy Actions tab.



The dialog box lists basic information about the action that you defined and its details.

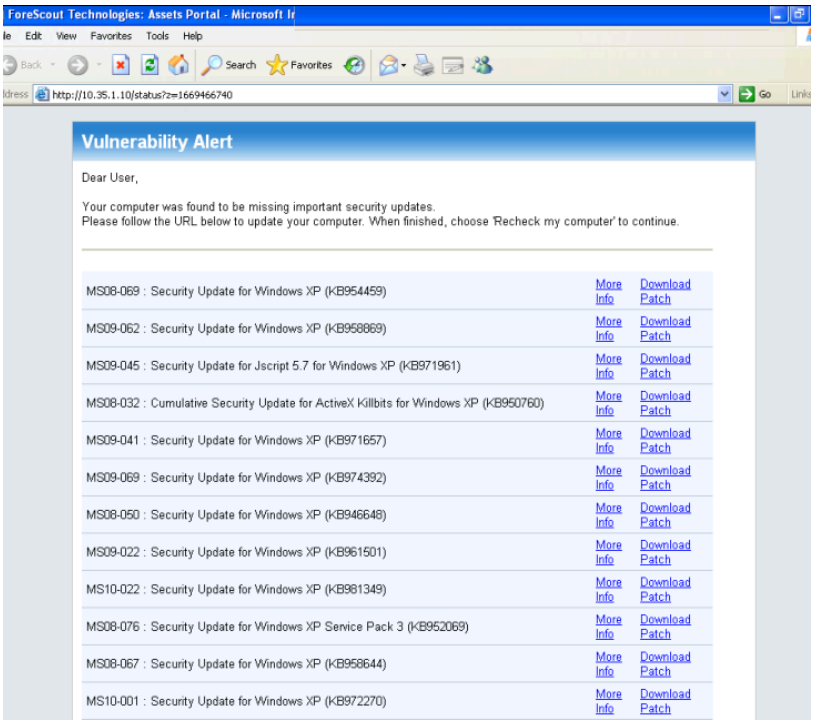
	Indicates whether the action was successful.

Time	Indicates the time the action was carried out.
Appliance	Indicates the Appliance at which the actions were carried out.
Status Details	Indicates whether the action failed.

Right-click the table to export information.

HTTP actions

HTTP actions let you to redirect network user web sessions and replace them with a customized HTTP page. For example, redirect the user's web page and instead display web notification indicating that specific vulnerabilities were detected on their machines. The notification includes a list of links that should be accessed in order to patch vulnerabilities. Users cannot access the web until their endpoint is patched.



Before using the HTTP actions, review the following:

- HTTP actions require that the Appliance sees traffic going to the web.
- HTTP redirection requires proper injection setup. See HTTP Redirection for details.
- If your organization uses a proxy for web connection, you must define the proxy ports to be used. See Policy Preferences for details.
- You can redirect user Intranet sessions. See Defining HTTP Redirect Exceptions for details.
- You can redirect via HTTPS. See Transmitting Actions via HTTPS.
- You can customize the default look and feel of the HTTP pages delivered to the endpoint. For example, you can add your company logo, and define background colors or background images to these pages. See Customizing HTTP Pages for details.

- Messages that appear in the redirected pages can be changed to the language defined at your operating system. See Localize Redirected Web Pages and Messages for details.
- You can customize HTTP preferences to include redirect exceptions that will not be affected by HTTP actions. These exceptions can be configured either globally or per action. See Defining HTTP Redirect Exceptions for details.
- The DNS Enforce Plugin lets eyeSight eyeControl implement HTTP actions in cases where stateful traffic inspection is not possible. This is relevant, for example, with a remote site or an unmanaged network segment. For more information, refer to the *DNS Enforce Plugin Configuration Guide*. To open this guide, select Tools > Options > Modules, then select DNS Enforce and then select Help.

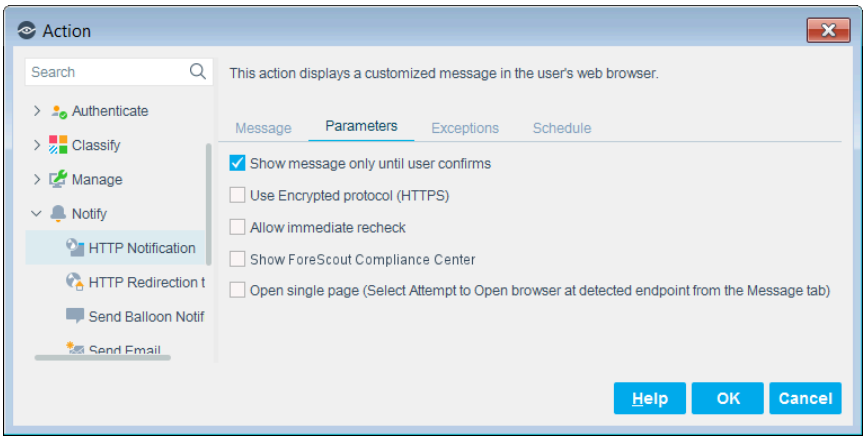
Transmitting actions via HTTPS

You can configure the connection method used for transmitting redirected traffic. Traffic can be transmitted via HTTPS, i.e., encrypted over a secured connection (TLS) or via HTTP.

If you transmit via HTTPS, network users will see a security alert in their web browsers when they attempt to access the web. The alert indicates that the site's security certificate was not signed by a known Certificate Authority (CA). (A default self-signed certificate is installed during product installation.) You can generate a known CA Security Certificate to avoid this situation. See Generating and Importing a Trusted Web Server Certificate and HTTP Redirection for details.

Use HTTPS per action

To send a redirected page via HTTPS, select Use Encrypted protocol (HTTPS) in the HTTP action definition. To send it via the non-encrypted HTTP protocol, clear the checkbox.



Note:
End user redirect pages may include several messages that are the result of different actions. The title bar on the redirected page represents the most secured state. Specifically, if several messages appear on one redirect page, and one of them is the result of a secured action, the title bar shows HTTPS .

Use HTTPS for all actions

Redirected traffic includes information sent to network users via the HTTP actions, as well as authentication credentials sent back to the Appliance. For example, when you use the HTTP Login

action, authentication credentials are sent back to the Appliance using the method that you defined.

See Globally Redirect via HTTPS for details. If you configure the eyeSight to work globally with HTTPS but defined specific actions to be HTTP, redirected traffic is transmitted only via HTTPS.

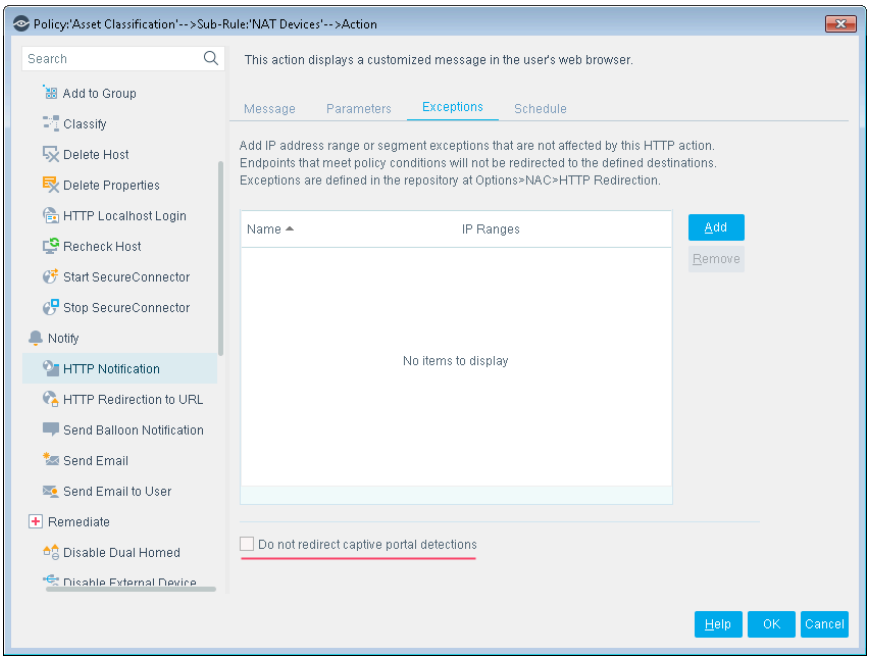
Captive portal detection exceptions

You can allow endpoints running Mac OS/iOS or Android to remain connected to the Internet without being automatically redirected by HTTP actions due to Apple or Android captive portal detection.

When endpoints connect to the network, the endpoint sends periodic requests to determine whether a captive portal is present. The motivation for this is that when using an application other than a web browser (for example, email), endpoint users may not be presented with the portal page and will fail to connect to the Internet. If the periodic request is redirected, the system recognizes that a captive portal is present.

If you want endpoints to *not* be periodically redirected by HTTP actions to a web page that requires user interaction, you can enable the Do not redirect captive portal detections option.

This configuration is applied to individual HTTP actions, in the Exceptions tab of each HTTP action.



This feature supports Apple WISPr and Android captive portal detections and is relevant for the following HTTP actions:

HTTP Redirection to URL

HTTP Login

HTTP Notification

HTTP Localhost Login

Start SecureConnector

Windows Self Remediation

Action thresholds

An action threshold is the maximum percentage of endpoints that can be controlled by a specific action type defined at a single Appliance.

In some scenarios, policy enforcement requires blocking or restricting network devices and users.

Action thresholds are designed to automatically implement safeguards when rolling out such sanctions across your network. Consider a situation in which you defined multiple policies that utilize a blocking action, for example, the Virtual Firewall or Switch Block actions. In a situation where an extensive number of endpoints match these policies, you may block more endpoints than you anticipated.

An action threshold is the maximum percentage of endpoints that can be controlled by a specific action type defined at a single Appliance. By working with thresholds, you gain more control over how many endpoints are simultaneously restricted in one way or another. See Working with Action Thresholds for details.

Configure audit trail logging

Configure which events are audited and logged by the eyeSight using two properties:

- `fs.audit.trail.severity.start.level [1-7]`
- `fs.audit.trail.severity.end.level [1-7]`

Only events within the range specified by `fs.audit.trail.severity.start.level` and `fs.audit.trail.severity.end.level` are logged. The default settings of `fs.audit.trail.severity.start.level 1` and `fs.audit.trail.severity.end.level 7` includes all events. Audit trail level settings also affect the audit log sent to the external Syslog server via the Syslog Plugin. You can change the Audit trail severity levels via the `fstool set_property` command.

The audit trail severity level settings are:

1	Alert
2	Critical error
3	Error
4	Warning
5	Warning

5	Notice
6	Information
7	Debug - default

To configure the range for one event, in this example, Information messages, set the start and end levels to the same value as follows:

1. In the Enterprise Manager, log in to the CLI.
2. Set the start level with the following command: **fstool set_property fs.audit.trail.severity.start.level 6**

   Note:
   To set the audit trail level values on all appliances that the Enterprise Manager manages preface the command with `fstool oneach -c` as in `fstool oneach -c fstool set_property fs.audit.trail.severity.start.level [1-7]`.

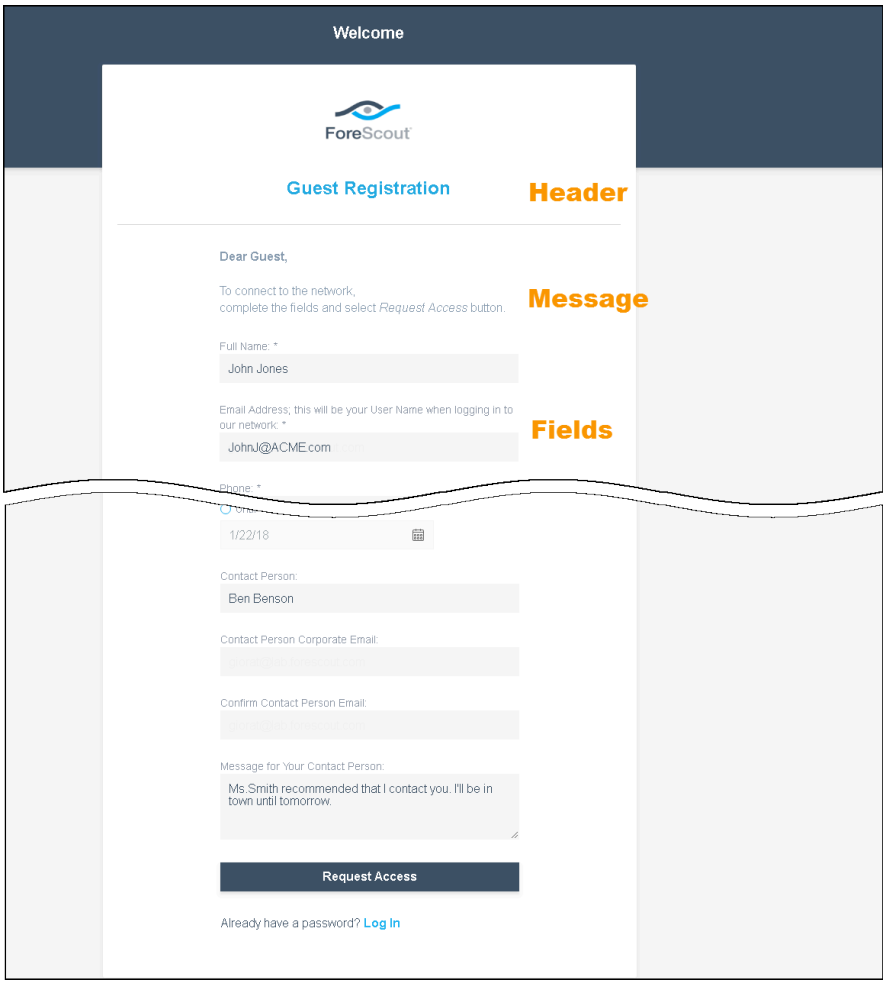
3. Set the end level with the following command: **fs.audit.trail.severity.end.level 6**

Now only Information messages are visible and sent to the server.

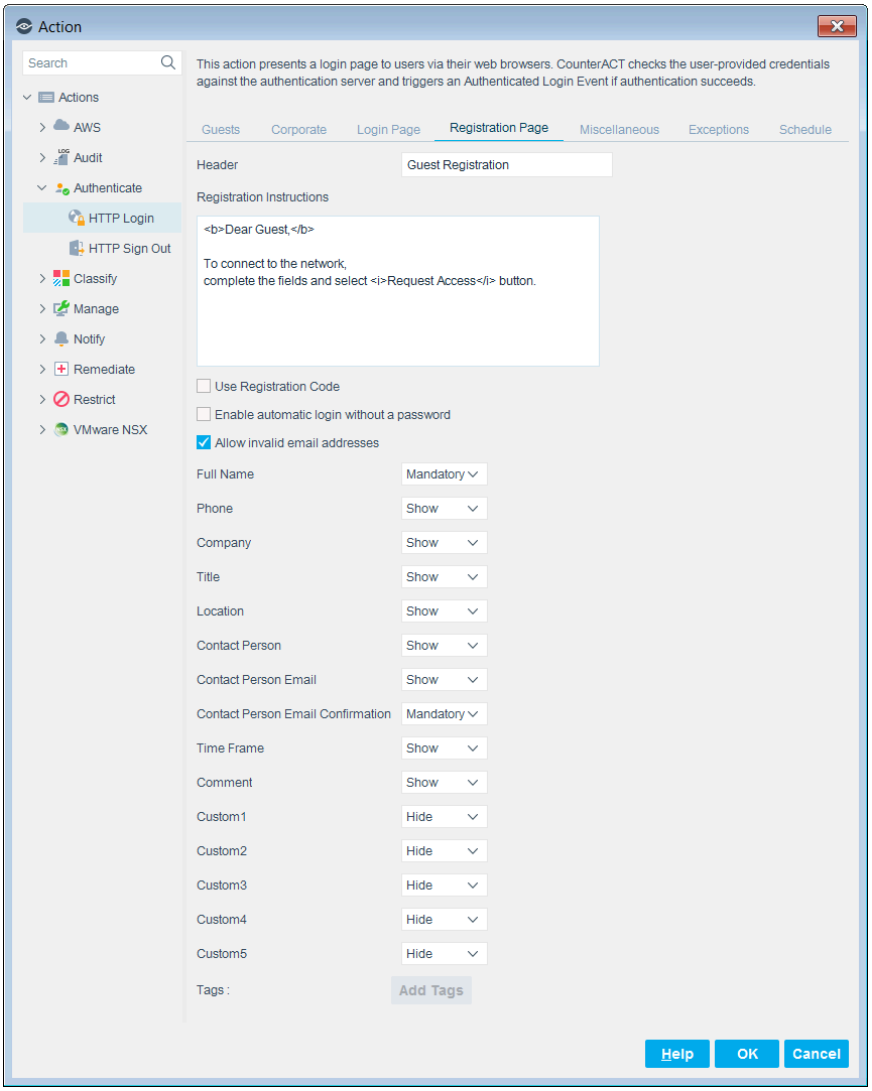
Registration page tab

The information in the Registration Page tab is only used if guest registration is enabled in the Guests tab.

Use the Registration Page options to design the Guest Registration form.



- Define the title and message that appears in the Guest Registration form.
- Define the form fields that you want guests to use.
- (Optional) Require guests to enter a registration code to begin the registration process.



To design the Guest Registration form:

1. In the Header field, define a Guest Registration form title.
2. In the Registration Instructions text box, define the message to appear on the page.
3. Select Use registration code to require guests to enter a registration code before beginning the registration process. This ensures that only guests with whom you've shared a registration code can apply for network access. These codes are automatically generated, but they must be shared with endpoint users manually. See Retrieving Registration Codes.
4. Select Enable automatic login without a password if you want to allow users to log in without a password. When this option is selected, there is no authentication.
5. The Email field is always mandatory, and guests are identified by its contents.
    - Clear the Allow invalid email addresses checkbox to ensure that this field contains a valid email address.
    - In environments where users are identified by information other than their email address, select Allow invalid email addresses so that any value is accepted in the Email field.

      Note:

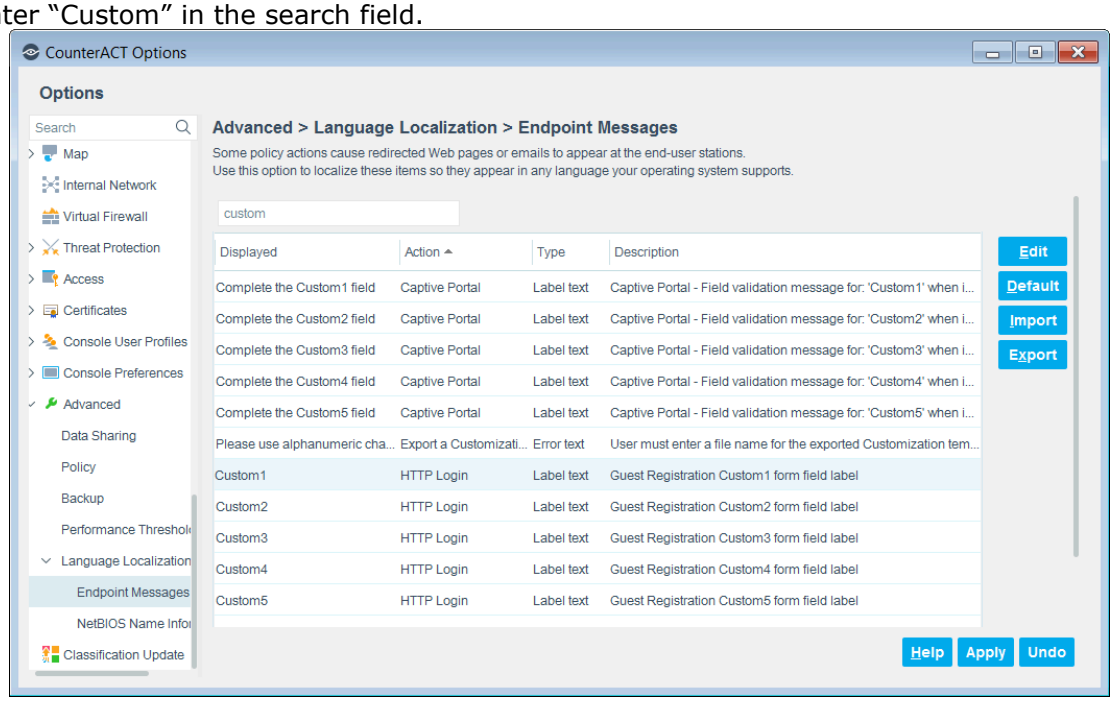
      To ensure that only one guest identification field is displayed in the Guest Registration form, it is recommended to set the Full Name drop-down menu to Hide whenever Allow invalid email addresses is selected. For

each field in the list, select one of the following:
- Hide: The field is not displayed in the registration form.
- Show: The field is displayed in the registration form and is optional.
- Mandatory: The field is displayed in the registration form, and the user must enter a value.

6. If tags are defined in your environment, you can add tags to the registration form. The available fields include five custom fields that you can configure. For example, Custom1 might be renamed Building Name to indicate the name of the building where the guest will be located.

   To assign custom names:

7. Select Tools > Options from the Console menu, and then select Advanced > Language Localization > Endpoint Messages .
8. Enter "Custom" in the search field.



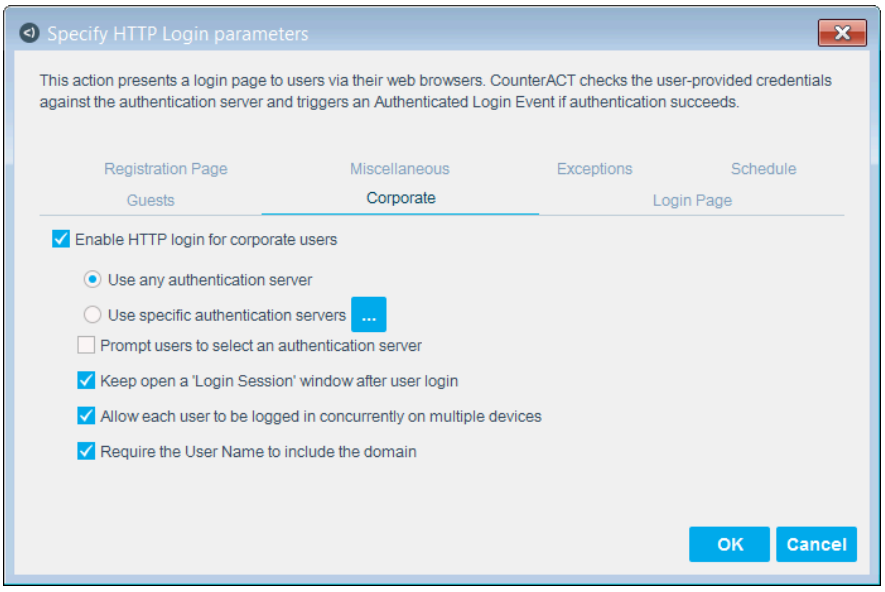
9. Edit the fields as required, select Close, and then select Apply.

Corporate tab

Use the Corporate tab to define which servers are used for domain authentication, as well as other authentication settings.

Before configuring corporate users, you must have already configured User Directory servers. Typically, this configuration is performed when setting up the Console using the Initial Setup Wizard.

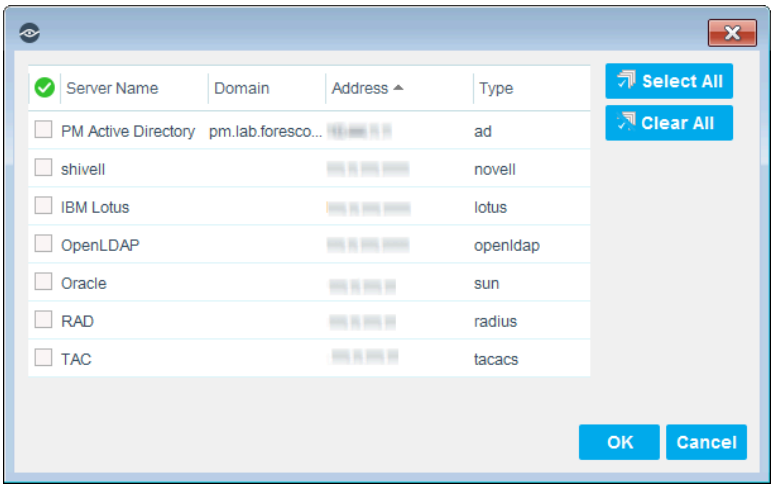
To see which servers are defined, select Tools > Options. See Initial Setup Wizard – User Directory for details.



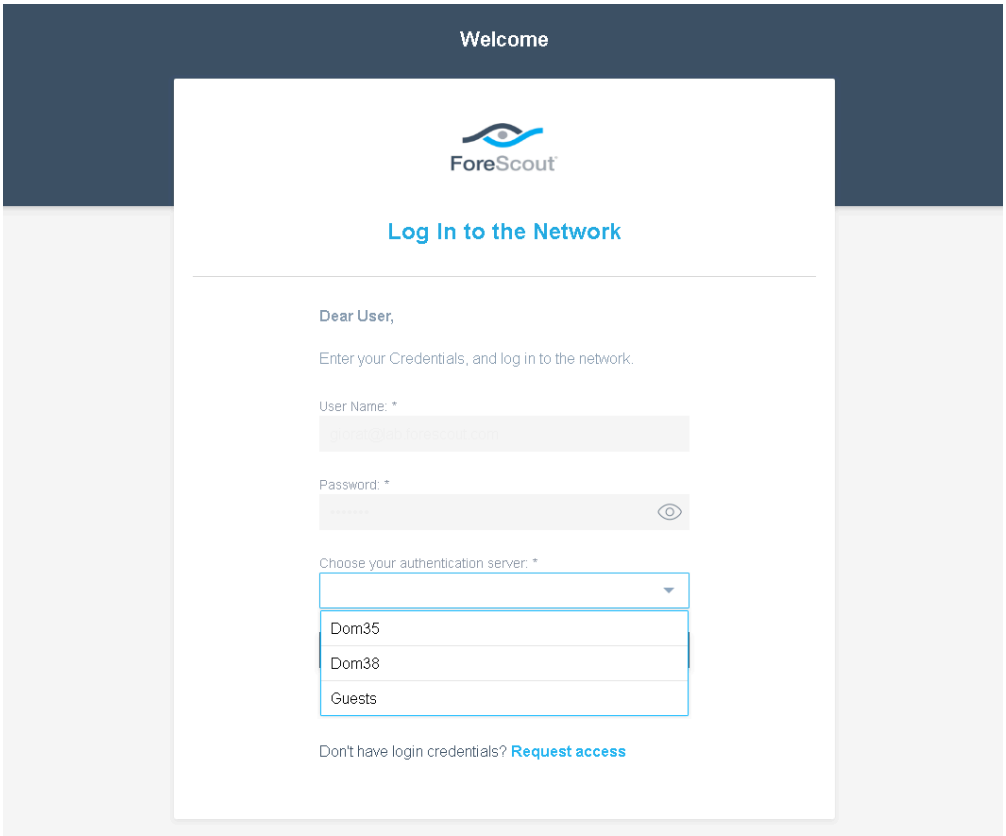
To enable corporate user authentication against an authentication server, select Enable HTTP login for corporate users.

To allow authentication against any of the authentication servers defined in the User Directory Plugin, select Use any authentication server.

To authenticate users against specific servers, select Use specific authentication server and then browse to and select those servers.



To allow the endpoint user to select a server against which to authenticate, select Prompt users to select an authentication server. When this option is selected, the Login page displays a Domain drop-down menu, from which the endpoint user can select a domain.



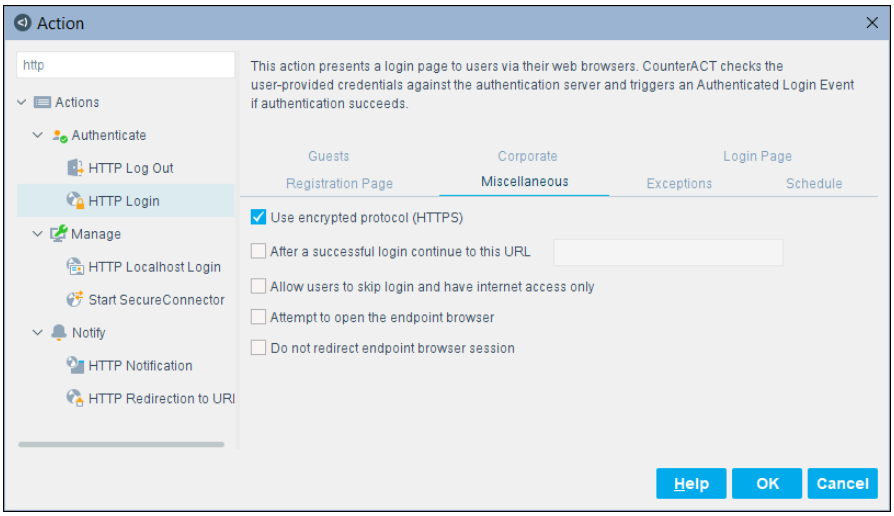
To display a Forescout Login Session window for corporate users, select the Keep open a 'Login Session' window after guest login option. The user must keep this window open to maintain a network to Internet connection, provided this access was granted in the policy. During this time, the Authentication, Signed In Status property for the endpoint is resolved as Signed In as a Domain User.

Control the number of machines a single user can log in to concurrently. Select Allow each guest to be logged in concurrently on multiple devices to allow multiple logins. If this option is not selected, a second login by the same user closes the first session on the original computer.

Select Require the User Name to include the domain to require corporate users to include the domain in the login page User Namet field.

Miscellaneous tab

Use the Miscellaneous tab to configure additional user login parameters.



Use encrypted protocol (HTTPS)

It is recommended to select Use Encrypted protocol (HTTPS) to send the Login page via HTTPS. To send it via the non-encrypted HTTP protocol, clear the Use Encrypted protocol (HTTPS) checkbox. See Transmitting Actions via HTTPS for details.

Direct user to a predestined site after successful login

To force the user to begin browsing at a specific website, such as your corporate home page, select After a successful login continue to this URL and enter the URL.

Allow user to skip login

If you think login credentials may not be available to users, and you want them to have browsing access, select Allow the user to skip login and have internet access only. When selected, the Login page includes a guest link option.

Attempt to open a browser at the endpoint

You can define the action to automatically open a browser at the endpoint, instead of waiting for the user to browse. This ensures that the HTTP message gets to the network user faster. Select Attempt to open the endpoint browser. (This option is for managed machines only, and is not available for Windows 2000 and Windows 2003 Server machines.) Forescout eyeControl uses a script when this option is selected.

Do not redirect endpoint browser session

If the previous option Attempt to open the endpoint browser is selected together with this option, the Login page opens as a new page. If the Attempt to open the endpoint browser option is not selected together with this option, endpoint users must right-click the desktop SecureConnector taskbar icon, and select View Compliance Center to view the page. Hosts must be managed.

Customize HTTP Login Action Text

You can customize text that the HTTP Login action generates at the user endpoint. These texts appear in re-directed HTML pages that are generated at endpoints of users who attempt to access the corporate network.

In the Endpoint Messages pane, customize any of the HTTP Login action texts. In the pane, identify HTTP Login action texts by any one of the following Action column entries:

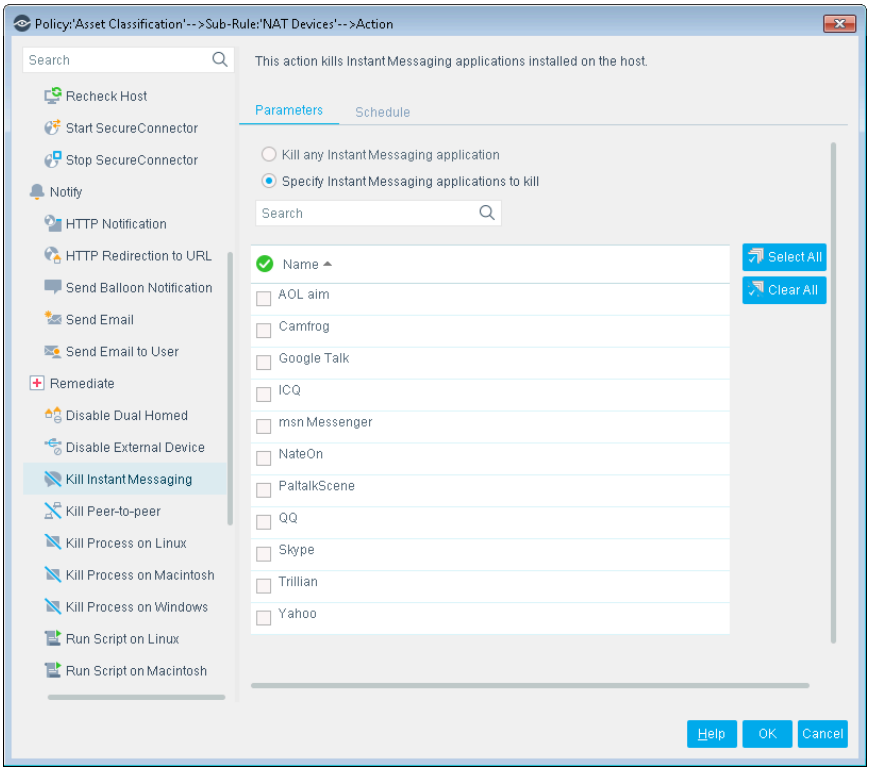
- Guest verification code...
- HTTP Login (with or without other values)
- HTTP Login mobile

For details about customizing texts that appear to endpoint users, see Localize Redirected Web Pages and Messages.

Kill instant messaging

The Kill Instant Messaging action halts specific instant messaging applications that are running on Windows endpoints.

The Windows Applications Plugin provides updates to the applications supported by this action. Refer to Windows Applications Configuration Guide for more information about the module. Select Tools > Options > Modules, then select Windows Applications, and then select Help.



By default, the application is killed once a minute. If the endpoint has SecureConnector installed it is killed once a second. You can automatically install SecureConnector on endpoints when this action is applied.

To install SecureConnector:

1. Select Tools > Options > HPS - Inspection Engine.
2. Select the SecureConnector tab.
3. Select SecureConnector.
4. Select Automatically run SecureConnector on Windows endpoints....

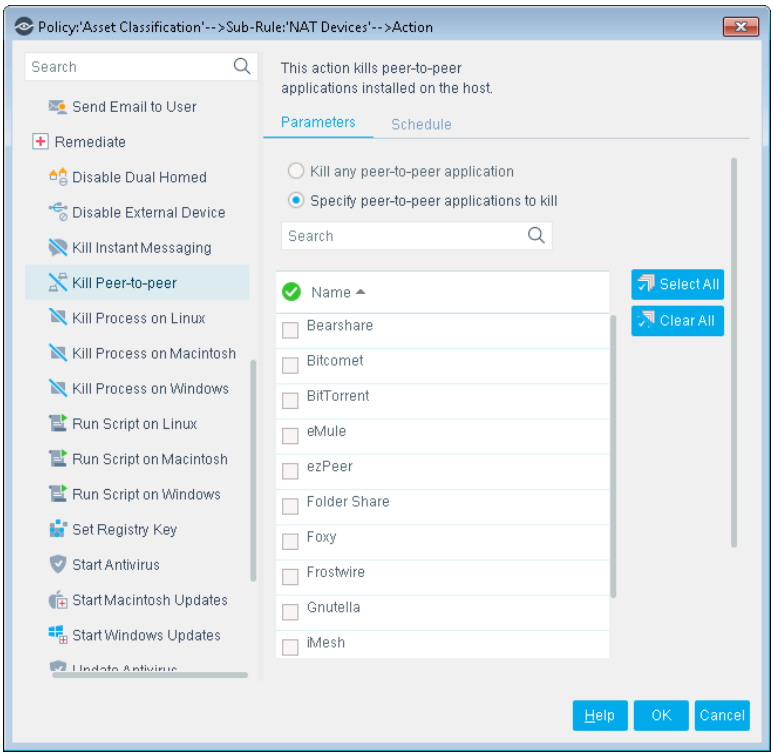
5. Select Apply and select Close.

   Note:

   Forescout eyeControl uses a script on the endpoint to apply this action if the endpoint is managed via domain credentials (Windows Manageable (Domain) is True). Refer to the *HPS Inspection Engine Configuration Guide* for details about scripts. Select Tools > Options > Modules, then select this plugin, and then select Help.

Kill peer-to-peer

The Kill Peer-to-Peer action stops specific peer-to-peer applications installed on Windows endpoints.



By default, the application is killed once a minute. If the endpoint has SecureConnector installed it is killed once a second. You can automatically install SecureConnector on endpoints when this action is applied.

To install SecureConnector:

1. Select Tools > Options > HPS - Inspection Engine.
2. Select the SecureConnector tab.
3. Select Automatically run SecureConnector on Windows endpoints….
4. Select Apply and then select Close. The Windows Applications Plugin provides updates to the applications supported by this action. Refer to the *Windows Applications Configuration Guide* for more information about the module. Select Tools > Options > Modules, then select Windows Applications, and then select Help.

   Note:

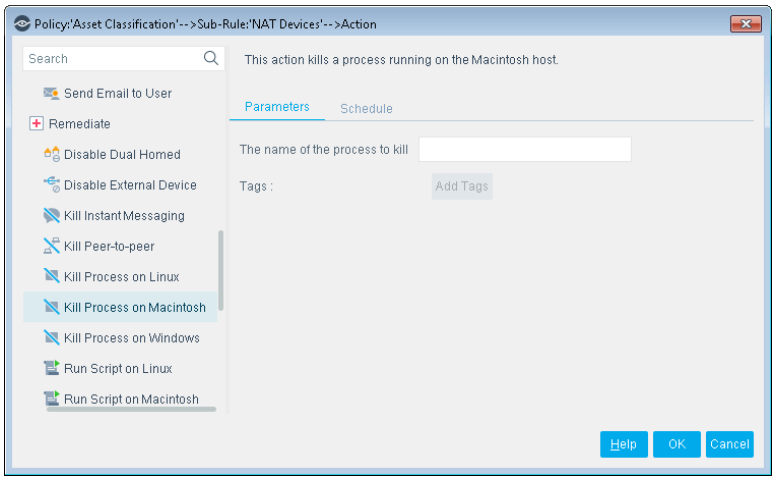
   eyeSight eyeControl uses a script on the endpoint to apply this action if the endpoint is managed via domain credentials (Windows Manageable (Domain) is

True). Refer to the *HPS Inspection Engine Configuration Guide* for details about scripts. Select Tools > Options > Modules, then select this plugin, and then select Help.

Kill process on Linux and kill process on Macintosh

These actions stop specific Linux and Macintosh processes. The process is killed once per second. To carry out this action, the endpoint must be connected to via SecureConnector.

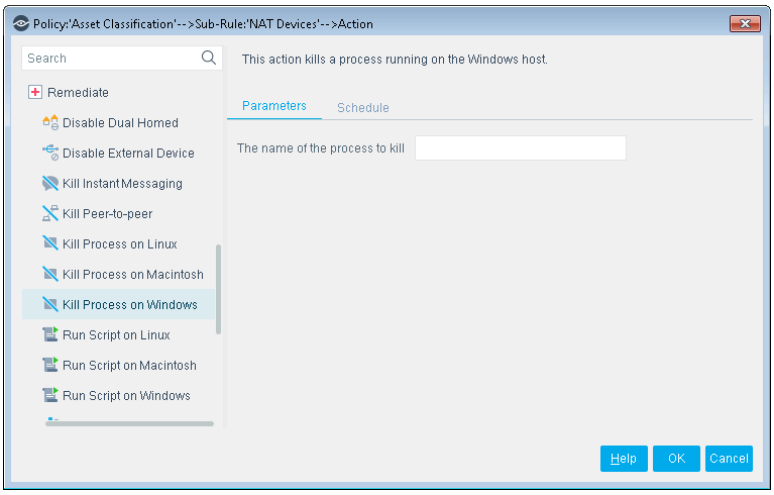
If the process name includes endpoint-specific or user-specific data such as the user name, you can add it as a variable by inserting a tag. For example, if you enter the {user} tag, the user name of the endpoint is automatically inserted into the process name. See Property Tags for details. Depending on the endpoint operating system, and how the endpoint is managed, this action is implemented by the Linux Plugin, or the OS X Plugin.



Kill process on Windows

use this action to halt specific Windows processes.

If the process name includes endpoint-specific or user-specific data such as the user name, you can add it as a variable by inserting a tag. For example, if you enter the {user} tag, the user name of the endpoint is automatically inserted into the process name. See Property Tags for details.



By default, the process is killed once a minute. If the endpoint has SecureConnector installed, it is killed once a second.

You can automatically install SecureConnector on endpoints when this action is applied.

Quickly find the endpoints with the process you are looking for by using the Windows Processes Running property.

To install SecureConnector when using this action:

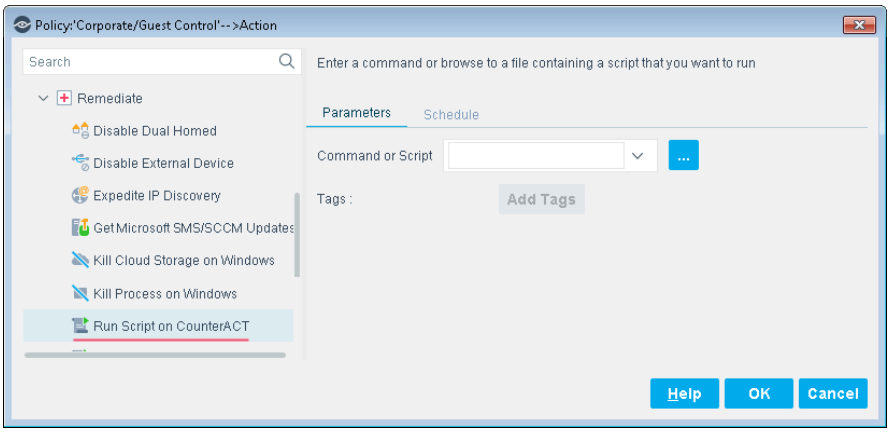
1. Select Tools > Options > HPS - Inspection Engine.
2. Select the SecureConnector tab.
3. Select Automatically run SecureConnector on Windows endpoints….
4. Select Apply and then select Close.

Note:

eyeSight eyeControl uses a script on the endpoint to apply this action if the endpoint is managed via domain credentials (Windows Manageable (Domain) is True). Refer to About the HPS Inspection Engine in the *HPS Inspection Engine Configuration Guide* for details about scripts. Select Tools > Options > Modules, then select this plugin, and then select Help .

Run script on CounterACT

The Run Script on CounterACT action runs a script or command for endpoints that match the conditions of the policy. This action is located in the Remediate group of the Actions tree.



Forescout eyeControl evaluates the script or command for each endpoint that matches previous conditions of the policy.

Note:
If you are running a script in an action, the `{IP}` tag must be added to the script by the Administrator if it is required as an argument.

Select the Schedule tab to apply scheduling options to this action.

Run script on Linux and run script on Macintosh

You can create a custom policy to use scripts to

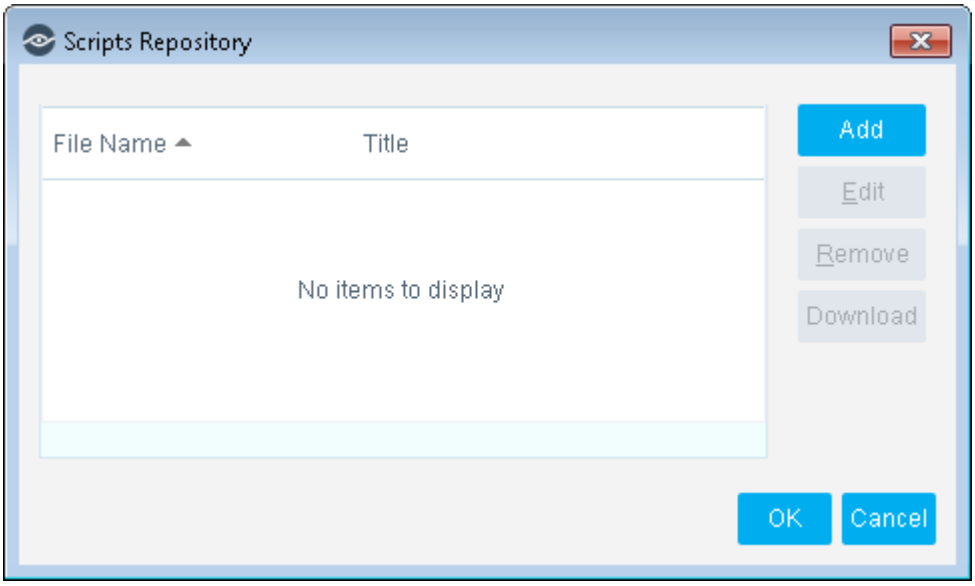
- Automatically run Macintosh and Linux updates.
- Automatically deploy vulnerability patches.
- Automatically delete files.
- Create customized scripts to perform any action that you want.
- Select the file transfer protocol (SFTP or SCP).

For example, to prevent music sharing, use these actions to run the following command on endpoints:

```
net share "my music"/delete
```

Depending on the endpoint operating system, and how the endpoint is managed, this action is implemented by the Linux Plugin or the OS X Plugin.

1. Specify a command or script to run on endpoints. Do one of the following:
   - Enter a command in the Command or Script field. To run a file that already exists on the endpoint, enter its absolute path. You can use property tags to include endpoint-specific or user-specific values in this field.
   - Select Continue to select from the repository of user-defined scripts and commands.



2. Specify the following optional behaviors, if required.

Run interactive (Macintosh endpoints)	Select this option to run the specified command or script interactively on Mac OS X endpoints. On endpoints managed by the OS X Plugin using SecureConnector, prompts are displayed to the currently logged in user in a terminal

	window. Refer to the OS X Plugin Configuration Guide for details.
Run script as root user on endpoint (Linux endpoints)	Select this option to run the specified script using root user privileges on Linux endpoints. Select this option when a script requires root privileges, but root credentials are not used to access the endpoint. To use this option the `sudo` utility must be enabled on Linux endpoints. When sudo mode is password protected, you must configure a password that lets the Forescout platform enter sudo mode. Refer to the *Linux Plugin Configuration Guide*.

3. Specify the file transfer protocol command to use. Your can choose either **scp** and **sftp**s

Run script on Windows

This action is used to achieve automated, centrally managed remediation across the network. Leverage scripts, for example, to:

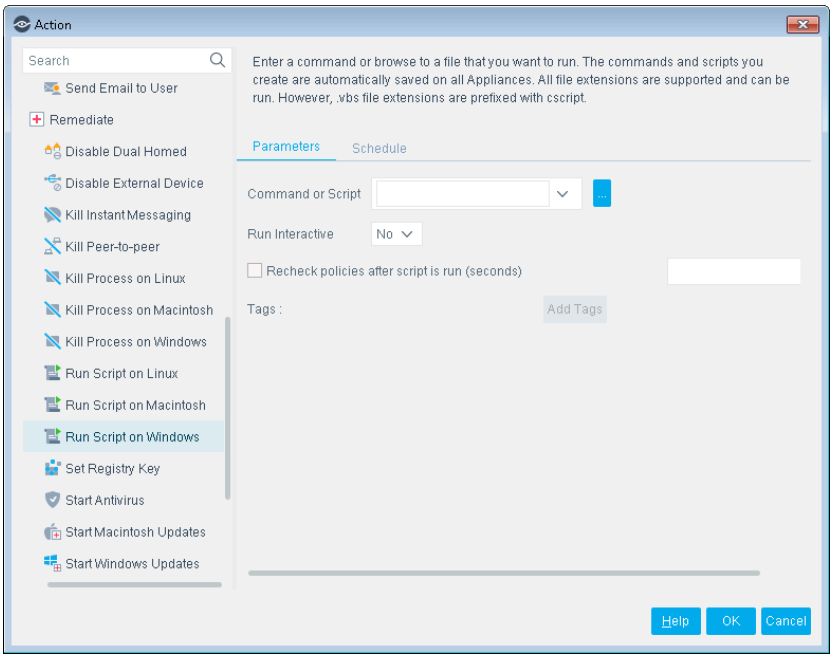
- Automatically run Windows updates.
- Automatically deploy vulnerability patches.
- Automatically delete files.
- Automatically deploy antivirus updates.
- Create customized scripts to perform any action that you want.

:

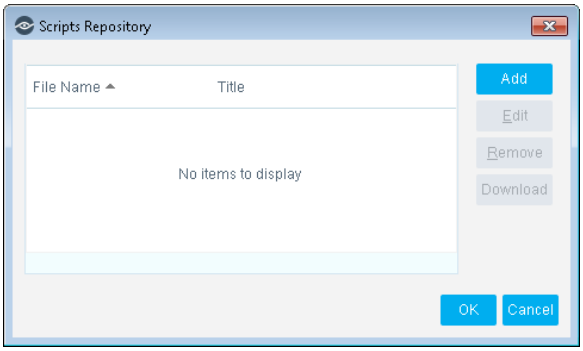
Note:
This action may only be used on managed Windows machines.

To run script on Windows:

- Select Yes from the Run Interactive drop-down menu if the script launches a process or dialog box at the endpoint.
  Note:
  The Terminal Services service must be running if interactive scripts are used. If you use this action and it fails, the service may have been stopped.



- Enter a command or browse to a file that you want to run. If you use a file that exists on the endpoint, enter its absolute path. The commands and scripts that you create are automatically saved on all Appliances. All file extensions are supported and can be run. You can also run `Powershell` scripts. However, VBS file extensions are prefixed with `cscript`.
- You can create a repository of scripts and apply them as needed. Select the browse button from the Parameters tab to manage the scripts you created.



- Quickly recheck endpoints after they are remediated by the script. Select Recheck policies after script is run (seconds) and indicate how many seconds to wait before carrying out the recheck.

  Note:

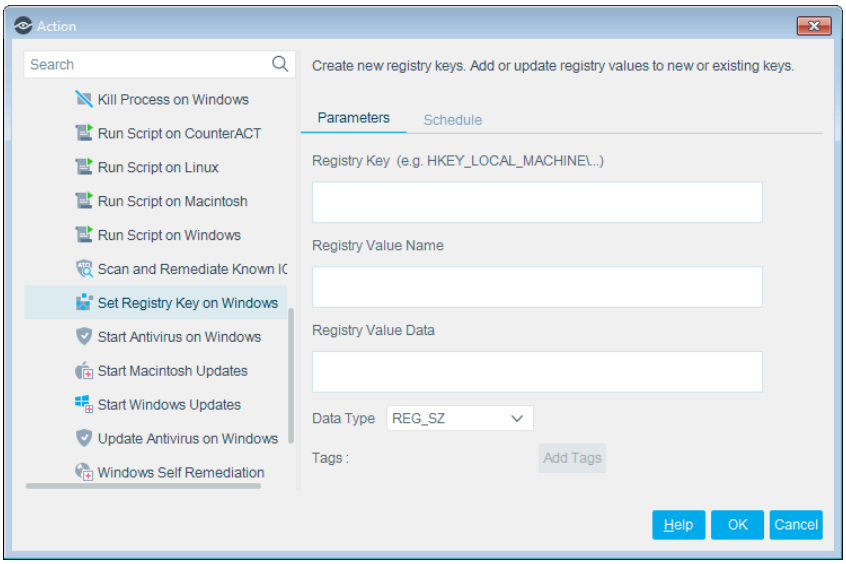
  eyeSight eyeControl uses a script on the endpoint to apply this action if the endpoint is managed via domain credentials (Windows Manageable (Domain) is True). Refer to About the HPS Inspection Engine in the *HPS Inspection Engine Configuration Guide* for details about scripts. Select Tools > Options > Modules, then select this plugin, and then select Help .

Set registry key on Windows

Create registry keys and add or update registry key values and data.

The following data types are supported:

- REG_SZ
- REG_BINARY
- REG_DWORD
- REG_EXPAND_SZ
- REG_MULTI_SZ



Registry Keys

Note:
Forescout eyeControl cannot set the registry key under "`HKEY_LOCAL_MACHINE`" unless permissions on the relevant registry key are set to everyone/full control.

Note:
eyeSight eyeControl uses a script on the endpoint to apply this action if the endpoint is managed via domain credentials (Windows Manageable (Domain) is True). Refer to About the HPS Inspection Engine in the *HPS Inspection Engine Configuration Guide* for details about scripts. Select Tools > Options > Modules, then select this plugin, and then select Help .

For most supported data types, enter a single value in the Registry Value Data field.

The REG_MULTI_SZ data type accepts multiple values. To define a list of values, press Enter so that each value occupies its own line in the Registry Value Data field.

To concatenate two lines, add the string `__fsln__` before you press Enter. For example, when the following text is entered in the Registry Value Data field, three key values are added:

- `aaa`
- `bbb__fsln__`
- `ccc`

- ddd

When the action implements this text, it defines the following Registry key values:

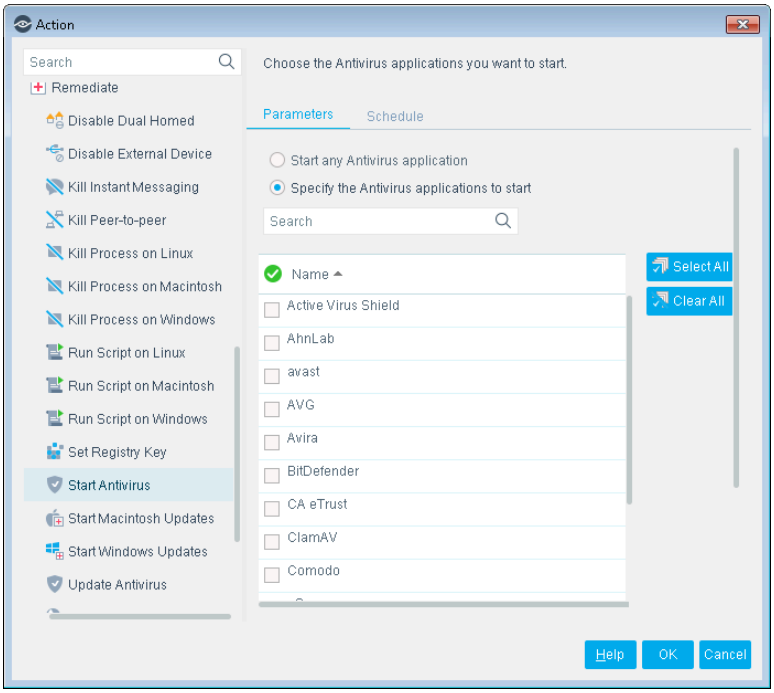
- aaa
- bbbccc
- ddd

The strings bbb and ccc are separated by an end-of-line character.

Note:
The string _a_fsln__ begins and ends with two underscore characters.

Start antivirus

Use the Start Antivirus action to launch antivirus applications that have been halted at Windows endpoints..



The Windows Applications Plugin provides regular updates to the applications supported by this action.

Suppress Splash Screens for Background Installation

As an option, you can choose to suppress the splash screen that is presented to end users by some vendors' installation/upgrade packages. This allows the action to implement silent, background installation of selected Antivirus packages on the endpoint.

Note:
This option is available for users working with Symantec, McAfee, and Trend Micro.

To suppress splash screens for the Update Antivirus action, log in to an Appliance command-line

interface (CLI) and run the following command:

```
fstool set_property config.av_non_interactive_mode.value <vendor>
```

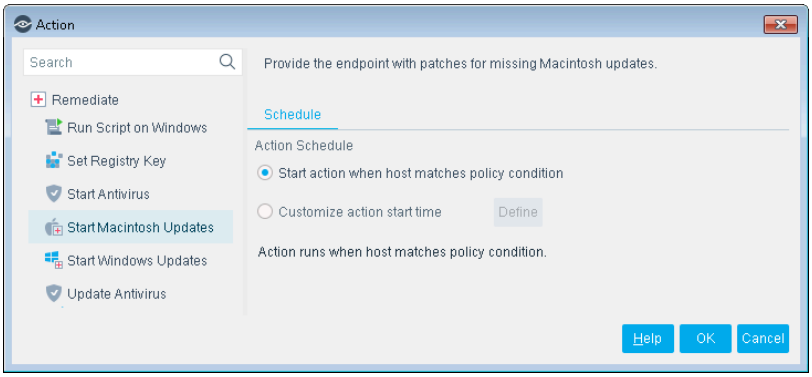
Where `<vendor>` is either Symantec, McAfee or Trend Micro.

Start Macintosh updates

The Start Macintosh Updates action lets you provide the endpoint with patches for missing Macintosh updates. It displays a notification to end users indicating that specific security and other updates are missing on their machines. The notification includes a list of links that should be accessed in order to install the updates.

Use the action in policies that have incorporated the Macintosh > Macintosh Software Updates Missing property. This indicates which software updates are missing on the endpoint.

Depending on the endpoint operating system, and how the endpoint is managed, this action is implemented by the Linux Plugin or the OS X Plugin.



The Software Update page continues to display at the endpoint after all the patches have been installed. The page, however, is empty. You can stop or disable the action if you do not want an empty Software Update page to appear.

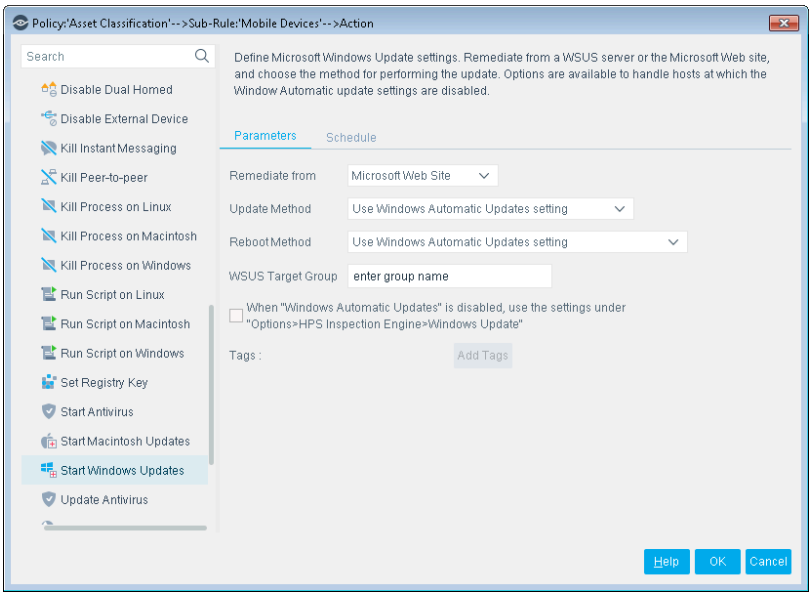
Start Windows updates

The Start Windows Updates action uses the standard Microsoft system for vulnerability remediation. It causes Microsoft software to assess the endpoint's vulnerabilities, decide which patches are required, and download and install the patches.

This action removes the need to manage the vulnerabilities of new endpoints before they connect to the network. It can automatically bring all new endpoints into vulnerability compliance when they connect to the network and keep them compliant.

You can also minimize bandwidth usage during Microsoft vulnerability patch download. See Minimize Bandwidth Usage During Microsoft Vulnerability Patch Download..

Use this action in policies that have incorporated the Windows Security>Microsoft Vulnerabilities property and the Windows Security>Windows Update Agent Installed property.



To work with this feature, you must define:

- A remediation server to work with
- An update method

Remediation Server

Microsoft remediation can be done via the Microsoft website or via a Microsoft WSUS server.

Microsoft Website

Remediation via the website requires connectivity to the Internet. For more information about these methods, refer to the Microsoft website.

WSUS Server

Remediation via WSUS requires connectivity to the WSUS server. You can also enter a WSUS Target Group name. This enhances update performance.

When using WSUS, consider the following:

- In addition to setting up the WSUS server, you must define the WSUS environment parameters in the HPS Inspection Engine (see below).
- When the Start Windows Updates action is performed on an endpoint, the WSUS parameters are permanently defined in the endpoint registry.
- You can clear the Apply WSUS settings parameter to avoid having the WSUS parameters defined in the endpoint registry. If you do this, be aware that if the endpoint's WSUS settings are not defined correctly, the endpoint will not be remediated.

To define WSUS environment parameters:

1. Select Tools > Options > HPS Inspection Engine.
2. Select the Windows Update tab.
3. Enter the URL of the WSUS server and the reports server.

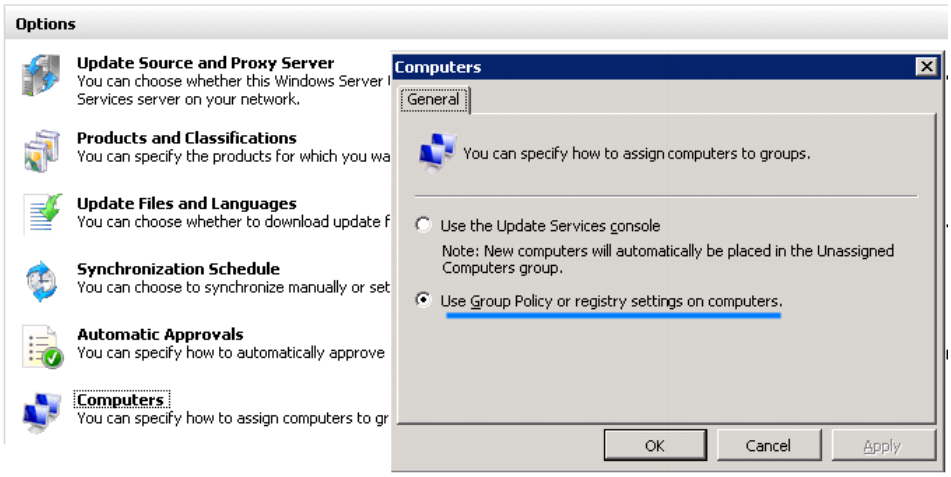
You can test connection with the server by selecting Test.

- Select Apply and then select Close.

Configuration in the WSUS Server

You can configure WSUS target groups to enhance update performance. To work with this feature, you must perform the following configuration in the WSUS server console.

1. Open the WSUS server console.
2. Select Options.
3. Select Computer.
4. Select Use Group Policy or registry settings on computer.



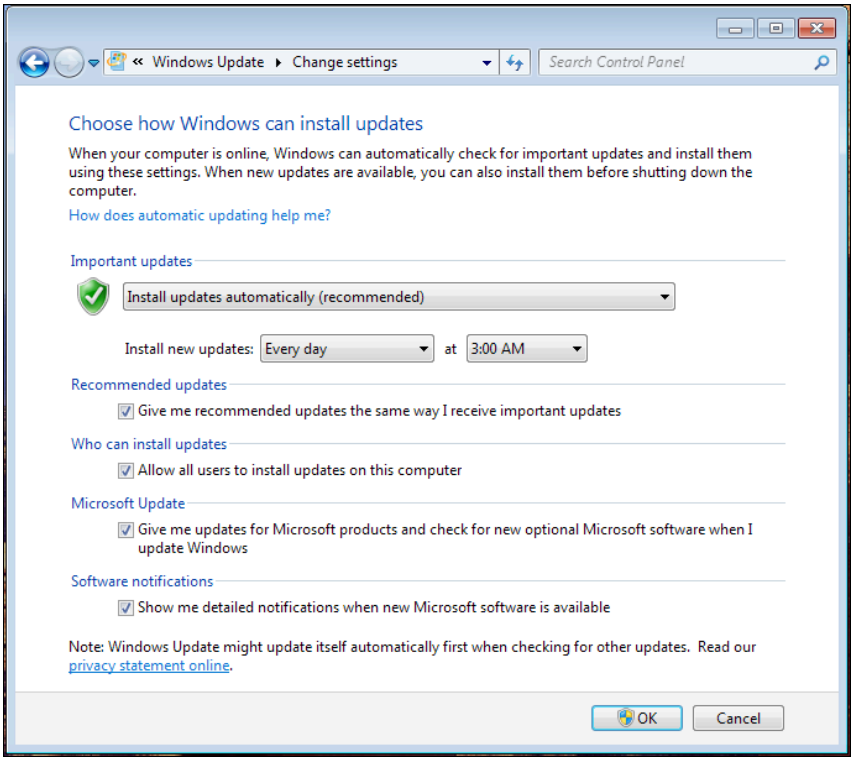
Update Methods

Three methods are available. Changes made at the endpoint as a result of the method selected here are kept permanently on the endpoint.

Automatically Download and Install	The patches are downloaded without user notification or interaction.
Automatically Download and Notify of Installation	The endpoint user is notified that updates are available. The endpoint user can either update immediately or wait till later. Some patches may require machine reboot; in this case, machine is rebooted according to endpoint settings. The Windows Automatic update may have been defined to let the user decide which patches to install.
Use Windows Automatic Update Settings	The Windows Automatic Update settings are used to determine how the update is performed. In a scenario where Turn off Automatic Updates is configured on the Windows Endpoint and the update method is defined as Use Windows "Automatic Updates" Settings, the action will not be carried out. To force the update, see

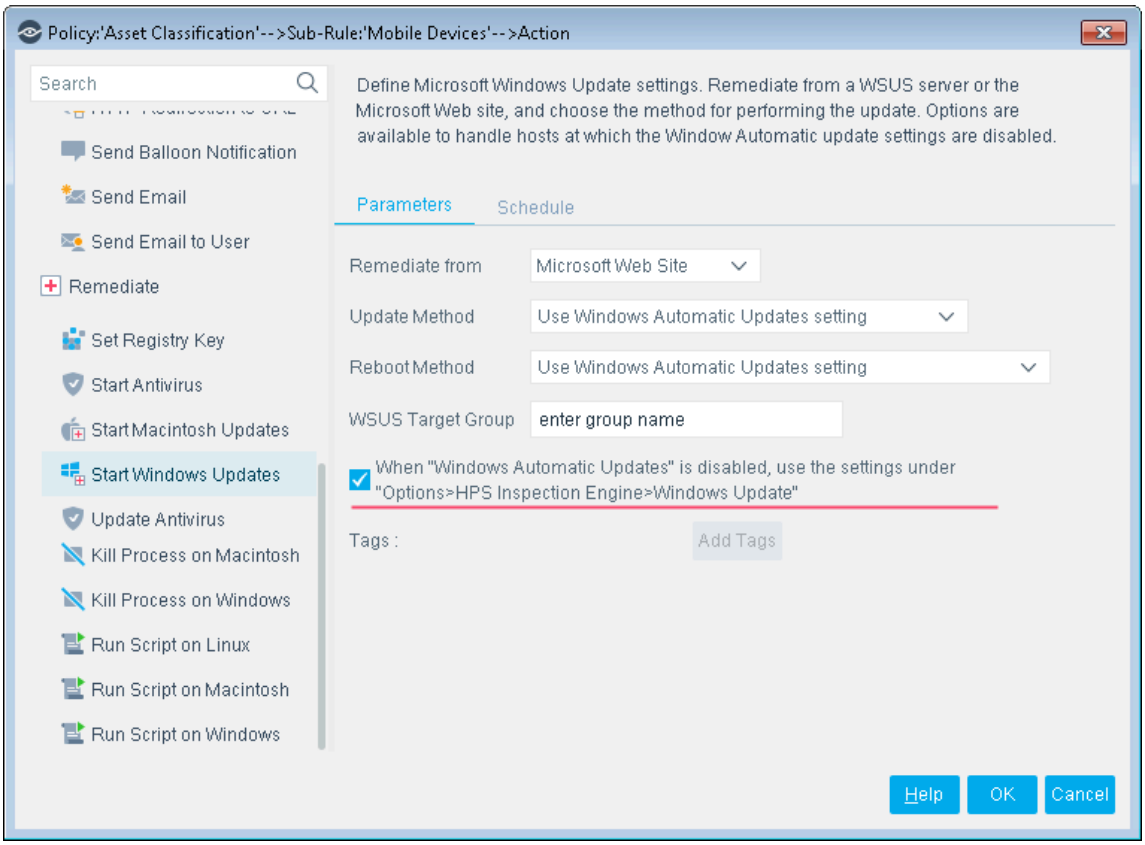
How to Handle Updates when Windows Automatic Updates Are Turned Off

If Turn off Automatic Updates is configured on the Windows endpoint, the Use Windows "Automatic Updates" Settings action is not carried out. Nonetheless, you can force the update by implementing the following configurations.

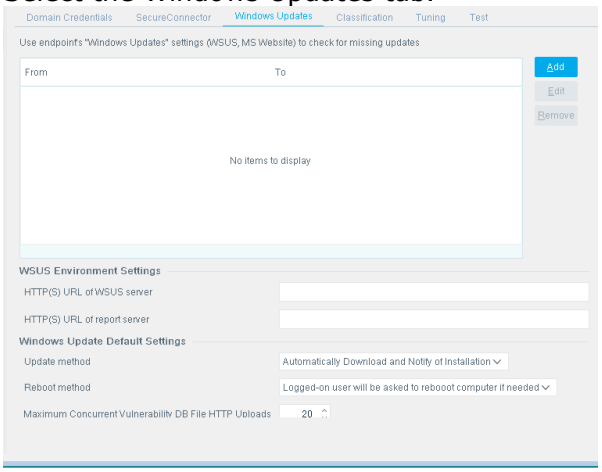


To force Windows automatic updates:

1. In the Windows Updates Dialog Box, select When 'Windows Update' is disabled. If the checkbox is cleared, and this scenario exists, the action is not carried out.



2. In theHPS Inspection Engine configurationpane.
    a. Select Options from the Tools menu and then select HPS Inspection Engine.
    b. Select the Windows Updates tab.



    c. In the Windows Update Default Settings section, select the Update Method to use. The following options are available:
        - Automatically Download and Install
        - Automatically Download and Notify of Installation

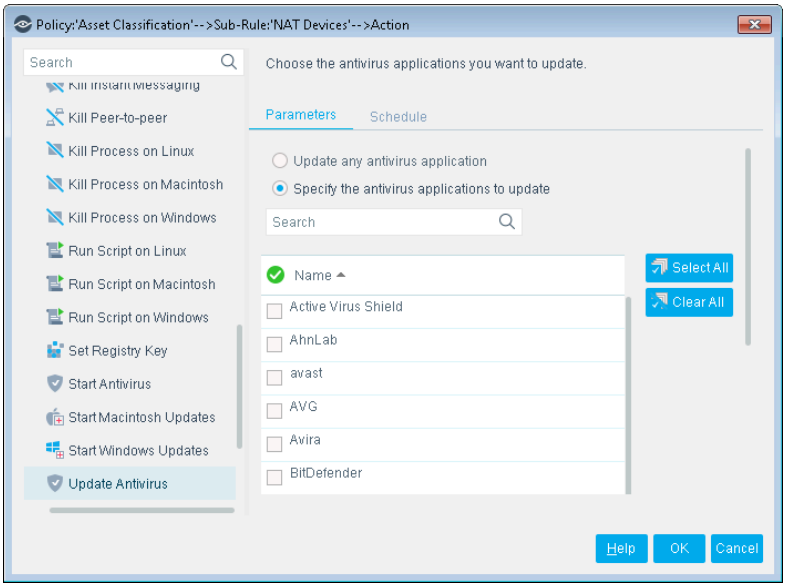
Minimize Bandwidth Usage During Microsoft Vulnerability Patch Download

The Windows Vulnerability DB provides Microsoft vulnerability updates to Appliances. The plugin works by pushing Microsoft vulnerability update information to the HPS Inspection Engine installed on Appliances. These updates are used when working with vulnerability policies and are downloaded at the endpoint.

Users can reduce network bandwidth during this process by limiting the number of concurrent HTTP downloads to endpoints. By default, the maximum is 20.

Update antivirus

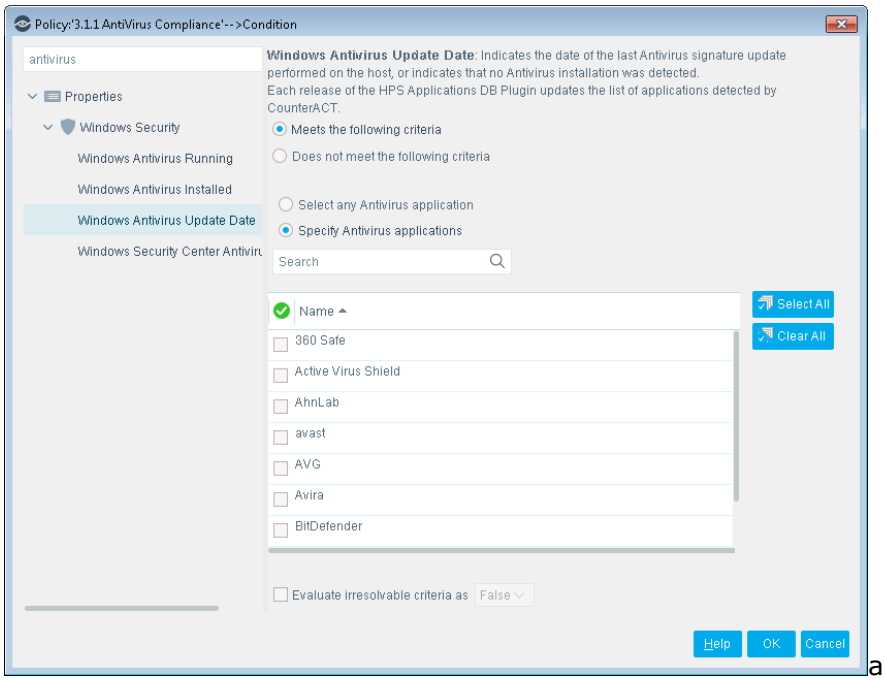
The Update Antivirus action updates outdated antivirus applications at Windows endpoints.



You may need to select more than one vendor if you think different antivirus vendors are installed on the same endpoints in the policy scope. This setup is not recommended. If more than one vendor is installed on the same endpoint, the update will only be run on one.

Note:
Forescout eyeControl uses a script on the endpoint when carrying out this action if the endpoint is managed via domain credentials Manageable (Domain). Refer to About the HPS Inspection Engine in the *HPS Inspection Engine Configuration Guide*. for details about how scripts work. Select Tools > Options > Modules, then select this plugin, and then select Help.

The Windows Applications Plugin provides updates to the vendor applications supported by this action. Refer to the *Windows Applications Configuration Guide* for a detailed list of supported applications. Select Tools > Options > Modules, then select Windows Applications, and then select Help.


a

Windows self remediation

The Windows Self Remediation action delivers web notification to network users indicating that specific vulnerabilities were detected on their machines.

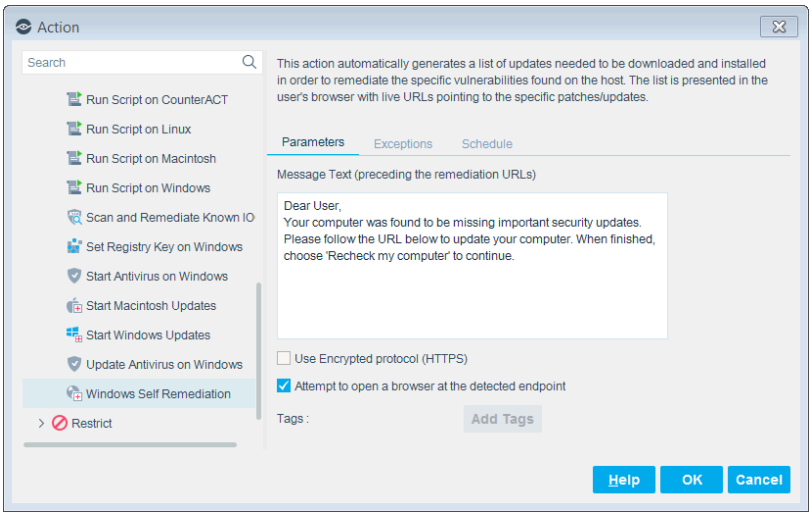
The notification includes a list of links that should be selected by the endpoint users in order to patch vulnerabilities. Users cannot access the web until their endpoint is patched. The process for verifying this is automated when the endpoint is rechecked. An option is also available for the user to run the recheck directly from the web page.

Remediation patches are automatically be downloaded in the language supported by the endpoint operating system. Messages that appear during the remediation process are displayed in the local language as well.

Note:
Automated remediation is also available. See Start Windows Updates .

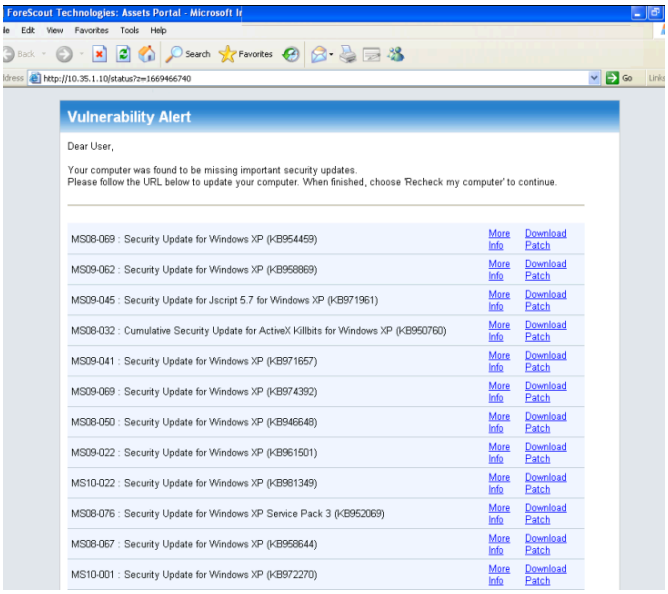
Note:
Use the manual option if you want endpoint users to have more control over patching vulnerabilities on their machines.

Note:
Windows Self Remediation is not accessible when HTTP Redirection is disabled. For details, see Disable Web Portals .

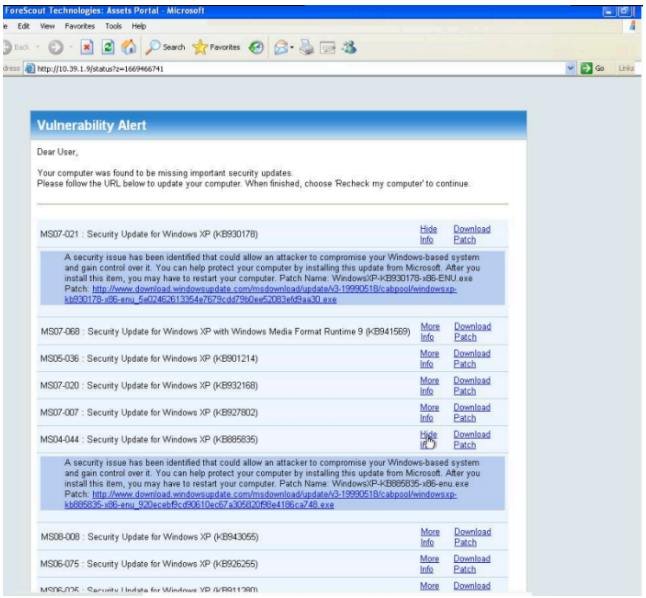


It is recommended to select Use Encrypted protocol (HTTPS) to send the redirected page via HTTPS. To send it via the non-encrypted HTTP protocol, clear the Use Encrypted protocol (HTTPS) checkbox. See Transmitting Actions via HTTPS for details.

You can define the action to automatically open a browser at the endpoint instead of waiting for the user to browse. This ensures that the message gets to the user faster. Select Attempt to open a browser at the detected endpoint. (This option is unavailable for Windows 2000 and Windows 2003 server machines, and for unmanaged machines.) eyeSight eyeControl uses a script when this option is selected and the endpoint is managed via domain credentials. Refer to About the HPS Inspection Engine in the *HPS Inspection Engine Configuration Guide*. for details about scripts.



Network users can select the More Info link to review details about the vulnerability detected.



Network users can select the Recheck my Computer link to immediately recheck the status of their computer. If the required files are not downloaded and rechecked, redirection continues.

Recommended Conditions

When using this action, you should configure the following condition property:

- Windows Security>Microsoft Vulnerabilities>Meets the following criteria

The required patches are automatically listed for the vulnerabilities selected here.

Users cannot access the web until one of the following happens:

- Remediation is complete.
- The endpoint is released via the Home view, Detections pane or Assets Portal.

Local Patch Path

By default, the eyeSight continuously displays patch links that reside on the Microsoft website. An option is available, however, to define a local server from which to centrally manage your patch updates. You may want to do this if you are using customized patch packages. If necessary, you can also restore to the original Microsoft path.

To change the path:

1. Define a location on a local server from which to download the patches.
2. Log in and run the following command:

   ```
   fstool convert_patch_path
   ```

3. The following prompt is displayed

   ```
   This fstool replaces vulnerabilities patches from %root%/patch to
   %user_root%/patch.If necessary, it can also restore original
   patches.Input parameters: [restore | replace <user_root>]
   ```

: `fstool convert_patch_path replace` http://server1/patches

eyeSight Base modules, Content modules, and eyeExtend modules

eyeSight Base Modules, Content Modules, eyeSegment Module, and eyeExtend modules significantly expand the scope of the eyeSight's network inspection, data exchange, remediation and control.

Information obtained from these modules is incorporated into Forescout tools used for creating policy properties and actions, generating reports and inventory items, and more.

The Check for Updates feature automatically checks if the most recently released module versions are installed on your Devices. This saves you the trouble of checking for updates manually.

Forescout eyeSight Base modules

Base Modules enhance eyeSight visibility, network connectivity, detection, and control capabilities. Base Modules are delivered with each eyeSight release. Upgrading the Forescout version or performing a clean installation installs these modules automatically.

Note:
Additional modules are available to legacy customers who had them installed in earlier versions, such as the Router Blocking Module, Cisco PIX/ASA Firewall Integration Module, and NetFlow Plugin.

Authentication module

Plugin Name	Details
RADIUS	Ensures seamless, comprehensive 802.1X pre-connect security and post-connect control for wired and wireless devices, and both corporate and guest users.
User Directory	Resolves endpoint user details via a User Directory server. Enables a variety of other features for handling network guests and the sponsors who approve guest access to the network.

Core Extensions module

Plugin Name	Details
Active Probing	Uses active discovery techniques to support endpoint classification. Use of multiple information sources enhances and sharpens Forescout device classification, and supports related functionality such as risk assessment.
Admin API	Provides automatic configuration capabilities for managing deployments on the Forescout eyeSight, where network entities, such as the segment tree and default groups ranges, can change on a daily basis.
Advanced Tools Plugin	Provides host properties and actions that enhance and extend existing functionality. For example: More detailed endpoint detection. Enhanced use of commands and scripts to retrieve endpoint information. Use of labels and counters to implement complex policy logic, and to retain endpoint status across policy rechecks.
CEF Plugin	Sends policy compliance and other host information detected by Forescout eyeSight to SIEM systems using the CEF messaging format. SIEM servers can trigger remediation actions by sending alert messages to the Forescout eyeSight. This functionality uses the alert messaging function common to most SIEM servers, and non-CEF-standard text messages.
Cloud Classification Gateway	Queries an external information resource for endpoint classification information. Use of multiple information sources enhances and sharpens Forescout device classification, and supports related functionality such as risk assessment.
Cloud Uploader	Compresses data from Forescout devices and uses encrypted protocol to send the compressed data to cloud services where the data is processed and analyzed.
Dashboards	Web-based information center that provides a real-time overview of the network and delivers dynamic at-a-glance information about: Device visibility Device compliance Forescout policy data
Data Publisher	Gathers device policy information from Appliances in your Forescout deployment and sends it to the Data Receiver. This information is used by the Device Compliance Dashboard, an out-of-the-box dashboard included in the Dashboards view.

Plugin Name	Details
Data Receiver	Receives and stores device policy information sent from the Data Publisher. This information is used by the Device Compliance Dashboard, an out-of-the-box dashboard included in the Dashboards view.
Device Classification Engine	By comparing the values of endpoint properties with the profiles in the Device Profile Library, this engine can resolve classification-related properties for comprehensive endpoint classification.
Device Data Publisher	Collects device information from Appliances in your Forescout deployment and sends it securely to The Forescout Research Program. This program helps Forescout improve the security platform effectiveness.
DHCP Classifier Plugin	Extracts host information from DHCP messages. This information complements information sources used by Forescout eyeSight, such as the HPS Inspection Engine and Nmap queries.
DNS Client Plugin	Resolves the DNS host name of a given IP address. The DNS Name property stores the name returned by the DNS server.
DNS Enforce Plugin	Implements HTTP-based policy actions, such as HTTP Notification and HTTP Redirection to URL, in cases where stateful traffic inspection is not possible. This is relevant, for example, with a remote site or an unmanaged network segment.
DNS Query Extension Plugin	Views traffic via the monitor interface (SPAN port), and detects and parses DNS messages in the network that reference specific host names. Determines whether a given endpoint in the network is a DNS server. Checks DNS lookups of specific domain names by endpoints in the network.
External Classifier Plugin	Accesses a set of MAC addresses maintained in an FTP server or an LDAP server to: Assigns a configured text label to any host whose MAC address matches a MAC address in the retrieved set. Uses the assigned text label in a policy to follow up with required actions.
Flow Analyzer	Detects flow information regarding the endpoints in your environment. It collects a statistical sampling of data about network traffic in your environment, such as average packet size, average packet rate per second, inbound and outbound bandwidth usage, and DNS resolutions.
Flow Collector	Analyzes the traffic flows exported by network devices, and reports flow session data that is used to resolve endpoint properties. The flow session data can also be used by other

Plugin Name	Details
	Forescout modules.
IOC Scanner Plugin	Leverages the threat detection and threat prevention mechanisms of third-party systems with the network visibility and enforcement capabilities of Forescout.
IoT Posture Assessment Engine	Assesses the security risk associated with IoT devices based on their use of weak login credentials.
NBT Scanner	Obtains the user information of any user that is logged in to a given host, as well as the MAC address of that host. Discovers the NetBIOS name of the host, based on port 137 traffic on the network. It is installed and started by default. Various policy and Assets Portal features do not work properly if the plugin is stopped.
Packet Engine	Provides network visibility by deploying real-time port mirroring in the network.
Reports	Generates reports with real-time and trend information about policies, host compliance status, vulnerabilities, device details, assets, and network guests. Reports help keep network administrators, executives, the Help Desk, IT teams, security teams, or other enterprise teams well-informed about network activity.
Syslog Plugin	Sends, receives, and formats messages to and from external Syslog servers.
Technical Support Plugin	Automatically analyzes an extensive range of log files on your system and send them to the Forescout Customer Care team for further investigation. Analysis of log files is carried out on a wide range of issues, for example, service restarts, database issues, plugin errors, issues dealing with policies, internal processes, reports, or any other issue occurring on your Forescout system.
Web Client Plugin	Delivers the Forescout Web Client, which hosts the following web-based tools: Dashboards. See Dashboards for details. Assets. See Assets View for details. Segmentation (eyeSegment). See eyeSegment Module for details.

Endpoint module

Plugin Name	Details
HPS Agent Manager	Performs background functions to support the endpoint discovery and management activities of the Endpoint Module.
HPS Inspection Engine	Accesses Microsoft Windows endpoints. Performs comprehensive, deep inspection for the purpose of resolving an extensive range of endpoint information. Activates a variety of Forescout actions to manage, remediate or control endpoints.
Hardware Inventory Plugin	Extends the host properties discovered by the HPS Inspection Engine to include physical hardware devices, endpoint configuration settings, and related information such as serial numbers.
Linux Plugin	Manages endpoints running Linux operating systems. The plugin supports properties, actions, and other management functionality for Linux endpoints.
Microsoft SMS SCCM Plugin	Retrieves and displays advertisement and report information related to SMS/SCCM hosts in the Console. Updates SMS/SCCM clients with new advertisements, and updates the SMS/SCCM server with new host information.
NBT Scanner Plugin	Obtains information for the user that is logged in to a given endpoint and the MAC address of that endpoint.
OS X Plugin	Manages endpoints running Mac/OS X operating systems. The plugin supports properties, actions, and other management functionality for Linux endpoints.

Hybrid Cloud module

Plugin Name	Details
AWS	Provides visibility of EC2 instances, VPCs, IAM Users/Roles, and S3 buckets in Amazon’s public cloud Enables you create and apply Forescout policies Maintains security of cloud services Enforces compliance on endpoints

Plugin Name	Details
Azure	Provides visibility of Azure instances, VNets, local network gateways, and subscriptions in Azure's public cloud Lets you create and apply Forescout policies Maintains security of cloud services Enforces compliance on endpoints
VMware NSX	Allows control functionality for virtual endpoints that are part of the data center managed by VMware vCenter® and VMware NSX. Using the capabilities offered by this integration, you can apply micro-segmentation on virtual machines (VM) based on user-defined security policies.
VMware vSphere	Supports detailed discovery and management of endpoints that are Virtual Machines in vSphere environments.

Network module

Plugin Name	Details
Centralized Network Controller	Enables you to monitor Cisco Meraki, Juniper Mist Wireless, Cisco ACI, and Fortinet cloud-managed networks. The integration enables discovery of endpoints connected to these networks. .
Network Controller Plugin	Monitors centrally managed network solutions to discover (detect) endpoints that connect to centrally managed, network devices and to report endpoint and network device information in the Console. Current integrations include Cisco Meraki, Ruckus SmartZone and Arista CloudVision. Allows users to apply eyeSight eyeControl actions (subject to specific vendor integration) on connected, targeted endpoints.
Network Controller Content Plugin	Supplies product definitions about centrally managed network solutions to the Network Controller Plugin. Each product definition enables Network Controller Plugin integration with the relevant vendor solution to both monitor the centrally managed network and apply actions on connected, targeted endpoints.
Rogue Device Plugin	Continuously monitors Switch Plugin-managed switches to identify suspicious MAC spoofing events occurring to endpoints that are connected to these switches. Identifies suspicious events regardless of whether the involved endpoints are located on (connected to) the same managed switch or two different, managed switches.

Plugin Name	Details
	Allows users to apply a eyeSight eyeControl action on connected, targeted endpoints.
Switch Plugin	Tracks the location of endpoints connected to network switches and retrieves relevant switch information. Quickly detects new endpoints on the network. Assigns switch ports to VLANs; you can set up dynamic, role-based VLAN assignment policies and quarantine VLANs. Uses ACLs to open or close network zones, services, or protocols for specific endpoints at a switch and handle scenarios that address broader access control.
Switch Content Plugin	Supplies product definitions about vendor network devices (L2/L3 Switches, Layer 3 Devices) to the Switch Plugin. Each product definition enables Switch Plugin integration with a vendor's network device(s) to both manage these devices and apply actions on connected, targeted endpoints.
VPN Concentrator Plugin	The VPN Concentrator Plugin is used to track VPN users, disconnect them from the VPN and prevent them from reconnecting. Blocking is carried out by communicating with multiple VPN devices and an authentication server.
Wireless Plugin	Provides NAC capabilities to wireless network controllers and access points for the purpose of controlling wireless endpoints connected to them.

Operational technology module

Supports OT/IoT applications and ICS/SCADA automation environments. The module integrates the traffic inspection and protocol analysis capabilities of the Forescout eyeInspect solution with eyeSight eyeSight and eyeControl. This yields enhanced discovery, classification, and assessment for the full spectrum of IT and OT endpoints.

Content Modules

Content Modules deliver data that is used by other Modules for classification, inspection, and control. For example, the Windows Applications Module delivers host properties and actions used by the HPS Inspection Engine to support in-depth discovery and management of software and applications on Windows endpoints.

Module Name	Details
Deep Packet Inspection Plugin	Uses deep packet inspection techniques to passively audit the network traffic to support endpoint classification and compliance assessment on the eyeSight.

Module Name	Details
Device Profile Library	A library of pre-defined device classification profiles, each composed of properties and corresponding values that match a specific device type. Each profile maps to a combination of values for function, operating system, and/or vendor and model. The Device Classification Engine uses this information to provide the best possible classification for the device.
Visibility Content	Provides updated protocols, fingerprints, and device profiles used by the Active Probing Plugin and the Deep Packet Inspection Plugin. These updates enhance device visibility and classification capabilities.
Windows Vulnerability DB	Makes vulnerability updates available to the eyeSight soon after they are released from Microsoft. These updates are used when working with vulnerability policies.
IoT Posture Assessment Library	Delivers a library of pre-defined login credentials that are used by the IoT Posture Assessment Engine to aid in determining the security risk of devices.
NIC Vendor DB	Works with the HPS Inspection Engine to map Network Interface Controllers to their vendors based on their MAC address. Delivers host properties that let you detect and manage endpoints based on this information.
Switch Content	Supplies product definitions about vendor network devices (L2/L3 Switches, Layer 3 Devices) to the Switch Plugin. Each product definition enables Switch Plugin integration with a vendor's network device(s) to both manage these devices and apply actions on connected, targeted endpoints.
Windows Applications	Delivers host properties and actions used by the HPS Inspection Engine to support in-depth discovery and management of software and applications on Windows endpoints.
Security Policy Templates	Security policy templates use existing eyeSight functionality to detect, evaluate, and respond to vulnerabilities and threats – speeding and simplifying your network response. When you install this plugin, templates are available in the Policy view of the Console.

eyeSight eyeSegment module

eyeSight 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 eyeSight 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 eyeSight 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 eyeSight eyeSegment policy rules.
- Visualize the policy rules as a layer in the matrix, and ensure that devices are not managed by conflicting rules.
- Export details about selected traffic for further study.

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

The eyeSight eyeSegment Module requires a valid eyeSegment license. See License Management for the relevant licensing requirements and to learn more about licensing modes.

eyeSight eyeExtend modules

Note:
In Per-Appliance Licensing mode, eyeSight eyeExtend modules are referred to as Extended Modules in the user interface.

eyeSight eyeExtend modules expand eyeSight capabilities by sharing contextual device data with third-party systems and by automating policy enforcement across those disparate systems. Organizations can bridge previously siloed security solutions to accelerate system-wide response and more rapidly mitigate risks.

eyeSight eyeExtend modules require valid licenses. License requirements for eyeExtend modules differ depending on the licensing mode your Forescout deployment is using. See License Management for the relevant licensing requirements and to learn more about licensing modes.

Access eyeSight eyeExtend module software downloads and related documentation from the Customer Support Portal, Downloads Page.

Advanced Threat Detection (ATD)

ATD eyeSight eyeExtend modules provide security orchestration between the eyeSight and your ATD system. The combined solution lets you automatically detect indicators of compromise (IOCs) on your network and quarantine infected devices, thereby limiting malware propagation and

breaking the cyber kill chain. eyeExtend modules in this category include Check Point Threat Prevention, FireEye NX, and Palo Alto Networks WildFire.

Client Management Tools (CMT)

Forescout's CMT eyeExtend modules provide visibility and control across network-connected devices, including corporate devices, while they are off the enterprise network. They also verify device compliance with security and regulatory mandates and take remediation actions. eyeSight eyeExtend modules in this category include eyeSight eyeExtend for HCL BigFix.

Endpoint Protection, Detection, and Response (EPP/EDR)

eyeSight EPP/EDR eyeExtend modules provide bi-directional integration between the eyeSight and leading endpoint security platforms to let you verify device compliance for functional antivirus, up-to-date signatures, encryption, and other endpoint policies, as well as facilitate remediation actions. eyeSight eyeExtend modules in this category include eyeExtend for Carbon Black, CrowdStrike, FireEye EX, FireEye HX, McAfee ePO, and Symantec Endpoint Protection.

IT Service Management (ITSM)

eyeSight eyeExtend for ServiceNow helps maintain a complete and accurate ServiceNow asset repository at all times. It also helps automate ServiceNow IT service and security incident creation and prioritization with complete device and network context and facilitates policy-driven remediation actions against noncompliant or compromised devices.

Next Generation Firewall (NGFW)

Forescout's NGFW eyeExtend modules let you implement dynamic network segmentation, automate controls for secure access to critical resources, and create context-aware security policies within your next-generation firewalls based on device context from eyeSight. eyeExtend modules in this category include eyeExtend for Check Point NGFW, Palo Alto Networks NGFW, and Fortinet NGFW.

Privileged Access Management (PAM)

Forescout's PAM eyeSight eyeExtend modules provide you with real-time agentless visibility into undiscovered local privileged accounts and let you automate responses to threats based on holistic visibility into user activity, device security posture, incident severity, and overall threat exposure. eyeSight eyeExtend modules in this category include eyeExtend for CyberArk.

Security Information and Event Management (SIEM)

Forescout's SIEM eyeSight eyeExtend modules facilitate information sharing and policy management between the eyeSight and leading SIEM systems to improve situation awareness and mitigate risks using advanced analytics. The solution shares comprehensive device information with your SIEM, including IoT classification and assessment context for correlation and incident prioritization. eyeSight eyeExtend modules in this category include eyeExtend for IBM QRadar, Micro Focus ArcSight, and Splunk.

Vulnerability Assessment (VA)

eyeSight VA eyeExtend modules share comprehensive vulnerability assessment data between the Forescout eyeSight and leading VA systems to initiate VA scanning of devices and automate policy-based enforcement actions as necessary. eyeSight eyeExtend modules in this category include eyeExtend for Qualys, Rapid7 InsightVM (Nexpose), and Tenable.

Advanced Compliance Module

eyeSight Advanced Compliance Module automates on-connect and continuous device configuration assessment to comply with security benchmarks. It enables you to leverage standards-based security benchmarks and content published in the SCAP format.

eyeExtend Connect (formerly the Open Integration Module – OIM)

eyeSight eyeExtend Connect allows customers, systems integrators, and technology vendors to easily integrate custom applications, security tools, and management systems with eyeSight. It enables new integrations to be created as applications that are easy to build, consume, and share with the wider community.

Centralized module management

eyeSight Modules are centrally managed across the enterprise. If you install or update a Base Module, a Content Module, or an eyeExtend module (Extended Module) on the Enterprise Manager, it is automatically installed or updated on all registered Appliances.

You can perform the following actions on several modules simultaneously:

- Start
- Stop
- Test (When available)
- Install and Uninstall
- Rollback (Can only be carried out on one module at a time)

You should carry out the above tasks from the Enterprise Manager, and not from individual Appliances.

If an Appliance on which a module is running is disconnected, it does not appear in the Modules pane. A warning message in the pane indicates that the Appliance is not connected.

The transfer of information between the eyeSight and installed plugins or modules is secure. All passwords defined in plugin and module configurations are:

- Kept encrypted on the hard drive Never printed to log files (even in their encrypted format)
- Encrypted before transfer between Forescout components

Install a module

To install the module:

1. Navigate to the Downloads page on the Customer Support Portal.
2. Download the `.fpi` file for the component.
3. Save the file to the machine where the Console is installed.
4. Log into the Console and select Tools > Options from the menu.
5. Select Modules > Install. The Open dialog box opens.
6. Browse to and select the saved component `.fpi` file.
7. Select Install. The Installation screen opens.
8. Read the License Agreement. The installation cannot proceed unless you accept the License Agreement.
9. After you have read the License Agreement, select I agree to the License Agreement to confirm that you have read and agree to its terms, and then select Install. The installation cannot proceed unless you agree to the License Agreement.

   Note:

   The installation begins immediately after selecting Install and cannot be interrupted or canceled. In modules with multiple components, components are processed serially.
10. When the installation completes, select Close to close the window. The installed component (module or plugin) is displayed in the Modules pane.

    Note:

    Some components are not automatically started following installation.
11. Start the plugin. In Tools > Options > Modules, right-click on the component name in the Modules pane. In the menu that appears, click Start.
12. To confirm that your installed and configured component is running, in Tools > Options > Modules, hover over the component name in the Modules pane to view a tooltip indicating whether it is running on eyeSight devices in your deployment.

    - The component is stopped on all eyeSight devices.

    - The component is stopped on some eyeSight devices.

    - The component is running on all eyeSight devices.

Plugin configuration management

Configurations made to certain plugins and modules via the Enterprise Manager are automatically applied to all registered Appliances. These configurations may not be updated per Appliance. See Device Management Overview for more information about managing Forescout Devices.

Manage a plugin or component on an individual appliance

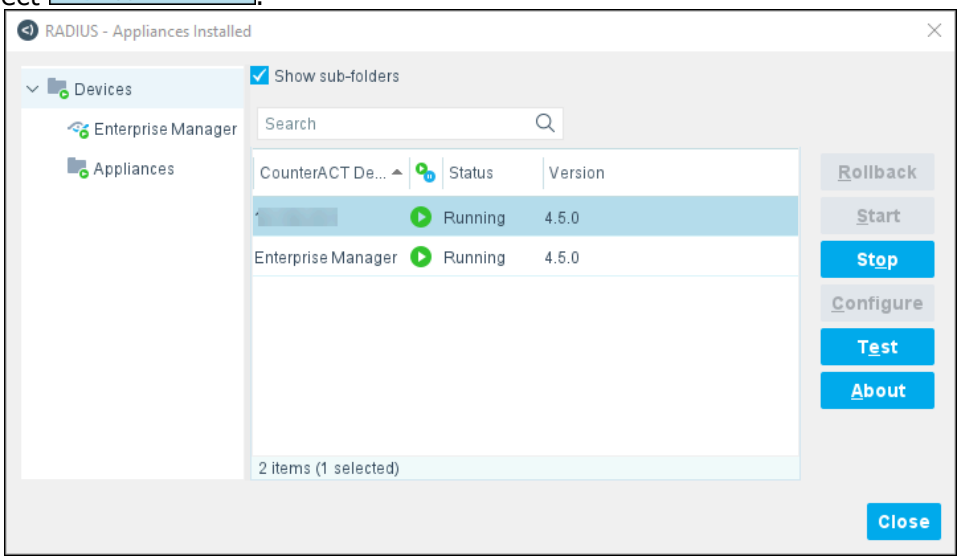
You can manage the following actions for a component or plugin installed on an individual appliance.

- Start
- Stop
- Test (When available)
- Configure (when available)
- Rollback (when available)

Note:
To ensure that a component or plugin is running, see .

To manage a plugin or component installed on a specific Appliance:

1. From Tools > Options > Modules, select a plugin or component in the *Modules* pane.
2. Select Appliances on the right of the screen, or right-click the plugin or component and select Appliances.



3. In the Appliances Installed dialog box, select the required appliance.
4. Select one of the available active buttons on the right.

Check for updates

The eyeSight automatically checks to see if updates are available for software already installed on your Devices and for software that you have purchased but have not yet installed (when using Flexx licensing). This saves you the trouble of checking for updates manually and helps keep your system updated with the most current tools.

Updates are delivered for Base Modules, Content Modules, and eyeSight eyeExtend modules (Extended Modules), and notifications of Forescout updates. Occasionally, plugins may also be available as hotfixes.

The Check for Updates icon appears on the status bar of the Console when an update is available for any installed or purchased Forescout component (when using Flexx Licensing). For more information, refer to About Flexx Licenses in the *Forescout eyeSight Flexx Licensing How-to Guide*. (when using Flexx Licensing).

Note:
The installed Console automatically and periodically contacts the Forescout support server, using an HTTPS secured connection, to check for software updates.

To update software:

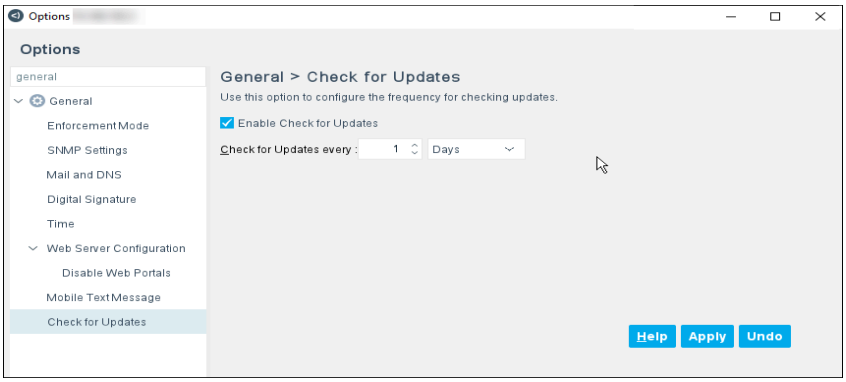
1. Double-click the Check for Updates icon. The Software Updates dialog box opens. The dialog box displays new and current version information, links to Release Notes and Help files, and other release information.

2. Select the software items you want to install and click Install. The Install wizard opens. Certain Forescout release items may appear but cannot be checked. eyeSight releases are upgraded from the CounterACT Devices menu. Select Tools > Options > CounterACT Devices > Upgrade.
3. Select I agree to the License Agreement, and then select Install. Installation will not proceed if you do not agree to the license terms. A progress bar indicates the progress of the installation. You can view the installation log file, which itemizes any installation failures.

Configure check for updates

You can enable or disable the Check for Updates option and configure how often it is run. The default frequency is once per day (daily).

To Check for Updates configuration settings are located at Tools > Options > General > Check for Updates.



Check for Updates-Global mode

If you want the Enterprise Manager's Check for Updates settings to always be automatically applied to all Consoles that are connected to that Enterprise Manager, you must enable the Check for Updates-Global Mode. By default, Check for Updates-Global Mode is disabled, meaning that each connected Console controls the configuration of its own Check for Updates settings.

To enable/disable Check for Updates-Global Mode:

1. Log in to the CLI of the Enterprise Manager.
2. Perform either of the following:
    a. To enable this mode, run the following command:

    ```
    fstool set_property software.update.period.active.global true
    ```

    b. To disable this mode, run the following command:

    ```
    fstool set_property software.update.period.active.global false
    ```

3. On the Enterprise Manager, restart the service.

Roll back to previous module versions

Under certain circumstances, you may want to roll back a module/component to a previously installed version, for example, if your system is not operating as expected after upgrade.

The following rollback/upgrade activities are NOT supported:

-
- Upgrading to a base module version (or one of its components) released with 8.2.x when running a version of the eyeSight lower than version 8.1.1.

If you upgrade to a newer module or component version that becomes available after this release, you may be able to roll it back. When rollback is supported, the Rollback button is enabled in the Console.Modules/components on Appliances connected to the Enterprise Manager are rolled back to the selected version. Modules/components on Appliances that are not connected to the Enterprise Manager during the rollback are rolled back when the Enterprise Manager next reconnects to the Appliances. To roll back the module or component:p

1. Select Tools > Options > Modules from the Console menu.
2. In the Modules pane, select the module or component to roll back.
3. Select Rollback. A dialog box opens listing the versions to which you can roll back.
4. Select a version and select OK. A dialog box opens showing you the rollback progress.

Accessing Forescout eyeSight web portals

Web portal users are defined in the CounterACT User Profiles table. You can assign permission levels to ensure that only certain users have access to certain types of information or activities. For example, you can grant all users the ability to access a specific web portal but allow only selected users to access a different web portal. See Creating Users and User Groups for details.

Note:
The "admin" user has access to all Console and web portal features.

Note:
Web portal users must log in from an IP address within the permitted range. See Define Web Access.

Note:
The device runs a web server to operate the portals. (Access to the portal page requires a secured HTTPS connection, because the information displayed is sensitive.) During the installation of the Appliance, a default self-signed certificate is created for this purpose. However, the certificate was not signed by a known CA, which causes the web browser to display a security warning when network users attempt to use the portal. See Generating and Importing a Trusted Web Server Certificate for details. You can turn off this option and communicate via HTTP.

Forget your password?

If you are a Console user and you forget your password, contact your System Administrator or another user authorized to change your password at the Console.

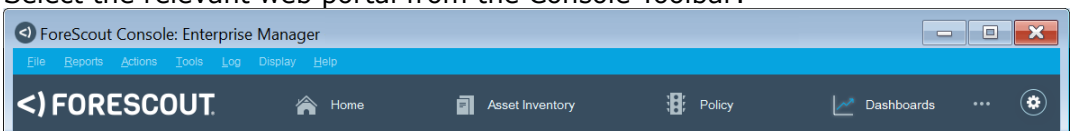
Logging in to Forescout eyeSight web portals

By default, the Forescout Console is configured to allow users to automatically access Forescout eyeSight web portals from the Console without additional login requirements.

You can require users who are logged into the Forescout Console to re-enter credentials when accessing Forescout eyeSight web portals and applications from the Console.

To log in from the Forescout Console:

- Select the relevant web portal from the Console Toolbar:



  - To open the Dashboards view (part of the Forescout eyeSight Web Client), select the Dashboards tab. After accessing this view, you can access the Assets view from within the web client.
  - For other web portals and applications, select the ellipsis icon , and then select a web portal or application from the drop-down menu.

  The web portal or application opens in a new browser window.

To log in from a web browser:

Open a browser, and enter one of the following:

- To access the Forescout Web Client (Dashboards and Assets view, and the eyeSegment application (Segmentation)), enter the following URL:

  `https://<Device_IP>/forescout-client`

  Where `<Device_IP>` is the IP address of the Enterprise Manager or an Appliance.

- To access other web portals, enter the following URL:

  `https://<Device_IP>/<Portal_Name>`

  Where `<Device_IP>` is the IP address of the Enterprise Manager or an Appliance.

  Valid `<Portal_Name>` values are:

  - assets – Legacy Assets Portal
  - customization – User Portal Builder
  - report – Reports Portal

  Note:
  Other portals might be available depending on your license. When running in Certification Compliance mode, the Assets Portal and the Reports Portal are disabled.

If you are not already authenticated to the Forescout eyeSight web portal, the Forescout Login dialog box opens. See Log In to the Forescout Console.

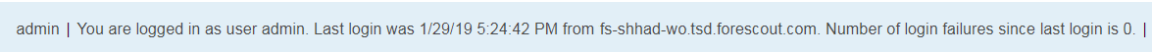
Last Login Information

In the Forescout eyeSight Web Client, you can hover the mouse over your user name to see the session information for your account.

In other web portals, the information is displayed when the portal opens.

The session information can include:

- The user name and IP address of your current login session
- The time and IP address of this user's previous successful login
- The number of this user's recent, consecutive login attempts that failed



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

Forescout eyeSight dashboards

The Dashboards view, part of the eyeSight Web Client, is a web-based information center that provides a real-time overview of the network through both out-of-the-box (OOTB) and user-created dashboard widgets.

Dashboards deliver dynamic, at-a-glance information about:

- Device visibility (OOTB)
- Device compliance (OOTB)
- Health monitoring (OOTB)
- Forescout policy data, including custom policies

Dashboards are designed to:

- Provide a quick overview of important network activities for corporate executives.
- Allow security administrators, security operations centers (SOC), and other users to easily monitor their security state.

This information is collected from policies and is periodically updated as endpoints are monitored and controlled by eyeSight eyeSight and eyeControl. By default, widget information is updated every 60 seconds.

Note:
Under certain circumstances, different widgets containing identical policy rules may temporarily display slightly different values for those rules. This is usually resolved when widget information is updated after 60 seconds.

Supported browsers

For a list of eyeSight supported browsers, see the Web Browser page of the Forescout Compatibility Portal.

Note:
When using Internet Explorer, you may experience widget display issues when resizing the browser window. It is recommended to use a different supported browser for optimal widget visualization.

Dashboard permissions

eyeSight users who work with dashboard functionality must be assigned the Dashboards: Access permission. Users who only have Dashboards: Access View permissions can view dashboard content and add existing dashboards to their view but cannot do any of the following:

- Create new dashboards
- Duplicate existing dashboards
- Add/edit/delete/reorder widgets

Users who have Dashboards view permissions must also have each OOTB dashboard individually enabled in their User Profiles.

For more information about the Forescout eyeSight Web Client, see Out-of-the-Box Dashboards and Access to Console Tools – On-premises Permissions for details about OOTB dashboard permissions.

Related Video: Forescout eyeSight dashboards

https://www.youtube.com/embed/kDhgZqX7Df4

Limit user access to Forescout eyeSight dashboards

By default, all Forescout Console users with Dashboards: Access permissions can access the Dashboards view. Using the Forescout command line interface (CLI), you can define a range of IP addresses that are not allowed to access the Dashboards view.

Access control consists of the following activities:

- Block user access to the Dashboards view
- List currently blocked users
- Allow user access to the Dashboards view

To limit user access:

1. On the Enterprise Manager, log in to the command line interface (CLI).

2. Run any of the following `fstool` command lines:
   a. To block user access to the Dashboards view:

      ```
      fstool www block_web_client_ip <affected user IP addresses>
      ```

   b. To list all currently blocked users:

      ```
      fstool www list_blocked_web_client_ip
      ```

   c. To allow user access to the Dashboards view:

      ```
      fstool www unblock_web_client_ip <affected user IP addresses>
      ```

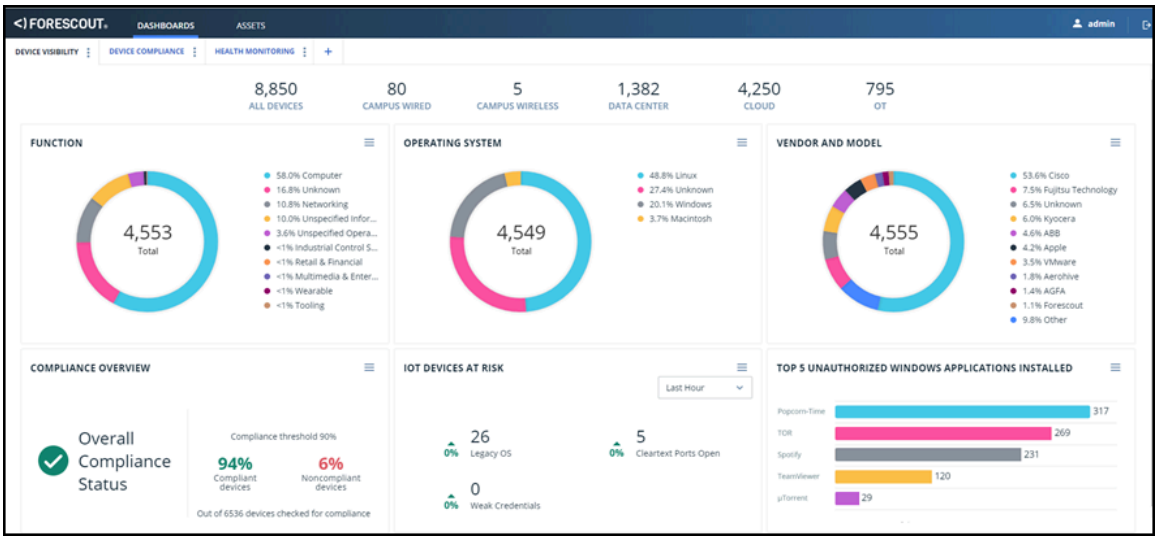
      In these fstool command lines, specify user IPv4 address(es) using any of the following IP address formats:
      - An individual IPv4 address, for example, `10.1.2.3`
      - Multiple IPv4 addresses, separated by a space, for example, `192.168.1.104 192.168.1.205`
      - A partial IPv4 address (the first 1 to 3 bytes of the address), for example, `10.1`
      - Multiple, partial IPv4 addresses, separated by a space, for example, `10 172.20 192.168.2`
      - A network/net mask pair, for example, `10.1.0.0/255.255.0.0`
      - A network/net mask pair (CIDR notation), for example, `10.1.0.0/16`

      In these `fstool` command lines, specify user IPv6 address(es) using any of the following IP address formats:

      - An individual IPv6 address, for example, `2001:db8::a00:20ff:fea7:ccea`
      - A partial IPv6 address, for example, `2001:db8:1:1::a`
        - A network/net mask pair (CIDR notation), for example:
          - `2001:db8:2:1::/64`
          - `2001:db8:3::/48`

Forescout eyeSight dashboard layout

The Forescout eyeSight Dashboards view layout is as follows:



Application Header

Forescout Web Client Items. Available tools that users can navigate to and access. The Forescout Web Client hosts the following tools:

DASHBOARDS (see Dashboards View)

ASSETS (see Assets View)

SEGMENTATION

User menu. User currently logged in to the Forescout Console.

? Provides a link to the *Forescout Documentation Portal* at https://docs.forescout.com/

Log out. Log out from your system.

Dashboards

Each dashboard in your view has its own tab.

Out-of-the-Box Dashboards appear in your view by default after installation.

See Working with Dashboards to learn how to manage dashboards, including how to add, duplicate and set dashboard privacy.

Overview Counters

Out-of-the-Box Dashboards include overview counters that identify the total number of devices detected in your deployment.

Widgets	Each dashboard can contain multiple widgets. See Working with Dashboard Widgets to learn how to manage widgets, including how to add, edit and drill-down into widgets.

Forescout eyeSight dashboard prerequisites

Do the following before working with dashboards:

- Verify that these Core Extensions Module components are running in the Forescout Console:
  - Dashboards
  - Data Publisher
  - Data Receiver
  - Technical Support (for Health Monitoring content)
- Run the Dashboard Policies Template
- Run the following Health Monitoring Templates:
  - Health Monitoring Policies Template
  - Physical Appliances Inventory Template
  - Virtual Appliances Inventory Template

  See Health Monitoring Templates for more information about how to run the templates and about the policies they create.

  Note:
  After you run the Health Monitoring Policies Template, the Health Monitoring Dashboard will be available to add to your Dashboards view. See Add a Dashboard to Your Vi for details.

How to populate Forescout eyeSight dashboards

To begin populating widget data in Out-Of-The-Box (OOTB) dashboards, verify that you are running a set of basic policies that retrieve relevant compliance, classification, and health monitoring property data from your network.

Populate the Forescout eyeSight Health Monitoring dashboard

Run Health Monitoring Templates to create the following policies, which populate specific Out-Of-The-Box dashboard widgets.

Policy	Widget that Policy Populates
Appliance Load Compliance	Appliance Load Compliance Widget

Policy	Widget that Policy Populates
Appliance Load Compliance Analysis	
Appliance Resource Utilization Appliance Resource Utilization Analysis	Appliance Resource Utilization Widget
Appliance Policy Efficiency Appliance Policy Efficiency Analysis	Appliance Policy Efficiency Analysis Widget
Plugin Health Plugin Health Analysis	Plugin Health Analysis Widget
Physical Appliance Inventory	Physical Appliance Inventory Widget
Virtual Appliance Inventory	Virtual Appliance Inventory Widget

Populate Forescout eyeSight device visibility and compliance dashboards

Run the Dashboard Policies Template to create the following policies, which populate specific out-of-the-box dashboard widgets.

Policy	Widget that Policy Populates
Campus Wired Campus Wireless Data Center Cloud OT Network	Device Overview Counters
Device Compliance	Compliance Overview Widget
IoT Devices	IoT Devices at Risk Widget

Policy	Widget that Policy Populates
	IoT – Top 5 Reasons for Noncompliance Widget
Cleartext Ports Open Weak Credentials* Legacy OS	IoT Devices at Risk Widget
Unauthorized Windows Applications Installed	Top 5 Unauthorized Windows Applications Installed Widget

* The Weak Credentials policy contains a Commonly-Used Credentials sub-rule, which attempts to find devices that use commonly used credentials. By default, the policy scope includes all devices on the network. Forescout checks for commonly used credentials on SSH and Telnet via login attempts, which may be interpreted as brute force attacks by devices or third-party security systems. If such a concern exists, Forescout recommends limiting the policy scope or adjusting the sub-rule accordingly.

To ensure that widget data is populated for widgets in the Device Compliance Dashboard, in addition to running the Dashboard Policies template, verify that:

- you have policies categorized as 'Compliance'
- these policies contain at least one sub-rule with a category label of Not Compliant
- devices match these sub-rules

For example, the Antivirus Compliance policy is categorized as Compliance, the AV Not Installed sub-rule has a category label of Not Compliant, and 35 devices match this sub-rule. For more information about categorizing a policy, see Categorizing Policies.

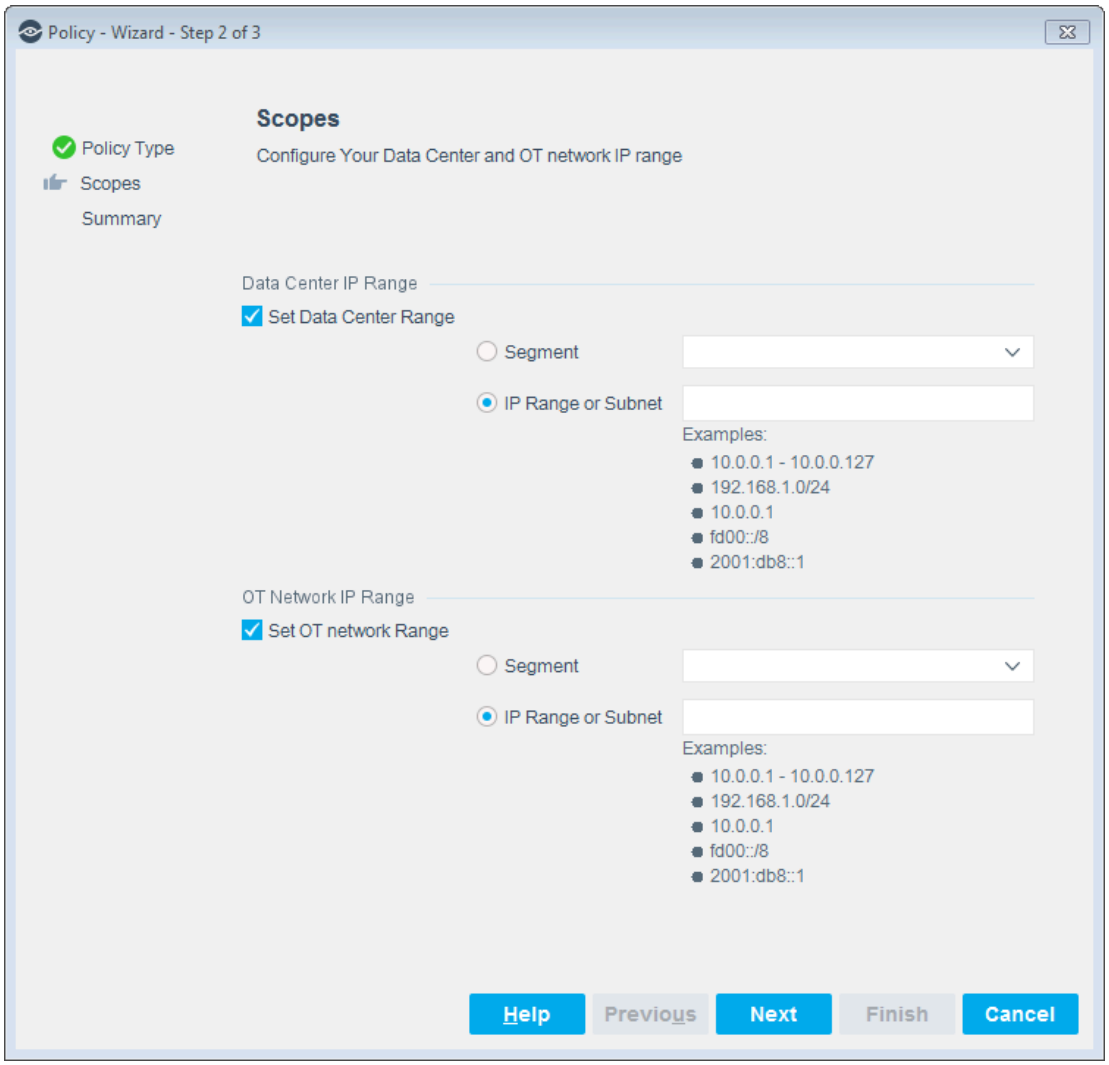
Run the Forescout eyeSight dashboard policies template

Use the Dashboard Policies template to activate the default Dashboard policies, and to configure the IP scope for your Data Center, Cloud, and OT Network.

It is important to run this template even if you already ran it in a previous version, since the policies it provides have been updated. Be aware that running this template removes outdated policies from your system. Refer to version Release Notes for details and upgrade considerations.

To run the template:

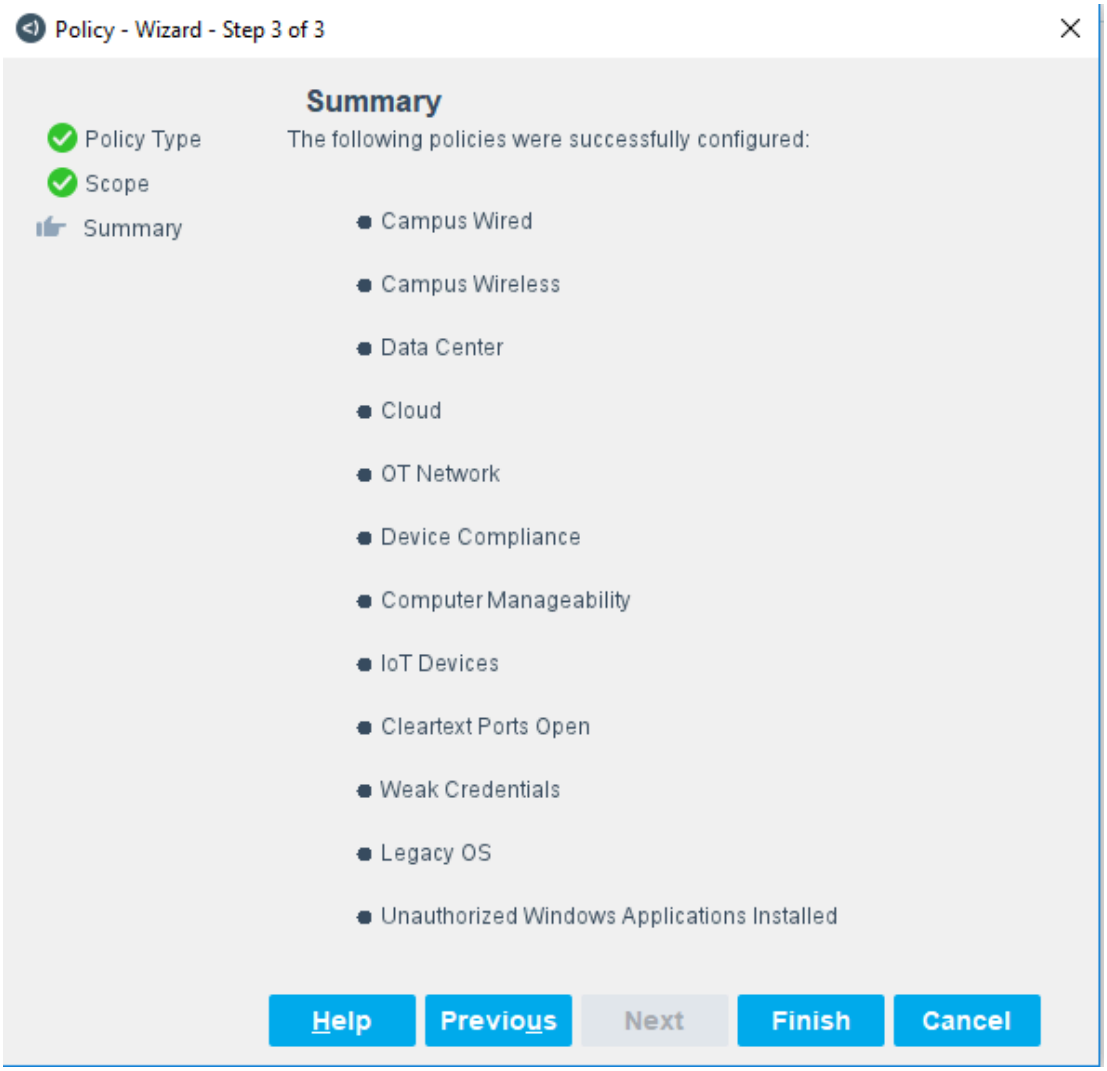
1. Select Add from the Policy Manager.
2. Expand the Dashboards folder and select Dashboard Policies. The Dashboard Policies pane opens.
3. Select Next. A customized version of the Scopes pane appears.



4. Use the Set Data Center Range and Set OT network Range options to define which endpoints are inspected.

Segment	A previously defined segment of the network.
IP Range or Subnet	a range of IP addresses or a Subnet.

5. Select Next. The Summary pane opens, displaying a summary of the policies that have been activated.



6. Select Finish.
7. Select Apply to save the policy settings.

Out-Of-The-Box (OOTB) Forescout eyeSight dashboards

Some dashboards are available OOTB with your eyeSight eyeSight license. Other dashboards are optional and you can add them to Dashboards view.

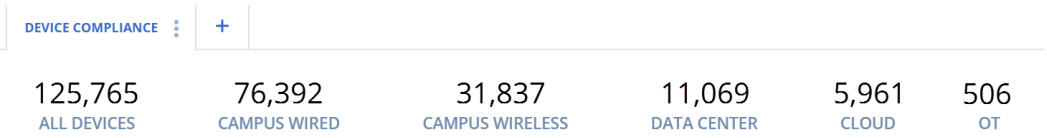
Users who have Dashboards view permissions must also have each OOTB dashboard individually enabled in their User Profiles.

For information about Forescout eyeSight Web Client permissions, see Access to Forescout Console Tools Permissions for details about OOTB dashboard permissions.

Device Overview Counters

In some dashboards overview counters display the total number of devices detected in your

deployment, and the number of devices of different categories.

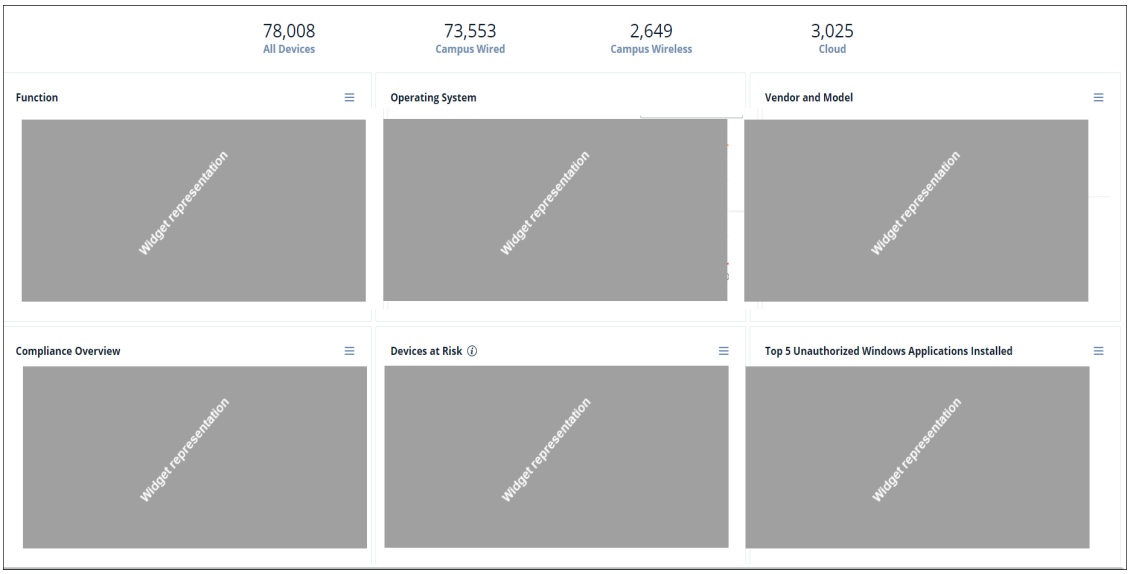


Forescout eyeSight device visibility dashboard

View at a glance, real-time inventory, compliance and risk data for devices on your network. This dashboard contains the following widgets, according to the following categories:

- Classification. These widgets provide a real-time view of diverse device functions, operating systems and models currently on the network based on information from Forescout Classification Properties. Each widget displays up to ten values for each property.
  - Function Widget
  - Operating System Widget
  - Vendor and Model Widget
- Compliance. This widget displays a continuous assessment of device compliance posture.
  - Compliance Overview Widget
- Risk
  - Devices at Risk Widget (default)
  - Top 5 Unauthorized Windows Applications Installed Widget

Forescout eyeSight Device Visibility Dashboard.

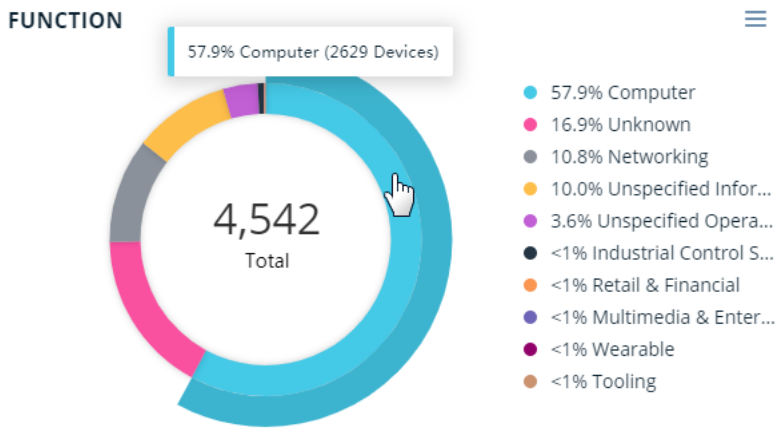


Function widget

View a breakdown of devices by function, as resolved by the Function property.

Two levels of values are displayed in the widget. The first level value is displayed as a slice in the donut, and the second level is displayed when you hover over a slice of the donut. For example, if a device is resolved as Accessory > VoIP > IP Phone, the widget will display Accessory as a slice in

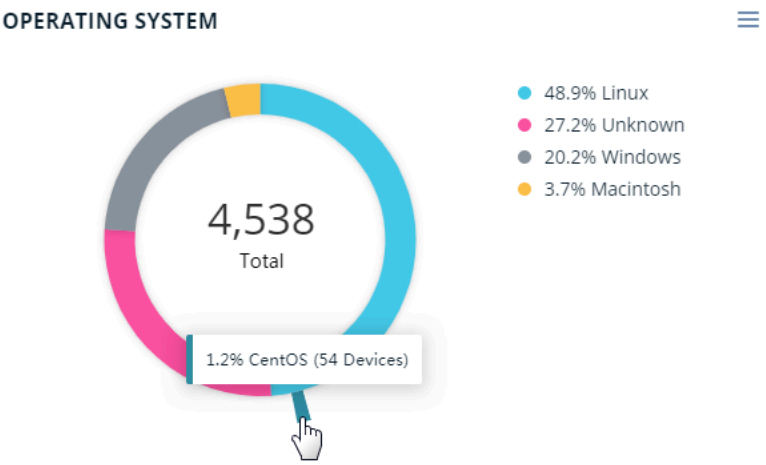
the donut, and VoIP when you hover over that slice. The third-level value is not displayed.



Operating system widget

View a breakdown of devices by operating system, as resolved by the Operating System property.

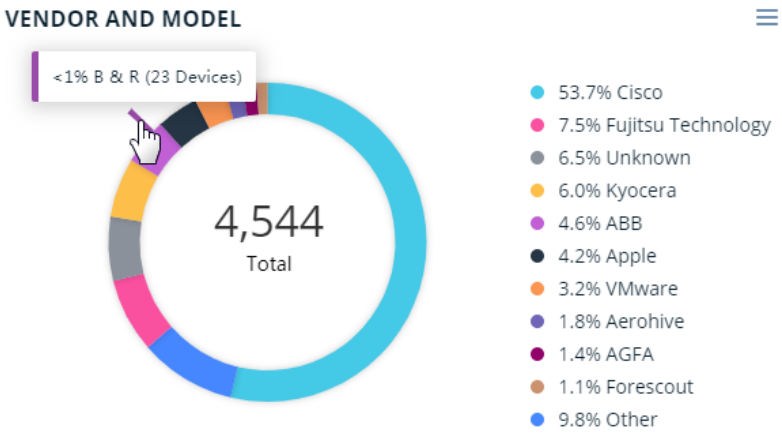
Two levels of values are displayed in the widget. The first level value is displayed as a slice in the donut, and the second level is displayed when you hover over a slice of the donut. For example, if a device is resolved as Linux > Debian, the widget will display Linux as a slice in the donut, and Debian when you hover over that slice.



Vendor and model widget

View a breakdown of devices by vendor and model, as resolved by the Vendor and Model property.

Two levels of values are displayed in the widget. The first level value is displayed as a slice in the donut, and the second level is displayed when you hover over a slice of the donut. For example, if a device is resolved as Samsung > Samsung Galaxy Tablet > Samsung Galaxy Tablet 10, the widget will display Samsung as a slice in the donut, and Samsung Galaxy Tablet when you hover over that slice. The third-level value is not displayed.

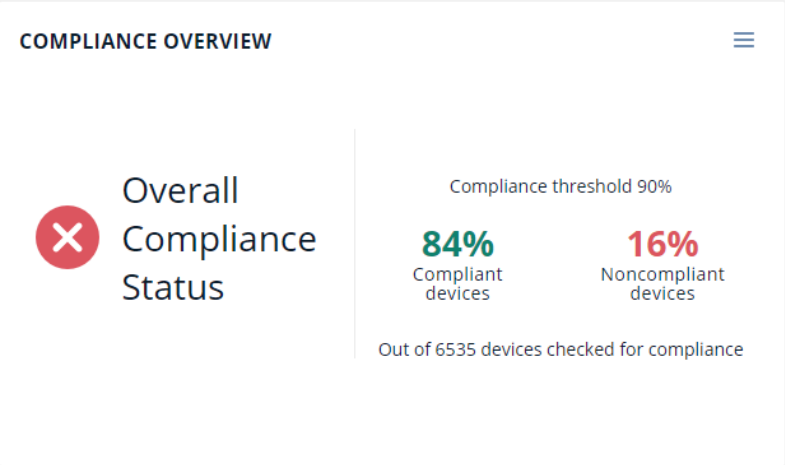


Compliance overview widget

View a continuous, real-time assessment of device compliance posture.

This widget shows a breakdown of devices by their compliance status (compliant / noncompliant), as resolved by the Compliance Status property. If the percentage of compliant devices exceeds the compliance threshold (default: 90%), the overall compliance status is Compliant.

If the percentage of compliant devices falls below the compliance threshold, the overall compliance status is noncompliant, and corrective action is required.

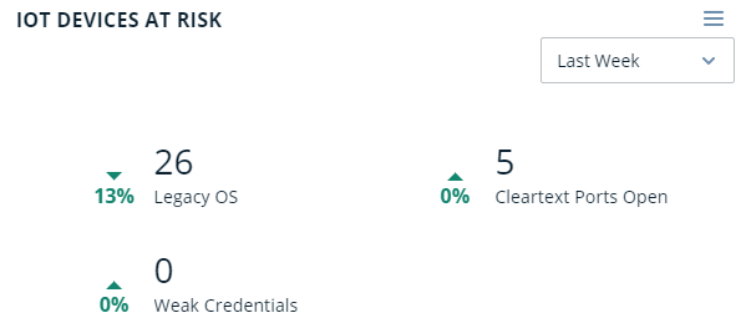


Widgets in Out-of-the-Box Dashboards cannot be edited. You can Duplicate a Dashboard to create a copy of the dashboard, and then edit the copied widget to change the threshold percentage and title of the widget.

IoT devices at risk widget

View IOT devices that are prone to attack, which present a high risk to the cybersecurity posture. Analyze this widget's data to plan a strategy for minimizing the attack surface on the devices in your network and reducing the likelihood of security breaches.

The IoT Devices policy (created by the Dashboard Policies template) classifies the device as an IoT device and adds the device to the IoT Group. There are three more policies, one for each device type counter (Cleartext Ports Open, Weak Credentials, Legacy OS).



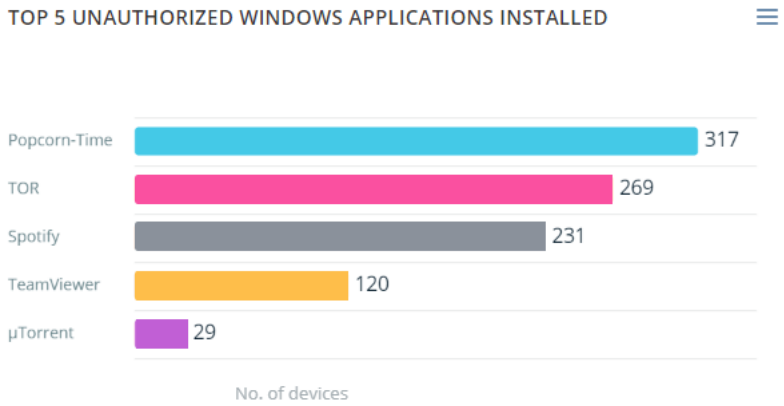
This widget displays the number of devices with:

- Cleartext Ports Open:
  - Telnet port open
  - FTP port open
- Weak Credentials
  - Factory default credentials (SSH, Telnet or SNMP)
  - Commonly used credentials (SSH, Telnet or SNMP)
- Legacy OS
  - Running EOL OS's (Windows XP*, Windows 2000)

Top 5 unauthorized Windows applications installed widget

View the most common unauthorized Windows applications installed on devices in your network to focus on sources of potential security incidents.

This widget displays the top 5 unauthorized applications installed on Windows devices via Add/ Remove Programs.



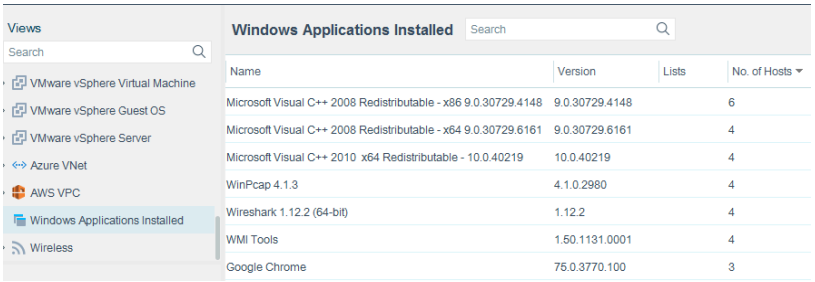
By default, this policy searches for devices that have the following unauthorized applications installed:

- Amazon Cloud Drive
- Bitcasa
- Box
- Copy
- Cubby
- CX
- Dropbox
- Google Drive
- iCloud Drive
- Mozy
- myflare
- OneDrive
- Popcorn-Time
- Spotify
- SugarSync
- Team Viewer
- TOR
- µTorrent

You can edit this list in the Console to change the applications that will appear in the Dashboard widget. Go to Tools > Options > Lists, and edit the Unauthorized Windows Applications list.

If you add more than five applications to the list, only those installed on the greatest number of detected devices appear in the widget. If you edit the list by importing values from a file, make sure the file is in TXT format and UTF-8 encoded.

For a list of currently detected Windows applications installed, access the relevant view in the Asset Inventory page of the Console.



If you add applications that contain regular expression special characters (for example, *$+), you need to add a backslash (\) before every special character. For example, if you add Notepad++ (32-bit x86), you need to type Notepad\+\+ \(32-bit x86\).

Forescout eyeSight device compliance dashboard

View at a glance, real-time data for improving compliance hygiene for devices on your network.

Forescout eyeSight Device Compliance Dashboard:

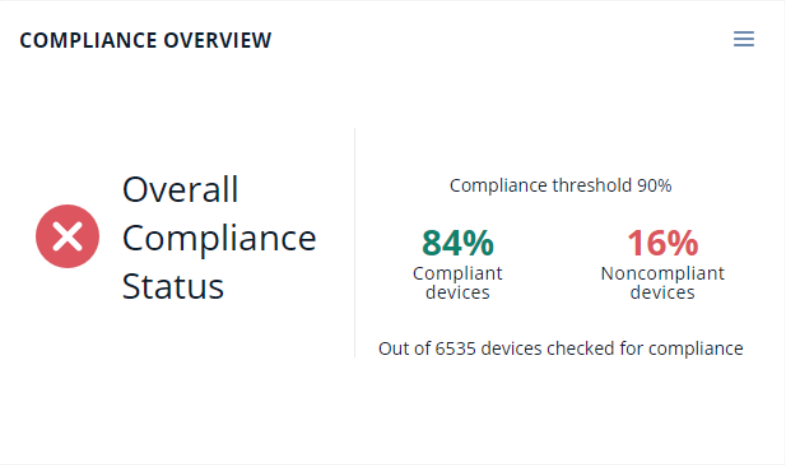
Compliance Overview Widget

View a continuous, real-time assessment of device compliance posture.

This widget shows a breakdown of devices by their compliance status (compliant / noncompliant), as resolved by the Compliance Status property. If the percentage of compliant devices exceeds the compliance threshold (default: 90%), the overall compliance status is Compliant.

If the percentage of compliant devices falls below the compliance threshold, the overall compliance status is noncompliant, and corrective action is required.

Note:
This widget also appears in the Device Visibility Dashboard.

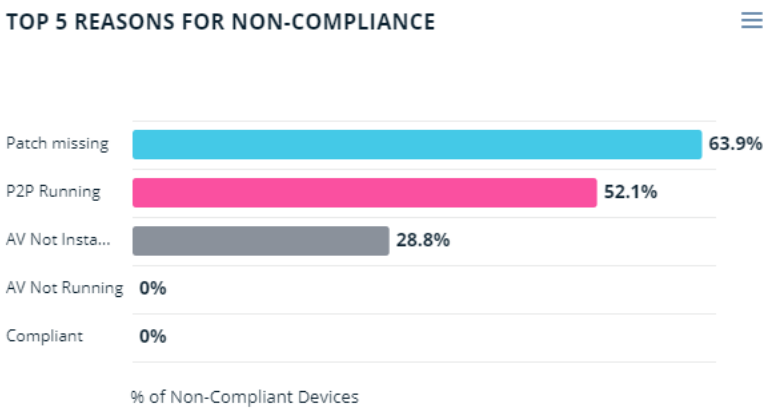


Widgets in OOTB Dashboards cannot be edited. You can Duplicate a Dashboard to create a copy of the dashboard, and then edit the copied widget to change the threshold percentage and title of the widget.

Top 5 Reasons for Noncompliance Widget

View the top reasons for non-compliance in your network, helping you to prioritize remediation activities for the most widespread vulnerabilities.

This widget displays the top 5 reasons for non-compliant devices in your network, via the compliance policy sub-rules (the reasons) that have the highest numbers of noncompliant devices. Each reason is presented as a percentage of the total.

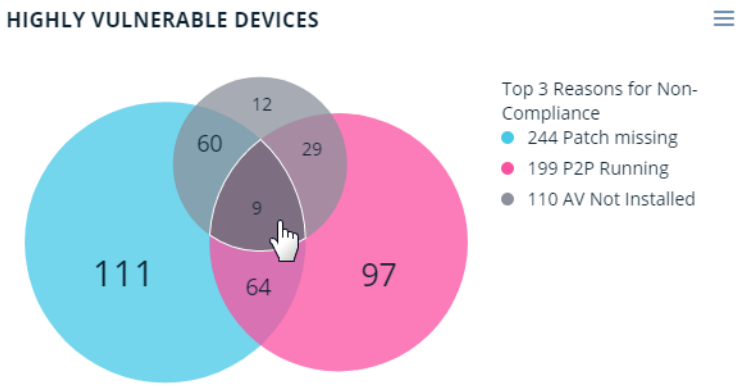


Highly Vulnerable Devices Widget

View vulnerable devices that are non-compliant for multiple intersecting reasons to take action on the most vulnerable devices in your network.

This widget displays up to 3 sub-rules with the greatest number of matched devices. Devices that match a sub-rule of a policy categorized as Compliance (specifically, a policy sub-rule labeled as Not Compliant) are displayed in this widget.

The widget will only display intersections between sub-rule matches if the sub-rules are in different policies.

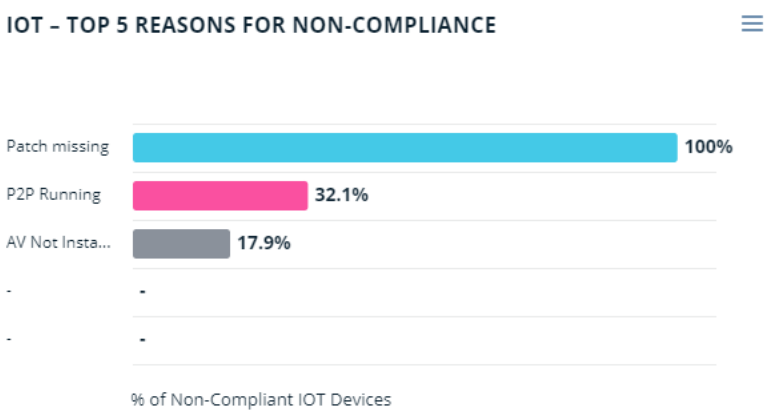


IoT – Top 5 Reasons for Noncompliance Widget

View the most common compliance issues related to IoT devices, helping you prioritize remediation efforts.

This widget displays the percentage of IOT devices that match policy sub-rules categorized as *Not Compliant*. The widget displays up to 5 sub-rules with the greatest number of matched devices.

The percentage of noncompliant devices is calculated from the total number of noncompliant devices classified by the IOT Devices policy. For example, if 20% is displayed next to the FTP Open sub-rule, this means that 20% of all noncompliant IOT devices are noncompliant because they matched this sub-rule. Use this information to help identify and remediate noncompliant devices.



The IoT Devices policy classifies devices as IoT devices according to the Function property. Devices resolved with any of the following property values are added to the IoT Devices Group:

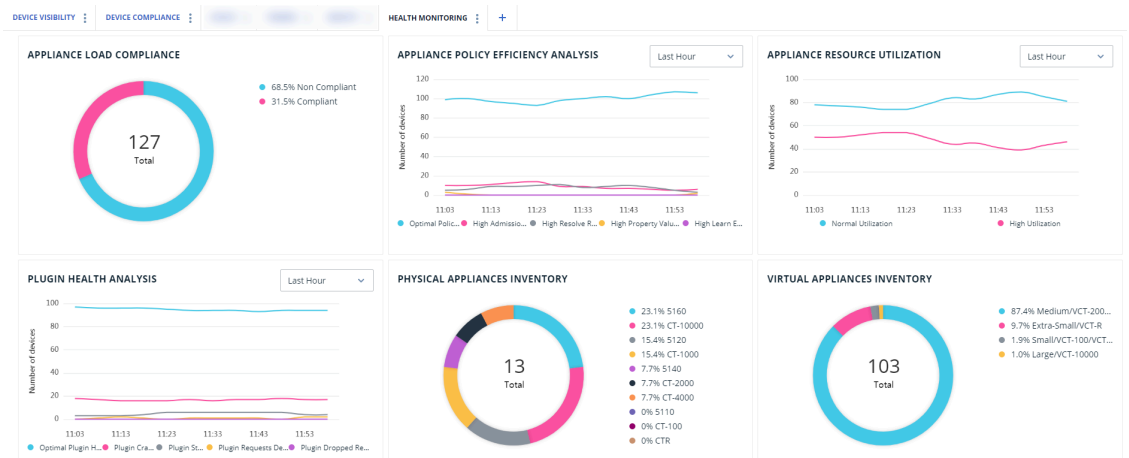
- Information Technology > Accessory
- Information Technology > Mobile
- Information Technology > Multimedia & Entertainment
- Information Technology > Networking
- Information Technology > Wearable
- Operational Technology

Devices that match a sub-rule of both the IoT Devices policy and a policy categorized as Compliance (specifically, a policy sub-rule labeled as Not Compliant) are displayed in this widget.

Forescout eyeSight health monitoring dashboard

View at a glance, real-time data that helps you monitor and improve the health of Forescout Appliances in your deployment.

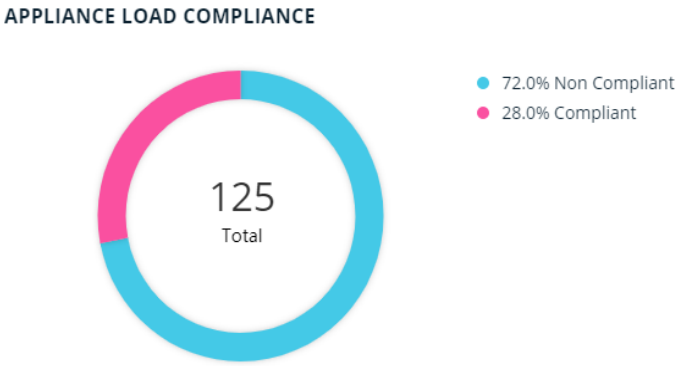
After you run the Health Monitoring Templates, this dashboard will be available as a public dashboard to add to your view. See Add a Dashboard to Your View for more information.



Appliance Load Compliance Widget

View the number and percentage of Appliances that are compliant with Forescout eyeSight load specifications as laid out in the Forescout Sizing Guide.

Load compliance is based on a detailed analysis performed by Appliance Load Compliance Policies, which analyze factors like HTTP Login Rate, traffic bandwidth, number of managed endpoints, and others. For a complete list of factors analyzed by this policy, see the list of properties in Health Monitoring – Load Specification Compliance.

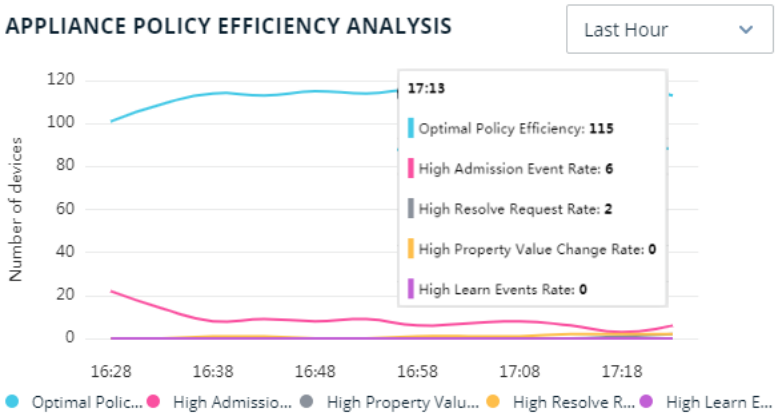


Appliance Policy Efficiency Analysis Widget

View whether policies are performing efficiently on Appliances in your deployment.

This widget displays the number of Appliances with optimal policy efficiency, as well as the number of Appliances that have high (sub-optimal) rates of the following policy-related factors:

- Admission Event Rate. Average rate of new endpoints being admitted into the network, per minute.
- Property Value Change Rate. Average rate that property values are changing, per minute.
- Learn Events Rate. Average rate that plugins report to the Forescout platform about new learned properties, per minute.
- Resolve Request Rate. Average rate that requests to resolve endpoint properties are made, per minute.

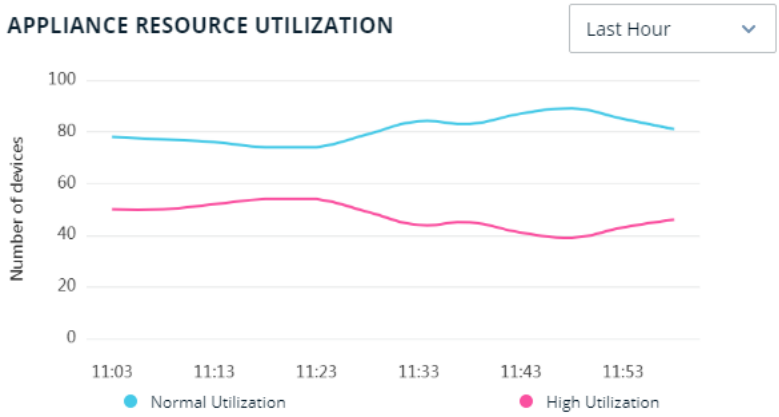


Appliance Resource Utilization Widget

View how effectively Appliances actually utilize their resources (irrespective of whether Appliance

specifications are found compliant with Forescout guidelines - see Appliance Load Compliance Widget).

This widget displays the number of Appliances that have either 'high' or 'normal' resource utilization. This categorization is based on a detailed analysis performed by Appliance Resource Utilization Policies, which analyze factors like CPU usage, disk latency, packet loss, and others. For a complete list of factors analyzed by this policy, see the list of properties in Health Monitoring – Resource Utilization.

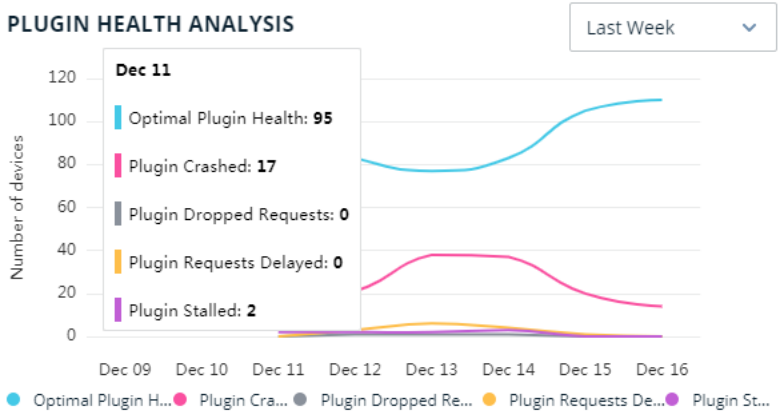


Plugin Health Analysis Widget

View the overall status of plugin health on Appliances in your deployment.

This widget displays the number of Appliances with optimal plugin health, as well as the number of Appliances that have occurrences of the following plugin-related events, indicating degraded plugin health:

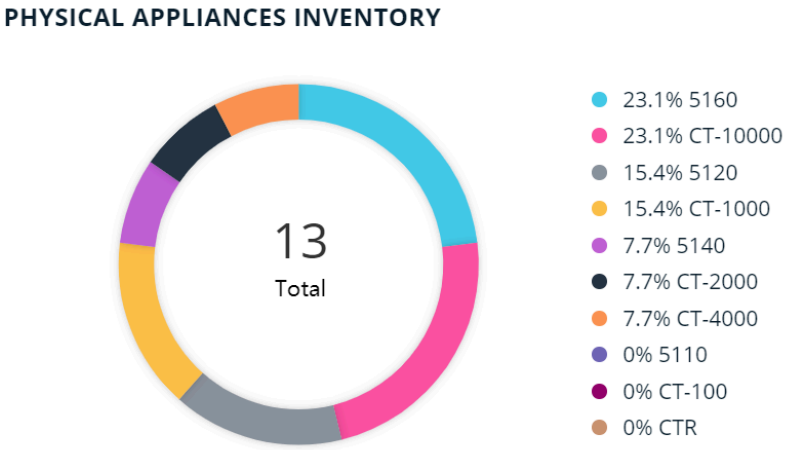
- Plugin Crashed. Whether a Forescout plugin crashed sometime in the last 30 minutes.
- Plugin Stalled. Whether a Forescout plugin stalled sometime in the last 30 minutes.
- Plugin Dropped Requests. The maximum number of plugin requests dropped per minute.
- Plugin Requests Delayed. The average amount of time, in seconds, that plugin requests are delayed on this Appliance



Physical Appliance Inventory Widget

View a list of all Forescout physical Appliances in your deployment, categorized by model/series. For example, if the Appliance model is 5120 (5100 Series) or CT-2000 (CT Series).

This categorization is based on the Physical Appliances Inventory policy, which uses the Forescout Device Models property (see Health Monitoring properties) to categorize Appliances.



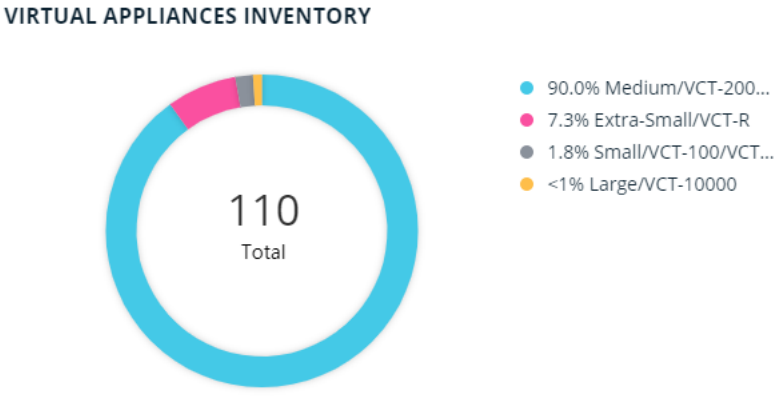
For more information about physical Appliance models, including performance and machine specifications, refer to the Forescout Sizing Guide.

Virtual Appliance Inventory Widget

View a list of all Forescout virtual Appliances in your deployment, categorized by model/size. Virtual Appliances are grouped by size, as follows:

- Large/VCT-10000
- Medium/VCT-2000/VCT-4000
- Small/VCT-100/VCT-1000
- X-Small/VCT-R

This categorization is based on the Virtual Appliances Inventory policy, which uses the Forescout Device Models property (see Health Monitoring properties) to categorize Appliances.



For more information about virtual Appliance models, including performance and machine specifications, refer to the Forescout Sizing Guide.

Work with dashboards

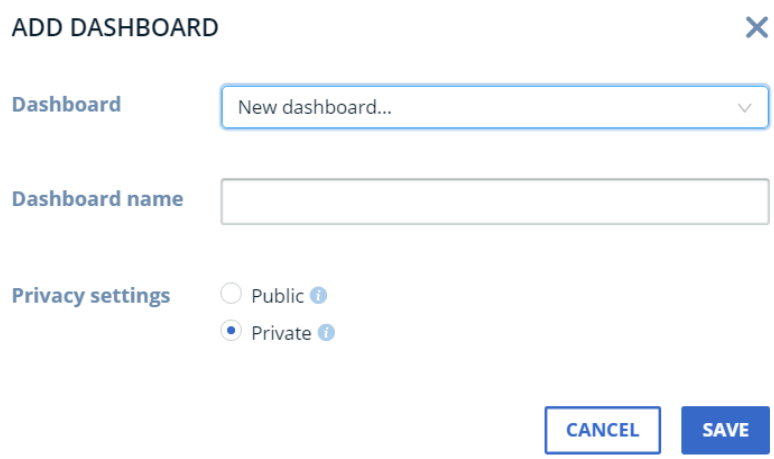
Add a Forescout eyeSight dashboard to your view

In addition to the OOTB Dashboards provided, you can add custom dashboards to your view to address specific use cases. Dashboard views are customizable for each user.

You can manually add:

- New dashboards that you create. You can populate these dashboards with widgets that you select.
- Public dashboards that were created by other users.
- Health Monitoring Dashboard. Although the widgets in this dashboard are available OOTB (after running Health Monitoring Templates), you must manually add this dashboard to Dashboards view.
- Dashboards that were hidden. See Hide a Dashboard for more information.

There is no limit to the number of dashboards you can add.



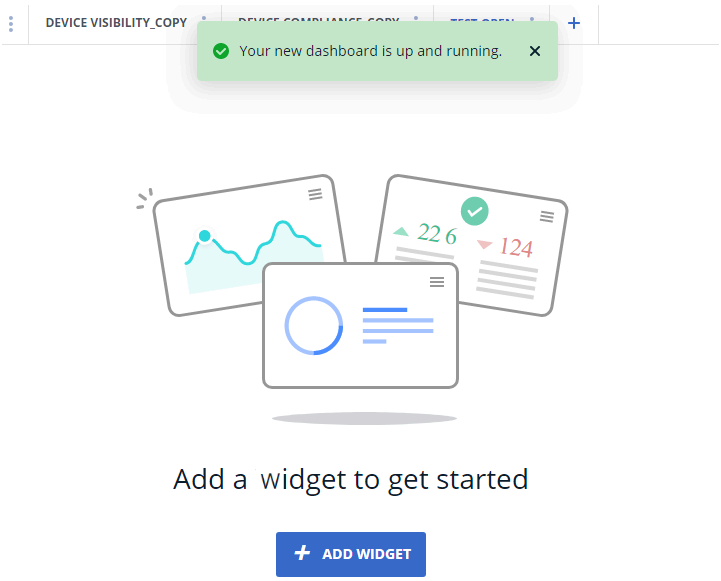
To add a dashboard:

1. Select + from the end of the dashboard tabs.
2. In the Add Dashboard dialog box, specify the following options:

Dashboard	Select a currently hidden dashboard or a public dashboard created by another user. The user name of the dashboard creator appears in parentheses after the dashboard name. For example, East Coast Compliance (John). Select New Dashboard to create a new dashboard.

Dashboard Name	If you are creating a new dashboard, enter the Dashboard name (up to 50 characters).
Privacy settings	Valid values include: Public: Everyone can add this dashboard to their view. Private (default selection): Only I can see this dashboard. After creation, you can change the privacy of dashboards that you create.

3. Select Save. If you created a new dashboard, the board is blank and you are prompted to add a widget to get started.



Manage Forescout eyeSight dashboards

Access these dashboard management tools from the dashboard menu icon ⋮.

Hide Dashboard	Remove a dashboard from your view. To add a dashboard back to your view you can Add a Dashboard to Your View and select it from the drop-down list of dashboards. Hiding a public dashboard does not affect other users' views. To permanently

	remove a dashboard, you can Delete a Dashboard.
Rename Dashboard	Rename a dashboard that you created.
Set Privacy	Change the privacy setting of a dashboard you created. Public. Everyone can add this dashboard to their view. Private. Only I can see this dashboard. If you change a dashboard from public to private after other users already added it to their view, the dashboard will be removed from their view. Similarly, when the creator of a public dashboard modifies the widgets or other content of the board, changes are pushed to all other users who added the board to their view.
Duplicate Dashboard	Copy the widgets and layout of a dashboard to a new dashboard. Initially, the new dashboard is private. Changes made to a duplicated dashboard do not affect the original dashboard that it was duplicated from.
Delete Dashboard	Completely remove a dashboard that you created. Use Hide a Dashboard to no longer view a dashboard created by someone else. When you delete a public dashboard that other users added to their view, the board is removed from their view.
Move Left /Move Right	Reorder dashboard tabs to change their position within the Dashboards view. You can also drag and drop dashboard tabs.
Save Dashboard	Export the dashboard as a PDF file with current values.

as PDF

Working with Forescout eyeSight dashboard widgets

Add a Forescout eyeSight custom widget

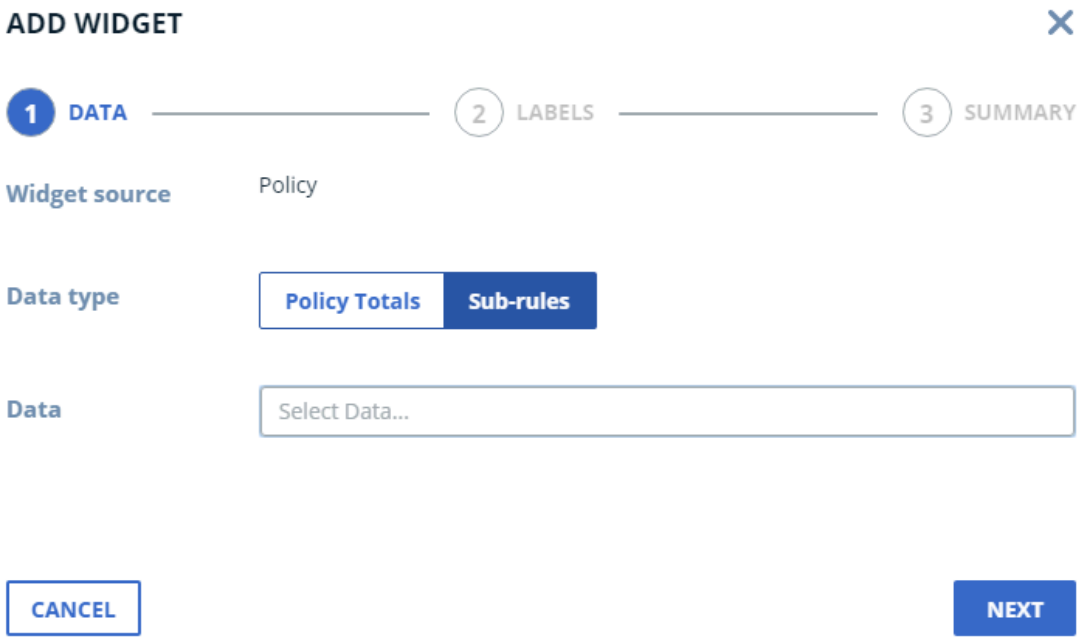
You can add widgets to a dashboard to visualize information about Forescout eyeSight policies. You can add widgets to any dashboard that you created. Depending on the data you select to populate the widget, different chart type displays are available (see Widget Chart Type for more information).

To create widgets that accurately reflect the information you want to see in the dashboard, you should understand how Forescout policies and other basic features work.

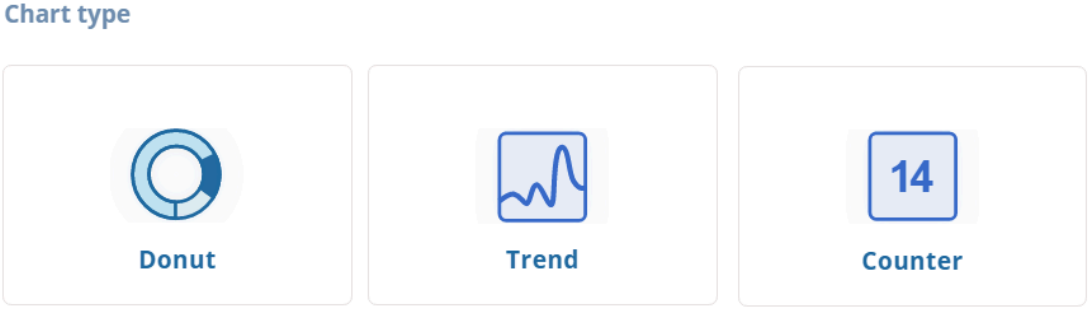
To add a widget:

1. At the lower right corner of the dashboard, select Add Widget

. The Add Widget wizard opens.



2. In the Data tab, specify the following options.



Data type	Policy Totals. Select policy totals for one or more policies. The policy total is the total number of devices that match any of the sub-rules for a specific policy. This does not include devices that only match the policy main rule, but not any of the sub-rules. Sub-rules. Select one or more individual sub-rules from a single policy.
Data	The policies or sub-rules on which the dashboard is based.
Widget Type	Some or all of these widgets may be available, depending on the number of policy totals or sub-rules reported by the policy. Donut: 10 individual sub-rules from any one policy Trend: 5 individual sub-rules from any one policy, or 5 policy totals of different policies Counter: 4 individual sub-rules from any one policy, or 4 policy totals of different policies

3. Select Next.
4. In the Labels tab:
    - Enter a title for the new widget.
    - If you are adding a Counter widget, configure the following additional options:
    - Configure whether to display an additional counter with the total number of all selected policies/sub-rules.
    - Configure whether to display trend arrows next to chart values.
    - Enter labels for sub-rules to be displayed in the legend of the widget. By default, the label name is identical to the name of the sub-rule.
    - If you are adding a Counter widget, toggle the trend arrows indicator next to each policy/sub-rule to configure whether upward and downward trend arrows are marked as positive or negative.
5. Select Next.
6. On the Summary page, review the information and select Finish.

Drill down into a Forescout eyeSight widget

From the Dashboards view, you can drill-down into a widget to access tabular information about the devices corresponding to the widget.

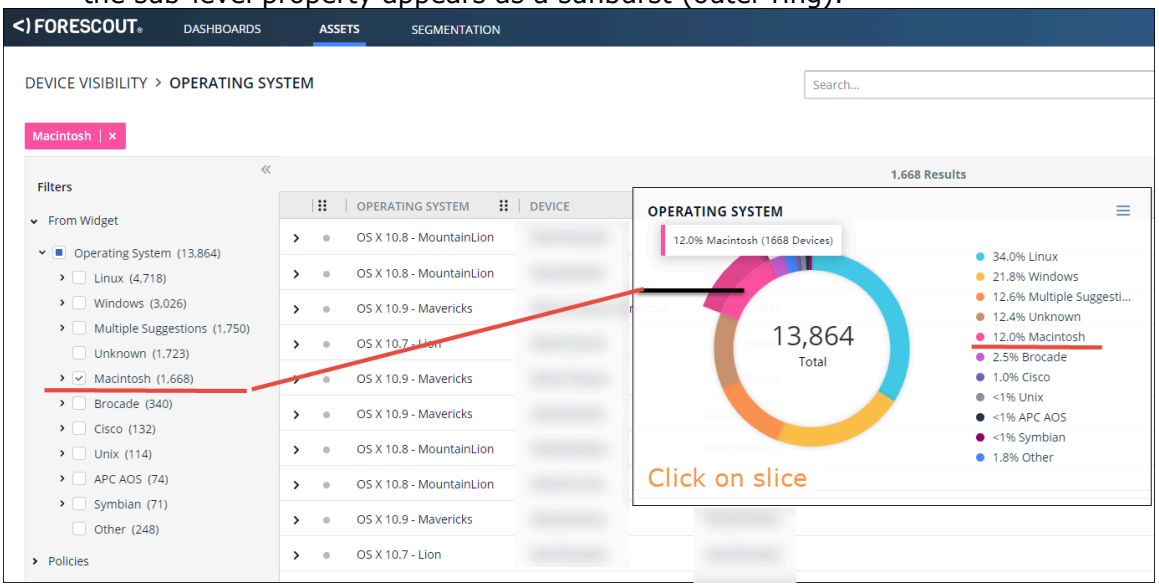
For information about widgets, see Out-of-the-Box Dashboards, and Add a Custom Widget.

When you drill down into a widget by clicking on a specific area within the widget, tabulated information about all corresponding devices is displayed in the Assets view. For more information about the Assets view, see Assets View.

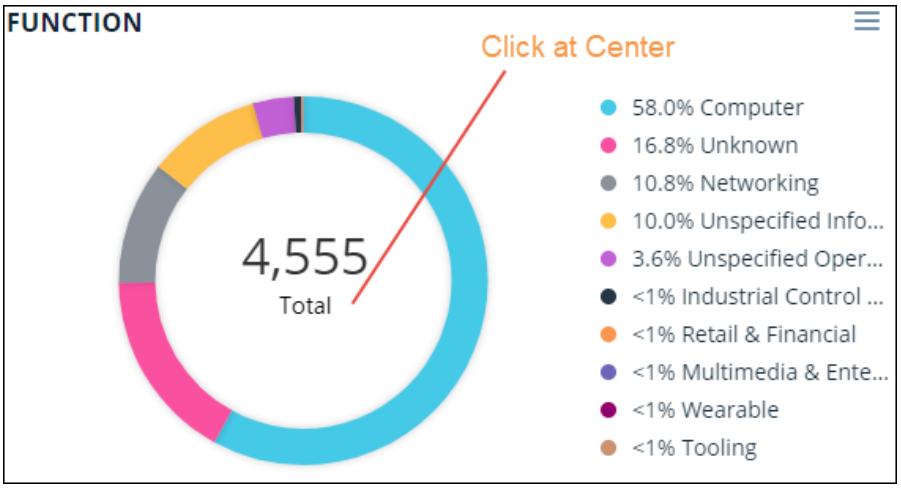
In a donut / sunburst widget, you can click on a specific slice or segment to view information about the assets (devices) that match the device aggregation corresponding to that specific slice or segment.

The sample Assets view below shows a device list for Forescout Vendor and Model devices, accessed by clicking the Forescout slice in the ring of a sunburst widget. The Filters pane>From Widget tree on the left contains the information displayed in the table.

Note:
For sunburst widgets that come with OOTB Dashboards , when you hover over the widget, the sub-level property appears as a sunburst (outer ring).

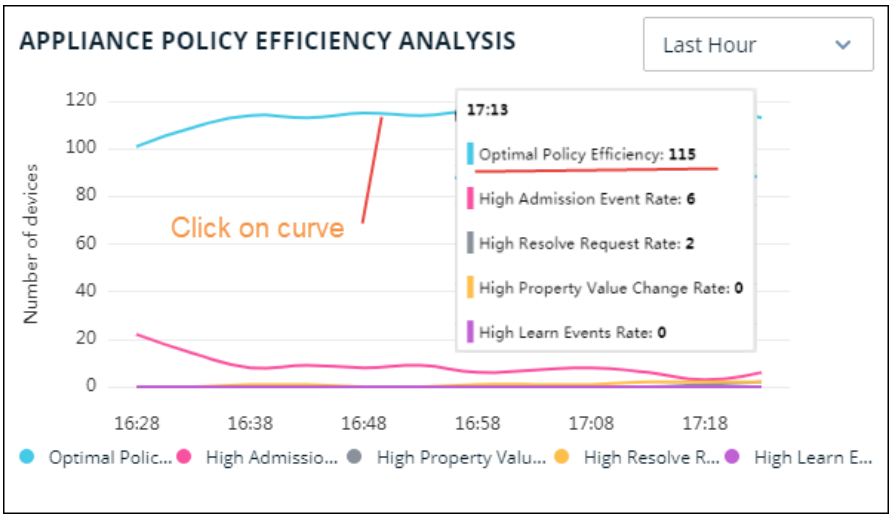


For donut / sunburst widgets only, you can select the center of the widget to view a list of all devices (total of all aggregations) that correspond to the widget.

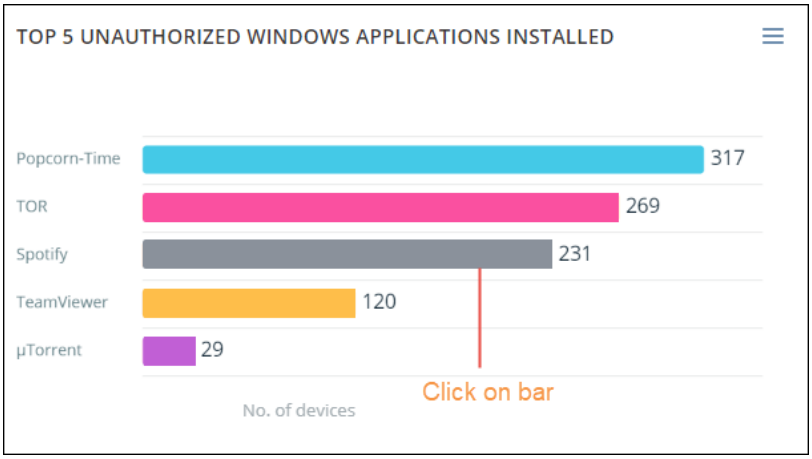


In a Trend widget, you can view the progression through time of several trends.

Note:
The listed values in a trend widget correspond to the current time, regardless of where you click on the curve.

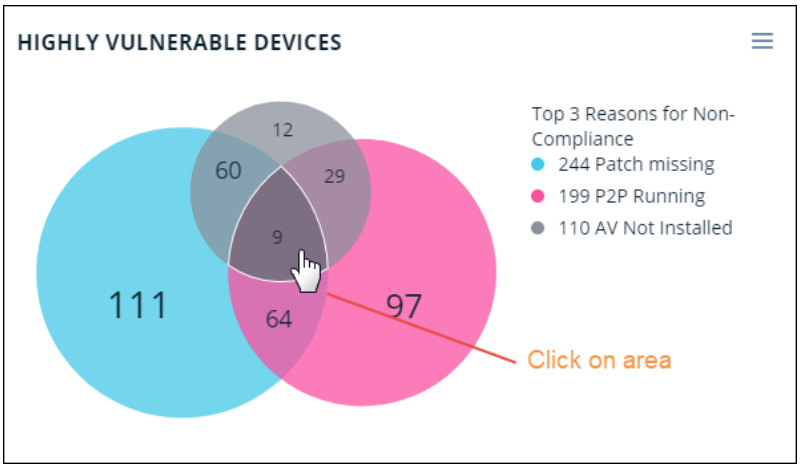


In a Bar Chart widget, you can click on a specific bar to view tabulated information about the devices that correspond to the bar.



In an Intersecting areas widget, you can click on a specific area to view tabulated information about the set of devices that correspond to the intersecting area.

Clicking on an area displays devices that match all highlighted sub-rules. In the example below, clicking on the outermost blue circle will display all 244 devices that match the Patch missing sub-rule, and not only the 111 devices that do not match other sub-rules.



Note:
You can switch between Dashboard view and Assets view by selecting ASSETS or DASHBOARD at the top of the page.

Manage Forescout eyeSight widgets

This topic describes widget management tasks.

Edit a Widget

You can only edit a widget that is in a dashboard that you created or duplicated.

You can edit the data of property-based Classification widgets (in a duplicated dashboard), to either display the property values with the highest number of matched devices (default), or a manual selection of values.

Since property value names are predefined by Forescout, you cannot edit thee label names of values.

To edit a widget:

1. Select Edit Widget… from the menu icon ☰ in the widget.
2. In the Edit Widget wizard, edit relevant information in the Data or Labels tab.
3. (Classification widgets only) In the Data Type field of the Data tab, select one of the following:
   - Top Values (default). Display the property values with the highest number of matched devices.
   - Manual Selection. Select up to 10 property values to display.
4. (Compliance Overview Widget only) In the Compliance threshold field of the Data tab, edit the threshold percentage with a number between 1 and 100. The default value is 90%. If the percentage of compliant devices exceeds the threshold, the overall compliance status is Compliant ✅.
5. On the Summary page, review the information and select Finish.

Reorder Widgets

Drag and drop the widget to change its position in the dashboard.

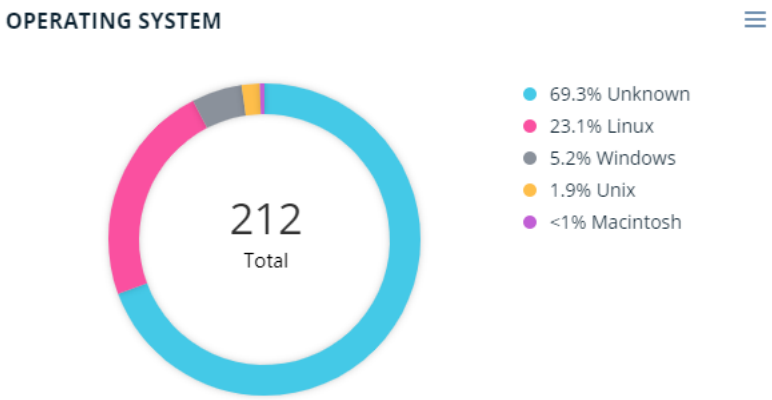
Delete a Widget

Select Delete Widget… from the menu icon ☰ of a custom widget to remove it from a dashboard that you own. Widgets in Out-of-the-Box Dashboards can't be deleted.

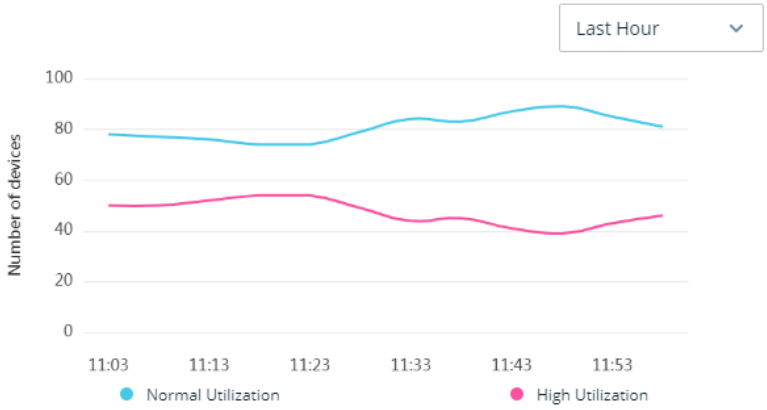
Forescout eyeSight widget chart type

Custom widgets can be visualized as one of the following chart types:

- Donut: A circular chart that displays the number and relative percentages of devices that match individual sub-rules (up to ten) from a single policy. The total number of devices that match all selected sub-rules is displayed in the center of the donut.
  Note:
  Unlike out-of-the-box classification widgets, which display up to two levels of values by hovering over slices of the donut, custom donut widgets display one level.

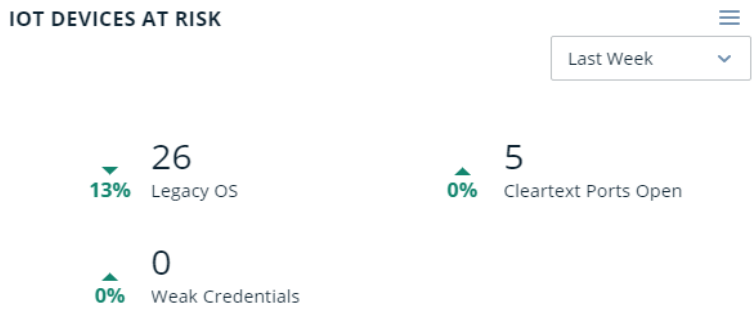


- Trend: A chart that displays the number of devices that match policy sub-rules over a set period of time (Last hour, 24 hours, week, month or year). Each sub-rule or sub-rule total represents a single line in the chart.



- Counter: Displays the number of devices that match policy sub-rules along with the percentage of change over a set period of time (Last hour, 24 hours, week, month or year). You can display up to four counters in each widget, plus an additional counter with the total number and percentage of all selected sub-rules. You can display trend arrows next to chart values and toggle the arrow indicator next to each sub-rule to configure

whether upward and downward trend arrows are marked as positive or negative.



Assets view

The Assets view, part of the eyeSight, is a web-based search, filter and discovery tool that lets you leverage extensive network and device information collected and correlated by Forescout products.

Assets view information is valuable to various groups across your organization, including:

- Security teams: Use device or policy information to quickly locate risky assets.
- IT departments: Use an IP address or other device information to locate and contact users when maintenance is required at the device.
- Help Desk/SOC: Use device information to handle security incidents in real time.

By using the Assets view, crisis management and subsequent remediation time is shortened.

Use this view to display a tabulated list of all the devices that Forescout eyeSight detects, subject to any selected device filters. The Assets view provides several device filter methods, which you can apply separately, or in tandem. You can filter the Assets view or drill down from a widget into Assets view to list only the devices relevant to a specific area of interest, for example, devices corresponding to a certain policy / sub-rule. You can view information about any device on any segment for which you have permissions, which is defined as part of your user scope.

In addition, you can save your own customized Assets view, and you can export any filtered list of devices to a CSV file.

Note:
For information on how the Assets view works in the Dashboards and Web Client plugins see, Assets View.

Note:
The Assets view does not replace the existing Assets Portal (see Assets Portal), but instead provides a newer interface with more robust filter/search capabilities. The Assets Portal allows users to clear event detections and stop policy actions. Depending on your needs, you may prefer to use one or the other, or both tools.

Supported browsers

For a list of Forescout eyeSight supported browsers, see the Web Browser page of the Forescout Compatibility Portal.

Assets view permissions

Forescout eyeSight Web Client users who work with Assets view functionality must be assigned the appropriate OOTB Dashboards view permissions. See Access to Console Tools – On-premises Permissions for details about Console user permissions.

Access the Assets View

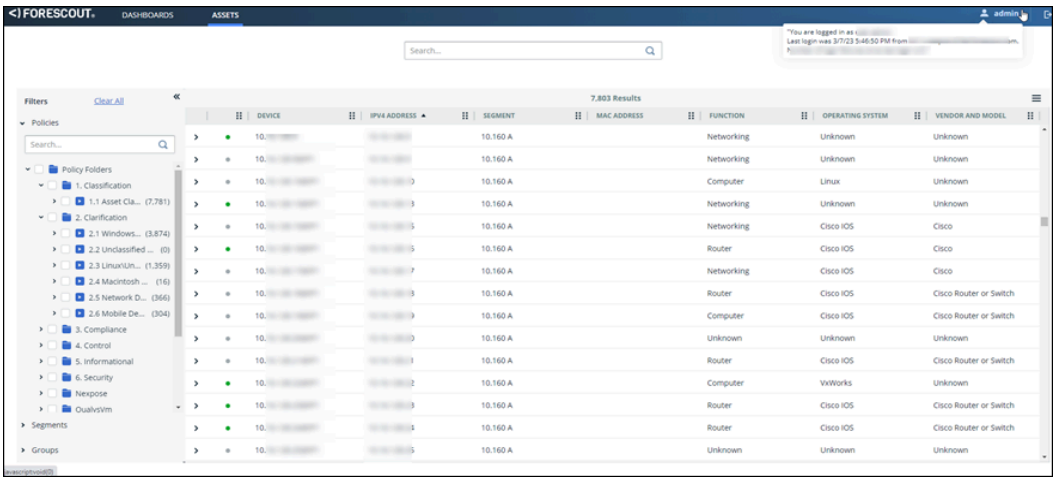
Access the Assets view via the Dashboards view of the Forescout eyeSight Web Client. See Logging In to Forescout Web Portals for more information.

Note:
You also access Assets view when you drill down into a Dashboard widget. See Drill Down

into a Widget .

Forescout eyeSight Assets view layout

The Assets view layout may differ according to the product you have purchased.



The Assets view displays columns with information about selected devices. The available columns depend on the product you have purchased.

Connectivity icon ●	A connectivity icon in each row to the left of the first column indicates the online or offline status of the device represented in the row.
Device	DNS name or IP Address of the device. **Note:** The Device column maps to the Host column in the All Hosts pane of the Console Home page. **Note:** About (optional) Overlapping IPs: When overlapping IPs are allowed in the Internal Network, the device name uses IP Reuse Domains (IRDs) to distinguish between two or more instances of an overlapping IP. For these devices, the device name has the format IP@IRD. For example, "abcd-ct1.pm.forescout.com@HQ". The IP address appears in the IPv4 column (per IRD).
IPv4 Address	IPv4 address for the device.
Segment	Segment to which device belongs.

	Note: Although you can view the number aggregations in a widget (in Dashboard view) for all segments in the internal network, you can only access the underlying information in Assets view for devices on any segment for which you have permissions, which is defined as part of your user scope.
MAC Address	MAC address for the device.
Function	This column reflects the Function classification property for the specific devices.
Operating System	This column reflects the Operating System classification property for the specific devices.
Vendor and Model	This column reflects the Vendor and Model classification property for the specific devices.

The page is initially sorted according to IP Address/DNS names of the devices.

Click in the column header to sort a column, or move the column in the table. You can also drag and drop columns to reorder the table.

Forescout eyeSight Assets view search and filter

The Assets view page can display up to 1000 devices. If you cannot find the device, use the Search field at the top of the page to refine your search.

Note:
eyeSight eyeSight searches the entire set of resolved device properties, not only the columns displayed on the page. Take this into account when analyzing the search results.

Note:
If you add text characters separated by a space, the program considers the space to be part of the searched text.

Note:
If a search returns less devices than expected: This might be due to disconnected or non-responding appliances.

The Filters pane on the left contains the Assets view filter families (Policies, Segments and Groups), as well as filters added as a result of Drill Down into a Widget.

For information about the filters in the Filter pane, see Filter Display of the Assets.

The order of the items in the filters is according to (descending) count. If two items have the same count, they are listed alphabetically.

Work with the Forescout eyeSight Assets view

Filter display of the Forescout eyeSight Assets

Relevant filters appear in the left pane of the Assets view.

For the Policy / Segment / Group families of filters, the relationship between the inclusive filters is based on OR logic. For example, if you select three sub-rules (sub- rule A, sub-rule B and sub-rule C) of a Policy, then the search will be for sub-rule A OR sub-rule B OR sub-rule C. If you select items from more than one family of filters, for example, from Policy and Segment, then the search will be for Policy AND Segment.

One or more colored rectangular tags at the top of the page help you identify which devices are currently filtered and displayed. For example, Group: UPS | × for a UPS device group.

Forescout eyeSight - From Widget

If you drilled down to Assets view from a Dashboard widget, the filter is saved under From Widget in the Filters pane.

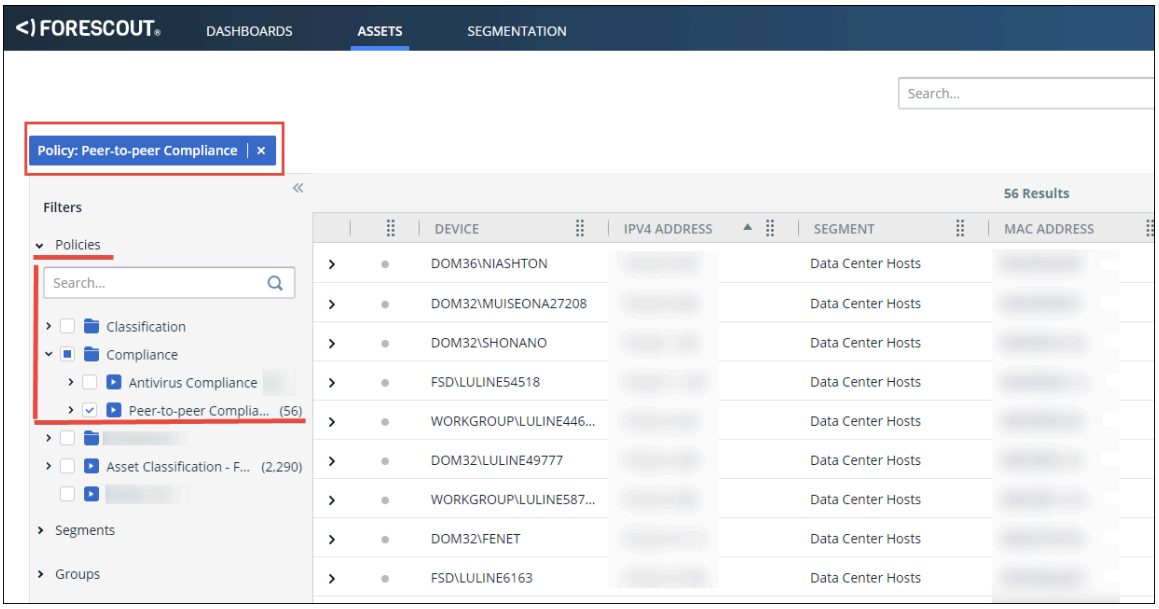
Note:
After drilling down into out-of-the-box compliance widgets, the selected filter in the Filters pane may display a larger number of devices than the number of results in the Device list. This may happen, for example, if an Appliance was disconnected from the Enterprise Manager. The two values are synchronized every 24 hours.

Forescout eyeSight Assets view policy / sub-rule filters

You can drill down to view only the devices that match a configured policy or sub- rule, to focus on specific devices of interest.

To open the Policies tree, select Policies in the Filters pane. Select check boxes to isolate specific policies / sub-rules / devices. Use the Search field to locate a specific device.

In the sample below, Assets view is filtered to display only devices that match the Peer-to-peer compliance sub-rule.



Note:

Your Assets view layout may differ from that shown. See Assets View Layout .

You can select / deselect filter checkboxes to switch between different policies / sub-rules / devices.

The policy Status icon in the Policies navigation item indicates whether the Forescout eyeSight detection mechanism is paused or running. When paused, new detection events are ignored.

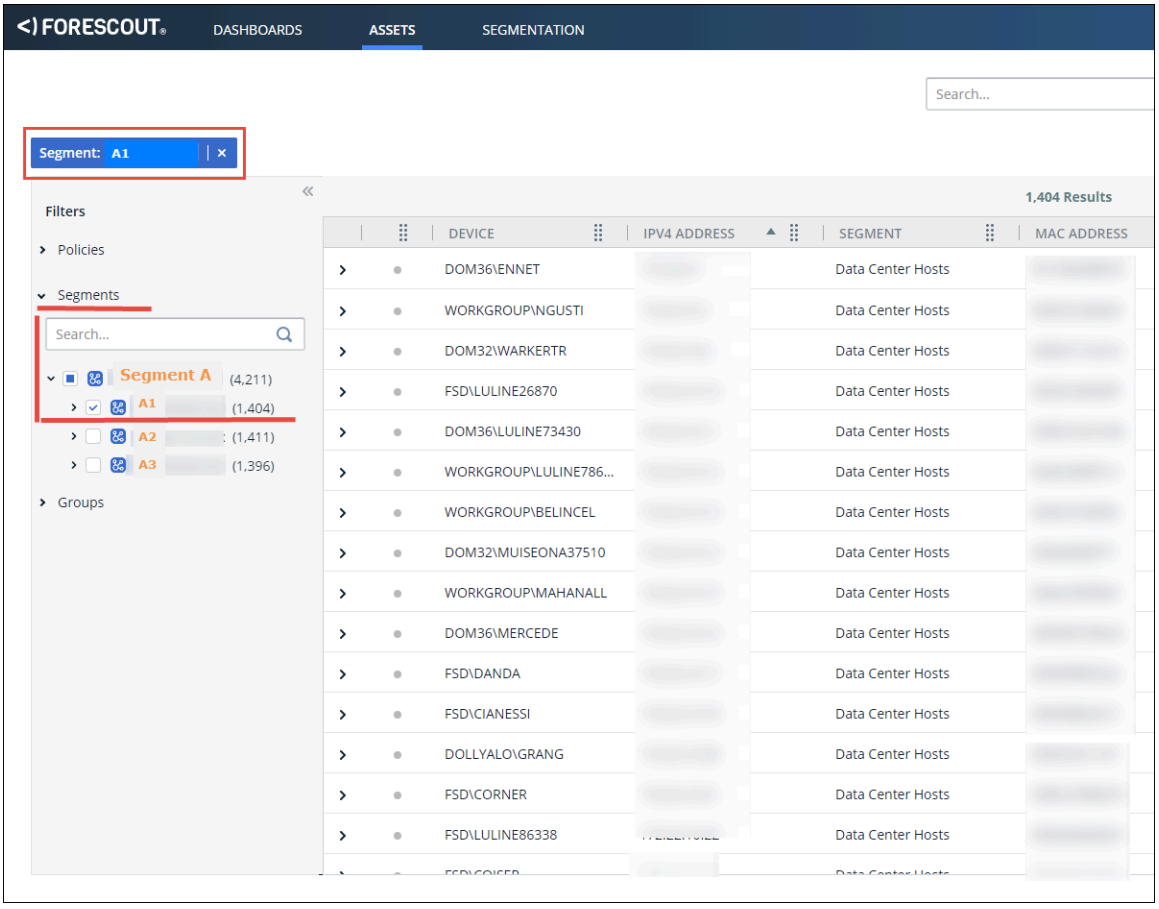
Forescout eyeSight Assets view segment filters

The Internal Network comprises network Segments or IP ranges that define the network in the Forescout eyeSight. Depending on your user permissions, you will have access to a subset of these segments. For more information about segments, see Initial Setup Wizard – Internal Network.

You can drill down to view only the devices that match one of your authorized segments, to focus on specific devices of interest.

To open the Segments tree, select Segments in the Filters pane. Select check boxes to isolate specific segments / devices. Use the Search field to locate a specific device.

In the sample below, the Assets view is filtered to display all the devices in the first sub segment A1.



Note:

Your Assets view layout may differ from that shown. See Assets View Layout .

You can select / deselect filter check boxes to switch between the different segments / devices.

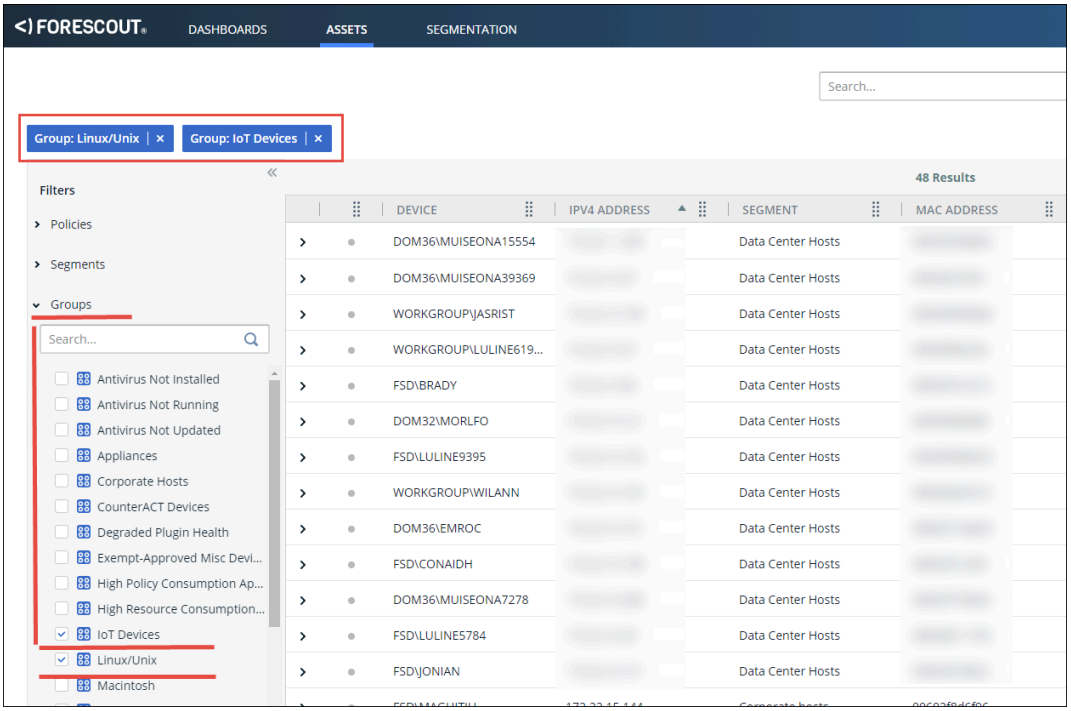
Forescout eyeSight Assets view group filters

A Group is a collection of devices with something in common, such as groups that run Windows OS or network guests. A device can belong to any number of groups.

You can drill down to view only the devices that belong to a specific Group.

To open the Groups tree, select Groups in the Filters pane. Select check boxes to isolate specific groups / devices. Use the Search field to locate a specific device.

In the sample below, Assets view is filtered to display only the devices that belong to the IoT Devices group, and Linux / Unix Group.



Note:
Your Assets view layout may differ from that shown. See Assets View Layout .

You can select / deselect filter tree check boxes to switch between the different device groups.

Add or remove columns in the Assets view

You can customize the Assets view through adding and removing Property columns according to your personal preferences, for example, to see more information about specific devices.

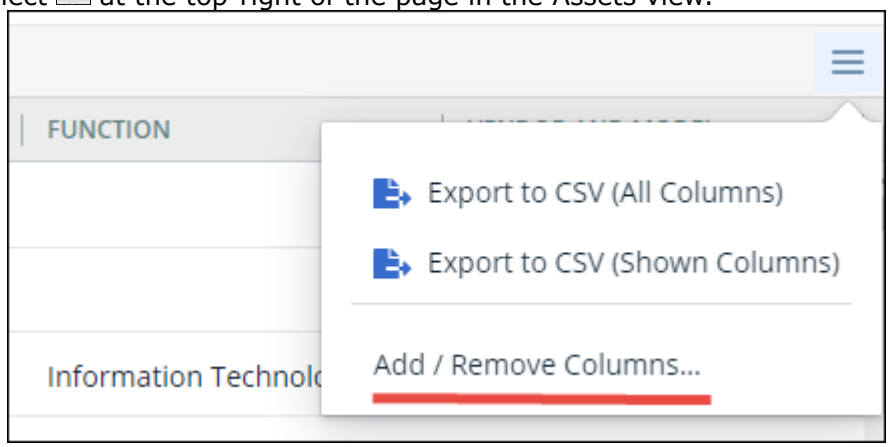
Note:
Add / remove columns does not apply to composite properties or lists.

Your customized Assets view is global for all your policies, within the scope of your user permissions. A different user does not have access to your customized Assets view. The Assets view maintains your customized configuration after you log out and then log in again.

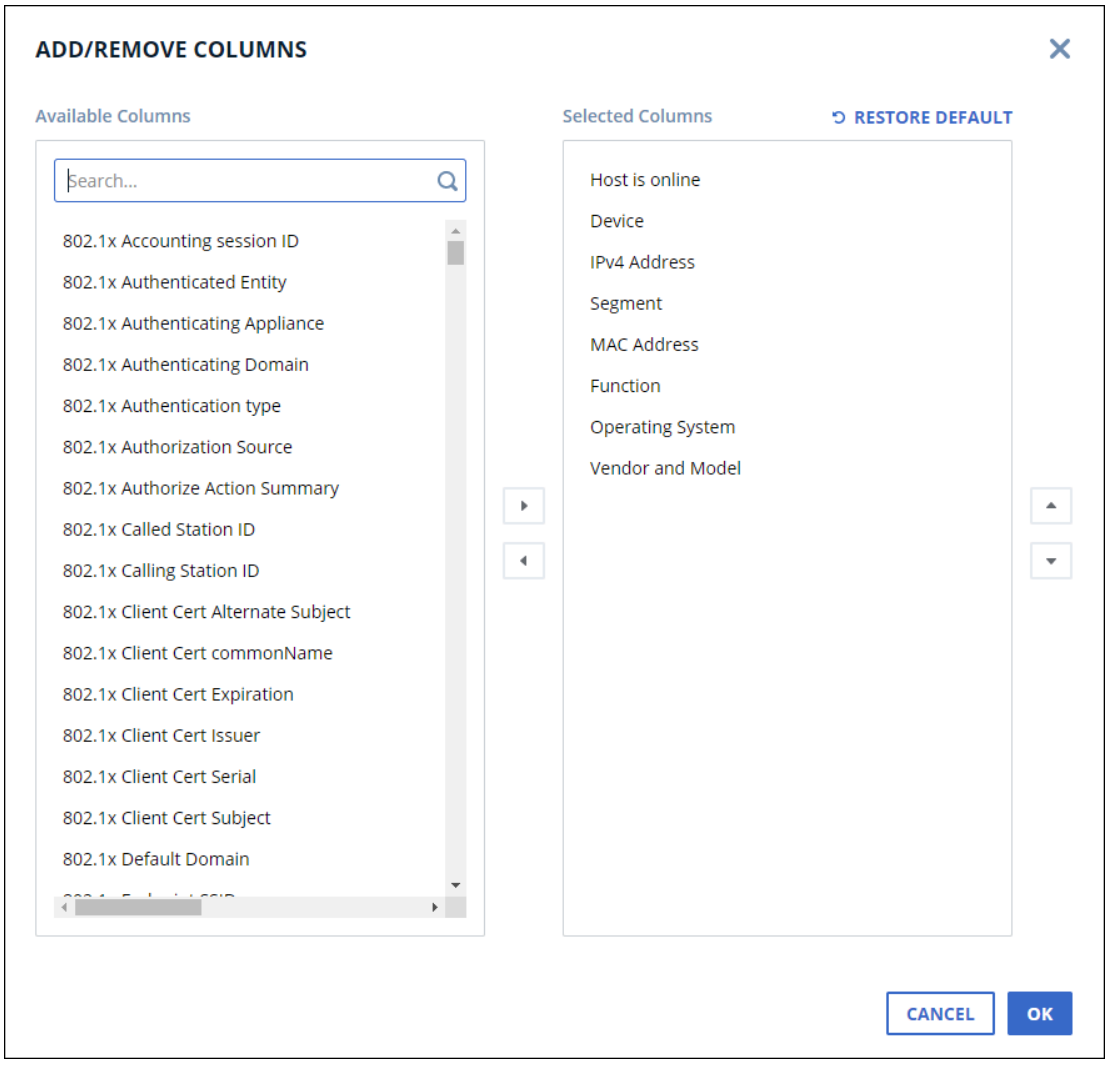
At any time, you can revert to the initial (default) column display provided at the time of installation.

To add or remove columns in the Assets view:

1. Access Assets view via the Dashboards view: For the Web Client, see Logging In to Forescout Web Portals. .
2. Select ☰ at the top-right of the page in the Assets view.



3. Select Add / Remove Columns...



4. In the Available Columns list, select the columns that you need to add and then select ▸.
5. In the Selected Columns list, select the columns that you need to remove and then select ◂.
6. To sort the order of the selected columns for the Assets view, select a column name, and then select ▲ to move the column up, or ▼ to move the column down.
    - Moving a column one place up or down in Add / Remove columns - Selected Columns corresponds to moving that column one place to the left or right in the Assets view.

      Note:

      To restore the original default set of columns and their initial order in Assets view, select Restore Default above the Selected Columns list.

      Note:

      The Host is online column contains an • icon that indicates the online / offline status of the device represented in the row.
7. To save the configuration, select OK.

View the details for a device in the Forescout eyeSight Assets view

To view the details for a specific device:

1. Access Assets view via the Dashboards view: For the Web Client, see Logging In to Forescout Web Portals.
2. Select the icon to the left of the row for the specific device.

   The Device Details area for the selected device is divided into logical categories, accessed through a list of tabs. When you select a tab, the properties associated with the category are displayed to the right of the tab. The General (category) tab is selected by default.

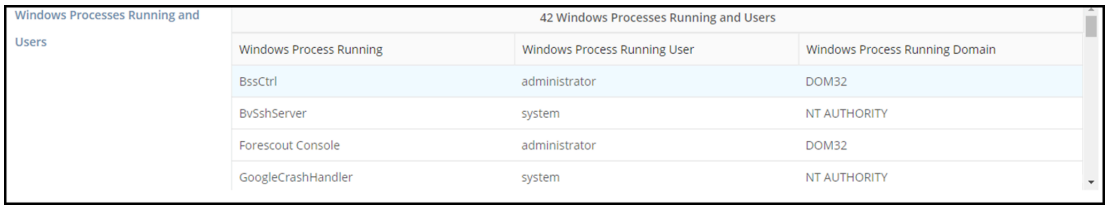
   The categories and their associated properties include:

General	Displays widely used device information, such as OS details, IP and MAC addresses, IP Reuse Domain, running processes, and listening ports, related to Forescout and third-party plugins, as well as hotfixes.
User	Displays user roles and logged-in status, for access to Forescout and third-party plugins.
Network Access	Displays network access information, such as MIB, switch ports, and WLAN, related to Forescout and third-party plugins.
Peripherals	Displays information about external devices that work with Forescout and third-party plugins.
Applications	Displays information about applications installed on the device for working with Forescout and third-party plugins. Application type examples are peer-to-peer, cloud storage, and IM.
Security	Displays information about antivirus, spyware, vulnerabilities, software updates, and compliance, for Forescout and third-party plugins.
Authentication	Displays information about authentication, such as for appliances, modules, states, methods, and certifications, for Forescout and third-party plugins.
Health Monitoring	At a glance, real-time data that helps you monitor and improve the health of Forescout Appliances in your deployment.
Risk	Displays real-time data that helps your security teams to identify and prioritize the different vulnerabilities, allowing them to focus on the devices with the highest risk.

Note:
A specific category tab is displayed only when there is relevant information for the selected device.

For properties with long lists of values, use the scroll bar to move up or down the list.

Device Details displays composite properties in the form of a table. In the example below, the Windows Processes Running and Users item consists of Process Running, User, and Domain properties.

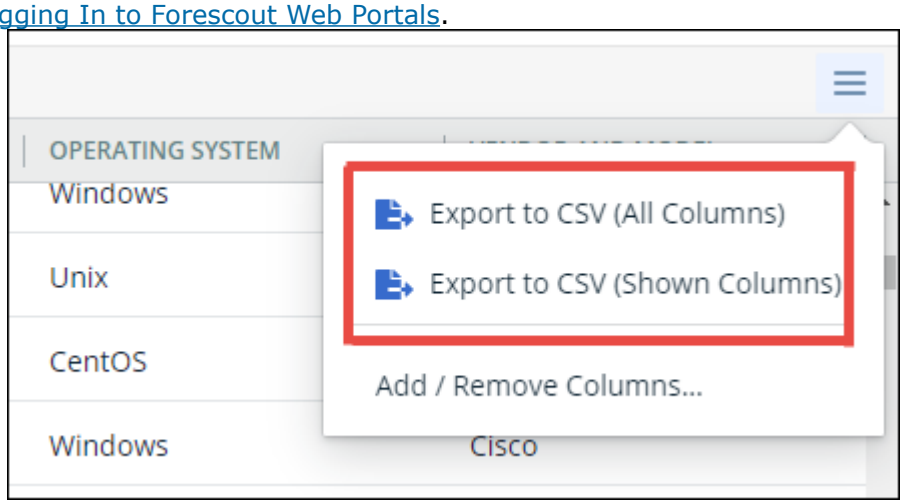


Export Forescout eyeSight device list to CSV file

From the Assets view, you can export a drilled-down list of devices to a CSV spreadsheet for offline analysis. You can export the device list (as is) with data from only the currently displayed columns on the page, or you can optionally export the device list with data from all columns in the database.

To export a list of devices to a CSV file:

1. Access Assets view via the Dashboards view: For the Forescout eyeSight Web Client, see Logging In to Forescout Web Portals.



2. Select ☰ at the top-right of the page in the Assets view.
3. Select from the drop-down menu:
   - Export to CSV (All Columns), to include data from all database columns
   - Export to CSV (Shown Columns) to include data from only the currently displayed database columns in the Assets view.

The file name of the exported CSV has the following format:

"Devices_" + YYYY + "_" + MM + "_" + DD + "_" + hh + "_" + mm + ".csv"

For example, Devices_2019_08_26_11_53.csv”

Note:

Once the file download has initiated, if you click to export the same file again (without changing the set of devices displayed in the Assets view), a second file download will not initiate if the first file download has not finished.

Generate Forescout eyeSight reports and logs

Your Forescout Console is equipped with powerful report generation tools.

On-Screen Threat Protection Reports

These reports provide you with important system information about policies and detections; the services most frequently targeted by malicious endpoints; the origin of a worm outbreak or the infected endpoints in each network segment. You can also generate detailed reports on events, such as the number of probe and infection attempts per host or service, or the number and types of marks distributed over a time period. See On-Screen Threat Protection Reporting for details.

Real-time reports

You can generate comprehensive real-time reports regarding policy detections and endpoint discovery information. See Reports Portal for details.

Automated updates to these reports are available via the Modules pane.

Audit trails reports

You can view user audit trail reports that contain information about user activities during a specified time period. These reports can be exported. See Monitoring User Activity for details.

Forescout eyeSight on-screen threat protection reporting

This section details the Console reports.

Report results display activity that occurred within a specified time range for the Appliances that you select. For example, you can generate a report that covers a two-day, two-week, or two-month period, for one, several, or all the Appliances in your enterprise. By default, all Appliances are selected.

Note:
Reports may include information about both bites and infection attempt events. The bite event is the event in which the endpoint used a mark to try and gain access to your network. An infection attempt event is an event followed by a bite event that is detected at an open, real port on the service where the bite event was detected.

Executive reports

The Executive Report provides a concise overview of important Forescout platform and endpoint activities.

Report	Details
Executive Summary	A detailed briefing of malicious endpoints activity and policy detections in your network during a specified time period. The report provides: • Information about endpoints detected via the policy. • Top 10 infected endpoints. The report shows the IP address of the endpoints that have carried out the most infection attempts, and the number of infection attempts carried out • Infected/Targeted Hosts per Service: Shows the number of infected endpoints that attempted to infect a service, and the number of endpoints in the network at which an infection attempt was carried out for that service • Event summary showing important Forescout platform and endpoint events.. Report customization options let you adjust the following for the top 10 reports: • Display only results greater than a set value. • Update, for example, the top 10 value to top five or top 15.

Operational reports

Operational reports provide extensive information about probe, scan, bite, and infection attempt events that occur at targets, endpoints and services in your network. These reports allow in-depth drill-down of security information gathered by Forescout products.

Report	Details
External Blocking	Provides information about external blocking activity, including: • Domains targeted outside your network and blocked • Endpoints that attempted to infect domains outside your network.. • Infection attempts targeted at domains outside your network. By default, the top 10 infected endpoints are displayed. This value can be changed from the Report Options dialog box.

The following reports show information about infected endpoints in your network.

Report	Details
Worm Originator	Displays the origin of a worm outbreak, tracking down the worm host to where it was originally detected in your network.
Infected Hosts by Segment	Displays the infected endpoints in your network, sorted by segment. Report options let you generate a table that lists the details of all the events shown in the

Report	Details
	report.
Infected hosts by Service	Displays the infected endpoints in your network, sorted by service. Report options let you generate a table that lists the details of all the events shown in the report.
Top Worm-Infected Hosts	Displays the IP addresses of infected endpoints that carried out the most infection attempts. By default, the top 10 infected endpoints are displayed. This value can be changed from the Report Options dialog box. Report customization options also allow you to: • Display only results greater than a set value. For example, show results only if infected endpoints initiated more than 10 infection attempts. • Generate a table detailing report events.

The following reports give results of endpoint probing.

Report	Details
Probing Hosts by Segment	Displays the probing endpoints in your network, sorted by segment.
Probing Host by Service	Displays the probing endpoints in your network, sorted by service.

The following reports give details of email worm infection attempts.

Report	Details
Top email Infected Hosts	Displays the endpoints in your network that generated the most email worm infection attempts. By default, results are limited to the 10 most active endpoints. You can change the default setting. Additional report customization options let you display only results greater than a set value. For example, show the results only if the endpoints generated more than five email events.
Email Infected Hosts per Segment	Lists endpoints in your network that generated email worm infection attempts, sorted by segment. Important information about each endpoint is presented, including the email address from which the attempt was made, the number of senders, and the number of mails sent.

Report	Details
Related Worm Names for Hosts	Displays endpoints, and names of high-profile worms that performed activities similar to that of the endpoint. You can load the most current related attack name file by selecting Load Related Attack Names from the Tools menu. This option installs new related worm names and the associated services that they attacked. Updated files can be found on the support page of the Forescout website.

The following reports display information about infection attempts that occurred at the endpoints in your network.

Report	Details
Top Infection Attempts per Host	Displays the most frequently targeted real endpoints in your network. The report lists the endpoint IP addresses and the number of infection attempts at each real endpoint. By default, the 10 most frequently targeted, real endpoints are displayed. This value can be changed from the Report Options dialog box. Additional report customization options let you display only results greater than a set value. For example, show the results only if the real endpoint was targeted more than 10 times.
Infection Attempt Summary for a Selected Host	Displays all infection attempts that targeted a specific endpoint. Report options let you generate a table that lists the details of all the events shown in the report. For example, the date and time the event occurred and the endpoint IP address that initiated the event.

The following reports display information about services targeted in your network.

Report	Details
Infected Hosts / Targeted Hosts per Service	Shows the number of infected endpoints that attempted to infect a service, and the number of endpoints in the network at which an infection attempt was carried out for that service. Report customization options let you adjust the following for the top 10 reports: • Results greater than a set value (calculated according to infected endpoints). • Update, for example, the top 10 value to top five or top 15 (calculated according to infected endpoints).
Top Infection Attempts per Service	Displays the top infection attempts per service. The report displays the service and the number of infection attempts at each service.

Report	Details
	This lets you evaluate which services in your network are more attractive to worms and can help in analyzing the security mechanism protecting these services. By default, the 10 most frequently targeted services are displayed. This value can be changed from the Report Options dialog box. Additional options let you display only results greater than a set value, for example, display a service only if it was attacked more than 10 times.

The following report display information about Scan policy results.

Report	Details
Scan Results	Displays information regarding vulnerable machines detected in your network. The report lists the name of the vulnerability, the number of machines at which it was detected, as well as the number of services closed. By default, the 10 most common vulnerabilities detected in your network are displayed. This value can be changed from the Report Options dialog box. Report customization options allow you to: Display only results greater than a set value. Generate a table detailing report events.

The following reports show activity statistics.

Report	Details
Infection Attempts Over Time	Displays the number of infection attempt events that occurred during a specified time period. Report customization options allow you to: Define the intervals at which results are displayed, i.e., hourly, daily, or weekly. Generate a table detailing report events.
Scan Detections Over Time	Displays the numbers of scan events that occurred during a specified time period. Report customization options allow you to: • Define the intervals at which results are displayed, i.e., hourly, daily, or weekly. • Generate a table detailing report events.
Top Bite Methods	Displays the most common bite methods used over a specified time period, as well as the number of times each method was used.

Report	Details
	By default, the top 10 bite methods are displayed. You can update this value from the Report Options dialog box. Report customization options also allow you to: • Display only results greater than a set value. For example, display results for a method only if the method was used more than 10 times. • Generate a table detailing report events.
Top Scan Methods	Displays the most common scan methods used over a specified time period as well as the number of times each method was used. By default, the top 10 scan methods are displayed. You can update this value from the Report Options dialog box. Report customization options also allow you to: • Display only results greater than a set value. For example, display results for a method only if the method was used more than 10 times. • Generate a table detailing report events.
Top Mark Types	Displays the top mark types distributed during a specified time period, as well as the number of times each mark type was distributed. By default, the 10 most frequently distributed mark types are displayed. You can update this value from the Report Options dialog box. Report customization options also allow you to: • Display only results greater than a set value. For example, display results for a mark type only if the mark was distributed more than 10 times. • Generate a table detailing report events.
Top Always Allowed Services	Shows the *always allowed services* that were most frequently accessed by blocked endpoints. Always allowed services are defined when creating exception rules from the Virtual Firewall pane. The results of this report help you evaluate the implications of maintaining always allowed services. By default, the 10 always allowed services that were most frequently accessed are displayed. This value can be changed from the Report Options dialog box. Report customization options also let you: • Display only results greater than a set value. For example, only show services that were accessed more than 10 times. • Generate a table detailing report events. See Managing Your Virtual Firewall Policy for details.

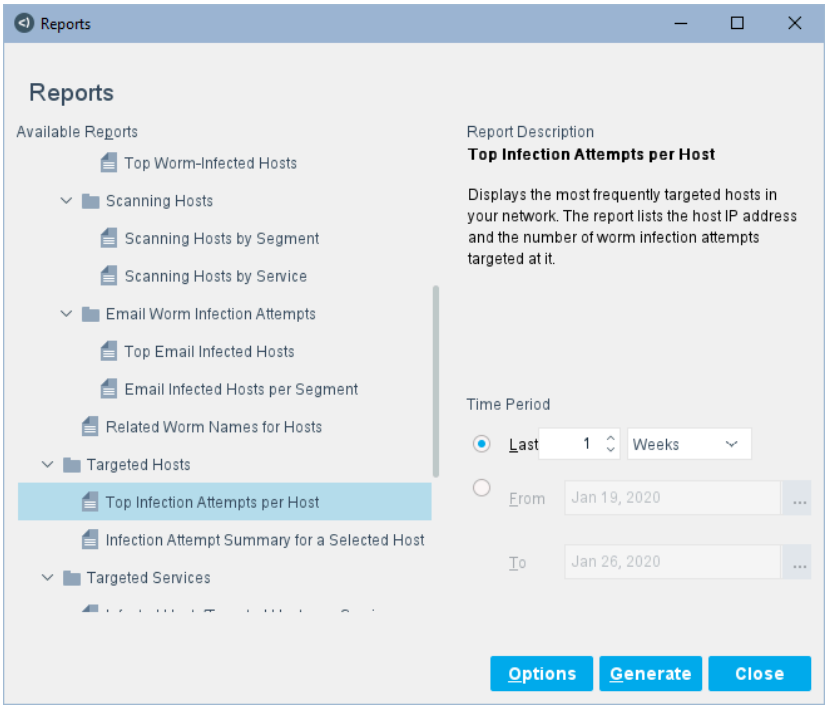
The following report displays information per Appliance.

Report	Details
Hosts Per Appliance	Displays the number of endpoints handled at each Appliance in your enterprise as well as the average for all Appliances. By default, all Appliances are displayed.

Generate on-screen threat protection reports

You can generate reports on-screen and access the on-screen management tools, such as printing and exporting reports.

To generate a report, select Reports > Threat Protection Reports > New.



To display a list of open report windows, select Window>Reports and then select the report to open.

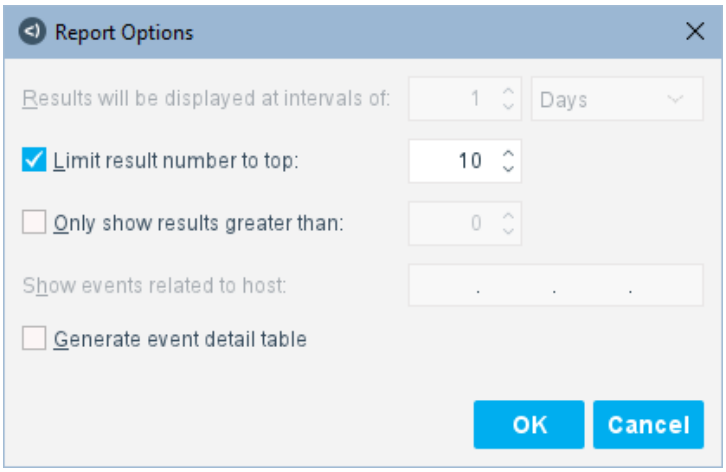
In a report window, select View>Report Definitions to display the definitions used to generate the report.

Customize reports

Reports are generated with default customization options. These options can be modified so that you can better manage results and view information that is important to you. The following report customization options are available for reports. Not all customization options are applicable to all reports.

If you update a default, it is only applied to the current report; after the report is generated, the default is restored.

In the Reports dialog box, select a report and time period, then select Options.



Results will be displayed at intervals of	Enter a numerical value and select a time unit.
Limit result number to top	The number of top results to display. For example, enter 5 to report the five endpoints with the most events.
Only show results greater than	Enter a thresholds value. For example, enter 20 to only report endpoints on which 20 events occurred.
Generate event detail table	When this option is enabled more detailed information is available from the report toolbar.

Work with on-screen report management tools

On-screen tools are available to manage and navigate your reports. These tools can be accessed from the menus and the report toolbar.

	First/Last Page Moves to the first or last page of the report. (Only available when the report is displayed in print layout view).
	Previous/Next Page

	Moves to the previous or next page of report. (Only available when the report is displayed in print layout view).
	Print Report Sends the report to the printer.
	Save Saves the current report to a file. The file is automatically saved to a default location, which you can change if required. You can open saved reports from the Reports menu on the Console.
	Print/Normal Layout View Displays the report in print layout view or normal layout view. The cover page and the header and footer are visible in print layout view.
	Displays the report chart or the event detail table, if you generated one.

Save reports

The reports you save are stored by default at the location where you installed the Console.

Select Reports > Threat Protection Reports > Manually Saved Reports to open a saved report.

To change the location for manually saved reports, select Options > Console Preferences > Misc > Reports.

Reports portal

You can access a web-based Reports Portal to generate comprehensive real-time and trend information about policies, vulnerabilities and the network inventory.

The Reports Portal is enabled by the Reports Plugin, a component of the Forescout Core Extensions Module.

Note:
When running in Certification Compliance mode, the Reports Portal is disabled.

To access the portal, see Logging In to Forescout Web Portals.

The Reports Plugin lets you generate reports with real-time and trend information about policies, host compliance status, vulnerabilities, device details, assets and network guests.

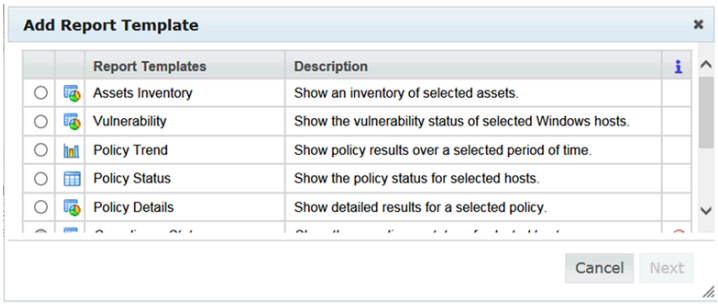
Use reports to keep network administrators, executives, the Help Desk, IT teams, security teams or other enterprise teams well-informed about network activity. Reports can be used, for example, to help you understand:

- Long term network compliance progress/trends
- Immediate security needs
- Compliance with policies
- Status of a specific policy
- Network device statistics

You can create reports and view them immediately, save reports or generate schedules to ensure that network activity and detections are automatically and consistently reported.

In addition, you can use any language supported by your operating system to generate reports. Reports can be viewed and printed as either PDF or CSV files.

To add a report, select Add from the Reports portal home page. Select a report template, then select Next to define parameters and generate the report.



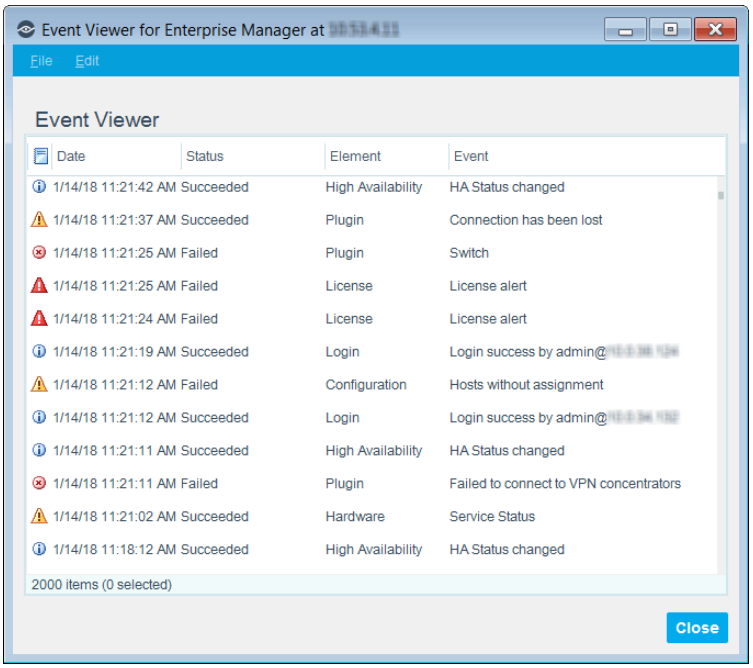
Work with system event logs

You can view logs about system activity, for example, successful and failed user login operations.

Not all users have access to this feature.

An option is also available to forward various event messages to third-party logging systems via the Syslog Plugin. For details, refer to the *Syslog Plugin Configuration Guide*..

To view events, select Log > Event Viewer from the Console menu, and define a time period.



The following information is available:

Severity The severity level of a system event indicated by a colored icon.

Emergency

Alert

Critical

Error

Warning

Notice

Information

Debug

Date	The date and time when the event occurred.
Status	Whether the operation succeeded or failed.
Element	The resource or component the operation was performed upon (for example, users).
Event	The name of the event that occurred.

Double-click an entry in the log to view more details about the event.

Select File>Clear All to clear all data from the table. This information remains in the system. Select File>Reload to load the latest data from the database.

Select Edit>Find to search for a text string in the event viewer.

Select File>Exports to save the log to a TXT or XLS file.

View block events

A Block Events log provides an at-a-glance display of the block events for the Virtual Firewall (VFW) and threat detections. For example:

- Host blocks
- Port blocks
- External Port blocks
- External Host blocks
- Services closed as a result of service attacks
- Services closed as a result of the blocking rules that you defined via the Virtual Firewall

Use the log to troubleshoot problematic network block events. You can export the information to a CSV file.

Note:
These events are sent automatically to the Syslog server. If you do not want to send them, configure the Forescout Syslog Plugin to not transfer this information. Select Tools > Options > Modules > Core Extensions > Syslog > Configure > Events filtering .

Note:
Block event logs do not provide Switch or WLAN block events at this time.

To view blocked events, select Blocking Logs from the Log menu, and then define a time period.

The following information is available:

Host	The endpoint that was blocked.
Target	The IP address to which the blocked endpoint attempted to connect.

Time	The time when the endpoint was blocked.
Service	The service at which the endpoint was detected when it was blocked.
	Indicates whether the block event was the result of a Virtual Firewall block rule.
Reason	The reason the source was blocked.

Select View>Find to search for text.

If you selected a relative time when generating the block events list, select File>Refresh to include events blocked from the indicated start time, up to and including the current time while the dialog box is open.

View a history of monitored and blocked services

Your system policy may be defined so that your system monitors or blocks selected services in your network. You can view a history of the services that were monitored or blocked during a specific time period.

For information about how to work with these policy definitions, see Handling Service Attacks

Select Log>Service Attack History and define a time period.

The following information is available:

Service	Displays the port and protocol of service.
State	Displays the state, i.e., if the service was blocked or monitored. Use your cursor to view a tooltip that lists the IP addresses of endpoints that scanned the service, and the endpoint IP addresses that they probed. Normal indicates that the service state was removed.
Date	Displays the date and time when the monitor or block state was initiated.
Related Worms	Displays the name of a related worm. A related worm is the name of a known worm that performed events similar to the events carried out by sources in your system. For example, if a source scans port 1434/UDP more than once, the worm name Slammer is displayed as a related worm name because this is the

	service that the Slammer worm attacked.
Appliance	Displays the dedicated device that monitors traffic going through your corporate network.

Exporting reports and report event details

You can export reports and report event detail tables in the following formats:

- PDF file, view in Adobe Acrobat
- CSV file, view in Microsoft Excel
- HTML format, view in your web browser

To export a report:

1. Select File > Export from the Console. A standard browse (Save As) dialog box opens.
2. Select the location and format in which to export the report.
3. To export the table, use the Save Event Table menu option to save the table as a CSV file, or the Export Event Table menu option to export the table as a PDF file.

Assets portal

The Assets Portal is a web-based search and discovery tool that lets you leverage extensive network information collected and correlated by Forescout products. This includes not only endpoint information, but also policy violations, login information, User Directory details, organizational mapping details, and endpoint device connections.

The information is valuable to groups across your organization, including:

- Security teams: Use an IP address to quickly locate and shut down switch ports and eliminate a security threat (from the Console).
- IT departments: Use an IP address to locate and contact users when maintenance is required at the endpoint.
- Help Desk: Effortlessly link IP addresses, computer hardware addresses, and switch ports to employees, in real time.

By using the portal, response time is shortened, translating into efficient remediation and crisis management.

In addition, you can clear event detections, and stop policy actions from the portal.

Note:
When running in Certification Compliance mode, the Assets Portal is disabled.

The Appliance runs a web server to operate the portal. (Access to the portal page requires a secured HTTPS connection, because the information displayed is sensitive.) During the installation of the Appliance, a default self-signed certificate is created for this purpose. However, the certificate was not signed by a known CA, which causes the web browser to display a security warning when network users attempt to use the portal. See The Certificates pane for details. You can turn off this option and transmit via HTTP.

Note:
The Assets view (part of the Forescout Web Client, see Assets View) does not replace the existing Assets Portal, but instead provides a newer interface with more robust filter/search capabilities. The Assets Portal allows users to clear event detections and stop policy actions. Depending on your needs, you may prefer to use one or the other, or both tools.

The Assets Portal runs in Internet Explorer, Chrome, and Firefox version 2 and above.

To access the portal from the Home view of the Console, right-click an endpoint in the Detections pane and select Information>Show in Assets Portal.

Search tools in the Assets Portal

To access the portal from the Home view of the Console, right-click an endpoint in the Detections pane and select Information>Show in Assets Portal.

Powerful search tools provide immediate access to an extensive range of endpoint and user information.

- Wild card searches: Search items are highlighted on the results page.
- Exact searches.

- Searches per category. For example, you can search by IP addresses, MAC addresses, Email addresses or DNS host names, and User Directory names.

From the Search Results page, you can easily pinpoint problematic endpoints, events, and users. In addition, action tools let you control endpoints directly from the portal.

The Assets Portal search result page indicates how many Appliances have been queried and how many responded to your Assets Portal search.

Hold your cursor over this string to view a tooltip that details this information.

Appliances disconnected at the time of the search are not queried. If you search for a specific address, the Appliance to which the IP address is assigned is queried. Other Appliances are ignored.

Expand information discovered by the Assets Portal

By default, Forescout eyeSight automatically discovers the following information about endpoints and displays that information in the Assets Portal:

- Domain User names
- NetBIOS host names
- MAC addresses
- DNS names
- Basic User Directory Plugin properties (this plugin is bundled with the Forescout eyeSight)
- Switch Plugin properties (this plugin is bundled with the Forescout eyeSight)

You can update the default to include additional information, for example, properties that are only available via the policy (Nmap details). See Endpoint Discovery Rules for details. You can also broaden the scope and capacity of the portal when you install plugins/modules. For example, if you installed the VPN Concentrator Plugin, related VPN properties are displayed in the portal. See Base Modules, Content Modules, and eyeExtend Modules for details.

Assets Portal information can be imported and exported by using standard import and export tools from your web browser.

Access the Assets Portal

Note:
You may need to verify that Assets Portal users can access the portal. By default, all users in the NAC network are granted access. If someone outside the Internal Network needs access or if, for some reason, you need to update the default, the setting can be modified. To update the setting, select Tools > Options > AccessWeb . If you remove a user from the default range, that user no longer has access to the portal. In addition, the user no longer receives HTTP actions defined as part of policies. Such actions include HTTP alerts, self-remediation, and login pages. It is not recommended to deny portal access.

To access the Assets Portal, see Logging In to Forescout Web Portals.

Perform an Assets Portal search

After logging in to the Assets Portal, you can use the search features to quickly and efficiently

pinpoint network information that you need.

Wildcard searches are automatically performed, meaning that the search results display all terms beginning with the characters that you enter. Alternatively, you can choose to look for only certain types of information, for example, only email addresses or DNS names.

Searches are not case sensitive.

The following options are available for performing endpoint-based searches:

- IP Address
- MAC Address
- DNS Name

The following options are available for performing user-based searches:

- Login Name
- User (from User Directory)
- LDAP User Name
- Email (from User Directory)

Note:
Searches are only available for previously detected endpoints. The User Directory search is only available for endpoints detected via a NAC policy or as a result of a Threats policy.

To perform the search:

1. Log in to the Assets Portal.
2. From the Home page, enter a value.
3. Alternatively, select a search type from the search drop-down menu.
4. Select Search.
5. The Search Results page lists the items that match the search query. If the search text was found in a field that is not shown by default, the value of the relevant field is shown in the More Info column.
6. Select an IP address or any other information item of interest or select any other linked item to continue the search. If the search produces only one result, the related ticket page opens. The Host Ticket page displays information about the selected item.

Host information	The IP address, MAC address, DNS host name, NetBIOS host name, and NetBIOS domain name for the endpoint.
User Details	Information about the logged-on user where the endpoint was detected.
Policy – Status	A list of the policies applied to the endpoint and the current endpoint status. You can select the Undo link to reverse any action taken at the endpoint, for example, releasing an endpoint if it is blocked. The blocking action will no longer be deployed at the endpoint for this policy, even if the endpoint is detected again.

	If you incorrectly reversed the action, you could return to the previous state by reassigning the action from the Home view, Detections pane.
Threat Protection Activity Detected	Details regarding malicious endpoints activity currently detected. **Manual Actions** Manual policy actions currently taken at the endpoint (actions carried out from the Home view, Detections pane).
Host Open Service	Services at the endpoint that are accessible to other network users, and the time the services were last detected. Basic information about the service is also provided.
Authentication Login Events	The most current authentication login events and the time when they were detected, for example, the last MAPI authentication or User Directory authentication. See also Clearing Events Detections.
Admission Events	The most current admission events detected and the time of detection. The following events may be detected: New IP: By default, endpoints are considered new if they were not detected at your network within a 30-day period. For example, if an IP address was detected on the first of the month, and then detected again 31 days later, the detection initiates the activation. The default time period can be changed. See Policy Preferences for details. IP Address Change Switch Port Change DHCP Request Authentication via the *HTTP Login* action Login to an authentication server SecureConnector connection

	If you have installed plugins or modules, additional admission event types may be available. For example, the *New Wireless Host Connected Events* option is available if you installed the Wireless Plugin. See also Clearing Events Detections.

The following user-based ticket results may also be displayed.

User Information	Displays the user login name entered to log in to the computer.	
	Machines Currently Logged On	Displays the last machine to which the user logged on. You can select the IP address or MAC address and view an endpoint ticket for that machine.
User Directory Server Information	Displays related user information.	

An icon in a row of the Host Ticket page indicates that additional information is available in a tooltip. Hold the cursor over the icon to view it.

An icon in a row of the Host Ticket page indicates that additional troubleshooting information is available. Place the cursor over the icon to view details in a tooltip. Select the icon to open the matching troubleshooting page. See On-Screen Troubleshooting for details.

Clear events detections

You can clear Event property detections, for example, admission or authentication login events. You may need to do this for troubleshooting purposes.

To clear an event, navigate to the event that you want to clear on the ticket page and select the Clear icon .

Manage your virtual firewall policy

Virtual Firewall protection lets you create network security zones, giving you greater control over network traffic. Specifically, by defining a Virtual Firewall policy you can:

- Create network zones or segments that you want to close off entirely as a result of new threats or newly detected vulnerabilities.
- Create network zones or segments that you want to close off to specific sources.
- Prevent the transmission of unwanted protocols within your network or between specific network segments, for example, if you know that RPC traffic should not be transmitted between various departments in your organization.
- Designate business critical services that should always remain open.

The Virtual Firewall gives you all the benefits of an inline firewall, without being located inline. This means there are no issues of latency. In addition, you can export a list of allow and blocking rules to a CSV file, and you can view a list of the block events detected as a result of the blocking rules that you defined.

Note:
If you create an exception rule via the Virtual Firewall and also create a policy rule that blocks detected endpoints, the Virtual Firewall exception rule takes precedence, i.e., the endpoints will not be blocked.

Virtual Firewall rules are centrally managed. Rules cannot be added, edited, or removed from individual Consoles that are part of your enterprise.

View Virtual Firewall rules

The Virtual Firewall pane displays rules generated from the following locations:

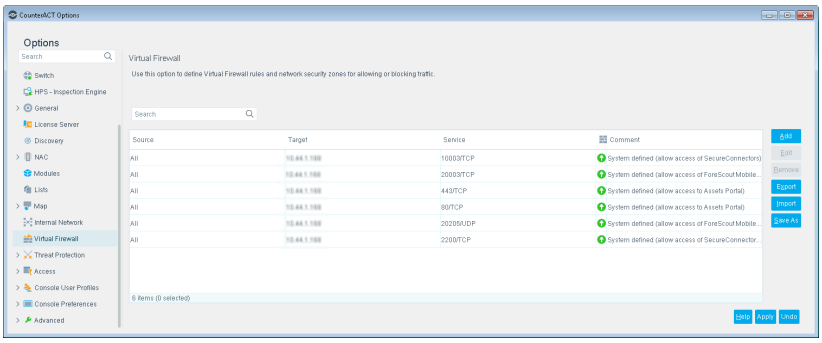
- Rules defined directly from the Virtual Firewall box, as detailed in this section.
- Endpoints detected as a result of a policy Virtual Firewall action.
- System-defined rules: These are rules that support basic Forescout features, for example, Authentication servers defined at the initial Console setup or Assets Portal access.
- Virtual Firewall rules manually defined from the Console, Detections pane.

Rules that appear in the Virtual Firewall pane that were created via the policy, Authentication Servers rule or manually from the Home view, Detections pane, cannot be edited or removed directly from the pane. These rules can only be modified from the feature where they were created.

Information in the Virtual Firewall pane is automatically updated for:

- Policy items if:
  - The rule is updated and no longer includes the Virtual Firewall action.
  - The IP address range or condition is changed and no longer includes the endpoints previously defined.
- Authentication Servers, if you remove, edit or add the server. See Defining Authentication Servers.
- Manual Virtual Firewall blocking, defined in the Home view, Detections pane, if you release the endpoint from this location.

To access the Virtual Firewall pane, select Tools > Options, and then select Virtual Firewall.



Virtual firewall policy priorities

Rules created directly via the Virtual Firewall pane take precedence over Virtual Firewall rules created via the policy.

The following hierarchies, from highest to lowest, are applied when an endpoint is detected as a result of different policies:

- Virtual Firewall – Allow Rule
- Threat Protection Policy – Threat Protection Blocked (source, port) and Virtual Firewall – Block Rule
- Group Definition – Authentication Servers (allow access)
- Policy – Virtual Firewall Block

View block events

Use the Events log to generate a report of block events. See View Block Events for more information.

TCP vs. UDP blocking

The Virtual Firewall is designed to block traffic that uses the TCP protocol, which represents over 95% of all traffic. With TCP traffic, three packets are sent before the first data packet. Each packet gives the Virtual Firewall an opportunity to terminate the session, making it very effective.

The Virtual Firewall can also block traffic using the UDP protocol, but its effectiveness depends on the nature of the service. With UDP traffic, the number of wait periods for response packets can take any value including zero.

If there is no response packet, there is no opportunity to intervene. The greater the number of packets sent, the more opportunities to terminate the session. Consider these examples:

- With syslog, there is no opportunity to terminate the session. The sender transmits the data message to the syslog server but does not wait for a reply.
- With DNS, there is a single opportunity to terminate the session. After the sender transmits a query, they wait for a reply. If the Virtual Firewall responds quickly enough with a "port unreachable" ICMP message before the server response, the session is terminated.

- With TFTP, the Virtual Firewall has multiple opportunities to terminate the session. Chunks of the files are transferred within individual packets, and each packet provides a termination opportunity.

Note:
To make sure that UDP sessions are terminated, it is recommended to block them using the Switch Port Access List or integrate eyeSight with a third-party firewall such as Cisco ASA. See Base Modules, Content Modules, and eyeExtend Modules for details.

Work with Block and Allow rules

Block rules use the Virtual Firewall to prevent outbound traffic at source IP addresses from reaching target IP addresses.

Use Allow rules to keep mission-critical services available. You can allow unconditional access at selected services in your protected and source network. This means access is permitted to and from the endpoint even when:

- The Threat Protection Policy is set to block
- The source is manually blocked or ignored
- The policy is set to block
- The policy for handling email worm infection attempts is set to block
- You have manually blocked an endpoint from the Home view, Detections pane
- You have assigned an identical blocking rule

Allow rules are not applied to endpoints that are blocked by external systems, i.e., switches, router, VPNs or firewalls.

To define Block or Allow rules:

1. Select Tools > Options. and then select Virtual Firewall.
2. To delete a rule, select the rule, then select Remove.
3. To modify a rule, select the rule, then select Edit.
4. Select Add. Define the following options.

Action	The action applied by this virtual firewall rule. Valid values are Allow or Block.
Source IP	Specify the IP addresses in your internal network to which the rule is applied. All IPv4 – include all IPv4 addresses in the internal network. Segment – select a named segment of IPv4 addresses. IPv4 Range – specify a range of IPv4 addresses.
Target IP	IP addresses that are blocked or allowed. Endpoints with IP

	addresses defined by the Source IP field can/cannot access these IP addresses. All IPv4 – include all IPv4 addresses in the internal network. Segment – select a named segment of IPv4 addresses. IPv4 Range – specify a range of IPv4 addresses.
Target Service	The services on Target IP endpoints that are blocked or allowed. All (TCP and UDP) – block/allow all services on the endpoint. Single – specify a port and protocol to block/allow. List – specify a comma-separated list of services.
Comments	A brief description of this rule's purpose.

5. Select OK. The rule is displayed in the Virtual Firewall pane.

Threat protection

A network threat is a device from which a malicious event, for example, a NetBIOS attack, was detected via a Threat Protection policy.

If you are using Flexx licensing, ensure that you have a valid eyeSight eyeControl license to use the full capabilities of this feature.

How threats are detected

This topic describes how infection attempts are carried out, and how Forescout eyeControl protects your network.

Note:
Forescout eyeControl detects and handles email worm infections differently than network worm infections.

During an infection attempt, self-propagating malware tries to establish connections with endpoints within your network. These are called "scans." After connections are established, the malware uses these connections to learn about the endpoints' available services and resources (ports). In response, the network sends information about these available services and resources back to the worm.

With this information, the malware carries out threats using known or new attack methods. Malicious traffic quickly infects your network through various entry points, such as VPN users, trusted partner networks, or vulnerable laptops.

The eyeSight prevents infection attempts by identifying and suppressing malware before it propagates within your network and to organizations outside your network. eyeSight eyeSight monitors traffic directed toward your network for signs of scans, and then identifies the techniques used to launch port or NetBIOS scans.

In response to this activity, eyeSight eyeControl generates virtual resource information sought by malware programs and sends the information back to them. This information is referred to as a mark. For example, if a request for a service in the network is identified, eyeSight eyeControl responds by creating and returning a mark in the form of the service requested.

Malware programs cannot distinguish between a mark and a legitimate network response. When malicious traffic attempts to access the network using the mark, the eyeSight immediately recognizes it and either:

- Continues to monitor it.
- Prevents the malware program from establishing communication with the network and external domains or with the service at which the infection attempt took place.

When an endpoint uses a mark, it is referred to as a bite event.

The eyeSight also automatically detects heavily scanned services and responds by either monitoring or blocking these services. When a service is monitored, the platform records all traffic going to the service. When a service is blocked, no communication with that service is permitted.

eyeSight eyeControl also responds to:

- Service attacks
- Emails worms

Worm slowdown mechanism

A worm slowdown mechanism, part of the threat protection technology, provides two significant benefits:

The worm slowdown mechanism enables Forescout eyeControl to notably reduce the amount of traffic generated by an infected machine while it attempts to propagate within your network. Specifically, the mechanism allows eyeControl to lock the infected machine in a static TCP dialog. As a result, traffic from the infected machine is kept at a standstill.

The worm slowdown mechanism keeps worm threads at a standstill, preventing them from reaching vulnerable endpoints within cells and at locations where there is no eyeControl protection. This is possible when the system locks an infected machine in a TCP dialog before the machine has a chance to infect other endpoints in the network.

Basic terminology

This topic lists and describes malicious host concepts and terminology.

Malicious Endpoints

A malicious endpoint is a machine from which a malicious event was detected, i.e., a worm infection or malware propagation attempt.

Cells

A cell is a group of endpoints that are monitored and protected by a single Appliance. eyeSight can see and intervene with traffic entering and exiting the cell. Traffic viewed is determined by:

- The network topology and the type of hardware that is placed in front of the Appliance, for example, a hub, router, or switch.
- The Active Response range handled. This is the range of IP addresses that are protected by the Threat Protection policy. This range must be included in the Internal Network.

Note:
Forescout eyeControl does not directly protect endpoints located in a cell against attacks initiated upon each other. However, intracell protection may be achieved by the worm slowdown mechanism. This mechanism prevents an infected endpoint from reaching vulnerable endpoints even within its cell. This happens when eyeControl locks the infected endpoint in a TCP dialog before the endpoint can infect the rest of the cell.

Scans

An endpoint-initiated scan is detected when an endpoint performs a specific probe a defined number of times within a defined time period. By default, when an endpoint initiates three probes within one day, Forescout eyeControl considers this activity a scan. The default probe count is five probes for port scans.

The system identifies the following scan categories:

- Finger
- HTTP
- Login
- NetBIOS (disabled by default)
- Port (Specific port scan categories, such as TCP or UDP port scans are also recognized.)
- SNMP

Port scan categories

The following port scan sub-categories are detected and displayed:

Vertical Scan	A vertical scan is detected when a defined number of UDP or TCP probes are carried out at a single endpoint.
Vertical UDP/TCP Scan	A vertical UDP scan or vertical TCP scan is detected when a defined number of probes are carried out either on UDP services or TCP services at a single targeted endpoint.
Horizontal UDP/ TCP Scan	A horizontal UDP scan or horizontal TCP scan is detected when a defined number of probes are carried out on the same service at a defined number of targeted endpoints.
Ping Sweep Scan	(ICMP) A Ping Sweep scan is detected when a defined number of Ping Sweep probes are carried out at any endpoint in the Active Response network.
TCP/UDP Scan	A TCP scan or UDP scan is detected when port scan activity does not meet the Vertical, Vertical TCP/UDP, Horizontal TCP/UDP, or ICMP scan recognition criteria.

The default probe endpoint count and required time range for port scans is five in one day. For example, by default:

- A horizontal UDP scan is detected when an endpoint probes the same UDP port on five different endpoints within one day.
- A vertical scan is detected when an endpoint probes five different services on the same endpoint within one day.

Use the Scan Details dialog box to change the default setting. See Customize Scan Settings for details.

Note:
Forescout eyeControl updates the port scan category when subsequent probe activity takes place within the defined time period. For example, if an endpoint probes a single endpoint at two TCP ports and one UDP, the port scan activity is categorized as a Vertical Scan. If an additional probe is carried out at another TCP port within the defined time period, the

category is changed to a TCP vertical scan.

The detected port scan categories are indicated in the Reason column in the Detections pane and on the Activity tab of the Host Details dialog box.

Probing Endpoints

A probing endpoint is an endpoint that has probed your Internal Network.

By default, probing endpoints are monitored by the system for 12 hours. During this time, Forescout eyeControl allows the endpoint to communicate with the network and records the endpoint activity. In addition, eyeControl responds by sending marks to the endpoint – virtual resource information required to carry out the infection.

If the endpoint continues to scan your network, the monitoring period is extended. If the probing endpoint uses a mark, it has performed a bite event, and it is blocked.

An option is also available to prevent probing endpoints from establishing communication with your network before they use a mark.

Bite event

A bite event is identified when an endpoint tries to gain access to your network using a system mark. When the endpoint uses a mark, it is referred to as a bite event.

The endpoint can be a probing endpoint or any endpoint that received and tried to use the mark. Endpoints that perform a bite are referred to as infected endpoints.

Infection attempt events

An infection attempt includes

- An event followed by a bite event that is detected at an open, real port on the service where the bite event was detected. Several infection attempts may occur after the bite event.
- An email worm infection.
- An event that was received as a lockdown event from another Appliance (for Appliances that are part of an Enterprise solution).

Infected endpoints

An endpoint is considered infected if it has used a mark to try to gain access to your network or if it has passed the email anomaly threshold.

Forescout eyeControl responds to infected endpoints by performing one of the following:

- Monitoring the infected endpoint: The infected endpoint is permitted to communicate with your network and domains outside your organization for a specified time period. During this period, eyeControl records the activity of the infected endpoint and distributes marks to it. These endpoints are referred to as monitored infected endpoints.
- Blocking the infected endpoints: The infected endpoint is prevented from establishing communication with the network and domains outside your organization for a specified time period. These endpoints are referred to as host blocked endpoints.

- Blocking the infected endpoint in the service it attempted to infect: The infected endpoint is prevented from establishing communication with the service it attempted to infect for a specified time period. These endpoints are referred to as port blocked endpoints.

The default block or monitor period for infected endpoints is 12 hours. If the infected endpoint performs another scan or uses any system mark during this time, the blocking or monitoring period is extended.

Your policy definitions determine how eyeControl responds to infected endpoints.

Manually Added Endpoints

Manually added endpoints are endpoints that you manually add to your system. When you add an endpoint, you enter an IP address, assign it a block or monitor or ignore state, and assign it a time for blocking or monitoring or ignoring the endpoint. Manually added endpoints cannot be blocked at ports (port block).

Lockdown endpoints for appliances registered with an Enterprise Manager

A lockdown endpoint is an endpoint that is blocked or monitored at one Appliance as the result of an event detected at another Appliance.

If one Appliance in your enterprise detected a bite event, a lockdown notification is sent to the Enterprise Manager, and the Enterprise Manager alerts the other Appliances that the endpoint performed the event. If the remaining Appliances detect that the endpoint is communicating with the network they are protecting, the endpoint is automatically blocked or monitored according to the policy. For more details, see Managing Enterprise Lockdown Alerts.

Diverse endpoints

A diverse endpoint is an endpoint that scans for multiple services. This may indicate that the source is a human attacker rather than a worm, which typically looks for one service across multiple endpoints.

Host block or monitor period

The block or monitor period for malicious endpoints is determined by your system policy. The default setting is 12 hours. If the endpoint performs another scan or uses any system mark during this time, the blocking or monitoring period is extended. For example, if the endpoint is blocked and after two hours uses a system mark, the 12-hour block period is restarted, and the total block time is 14 hours. If the endpoint does not perform another event, it is released when the block or monitor time has expired.

The expiration time for each malicious endpoint can be seen in the Detections pane in the Expires In column.

Email worms

Forescout eyeControl identifies and responds to email worms sent over email, detecting the worms when:

- More than a certain number of emails are sent within a specified time period.
- Certain attachment formats are sent within a specified time period.
- Numerous sender names are delivered from one endpoint within a specified time period.
- Multiple emails with the same subject are sent to different recipients within a specified time period.
- More than a certain number of emails are sent to several email servers within a specified time period.

This method of defense varies from the standard protection in that it does not deal with probing endpoints, but rather with email anomalies.

Service attacks

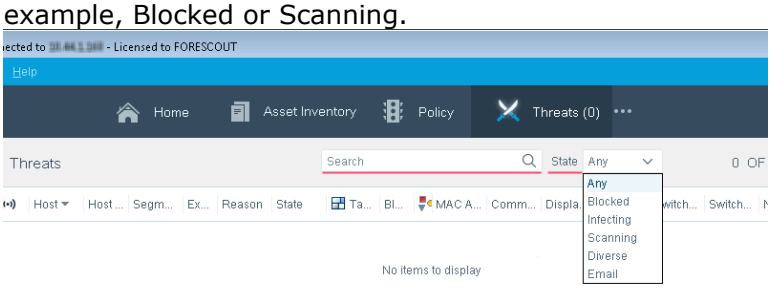
The Forescout platform identifies service attacks when a service-probing criterion is met, i.e., when a service is heavily probed by multiple endpoints. The platform calculates this criterion based on the size of the network. Service attacks are handled by monitoring or blocking all endpoints at attacked services only. This differs from the standard response to individual infected endpoints that are monitored or blocked at any service in the network or in the service that they attempted to infect. By default, most TCP and UDP ports are monitored. TCP ports 68, 80, 113, 443, and 1080 are ignored. UDP ports 68, 113, 1080, and 33434-33524 are ignored.

View threat detections

Endpoints detected by your threat detection policies are displayed in the Console, Threats view.

The Detections pane is updated with threat detection information when the Threats tab is selected. Quickly find threat detections of interest to you. Use the:

- Filters : See Working in the Filters Pane.
- Text search: Endpoints that meet the search requirements appear as you type.
- State filter: Filter the list to display endpoints that were resolved with a specific state, for example, Blocked or Scanning.



During periods of high activity, Forescout eyeControl stops displaying new endpoints scanning your network in order to give higher priority to the display of offensive endpoints. The threshold for switching to the High Activity mode is when 5000 malicious endpoints are handled simultaneously.

When this threshold is exceeded, new scanning endpoints are monitored but not displayed. If, however, the scanning endpoint performs a bite event, it is displayed in the Console. During high activity periods, the status bar in the Console reads High Activity Mode.

About the threat protection policy

Block worms using plugins

When working with plugins to block worms, you must create an associated policy rule to carry out the blocking action. Examples of these plugins are the Switch, Router and VPN Concentrator Plugins. Refer to the relevant plugin configuration guide for details.

You can use a policy rule to perform additional actions on the infected endpoint. For example, you can send email to the user at the infected endpoint, prevent the user from surfing the web, or check for vulnerabilities and deploy self-remediation patches.

Customize basic policy settings

Advanced policy tools let you customize how Forescout eyeControl identifies and handles scan and bite events, email worms, and more. For example, you can customize the period in which to monitor endpoints that use certain scan types and methods. NetBIOS scans may be monitored for a certain period of time while Port scans may be handled differently. You can also customize the block or monitor response according to the types of infection methods used. For example, you might block endpoints that carried out a NetBIOS infection attempt for four hours and monitor endpoints that carried out a Port infection attempt for one day. Options are also available to customize email notification status for various types of scan and bite events.

Advanced service attack options let you update the default response to service attacks, adjust the sensitivity level for identifying such attacks, and customize responses to various types of service attacks. You can also make mission critical services accessible to all endpoints or select specific ports that are accessible to specific endpoints.

Customize scan settings

Your system is installed with predefined scan values that determine:

- How to identify probing endpoints
- How to handle probing endpoints

These policy options let you customize these values for specific scan types and scan methods.

Customize bite settings

Your system is installed with predefined bite values. These parameters determine how Forescout eyeControl responds to infected endpoints.

The advanced policy options let you customize bite parameters. You can define different handling methods for various types of bite events. For example, a Login bite may be blocked for two hours, while a Port bite may be monitored only or blocked for two days. In addition, certain bite types may be handled by blocking the endpoint that performed the bite type in the service it attempted to infect, rather than blocking the endpoint from the entire network.

You can also customize the block or monitor response according to the type of mark used by the endpoint, and according to the machine that the endpoint attempted to connect to (virtual or real).

Bite type details

This section details the possible bite types.

Port Bite

Real/Virtual Host – Mark Used	Details
Trojan port	Detected when an endpoint tries to connect to a port used by Trojan horse software.
Known port	Detected when an endpoint tries to connect to a known service, for example, FTP or telnet.
Other port	Detected when an endpoint tries to connect to ports not belonging to Trojan or known ports.

HTTP Bite

Real/Virtual Host – Mark Used	Details
Virtual Port 80	Detected when an endpoint refers an IP address URL to a Virtual HTTP service.

NetBIOS Bite

Real/Virtual Host – Mark Used	Details
Hostname	Detected when an endpoint uses a Hostname mark during a NetBIOS session.
Share mark	Detected when an endpoint uses a Share name mark during a NetBIOS session.

Finger Bite

Real/Virtual Host – Mark Used	Details
Hostname	Detected when an endpoint uses a Hostname mark during a finger forward session.
User Mark	Detected when an endpoint uses a User mark during a finger session.

Login Bite

Real/Virtual Host – Mark Used	Details
User Mark	Detected when an endpoint tries to log in to a service using a user name mark.

Work with manually added endpoints

Manual endpoints are endpoints that you manually add to your system by entering an IP address and a state for that address into the system. If the endpoint sends a packet to your network, the system handles it according to the specified state.

The endpoint does not have to meet the scan criterion or use a system mark in order for the system to respond to it. You can later update the values defined for the endpoint or instruct the system to respond to it as it would any other endpoint. You can also manually set an endpoint state or duration for endpoints detected by the system – probing or offensive.

In addition to manually adding an endpoint to the system, you can change the state of an endpoint that was automatically detected by the system. Use this feature if you want to handle a particular endpoint in a different manner than defined in the Current Policy.

Note:
You cannot manually update an endpoint to the Port Block state.

Disable the worm slowdown mechanism

If necessary, you can disable the worm slowdown mechanism using the command `fstool wormdelay`. This option can only be carried out from the Appliance.

To disable or enable the worm slowdown mechanism:

1. Log in to an Appliance through the command-line interface (CLI).
2. Run the following command: `fstool wormdelay disable`.

   The following message is displayed:

```
CounterACT should be restarted for changes to take effect. Restart
CounterACT?
```

3. Type yes.
4. To enable the worm delay mechanism, use the following command: `fstool wormdelay enable`

Customize parameters for each scan type

The system handles the following scan types:

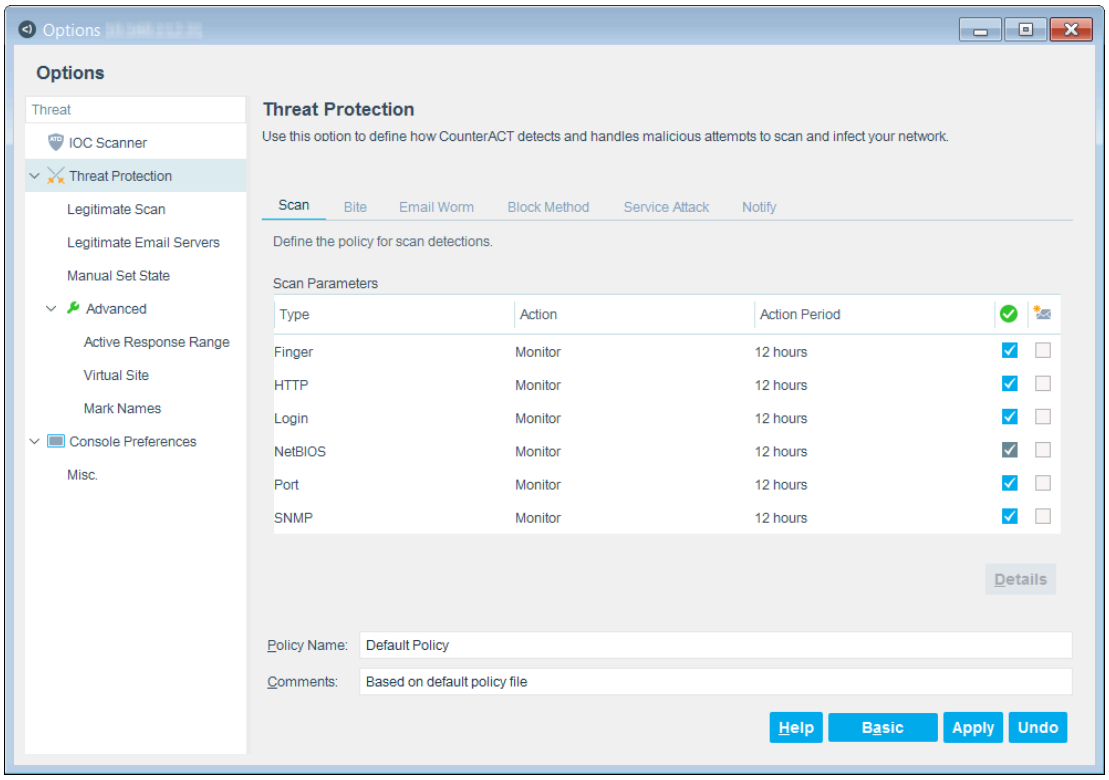
Finger	Forward Scan, Host Name Scan and User Scan
HTTP	Method Scan
Login	Password Scan and User Scan
NetBIOS	General Scan and Node States Scan
Port	Port Scan
SNMP	Community Scan and Port Scan

You can customize the following parameters for each scan type:

- Scan method
- The monitor or block response to probing endpoints
- The period that the probing endpoint is monitored or blocked
- The system's response to the scan event
- The email notification per event type

To customize parameters for each scan type:

1. Select Tools > Options, and then select Threat Protection.
2. At the bottom of the Threat Protection pane, select Customize and then select the Scan tab.



3. Double-click an Action field and select Monitor or Host Block from the drop-down menu.
   Note:
   Blocking NetBIOS, Port and SNMP scans that are UDP based is strongly discouraged. If you block these scans, an endpoint can scan your network using a spoofed endpoint IP address, in which case Forescout eyeControl will block the spoofed address instead of the scanning endpoint address.
4. Double-click the value in the Action Period column and update the time period.
5. Verify that the first checkbox is selected to enable system response to the event. Clear the checkbox for the system to ignore the event.
6. Select the second checkbox [operator email] to send email notification for this type of scan event.
7. Adjust the Policy Name and Comments if required. If you update the current policy and change the policy name, the new policy is automatically applied when you save the changes.
8. Select Apply to save your changes.
9. Select Basic to return to the basic policy settings. Alternatively, you can select Details to customize the scan recognition criteria for each scan type. For more information, see Customize Scan Recognition Criteria.

Customize scan recognition criteria

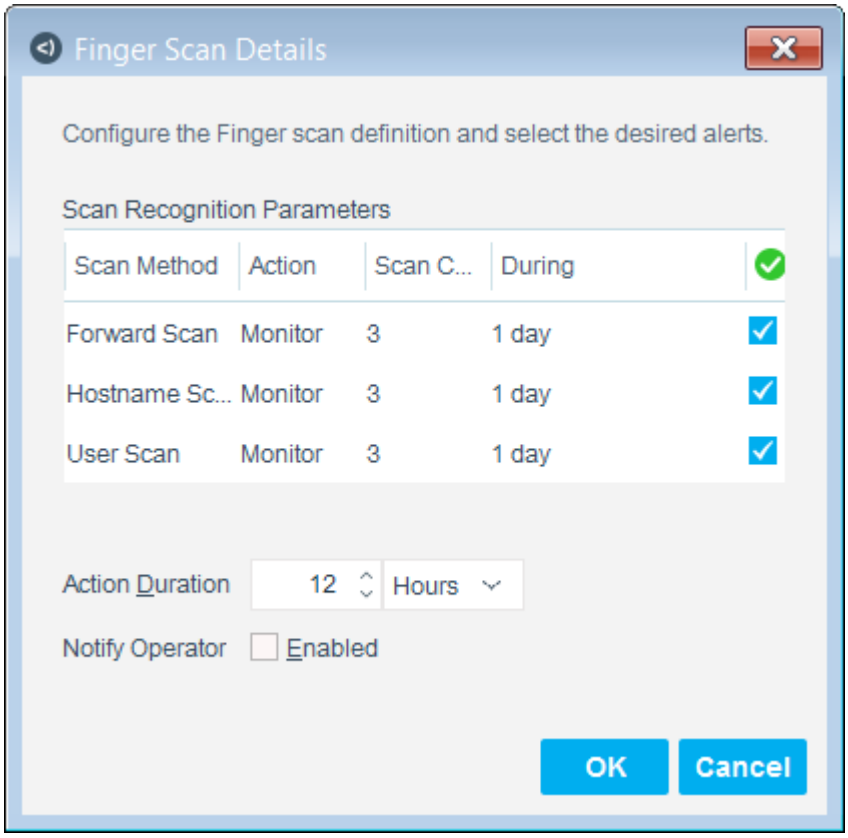
You can customize the scan recognition criteria for specific types of scan events. For each scan type, you can define the number of probe events that must occur within a specified period for the system to identify the probing endpoint. This is referred to as a probe count.

In addition, the system supports various scan methods for each scan type available. For example, a Login scan can be performed using the password scan or user scan method. Customization tools let you define different scan criteria for each scan method. For example, you can require endpoints using the Login password method to perform one probe within one day to be monitored, while

endpoints using the Login user method are required to perform nine probes within one day to be monitored.

To customize scan recognition parameters:

1. Select Tools > Options, and then select Threat Protection.
2. At the bottom of the Threat Protection pane, select Customize and then select the Scan tab.
3. Select a Scan Parameter row and select Details. The relevant Details dialog box opens.



4. Double-click the Action field to define how Forescout eyeControl will handle this scan.
5. Double-click the Scan Count field to define the number of probe events that must occur within a specified period for the system to identify the probing endpoint activity as a scan.
6. Double-click the During field to adjust the time interval in which the events must occur.
7. Verify that the checkbox is selected to enable detection of a specific scan method. Clear the checkbox for the system to ignore the event.
8. Update the Action Duration field to adjust the time interval in which the system blocks or monitors these endpoints. The value is applied to all methods listed. Use the drop-down menu to assign a unit of time.
9. Enable Notify Operator to send email notification to designated operators when the event occurs.
10. Select OK to save your changes and close the dialog box.

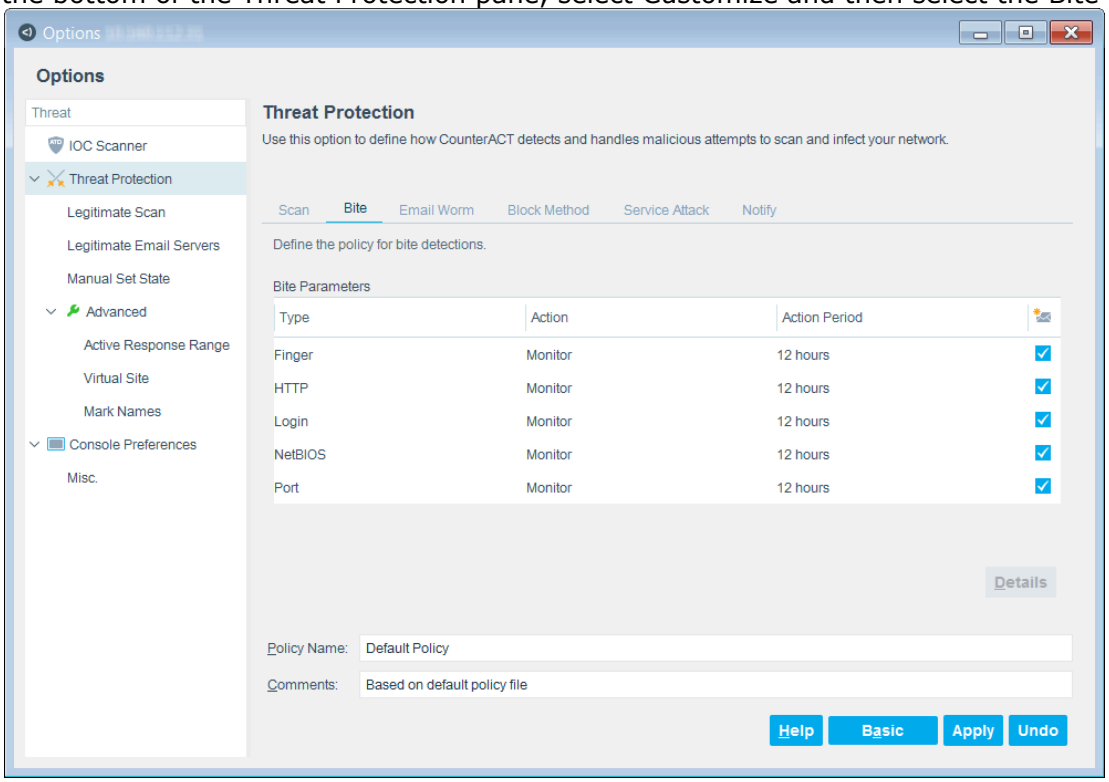
Customize block or monitor response to each bite type

You can customize the following parameters for each bite type handled by Forescout eyeControl:

- The block or monitor response
- The period that the endpoint is blocked or monitored
- Email notification for specific types of bite events

To customize bite parameters:

1. Select Tools > Options, and then select Threat Protection.
2. At the bottom of the Threat Protection pane, select Customize and then select the Bite tab.



3. Double-click the Action field for the required bite and select Monitor, Port Block, or Host Block from the drop-down menu.

   Note:

   If you update the action for a bite type to Port Block while the endpoint is blocked from the network, the Port Block is postponed until the Host Block period expires and the endpoint performs another bite.
4. Double-click the value in the Action Period column and update the period during which the system blocks or monitors this bite type.
5. Select the checkbox [operator email] to send email notification for this type of event.
6. Edit the Policy Name and Comments if required. If you update the current policy and change its name, the new policy is automatically applied when you save the changes.
7. Select Apply to save your changes.
8. Select Basic to return to the basic policy settings. Alternatively, you can select Details to customize the block or monitor response for each bite type, based on the kind of bite mark used. For more information, see Customize Bite Type Values.

Customize bite type values

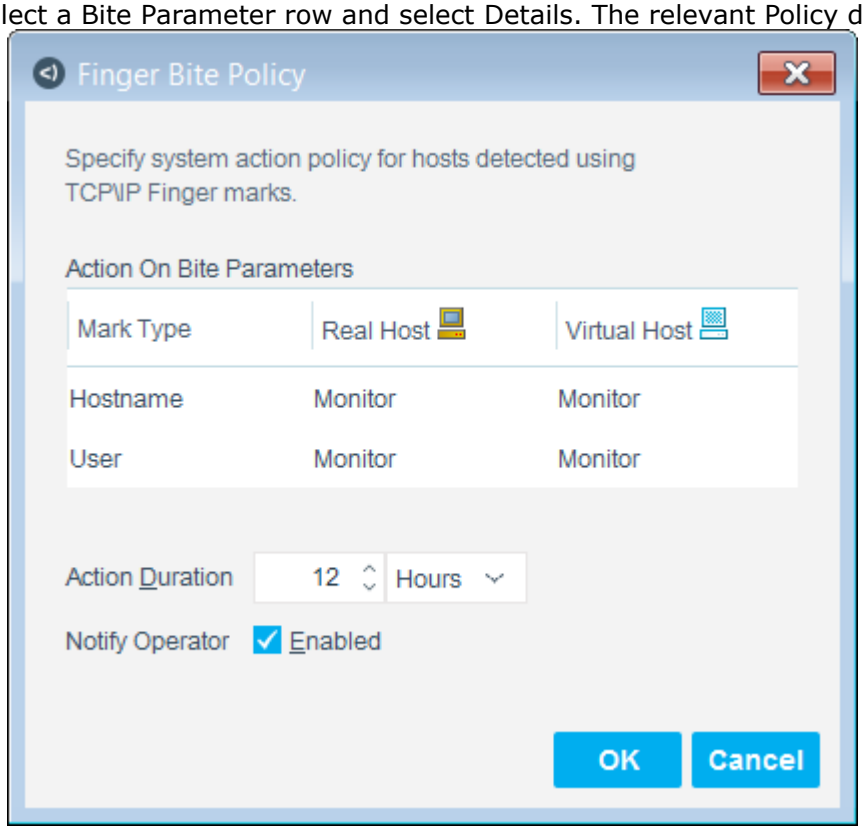
The system supports various marks for each bite type. For example, the NetBIOS bite method is an event in which a Hostname mark or Share mark was used. You can customize the block or monitor response for each type of mark and customize the block or monitor response according to

the endpoint that the infected endpoint attempted to connect to (virtual or real). For example, you can customize the policy to block NetBIOS bites only if they occur at real endpoints.

Note:
If the action is both blocked and monitored, the Bite Type field is disabled on the Bite tab.

To customize bite type values:

1. Select Tools > Options, and then select Threat Protection.
2. At the bottom of the Threat Protection pane, select Customize and then select the Bite tab.
3. Select a Bite Parameter row and select Details. The relevant Policy dialog box opens.



4. In each Real Host and Virtual Host column, select the required row, and then select Monitor, Port Block or Host Block from the drop-down menu.
5. Update the Action Duration field to adjust the time interval in which the system blocks or monitors endpoints that attempt to carry out this type of infection method. The value is applied to all mark types listed. Use the drop-down menu to assign a unit of time.
6. Enable Notify Operator to send email notification to designated operators when the event occurs.
7. Select OK to save changes and close the dialog box.

Customize email worm settings

Forescout eyeControl identifies and responds to email worms by detecting email worm anomalies that are sent over email. This varies from the standard method of defense, which provides protection as a result of endpoint bites. Anomaly thresholds can be configured.

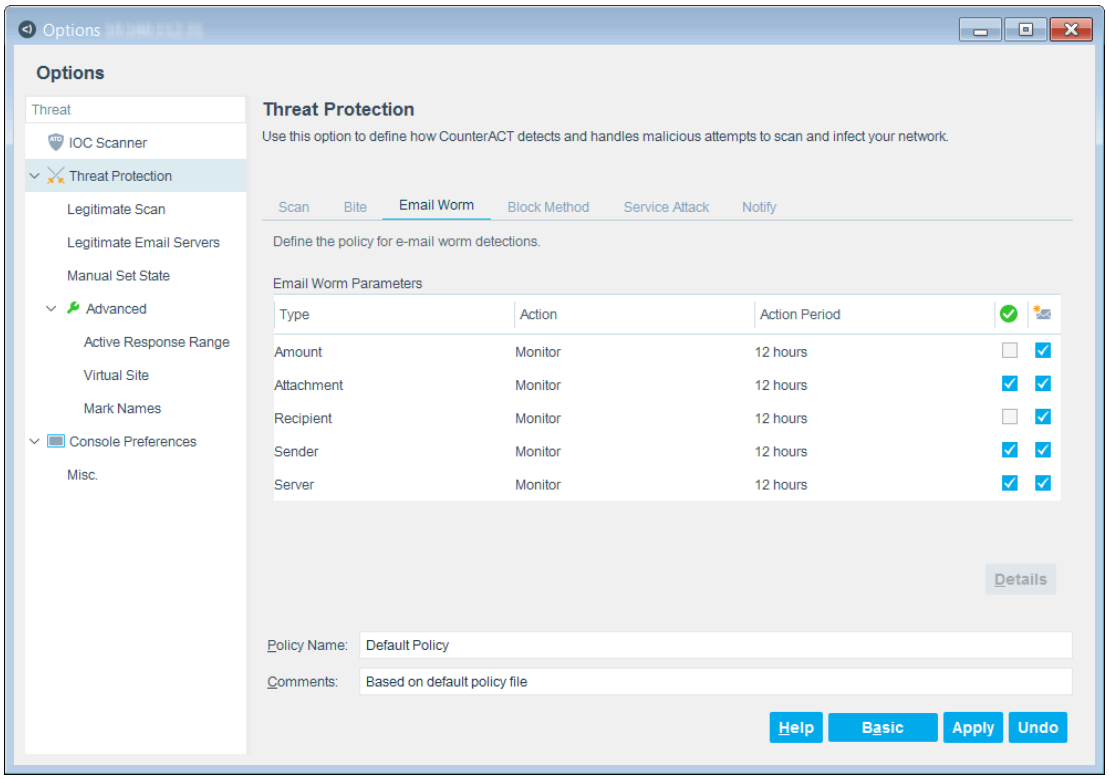
You can block or monitor endpoints that carry out any of the following email violations:

Amount	Endpoints that send more than a set number of emails within a specified time period. The default is 10 mails within one minute.
Attachment	Endpoints that send email with the following attachment formats within a specified time interval: .vbs, .vbe, .vb, .scr, .com, .pif, .bat, .shs, .exe, .wsc, .wsf, .wsh, .sct, .reg, .pcd, .mst, .msp, .msi, .msc, .mde, .mdb, .jse, .isp, .ins, .hta, .crt, .cpl, .cmd, .chm, .bas, .adp, .ade, .zip, .lnk, .inf, .job, .ini, .shb, .scp, .scf, .dll, .386, .acm, .asp, .avb, .bin, .cla, .cnv, .cs, .drv, .gms, .hlp, .nta, .hit, .mht, .mpd, .ocx, .ov, .sys, .tlb, .vxd, .wbt, .wiz To edit this list: Log in to the Enterprise Manager through the command-line interface (CLI). Run the command: `fstool smtp_extensions`. The file containing the list opens in a text editor utility. Repeat these changes on all Appliances.
Sender	Endpoints that send email from one machine using more than a certain number of sender names within a specified time period. The default three different sender names within one minute.
Recipient	Endpoints that send multiple emails with the same subject to different recipients within a specified time period. The default is 10 mails with the same subject within one minute.
Server	Endpoints that send email to a specified number of email servers within a defined time period. The default is 10 mails to 10 servers within one minute.

Information about email violations is displayed in the Detections pane and in the Host Details dialog box. In addition, you can generate reports regarding email worms. See Generating Reports and Logs for details.

To customize email worm settings:

1. Select Tools > Options, and then select Threat Protection.
2. At the bottom of the Threat Protection pane, select Customize and then select the Email Worm tab.



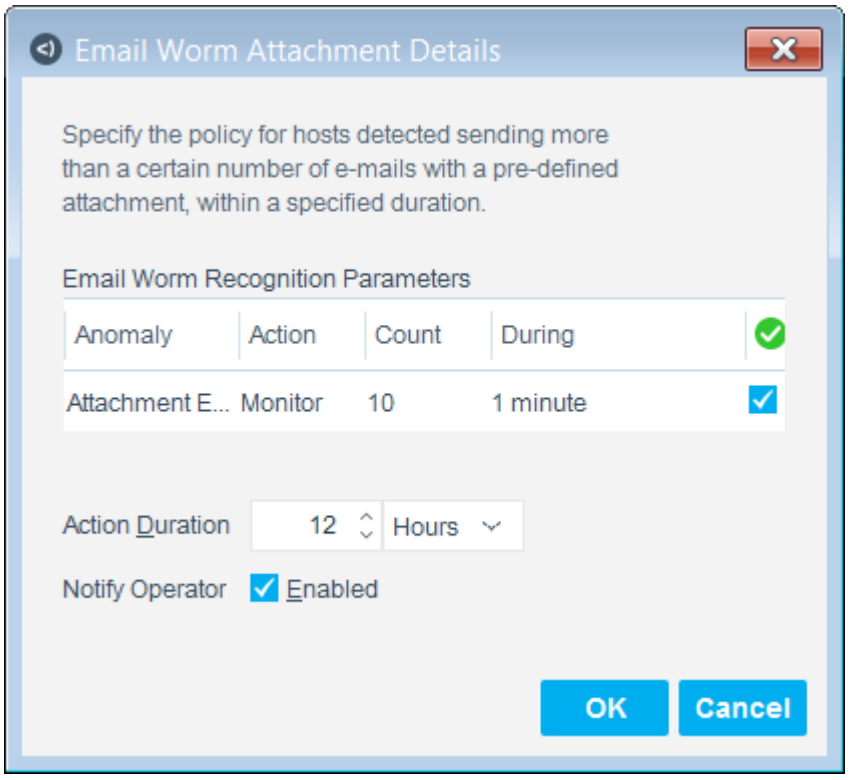
3. Double-click the Action field for the required email anomaly type and select Monitor, Port Block, or Host Block from the drop-down menu.
4. Double-click the value in the Action Period column and update the time period.
5. Verify that the first checkbox is selected to enable system response to the event. Clear the checkbox for the system to ignore the event.
6. Select the second checkbox [operator email] to send email notification for this type of event.
7. Edit the Policy Name and Comments if required. If you update the current policy and change the policy name, the new policy is automatically applied when you save the changes.
8. Select Apply to save your changes.
9. Select Basic to return to the basic policy settings.

Customize email anomaly recognition values

Forescout eyeControl recognizes various email anomaly patterns. For example, when more than a certain number of mails are sent from one machine to several email servers within a certain time period. You can customize the anomaly recognition patterns to suit your business environment.

To customize email anomaly recognition patterns:

1. Select Tools > Options, and then select Threat Protection.
2. At the bottom of the Threat Protection pane, select Customize and then select the Email Worm tab.
3. Select an Email Worm Parameter row and select Details.



4. Double-click the Action field for the anomaly and select Monitor, Port Block or Host Block from the drop-down menu.
5. Double-click the Count field to define the number of events that must occur within a specified period in order for the system to identify the anomaly.
6. Double-click the During field to adjust the time interval in which the endpoint must send the emails in order to be identified by the system.
7. Verify that the checkbox is selected to enable system response to the event. Clear the checkbox if you want the system to ignore the event.
8. Update the Action Duration setting to adjust the time interval in which the system blocks or monitors this anomaly type. Use the drop-down menu to assign a unit of time.
9. Enable Notify Operator to send email notification to designated operators when the event occurs.
10. Select OK to save the changes.

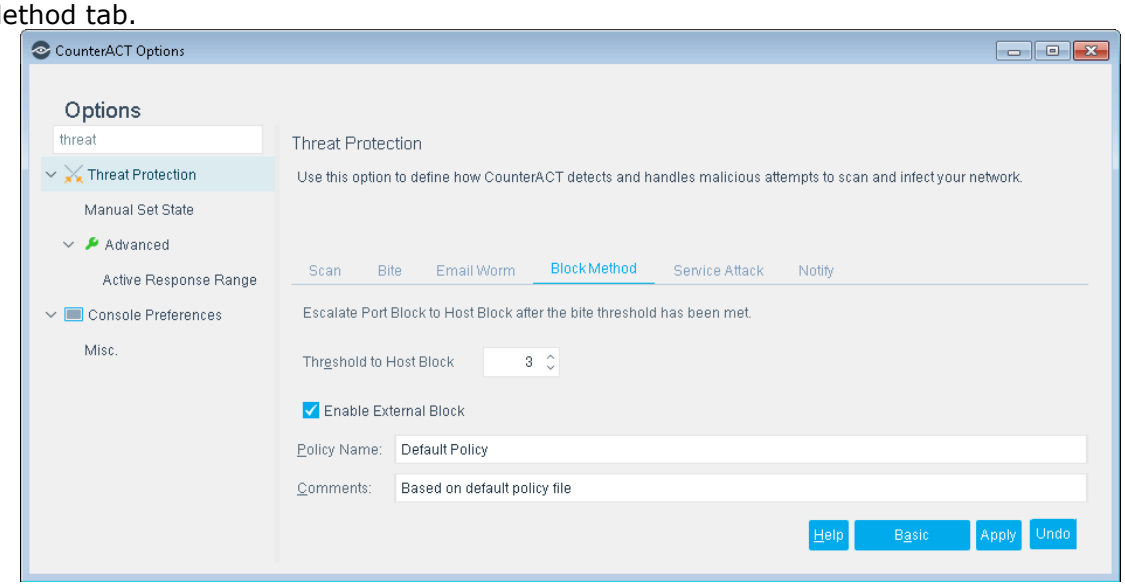
Configure the block method

The following options are available to help you fine-tune the Forescout eyeControl blocking mechanism:

- Update the escalate threshold for moving from Port block to Host block: When escalated, the endpoint is prevented from communicating with the entire network and endpoints outside the network rather than the service it attempted to infect. Port blocking is useful for letting the endpoint continue working with services that it did not attack.
- Disable the external block mechanism: By default, blocked endpoints are prevented from establishing communication with the network as well as with domains outside your organization. You can disable this mechanism to only block endpoints from your network.

To fine-tune the block method:

1. Select Tools > Options, and then select Threat Protection.
2. At the bottom of the Threat Protection pane, select Customize, and then select the Block Method tab.



3. By default, the Port block policy is escalated to Host block after the endpoint attempts to infect three separate services, i.e., when the third service is bitten. Set the Threshold to Host Block field to change the default setting.
4. Clear Enable External Block to block endpoints in the network only.
5. Adjust the Policy Name and Comments if required. If you update the current policy and change the policy name, the new policy is automatically applied when you save the changes.
6. Select Apply to save your changes.
7. Select Basic to return to the basic policy settings.

Handle service attacks

Forescout eyeControl identifies a service attack when a certain service-probing criterion is met. This criterion is automatically calculated and is based on the size of your network. The sensitivity threshold can be adjusted to identify the attack after fewer or more service-probing events occur.

Forescout eyeControl handles service attacks by monitoring or blocking all endpoints at attacked services in the network. This differs from the standard response to individual endpoints that attempt to scan or attack any port in the network.

By using the monitor option, all traffic going to attacked services is recorded for a defined time period and not just the traffic of the probing endpoint. After the time period has expired, eyeControl stops recording traffic in the services. If the service attack criterion is met again, endpoints are monitored again for the time set.

By using the block option, you are blocking all traffic to the attacked services for a defined time period and not just the traffic of the infected endpoint. After the time period has expired, traffic is allowed. If the service attack criterion is met again, endpoints are blocked again for the time period set. Use the block option to prevent worm attacks from reaching the service at other endpoints in your network.

By default, both UDP and TCP are monitored for 12 hours. TCP ports 68, 80, 113, 443 and 1080 are ignored. UDP ports 68, 113, 1080 and 33434-33524 are ignored.

You can disable this feature for either service. When disabled, traffic going to the selected service is neither blocked nor monitored. The response is disabled until you enable it again.

You can also remove the current monitor or block state endpoints in the service.

In addition, users listed in the Email configuration dialog box are sent an email notification alert whenever a service attack occurs.

Note:
Blocking services should be carried out carefully. When the service is blocked, no communication to the service is allowed for any endpoint, even if the endpoint is not malicious. Therefore, it is recommended to only monitor services.

UDP blocking prerequisites

To block endpoints at UDP services, you must configure your system to block with Forescout eyeControl and a firewall. Not all firewall products support service blocks. If your firewall does not support service blocks, you receive an error message.

How do I know when a service has been attacked?

The service attack indicator on your status bar flickers when a new service is attacked.

You can view service attacks from the Threats view, the Service Attack folder.

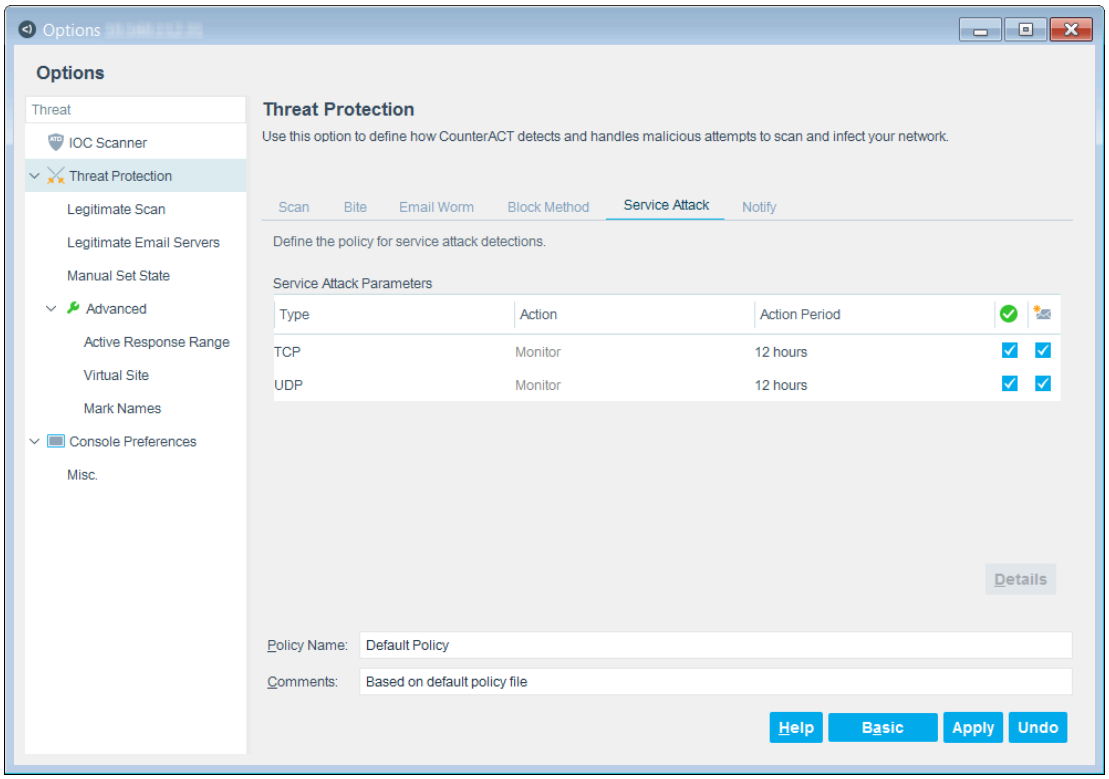
In addition, email alerts are sent when a service attack occurs, provided that you do not disable this option. The following tools are also available:

- Viewing the currently monitored and blocked services.
- Viewing a history of monitored and blocked services. See View a History of Monitored and Blocked Services.
- Displaying a report with the number of UDP/TCP scans that occurred during a specific time period.
- Sending service attack traps to your management station. See Base Modules, Content Modules, and eyeExtend Modules.

Set the service attack policy

To set the service attack policy:

1. Select Tools > Options, and then select Threat Protection.
2. At the bottom of the Threat Protection pane, select Customize and then select the Service Attack tab.



3. Double-click the Action field for TCP or UDP. From the drop-down menu, set one of the following actions:
    - Select Monitor to record all traffic going to the selected service.
    - Select Block to prevent all traffic from communication with the service.

    By default, service attacks are monitored for 12 hours. These settings can be customized on a per port basis. See TCP Customize Service Attack Criteria for details.

4. Double-click the value in the Action Period column and update the time period that the system blocks or monitors this type of service.
5. Verify that the first checkbox is selected to enable system response to the event. Clear the checkbox for the system to ignore the event. If the checkbox is cleared, service attacks will not be monitored or blocked.
6. Select the second checkbox [operator email] to send email notification when the attack occurs.
7. Adjust the Policy Name and Comments if required. If you update the current policy and change the policy name, the new policy is automatically applied when you save the changes.
8. Select Apply to save your changes.

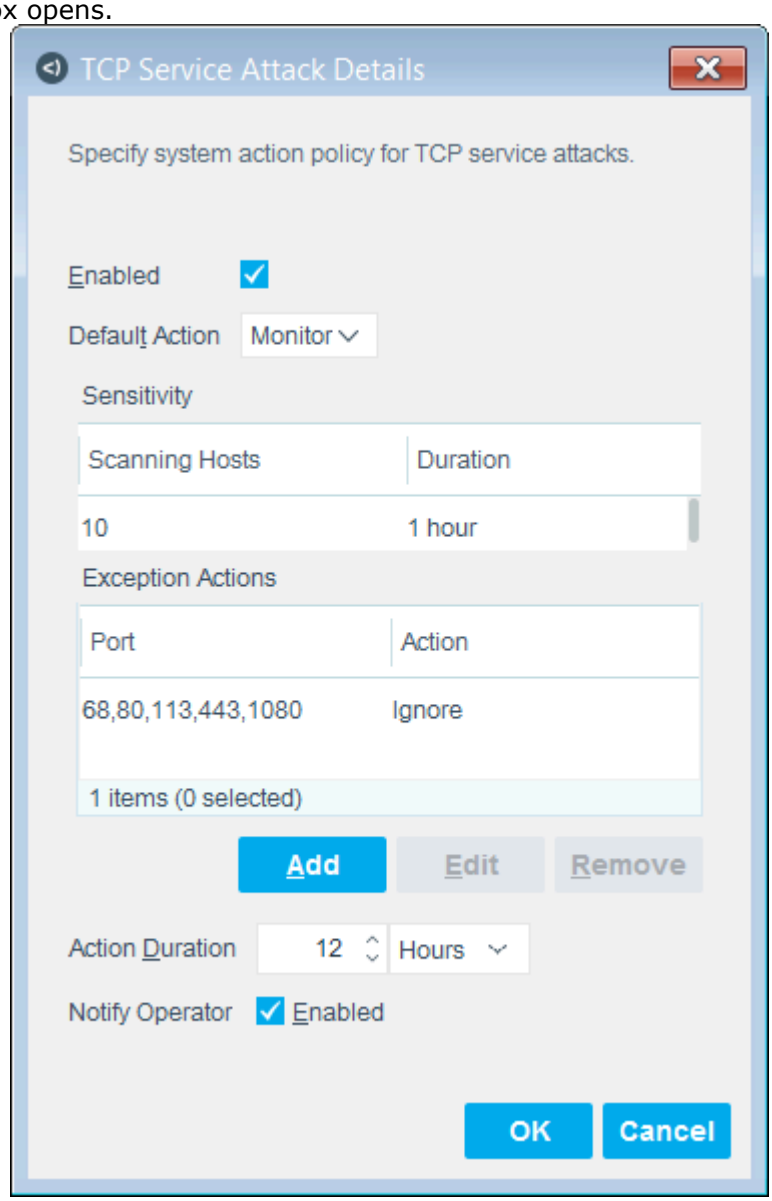
Customize service attack criteria

Service attack values set in the Service Attack tab can be customized. Two options are available for customization:

- Adjust sensitivity threshold for identifying an attack.
- Customizing the service attack response at specific ports.

To customize service attack parameters:

1. Select Tools > Options, and then select Threat Protection.
2. At the bottom of the Threat Protection pane, select Customize and then select the Service Attack tab.
3. Select the TCP or UDP row and select Details. The relevant Service Attack Details dialog box opens.



4. Select Enabled to enable system response to the event. Clear the checkbox for the system to ignore the event. If the checkbox is cleared, service attacks are not monitored or blocked (recommended).
5. From the Default Action drop-down menu, select Monitor to record all traffic going to the selected service, or select Block to prevent all traffic from communication with the service for the selected protocol.
6. In the Sensitivity section, adjust the sensitivity threshold for identifying a service attack. Forescout eyeControl identifies services attacks when the default service probing criterion is met. However, the sensitivity level of the criterion can be adjusted to identify the attack after either fewer or more probing endpoints are detected at a service within a set specified time period.
    - Double-click in the Scanning Hosts field to specify the number of endpoints to be detected at a service.

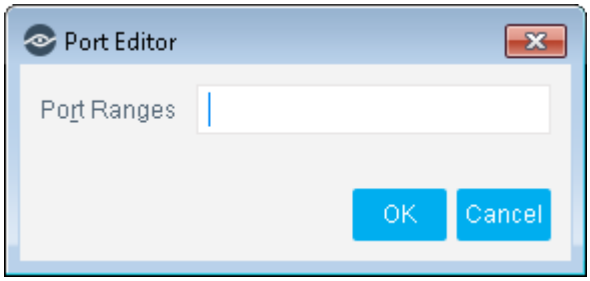
- Double-click in the Duration field to assign a unit of time.

7. In the Exception Actions section, select a port and an action. Double-click the relevant Action field and select Monitor, Block or Ignore from the drop-down menu.
8. Update the Action Duration setting to adjust the time interval in which the system blocks or monitors the UDP or TCP services. The value is applied to all ports listed for the UDP or TCP service. Use the drop-down menu to assign a unit of time.
9. Enable Notify Operator to send email notification to designated operators when the event occurs.
10. Select OK to save changes and close the dialog box. The Exception Actions section lets you customize the system response to service attacks at specific ports.

    For example, if you choose to block all UDP services, you can customize the block by indicating specific UDP services in which communication will only be monitored. You can enter a list of ports, a range of ports or a combination of both. An option is also available to ignore activity at ports, in which case the service is neither blocked nor monitored.

    To define service exceptions:

11. In the Exception Actions section of the relevant Service Attack Details dialog box, select Add.



12. Enter the required port numbers. Use a hyphen to indicate port ranges. Ports and ranges must be comma-separated.
13. Select OK. The Service Details dialog box includes the additional port numbers.
14. Click the action field for the related port. and select an action response from the drop-down menu. The following options are available:

Option	Description
Block	Prevents all endpoints from establishing communication with the port.
Monitor	Records all endpoint activity with the selected port.
Ignore	Does not block or monitor traffic.

15. Select OK.

Remove the monitor or block state from a service

You can remove the monitor or block state assigned to the services in your network; the system stops monitoring or blocking the service and the service is removed from the table.

Forescout eyeControl will respond to the service by monitoring or blocking the next time the

service attack criterion is met.

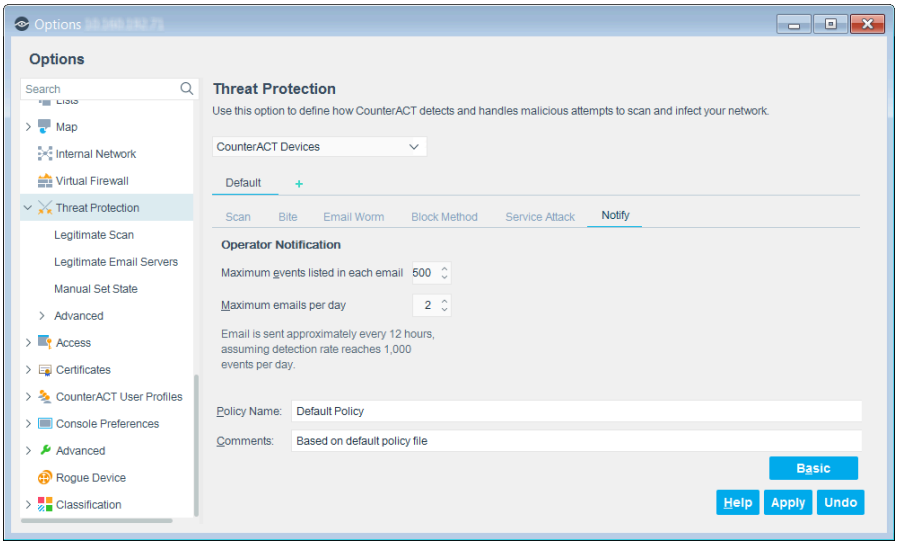
To remove the monitor or block state from a service:

1. Select a service in the Detections pane.
2. Right-click and select Remove and then Apply.

Manage threat protection mail alert deliveries

Forescout eyeControl delivers an infection alert to the operator by email notification to specified email addresses regarding bite detections in the network.

To access email notification settings, select Tools > Options, and then select Threat Protection. At the bottom of the Threat Protection pane, select Customize, and then select the Notify tab.



Forescout eyeControl sends email notification to specified email addresses regarding bite detections. If there is extensive activity at your network, email recipients may receive an overwhelming number of emails.

The following tools are available to help you manage email delivered to email recipients:

- Define the maximum number of email alerts delivered per day (from midnight)
- Define the maximum number of events that are listed in each email

For example, you can define that you only want to receive 50 emails per day, and that each email should contain no more than 50 events.

By default, up to 100 mails are sent within 24 hours. For example, if there is extensive activity early in the day and 100 mails are sent by 11 AM, you will not receive mails about events that occur during the rest of the day.

After the maximum number of emails is sent, a warning email is delivered; indicating that the email delivery threshold has passed, and you will no longer receive email alerts again until midnight. At midnight, an email is sent summarizing events that were not delivered. The summary includes the type of events detected and the number of events for each type, for example, 25 Port Bites and 65 Login Bites.

By default, mail is delivered approximately every 15 minutes provided that at least one event has occurred; it is delivered more frequently if more than 100 events occur in less than 15 minutes.

Note:
You can view information about these events from the Console.

You can change the default parameters and receive email alerts at a frequency that is more manageable for you.

To update operator notification parameters:

1. At the bottom of the Threat Protection pane, select Customize and then select the Notify tab.
2. Specify the Maximum events listed in each email value.
3. Specify the Maximum emails per day. The system calculates how often you receive mail according to this value, provided an event occurs. To receive an email alert each time an event occurs, enter the value 1 in the Maximum emails per day field.

   Note:
   Emails are also sent when the system detects a service attack. You cannot customize this delivery parameter, but you can disable the email delivery feature for service attacks.

   The following email options are also available:

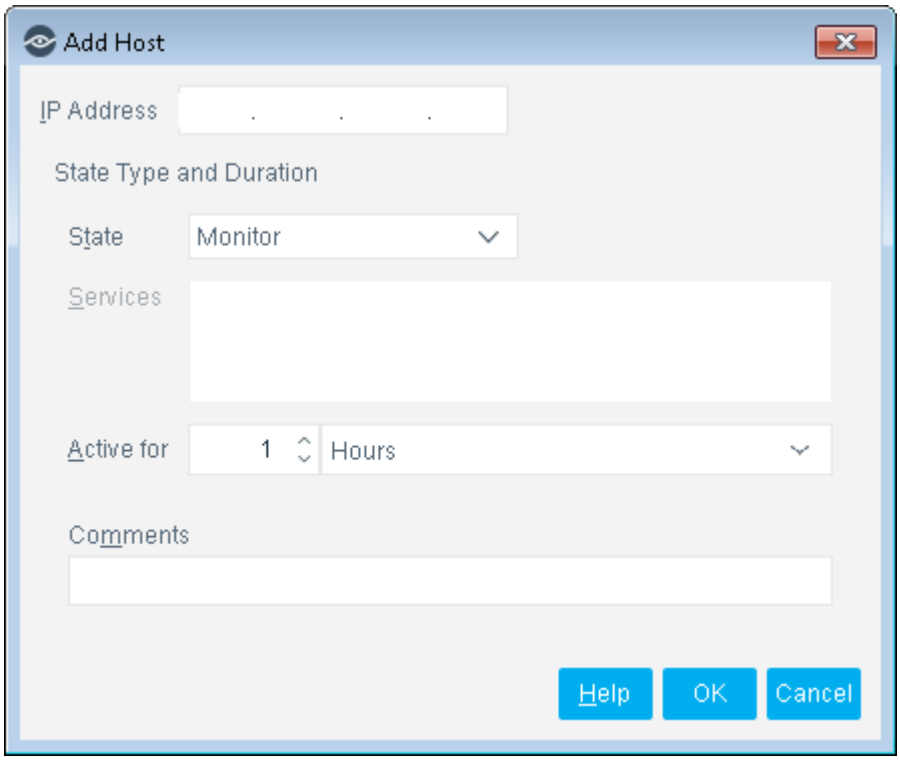
Update addresses that will receive email alerts	By default, your system sends email alerts to specified addresses when bite events occur. These addresses are defined during installation and can be changed.
Receive mail only for certain event types	You can define that you want to receive alerts only when specific types of endpoint activity occur, for example, only when Login bites occur.
Perform parsing on event information displayed in email alerts	Email alerts regarding endpoint and service events include a summary of events. This information is displayed in a format that can be easily parsed by external applications. See Parsing Event Information Displayed in Email Alerts for details.

Manually add an endpoint

Use this feature if you already know the IP address of an endpoint, and know that you want to either ignore, monitor, or block its activities for a specified period of time. After that period expires, the endpoint is handled according to the current system policy.

To add an endpoint:

1. Select Tools > Options, and then select Threat Protection > Manual Set State.
2. Select Add.



3. Enter the endpoint IP Address.
4. From the State drop-down menu, select the required state.

Monitor	Monitors endpoint activity for the length of time that you specify.
Host Block	Blocks the endpoint from the network for the length of time that you specify.
Port Block	Blocks the endpoint in the services that you define in the Services field. Multiple services must be comma-separated.
Ignore	The system ignores all endpoint activity for the length of time that you specify. After this time, the system responds to the endpoint activity according to the policy definitions. When you select this option, the Firewall block options and HTTP redirection actions are also ignored for the time specified on these endpoints.

5. In the Active for area, specify how long you would like the selected endpoint to remain in the chosen state.
6. You can use the Comments field as required.
7. Select OK to accept the entry.

Managing Manually Added Endpoints

You can view a list of the manually added endpoints that the system is currently handling, remove those endpoints from the list, or modify their state and how long the system maintains that state.

These tasks are performed from the Current Added Hosts dialog box. The list is updated each time you open the dialog box.

To view manually added endpoints:

1. Select Tools > Options, and then select Threat Protection > Manual Set State.
2. Define the following:

Host	The endpoint's IP address.
State	The endpoint's state: Host Blocked, Port Blocked, Monitored or Ignored.
Blocked Ports	The ports at which the endpoint is blocked.
From/Until	The length of time that the endpoint is in the state.
Issued By	The name of the user that manually added the endpoint.
Comments	Related comments.
CounterACT Appliance	The Appliance that received the command.

3. Select OK.

Changing the Host State Maintenance Time

You can change the expiration of the endpoint state, without changing the state.

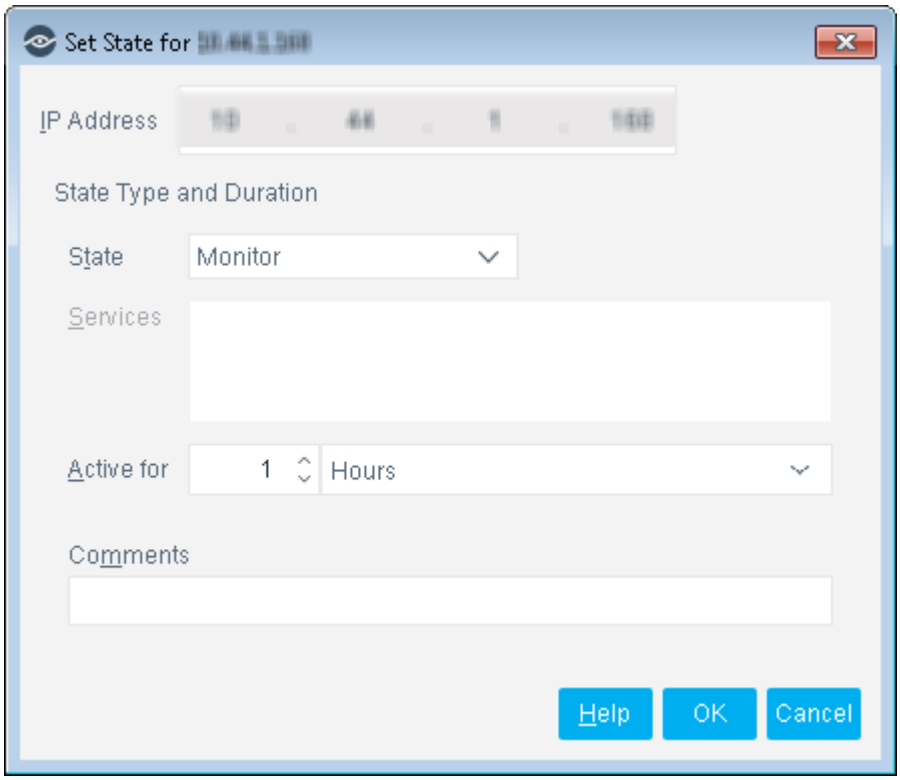
To change the expiration time:

1. Select the Threat Protection folder from the Console.
2. Right-click an endpoint in the Detections pane, select Threat Protection, and then Set State Time.
3. Specify how long you want the host to be monitored. Use the drop-down menu to assign a unit of time.
4. Select OK.

Changing the Host State

You can change the endpoint state. The endpoint expiration time remains the same.

1. Right-click an endpoint in the Detections pane, and then select Set Threat Protection State.



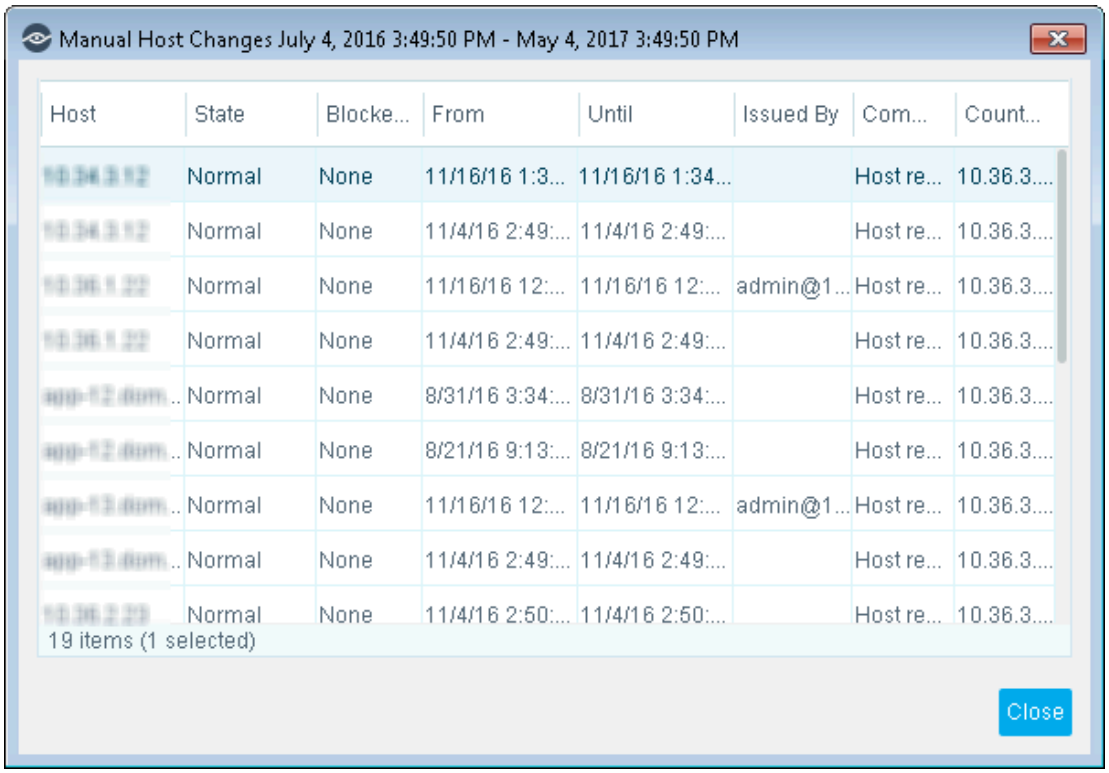
2. Update the endpoint parameters in the Set State dialog box.
3. Select OK.

Viewing a History of Manually Added Endpoints and Manual Changes

You can view a list of manually added endpoints and endpoints whose states or times were manually changed.

To view the history list for manual changes:

1. Select Tools > Options, and then select Threat Protection > Manual Set State.
2. Select History.
3. In the Time Period dialog box, set the required time range.
4. Select OK. The Manual Host Changes dialog box opens, showing endpoints that were entered manually during the time that you specified.



Define the active response range

By default, the entire Internal Network is protected by Forescout Active Response technology. This procedure describes how to change the Active Response range. For example, if you need to limit Active Response protection to core operational segments of your network.

Note:
Segments you place in the Active Response range must be included in the Internal Network.

Note:
Only endpoints with an IPv4 address are protected by Active Response technology. In dual-stack networks, only the IPv4 ranges of a segment are included in the Active Response range. IPv6 subnets are ignored.

To edit Active Response range definitions:

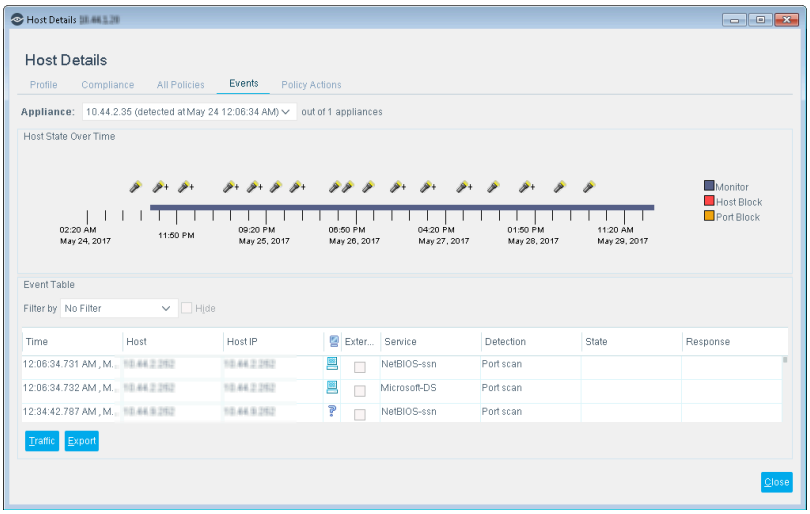
1. If necessary, define segments in the Console that support your Active Response range configuration. See Working with Forescout Segments.
2. Select Tools > Options, and then select Threat Protection > Advanced > Active Response Range.
3. The table lists segments that are in the default Active Response range.
4. (Optional) Create a configuration for a group of Appliances or select a configuration to modify. See Configure Features for an Appliance or Group of Appliances.
5. Do one of the following:
   - Select Segments. Then, in the Segment selection dialog box, select or clear checkboxes to include or remove segments, and select OK. The selected segments define the Active Response range.
   - Select segments in the table and select Remove. The selected segments are deleted from the Active Response range.

Changes made to the Active Response range must be supported by your network architecture. Specifically, addresses included the Active Response range defined for an Appliance must be visible to the Appliance.

View endpoint activity details

You can view comprehensive details regarding activities carried out by endpoints in the Threats view by double-clicking a malicious endpoint from the Detections pane to open the Host Details dialog box.

The endpoint's address is displayed in the title bar. The Events tab displays the date and time of the first event.

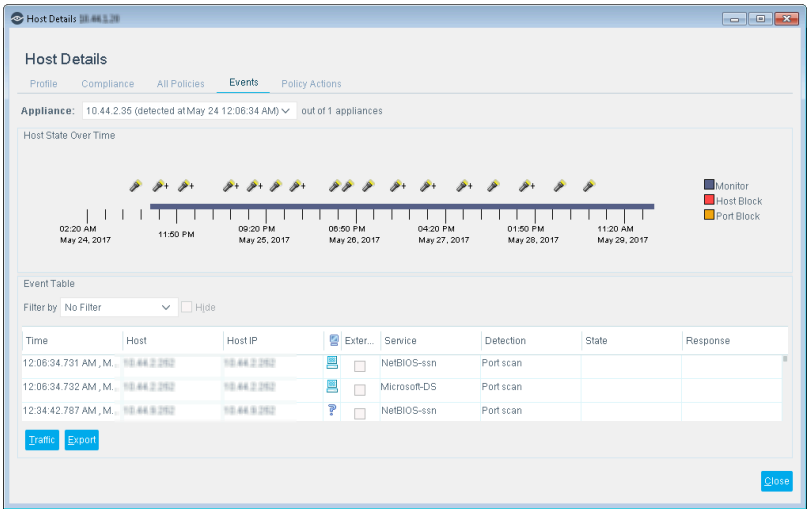


The Host Details dialog box displays general information and detailed information about the event. For example, you can review specifics about packets transferred during the session.

In addition, you can view information about the endpoint in the Assets Portal by selecting Show full host details. See Assets Portal for details.

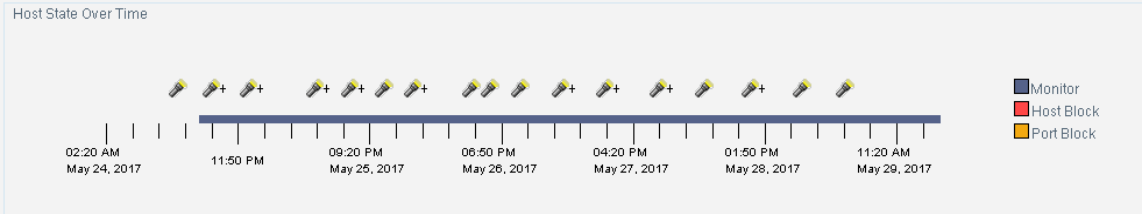
Events tab

The Events tab displays a graphic time-line summary of the source state for the period that the source is active. In addition, the tab includes an Event table, which provides extensive, real-time information about the source events and responses to those events.



Host state time-line summary

This section displays a graphic time-line summary of the source state for the period that the source is active. The Bite/Scan/Email icon will appear over the time-line summary each time the source state changes. The Flashlight icon indicates that the source performed scan event. The red and white Bite icon indicates that the source performed a bite event. If an Email icon is displayed, an email anomaly was detected. A plus sign (+) indicates that the source performed more than one event. Use your cursor to view tooltip information about the scan or bite events detected.

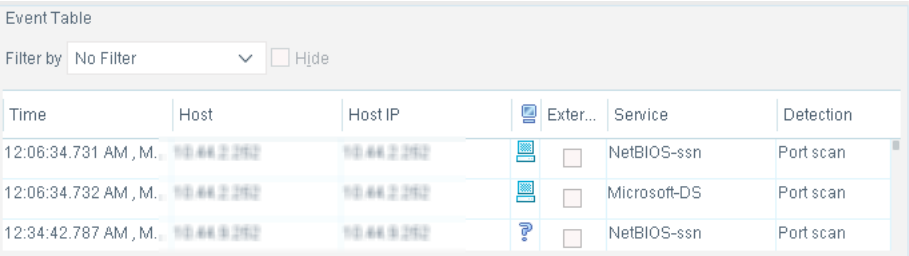


Event table

The Event Table provides extensive, real-time information about source events and eyeSight activity that occurs while the source is active. An event is defined as any attempt to access an endpoint on the network.

For example, the table displays information about the targeted endpoint for each event, including the endpoint IP address and the targeted service. Information about the response to events is also available. For example, if Forescout eyeControl responded by sending a service mark to the source, the returned data will indicate the service sent. The information provided here should be used for in-depth analysis of source and eyeSight activity.

Default columns appear with basic information about sources and related source activity. Additional information can be displayed by adding other columns.



The following table details source activity for the selected event.

Time	The time and date the event occurred.
	Indicates that the source address is verified. Indicates that the source address is unverified and possibly spoofed.
Event Fragmentation	 Indicates whether the packets sent during the event were normally fragmented or abnormally fragmented. Abnormally fragmented packets may indicate that the event was carried out by a human attacker and not by a worm.
Host, Host IP	Displays the IP address at which the event took place.
Accessed Host Type	 Indicates that the targeted host was a virtual address. Indicates that the targeted host is unknown. Indicates that the targeted host was a real address.
External	Indicates whether the targeted host resides outside the network.
Service	Displays the name of the services accessed on the targeted host.

The following table details activity for the selected event.

Detection	Indicates the event detected, e.g., NetBIOS scan or infection attempt.
Response	Indicates the response to the detection. Options include: Block: Forescout eyeControl does not allow packets from the source to go through to the specified destination (host + service). Stall: Forescout eyeControl simulates a virtual service for an infected source. This occurs when the policy is not set to block infected sources. Mark: Forescout eyeControl distributes a mark to the source.
Resulting State	Displays the new source state after detection and response.
Returned Data	Displays the data sent to the source from eyeControl. For example, if eyeControl responded by sending a user name mark to the source, the returned data will indicate the user name sent.
Expiration	Indicates the date and time the source state will expire.

Filtering the information displayed in the event table

The Event Table can be filtered so it only includes information of particular interest to you. For example, you can select filter settings, so the table displays only events in which a real site was accessed.

You can choose to either display events that meet the filter criteria or hide the events that meet the criteria. Filter settings are automatically saved and applied to your table each time you open the Console.

The following filter options are available:

Detections	Events that caused Forescout eyeControl to either change the current source state or extend the source state.
Detections and Marks	Events that caused Forescout eyeControl to either distribute marks or change the current source state or extend the source state.
Infection Attempts	Events in which an infection attempt was made.

Real Site Accesses	Events in which the source attempted to probe, scan or infect a real site, or in which a valid event was carried out at a real site.
Same Host	Events targeted at the same host as the endpoint selected in the table.
Same Service	Events targeted in the same service as the service selected in the table.

To filter the table:

- Select a filter type in the Filter by drop-down.
- Select or clear the Hide option.

Add legitimate traffic rules from the event table

You can add a Legitimate Traffic rule for a source or event listed in the Event table.

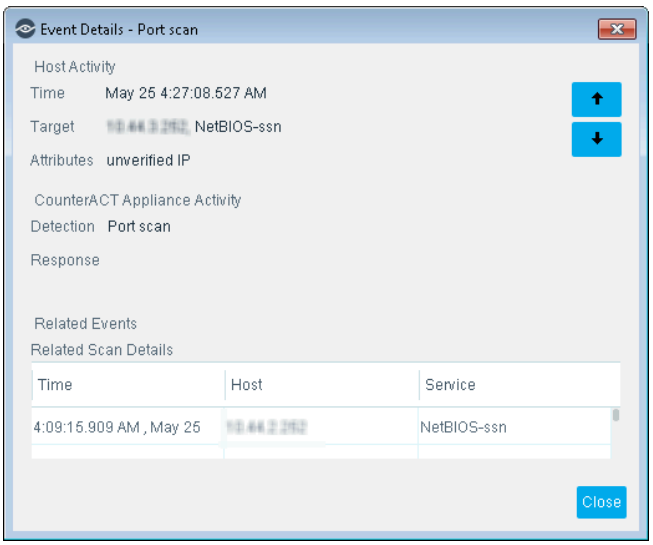
To create a rule:

1. Right-click an event in the Event table and select Legitimize Traffic. The Add Custom Rule dialog box opens. The selected source is displayed in the Source section. The targeted host and service selected in the Events table are also included in the Legitimate Traffic rule.
2. Edit the rule if required.
3. Select OK.

View a summary of event details

An Event Details dialog box summarizes event details for a selected event and displays related events. For example, if you select a scan event, the probes included in the scan are listed.

Double-click an entry in the Event Table or right-click an entry and select Details.



The following information is available:

Host Activity	Summarizes information regarding source activity for the selected event.
CounterACT Appliance Activity	Summarizes information regarding activity for the selected event.
Related Events	Lists events related to the selected event. Related Scan Details displays all probe events related to the scan event. Related Probe Details displays additional probe events related to the scan event. Related Mark Details displays marks that triggered the bite event. You can review a history of related mark events. Related Bite Details displays the bites that responded to the distributed mark.

Click a scroll arrow to display information about other sources in the Event table.

View event traffic

Use this procedure to display information about the packets transferred between a host and the network.

To view event traffic for a selected source:

1. Select an event from the Event table.
2. Select Traffic. The Traffic dialog box opens.

Address type	: From a virtual address : From a real address
Host	The targeted host that communicated with the infected source.
Service	Name of service or port number, for example, FTP or email.
Count	The total number of packets per session.

Bandwidth	The total of all packet sizes divided by the duration of the session in seconds.
First/Last Packet Arrival	The date and time of the first or last packet of the session.

Packet List Section

	Indicates whether the packet destination or source is: : A virtual address : A real address
	Indicates the direction of the activity: : From Threat Protection site to source : From source to Threat Protection site
Size	Size of the packet in bytes.
Date	The date and time the packet was sent.

Select an entry from the Packet List to display the raw packet data.

To save packet data:

3. Select the session from the Traffic tab. To save all sessions, do not select any sessions.
4. Select Save. The Save Options dialog box opens.
5. Select Save all session or Save selected session, and then select OK. A Save As dialog box opens enabling you to save the information in a selected directory.

   Note:
   If the selected source is still active, a message indicates that the source is still active and that you are not saving all the source sessions.

Manage enterprise lockdown alerts

Enterprise lockdown alerts enable malicious endpoint activity detected in one Appliance to be immediately communicated and simultaneously handled by all the Appliances in the enterprise. As a result, if one Appliance in your enterprise has detected a bite event, a lockdown alert is sent to the other Appliances, alerting them of the source that performed the event. If the other Appliances

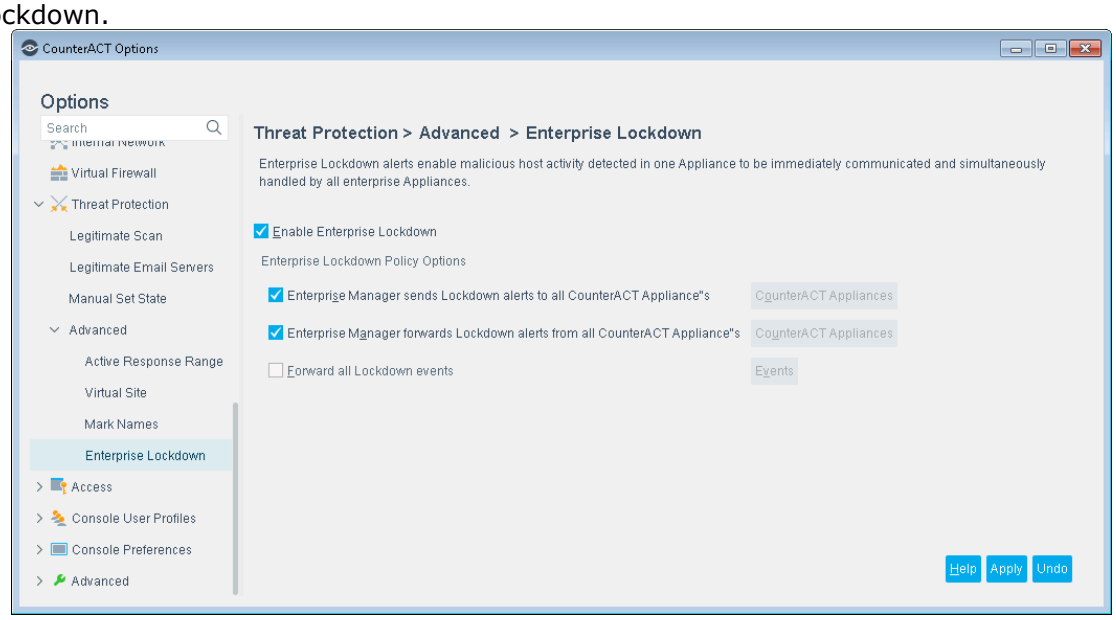
detect that a source is communicating with the network that they are protecting, the source is automatically blocked or monitored according to the policy.

For example, if Appliance 1 detects a port bite from source XYZ, an alert is sent to the other Appliances, notifying them of the source. If Appliance 2 detects source XYZ communicating with the network it is protecting, the source is either blocked or monitored according to the port bite block or monitor policy defined in the Appliance. The source is blocked or monitored for the time indicated in the policy of Appliance 2 and then released.

You can include or exclude specific Appliances that send or receive alerts and customize the kind of bite events that are included in the lockdown alert.

To manage lockdown alerts:

1. Select Tools > Options, and then select Threat Protection > Advanced > Enterprise Lockdown.



2. Select Enable Enterprise Lockdown to activate the lockdown policy.
3. Define a lockdown policy.

Enterprise Manager sends Lockdown alerts to all Appliances	When selected, the Enterprise Manager sends lockdown alerts to all Appliances in the enterprise. Clear the checkbox to define specific Appliances that will receive lockdown alerts.
Enterprise Manager forwards Lockdown alerts from all Appliances	When selected, the Enterprise Manager accepts all lockdown alerts from all Appliances. Clear the checkbox to define specific Appliances that will send lockdown alerts to the Enterprise Manager.
Forward all	When selected, all bite event types are included in lockdown.

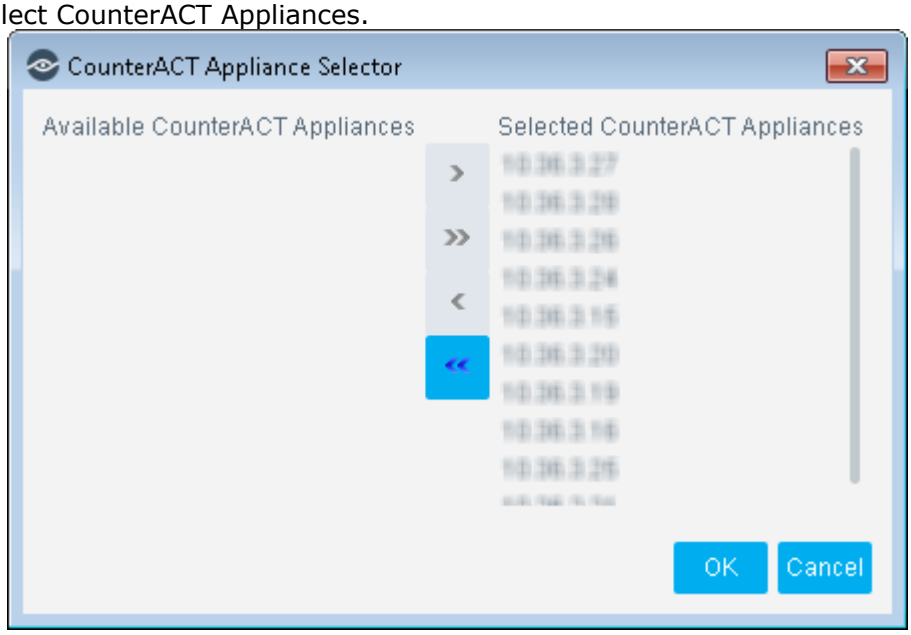
Lockdown events	Clear the checkbox to select specific types of bite events that are included in the lockdown alert.

4. Select Apply.

Send events to specific appliances

To send events to specific appliances:

1. Clear one of the first two Enterprise Policy Lockdown options.
2. Select CounterACT Appliances.

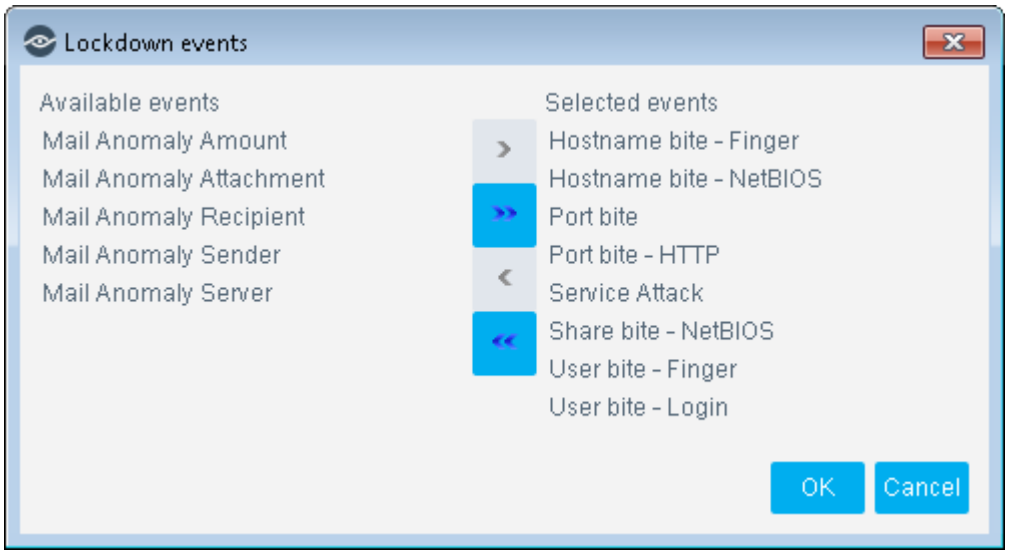


3. Select and move Appliances to and from the Available CounterACT Appliances list to the Selected CounterACT Appliances list as required.
4. Select OK.

Customize the forward all lockdown events policy

To customize the Forward All Lockdown Events policy:

1. Clear Forward all Lockdown events.
2. Select Events.



3. Select and move events from Available events list to, and from the Selected events list as required.
4. Select OK.

Legitimate traffic

Forescout provides a set of options for handling legitimate traffic in your network.

About handling legitimate activity from malicious sources

You can define rules for allowing specific kinds of probes at your network. This type of activity is referred to as legitimate traffic activity. Once these rules are defined, endpoints that perform Legitimate Traffic are ignored. Specifically, they are not counted in the probe count by Forescout eyeControl when attempting to probe defined services or host.

By default, the Legitimate Traffic rule is set to ignore NetBIOS and port probes by any source to any real host on any service. This allows eyeControl to ignore legitimate network activity and handle activity on virtual endpoints that it creates.

You should keep the default settings, and then use the Legitimate Traffic tools to add other Legitimate Traffic rules, as required. For example, if you are performing vulnerability assessments from specific addresses on specific ports, or for a printer that is required to scan the network to find a server to connect to, or any other business requirement that compels you to grant full access to specific addresses.

Centralized Management

Legitimate Traffic rules can be centrally managed via the Enterprise Manager for all connected Appliances. This means the rules defined in the Enterprise Manager are applied to all Appliances. Centralized management ensures consistency in Legitimate Traffic probe definitions across your enterprise. This eliminates the process of redefining the rules at each Appliance, making it easier to conclude deployment.

When registering an Appliance to the Enterprise Manager, all legitimate traffic rules configured on that Appliance are replaced by the rules on the Enterprise Manager.

Legitimizing Traffic Options

The following options are available for setting Legitimate Traffic rules:

- Define legitimate known scanning applications, for example, Exchange IM or Lotus.
- Define servers that have been removed but are still probed by network users.
- Define specific services and endpoints at which scanning is allowed.
- Define email servers and sources that should be allowed to send email traffic.
- Use the Legitimate Scan Tuning wizard to automatically locate and allow legitimate scanning activity generated by known scanning applications or directed at unused servers.
- Create rules for detected endpoints.
- Import or export Legitimate Traffic.

Activity at Other Services

If a legitimate source probes the legitimate endpoints and ports assigned to it, and does not probe any other ports or endpoints, that source is not marked as a probing source, and thus is not a candidate for monitoring and blocking. If the same source also probes at least three endpoints or ports not marked as legitimate within the defined time period, a mark is distributed to the source. If the source uses the mark, it is considered an infected source and as such is a candidate for monitoring and blocking.

Note:
The default settings require that the source perform three probe events within a day in order for the system to mark the source as a probing source. See Customize Scan Recognition Criteria for details about changing the probe count criteria.

After a source is detected as offensive, its attempts to access the legitimate endpoints and ports assigned to it are blocked and monitored.

Manually Ignoring a Source or Defining a Legitimate Scan

In addition to using the legitimate scan feature, an option is available to ignore selected sources for a specified time period. When a source is ignored, all communication from it is allowed at any port.

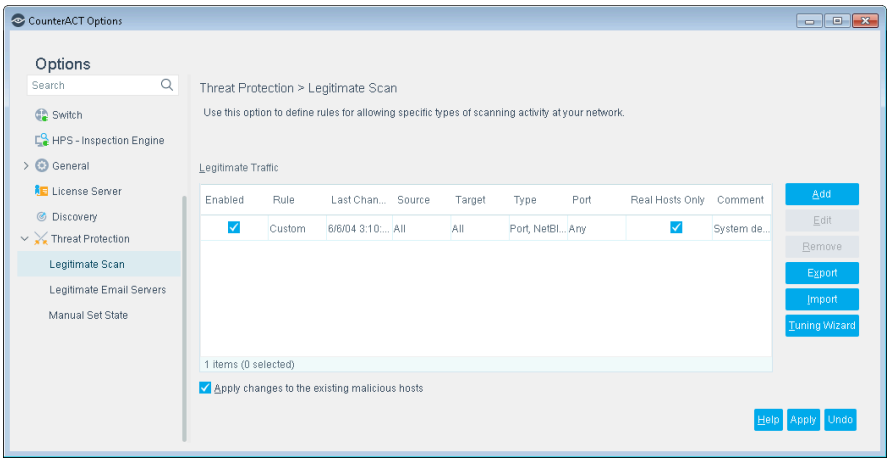
The difference between manually ignoring a source and using the Legitimate Traffic rule is:

- The manual ignore feature is limited to a certain time, while the Legitimate Traffic rule is enabled until you disable it.
- The manual ignore feature does not let you customize specific endpoints or ports on which to ignore the source.
- The manual ignore feature lets you ignore the source under all circumstances. If you use the Legitimate Traffic feature, and the source scans or attempts to infect endpoints or ports not specified as Legitimate Traffic, the source is blocked according to policy at all ports and endpoints, including the legitimate ones.

View legitimate traffic

Legitimate Traffic is defined and managed from the Legitimate Traffic dialog box. From the dialog box, you can add, edit, and remove rules, as well as to filter information about the rules that you have already defined. A feature is also available to import and export Legitimate Traffic rules.

To view the legitimate traffic list, select Tools > Options, and then select Threat Protection > Legitimate Scan.



The following information is available:

Enabled	Indicates that the rule is enabled.
Rule	Several types of rules can be created. For example, custom design rules, known scanning application rules or removed server rules. This column details the rule type created.
Last Change	The date the rule was most recently modified.
Source	The source addresses to which the rule is applied.
Target	The destination addresses to which the rule is applied.
Type	The probe types included in the rule. For example, to allow HTTP probes only. The following options are available: Finger, HTTP, Login, NetBIOS, SNMP, and Port.
Port	The service to which the rule applies.
Real Hosts Only	Indicates that the rule was applied to real endpoints only.
Comment	Displays one of several methods used for defining Legitimate Traffic rules. The methods are detailed later in this section.

Define legitimate scanning activity – wizard

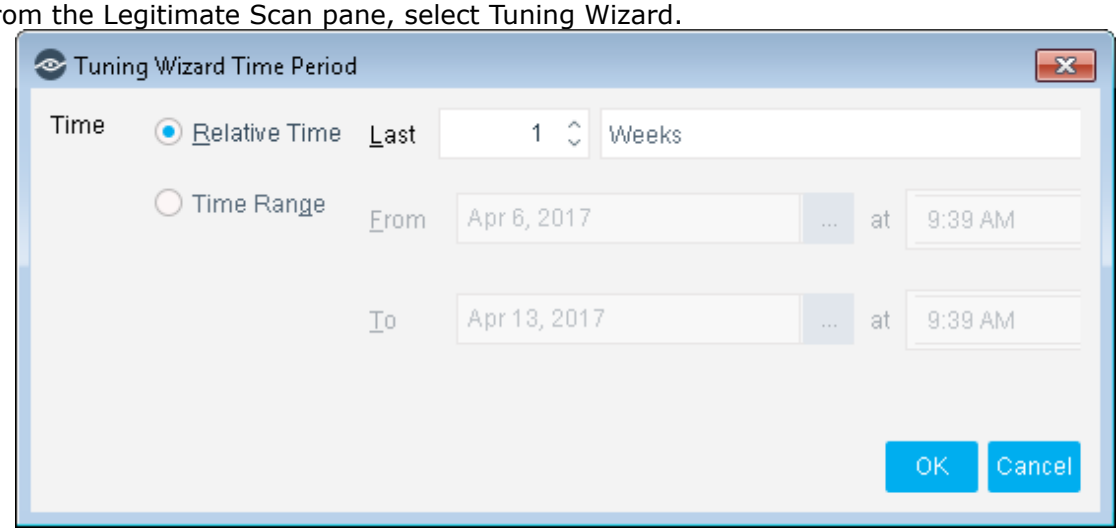
The Legitimate Scan Tuning wizard automatically detects applications installed at your network

that may be used for legitimate scanning activity and detects servers that have been and continue to be probed by network users. Use the wizard to define these applications or servers as sources of legitimate traffic.

Although the Legitimate Traffic wizard (see Create customized legitimate traffic rules) automatically identifies most of the rules required, fine-tuning may be required and can be done by adding custom rules.

To fine tune traffic with custom rules:

1. From the Legitimate Scan pane, select Tuning Wizard.



2. Specify a time period in one of the following ways:

Relative Time	Specify a number of hours, days, weeks, or months.
Time Range	Specify the start and end of a date/time range.

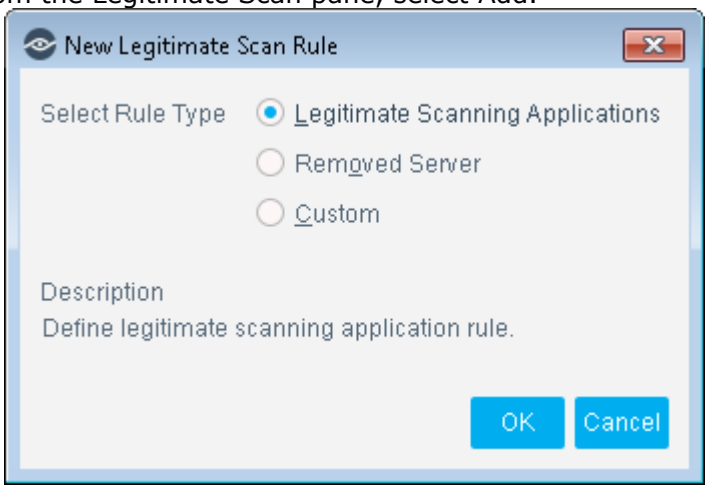
3. Select OK. If results are discovered, the Welcome dialog box opens.
4. Read the contents and select Next. The Legitimate Applications dialog box opens, containing the known scanning applications detected at your network.
5. Select the Allowed checkbox for each application you need to allow to scan your network.
6. Select Next. The Removed Servers dialog box opens, listing removed servers that continue to be probed by network sources, but cannot be reached. This may occur, for example, because the server is uninstalled or no longer in use. Forescout eyeControl may unnecessarily block sources detected at these locations. Activity should be allowed at such servers. The 10 servers most frequently probed by sources during the time period that you specified are displayed. After the wizard completes, you can run it again to see if other servers are found.
7. Select the Allowed checkbox for each server that should be open for scanning activity.
8. Select Next. The Finish dialog box opens. The applications or servers marked Allowed are added to the Legitimate Probes Manager.
9. Select Finish. The Legitimate Traffic List opens, listing the allowed applications and allowed removed servers that you defined in the wizard.
10. Select Apply.

Manually define legitimate scanning applications

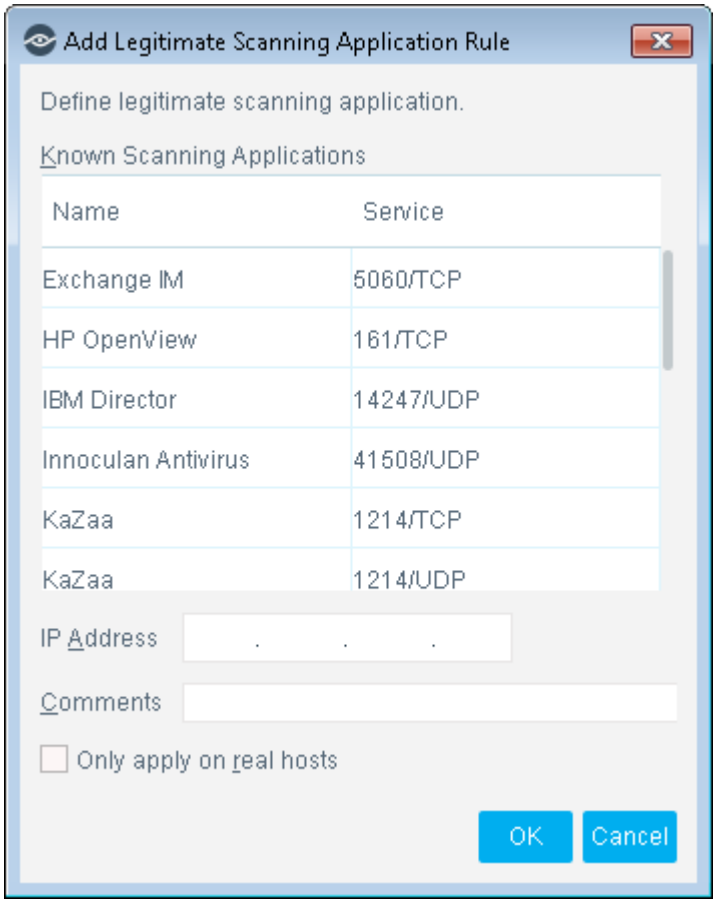
Use this strategy to define specific legitimate scanning applications from which Forescout eyeControl ignores scanning activity.

To manually define Legitimate Scan Rules:

1. Select Tools > Options, and then select Threat Protection > Legitimate Scan.
2. From the Legitimate Scan pane, select Add.



3. In the New Legitimate Scan Rule dialog box, select Legitimate Scanning Applications, and then select OK.



The Add Legitimate Scanning Application Rule dialog box displays the currently

downloaded list of known legitimate scanning applications.

4. Select an application from the list, and define the following settings.

IP Address	The address at which the application is installed.
Comments	A brief explanation of the purpose of this rule.
Only apply on real hosts	When this option is selected, a probe is considered legitimate only if the destination address was learned as a real host, not a virtual endpoint..

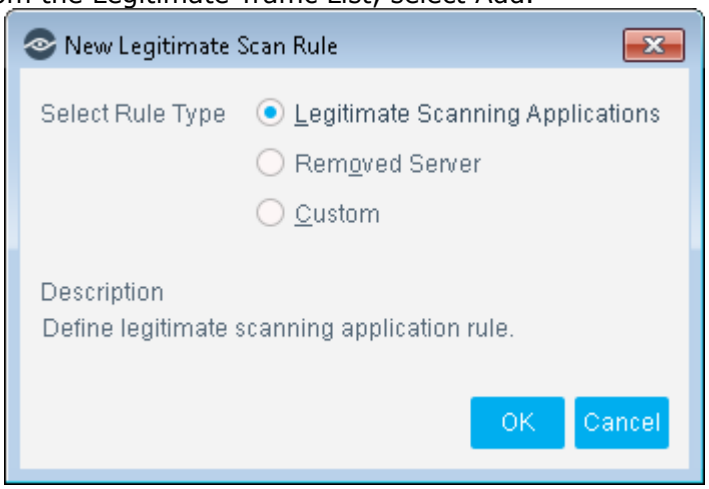
5. Select OK. If the application is installed at several locations, repeat the process for additional IP addresses.

Manually define removed servers

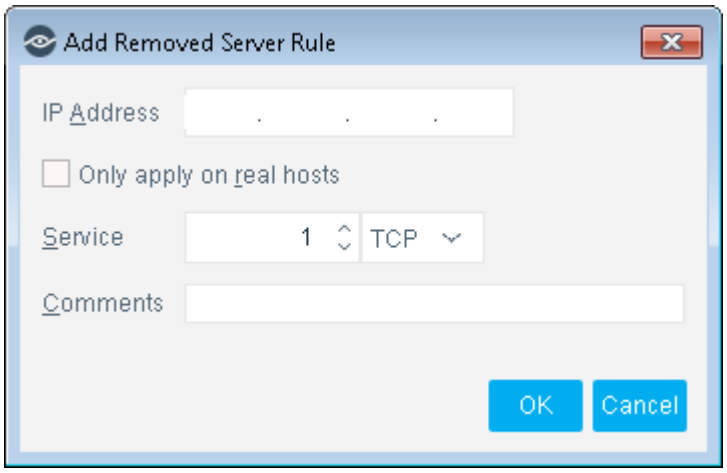
Removed servers are servers that network users have attempted to connect to but cannot be reached. This may occur, for example, because the server is uninstalled or because the server is no longer in use. Forescout eyeControl may unnecessarily block sources detected at these locations. Activity should be allowed at such servers.

To manually define removed servers:

1. From the Legitimate Traffic List, select Add.



2. In the New Legitimate Scan Rule dialog box, select Removed Server and then select OK.



3. In the Add Removed Server Rule dialog box, specify the following settings.

IP Address	The address at which the application is installed.
Only apply on real hosts	When this option is selected, the rule is applied only if the server was learned as a real host, not a virtual endpoint.
Service	Specify a port and service.
Comments	A brief explanation of the purpose of this rule.

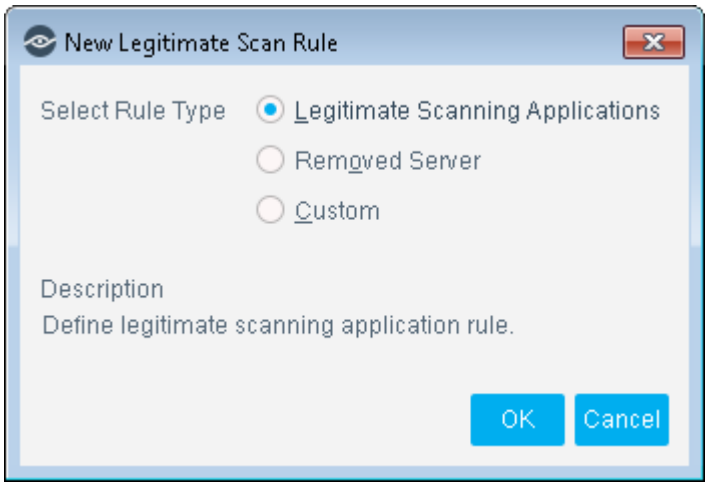
4. Select OK.

Create customized legitimate traffic rules

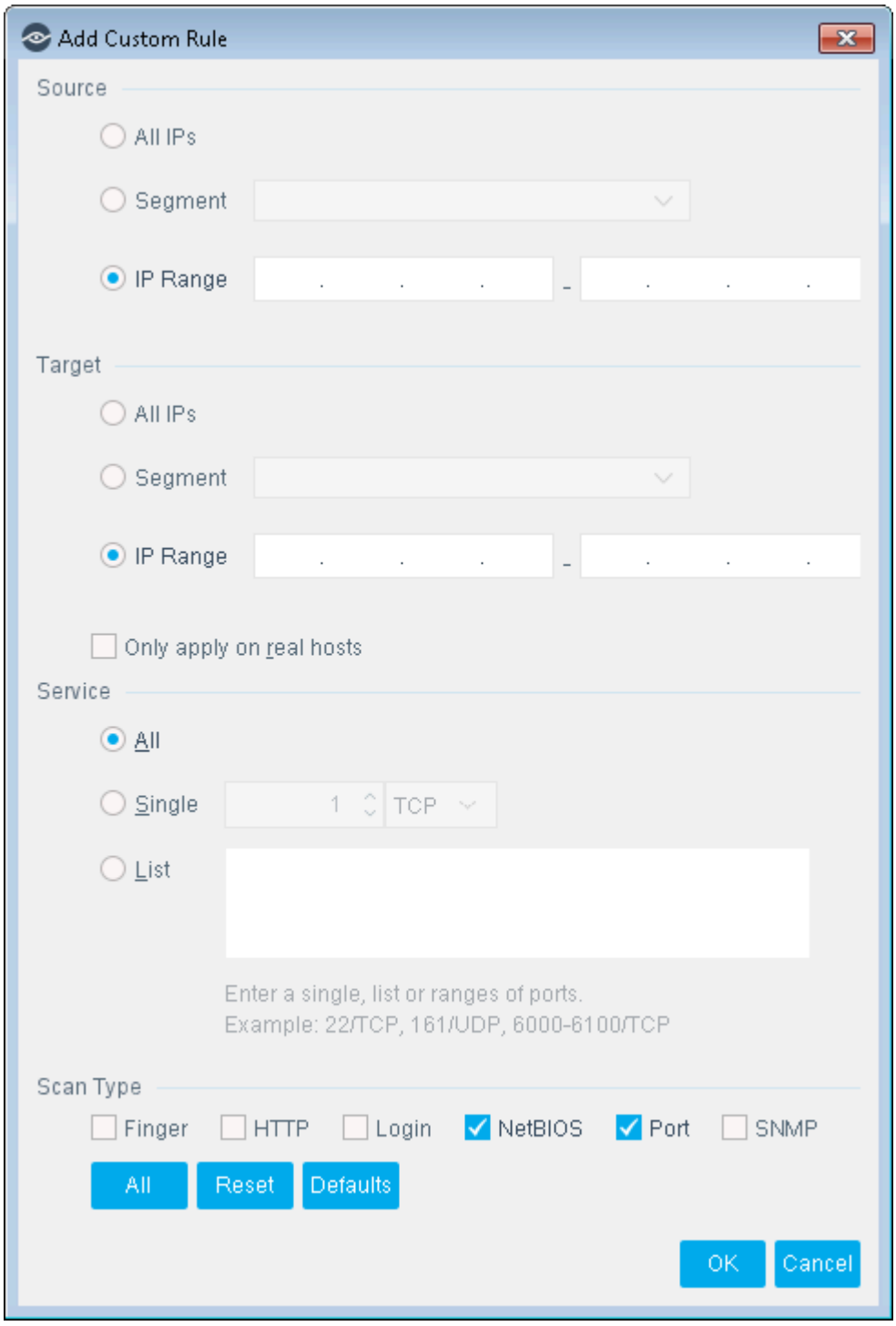
The Legitimate Traffic wizard automatically identifies most of the legitimate scanning applications and servers at in your network. Fine-tuning may be required, for example, if a network manager performs a network scan for legitimate reasons and can be done by adding customized rules.

To create customized Legitimate Traffic rules:

1. From the Legitimate Traffic List, select Add.



2. In the New Legitimate Scan Rule dialog box, select Custom and then select OK.



3. Define the following settings.

Action	The action applied by this virtual firewall rule. Valid values are Allow or Block.
Source IP	Specify the IP addresses in your internal network to which the rule is applied.

	All IPs – include all IP addresses in the internal network. Segment – select a named segment in the internal network. IP Range – specify a range of IP addresses in the internal network.
Target IP	IP addresses that are blocked or allowed. Endpoints with IP addresses defined by the Source IP field can/cannot access these IP addresses. All IPs – include all IP addresses in the internal network. Segment – select a named segment in the internal network. IP Range – specify a range of IP addresses in the internal network.
Only apply on real hosts	When this option is selected, the rule is applied only if the target IP was learned as a real host, not a virtual endpoint.
Service	The services for whom traffic between Source IPs and Target IPs is legitimate and ignored. All – block/allow all services on the endpoint. Single – specify a port and protocol to block/allow. List – specify a comma-separated list of services.
Scan Type	Select the probe types that are considered legitimate. Valid values: Finger, HTTP, Login, NetBIOS, Port and SNMP. For example, you can create a rule in which only HTTP probes at port 80/TCP are legitimate. If the services and the probe types do not match, you are warned, but you can still save the rule. For example, if a user selects HTTP and Login Probe types on 21/TCP and 23/TCP, the system will ignore HTTP and Login probes only on those services.

4. Select OK.

Define legitimate email traffic

Certain servers and endpoints in your network may generate suspicious email traffic that is detected as an email infection. In some cases, this traffic actually qualifies as legitimate activity. Examples include traffic generated by email servers and traffic generated when several users are logged on to one endpoint and are sending large amounts of email traffic. Forescout eyeControl should allow this type of activity.

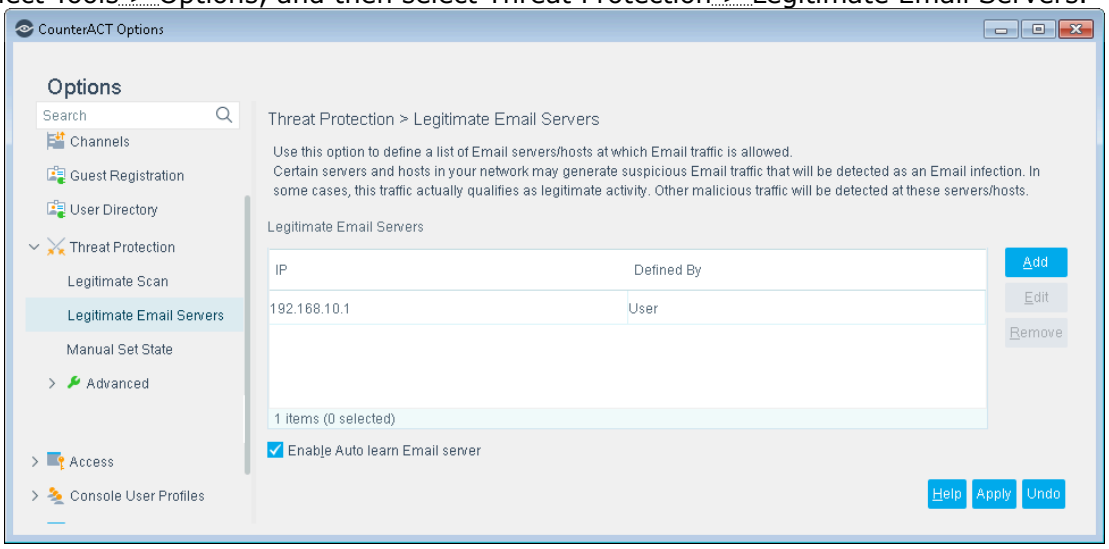
To do this, you can define a list of email servers and endpoints for which to allow email traffic. Other malicious traffic is detected at these servers and endpoints.

By default, eyeControl automatically learns and ignores real email servers on your network. In addition to automatically learning real servers, you can manually list endpoints that should be allowed to handle all email traffic.

If the email source is detected as performing other Threat Protection activity, it is handled according to the block or monitor policy.

To define endpoints:

1. Select Tools > Options, and then select Threat Protection > Legitimate Email Servers.



2. Select Add.
3. In the Add dialog box, enter the IP address of the relevant endpoint and select OK. The address is displayed in the IP column of the dialog box. The Defined By column indicates whether the server was automatically learned by Forescout eyeControl or entered by a user.
4. Remove or edit endpoints as required.
5. Verify that Enable Auto learn Email server is selected to enable eyeControl to automatically locate email servers and ignore email traffic generated by them. You can disable this option to detect email activity at these servers, for example, if you suspect that they may be infected with a worm (recommended).

   Note:

   If there is no traffic at the server for a month, eyeControl unlearns it.
6. Select Apply.

Create rules for detected endpoints

Legitimate Traffic rules can be created for sources and endpoints directly from the Source Details dialog box. Use this feature, for example, if you see that a source was blocked from a specific port and want to ensure access in the future.

To create rules from the Detections pane:

1. Double-click an endpoint from the Detections pane.
2. Select the Events tab, and then select the event that you think is legitimate.
3. Right-click and select Add Legitimate probe. The information required is displayed in the Add Rule dialog box.
    - Source address of the probing source
    - Target address of the probe target
    - Probe type and service on which the probe was detected

    When you save the rule, you are prompted to reset the source. If your Appliance is registered with an Appliance and you confirm this action, the rule is applied to all connected Appliances.

Threat protection advanced tools

Conventions

Forescout eyeControl responds to reconnaissance activity by generating marks – virtual resource information expected by probing endpoints – and forwards this information back to them. For example, if the system identifies a probing endpoint that is attempting to gather information about user names in your network, the system responds by creating and returning a mark in the form of a virtual user name to that attacker.

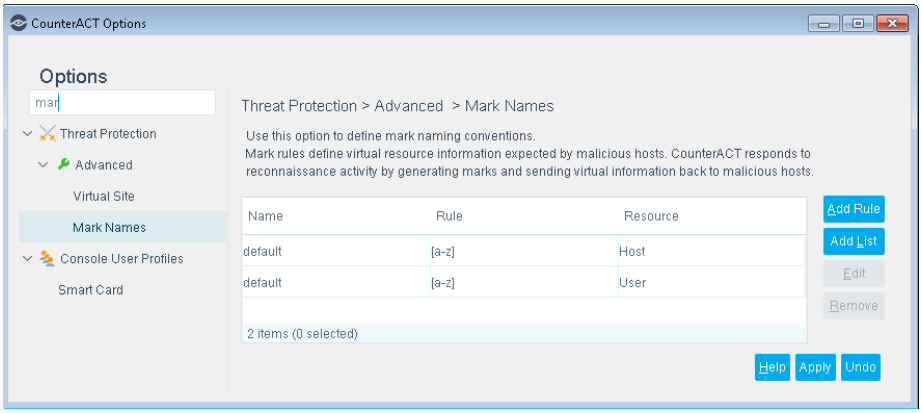
Two types of naming options are available:

- Create mark rules that reflect the naming conventions used for host and user names in your network.
- Create lists of names similar to the host and user names used in your network.

These tasks are performed from the Mark Names pane.

Access to the tools detailed in this section is limited by permissions. See Access to Console Tools – On-premises Permissions for details.

To open the Mark Names pane select Tools > Options, and then select Threat Protection > Advanced > Mark Names.



About mark rules

Endpoint and user names are often organized into logical segments, i.e., host names begin with a fixed text string and end with a specific number combination.

For example, computers in your network may be organized and named as follows:

- SC_WIN_123
- SC_WIN_223
- SC_LINX_123
- SC_LINX_223

Where:

- SC = the company name (Sample Company)
- WIN/LINX = the platform (Windows or Linux)
- 123/223 = a numeric sequence

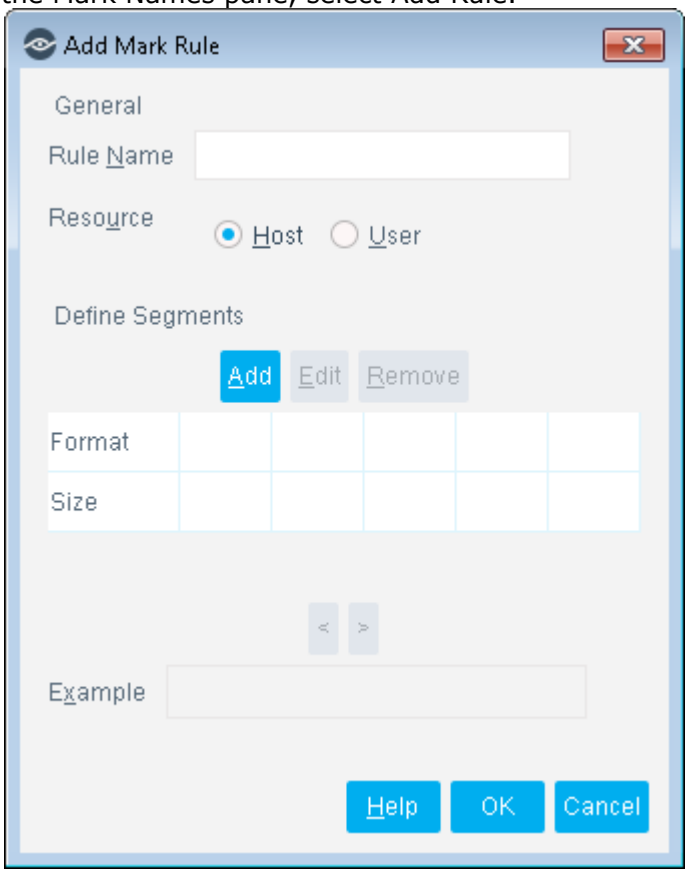
You can define the naming convention rules for the host and user resource names to use as marks for your system. The mark rules can contain several segments that reflect the naming conventions used in your networking/organizational environment.

Forescout eyeControl is set up with default mark rules, which appear in the Mark Names pane. If you add mark-naming conventions, marks are sent according to the default rules and rules that you create. It is recommended that you delete the default names if your company maintains a policy where all host or user names are created according to a specific convention. This ensures that marks appear consistently and realistically to probing endpoints.

Define Mark Rules

To define mark rules:

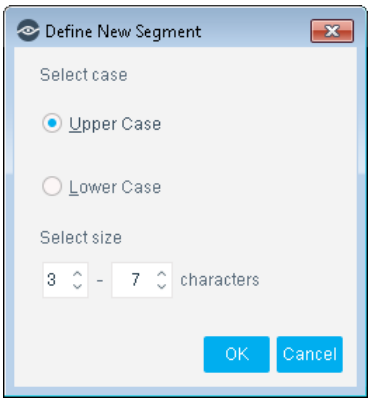
1. In the Mark Names pane, select Add Rule.



2. Enter a rule name in the Name field.
3. Select Host or User to be applied to this resource type.
4. Select Add to create the rule segments. The Select Segment Type dialog box opens, allowing you to select a rule segment type.
5. Select a segment type from the drop-down menu and select OK. The dialog box is refreshed. Three types of rule segments can be created:

Alphabetic Segment

Define the rules for random text string segments that appear in the resource name.

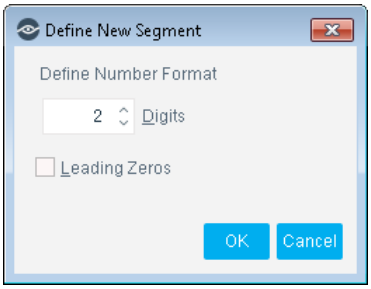


To define a random text string:

- In the Select case section, select Upper Case or Lower Case.
- In the Select size section, specify the minimum and maximum character length.
- Select OK.

Numeric Segment

Define the rules for the maximum number of digits that appear in the resource name.

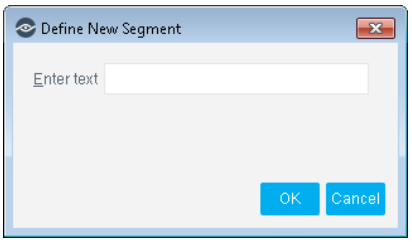


To define a number:

- In the Digits field, specify the maximum number of digits that appear in the segment. For example, if you select 3, the number can include up to three digits, such as 78, 5, 333, 999, 123.
- Select Leading Zeros to include leading zeros in the number. For example, 08, 003, 099, 023.
- Select OK.

Constant Segment

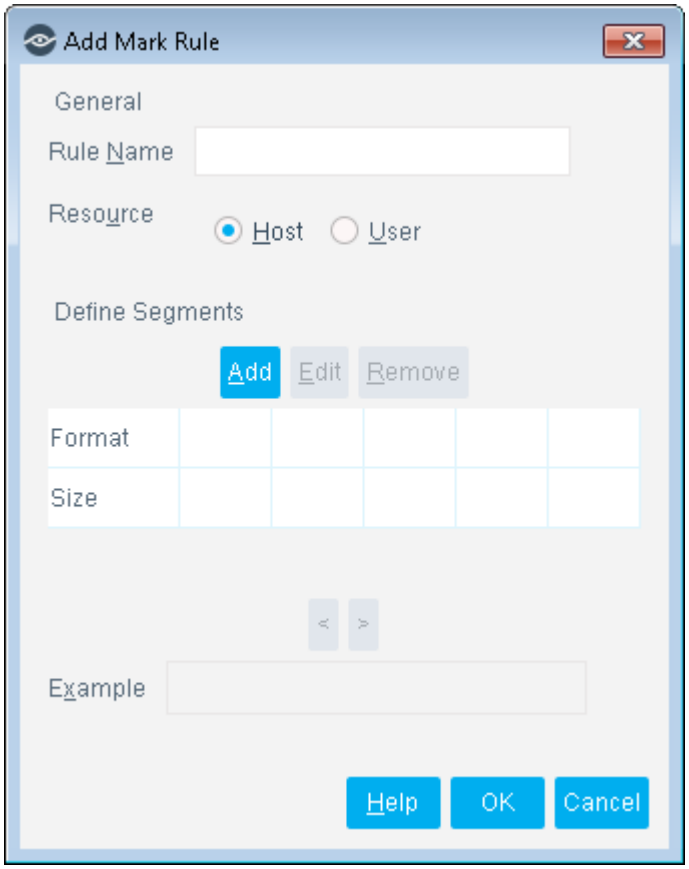
Define fixed string segments that will appear in the resource name.



To define a fixed text string:

- Type a string in the Enter Text field.
- Select OK.

You can create up to five segments. The rule conventions that you build appear in the Format and Size fields of the Add Mark Rule dialog box. A sample name that matches the rule is displayed in the Example field.



6. Use the arrows to adjust the location of the segments, as needed.
7. Select OK. The rule is displayed in the Mark Names pane.
8. Select Apply to apply all the rules to your system.

Note:

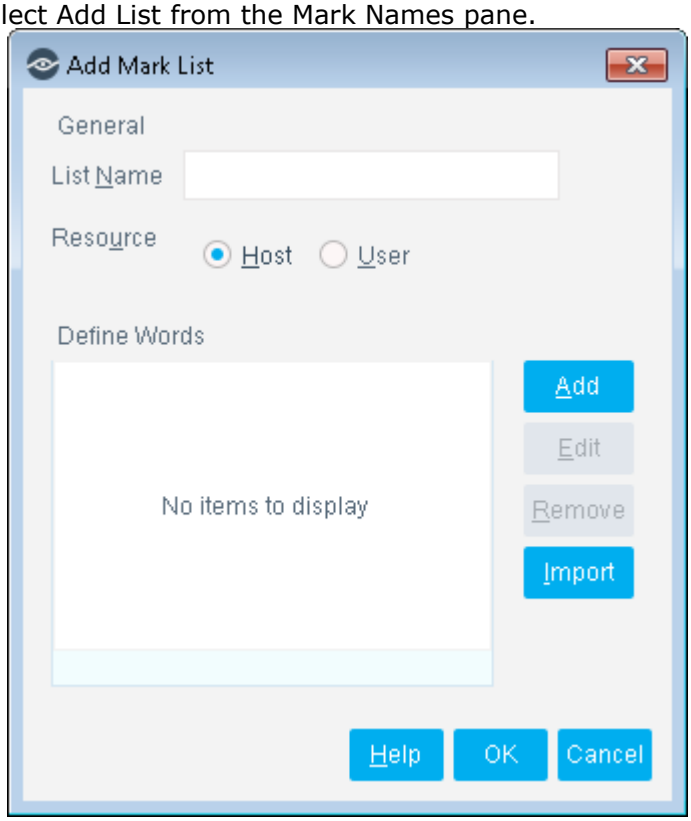
You must apply all the rules that appear in the Mark Names pane. If you do not want to apply a rule, remove it.

Define List Rules

Endpoint and user names for your network may be designed to meet specific networking or organizational needs. For example, user names may be created to reflect specific departments in your organization or cities in which your organization is represented, or any group of names created by your security administrator. You can define a similar list of host and user names to be used when sending marks.

To define list rules:

1. Select Add List from the Mark Names pane.



2. Enter a list name in the List Name field.
3. Select a Host or User to be applied to this resource type.
4. In the Define Words area, add a word to the list.
5. Select Add.
6. Continue adding or deleting names as required. You can also import a list of names by selecting Import. A standard import dialog box opens, on which you can locate the relevant file to import.
7. Select OK. The list is displayed as an entry in the Mark Names pane and you can apply the list to your system.
8. Select Apply to apply all the rules to your system.

   Note:

   You must apply all the rules that appear in the Mark Names pane. If you do not want to apply a rule, remove it.

Define virtual site endpoint Operating System parameters

When responding to network scans, Forescout eyeControl generates a virtual site. The site contains virtual endpoints and resources that are visible to attackers.

To more realistically reflect the endpoints in your network environment, you can define:

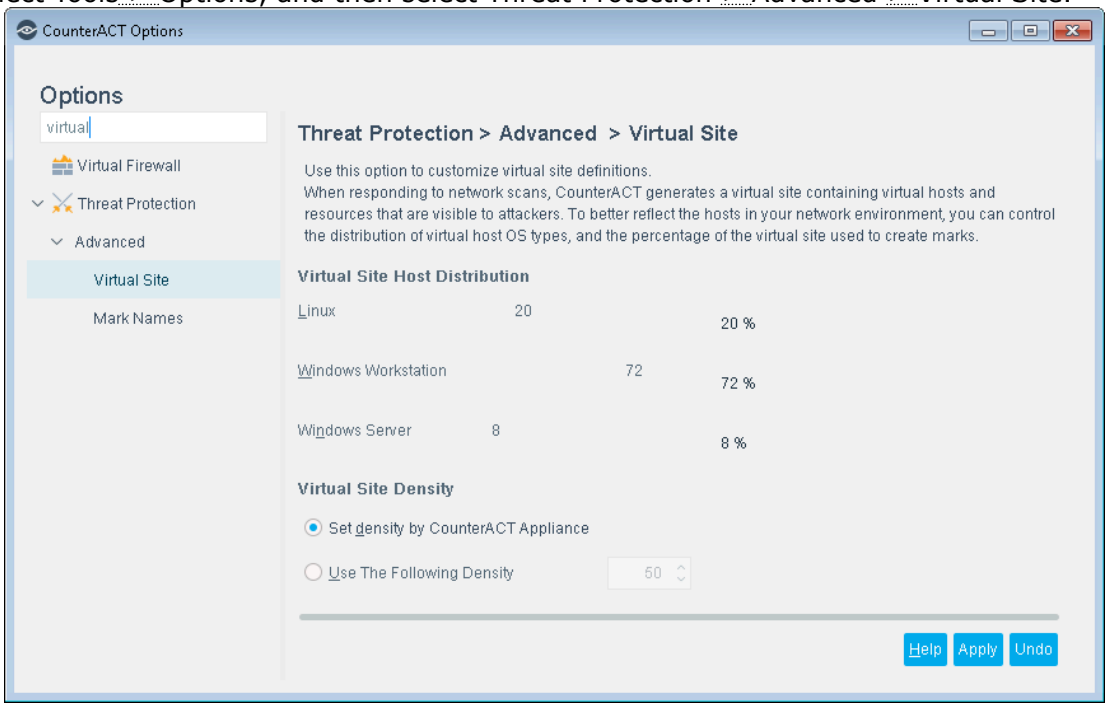
- The distribution of virtual host OS types that are presented on your virtual site. For example, Linux, Windows Workstations or Windows Servers.
- The density of virtual endpoints in your network. Density refers to the percentage of the virtual site, built with unused network resources (such as free IP addresses, closed ports), to be used to create marks.

Note:
If you work with this tool incorrectly, Forescout eyeControl may not protect your network properly.

Note:
Only users with the required permission have access to this tool.

To define the virtual host OS distribution:

1. Select Tools > Options, and then select Threat Protection > Advanced > Virtual Site.



2. Use the sliders to allocate a ratio. Distribution changes are built gradually. This means the changes are not implemented immediately.
3. Set the virtual site density, either:
    - Select Set density by CounterACT Appliance, for a value optimally calculated by Forescout eyeControl.
    - To manually set the virtual host density, select Use The Following Density and adjust the value. The value is set in percentages, for example, utilizing 50% of the virtual site.

4. Select Apply.

Parse event information displayed in email alerts

Email alerts that you receive regarding host activity and service attacks include a summary of events and details of each event. Detailed event information is also displayed in the email in a format that can be easily parsed by external applications.

The parsing event information is located at the bottom of the email in the Event Details for Parsing area. Each event is represented by a single line that begins with the word SUMMARY. Fields are separated by colons.

Example:

```
SUMMARY: 192.0.2.1:Port bite: port block: 1037871052:1037885452
```

where

192.0.2.1	Endpoint address.
Port bite	Event type.
port block	Forescout eyeControl action. (Monitor, Host Block or Port block)
1037871052	Event time. Calculated in seconds from 1 Jan 1970.
1037885452	Expiration time. Calculated in seconds from 1 Jan 1970.

Manage Forescout eyeSight users

You can:

- Create user management accounts for single users or user groups
- Assign permissions to allow, limit, or prevent user access to specific Console and web portal tools
- Limit view of endpoints per user
- Lock and unlock users
- Generate reports detailing user activity
- Create user password policies
- Create Terms & Conditions to be accepted during login
- Implement advanced security login methods

The Permissions and Scope options offer powerful user control. For example:

- Allow access to the entire network range, but never allow access to certain high security features, such as the Appliance configuration or Action Threshold features.
- Allow access to a specific network range, such as a particular building, and grant permission to all Forescout tools.

In addition, you can create users or user groups that have access to only the Console or only to web portals, or users that can access both.

Note:
Users who have no permissions cannot log in to the Console or to any of the Forescout web portals.

Forescout eyeSight users and user profile types

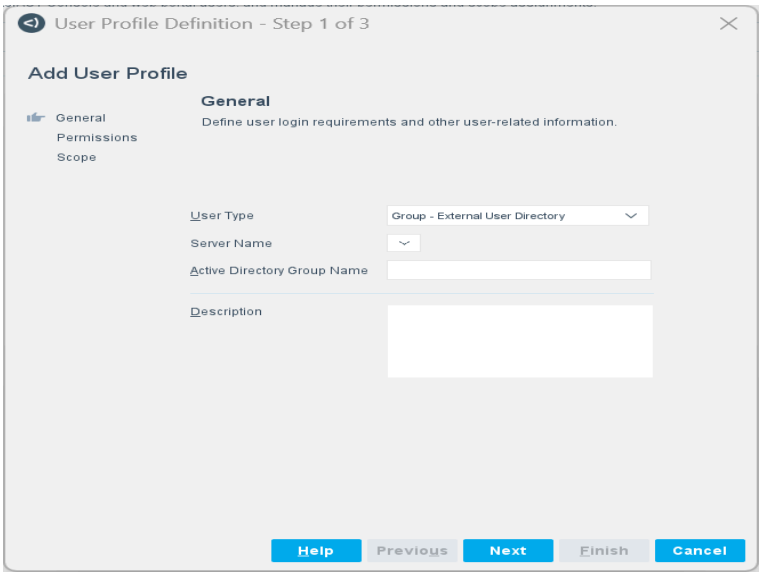
Working with user groups lets you streamline and simplify user creation. Specifically, you can define user groups based on RADIUS or user directory user groups. All users associated with a group are granted identical Forescout permissions and scope assignments.

For example, you can create one group of administrative users with full permissions and full access to all network segments and create another group of users who can only access certain features or certain network segment.

Users in a group log in to the Console and web portals using their user directory or RADIUS server credentials. They are authenticated via the authentication server defined when the group was created.

Two methods are available for grouping users:

- Associate user groups with a specific RADIUS attribute and value (shown below) .
- Associate user groups with a specific User Directory group membership.



Users and user groups are defined in the CounterACT User Profiles table and assigned the following:

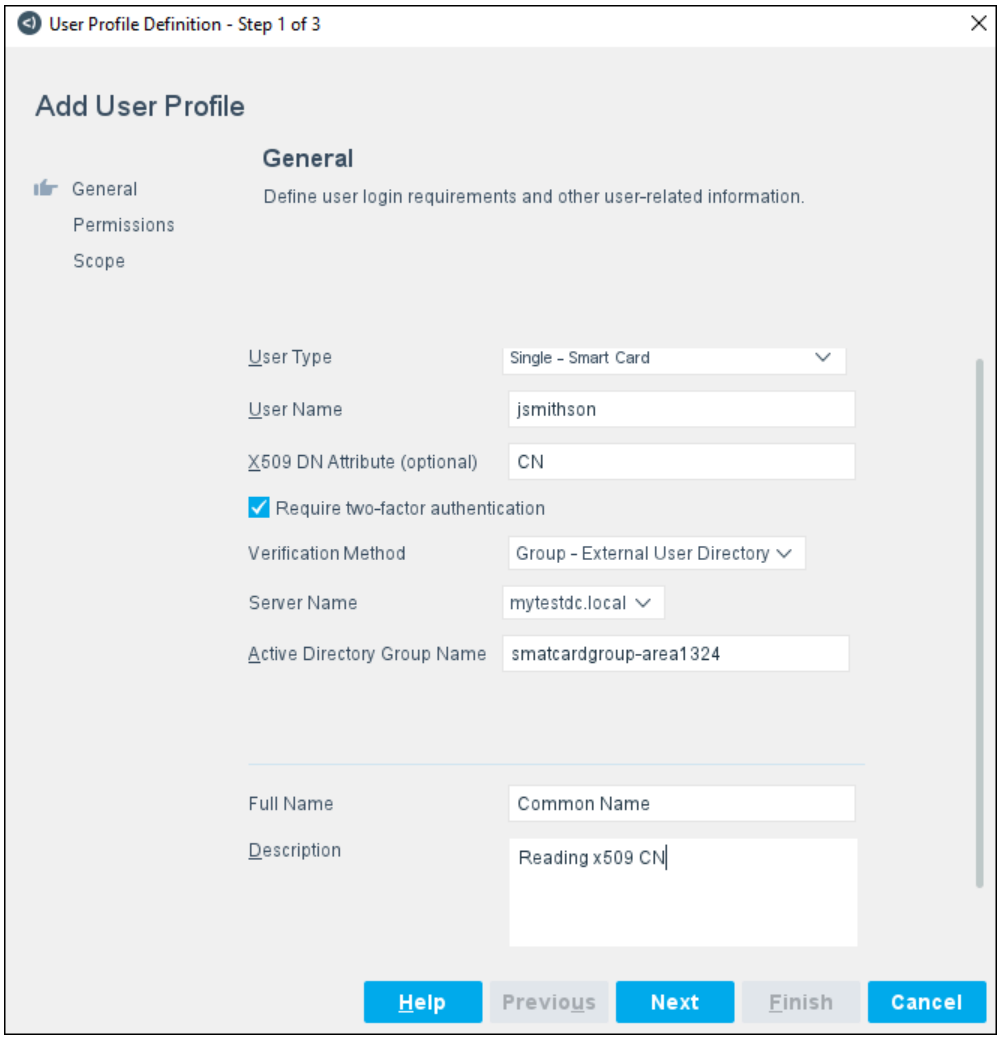
- Authentication requirements: Define which authentication method is required when logging in.
- Feature permissions: Prevent or allow access to specific Console and web portal feature
- Scope access: Define which network devices can be viewed and controlled.

Note:
The "admin" user always has access to all Console and web portal features throughout the network.

Following is a list of User Types:

Single – Password	Use this option to create user profiles for individual users who authenticate via the Forescout server with a user name and password. Individual users who authenticate via the Forescout server using a user name and password. The user must authenticate with a User Name and Password.
Single – SSO (Web Only)	Use this option to create user profiles for individual users who provide their single sign-on (SSO) credentials to authenticate with an external identity provider. See External Identity Provider User Authentication. These users can only access Forescout web portals (Web Access permissions). The user must authenticate with an email address as the User Name.
Single - External User Directory	Use this option to create user profiles for individual users who authenticate via a User Directory server defined in the User Directory Plugin, with the Use for Console Login option enabled.

	The user must authenticate with a User Name, the User Directory Server Name, and a Full Name.
Single - Smart Card	Use this option to create a user profile for an Individual user who authenticates via a Smart Card. Related certificates and CRLs must be defined in Forescout, and the User Name defined here must be identical to the Common Name (CN) of the Smart Card certificate. **Note:** For information about Smart Card certificates, see Smart card certificate configuration for Forescout eyeSight. The user must authenticate with a User Name and a Full Name. Authentication can optionally include an x.509 DN Attribute (CN, SerialNumber, or emailaddress). Authentication can optionally include two-factor authentication with one of the following verification methods: • Single - Password • Single - External User Directory • Group - External RADIUS • Group - External User Directory **Note:** For information about these x.509 attributes, see x.509 digital certificate attributes for Forescout eyeSight A sample of a user profile for a Single Smart Card user (General tab) is shown below:



Group - Smart Card - External User Directory

Use this option to create a common user profile for a group of Smart Card users. The user must authenticate with an x.509 DN attribute: Supported types:

- CommonName
- EmailAddress
- SerialNumber
- Subject Alternative Names (SAN): with Field Value of Principal Name or EmailAddress

Note:

For information about these x.509 attributes, see x.509 digital certificate attributes for Forescout eyeSight

Related certificates and CRLs must be defined in Forescout, and the User Name defined here must be identical to the x.509 attribute of the Smart Card certificate.

Note:

For information about Smart Card certificates, see Smart card

certificate configuration for Forescout eyeSight.

The user must also enter the User Directory Server Name, and the Active Directory Group Name as (mandatory) secondary authentication.

The Active Directory (AD) User Identifier drop-down menu allows you to choose which AD User Identifier to use to match the certificate when logging in.

AD User Identifier settings:

- When X509 DN attribute is set to CommonName, AD User Identifier defaults to sAMAccountName.
- When X509 DN Attribute is set to Email Address, AD User Identifier defaults to mail.
- When X509 DN attribute is set to Subject Alternative Names and SAN Field Value is set to Email Address, AD User Identifier defaults to mail.
- When X509 DN attribute is set to Subject Alternative Names and SAN Field Value is set to Principal Name, AD User Identifier defaults to userPrincipalName.

Group - External User Directory	Use this option to create a user profile to associate a Forescout user group with a specific external directory group membership. All users associated with this group receive the permissions and scope assignments defined for this group user. In the User Directory Plugin, this external directory server must be defined with the Use for Console Login option enabled. Because access control is determined at the authentication server, the Lock and Unlock buttons are disabled for this user type. The user must authenticate with the User Directory Server Name, and the Active Directory Group Name.
Group – SSO with User Directory (Web Only)	Use this option to grant access based on group membership in their organization. After SSO login is authenticated, the eyeSight queries the organization's Active Directory server to verify the user's group membership. These users can only to access Forescout web portals (Web Access permissions). The user must authenticate with the User Directory Server Name, and the Active Directory Group Name.
Group - External RADIUS	Use this option to associate Forescout user groups with a specific RADIUS attribute and value.

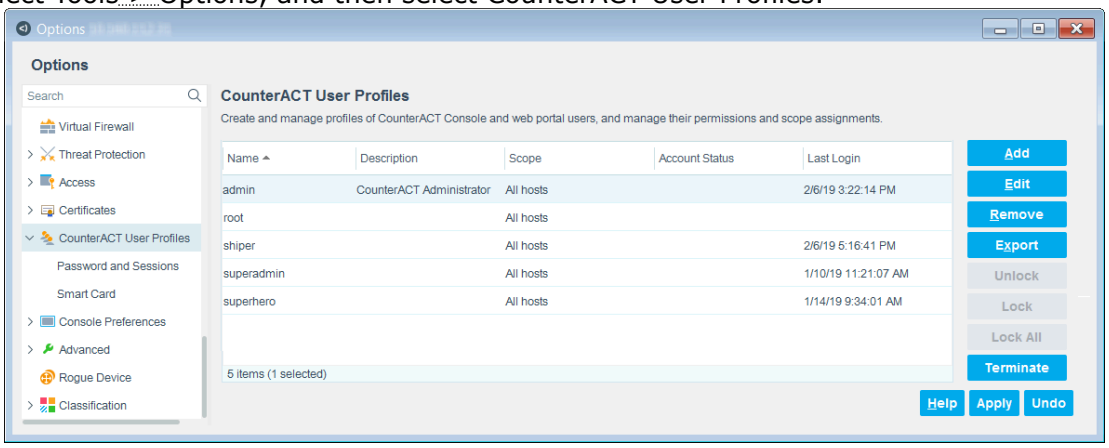
Because access control is determined at the authentication server, the Lock and Unlock buttons are disabled for this user type.

Create users and user groups

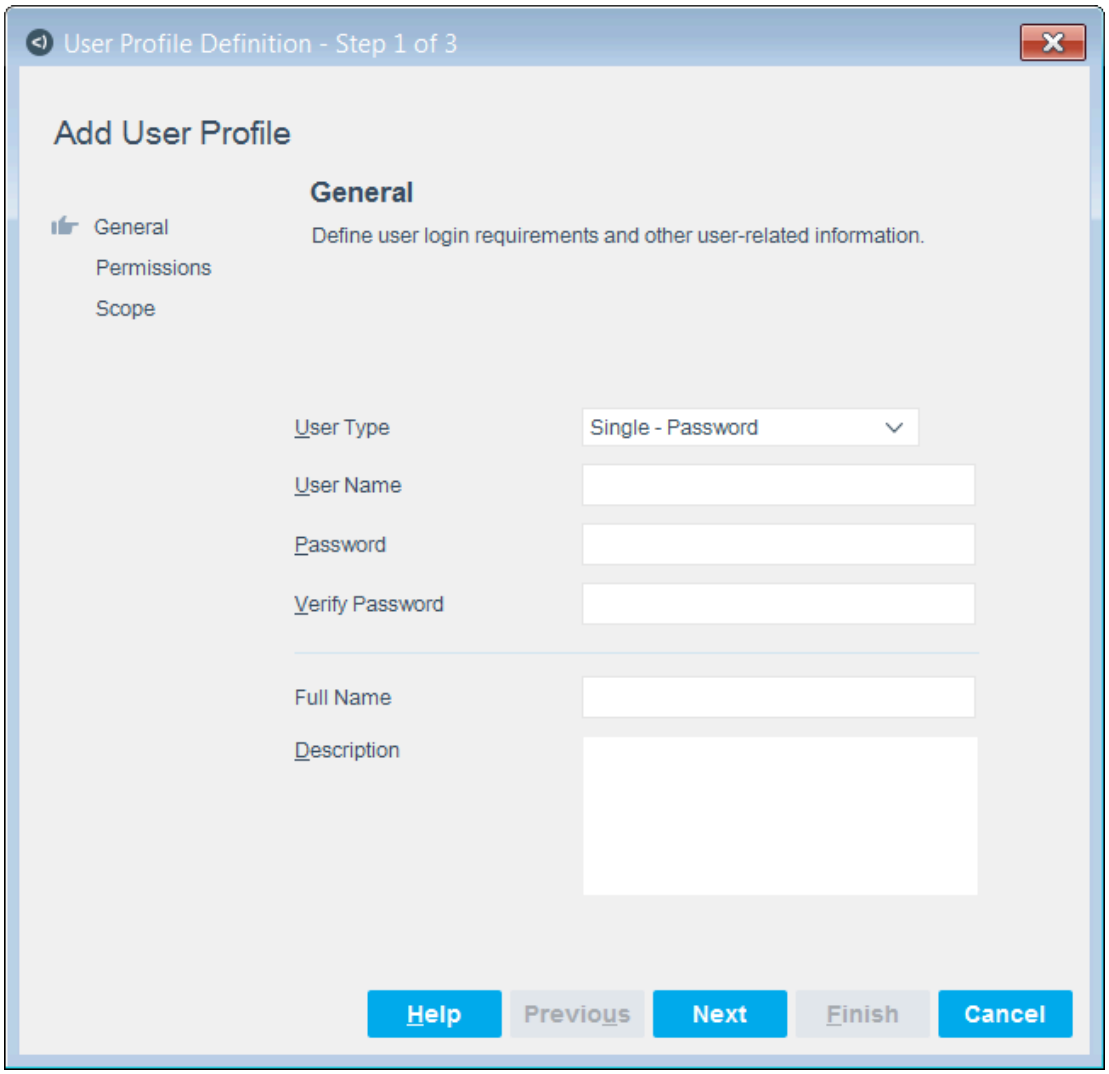
Note:
This procedure ONLY applies if you need to set up users or user group for the on-premises Console / Console Web Client. Before running this procedure, see Users and User profile Types .

To create a user or user group for Forescout eyeSight / Console Web Client:

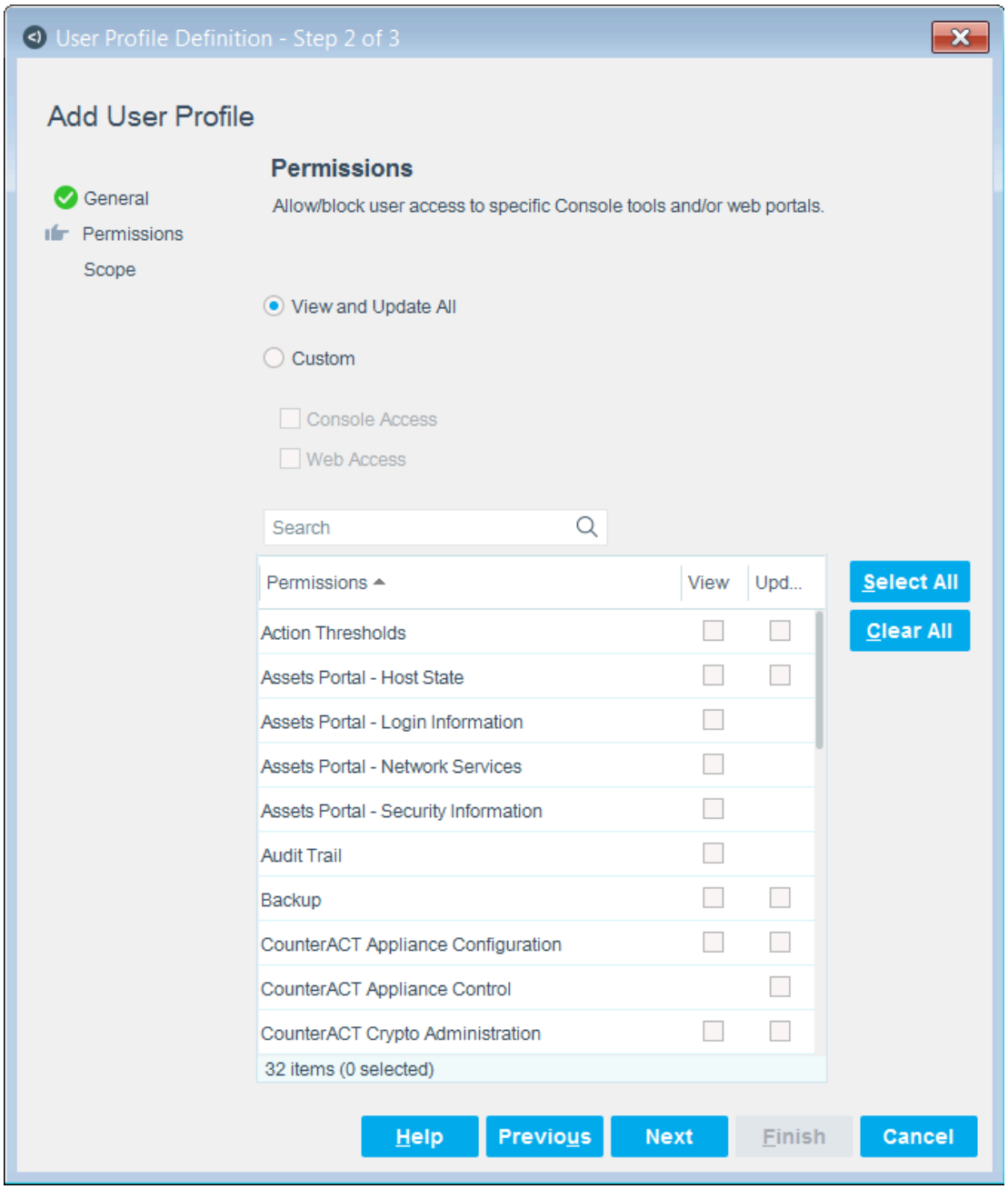
1. Select Tools > Options, and then select CounterACT User Profiles.



2. Select Add. The Add User Profile wizard opens and displays the General pane.



3. In the General pane, select a user type from the User Type drop-down menu, as well as the authentication method to be used. Authentication parameters available change depending on the user type selected.
4. (Optional) After defining the user type and authentication setting, enter a full name and description of the user or group. The full name is displayed in the Change Password dialog box whenever the user updates their password. See Manual User Password Change.
5. Select Next to continue with permissions.



6. To allow the user to work with only the Console or only web portals, select Custom, and then select either Console Access or Web Access. Users that are assigned either the user type Single – SSO (Web Only) or the user type Group – SSO with User Directory (Web Only) can only access a subset of Forescout web portals.
7. In the Permissions table, select the specific permissions for the user: See Access to Forescout Console tools permissionsfor the full list of permissions.
    - No selection: Prevents users from viewing the feature.
    - View: Allows users to only view information.
    - Update: Allows users to view and update information.
    - When you update permissions for other users, those users must exit and then log in again for the permissions to take effect.

    Users not assigned permissions cannot log in to the Console or any of the Forescout web portals.

Note:
Forescout users must log in from an IP address within the permitted range. See Define Console Access. Web portal users must log in from an IP address within the permitted range. See Define Web Access .

8. Select Next to continue with Scope.
9. Use the Scope pane to grant and limit access to specific IP address ranges or segments in the Console or web portals, and complete this procedure. See Access to Forescout eyeSight network endpoints – scope

Access to Forescout Console tools permissions

Action Thresholds	Implement Action Thresholds when working with blocking and restrictive actions. See Working with Action Thresholds for details.	
Assets Portal –Host State	View and change the host state from the Assets Portal.	
	Assets Portal –Login Information	View user login information for a specific address, an endpoint name, a server, within a group.
Assets Portal –Network Services	View information about open network services.	
	Assets Portal –Security Information	View security information, such as information about antivirus installations.
Audit Trail	View reports on user activities during a specified time period. See Monitoring User Activity.	
Backup	Back up and restore system and component settings. See Backing Up System and Component Settings.	
CounterACT Appliance Configuration	Configure the Appliance using a variety of configuration tools, including Channels, Organizational Units tools and more.	
	CounterACT Appliance Control	Start, restart, or stop Appliances, and define mark-naming rules. The rules can be designed so that they reflect naming conventions used in your organization or network environment. This makes the marks more realistic. See About Mark Rules.
CounterACT	Import, edit, and remove trusted and system certificates in the eyeSight and	

Crypto Administration	configure certificate-related settings, such as certificate expiration monitoring and checking for new CRLs and ongoing TLS sessions.
CounterACT Device Script Management	Work with pre-defined scripts in Tools > Options > Advanced > Configuration Script.
Enforcement Mode	Control the Forescout Enforcement mode. Full Enforcement mode allows complete functionality. Partial Enforcement mode lets you monitor network traffic with limited ability to respond. Partial Enforcement mode is recommended for evaluation purposes only. See Set the Enforcement Mode.
Enterprise Manager Control	Start, restart, or stop Enterprise Managers.
Event Log	View the Event Log that displays system events. See Work with System Event Logs.
eyeSegment	For users with an eyeSegment license, view and change the eyeSegment matrix and the eyeSegment policy. For specific permission settings, refer to the *Assign eyeSegment User Permissions* section in the *Forescout eyeSight eyeSegment Module Configuration Guide*.
Group Management	Add, edit, remove, or update Forescout Groups. The Group Management permission cannot be changed (to read-only or view only) if the Policy Management permission is selected. See Working with Forescout Groups.
Host State Override	Update the state of endpoints and how long the state is maintained. See Changing the Host State and Changing the Host State Maintenance Time.
IPS Scheduled Reports	Work with scheduled Threat Protection Reports.
Legitimate Traffic	Define the addresses of legitimate traffic at your network. See View Legitimate Traffic.
License Management	Install and manage Forescout licenses. See License Management.

Dashboards: Access	View and change information in the Dashboards and Assets views of the Forescout Web Client. See Dashboards and Assets View.
Dashboards: Device Compliance (OOTB)	Enabling this option permits a user to access the Device Compliance dashboard.
Dashboards: Device Visibility (OOTB)	Enabling this option permits a user to access the Device Visibility dashboard.
Dashboards: Health Monitoring (OOTB)	Enabling this option permits a user to access the Device Health dashboard.
Dashboards: Policies, Segments and Groups in Assets Tab	Enabling this option permits a user to view the Policies, Segments, and Groups in the Assets tab.
Malicious Traffic	View malicious traffic. See Threat Protection.
Module Control	Start, stop, test, and get help on plugins and modules.
Module Management	Install and uninstall plugins and modules.
Multiple CounterACT Appliance Management	Manage a number of Appliances within the network. See Managing Appliances, Enterprise Managers, and Consoles.
Policy Control	Start, stop, pause, test, and clear all policy actions without changing the policy definitions. See The Policy Manager.
Policy Management	Create, edit, delete, import, and export either policies, segments, groups, or lists. The Policy Manager Working with Forescout Segments

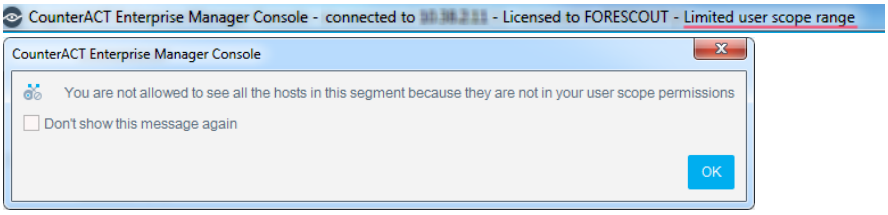
	Working with Forescout Groups Defining and Managing Lists
Policy Reports	View NAC reports. See Policy Reports and Logs.
Reports	Work with the Reports Portal. See Reports.
Software Upgrade	Upgrade Appliance / Enterprise Manager software.(Refer to About this Upgrade Guide in the *Forescout eyeSight Upgrade Guide*, which covers the software upgrade procedures.
Threat Protection Policy	View and manage Threat Protection Policy settings.
User Management	View and edit user management features. See Managing Users.
User Portal Builder	Create, duplicate, preview, or export/import customized Guest Management Portal and HTTP pages.
Virtual Firewall	Protect specific services by allowing or preventing traffic and defining various traffic rules. See Managing Your Virtual Firewall Policy.

Access to Forescout eyeSight network endpoints – scope

Use the Scope pane to grant and limit access to specific IP address ranges or segments in the Console or web portals. Users can only see or control the following Forescout features in the ranges or segments assigned to them:

- Policy Management
- Segment Management
- Group Management
- Organizational Units
- All tools listed in the Forescout Options window, with the exception of the Console Preferences folders
- Check for Updates
- Lists

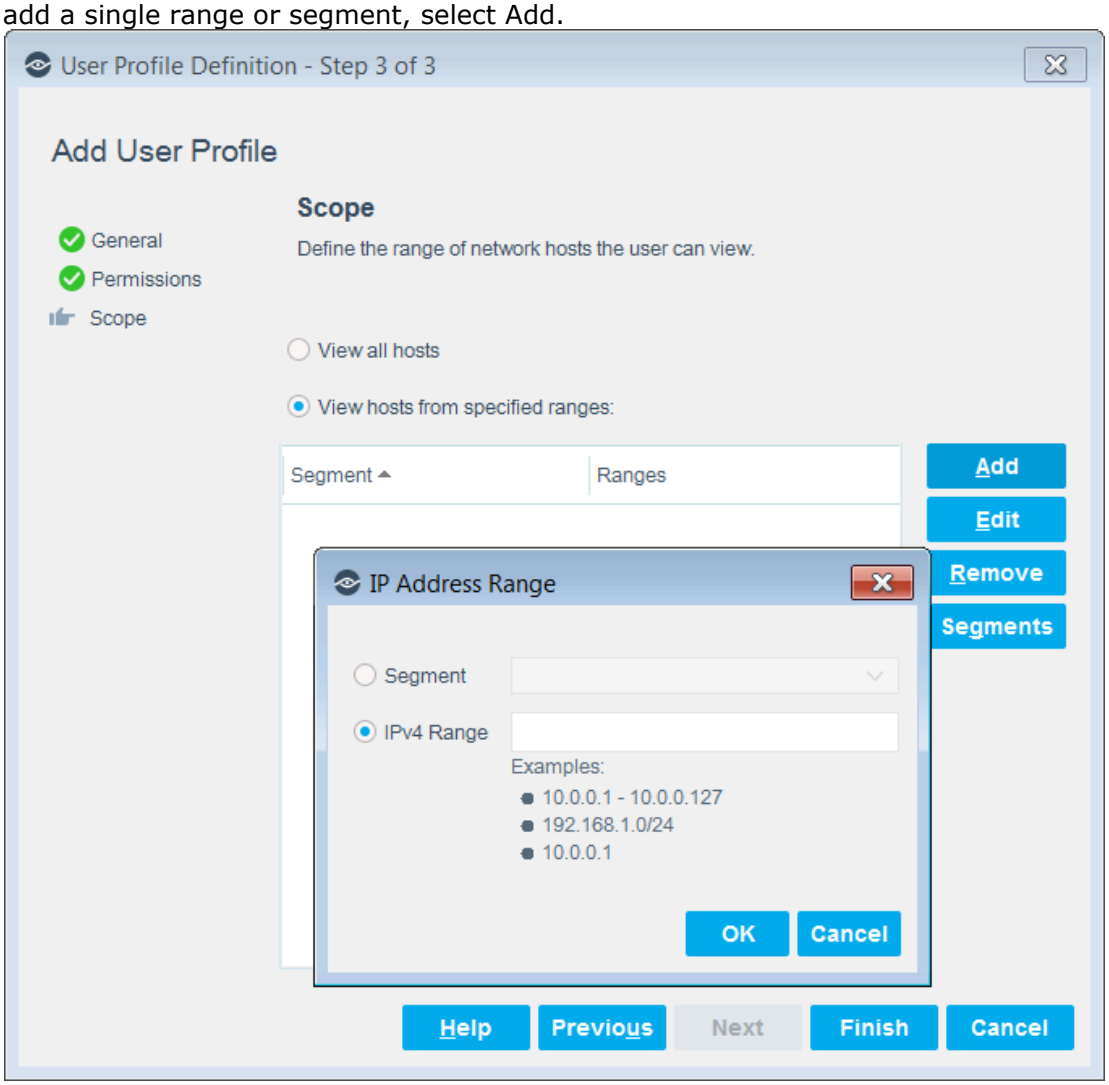
If a user's scope does not include a particular segment, options for that segment are grayed out (disabled) and/or messages are displayed in toolbars or dialogs.



To allow users access to a specific range but limit their access to a specific feature, grant Scope access and then limit Permissions for that feature. For example, grant users permission to view the entire network range while restricting their access to Appliance configuration features.

To limit the Scope access:

1. Select View hosts from specified ranges.
2. To add a single range or segment, select Add.



3. In the IP Address Range dialog box, enter the range or segment you want the user to be able to access, and select OK.
4. To add multiple segments, select Segments, select the appropriate segments, and select OK.
5. Select Finish. The user definition is displayed in the CounterACT User Profiles pane.
6. Select Apply.

Default Forescout Console admin user

The Forescout Console is installed with an "admin" user who always has access to all Console and web portal tools and features. You do not need to create a new user to operate the system. You can create additional Forescout users and user groups and customize their permissions and scopes.

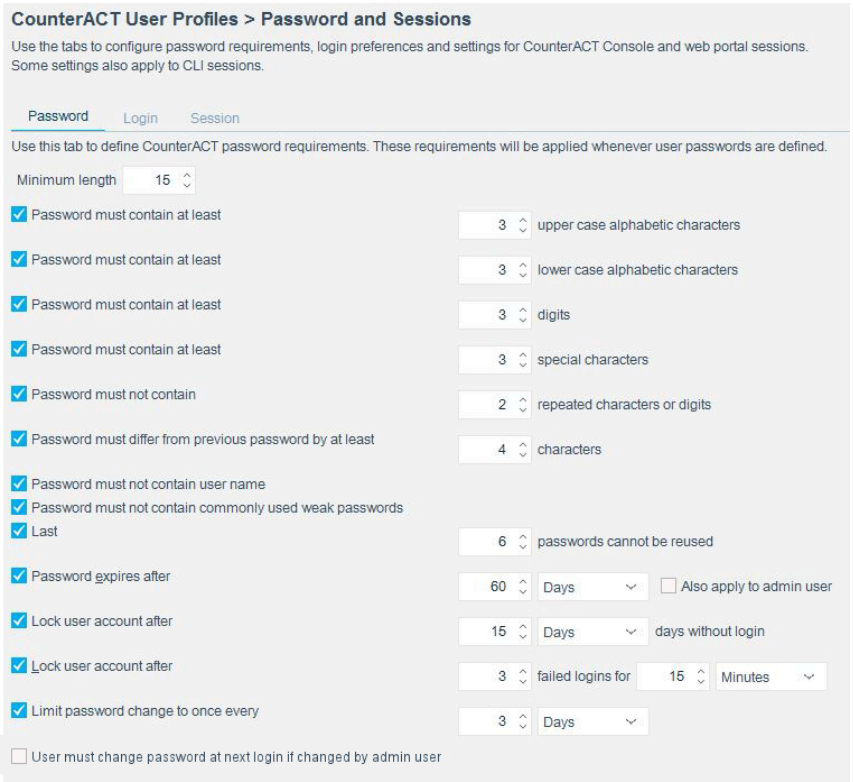
Note:
You cannot modify the permissions for the default Forescout "admin" user.

Note:
You cannot remove the default Forescout "admin" user.

Forescout Console password protection

To configure password protection preferences, select Tools > Options > CounterACT User Profiles > Password and Sessions, and then select the Password tab.

Note:
Unless specified otherwise below, these settings apply to Console users, web portal users, and users logging in to eyeSight devices through the command-line interface (CLI).



Minimum length Minimum configurable: 6

Default: 15

Password must contain at least {x} upper-case alphabetic characters	Default: 3	
	Password must contain at least {x} lower-case alphabetic characters	Default: 3
Password must contain at least {x} digits	Default: 3	
	Password must contain at least {x} special characters	Default: 3
Password must not contain {x} repeated characters or digits	Default: 2	
	Password must differ from previous password by at least {x} characters	Default: 4
Password must not contain username	Enabled by default.	
	Password must not contain commonly used weak passwords	Selecting this option also enforces the following additional requirements: • Password must contain at least five different characters • Password must not contain multiple pairs of consecutive characters (e.g., abcd1234) • Password must not be in National Insurance number format (e.g., QQ123456C) Enabled by default.
Last {x} passwords cannot be reused	This option applies only to Console and web portal users, and not to users logging in to CounterACT devices through the command-line interface (CLI). Default: 6	

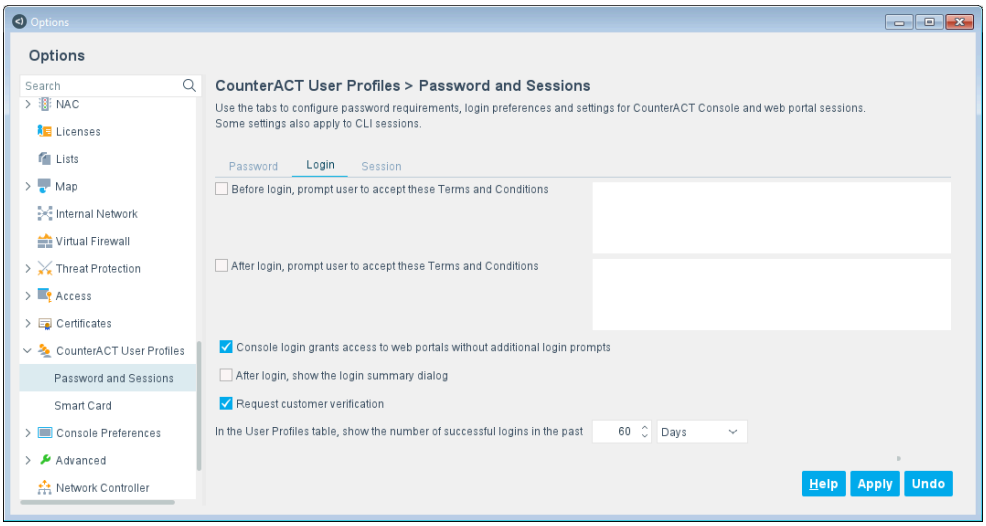
Password expires after {x} {days/ weeks}	A Change Password dialog box opens during login when this period expires. Select whether to apply to Forescout "admin" users also. Selecting this option does not affect users of types Group - External User Directory, or Group - External RADIUS. Default: 60 days
Lock user account after {x} {days/weeks} days without login	This option applies only to Console and web portal users, and not to users logging in to eyeSight devices through the command-line interface (CLI). Selecting this option does not affect users of types Group - External User Directory, or Group - External RADIUS. Default: 15 days
Lock user account after {x} failed logins for {x} {minutes/ hours}	The Forescout "admin" user cannot be locked out. Users who enter the wrong username are not locked out. Selecting this option does not affect users of types Group - External User Directory, or Group - External RADIUS. Default: 3 failed logins, for 15 minutes
Limit password change to once every {x} {hours/days}	This applies only when the password was last changed by the same user. If, for example, the Forescout "admin" user last changed the password of a non-admin user, the non-admin user is not restricted by the time defined in this setting. Default: 3 days
User must change password at next login if changed by admin user	Selecting this option will prevent users who only have permissions to access Forescout Web Client tools (for example, Dashboards) from logging in to the Web Client after an admin user changes their password. This option only applies to Console and web portal users, and not users

logging in to CounterACT devices through the command-line interface (CLI).

Default: Disabled

Forescout Console login preferences

To configure login preferences, select Tools > Options > CounterACT User Profiles > Password and Sessions, and then select the Login tab.



Before login, prompt user to accept these Terms and Conditions

When you enable this option, a message you create is displayed before user login to the Console, web portals and CLI.

You must define the message that is displayed. Messages can describe legal or usage restrictions or other information.

After login, prompt user to accept these Terms and Conditions

When you enable this option, a message you create is displayed after user login to the Console, web portals and CLI.

You must define the message that is displayed. Messages can describe legal or usage restrictions or other information.

Console login grants access to web portals without additional login prompts

By default, users who log in to the Console can access Forescout web-based tools without additional login prompts. Enable this option to require users who are logged into the Console to re-enter credentials when they access Forescout web portals from the Console.

After login, show Enable this option to display a summary of the user's

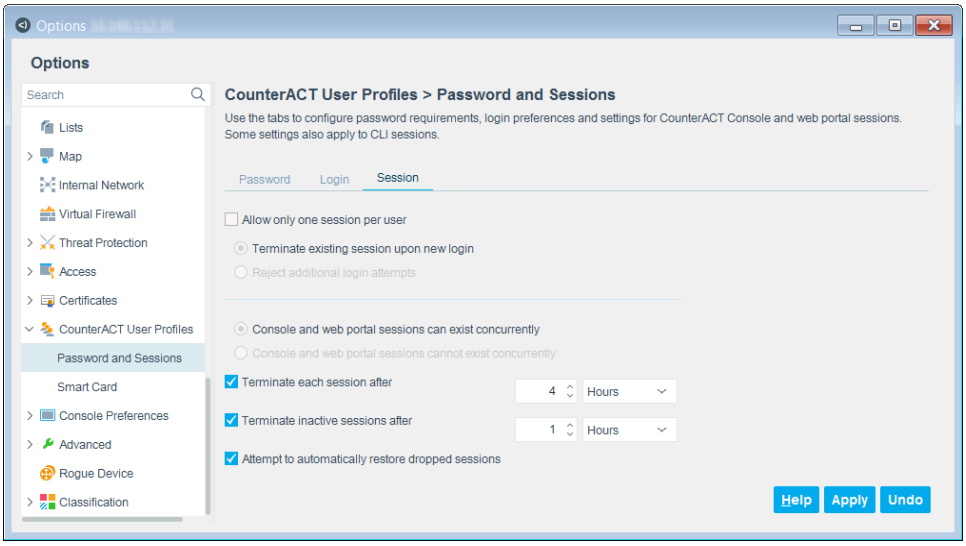
the login summary dialog	recent logins immediately after successful user log in. By default, this option is disabled. In Certification Compliance mode, this option is not available.
Request customer verification	Enable this option to prompt users to complete customer verification if they have not done so. See Customer Verification for details.
In the User Profiles table, show the number of successful logins in the past	Specify the time period for the Number of Logins column in the CounterACT User Profiles table.

Forescout Console session handling preferences

Note:
When a user has a current, Forescout Console session open and, during this time, the eyeSightm administrator changes the permissions of that user, the following occurs:

- The affected user's Console session automatically terminates (user is automatically logged out of the Console)
- The automatic session termination is accompanied by the display of following warning message: `Your session has been terminated. To continue working, please log in again.`

Session handling preferences determine how to handle idle, dropped, and concurrent user sessions. To configure session preferences, select Tools > Options > CounterACT User Profiles > Password and Sessions, and select the Session tab.



Note:
Most of these settings do not apply to CLI sessions.

Allow only one session per user	Enable this option to prevent a user from opening more than one concurrent Console session.
Terminate existing session upon new login	When a user tries to log in to a new session, the existing session ends and the Console or web portal closes.
Reject additional login attempts	When a user tries to log in to a new session, the existing session ends and the Console or web portal closes.
Console and web portal sessions can exist concurrently	By default, the system allows Console and web portal sessions to exist concurrently.
Console and web portal sessions cannot exist concurrently	Enable this option to prevent a single user from opening simultaneous Console and web portal sessions.
Terminate each session after	The maximum length of time that any Console or web portal session can be open. After this time even active sessions are terminated. A message is displayed before the session is closed.
Terminate inactive sessions after	The maximum length of time that an inactive session is kept open. Inactive web console sessions that time out are closed, then automatically logged in again. This counts as a single session for the timeout value of the Terminate each session after field.
Attempt to automatically restore dropped sessions	When this option is enabled, Forescout attempts to reconnect a session that seems to have dropped. Forescout uses the previous session's credentials.

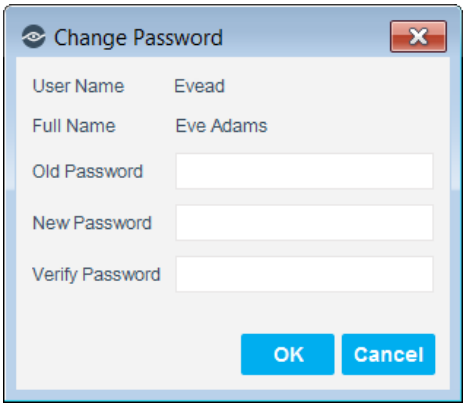
Forescout Console manual user password change

In addition to administrator-controlled password changes (see Creating Users and User Groups), users who authenticate using passwords can manually change their user password from the Console and from the Forescout web portals. The user password is global and applies to all Console and web portal logins.

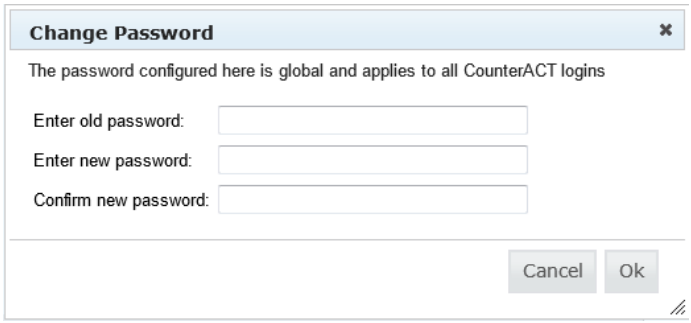
This option is disabled for users who log in to the eyeSight through an external User Directory server. For users not connecting through an external User Directory server, the Change Password option is always enabled and cannot be removed by an "admin" user.

Change password activity is written to the Audit Trail. To access the Audit Trail, select Log > Audit Trails. See Monitoring User Activity for details.

To change your Forescout User Password from the Console, select Tools > Change Password.



To change your Forescout User Password from some web portals, in the user name section of the web portal, select the Change Password icon .



Use Forescout eyeSight smart card authentication

The eyeSight and Forescout portals support Smart Card authentication, a highly secure method for users to authenticate using a physical card and a smart card reader that can require a PIN code. A single smart card can contain multiple certificates or cryptographic keys. The eyeSight supports certificate revocation lists (CRL) and Online Certificate Status Protocol (OCSP) for smart card authentication.

CRL validation

A certificate revocation list (CRL) is a list of certificates revoked by the issuing certificate authority (CA) before their actual or assigned expiration date. The CRL identifies certificates that are no longer trusted and is used by various endpoints to verify if a certificate is valid. The CA signs the CRL file for added security.

OCSP validation

OCSP is used to obtain the revocation status of X.509 digital certificates. Created as an alternative

to CRL, OCSP enables real-time status checks for the certificate and costs less overhead on the client side.

Validation method failover

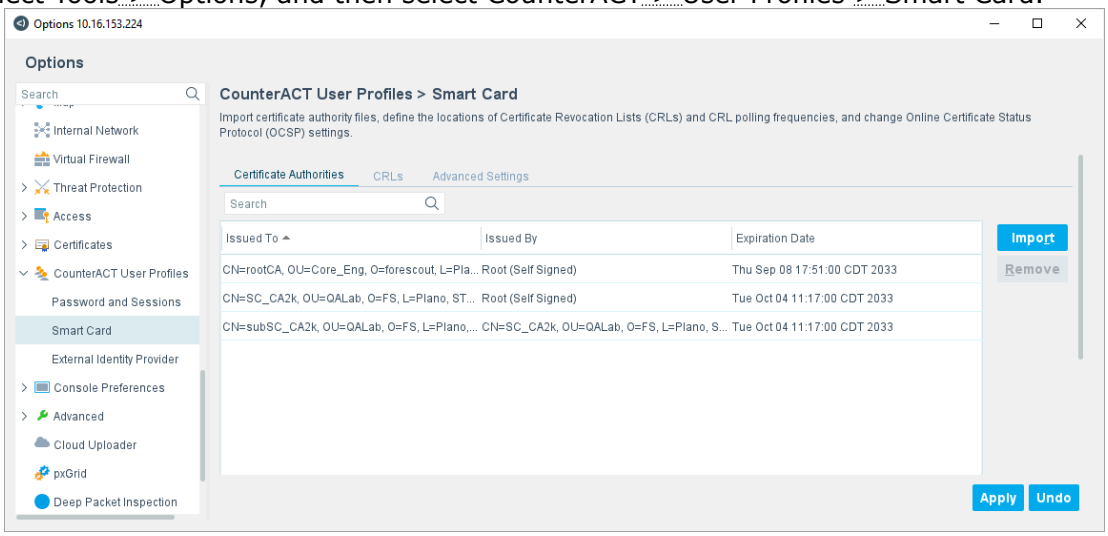
The eyeSight supports OCSP and CRL failover. After configuring a primary method, if that method is unavailable or the validation status is unknown, the other method is used to complete the certificate validation.

Smart card certificate configuration for Forescout eyeSight

To configure Smart Card authentication, you'll be asked to import certificate authority files and define the locations of certificate revocation lists (CRLs) and their polling frequencies. You can also configure the use of Online Certificate Status Protocol (OCSP) and set up validation method failover between CRL and OCSP.

To configure Smart Card authentication:

1. Select Tools > Options, and then select CounterACT > User Profiles > Smart Card.



2. Select Import. The Certificate Authority Wizard opens.
3. Select Import CA. An import dialog box opens.
4. Locate the required file and open it. There certificate file's information appears.
5. Select Next. The Define CRLs pane opens.
6. Select Add. The Add CRL URL dialog box opens.
7. Enter the URLs of the certificate revocation lists (CRLs) to use and the frequency to poll the lists.

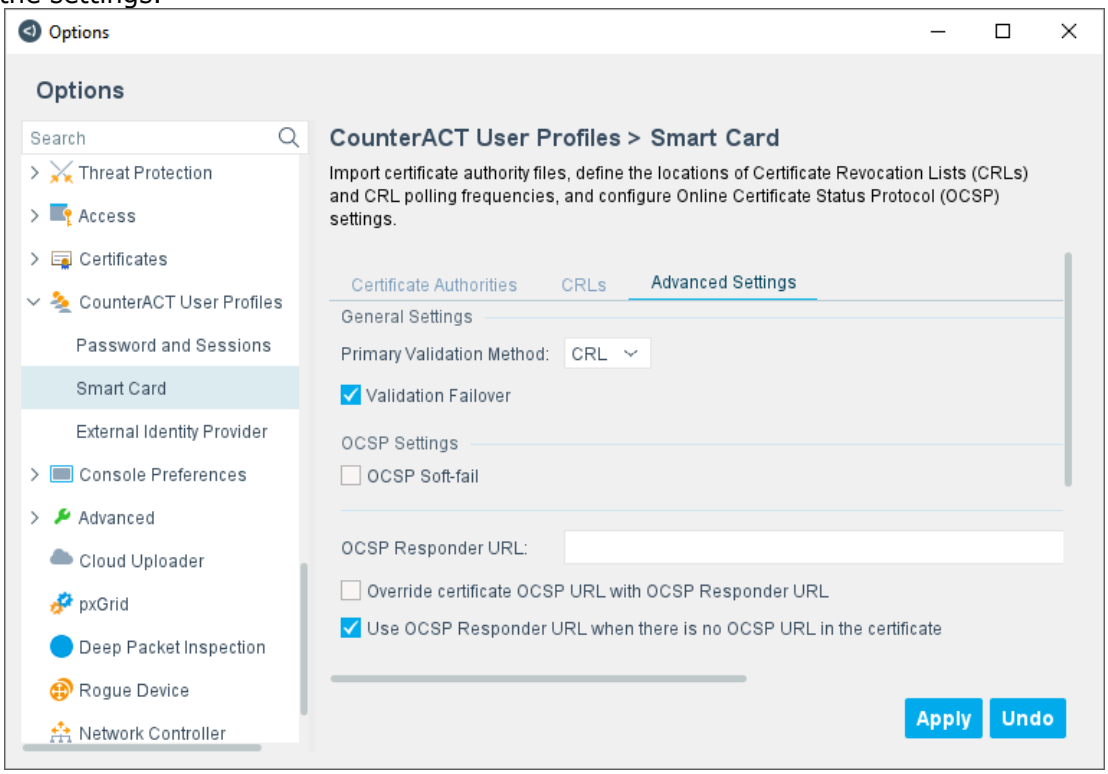
   Note:

   The minimum threshold for CRL download frequency is one (1) hour. Any configurations with a value less than one hour will automatically be adjusted to the minimum threshold value. This prevents excessive downloads of the CRL file and helps optimize Smart Card operations.
8. Select Finish. User sessions are authenticated as follows:
   - The eyeSight periodically checks the validity of certificates/trust chains used to authenticate live user sessions. If the certificate that authenticates a user session has been revoked, the user session is terminated. These events are logged in the Event Viewer.

- The eyeSight imports Certificate Revocation Lists (CRLs) at the specified frequency and updates its certificate store. After each update, all user sessions authenticated by certificates are rechecked.

Configure OSCP settings and fail over under the Advanced Settings tab, if desired.

9. Select the Advanced Settings Tab. See Smart card advanced settings for details about each of the settings.



10. Set the Primary Validation Method to either OSCP or CRL from the drop-down menu. CRL is the default. To use OCSP, configure the fields under OSCP Settings.
11. Enable OCSP Soft-fail to prevent an authentication failure if the status of a certificate is unknown or there are network connection issues producing an OCSP request timeout.
12. Enter a OCSP Responder URL of a valid OCSP Responder.
13. Choose to Override Certificate OCSP URL with OCSP Responder URL when a certificate has an Certificate Authority Information Access (AIA) extension that includes a OCSP Responder URL, if desired.
14. Enable Use OCSP Responder URL when there is no OCSP URL in the certificate to use the URL entered in the OCSP Responder URL field if an OCSP URL is not present in the certificate.
15. Click Apply.

Smart card advanced settings

The Smart Card Advanced Settings tab allows you to set validation method preferences including validation method failover.

Setting	Description
Primary Validation Method	Indicates whether OCSP or CRL is the primary method eyeSight uses to validate smart card certificates. The default is CRL.
Validation Failover	Enables failover if the primary method is unavailable or the validation status is unknown allowing the secondary method to complete the certificate validation.
OCSP Soft-fail	When enabled, if an OCSP response indicates a certificate status of UNKNOWN or there is network connection issue (timeout for OCSP request), the eyeSight does not fail the authentication.
OCSP Responder URL	Enter a valid OCSP Responder URL.
Override Certificate OCSP URL with OCSP Responder URL	A certificate can have a Certificate Authority Information Access (AIA) extension that includes a OCSP Responder URL. If enabled, the eyeSight ignores the OCSP Responder URL in the certificate and uses the URL entered into the OCSP Responder URL field instead.
Use certicate OCSP URL when there is no OCSP URL in the certificate	When enabled, the eyeSight uses the OCSP URL in the certificate, if present. If an OCSP URL is not present in the certificate, the eyeSight uses the URL entered into the OCSP Responder URL field instead.

x.509 digital certificate attributes for Forescout eyeSight

Smart Cards can use x.509 digital certificate attributes for authentication purposes.

Attribute	Description
CommonName	When selected in a Smart Card user profile, Forescout reads the CommonName field value from the DN of the Smart Card certificate, and will be validated with Active Directory (If the user has that name and is part of the group). This attribute is valid for both Single-Smart Card and Group-Smart Card-External Directory user profiles.
SerialNumber	When selected in a Smart Card user profile, Forescout reads the Serial Number field value from the DN of the Smart Card certificate, and will be validated with Active Directory (If user has that serial number and is part of the group). This attribute is valid for both Single-Smart Card and Group-Smart Card-External Directory user profiles.
EmailAddress	When selected in a Smart Card user profile, Forescout reads the Email address field value from the DN of the Smart Card certificate, and will be validated with Active Directory. (If user has that email address and is part of the group). This attribute is valid for both Single-Smart Card and Group-Smart Card-External Directory user profiles.
Subject Alternative Names with Principal Name	When selected in a Smart Card user profile, Forescout reads the SAN-Principal Name field value from the Smart Card certificate, and will be validated with Active Directory (If UPN exists as part of user account and is part of the group). This attribute is only valid for Group-Smart Card-External Directory user profiles.

Attribute	Description
Subject Alternative Names with Email Address	When selected in a Smart Card user profile, Forescout reads the SAN-Email address field value from the Smart Card certificate, and will be validated with Active Directory (If the email address exists as part of user account, and is part of the group). This attribute is only valid for Group-Smart Card-External Directory user profiles.

Note:
For information about Single-Smart Card and Group-Smart Card-External Directory user profiles, see Forescout eyeSight users and user profile types

Forescout eyeSight and OpenSC

OpenSC is a set of software tools and libraries that facilitate the use of Smart Cards in authentication, encryption, and digital signatures. OpenSC configuration files for Smart Card authentication are located in installdirectory\OpenSC\x86 and installdirectory\OpenSC\x64.

Note:
It is recommended to log on once as the admin after installing the Console to automatically update the JRE before allowing Smart Card authentication.

When logging on to the Console using a Smart Card as the Login Method, select the opensc_pkcs11.dll in the installation directory under Dll Location. See Log In to the Console for details.

Smart card user profile setup

In order to work with Smart Card authentication, you must verify that the Smart Card Common Name (CN) and the User Name are identical, including case-sensitive spelling. User profiles are defined in the CounterACT User Profiles pane.

You can define two types of Smart Card User Profile:

- Single - Smart Card
- Group - Smart Card - External User Directory

For information about these Smart Care options, and how to configure user profiles, see Forescout eyeSight users and user profile types and Creating Users and User Groups for details about creating users.

External Identity Provider User Authentication

Set up the eyeSight to work with an external identity provider for the purposes of performing single sign-on (SSO) authentication of users logging in to access the Forescout web portals. The Forescout platform works with any of the following identity providers:

- OKTA
- Ping Identity

In addition to these specific identity providers (IDP), the Forescout platform makes available the following IDP option:

- Other (SAML 2.0 compliant) - this option allows operators, who subscribe to any IDP

service that is compliant with the SAML 2.0 protocol for sharing information with a service provider, to set-up the eyeSight to work with that IDP, in order for the platform to provide its SSO authentication of users logging in to access Forescout web portals.

Users, whose user profile is assigned any one of the following user types, provide their SSO credentials to authenticate with the identity provider:

- Single – SSO (Web Only)
- Group – SSO with User Directory (Web Only)

For details about these user types, see Creating Users and User Groups.

There are two types of errors that may occur when an SSO Active Directory group user type attempts to log in to a Forescout portal that display the same error message, "There was an error trying to complete your request. Please notify your support desk or try again." The two error conditions are:

- The SSO group user does not exist on any User Directory server group.
- The SSO group user does exist in the User Directory server group but does not have the required permissions to view the portal.

After users of type Group – SSO with User Directory (Web Only) authenticate with the identity provider, the Forescout platform queries the organization's Active Directory domain server to verify the user's group membership. For the execution of this query, the eyeSight requires that the identity provider supply either one or both of the following user information, as attributes in its SAML response to the Forescout platform (the service provider):

- `sAMAccountName` in the format:

  `urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified`

- `userPrincipalName` in the format:

  `urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified`

If you are manually configuring your identity provider to work with the Forescout SSO service, make sure to first view the contents of the Forescout service provider metadata file (sp-metadata.xml) to determine whether Forescout URLs begin with an IP address or an FQDN. Whichever one is used in the Forescout service provider metadata file must also be used, in your identity provider, to configure the URLs that are used to access the Forescout SSO service.

Setting Up eyeSight to Work with an External Identity Provider

You must set up the eyeSight to be able to work with an external identify provider. There is a slight difference in the set-up process when you perform this set-up for the very first time ever.

To set-up, the Forescout eyeSight with an external identify provider:

1. Select Tools > Options, and then expand the **CounterAct User Profiles** folder.
2. Select External Identity Provider. The External Identity Provider window opens.
3. If this is the first provider being configured for Forescout, select the Enable External Identity Provider checkbox. Then select Apply. The Forescout platform proceeds to initialize the SSO service. This task can take several minutes to complete, depending on

the number of your deployed Forescout devices. When the initialization completes, the External Identity Provider window displays the remainder of the set-up process.

4. From the External Identity Provider drop-down menu, select the external identify provider you need the eyeSight to work with.
5. If the selected, external identify provider supports the presentation of an application icon, do the following:
    a. Select the Forescout application icon link and download this icon to your local machine.
    b. Upload the Forescout application icon to the <external identity provider>.
6. Select the Forescout metadata file link and download this metadata file to your local machine.
7. Upload the Forescout metadata file to the <external identity provider>. If the <external identity provider> does not allow the upload of the Forescout service provider metadata file (`sp-metadata.xml`), open this file and refer to its content to manually configure SAML information in the <external identity provider>.
8. In the <external identity provider>, create the <external identity provider> metadata file that Forescout web services must use.
9. Select Select File and then select and import the <external identity provider> metadata file to Forescout web services. The contents of the imported, metadata file with the heading <external identity provider> Metadata:display beneath the *Select File* button.
10. Select Apply. The eyeSight updates the SSO service and restarts the Forescout web server. These tasks can take several minutes to complete, depending on the number of your deployed Forescout devices. When the eyeSight setup completes, the Log in with SSO button is activated and appears in the Forescout Web Portal Login page.

    Note:

    Any URL that accesses the Forescout Web Portal Login page must begin with either the same IP address or FQDN, as found in the content of the Forescout service provider metadata file (sp-metadata.xml).

Reset Forescout eyeSight Metadata for an External Identity Provider

Some scenarios require resetting metadata:

- The imported <external identity provider> metadata file (`idp-metadata.xml`) is corrupt

and/or the Log in with SSO button does not appear in the Forescout Web Portal Login page
- You want to renew the Forescout certificate that is provided in the Forescout service provider metadata file (`sp-metadata.xml`)
- Deployment switchover from the Enterprise Manager to the Recovery Manager

The eyeSight provides an `fstool` command that deletes both the imported <external identity provider> metadata file and the Forescout service provider metadata file.

To reset metadata files:

1. Log in to the CLI of the Enterprise Manager.
2. Run the following command: `fstool www sso_config_reset`
3. Re-perform the procedure to set up the provider in Forescout. Although not a requirement, it is a best practice to reset metadata files prior to changing the external identify provider that the eyeSight must work with.

Monitor Forescout eyeSight user activity

You can view user audit trail reports that contain information about user activities during a specified time period. These reports list operations (add, delete, edit) performed by users related to Console configurations, for example:

- Policies
- Stopping or starting the eyeSight
- User passwords
- Plugins and Modules
- Blocked and released users can be viewed in the Events Viewer Log.

Note:
View authentication failure records and reset locked-out users with the user lock command-line interface (CLI) command. Refer to the *Forescout eyeSight CLI Commands Reference Guide* for more information.

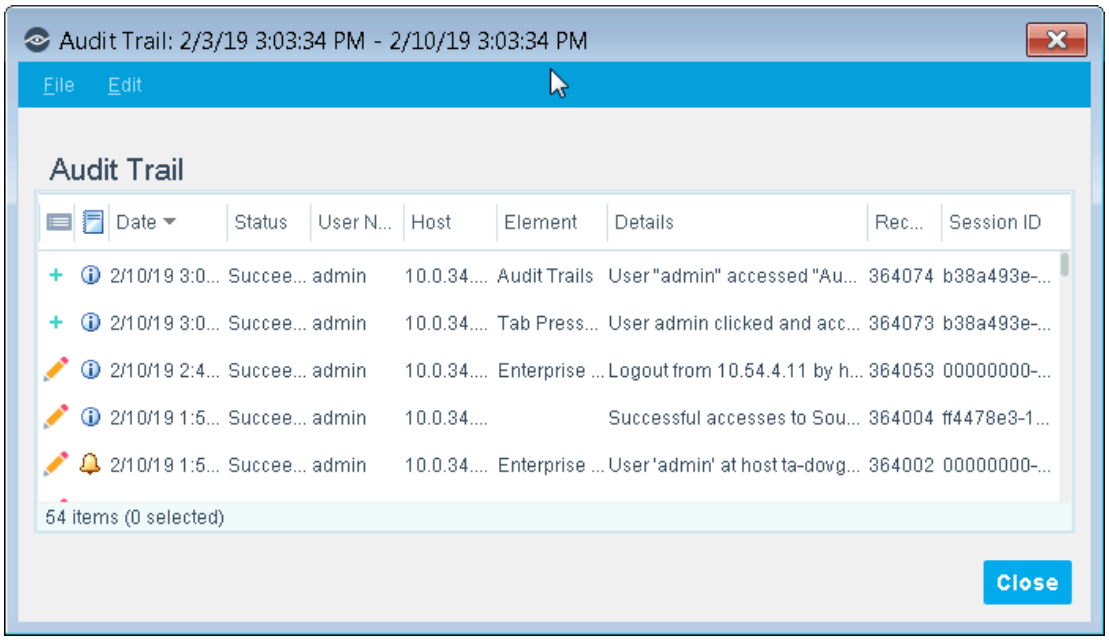
View Forescout eyeSight audit trail reports

To view audit trail reports:

1. In the Console, select Log > Audit Trails .
2. Specify a time period in one of the following ways:

Relative Time	Specify a number of hours, days, weeks, or months.
Time Range	Specify the start and end of a date/time range.

3. Select OK.

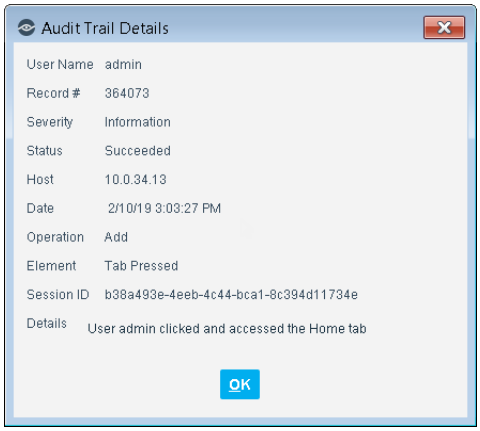


The following information is available:

(Operation)	+ Add
	Edit
	Delete
Severity	Emergency
	Alert
	Critical
	Error
	Warning
	Notice

	Information Debug
Date	The date and time when the operation was made.
Status	Whether the operation succeeded or failed.
User Name	The user who performed the operation.
Host	The IP address of the machine from which the operation was made.
Element	The resource or component the operation was performed upon (for example, users).
Details	The changed information for example, in 'adding a user', the operation data is the added name.
Record #	Unique index number for the log entry.
Session ID	A unique, positive integer value that identifies the Forescout user session associated with the reported event. A null (zero) value indicates an event generated by internal audit processes.

Double-click a line in the table to view more details.



Audit Trail Details Dialog Box

To search the table, select Edit > Find.

To save the log to an external file, select File > Export.

Manage Forescout Licenses

Learn how to manage Forescout licenses, including activation, deactivation, revocation, and conversion from perpetual to subscription.

Overview

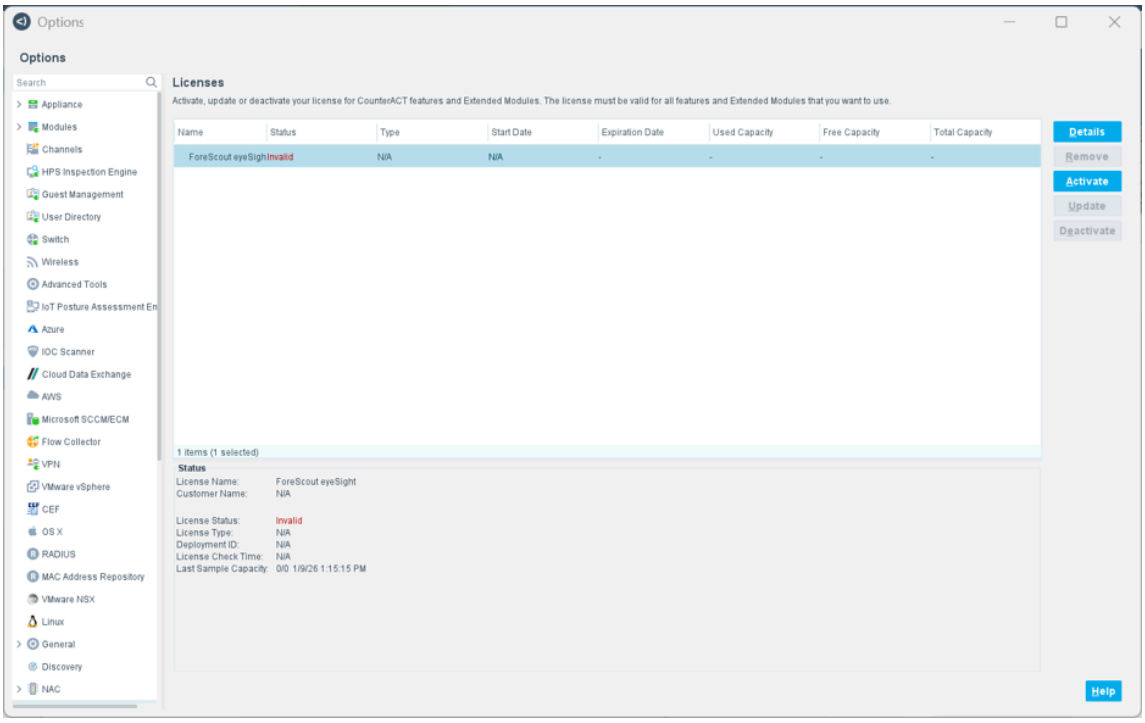
Forescout licenses control access to product features and endpoint capacity. You can manage licenses through the Forescout License Portal and Console.

This section covers:

- Activate a Forescout License: Add and enable licenses for your deployment.
- Update an Existing License File in the Forescout Console: Refresh your license file in the Console after renewal or changes.
- Upload License Requests and Download License Files: Submit a license request and retrieve the updated license file from the portal.
- Deactivate or Revoke a Forescout License: Remove or revoke licenses when they are no longer needed.
- Convert a License: Change a perpetual license to a subscription license.
- Receiving License Alerts: Set up notifications regarding your license expirations.

Important Notes

- You cannot mix perpetual and subscription licenses in the same deployment.
- All products in a deployment must use the same license type.
- License status in the customer portal changes based on your last action. For example, if you deactivate a deployment ID, it stays deactivated until you reactivate it.
- License expiration dates are set by your most recent order transaction, such as a purchase or renewal. These dates don’t change when you take actions in the portal.
- The Forescout Console shows license status and expiration dates from the portal. In the Licenses pane, you can view details such as name, status, type, start and expiration dates, and capacity (used, free, and total).



Related Topics

See the following topics for detailed instructions:

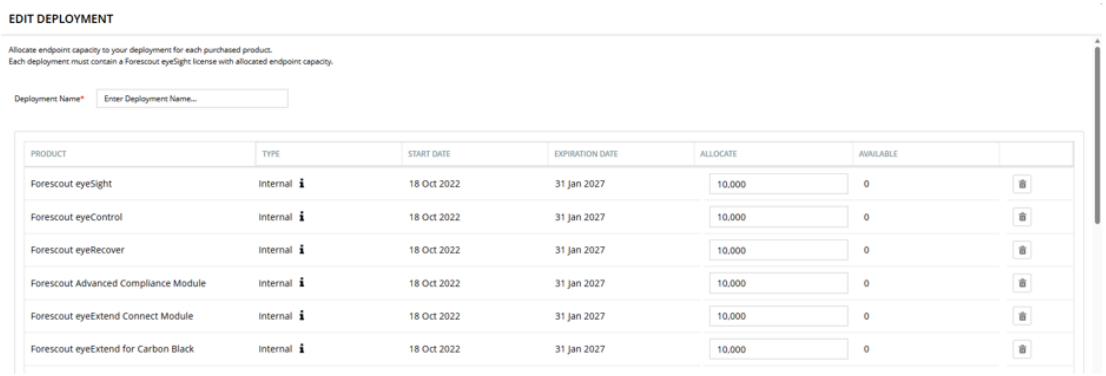
- Activate a Forescout License
- Update an Existing License File in the Forescout Console
- Upload License Requests and Download License Files
- Deactivate or Revoke a Forescout License
- Convert a Perpetual License to a Subscription License

Activate a Forescout License

Activate or update centralized licenses (FLEXX) using the Forescout dashboard and Customer Portal.

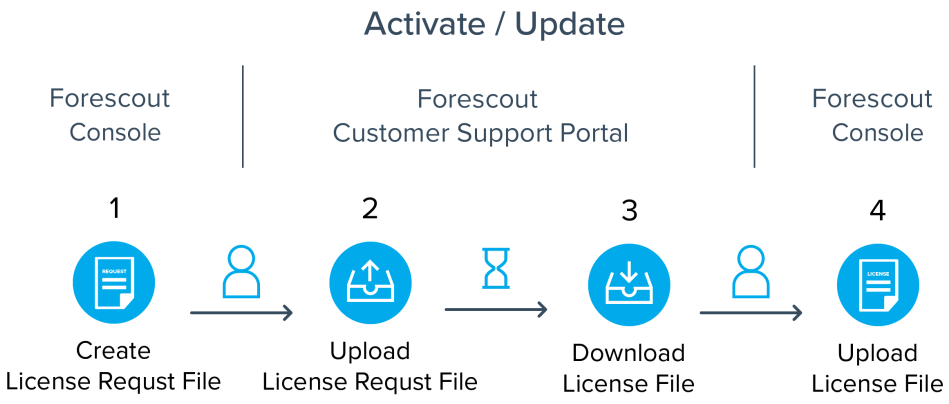
Use this procedure to activate or update centralized licenses (FLEXX) through the Forescout Console and Customer Portal.

1. Log into the Customer Portal at https://www.forescout.com/support/login/.
2. Navigate to the Licenses tab using your Support Portal credentials.
3. Scroll down to Deployments and select an existing Deployment or Add Deployment.



4. Select the EDIT tab, enter a deployment name and seat count, and select Save.
5. Copy the Deployment ID. Keep the Customer Portal open.
6. Log into the Forescout Console and go to Options > Licenses > Activate or Update.
7. Paste the Deployment ID and click Download License Request File. Keep this window open.
8. Return to the Customer Portal on the Licenses tab and scroll to License Management.
9. From the drop-down menu, select I want to: Activate License and select Upload License Request File.
10. Download and save the generated license file (.fsl).
11. Return to the Forescout Console, go to Upload License, click Choose File, and then select Activate License.
12. Wait for the process to finish.
    The system activates or updates the license.

Note:
If you renew your term license, you must perform an update transaction to apply the new dates.



Update an Existing License File in the Forescout Console

Use this procedure to update an existing license file in the Forescout Console after renewing a term license or making changes in the Customer Support Portal.

1. Log in to Enterprise Manager through the Forescout Console.
2. From the Tools menu, select Options > Licenses > Update.
3. In the Update License dialog box, select Download License Request, and then select OK. If

you don't upload the updated license within 14 days, the license becomes invalid.
4. Choose a file name and location for the update request, and select Save.
5. Go to the Forescout Customer Support Portal, and open the Licenses tab.
6. In License Management, upload the request file you saved in step 4, and then download the license file. For details, see Upload License Requests and Download License Files.
7. Return to the Update License dialog box in the Console: Navigate to Options > Licenses, and select Update.
8. In Upload License, select Choose file, find the new license file, and then select Update License. A confirmation dialog box appears when the license is updated successfully.
9. Select Close.

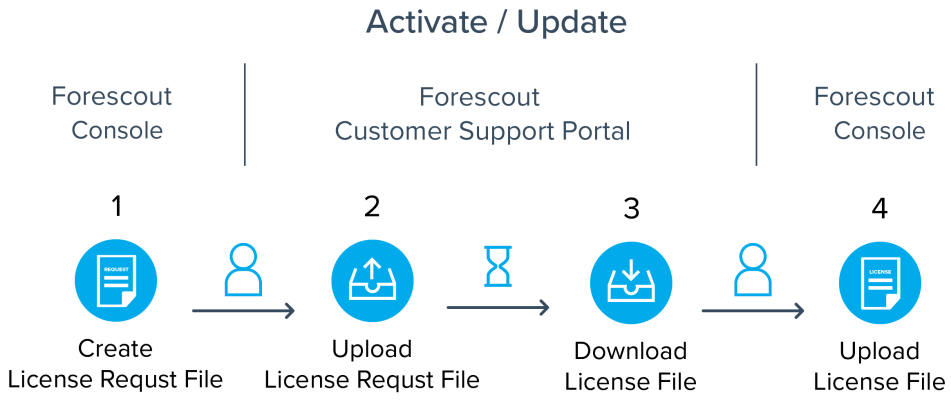
Upload License Requests and Download License Files

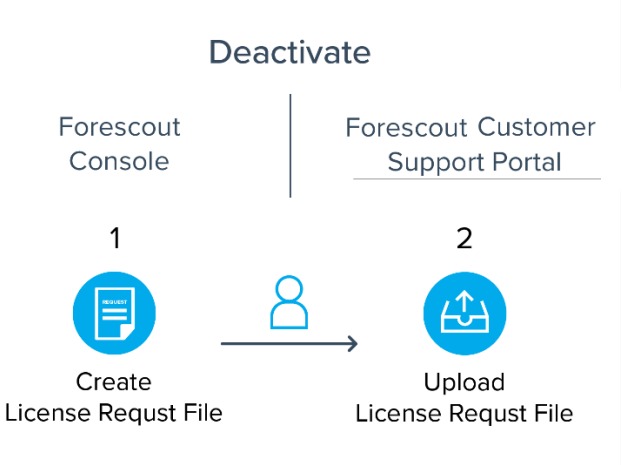
License activities in the Console are performed offline if you have not completed the Customer Verification process during Console login OR if your Enterprise Manager is not connected to the internet when you perform the activity. See Activate a Forescout License, Update an Existing License File in the Forescout Console and Deactivate or Revoke a Forescout License for more information.

To activate, update or deactivate a license, upload the license request file created in the Console to the Forescout Customer Support Portal.

When activating or updating a license file, or when switching to Flexx Licensing, if the upload is successful, the new license file becomes available for download. To complete the activity, upload the license file in the Console.

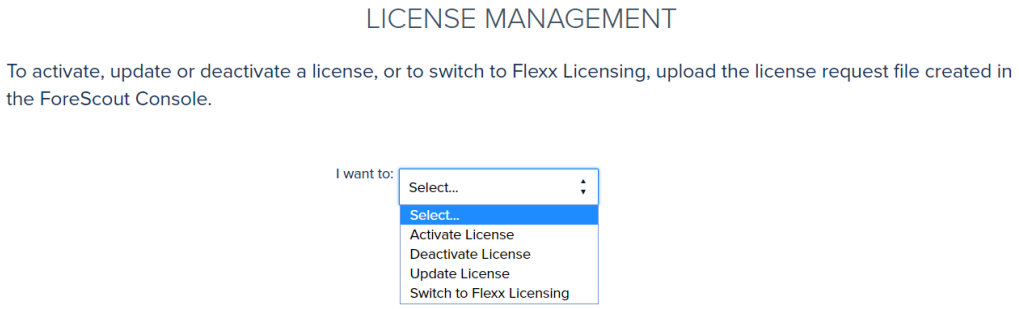
For more information about performing these activities in the Console, see Manage Forescout Licenses.





To upload requests and download license files:

1. Navigate to the Forescout Customer Support Portal and select Licenses.
2. Select License Management.



3. Select the activity you want to perform and follow the on-screen instructions. If you are activating or updating the license, or switching to Flexx licensing, and the upload succeeded, the download file will be available. After you successfully upload the request file, the latest license file will be available for future use next to the relevant deployment entry.

   Note:

   For license activation: After you upload the license request file in the Customer Support Portal, the generated license file will be locked to the machine you downloaded the request from. If you try to activate a license on another machine using an already locked Deployment ID, activation will fail. You must first Deactivate the License File.

   To access the license file in a deployment where files cannot be taken out of the internal network:

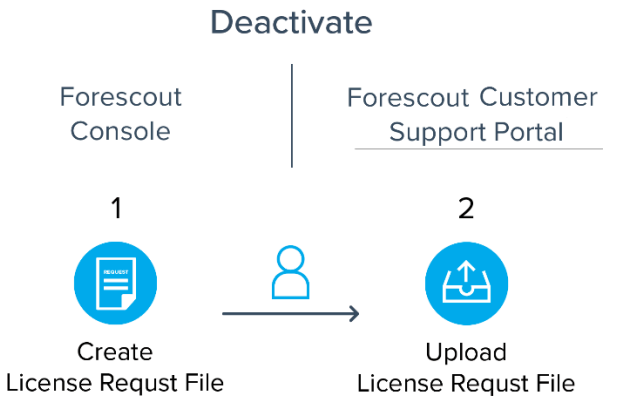
4. Open the license request file and copy its contents to an email.
5. Send the license request content to your Forescout representative who will generate and send back a license file using the request you sent.

Deactivate or Revoke a Forescout License

Deactivate Flexx licenses and reset license allocations using the Forescout Console and Customer Portal.

Use this procedure to revoke Flexx licenses and make allocations available for reuse. This includes deactivation of a permanent license previously applied to an eyeSight appliance.

1. Log in to the Forescout Console.
2. To view the deployment licenses, go to Options > Licenses.
3. Select Deactivate.
   This action deactivates the entire license deployment. You cannot selectively or partially deactivate licenses within the deployment.
4. In the dialog box, select Save to save the revocation request file to your local machine.
5. Log in to the Customer Portal at https://www.forescout.com/support/login/ using your Support Portal credentials.
6. Navigate to the Licenses tab and upload the saved revocation request file in the License Management section.
7. The system revokes the license and makes all allocations available for reallocation after you upload the file.



Convert a Perpetual License to a Subscription License

Convert an existing perpetual license to a subscription (term) license using the Forescout License Portal and Console.

Use this procedure to convert a perpetual license to a subscription license using the License Portal and Console.

1. Log in to the Forescout Customer Support Portal.
2. Navigate to Licenses > Deployments.
3. Locate and open the deployment that uses a perpetual license.
   Note:
   If the perpetual license is active, deactivate it in the Console before you can change the allocation.
4. Open the Console and go to Tools > Options > Licenses.
5. Select Deactivate, save the deactivation request file, and upload it to the License Portal under License Management.
6. Edit the deployment in the License Portal.
7. Add subscription license products, allocate the desired endpoint capacity, reduce the allocation of perpetual licenses to zero, and save.
8. Activate the subscription license in the Console.
9. Go to Options > Licenses > Activate, enter your Deployment ID, download the license request file, upload it in the License Portal, download the generated license file, and upload

it in the Console.

10. Validate the change.
11. Confirm the perpetual license is inactive, subscription licenses show as Active, endpoint counts are correct, and no licensing warnings appear.

Important:
You cannot mix perpetual and subscription licenses within the same deployment.

Important:
All products in a deployment must match the base license type.

Note:
If you switch from a perpetual license to a subscription license, you can revert to the perpetual license after the subscription expires or is deactivated, as long as the perpetual license status remains Active.

Note:
You can use your original perpetual license on a different deployment. Under standard policy, the perpetual license status remains Active, even if you switch to a subscription license.

The Deployment ID locks to the machine after activation.

For assistance, contact Forescout Customer Support.

Receiving license alerts

Forescout license alerts provide information about the status of your installed licenses, for example, if the license is about to expire or if you have added endpoints and exceed your license capacity.

You receive alerts if there are issues regarding your licenses. Alerts are displayed through:

- Periodic email reminders
  Note:
  You can sign these emails using a digital certificate, as specified by the Secure/ Multipurpose Internet Mail Extensions (S/MIME) standard. See Signing Emails with an S/MIME Certificate for details.
- Pop-up reminders at the Console
- An icon and tooltip on the Console status bar. The triangle is green if you are waiting for license approval and is red if there is a license violation.

Manage Appliances, Enterprise Managers, and Consoles

This topic describes the features available for managing eyeSight devices (Appliances and Enterprise Managers) and Consoles.

Note:
Not all Console users have access to these tools. For more information see Access to Console Tools – On-premises Permissions .

Device Management Overview

When an Appliance registers with an Enterprise Manager, most of the following Appliance settings are automatically replaced with Enterprise Manager settings. Any subsequent changes to these settings on the Enterprise Manager are automatically applied to all registered Appliances.

General	NAC	Plugins	Threat Protection
Internal Network Host Discovery Virtual Firewall Backup Settings Segments IP Assignments (centrally managed at Enterprise Manager but applied per Appliance)	Policies Preferences Group Configuration Settings	Plugin settings for Switch and VPN	Mark Names Enterprise Lockdown Virtual Site Legitimate Traffic Rules Legitimate Email Server Rules

The following settings are applied by default but may be fine-tuned per Appliance.

General	Threat Protection	Plugins
Mail Settings Assets Portal access control	Enforcement Mode Threat Protection policy Active Response network	HPS Inspection Engine

The following settings are unique per Appliance and are not affected by Enterprise Manager settings.

- Channel configuration
- License management (Per-Appliance Licensing only)

- Appliance upgrade

Forescout Console and Web Portal Management

This topic describes Console and web portal management options.

Configure NTP Server Synchronization

Forescout devices require connectivity to an NTP server on port 123 UDP. Select Tools > Options > General > Time and configure the NTP settings.

Enable sync with NTP server	Select this option to enable system clock synchronization with an NTP time server, and show additional NTP controls.

The table displays NTP servers defined in the Console.

To add an NTP server, select Add and provide the following information.

NTP Server	The hostname of the server, which can be the FQDN, or an IPv4/IPv6 address.
Key	(Optional, but recommended) The SHA-1 key string used for authentication of the NTP server connection
ID	A text label that identifies the server.

eyeSight Device Management

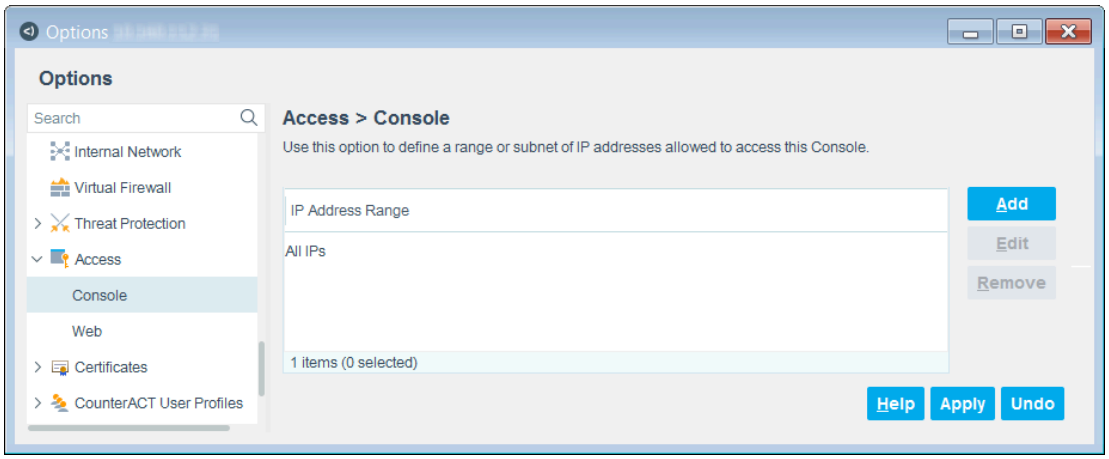
The Enterprise Manager is a dedicated, second-tier management and aggregation device that communicates with multiple Appliances distributed across the network. It manages Appliances, and collects information detected by them. This information is available for display and reporting in the Console.

Define Console Access

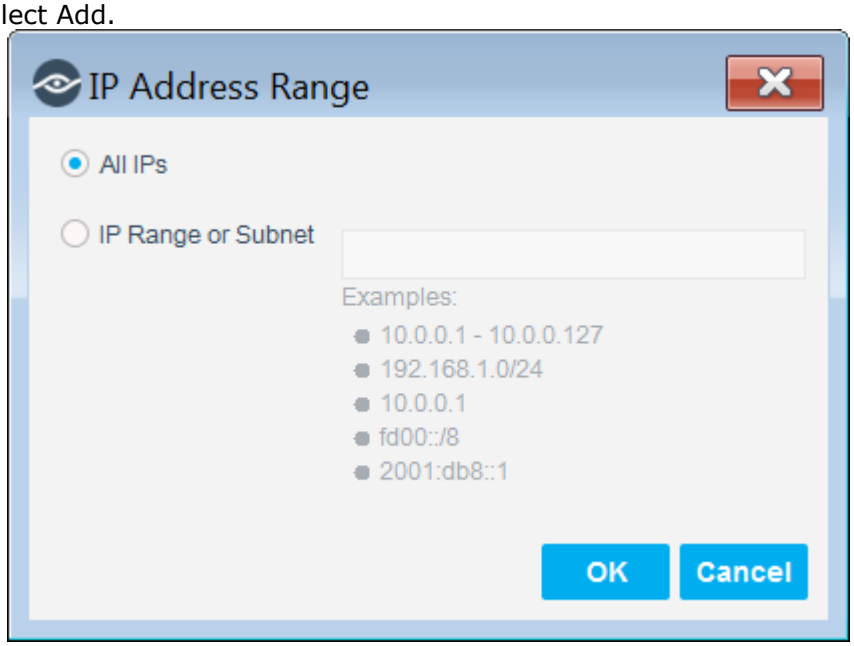
By default, all IP addresses have access to the Console. You can limit the IP addresses that can access the Console.

To manage Console access:

1. Select Tools > Options, and then select Access > Console. The Ranges table lists all IP addresses that are permitted to communicate with this Console.



2. (Optional) Create a configuration for a group of Appliances or select a configuration to modify. See Configure Features for an Appliance or Group of Appliances.
3. Select Add.



4. Enter an address range or subnet, and then select OK. The new range is added to the Ranges table.
5. To modify or delete an existing range of IP addresses, select it in the table and then select Edit or Remove.
6. Select Apply.

Multiple Console Logins

When more than one user logs in to a single instance of the Console, changes made by one user may overwrite changes of another user. Shared settings and files may be overwritten or corrupted when users work in this way, therefore it is not recommended for multiple users to log in to the same instance of the Console.

To support multiple users from a single endpoint, install a separate, uniquely named instance of the Console for each user.

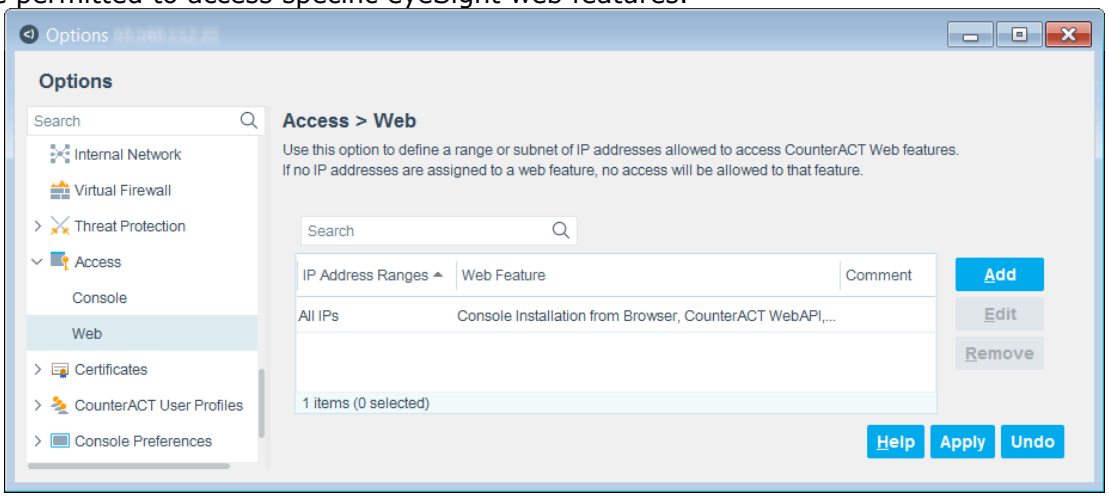
Define Web Access

You can define a range or subnet of IP addresses allowed to access specific Forescout web features, such as eyeSight web portals, the eyeSight Compliance Center and the eyeSight SecureConnector Distribution Tool. If you do not assign any IP addresses to a web feature, no access will be allowed to that feature.

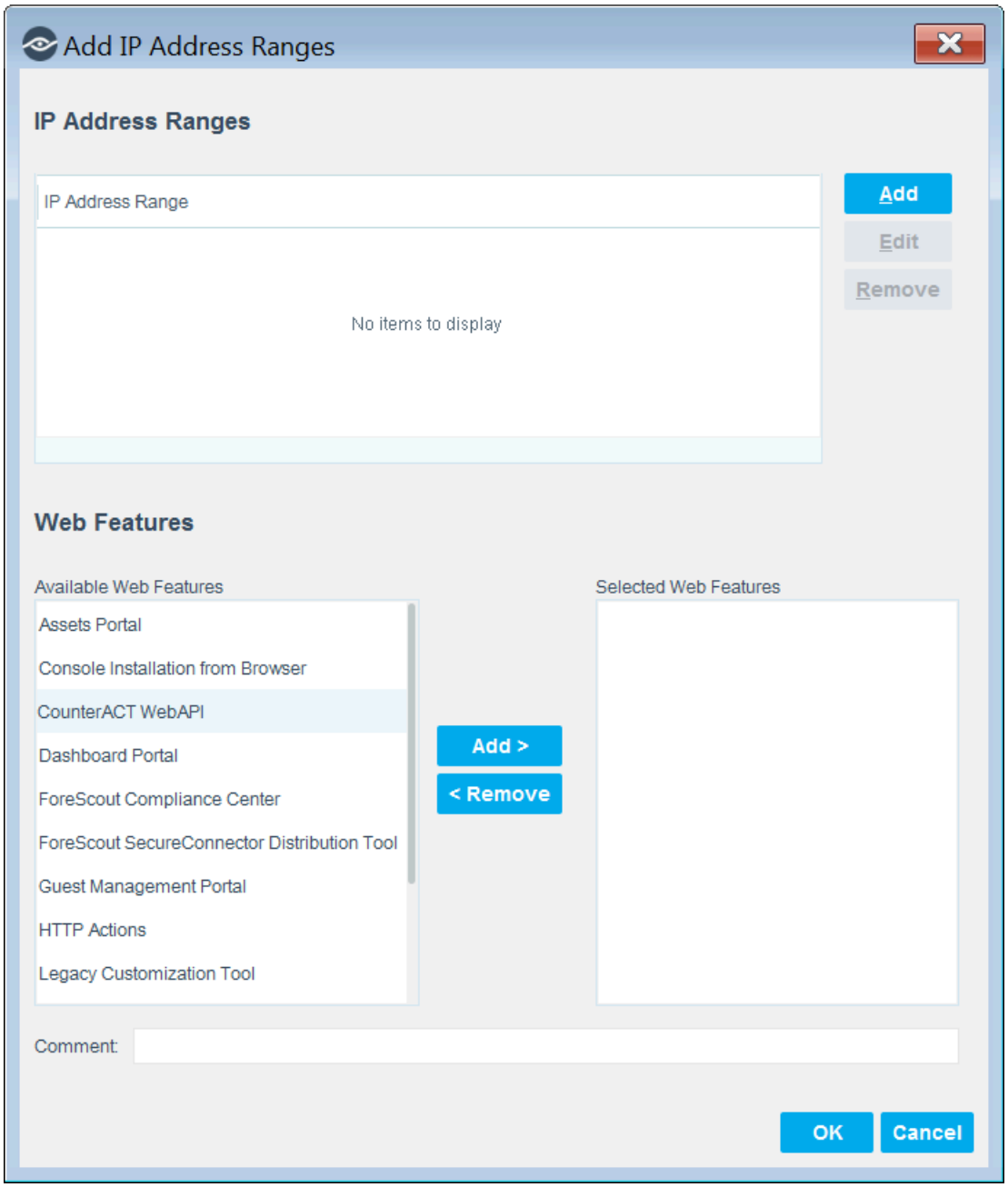
Note:
Grant web access only to IP addresses that are included in the Internal Network.

To define web access IP ranges:

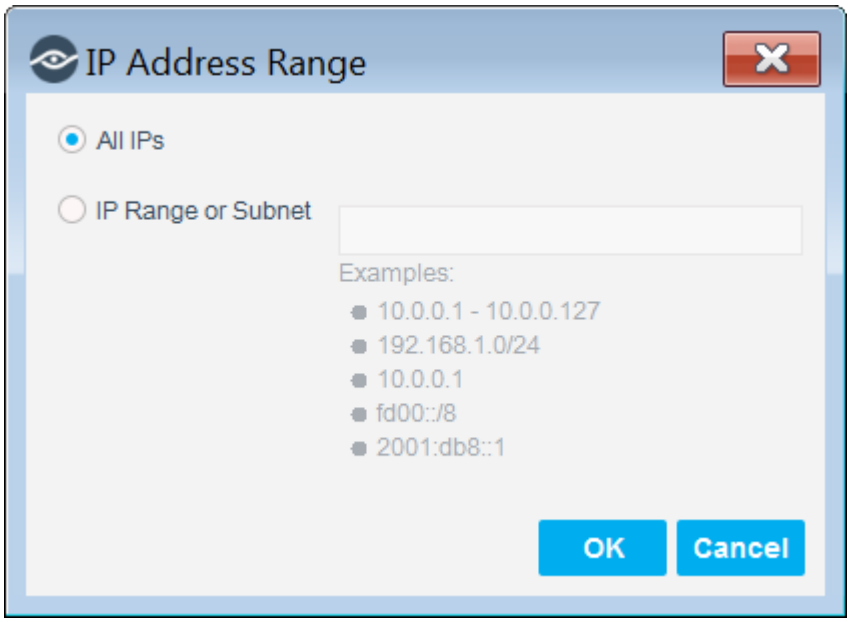
1. Select Tools > Options, and then select Access > Web. The table lists all IP addresses that are permitted to access specific eyeSight web features.



2. (Optional) Create a configuration for a group of Appliances or select a configuration to modify. See Configure Features for an Appliance or Group of Appliances.
3. Select Add to define an IP address range and the web features that range can access.



4. In the IP Address Ranges section, select Add.



5. Select All IPs to include all IP addresses in the Internal Network or enter a specific IP address range or subnet and then select OK.
6. In the Web Features section, select from the available list of web features and then select Add.
7. (Optional) Enter a comment.
8. Select OK. The IP address range and web feature/s are added to the table.
9. To modify or delete an existing range of IP addresses, select it in the table and then select Edit or Remove.
10. Select Apply.

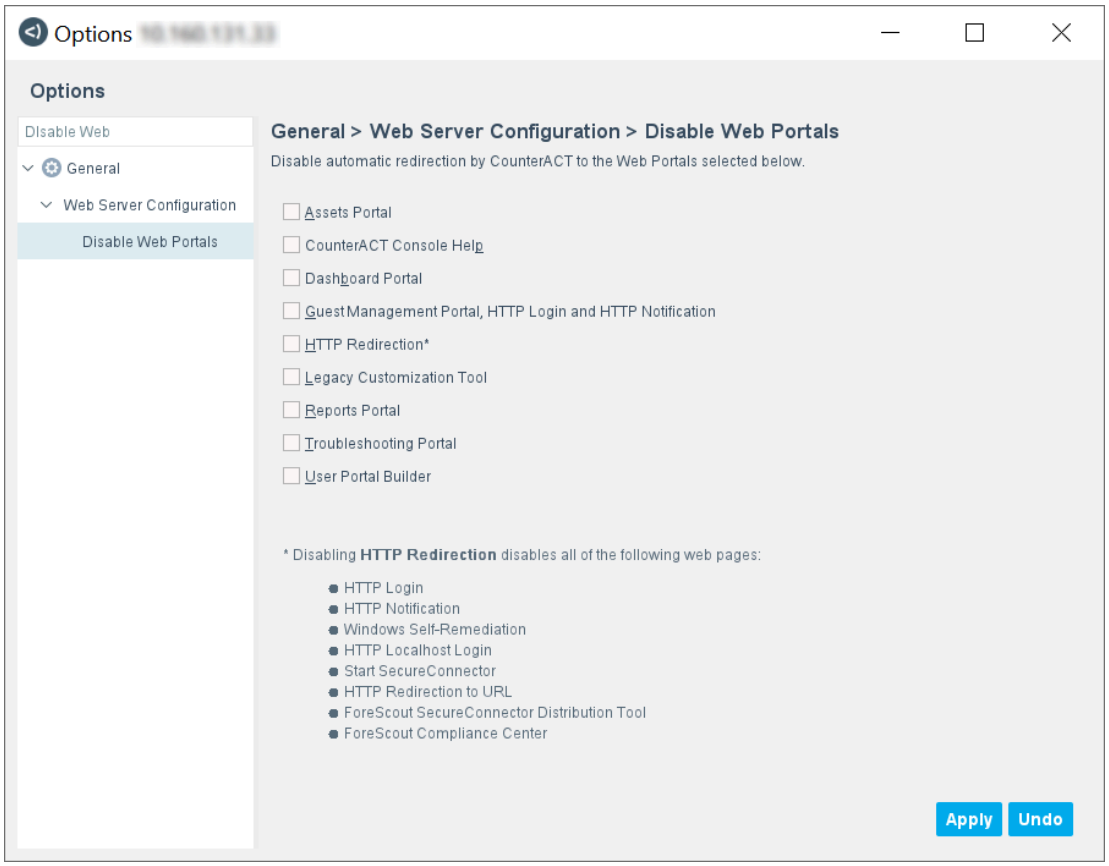
Disable Web Portals

Under some security scenarios, you may need to disable web access to one or more portals or web-based services, or to disable HTTP redirection.

Use the Disable Web Portals pane to disable automatic redirection by eyeSight eyeControl to web portals and web pages.

To disable a web portal or page:

1. Select Tools > Options, and then select General > Web Server Configuration > Disable Web Portals



2. Select one or more of the following options: HTTP Login
    - Assets Portal
    - Guest Management Portal, HTTP Login and HTTP Notification
    - Reports Portal
    - Console Help
    - Troubleshooting Portal
    - Dashboard Portal
    - Legacy Customization Tool
    - User Portal Builder
    - HTTP Redirection. Disabling HTTP Redirection also disables the following actions and web pages:
        - HTTP Notification
        - HTTP Login
        - Windows Self-Remediation
        - HTTP Localhost Login
        - Start SecureConnector
        - HTTP Redirection to URL
        - eyeSight SecureConnector Distribution Tool
        - eyeSight Compliance Center
3. Select Apply.

Configure Console Preferences

This topic describes Console preference options available under Tools > Options > Console Preferences.

Configure the Time Zone

Select Tools > Options > Console Preferences > Time Zone, and configure time zone.

At time zone	The time-zone used to display and record detection and action times in the Console.

Configure HTTP Proxy Settings

Select Tools > Options > Console Preferences > HTTP Proxy, and configure the settings.

Use HTTP proxy	Enable this option to use an HTTP proxy for Internet communication.
HTTP proxy host	The hostname of the proxy server
HTTP proxy port	The port used for communication with the proxy server.

Configure Console Memory Settings

Under certain circumstances, when event traffic information is loaded, an error message may appear stating that there was not enough memory available to accommodate the process. Select Tools > Options > Console Preferences > Console Memory to change the available memory.

Maximum Memory	The maximum size of the Console's Java Virtual Machine memory allocation pool, in megabytes.

Customize Alarm Indicators

An alarm flashes in the Console status bar when a specific type of malicious event occurs. To customize the alarm, select Tools > Options > Console Preferences > Misc. Select the Alarms and configure the settings.

Visual	Select this option to enable a flashing malicious event alarm icon on the Console display.
Audio	Select this option to play a sound signal for a malicious event alarm.
Alarm span	Specify the duration of the alarm.

Configure Console View Settings

Select Tools > Options > Console Preferences > Misc. Select the View tab, and configure the settings.

Fit table columns to view	Columns are resized to fit the window.
Display IPv4 CIDR	Determines whether ranges of IPv4 addresses are shown using CIDR subnet/mask notation or using start-end range notation.

Configure the Network Traffic Boundaries

The Console system tray hosts the network traffic gauge. The gauge reflects the eyeSight view of your current, network traffic load, using traffic boundaries that you can configure. Select Tools > Options > Console Preferences > Misc.Select the Network Traffic Gauge tab, and configure the settings

Low Traffic: Upper Boundary (Mbps)	
	Medium Traffic: Upper Boundary (Mbps)

Configure Additional NTP Servers (CLI)

Use a CLI (`fstool`) command to define additional NTP servers and also different NTP servers for individual Appliances.

Note:
Per Appliance configuration is in effect only until a restart of the Enterprise Manager or the Appliance service. If you need these settings to be in effect after an Enterprise Manager restart or a Appliance service restart, you must configure them again (run the `fstool` command) in each Appliance that restarted.

To define additional or per Appliance NTP servers:

1. Log in to the CLI of the Appliance.
2. Run the following command: `fstool ntp setup <server IP>@<key idx>@<authentication key>`

   where:

   - `<server IP>` is either the IPv4 address, the IPv6 address or the FQDN of the NTP server you prefer (local or remote)
   - `<key idx>` is the key identification index
   - `<authentication key>` is the SHA-1 key string used for authentication of the

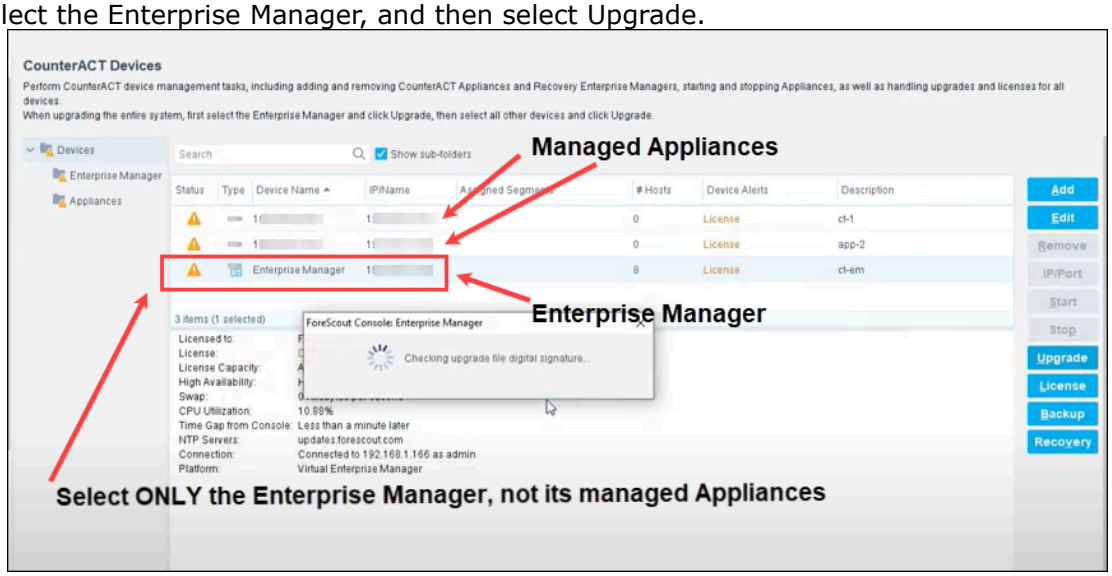
NTP server connection.

The Appliance/Forescout platform then uses this NTP server for time synchronization.

Upgrade the Enterprise Manager

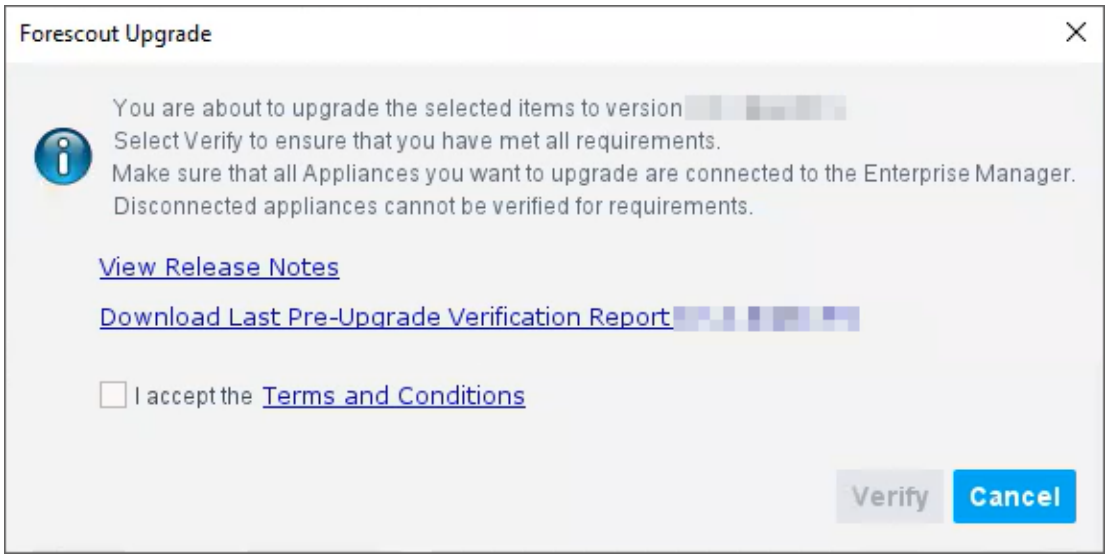
To upgrade the enterprise manager:

1. Download the upgrade file and save it to a location on your computer.
2. Select Tools > Options, and if necessary, select CounterACT Devices. The installed devices and their current versions are displayed.
3. Select the Enterprise Manager, and then select Upgrade.



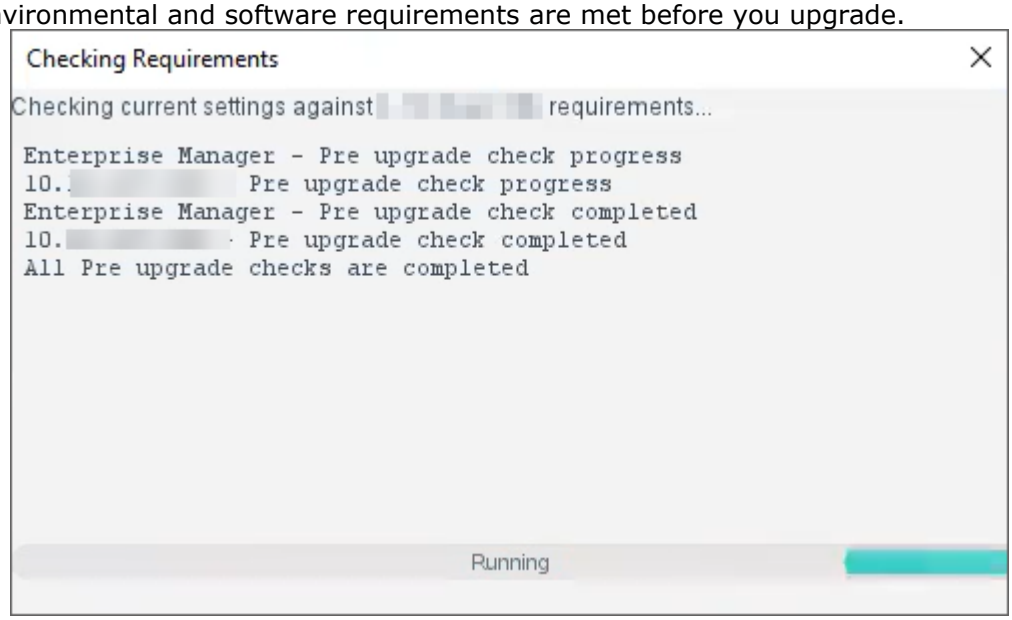
Note:
Select ONLY the Enterprise Manager, not its managed Appliances. Upgrades do not propagate automatically from an Enterprise Manager to its managed Appliances. Later on, you can upgrade the managed Appliances. See Upgrade One or More Appliances.

4. Locate the upgrade file you saved on your computer (using the Browse button), and select OK. After a check of the digital signature of the file is performed, the Forescout Upgrade screen appears.



Note:
If this is NOT the first time you are attempting to install this specific upgrade package, you can view the report from the previous attempt by clicking on the Download.... link provided. The report is named PreUpgradeVerifierLastReport.txt (by default), and you can save it in a folder of your choice.

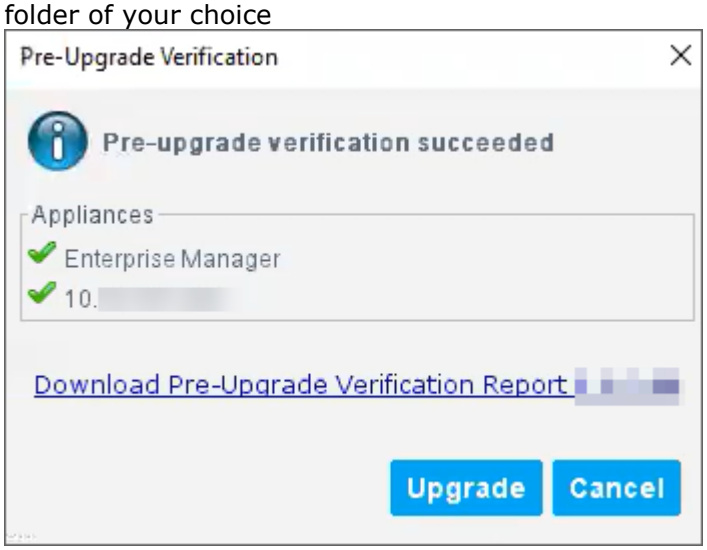
5. Read the terms and conditions, and then select I accept the Terms and Conditions. It is also recommended to read the Release Notes.
6. Select Verify. The pre-upgrade verification process is initiated to ensure that the environmental and software requirements are met before you upgrade.



Note:
The upgrade check also verifies attached Appliances. Later on, when you upgrade an Appliance managed by an already-upgraded Enterprise Manager to the new eyeSight version, the Verify button will not appear when you prepare to upgrade, and the Upgrade button will immediately be available in the CounterACT Upgrade screen.

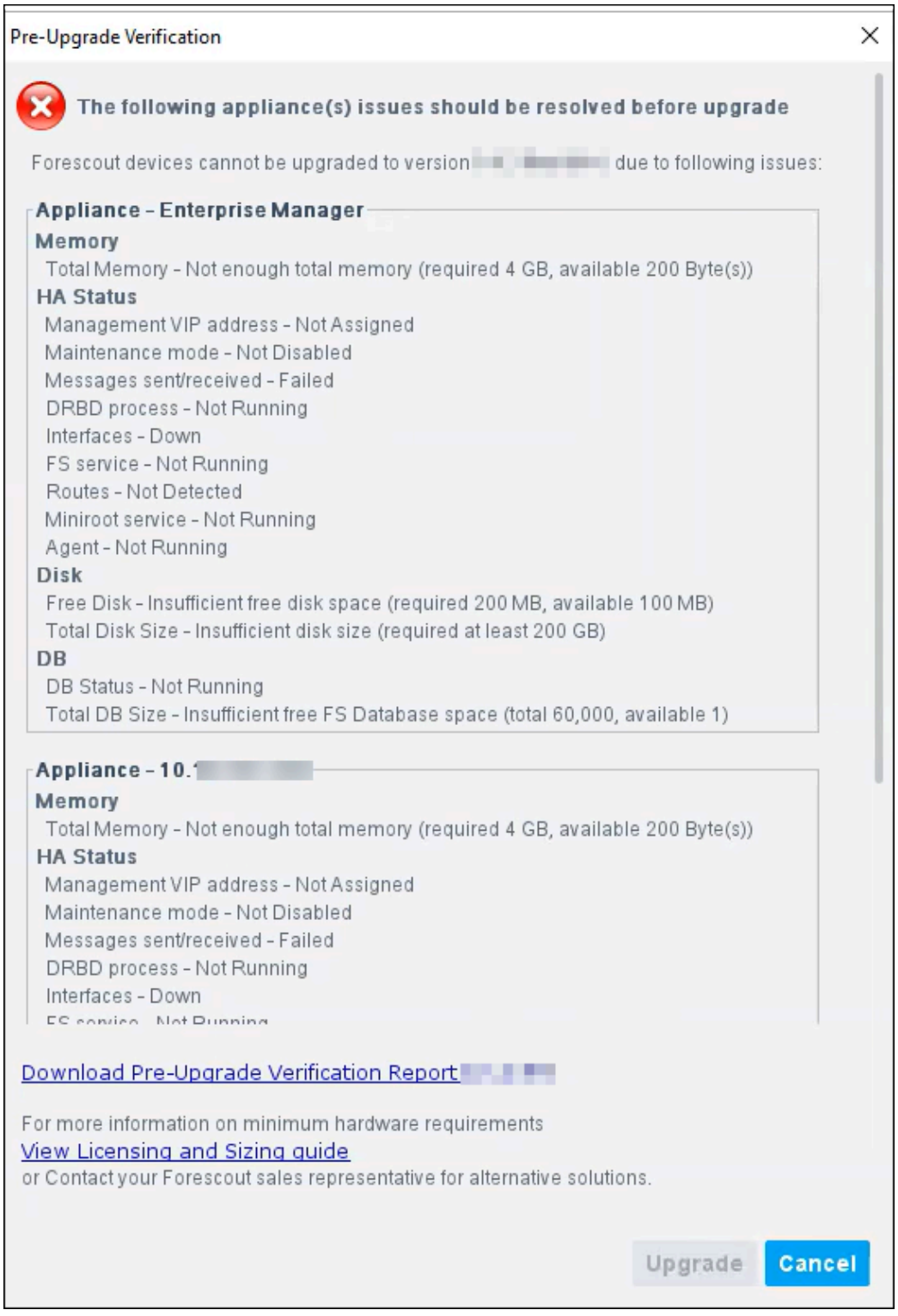
7. When the pre-upgrade verification process completes, the Pre-Upgrade Verification screen appears
   - if the pre-upgrade verification was successful (as shown below), you can optionally download the generated Pre-Upgrade Verification Report by clicking on the

Download... link provided in the screen. The report is named `PreUpgradeVerifierCurrentReport.txt` (by default), and you can save it in a folder of your choice



Or

- If the pre-upgrade verification was not successful (as shown below), the Upgrade button is disabled, and you can view the error report in the Console screen, which shows issues that need to be resolved before upgrading. You can optionally download this report by clicking on the Download... link provided. The report is named `PreUpgradeVerifierCurrentReport.txt` (by default), and you can save it in a folder of your choice.

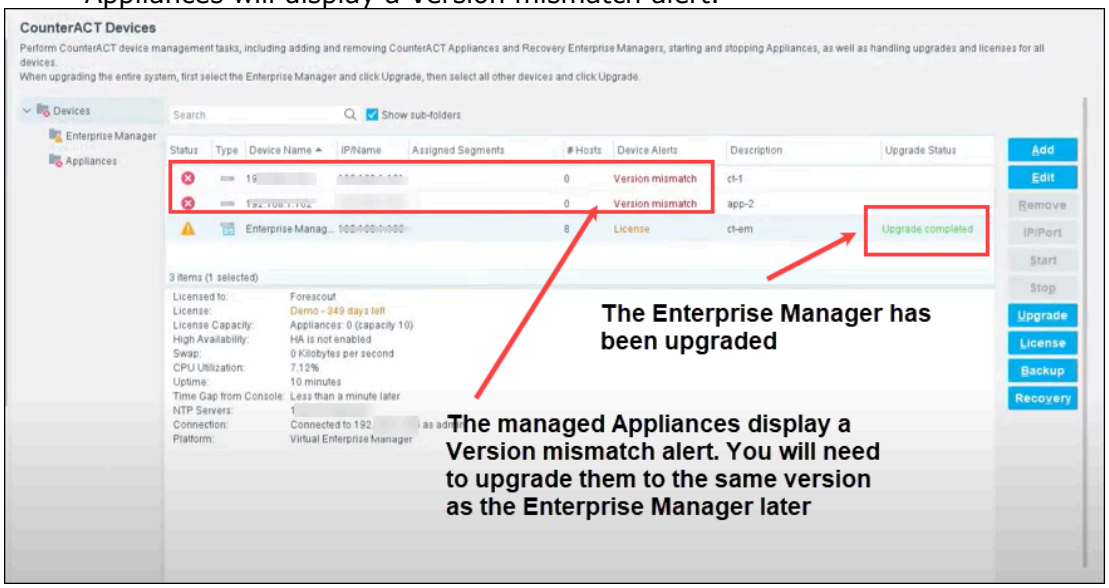


Note:
See Pre-Upgrade Verifier, which includes a table of Pre-Upgrade Verifier result scenarios with details of what to do in each case.

8. When you are ready to proceed with the upgrade, select Upgrade . Once you confirm, the upgrade process proceeds to completion and cannot be interrupted or canceled.
9. When the upgrade is completed successfully, select Close. If the upgrade is not successful, contact your Forescout representative and do not continue with more upgrades.

The Forescout Upgrade dialog box shows the status of the upgrade process and displays any error messages for the process.

Note:
When the upgrade of the Enterprise Manager is complete, note that any managed Appliances will display a Version mismatch alert.



10. After the upgrade is complete, download the Console and install it.

Note:
If the upgrade of the second node and the synchronization are not shown in the log, you can verify the status via icons on the Console status bar:

Icon	Description
	Indicates the status of the High Availability Appliances connected to the Enterprise Manager.
	Indicates the status of the Enterprise Manager High Availability pair.
	Indicates that High Availability is down on the Appliance.
	Indicates that High Availability is down on the Enterprise Manager.

Refer to the Forescout eyeSight Upgrade Guide for complete details.

Upgrade the Console

During an Enterprise Manager upgrade, Consoles that are connected to the Enterprise Manager lose their connection. When the upgrade is available, you are informed that your Console software needs to be automatically updated.

To update the Console software:

1. When prompted to perform a Console update, select Yes. If you select No, the application automatically closes. The update process consists of two stages.
    a. The software is downloaded. A dialog box shows the download progress.
    b. The software is upgraded. The Software Installation progress window opens, showing the installation progress.
2. When the upgrade completes select Launch Console at the bottom of the window to return to the Forescout Login dialog box.

Stop and Start the Enterprise Manager

You cannot start and stop the Enterprise Manager from the Console. It is possible, however, to halt Enterprise Manager communication with Appliances. This is done using the `fstool` utility..

To control communication, log in to the Enterprise Manager CLI and submit the following command:

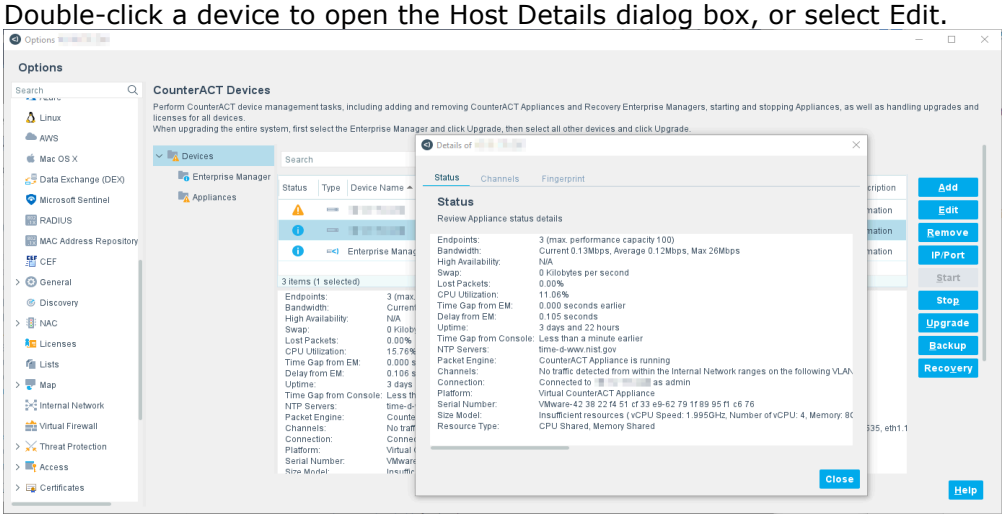
```
fstool service start|stop|restart|status|shutdown
```

View Forescout Device System Health Information

View at-a-glance system health information about your Forescout devices. This feature can be also used for troubleshooting.

Select Tools > Options > CounterACT Devices. The CounterACT Devices pane lists installed Enterprise Managers and Appliances. To view details:

- Select a device in the table. Details appear in the pane below the table.
- Hover over the Status icon of a device.
- Double-click a device to open the Host Details dialog box, or select Edit.



Items in red may require your attention.

The fields displayed are different for Enterprise Manager and Appliances, and can vary depending on your Forescout deployment, for example, the licensing mode you are using, or whether you are using a virtual machine.

Action Threshold	Indicates that actions are on-hold on the device. This happens when endpoints exceed the action threshold defined for the device. Action thresholds are designed to automatically implement safeguards when using restrictive actions. See Working with Action Thresholds for details.
Bandwidth	Statistical information on bandwidth usage.
Channels	Indicates whether Channel connections are working properly.
Connection	Information about the connection between Forescout components. For example: Enterprise Manager is connected to a Console. Appliance is running a release that does not match Enterprise Manager.
CPU Utilization	Indicates the percentage of actual CPU Utilization. If the value is high, contact your Forescout representative.
Delay from EM	Indicates whether the communication delay between the Enterprise Manager and an Appliance is more than one minute. If this happens, contact your Forescout representative.
High Availability	High Availability system status information: ◦ N/A: No High Availability system is installed. ◦ UP: High Availability is installed and running. Both nodes are up and synchronized. ◦ Not supported: Versions are incompatible. ◦ Degraded: Review the tooltip for details about why the High Availability system was degraded.
License	License type, validity, and the time to expiration, if applicable.
License Capacity	Bandwidth and endpoint assignment capacity violations. See for details.
License Request	License request details.
Lost Packets	Indicates whether the Appliance packet engine lost on an average

	more than a 10% packet loss in the last one minute. Packet loss is displayed in 10% accuracy, i.e., 0% is 0-10, 10% is 10-20, and so on. The string O.K. is displayed if the packet loss is less than 10%. When packet loss is more than 10%, HTTP Redirection and Virtual Firewall may not work consistently. For the same source and destination, they might work in some cases and fail in others. To resolve, upgrade the Appliance or configure the channels to monitor less traffic.
NTP	The NTP server connection status and server IP address.
Packet Engine	The status of the Forescout Packet Engine: this is the engine that runs the Appliance. If this is down, many Forescout features will not work.
Swap	Indicates whether the swap exceeded 100 kilobytes per second consecutively in the last minute, i.e., swap polling exceeded 100 on each of the polls (1 every five seconds). When this happens, the system may work slowly. To resolve this issue, add physical memory to the Appliance or replace the current Appliance with a new Appliance that has more physical memory.
Time Gap from Console	Indicates the time delay between the Console and the Enterprise Manager.
Time Gap from Console	The time delay between the Console and the Appliance.
	Time Gap from EM Indicates whether the time set in the Enterprise Manager and at an Appliance varies by more than five minutes. When this happens, the event time may be incorrectly displayed in the Console. To resolve this, the Appliance or the Enterprise Manager clock should be reset.
Uptime	Indicates the amount of time the device has been running.

Appliance Capacity

A Forescout Appliance has an hardware-based endpoint performance capacity and a license-based endpoint capacity.

Appliance Endpoint Performance Capacity

Each Appliance has a set number of allotted endpoints. This number is set automatically based on default values assigned to the hardware model of your Appliance. Limiting the number of endpoints per Appliance enables Forescout products to perform more effectively.

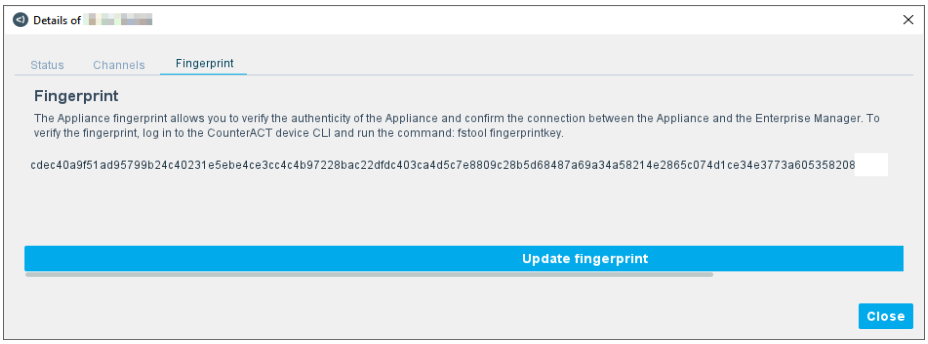
When the number of endpoints is exceeded, warnings are issued in the Appliance and Enterprise Manager Consoles, and in trace log files.

License Endpoint Capacity

In addition to endpoint performance capacity, Forescout licenses also have a license endpoint capacity which defines how many endpoints your deployment is allowed to handle.

Verify the Appliance Fingerprint

The Appliance fingerprint lets you verify the authenticity of the Appliance and confirm the connection between the Appliance and the Enterprise Manager. Compare the displayed fingerprint with the fingerprint retrieved from the device to verify.



To verify the fingerprint:

1. Log in to the CounterACT device CLI.
2. Run the following command: `fingerprintkey`

   Note:

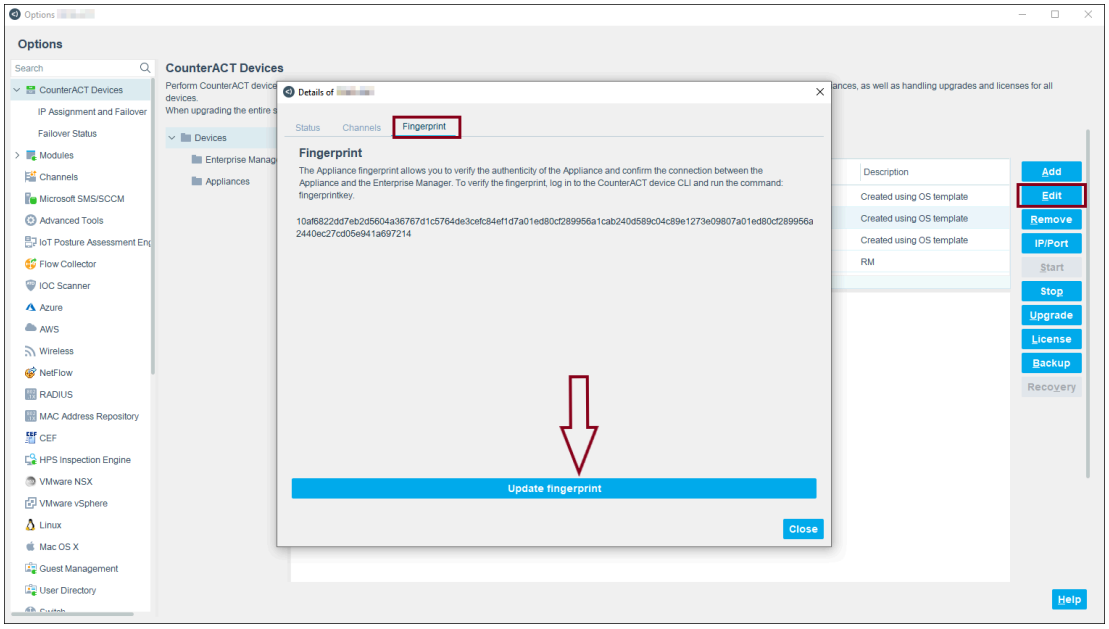
   In the Bash shell, run `fstool key` instead. Refer to the *Forescout eyeSight CLI Commands Reference Guide* for more information.
3. Verify that the output of the command matches the value displayed in the Fingerprint tab.

Update the Appliance Fingerprint

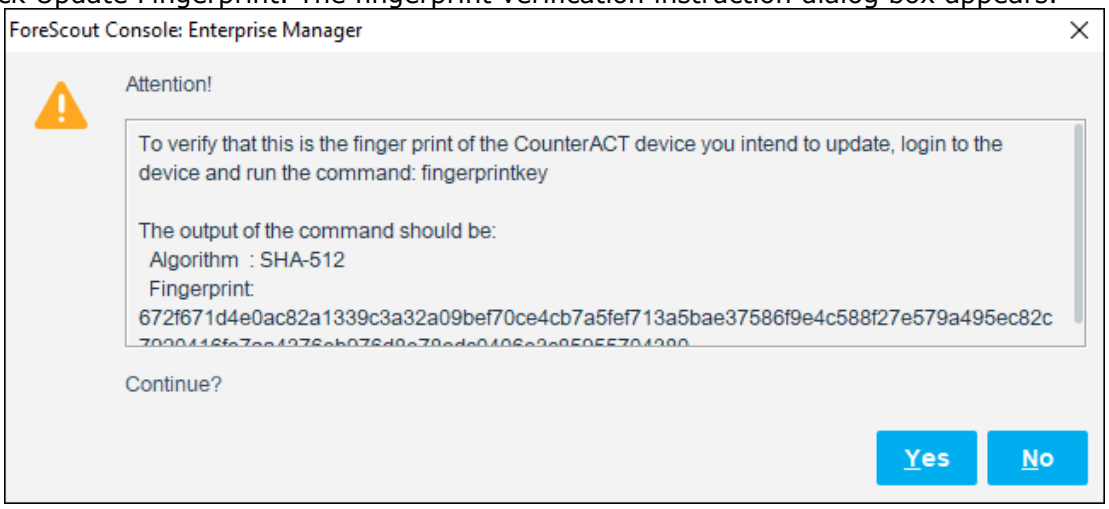
After replacing a certificate, you must update the Appliance fingerprint with this procedure.

To update the fingerprint:

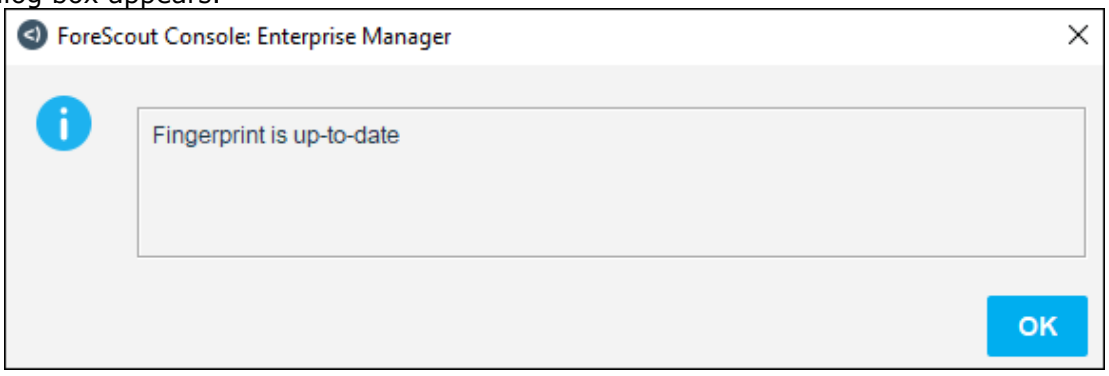
1. Select Tools > Options.
2. Select an Appliance or Recovery Enterprise Manager from the CounterACT Devices pane.



3. Click Edit.
4. Select the Fingerprint tab.
5. Click Update Fingerprint. The fingerprint verification instruction dialog box appears.



6. If the fingerprint has not be verified, follow the instructions, and click Yes. A confirmation dialog box appears.



7. Click OK.

Register Appliances with the Enterprise Manager

Your system is installed to begin working with minimal user intervention. However, the tools provided for managing Appliances through the Enterprise Manager are only available when you register your Appliances with the Enterprise Manager.

Your system is installed to begin working with minimal user intervention. However, the tools provided for managing Appliances through the Enterprise Manager are only available when you register your Appliances with the Enterprise Manager.

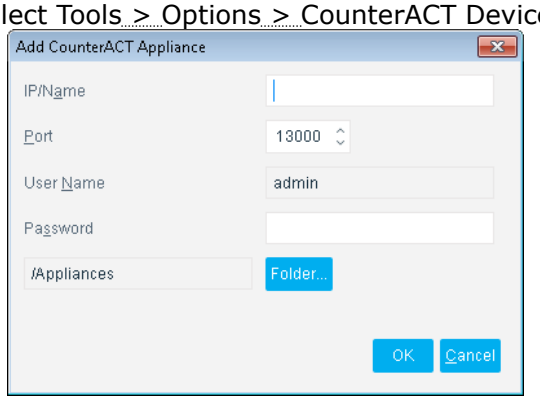
Appliances may have been added via the Initial Setup Wizard. If necessary, you can add additional Appliances. Verify that the Appliance is operating as a Standalone Appliance and is not connected to any other Enterprise Manager before you add the Appliance.

You cannot add an Appliance running eyeSight version 7 or below to an Enterprise Manager running eyeSight version 8 or above.

You must have a valid Forescout license installed for your deployment. See License Management for specific license requirements.

To add a new Appliance:

1. Select Tools > Options > CounterACT Devices > Add.

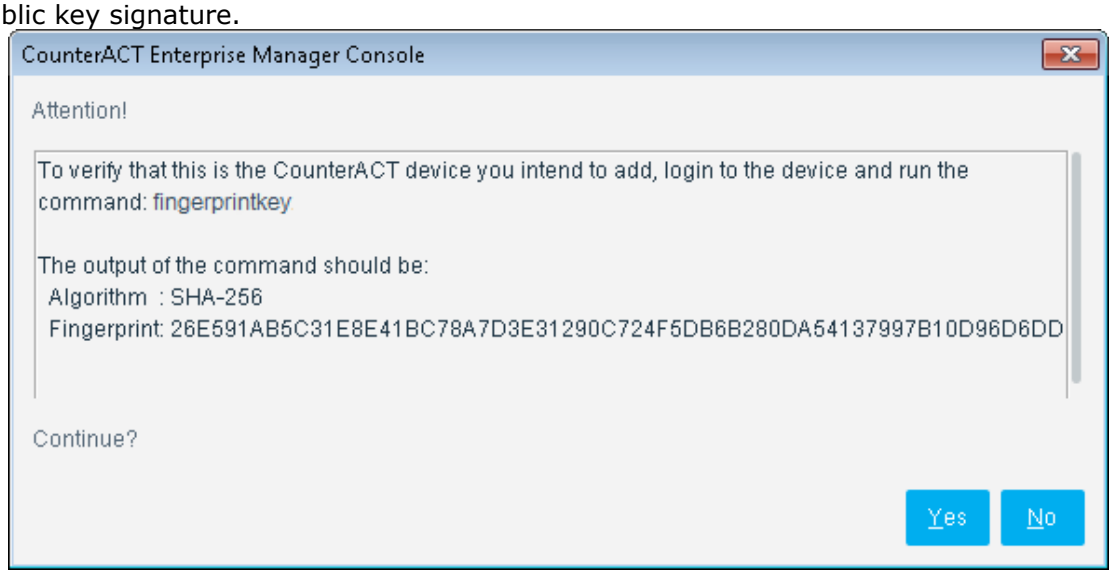


2. Specify the following settings:

IP/Name	The IP address or hostname of the Appliance.
Port	The port is used by the Appliance for network connection. It is recommended to keep the default setting.
User Name	The admin username that is used to connect to this Appliance.
Password	The admin password used to connect to this Appliance.
/Appliances	The folder in the Appliance tree in which you want to add the Appliance.

3. Select OK. Messages indicate that the components are connecting, and that the Appliance

is being registered with the Enterprise Manager. You are prompted to verify the Appliance public key signature.



4. To verify the Appliance key, log in to the Appliance CLI and run the following command: `fingerprintkey`

   Note:
   In the Bash shell, run `fstool key`. Refer to the *Forescout CLI Commands Reference Guide* for more information.

   A message opens with the key ID.

5. When the Initial Setup Wizard opens, set up the Appliance as required. See Set Up an Appliance with Enterprise Manager Settings for details.

Upgrade one or more Appliances

To upgrade Appliance software:

Note:
Before you can upgrade Appliances that are managed by an Enterprise Manager, you must first upgrade the Enterprise Manager separately. Upgrades do not propagate automatically from an Enterprise Manager to its managed Appliances. See Upgrade the Enterprise Manager.

Note:
This procedure assumes that you have already upgraded the Enterprise Manager that manages the Appliances.

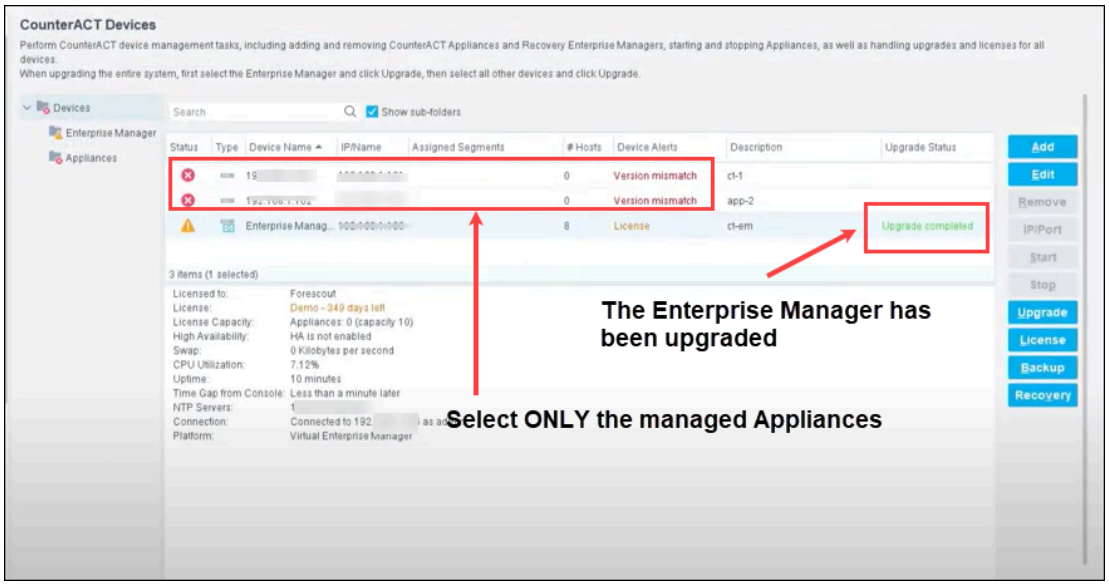
1. Download or obtain the upgrade file (FSP) and save it to your computer.

   Note:
   After the Enterprise Manager is upgraded, use the same FSP file to upgrade the managed Appliances. This ensures that you upgrade all devices to the same software version.

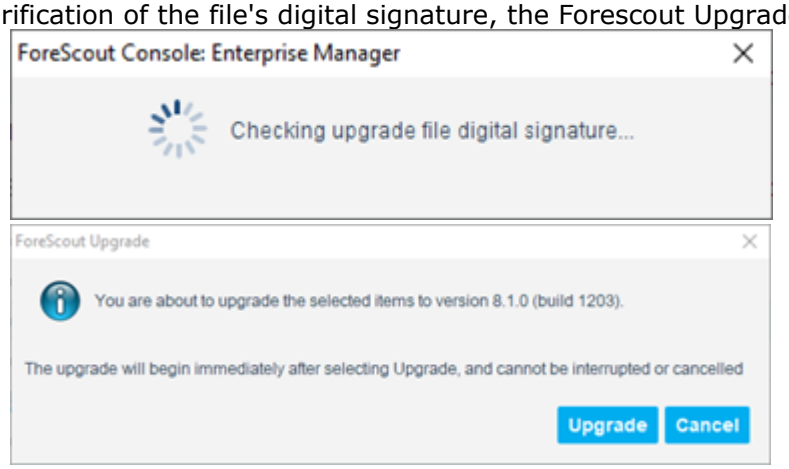
2. Select Tools > Options. Devices or Appliances are shown with their current version.

   Note:
   After the Enterprise Manager is upgraded, the managed Appliances display a Version mismatch alert.

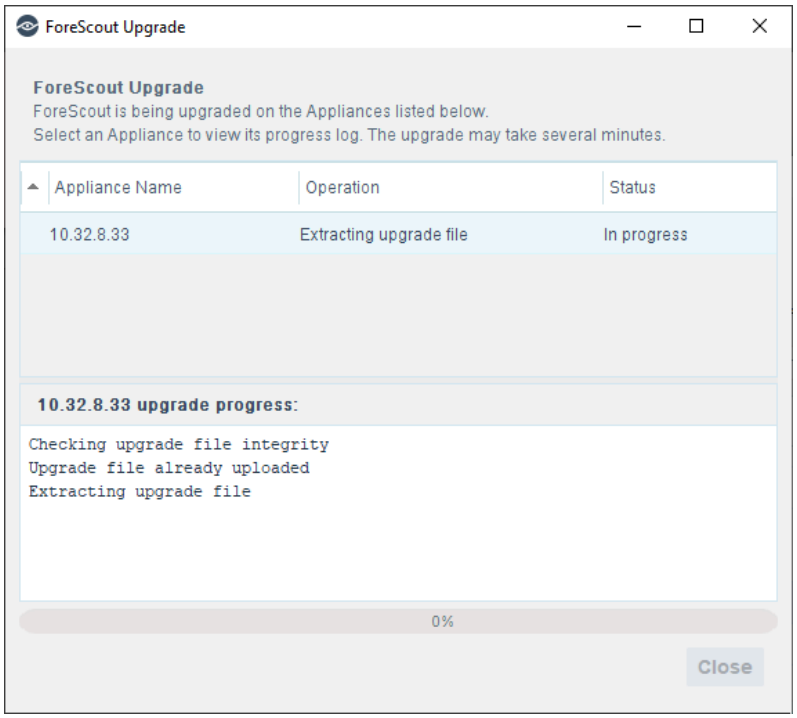
3. Select the Appliances, and then select Upgrade.



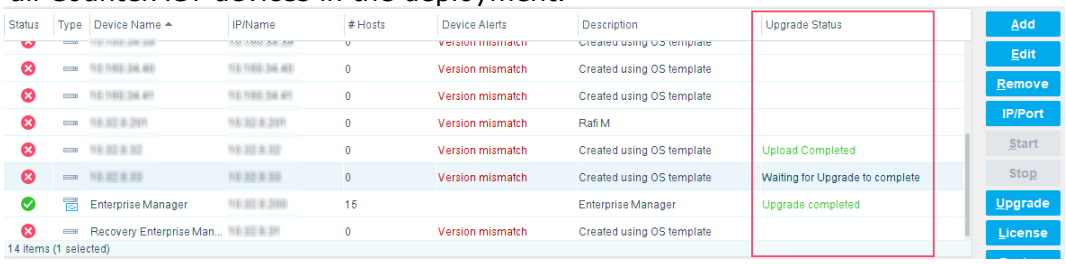
4. Select the scope of the upgrade:
    - Upload Only. Upload the file to the device but do not begin the upgrade.
    - Upload and Upgrade. Upload the file to the device and begin the upgrade.
    - Upgrade. Upgrade from the uploaded file. Only available after the file has already been uploaded to the Enterprise Manager.
5. Select Browse…, locate the upgrade file you saved on your computer and select OK. After verification of the file's digital signature, the Forescout Upgrade screen appears.



6. Select Upgrade. Once you confirm, the upgrade process proceeds to completion and cannot be interrupted or canceled.



7. Review the Forescout Upgrade dialog box to see the status of the upgrade process. You can close the dialog box and continue to see the status in the Upgrade Status column of the CounterACT Devices pane. This column disappears when the upgrade has completed for all CounterACT devices in the deployment.



Note:

If the upgrade of the second node and the synchronization are not shown in the log, you can verify status via icons on the Console status bar:

Icon	Description
	Indicates the status of the High Availability Appliances connected to the Enterprise Manager.
	Indicates the status of the Enterprise Manager High Availability pair.
	Indicates that High Availability is down on the Appliance.
	Indicates that High Availability is down on the Enterprise Manager.

8. When the upgrade is completed successfully, select Close. If the upgrade is not successful, contact your Forescout representative. Do not continue with more upgrades.
   The Forescout Upgrade dialog box shows the status of the upgrade process and displays any error messages for the process.

Upgrade the Console

During Appliance upgrade, any Consoles that are connected to the Appliance lose their connection. When the upgrade is available, you are informed that your Console software needs to be automatically updated.

For more information about updating Console software, see Upgrade the Console.

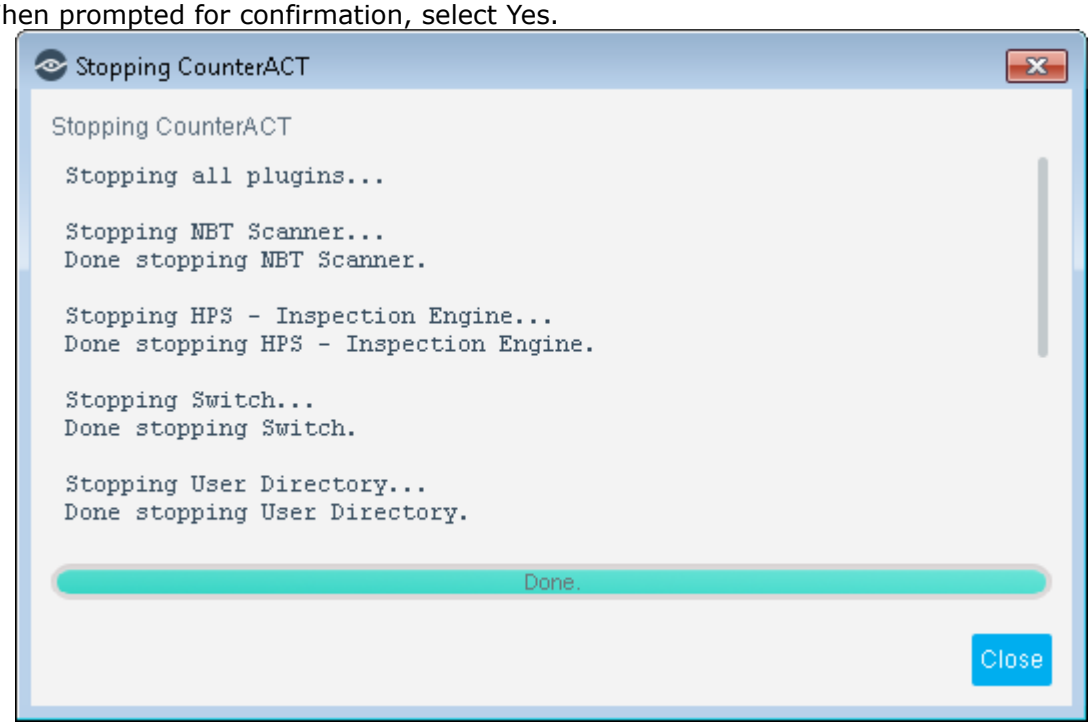
Start and Stop Appliances

When an Appliance stops, Threat Protection, NAC, Discovery detections and other functionality are stopped. In addition, plugin and module functionality is stopped. As a result, blocked endpoints are released, and plugin/module actions previously taken on endpoints are undone.

When you start the Appliance again, plugin/module activity and endpoint detection resume. In addition, all endpoints that were released by the Stop operation are returned to their previous state.

To start or stop an Appliance:

1. Select Tools > Options.
2. Right-click an Appliance in the CounterACT Devices pane and select Start or Stop.
3. When prompted for confirmation, select Yes.



4. Select Close. The Appliance is displayed as stopped. To start or stop the Appliance when logged on to a single Appliance:
5. Select Tools > Options.

6. Select the Appliance in the Appliances pane and then select Start or Stop.

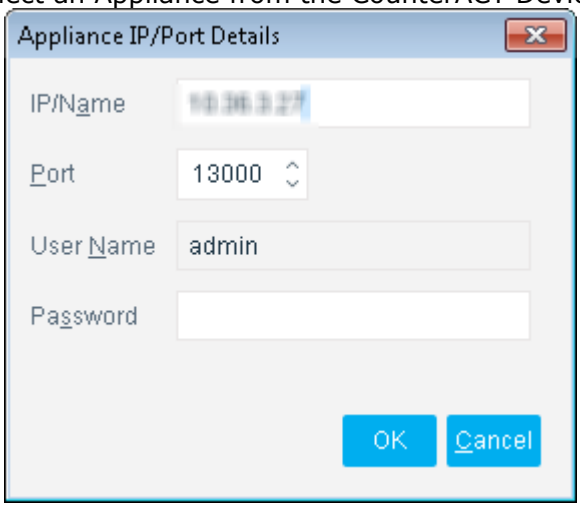
Update Appliance Connection Details

Update the IP address or port number used to connect an Appliance with an Enterprise Manager, while preserving all Appliance configurations. You may need to do this if:

- The Appliance IP address changes and you want to connect using the new IP address. In this case, the Status column and the Device Alert column indicate that the Appliance is disconnected.
- You can use the `fstool netconfig` command to change the Appliance IP. See Sample fstool netconfig Session for details.
- The Appliance is connected using the IPv4 address and the user wants to connect to it using its IPv6 address. In this case, the Status column and the Device Alert column indicate that the Appliance is connected.

To update Appliance connection details:

1. Select Tools > Options.
2. Select an Appliance from the CounterACT Devices pane and then select IP/Port….



3. Enter the new IP address or host name of the Appliance. Verify that you have updated the Appliance IP address and name on the machine.
4. Enter the port number for the Appliance. This port is used to communicate with the Enterprise Manager and the Appliance Console.
5. Enter a password for the "`admin`" user for this Appliance. Verify that you have updated the password for this user from the Appliance Console.

   Log in to the Console for this Appliance and select Tools > Options > CounterACT User Profiles. You must enter the current password even when only updating the IP address and name or port.

6. Select OK. The Appliance connection details are updated. The Device Alerts and connection status indicator columns in the CounterACT Devices pane is updated to indicate that the Appliance is connected.

Manually Upload the Upgrade File to an Appliance

In Forescout environments that experience connectivity issues (for example, the Appliance disconnects from the Enterprise Manager), you may prefer to manually upload the upgrade file to an Appliance/s.

To manually upload the file:

1. Before upgrading Appliances, you should upgrade the Enterprise Manager.
2. Download or obtain the upgrade file (FSP) and save it to a location on your computer.
3. Unzip the data.zip file from the FSP file.
   Note:
   The unzip can be performed on any machine.
4. Rename the data.zip file to fssetup.zip.
5. Copy the extracted ZIP file to the following location on the Appliance machine: /usr/src/fssetup.zip

   The copied file populates the Upgrade Status field in the Upgrade Status column of the CounterACT Devices pane after up to an hour from the time of copy, and only after the Enterprise Manager is upgraded with the current release of the Forescout eyeSight.

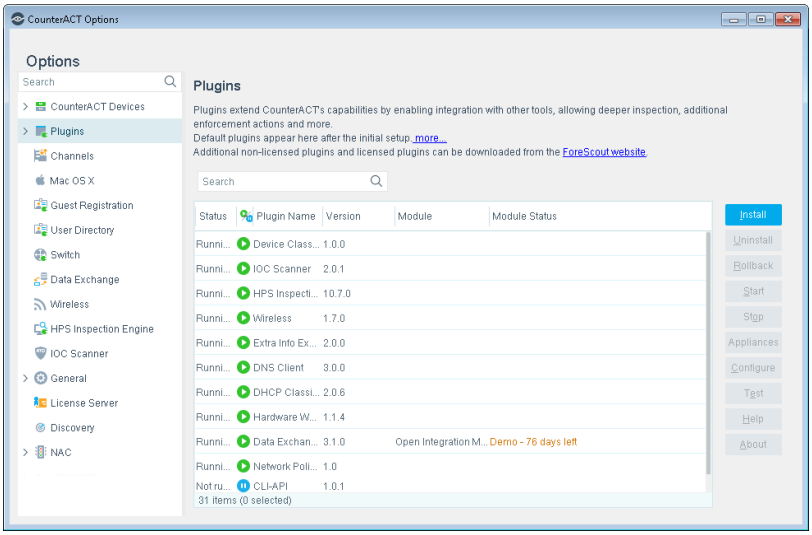
Managing Groups of Appliances

Forescout provides tools that simplify management of large numbers of Appliances. Use these tools when configuration settings or other management tasks must be applied to groups of Appliances. For example time zone and network connection settings are typically identical for all Appliances in a network location or geographical region.

View and Manage Plugin and Module Assignments per Folder

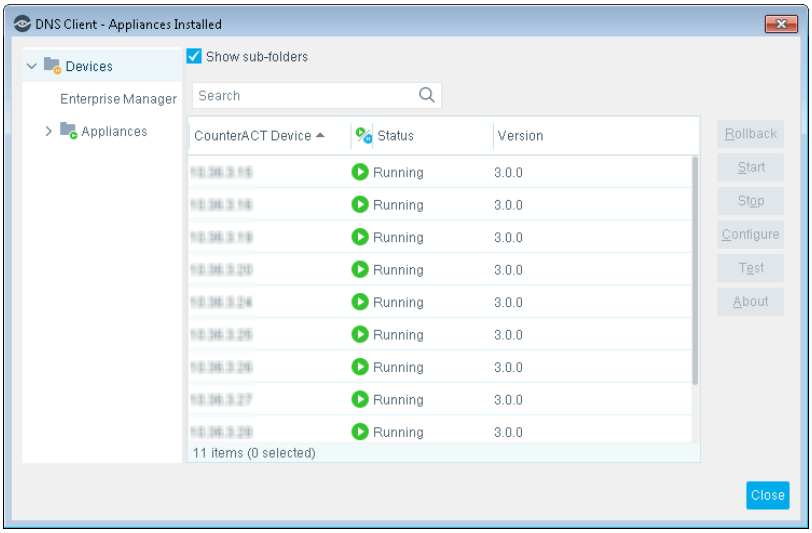
You can quickly view all Forescout devices with a specific plugin or module installed.

Select Tools > Options > Modules.



Note:
Management tasks, for example, Start, Stop, Rollback, and Configure, can also be performed from this dialog box.

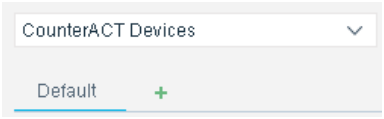
Double-click the required Content Module, or expand a module and double-click the required plugin. On the Devices tree, navigate to and select the Appliance, folder, or Enterprise Manager to display the list of devices on which the plugin or module is installed.



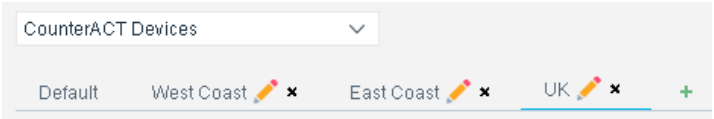
Configure Features for an Appliance or Group of Appliances

You can configure plugins and modules and certain features for individual Appliances or for a group of Appliances. This allows easy support of large, geographically dispersed environments.

When this option is available, configuration settings are organized using a row of tabs. Each tab duplicates all the configuration fields in the pane. Initially, only the Default tab is present.



In the following example, additional tabs have been added, with separate configurations for regional groups of Appliances.

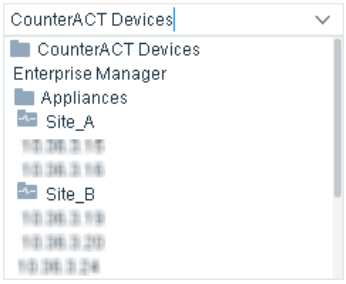


Note:
Settings of the Default tab apply to all devices that are not included in any other configuration. The Enterprise Manager always uses the settings of the Default tab.

Use the following controls to create and manage configurations:

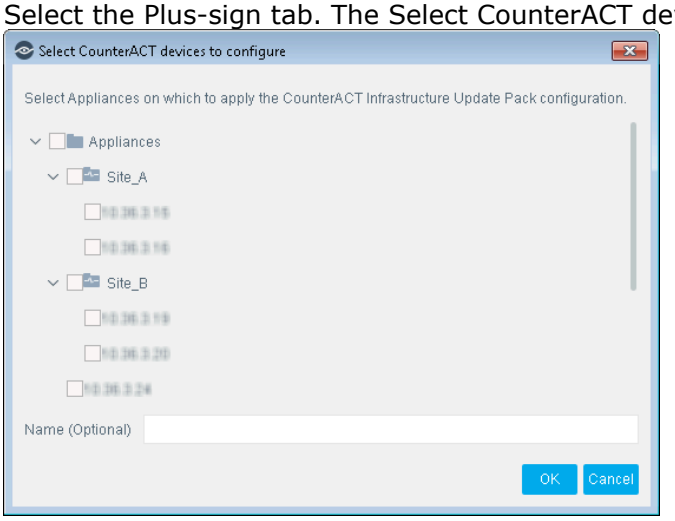
- Select the Plus-sign icon

to create a new configuration.
- Use the Edit icon and the Delete icon x on a tab to update a configuration.
- When there are several configurations, it may be difficult to locate the configuration that applies to a specific device. Select the device from the CounterACT Devices drop-down. The configuration that applies to that device is highlighted for editing.

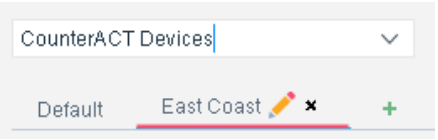


Example: To create a separate configuration for a device or group of devices:

1. Select the Plus-sign tab. The Select CounterACT devices to configure dialog box opens.



2. Select the devices to which these configuration settings you want to apply these settings.
3. (Optional) Specify a text label for this configuration instance in the Name (Optional) field.
4. Select OK. A tab is added to the pane.



Configuration settings you define while this tab is selected apply only to the devices you selected in step 2.

Working with Appliance Channel Assignments

A channel defines a pair of interfaces used by the Appliance to protect your network.

In general, one interface monitors traffic going through the network (monitor interface). The other interface generates traffic back into the network (response interface). Response traffic is used to:

- Protect against self-propagating malware, worms and hackers.
- Carry out Virtual Firewall blocking.
- Perform policy actions. These actions may include, for example, redirecting web browsers or blocking access to the Internet.

A single interface may also be used as both the monitoring and the response interface.

Monitoring and response interfaces are recorded in the Data Center when installing the Appliance. In addition, the appropriate physical connections are made when connecting the Appliance to the switch.

When first logging in to the Console, the Initial Setup Wizard prompts you to define Channel interface settings to match these connections. These settings appear in the Channels pane. They are also displayed when you select Edit in the CounterACT Devices pane and select the Channels tab.

If not defined via the wizard, you should manually define the channel interface settings. See Add Channels for details.

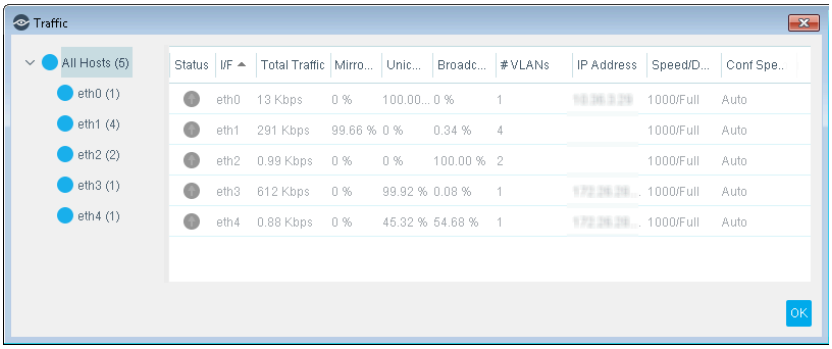
If this task was completed by the wizard, use the Channels pane to edit and remove channel definitions, modify VLAN tagging definitions and manually define VLANs.

Note:
If you change the monitoring interface assignment because no traffic is detected, or for any other reason, you must readjust the physical interface connections in the Data Center.

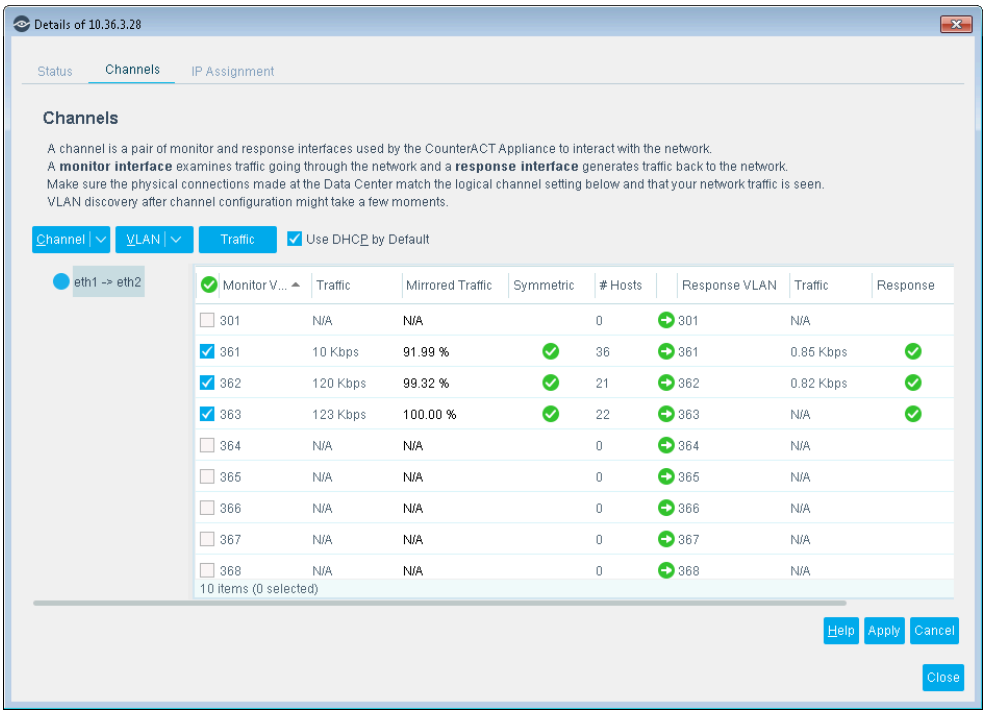
VLAN Tagged Traffic

By default, all VLAN tagged traffic and all untagged traffic is monitored by the Appliance. The Appliance matches these tags when sending response packets. This means response traffic has VLAN IDs identical to the IDs of the original monitored traffic. This (recommended) default applies when monitoring and responding to a trunk port.

To view dynamic network traffic information about the Appliances in your enterprise, select Right-click an Appliance from the Devices pane and select Traffic.



To view channel information, select Options. Double-click an Appliance in the Devices pane, or select it and select Edit. Select the Channels tab to view the logical setup and traffic between the monitor and response interfaces that the Appliance uses to interact with the network.



Alerts on specific channels where traffic problems have been detected appear at the bottom of the Channels pane.

- Select Channel to add, edit or remove channel listings.
- Select VLAN to add a single VLAN listing, or to perform actions on all VLANs listed including remove, enable and disable.
- Select Traffic to view the traffic monitored by a specific interface.

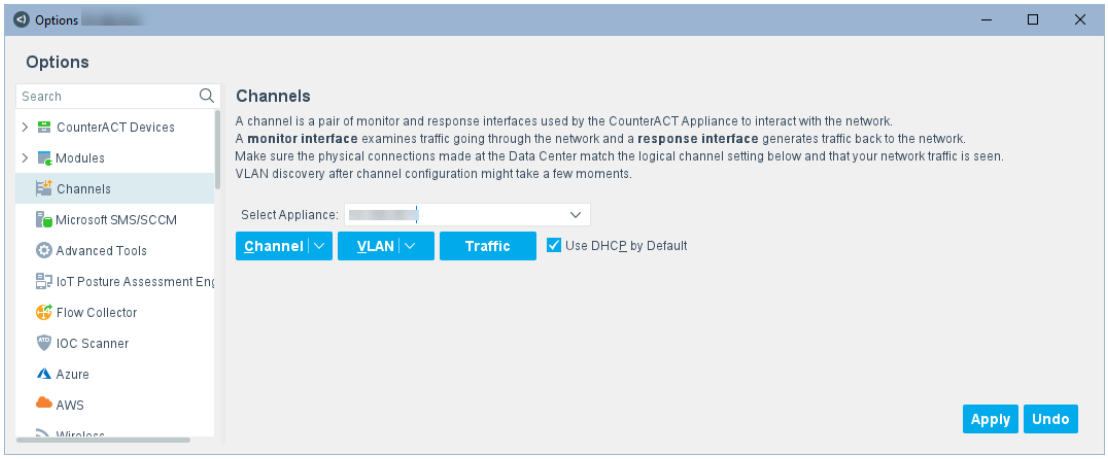
Add Channels

Forescout recommends to create channels to match Appliance interface connections, to monitor and respond to traffic on network interfaces.

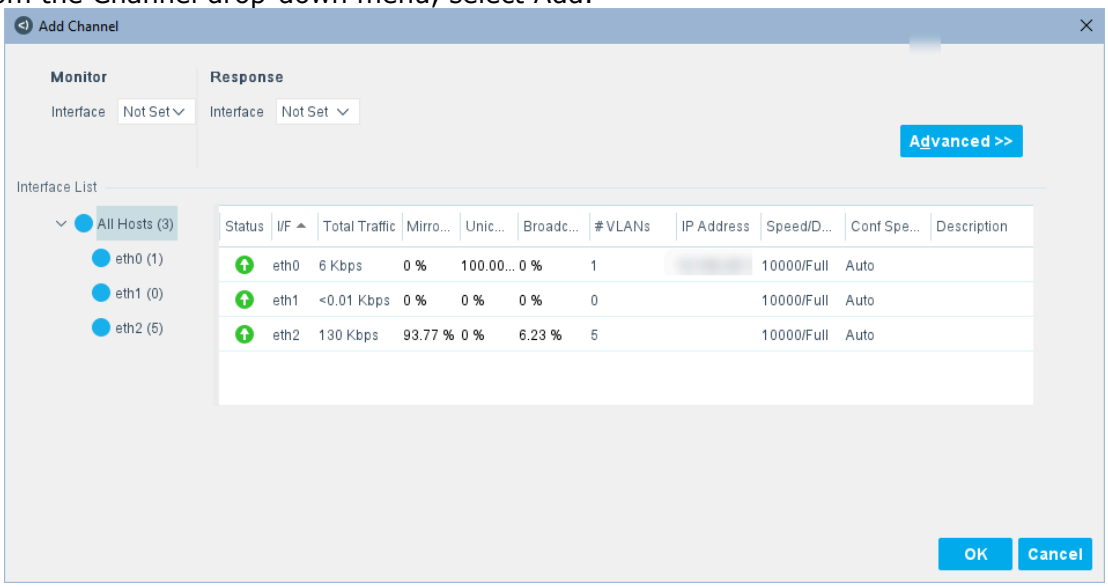
For performance optimization recommendations, refer to the *Packet Engine Configuration Guide*.

To add channels:

1. Select Tools > Options > Channels.
2. In the Select Appliance field, select the Appliance to which you want to add channels. The pane displays channels already defined for this Appliance, and the traffic detected on the Appliance.



3. From the Channel drop-down menu, select Add.



The interfaces detected on your Appliance appear in the Interface List. Every few seconds, traffic is captured on the selected interface according to the various VLANs.

Review the interfaces and related information to verify that traffic is visible on interfaces to which you connected in the Data Center, for example, if traffic is actually mirrored. If you change an interface assignment in this dialog box because no traffic is detected or for any other reason, you must go back to the Data Center and readjust the physical interface connections.

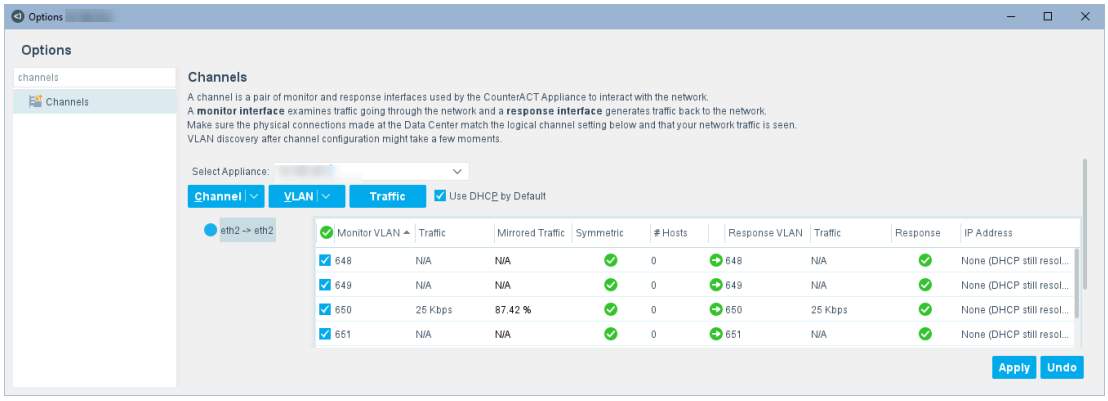
The following information is available:

Status	If the interface is up or down.
IF (Interface)	The monitoring interface.
Total Traffic (kbps)	The total VLAN traffic monitored by the interface.

Mirrored	The percentage of total traffic that is not broadcast and not directed at the Appliance. This information lets you know if the device is monitoring traffic. A value of less than 20% indicates that the switch was not correctly configured. Under most circumstances, the mirrored traffic percentage should be very high on all but the relatively quiet VLANs. A quiet VLAN displays a high percentage of Broadcast traffic.
Broadcast	The percentage of Broadcast traffic detected on the VLAN.
Unicast	The percentage of Unicast traffic sent to and from the Ethernet address on the interface.
# VLANs	The VLAN number.
IP Address	Interface IP address.
Speed Duplex	The current speed and whether the interface is automatic or full or half duplex.
Conf Speed/ Duplex	The configured speed and whether the interface is automatic or full or half duplex.
Description	A description of the interface.

Troubleshooting alerts appear at the bottom of the dialog box if traffic detection is exceptionally low or high.

4. From the Monitor drop-down menu, select the interface connected in the Data Center to a mirroring port.
5. From the Response drop-down menu, select the interface connected in the Data Center.
6. Select OK. The Channels pane displays the configured channel setup. Alternatively, select Advanced to modify VLAN tagging definitions. See Customize VLAN Tagging Definitions.



The dialog box contains the following information:

Enabled (checkbox)	When selected, activates the channel configuration. Monitoring and response activity will not function until you select Apply from the Channels pane.
Monitor VLAN	All VLAN IDs discovered for the selected monitoring interface. If you defined a channel that works with an IP layer, that VLAN is displayed as IP LAYER.
Traffic (Bps)	The total VLAN traffic detected on the monitored interface.
Mirrored Traffic	The percentage of mirrored traffic from the total VLAN traffic.
Symmetric Traffic	Indicates whether the interfaces passed the Symmetric Traffic test. The test verifies that the Appliance can see symmetric traffic on the monitoring interfaces. That is, for every TCP conversation both incoming and outgoing traffic is visible. When this condition is detected, the traffic received on the channel is ignored until the condition has cleared. The test runs continually. If the test failed, you can review related troubleshooting information at the bottom of the Channels pane.
# of Hosts	The total number of endpoints monitored on the VLAN.

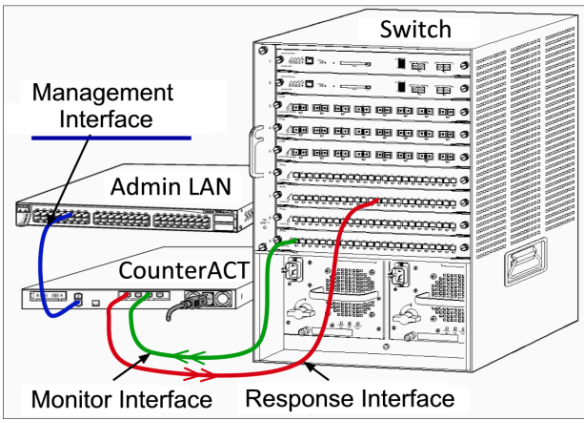
Response VLAN	All VLAN IDs discovered for the selected response interface.
Traffic (Bps)	The total VLAN traffic detected on the response interface.
Response	Indicates whether the Response test succeeded on the VLAN. The test verifies that the Appliance successfully sends response traffic to the network. The test runs continually. If the test failed, you can review related troubleshooting information at the bottom of the Channels pane.
IP Address	The response interface IP address, i.e., the DHCP address used by the Appliance for response traffic. By default, the IP address is acquired through DHCP. If the DHCP is not successful, the Forescout eyeSight cannot respond to ARP requests. In this case, manually define the address. Addresses are defined per VLAN, if required. See Manually Add a VLAN for details.

7. Select Use DHCP by Default if a DHCP address is used for monitored traffic. Clear Use DHCP by Default to manually configure the IP address.
8. Select the Enabled checkbox for each VLAN that you want to activate.
9. Select Apply. A Symmetric and Response test is performed. If the test fails, you can review related troubleshooting information at the bottom of the dialog box.

Customize VLAN Tagging Definitions

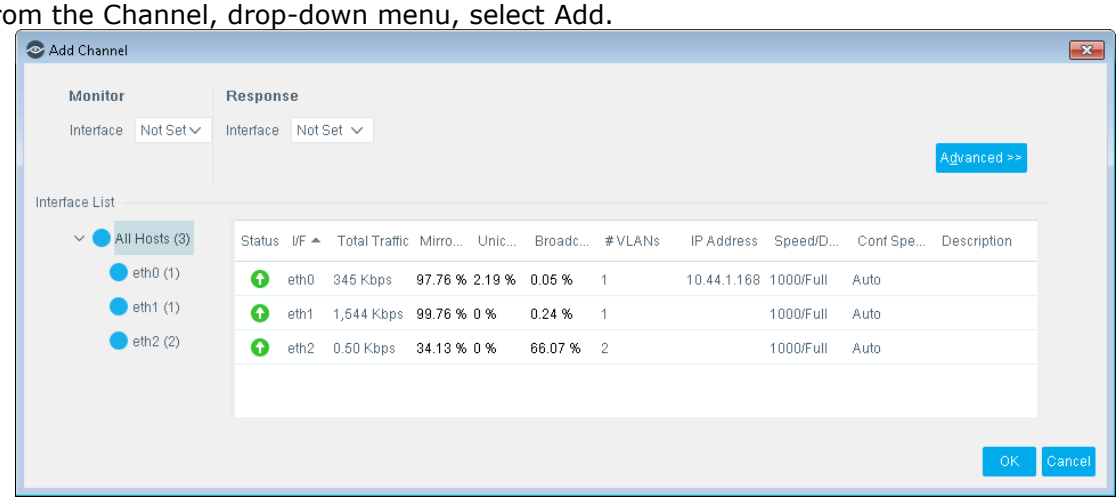
By default, all VLAN tagged and untagged traffic is monitored by the Appliance. These tags are matched when sending response packets. This means that response packets have VLAN IDs identical to the IDs of the monitoring packet that triggered the response. This default (recommended) applies when monitoring and responding to a trunk port.

The Appliance Management interface should be untagged.

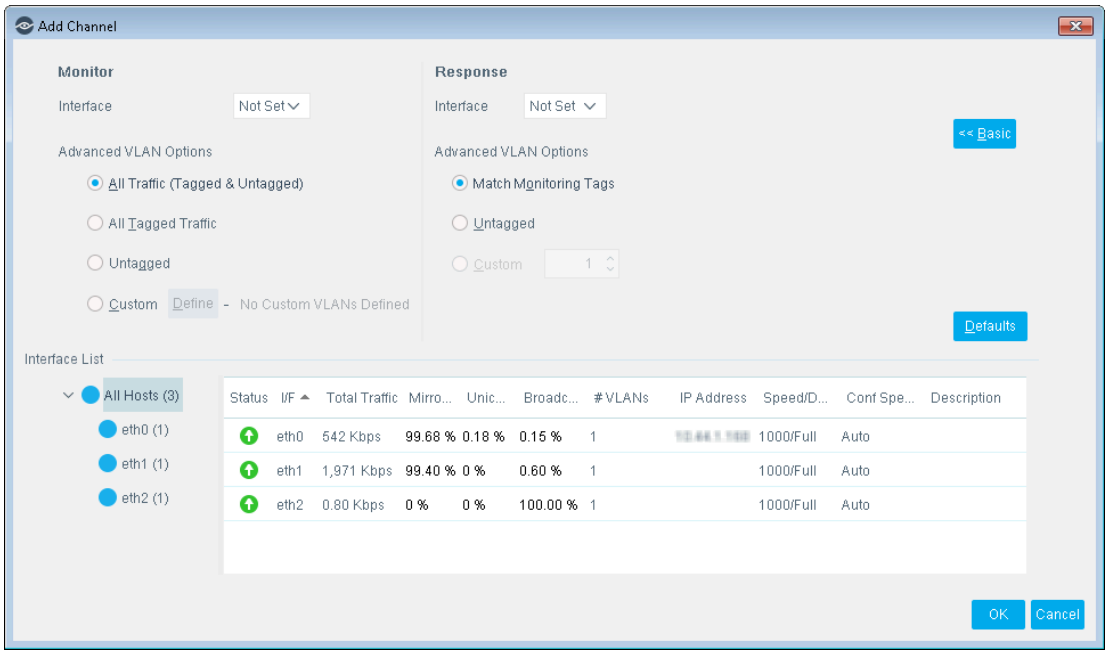


To customize VLAN tagging:

1. Select Tools > Options , and then select Channels.
2. From the Channel, drop-down menu, select Add.



3. Using the Monitor and Response drop-down menus, define the channel monitor and response settings and then select Advanced to access the advanced options.



4. In the Monitor – Advanced VLAN Options section, select one of the following options:
    - Select All Traffic (Tagged & Untagged) to monitor all traffic on the interface.
    - Select All Tagged Traffic to monitor all tagged traffic on the interface.
    - Select Untagged to monitor untagged traffic on the interface.
    - Select Custom to define specific VLAN IDs to include or exclude from the definition. You can include untagged traffic in this list by selecting Include Untagged Traffic.
5. In the Response – Advanced VLAN Options section, select one of the following options:
    - Select Match Monitoring Tags to send response packets with VLAN IDs identical to the IDs of the monitoring packet that triggered the response. Select this option when responding to a trunk port.
    - Select Untagged if the response packets for this channel are not tagged with VLAN IDs.
    - Select Custom to define a specific VLAN ID. This option is used when responding to a tagged port, on behalf of untagged traffic.
    - IP layer: The Appliance can use its own management interface to respond to traffic. Although this mode can be used with any channel, it is ideal where the Appliance is monitoring ports that are not part of any VLAN, and thus there is no way to respond to the monitored traffic using any other switch port. This is typical when monitoring a link connecting two routers. Using this mode has the limitation of not being able to respond to ARP requests, which limits the ability of the Forescout eyeSight to detect scans aimed at the IP addresses included in the monitored subnet. This limitation does not apply when traffic between two routers is monitored.
6. Select OK. The Add Channel dialog box closes.
7. Select Apply.

Manually Add a VLAN

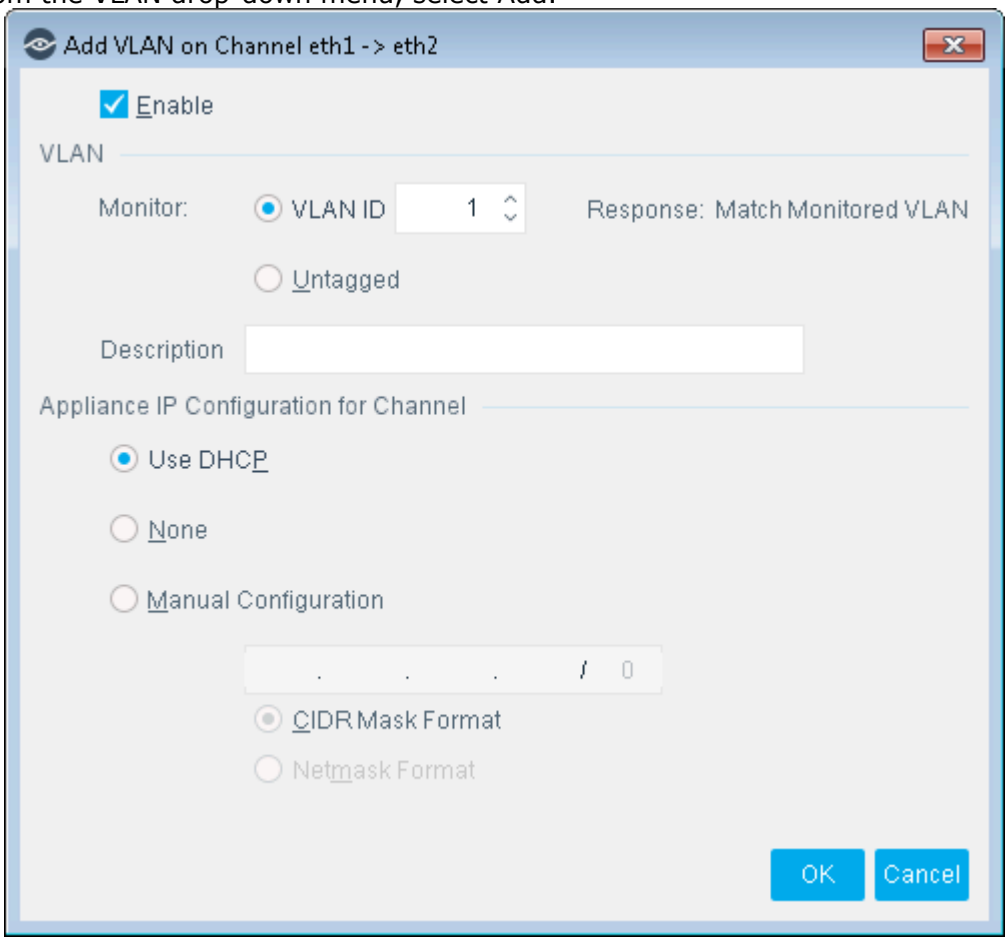
Add a VLAN to monitor a specific path of traffic. You may need to do this, for example, if there is currently no traffic running on the VLAN.

If this is the case, search for possible reasons, for example, the interface is not connected, a

switch is not correctly configured, or the ports are down.

To add a VLAN:

1. Select Tools > Options > Channels.
2. From the Select Appliance drop-down menu, select the Appliance to which you need to add a VLAN. The Appliance channel list is displayed in the Channels pane.
3. From the VLAN drop-down menu, select Add.



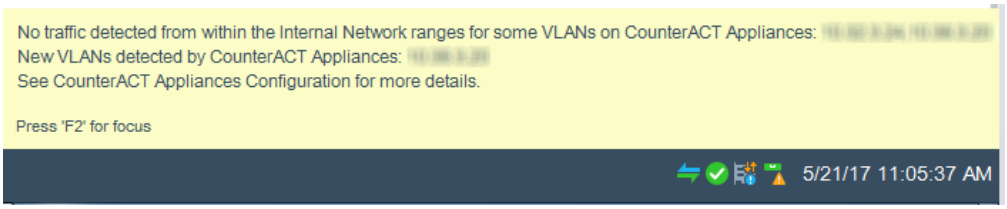
4. Configure the VLAN settings and select OK.

Console Indicators

An indicator is displayed on the Console status bar if:

- There is a connectivity problem on enabled VLANs or defined channels.
- No channels are enabled.
- A new VLAN is automatically discovered by the Appliance.

A tooltip provides details about the event that occurred.



802.1ad and 802.1QinQ VLAN Tag Termination Traffic

You can configure the Forescout Platform to identify 802.1ad and 802.1QinQ VLAN Tag Termination traffic. Identifying this traffic expands VLAN discovery, provides increased visibility and enables Forescout functionality for QinQ traffic, including:

- Threat Protection
- HTTP Actions
- Virtual Firewall

Identification of 802.1ad and 802.1QinQ VLAN Tag Termination traffic is only supported when the Response Interface is set to IP Layer in Options > Channels.

You can identify traffic containing either service provider VLAN tags (external) or customer VLAN tags (internal). Be aware that enabling either internal or external tag identification will determine which VLAN the traffic is associated with. Enabling either type of 802.1ad and 802.1QinQ VLAN Tag Termination traffic does not affect untagged/tagged traffic handling.

This feature is disabled by default.

To enable identifying 802.1ad and 802.1QinQ VLAN Tag Termination traffic, perform one of the following for each Appliance:

- To identify traffic containing service provider VLAN tags (external), log in to the Appliance CLI and run the following command:
- `fstool set_property engine.conf.params.VlanQStacking 1`
- To identify traffic containing customer VLAN tags (internal), log in to the Appliance CLI and run the following command:
- `fstool set_property engine.conf.params.VlanQStacking 2`

Run the following command to restart the service:

```
fstool service restart
```

To disable identifying 802.1ad and 802.1QinQ VLAN Tag Termination traffic, run the following commands:

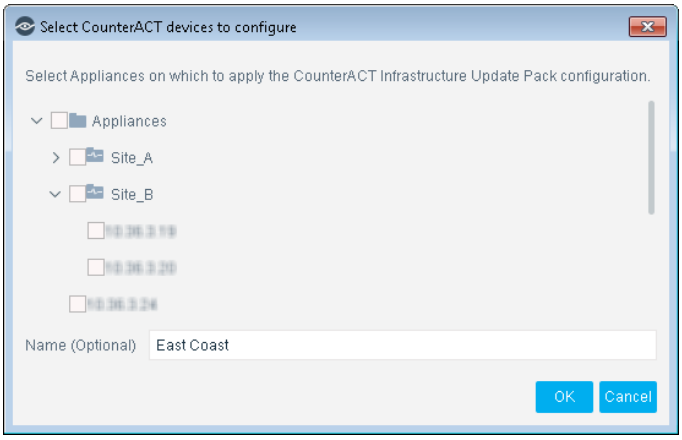
```
fstool set_property engine.conf.params.VlanQStacking 0

   fstool service restart
```

Limiting User Access to Appliances

Endpoint IP address assignments made to a particular Appliance may be out of your user Scope. When this happens, you cannot configure or edit the configuration. Appliances that contain

endpoint IP assignments out of your scope are displayed with an empty red circle or red circle with a line through it.

An empty red circle indicates that you do not have access to any IP addresses managed by the Appliance. A circle with a line indicates that you have partial access.



Scope definitions are made by Forescout administrators for the purpose of granting and limiting user access to specific endpoints or segments in the network. Scope definitions are configured in the CounterACT User Profiles pane. To access the pane, select Tools > Options, and then select CounterACT > User Profiles.

Viewing Limitations

Certain Appliances may contain endpoint IP address assignments that are not in your Scope. When this happens, you may not be able to view or edit the Appliance configuration.

A red no-entry icon appears on Appliances that contain endpoint IP address assignments partially out of your Scope. For example:

Other endpoint IP address assignments made to an Appliance may be entirely out of your user scope. When this happens, the Appliance does not appear in the drop-down menu.

Scope definitions are made by Forescout administrators for the purpose of granting and limiting user access to specific endpoints or segments in the network. Scope definitions are configured in the CounterACT User Profiles pane. To access the pane, select Tools > Options, and then select CounterACT > User Profiles.

Controlling Command-line Access to Devices

Forescout devices expose a command-line interface (CLI) that is used by administrators for device installation and setup, or to issue `fstool` commands, or when file import/export tools are not supported by the Console.

Note:
The user accounts defined at the CLI level are not related to Console or web portal users.

Configure Session Security Features for Command-Line Interaction

Define audit log file properties and other security features that apply when users log in to Forescout devices through the CLI. By default, logs report general operations related to, for example, some of the following activities:

- User login
- Stopping or starting the Forescout eyeSight

You can configure Forescout devices to monitor additional audit events to help discover violations of security policies used on your system (os.enable.audit.rules property). These additional audit events may relate to some of the following activities:

- Service requests
- File modification
- Time modification
- Permission changes

To configure security features for command-line interaction, log in to the Forescout device CLI use the `fstool set_property` command to configure the relevant property from the table below. After setting one or more of the properties, run the command `fstool os_security config`.

---

os.forward_audit_to_syslog Forward a copy of the audit log files to the syslog server.

Default value is 0 (disabled).

---

os.audit_max_log_size The size in MB of the audit log files to be generated.

Default value is 6 (6MB). Maximum value is 50 (50 MB).

---

os.audit_free_space_alert_value The percentage of free disk space left that triggers an alert.

Default value is 0.5 (0.5%). Maximum value is 10 (10%).

---

os.audit_num_log_files The number of recently created audit log files to be kept.

Default value is 5. Maximum value is 20.

---

os.enable.audit.rules When this property is set to True, devices monitor additional audit events and conditions that indicate security exposure (for example, service requests or file modifications).

os.enable.audit.rules.immutable It may be necessary to disable enhanced auditing, for example, if enhanced auditing causes performance issues.

When this property is set to True, the audit events monitored by the os.enable.audit.rules property cannot be disabled until the device is rebooted.

This property is only enforced if os.enable.audit.rules is set to True.

Configure Password Protection for the Boot Loader

Forescout devices use the GNU GRUB boot loader. To prevent malicious changes to boot settings, you can protect access to these settings by requiring a password.

Note:
Once you define a boot loader password, you cannot disable password protection or define a null password.

To configure password protection for the boot loader, log in to the device CLI and run the command `fstool grub –setpassword`.

The system prompts for this password when users try to edit boot loader settings.

Enterprise and Appliance Authentication

The Forescout eyeSight ensures secure communication between Enterprise Managers and Appliances through customer issued CA certificates. Customers can generate certificate sign requests to a CA Service and import the signed certificate, and its certificate chains for each Enterprise Manager and Appliance.

Create a Certificate Sign Request

Create a certificate sign request on each Forescout device. Log in to its command-line interface (CLI) and run the following command:

```
fstool replace_certificate --cert-req > <filename>
```

Send the request to the appropriate Certificate Authority to have it signed.

Import a Signed Certificate

After receiving the signed certificates, import each one to their corresponding Forescout device. Log in to its command-line interface (CLI) and run the following command:

```
fstool replace_certificate --import --server-cert <certificate-file> --ca-cert-chain <ca-chain-file>
```

Configure Certificate Verification Enforcement

Disabled by default, certificate verification enforcement can be enabled using the `fs.enforce.cert.verify` property. Once enabled, the Forescout eyeSight requires signed certificates of both existing and future Enterprise Managers and Appliances.

After importing a signed certificate on each Enterprise Manager and Appliance, enable certificate enforcement.

To enable certificate enforcement, log in to the Enterprise Manager command-line interface (CLI) and run the following commands:

```
fstool set_property fs.enforce.cert.verify true

fstool service restart
```

To disable certificate enforcement, log in to the Enterprise Manager command-line interface (CLI) and run the following commands:

```
fstool set_property fs.enforce.cert.verify false

fstool service restart
```

Working with appliance folders

Use Appliance folders to simplify and unify eyeSight device management and configuration tasks. These folders are especially useful for medium- and large-scale deployments.

Use Appliance folders to group devices into a tree structure, and to correlate Appliances with geographical or functional segments of the Internal Network. The Appliances in a folder handle endpoints in the Internal Network segments you assigned to the folder.

Define Appliance folders to:

- Efficiently support large or geographically disperse networks
- Implement automatic IP allocation between Appliances
- Create failover clusters (licensed feature. Refer to the *Forescout eyeSight Resiliency and Recovery Solutions User Guide*.

Use Forescout segments based on the Internal Network to assign IP addresses to folders or Appliances. Define these segments in the Segment Manager before you work with folder tools. For example, if your network expands, you typically:

- Install new Appliances
- Use the Segment Manager to define segments with your network's new IP addresses. See Working with Forescout Segments.
- Add these segments to the Internal Network. See Working with the Internal Network.
- Follow the procedures described in this section to define folders that contain the new Appliances, and to assign the new segments to Appliances.

Note:
If you change the definition of Internal Network segments, this can change which IP addresses are assigned to folders or Appliances.

The following general permissions are required to work with Appliance folders:

- CounterACT Configuration
- CounterACT Policy Management

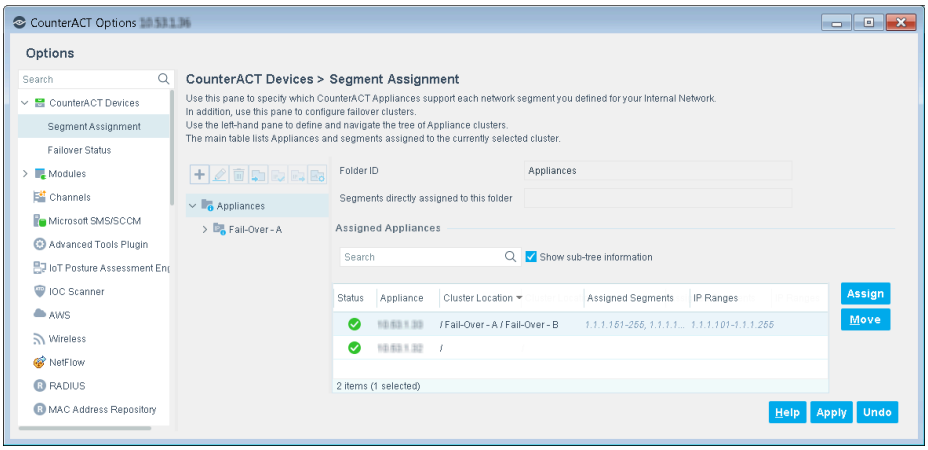
To work with folder tree actions, the following additional permissions are required:

- Multiple CounterACT Appliance Management (update)
- CounterACT Appliance Control

Write permission is required to save changes.

To work with Appliance folders select Options> CounterACT Devices > IP Assignment and Failover.

The IP Assignment and Failover pane opens.



The tree of Appliance folders is shown in the left pane. If you have already defined Appliance folders, they appear in the tree. To modify the folder tree, select a node in the tree and perform one of the following actions:

	Add a folder. You are prompted to name the new folder. The new folder is created as a child of the selected node.
	Edit the name of the selected folder. This string appears in the Folder ID field.
	Delete the selected folder. Before you can delete a folder, you must remove all its segment assignments and child nodes.
	Move the selected folder and its child nodes to another location in the tree. The selected folder is moved under the new parent node that you specify.
	Assign segments to the folder. The network segments you specify here appear in the Assigned Segments field. To support these segments, endpoints are allocated to free Appliances (which do not have statically assigned segments).
	Reassign segments to this folder from Appliances in child folders. All segments statically assigned to Appliances in sub-folders of the selected folder are assigned to the selected folder. Reassigned segments now participate in load sharing. Segments assigned to sub-folders are not reassigned This action skips sub-trees with a folder-level segment assignment.

	Configure the selected folder as a failover cluster. This folder should have only folder-level segment assignments. You cannot include an Appliance with static segments assignments in a failover cluster. This is an optional, licensed feature. For details on licensing and failover cluster configuration, refer to the Forescout eyeSight Resiliency and Recovery Solutions User Guide. .

The main pane lists the following information for each Appliance in the selected folder:

Status	An icon indicating the operating state of the Appliance, and its connection to Enterprise Manager.
Appliance	The name or other identifying label of the Appliance
Folder Location	The full path to the folder that includes this Appliance. This is the full path of the selected node in the Appliance Folders tree.
Assigned Segments	Segments defined in your internal network that are assigned to the Appliance. Segments listed in italic font are assigned to the parent folder; segments listed in plain font are statically assigned to the Appliance itself.
IP Addresses	IP address ranges associated with the segments assigned to the Appliance. If some segments are statically assigned to Appliances in the folder, this column indicates the remaining unassigned IP addresses.

The following tools are available in this pane:

Assigned Appliances	Use this search field to refine the table: Enter an Appliance name to locate its folder. Enter an IP address to locate the Appliance or folder that handles that network segment. Enter an Appliance folder to locate it in the tree.
Show child folder information	When this option is selected, the main table displays Appliances in sub-folders of the selected folder.
Assign	Assign segments to the Appliance you selected in the table.

Move	Move selected Appliances to another folder of the Appliance tree.

Static and automatic IP allocation

You can assign IP addresses to Appliances in two ways:

- Automatic IP Allocation: Assign segments to a folder. If the folder contains several Appliances, IPs in these segments are automatically assigned to available Appliances in the folder. Endpoint sessions are distributed proportionally based on each Appliance's licensed capacity.
- Static Allocation: Assign segments to a single Appliance. This Appliance handles endpoints in these segments. If this Appliance is part of a folder, it does not participate in automatic IP allocation.

  Note:

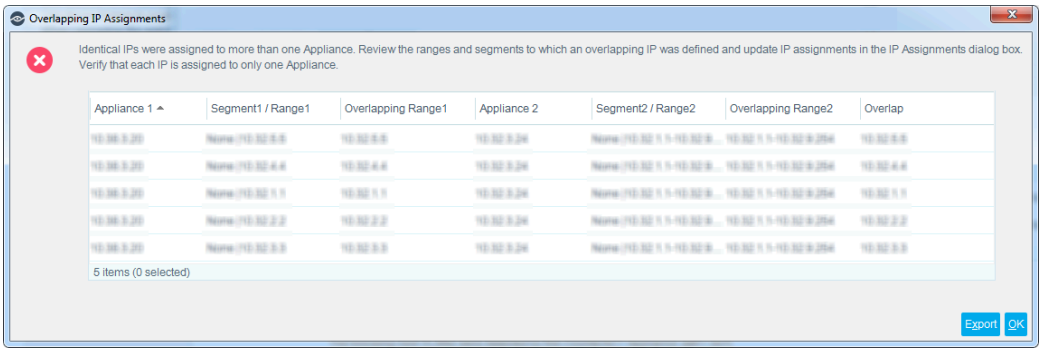
  IP addresses not assigned to a folder or Appliance are handled by the Enterprise Manager. The Enterprise Manager also handles IP addresses that are assigned to a folder that has no Appliances available.

Overlapping IP assignments

The Forescout eyeSight verifies that each network IP address is assigned to only one Appliance. This ensures, for example, accurate endpoint monitoring and policy execution.

If you mistakenly assign an IP address to more than one Appliance, the Console displays a table that lists the ranges and segments to which the overlapping IP address was defined, as well as the exact IP address ranges that overlap. Review this information and update IP assignments in the IP Assignment dialog box so that each IP address is only assigned to one Appliance. You can export the information in the table to a CSV file.

Networks can be intentionally configured with overlapping IP addresses, as in retail branches, Operational Technology environments, or merged corporate networks. You can enable support for these networks in the Internal Network. For more information refer to the Working with Overlapping IP Addresses How-to Guide. .

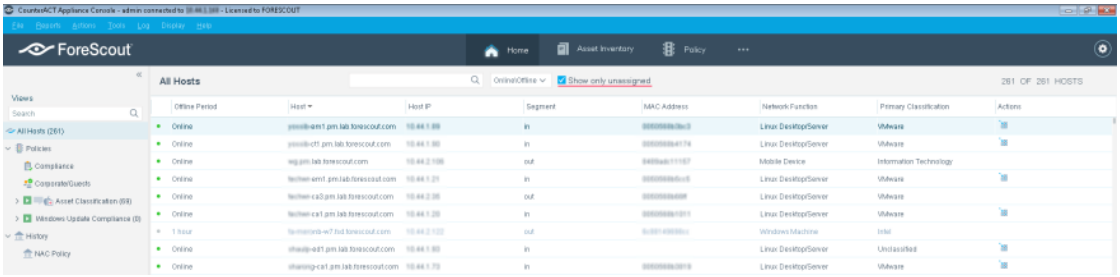


Note:

Although there is no limit to the total number of entries displayed in the Overlapping IP Assignments dialog box, a maximum of 10 overlapping ranges are displayed at any one time. To see any additional overlapping ranges that might exist, first resolve the overlap conflicts displayed in the table. Once resolved, additional ranges are displayed.

Unassigned IPs

When eyeSight eyeSight detects an endpoint with an IP address that is included in the Internal Network, but is not assigned to an Appliance, it generates an entry in the Event Log. These unassigned endpoints can be viewed in the Detections pane by selecting Show Only Unassigned.



Modify the Appliance Folders tree to assign the segment that contains the endpoint to an Appliance or folder. Forescout eyeSight can then connect to the endpoint. When there are no longer any unassigned endpoints, an entry in the Event Log indicates that all detected endpoints are assigned to an Appliance.

Conflicting configurations

When you configure Forescout modules and other components, you can define groups of Appliances that have the same configuration settings, as described in Configure Features for an Appliance or Group of Appliances.

In some cases, these configuration settings may conflict with the Appliance groupings you define in the Appliance Folders tree. For example, endpoint connection settings of the Endpoint Module may conflict with endpoint-handling settings of the Appliance Folders tree. A pop-up message notifies you of any conflicts when you save your Appliance Folders configuration. Review the two configurations applied to the Appliance to identify and resolve the conflict.

Additional Forescout eyeSight options

Work with the Forescout eyeSight internal network

The Internal Network is a set of network segments or IP ranges that defines your network in the eyeSight. When eyeSight eyeSight detects endpoints with IP addresses within the Internal Network, they are assumed to be in your network.

The Internal Network defines the extent of eyeSight management activity. For example, when a Forescout policy scope is defined as "All IPs," the policy is applied to all IP addresses in the Internal Network. Network segments that are part of your physical network, but are not included in the Internal Network definition, are not managed by Forescout products. In addition, endpoints in the Internal Network must be visible to Forescout Appliances.

Note:
From eyeSight Version 8.4, the Forescout Admin (REST) API provides you with automatic configuration capabilities for managing deployments on the eyeSight, where network entities, such as the segment tree and default groups ranges, can change on a daily basis. The Admin API allows you to integrate third-party network management IPAM (IP Address Management) tools, such as Infoblox and BlueCat, and ensures that segments defined on the eyeSight are synchronized with their latest IPAM database definitions. For more information, see Work with the Forescout Admin API in the *Admin API Plugin Configuration Guide*.

During installation, the Internal Network is defined when you run the Initial Setup Wizard. See Initial Setup Wizard – Internal Network for details.

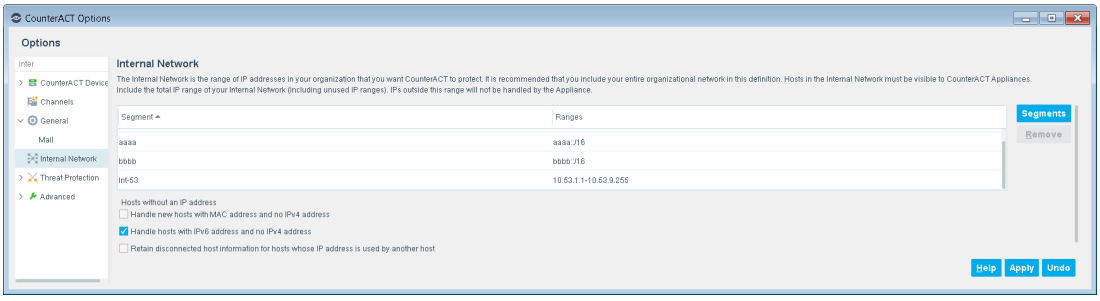
Administrators with appropriate permissions can use the Segment Manager tool to edit the segment definitions that define the Internal Network. See Working with Forescout Segments and Managing Users, Access to Console Tools – On-premises Permissions. For example, if your network expands, you typically:

- Use Segment Manager to define segments with your network's new IP addresses.
- Use the procedure described in this section to add these segments to the Internal Network

Several eyeSight tools use the segments that define the Internal Network. For example, you use these segments to assign sectors of your network to Appliances, to define the scope of a policy, and to define the active response range for Threat Protection features.

To configure the Internal Network, select Tools > Options > Internal Network.

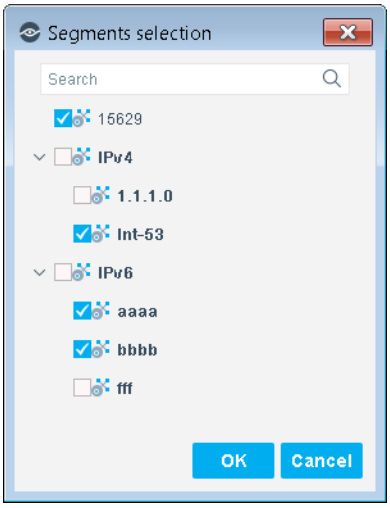
The main table lists segments that are part of the internal network.



The following options are available.

Handle new hosts with MAC address and no IPv4 address	When this option is enabled, the eyeSight detects and manages endpoints based on their MAC or IPv6 address when an IPv4 address is not available.
Retain disconnected host information for hosts whose IP address is used by another host	When this option is enabled, eyeSight retains previous authentication events for these hosts, and (depending on the relevant policy) do not require them to authenticate when they reconnect. This option is useful if you are working with guests or other hosts that frequently log in and out of the network.

To add segments to the internal network, select Segments. The full tree of segments defined in Segment Manager is shown.



Select and clear checkboxes to specify the segments that make up the Internal Network. Only the selected segments are included in the Internal Network. Select OK and the main table reflects any changes.

Work with hosts without IPv4 addresses

Optional settings let the eyeSight detect and manage endpoints based on their MAC or IPv6 address when an IPv4 address is not available.

This option is useful, for example:

- When a rogue device without an IP address is discovered by the network switch.
- When an IP address is discovered after the MAC address.
- If you want to create a white list of MAC addresses allowed to access your network. Create the white lists and then add them to policies. See Defining and Managing Lists for details.
- To detect IPv6-only endpoints in an IPv6 enabled environment.

Devices with no known IP addresses are presented in the Console with Layer 2 information only,

i.e., information related to the switch at which the endpoint is connected. When the IP address is discovered, and is part of the Internal Network, comprehensive endpoint information is displayed, along with the discovered IP address. If an IP address is later discovered, but that address is not in the Internal Network, the endpoint is still displayed in the Console with Layer 2 information.

Note:
When you enable these options, it is very important that the Internal Network definition includes all network segments that the eyeSight should be monitoring.

Not all host properties and actions are supported when only the MAC address is known for an endpoint. The following properties and actions can be performed on endpoints detected without an IP address:

- NIC vendor property
- All Switch properties

Manage Actions:

- Add to Group
- Add Value to List
- Recheck Host
- Set Device Criticality
- Delete Host
- Delete Properties

Audit Actions

- Send Message to Syslog

Notify Actions:

- Send Email

Restrict Actions:

- Switch Block
- Assign to VLAN
- 802.1X Plugin actions
- Wireless Plugin actions

Work with hosts whose IPv4 address Is used by another host

The eyeSight can retain host information on hosts that had an IPv4 address within the Internal Network but currently do not have one because another host obtained it. For example, if you are working with guest hosts that frequently log in and out of the network.

Selecting this option retains previous authentication events on these hosts, and (depending on the relevant policy) does not require them to authenticate when they reconnect.

Note:
Use the Last Known IPv4 address property to create conditions based on the previous IPv4 address.

Sign Forescout eyeSight emails with an S/MIME certificate

You can sign emails sent by the eyeSight using a digital certificate, as specified by the Secure/ Multipurpose Internet Mail Extensions (S/MIME) standard.

Note:
This does not include mails sent by the Forescout License Server (only relevant when operating in Per-Appliance Licensing), for example, mails sent regarding:- eyeSight eyeExtend license request and approval status.

Generate CSRs and import signed certificates

Use the Certificates pane to generate Certificate Signing Requests (CSRs) that are submitted to a Certificate Authority (CA). After the CA returns a signed certificate, use the Certificates pane to import the certificate.

After a signed S/MIME certificate is imported into Enterprise Manager, you can enable digital signing of email messages. For detailed information about defining and provisioning certificates, see The Certificates pane .

When you generate a CSR:

- In the Used for and Key Usage fields of the CSR wizard, specify that the certificate will be used for email signing.
- In the Email Address field, specify the email address of the Enterprise Manager that applies the digital signature to emails. When you install the signed certificate on the Enterprise Manager, emails are sent with this certificate and the email address configured in the certificate appears in the From field of the emails. The address should be meaningful, so that users can recognize that it comes from the Enterprise Manager.

Work with digitally signed emails in the Forescout eyeSight

When digital signatures are enabled, all emails sent by the eyeSight are signed using the S/MIME certificate. The body of the email is sent as clear text.

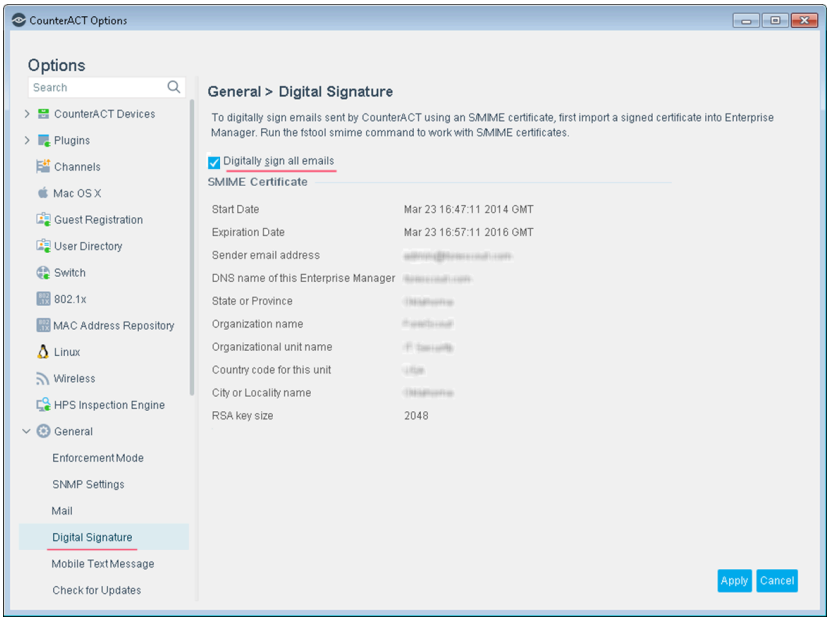
To work with digitally signed emails, select Tools > Options > General > Digital Signature. The tab shows data fields for the current signed certificate. Verify the certificate, then configure the following field. Restart the User Directory plugin to implement configuration changes.

Digitally sign all emails

When you enable this option, all emails sent by the eyeSight are signed using the S/MIME certificate. The body of the email is not encrypted. Restart the User Directory plugin if you change this setting.

Note:
The Windows Live Mail email client does not correctly display signed guest registration emails.

When this feature is enabled, the Enterprise Manager applies the digital signature to emails. Because of this, emails normally sent directly by the Appliance are routed through the Enterprise Manager.



Forescout eyeSight endpoint discovery rules

By default, eyeSight eyeSight automatically discovers information about endpoints, such as MAC addresses and NetBIOS names. This is referred to as endpoint property information.

Properties that are automatically discovered appear in the Home view, Detections pane, the Assets Portal and Reports.

By default, the following properties are discovered:

- Domain User names
- NetBIOS host names
- MAC Addresses
- DNS names
- Device Interfaces
- Basic User Directory Plugin properties. This plugin is bundled with the eyeSight.
- Switch Plugin properties This plugin is bundled with the eyeSight.

Additional properties may also be discovered by default, depending on the plugins installed. For example, if you installed the VPN Concentrator Plugin, related VPN properties are discovered.

You can use the Host Discovery feature to control properties automatically learned. You may need to do this to:

- Expand the information discovered at your network
- Limit the information discovered at your network
- Discover properties at specific network segments
- Discover properties at specific times or under specific conditions

Expand or limit the information discovered by default

You can update the default to include additional information, such as, properties that are only available via the policy (Nmap details) or properties that are discovered via plugins. See Base

Modules, Content Modules, and eyeExtend Modules and Policy Management for details.

Under certain circumstances, you may want to prevent discovery tasks on endpoints, where the information is not needed. You can use the host discovery wizard to perform this task as well.

Certain properties are learned regardless of the limitations defined in the Host Discovery tool, including:

- Properties learned passively by eyeSight eyeSight, such as admission events, MAC addresses, NetBIOS domain and host names, or open ports.
- Properties listed in policies.
- Properties displayed in Detections pane columns.

Note:
Limiting discovery does not impact the policy discovery mechanisms. If you choose not to discover certain properties via the Network Host Discovery Policy, they can still be discovered via the policy.

Note:
If you do not have a valid eyeSight license, you cannot add or edit endpoint discovery rules. If you do not have a valid eyeSight eyeExtend license, you cannot add properties supported by that license to discovery rules.

Set the Forescout eyeSight enforcement mode

You can choose to set up your system to work with either full enforcement or partial enforcement. The Full Enforcement mode allows for complete functionality, while the Partial Enforcement mode allows you to monitor network traffic but limits your ability to respond to it. Specifically, the Threat Protection, HTTP Actions, and Virtual Firewall options are turned off.

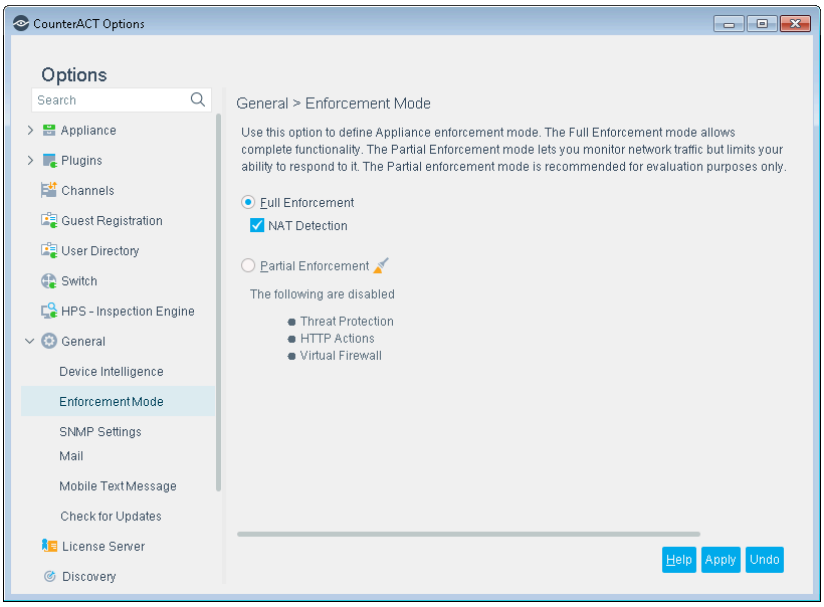
Note:
This mode is recommended for evaluation purposes only.

The Partial Enforcement icon is displayed on the status bar if your system is set to this mode.

The icon on the status bar may indicate that the eyeSight is running in Forced Partial Enforcement mode. This indicates there might be connectivity problems between the eyeSight and the network.

To set the Enforcement mode, select Tools > Options > General > Enforcement Mode and configure the following settings:

Full Enforcement	Enable this option to work with full Forescout functionality.
NAT Detection	Enable this option to detect NAT devices in your network.
Partial Enforcement	Enable this option to work with partial enforcement. Partial Enforcement lets you monitor network traffic but limits your ability to respond to it.



Backing up Forescout eyeSight system and component settings

Backup and restore procedures let you save Forescout device system or component settings and scheduled or saved reports. You can later restore them to the eyeSight device. This feature should be used in case of Forescout device hard drive failure or when data is lost for any other reason.

Endpoint events and your site structure (real and virtual endpoints) are not saved. The impact of losing this information is minimal, as the tool should be used in cases of hard drive failures and not to store endpoint and site information.

Note:
You must restore the same version of eyeSight as you backed up.

Note:
A remote recovery feature is also available. This feature lets you set up a comprehensive remote recovery system for Enterprise Managers that have failed as a result of a crisis, such as an earthquake or fire. See Recovering an Enterprise Manager .

You can schedule automatic backups of eyeSight system or component settings to a remote server, via FTP, SFTP, or SCP. Using scheduled backups provides extra safety and protection against hard drive failures and data loss.

If you are logged in to the Forescout Console via an Enterprise Manager, the Enterprise Manager and all registered Appliances are backed up to individual files.

You must first configure a backup server and an encryption password.

Forescout eyeSight system backups

The system backup feature saves all eyeSight device and Forescout Console settings. This data includes the following:

- Configuration
- License

- Operating System configuration
- Plugins/Modules

These categories include, for example:These categories include, for example:

- eyeSight IP address
- License information
- Channel
- Email
- Internal network parameters
- Basic and advanced NAC Policy definitions
- Legitimate traffic definitions
- Report schedules

Forescout eyeSight component backups

Component Backup is supported for the following components:

- Switch Plugin, Version 8.7.0 and above. When importing a backed-up Switch Plugin configuration (export_switch.xml), only those switch configurations that are both present in the export_switch.xml file and not listed in the Switch pane of the Console (Options > Switch) are imported. This is based on a comparison of switch IP addresses. Ensure the import of the complete Switch Plugin configuration backup by removing all configuration entries from the Switch pane, before performing the import.
- The Component Backup does not include the ACL Inventory in its backup of the Switch Plugin configuration.
- Wireless Plugin, Version 1.4.0 and above.
- Policies. Using the policy backup feature saves all policy-related data, including segment, condition and action information for each policy's rules and sub-rules. Policies are restored using the Policy import process. You cannot import a policy that has the same name as an existing policy. You must change the name of one of the policies for the import to succeed. You will be asked to enter the Encryption Password upon import.

Recover an Enterprise Manager

A eyeSight remote recovery tool offers a complete recovery system for restoring an Enterprise Manager that is no longer operational. This feature allows for the full management of Appliances from a remote Recovery Enterprise Manager after a failure.

Recovery Enterprise Manager sync status

You can monitor sync status and data synchronization between Enterprise Manager (EM) and Recovery Enterprise Manager (Recovery EM).

Note:
Once a Recovery EM is added, the dashboards configured on the EM will automatically sync to the Recovery EM.

There are three different Recovery sync statuses:

- In sync (Normal)
- Out of sync (Warning)
- Out of sync (Error)

A timestamp is available next to each status to indicate when the systems were last in or out of sync. The EM sends a Syslog message when its status changes.

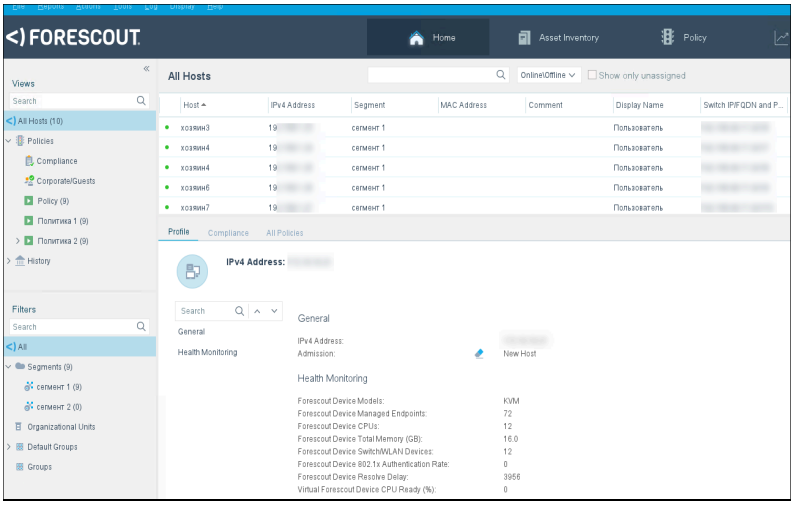
To view your Recovery EM sync status on the Forescout Console:

1. Go to Tools > Options > CounterACT devices > Recovery Enterprise Manager

To check your Recovery EM sync status via CLI, use fstool rem sync_status. See the Forescout CLI Reference Guide for more information.

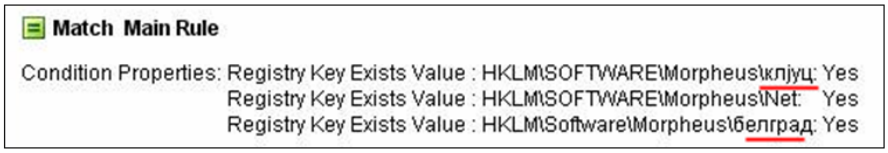
Language support

The eyeSight offers tools for language localization.



Display endpoint information in a local language

An extensive range of endpoint information can be displayed in other language character sets, such as user and host names, registry key information, file paths, and processes. This information is displayed in the required languages in the Console Detections pane, Details pane, Assets Portal, and in reports

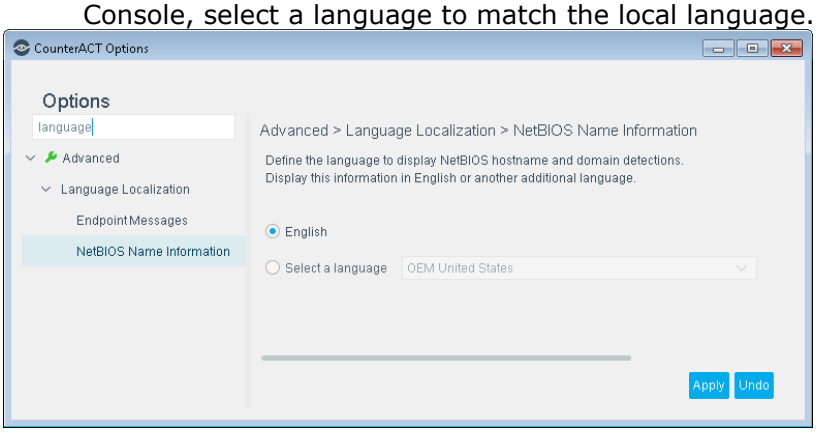


Display NetBIOS names and NetBIOS domains

The Console can display Microsoft Windows NetBIOS Names and NetBIOS Domains in a foreign language. The eyeSight resolves in the selected language and in English if both languages are detected.

Select Tools > Options > Advanced > Language Localization > NetBIOS Name Information, and then select a language or language set.

Note:
If Windows host names or Windows domain names appear as "######" (boxes) in the Console, select a language to match the local language.



Pre-registration and guest registration management

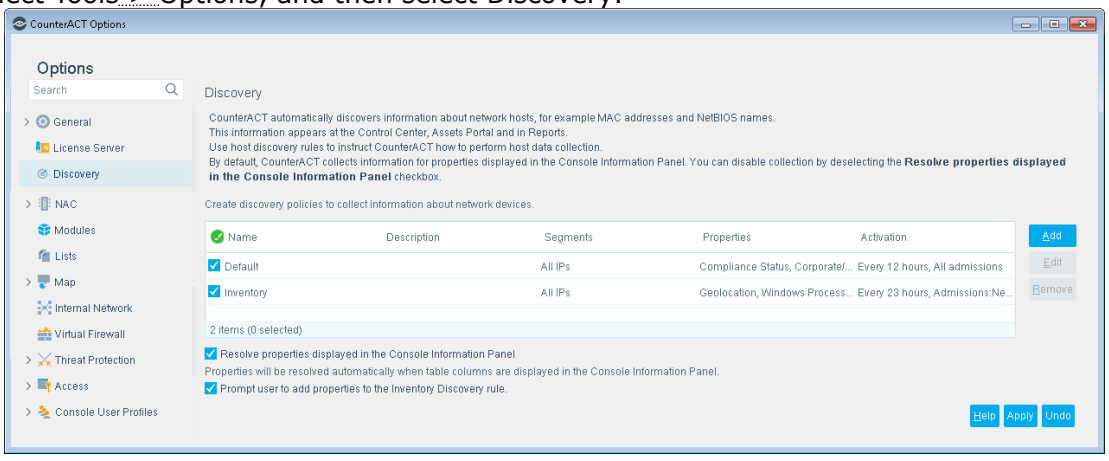
You may need to provide limited network and Internet access to company visitors, such as contractors, visiting professionals, and other network guests. You can use the HTTP Login action to detect, register and control network guests. Approved guest information is displayed in the Guest Management Portal and in the Guest Management Pane. In addition, you can manually add guests there and later verify that they are authenticated using the action.

Guest requests for access to your corporate network are generated when the HTTP Login action is manually applied to a detected endpoint or applied during a Forescout Corporate/Guest Control policy evaluation of detected endpoints.

Define endpoint discovery rules

To define discovery rules:

1. Select Tools > Options, and then select Discovery.

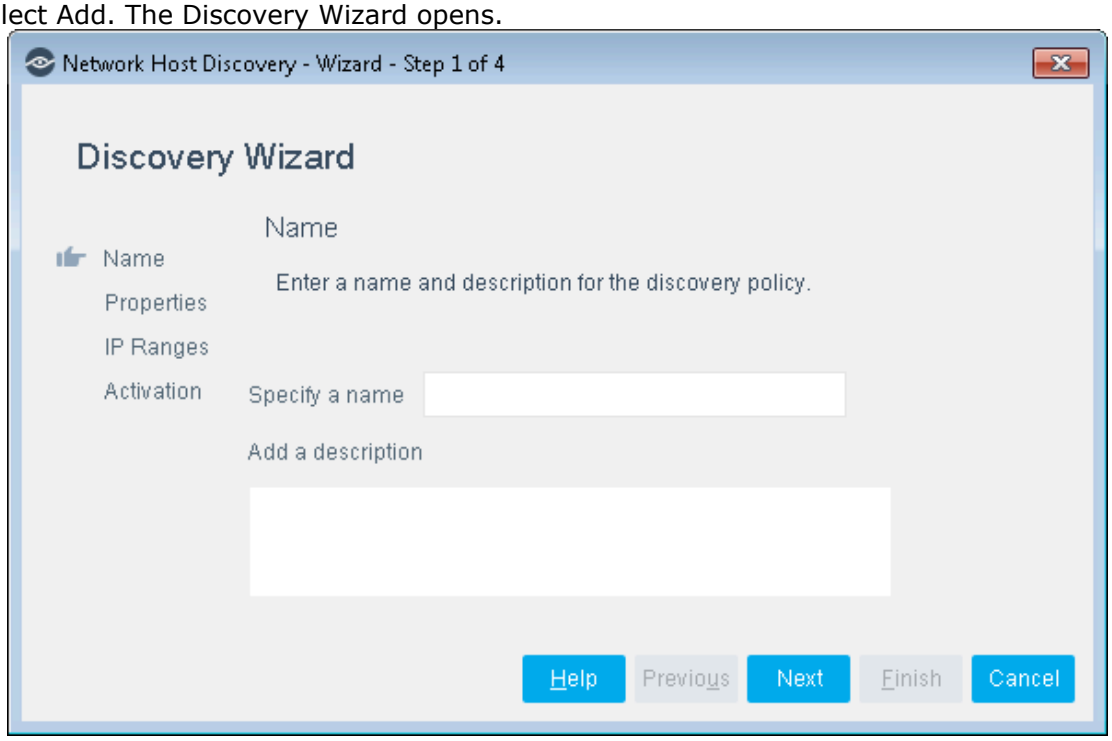


Note:
By default, Forescout eyeSight collects information for properties displayed in the Console table columns. You can disable this collection by clearing the Resolve properties displayed in the Console Detections pane check box.

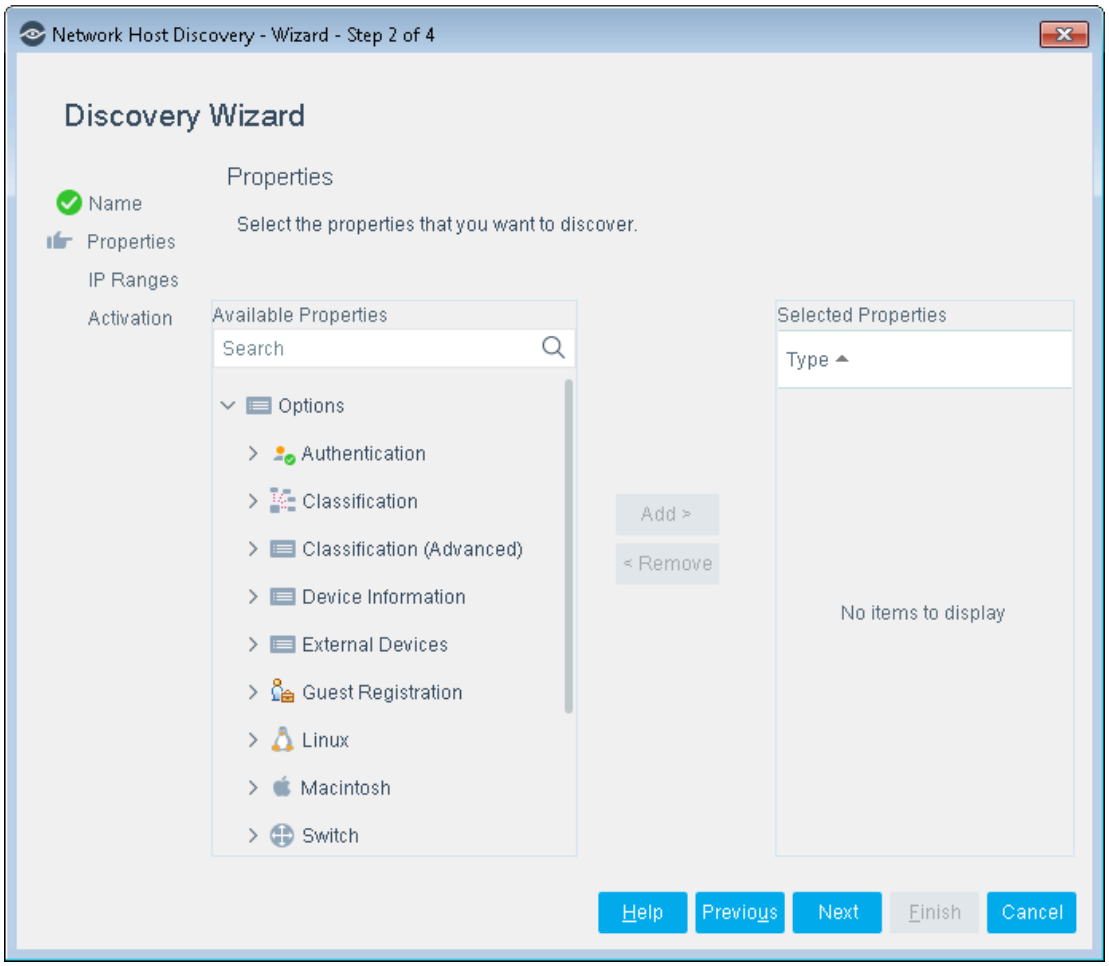
Note:

By default, the Console prompts users working in the Asset Inventory to add properties to the Inventory Discovery rule. You can disable this prompt by clearing the Prompt user to add properties to the Inventory Discovery rule check box.

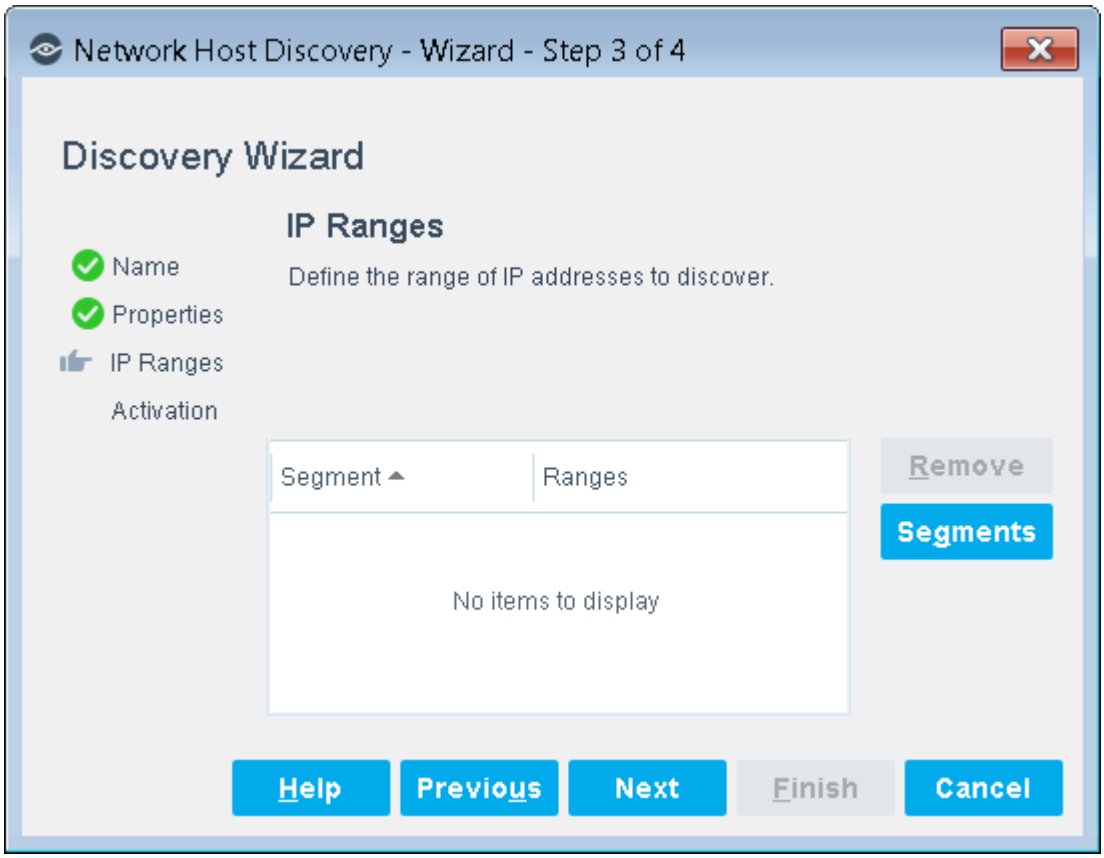
2. Select Add. The Discovery Wizard opens.



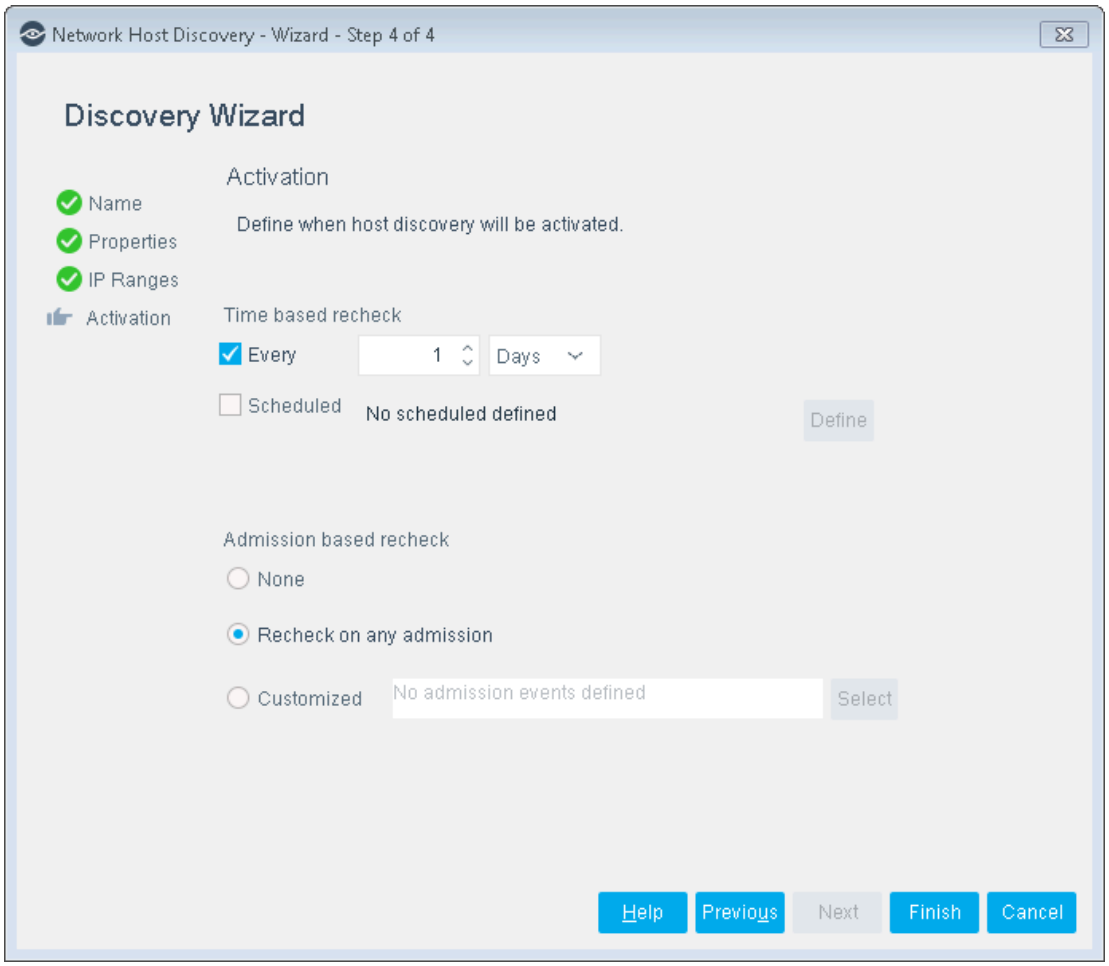
3. Enter a rule name and description, and then select Next.



4. Select the properties to be discovered, and then select Next.



5. Define the IP addresses to which to apply the rule.
    - Select Segments to add segments of the eyeSight Internal Network to the scope of the rule.
    - To remove a segment, select it in the table and select Remove.
6. Select Next.



Use the activation options to define when inspection is activated for this policy. For example, the Admission Event trigger is activated when a user joins the network. You can configure more than one trigger.

7. Select the activation events required to initiate endpoint evaluation.

Time Based Recheck	The policy is run at a certain date and time. Two options are available: Every: Select this option to run a policy at specific intervals. Short intervals are recommended, for example, if you want to check that a web or email service is consistently running, or if you want to verify the integrity of any other mission critical service in your network. Scheduled: Define a schedule for running the policy.
Admission Based Recheck	Three options are available: None: Do not inspect on the basis of an admission event.

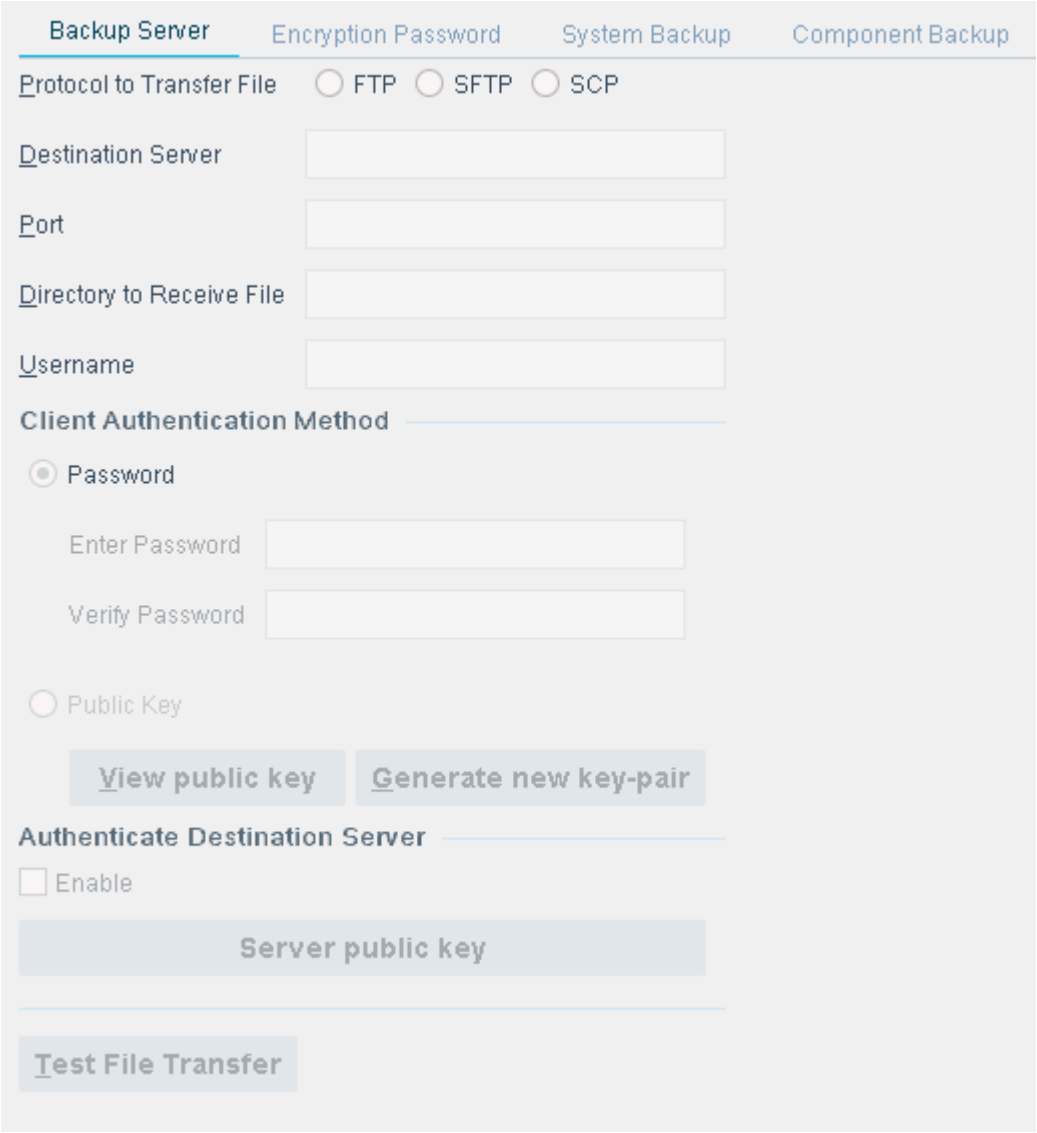
	Recheck on any admission: When any of the following admission events occur: An endpoint performed a DHCP request and then sends ARP request. An endpoint IP address was changed. A new endpoint was detected. An endpoint was connected to a switch port. Customized: Customize admission-based inspection. Select Define to customize the admission values. A delay time exists between the detection of Network Admission triggers and the onset of the policy evaluation. When an endpoint boots, the IP address is assigned quickly, before most of its services have loaded. Waiting 30 seconds (default delay time) increases the chances that the policy evaluation starts when more details could be learned about the endpoint (after all services have loaded). You can update the delay default time.

8. Select Finish.

Configure a Forescout eyeSight backup server

You should configure a backup server:

1. Select Tools > Options, and then select Advanced > Backup.



2. Select a protocol to use to transfer the backup file.
3. Enter transfer details, including the destination server, port, directory to receive the file, and the user name.
4. In the Client Authentication Method section, select one of the following authentication methods:
    - Password. Standard password authentication.
    - Public Key (SFTP and SCP only). The public key is used to establish the connection between the eyeSight device and the backup server in order to transfer the backup file to the server. A key-pair consisting of a public and private key is automatically generated during Forescout platform installation. The private key is protected by a passphrase. You can also generate a new key-pair by selecting Generate new key-pair.

      Note:

      Select View public key to view the key in OpenSSH (one-line) or RFC 4716 (SSH2) format. Key-pair information is shared with Recovery Enterprise Managers and High Availability eyeSight devices. You can view the status of the creation and transfer of each backup file in the Event Viewer. Only eyeSight users with update permissions for Backup can generate key-pairs.

5. (SFTP and SCP only) In the Authenticate Destination Server section, perform the following to validate the server used during the transfer of the backup file:
    a. Select Enable.
    b. Select Server public key. You must enter a destination server before selecting a key.
    c. In the Server Public Key dialog box, select Retrieve Key to retrieve the public key of the defined server. If you already have the key information, you can type/copy it into the dialog box.
    d. Select OK.
6. (Optional) Select Test File Transfer to verify connectivity.
7. Select Apply.

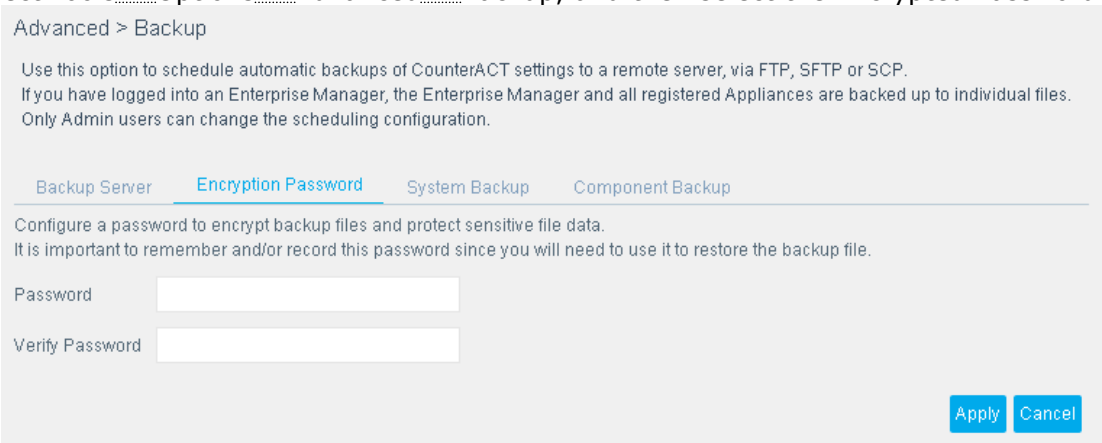
Configure a Forescout eyeSight encryption password

Both system and component backup files, backed up either manually or via a schedule, are encrypted using AES-256 to protect sensitive file data. To encrypt backup files, you must configure an encryption password. This password is mandatory and must be defined before backup configuration.

The encryption password is also used to encrypt files manually backed up via Tools > Options > CounterACT Devices. When backing up files using this method, you are requested to define a password if you have not previously done so.

To configure the password:

1. Select Tools > Options > Advanced > Backup, and then select the Encrypted Password tab.



2. Define a password. The password must be at least six characters long and must contain at least one digit and one letter.

    Note:
    Remember and/or record this password as you will need to use it to restore the backup file.

Perform a scheduled Forescout eyeSight backup

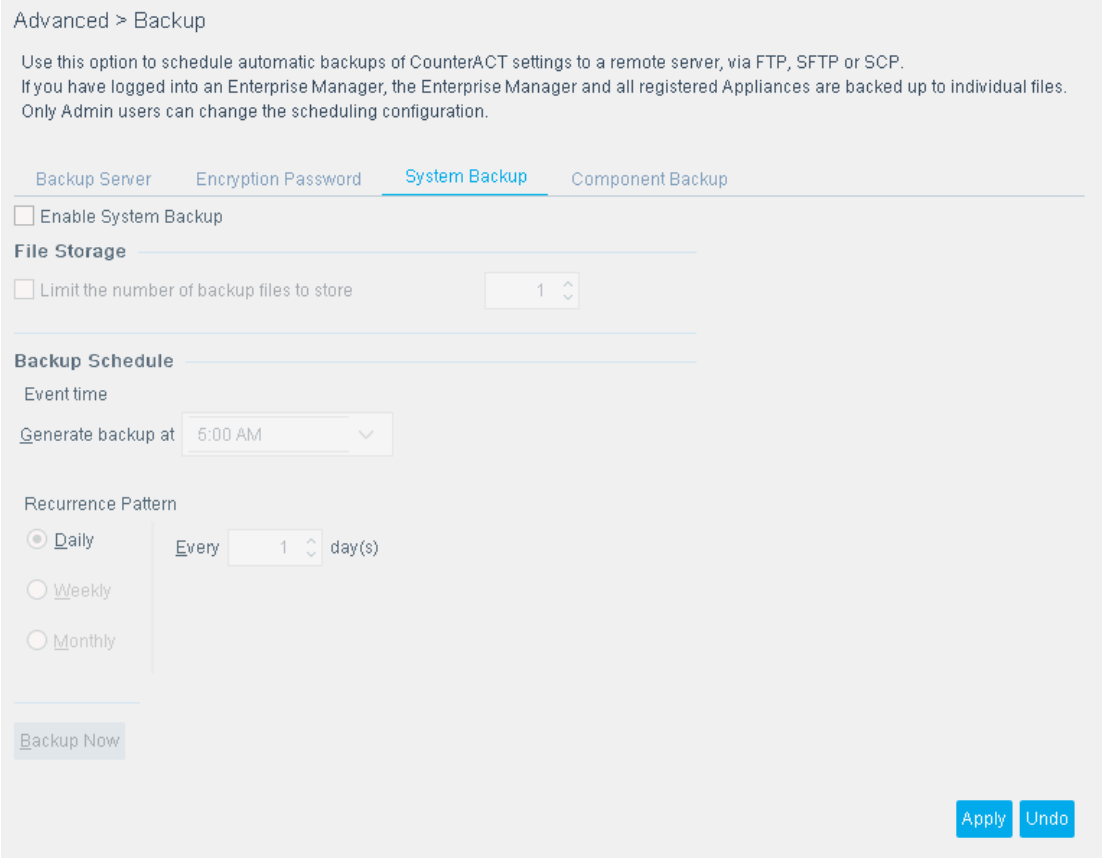
Use this procedure to schedule system and component backups.

Note:
To perform a scheduled backup, you must first configure a backup server and an encryption

password. See Configure a Backup Server and Configure an Encryption Password .

To schedule a backup:

1. Select Tools > Options > Advanced > Backup,
2. To schedule system backups, select the System Backup tab
3. To schedule component backups, select the Component Backup tab.



4. Configure the following settings.

Enable System Backup — When you enable this option backups are performed according to the schedule you define in this tab.

Enable Component Backup — When you enable this option backups are performed according to the schedule you define in this tab.

Limit the number of backup files to store — The maximum number of backup files that are retained.

The number of backup files stored is equal to the number you configure plus one additional backup file.

	If you reduce this value, existing backup files are not removed.
Maximum number of concurrent backups	The number of Appliances that can be backed up simultaneously. The maximum value is 100.
Generate backup at	Specify the time at which backups begin.
Recurrence pattern	The frequency with which backups are performed. Use the Every… field to configure a backup interval less that a week, but not daily.

5. Select Apply.
6. (Optional) Select Backup Now to perform a one-time backup to the defined server. The backup files are saved to the server defined in the Backup Server tab, in the following format:
   `EnterpriseManager_<EM_IP_Address>_<backup_index>.fsb`
   `<Appliance_IP_Address>_<backup_index>.fsb`

Perform a one - time Forescout eyeSight system backup

You can perform a one-time backup of eyeSight system settings. Before you perform a backup, you must configure an encryption password, which will encrypt the settings using AES-256 to protect sensitive file data. See Configure an Encryption Password for details.

To back up your system settings:

1. Select Tools > Options.
2. Select a component from the CounterACT Devices pane.
3. Select Backup. By default, the device name, Forescout eyeSight version number, date, and time make up the name of the backup file.
   Note:
   The backup file name can only contain alphanumeric characters. Special characters are not allowed (for example, $ % *).

Back up and restore the Forescout eyeSight site for your appliances

You may want to back up and restore your rSite – machines and open services currently learned by the Appliance. Because the Appliance continuously learns and maintains the rSite, this is recommended. You can use it, for example, to replace an Appliance.

Note:
This tool may only be used for a single version. You cannot back up the rSite from one version and restore to another.

To back up and restore the rSite:

1. Log in to the CLI of the device that contains the rSite that you want to back up.
2. Run the following command: `fstool set_property fs.backup.def config license os plugin site`

   Note:

   There is no need to restart the Appliance.
3. Perform backup and restore of the device.
4. To restore original backup behavior, run the following command: `fstool set_property fs.backup.def config license os plugin`

Rsite information is no longer included in backups.

Forescout eyeSight backup best practices

- Use scheduled backups to provide extra safety and protection against hard drive failures and data loss.
- Use a 3-2-1 strategy:
  - Keep at least 3 copies of your data
  - Store 2 copies on different storage media, such as CD or hard drive
  - Keep one copy of your data completely offsite
- Daily / Weekly / Monthly backup strategy:
  - 6 daily backups
  - 5 weekly backups
  - 12 monthly backups
- Calculate the total amount of offline storage needed:
  - 40 Appliances x 300 MB each = Around 12 GB
  - 2 Enterprise Managers x 3 GB each = Around 6 GB
- Back up before major changes

Localize redirected web pages and messages

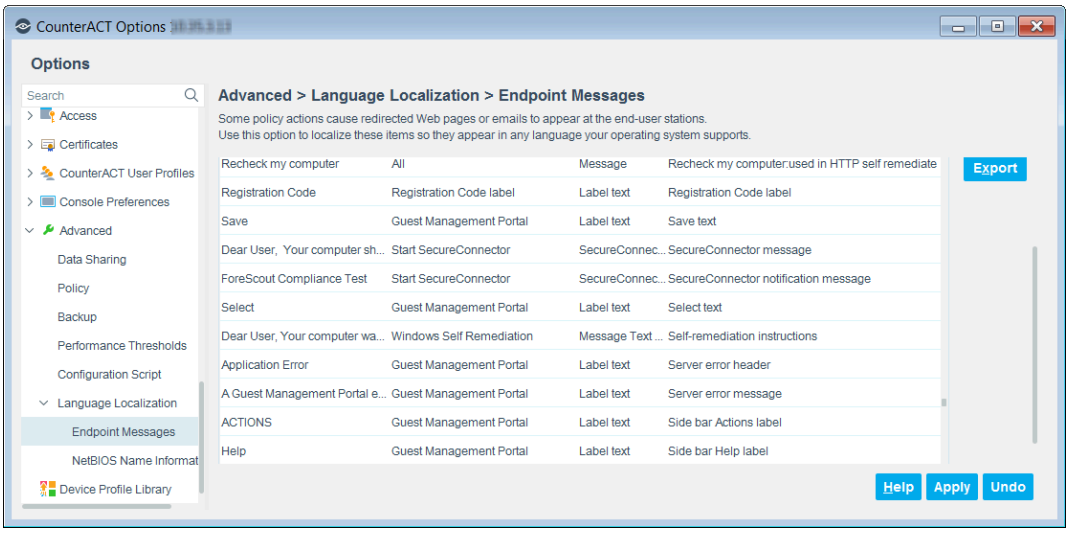
Some policy actions send web page messages and emails to endpoints. You can edit these messages or localize them so that they appear in any language your operating system supports.

The following message or end-user interaction pages can be localized:

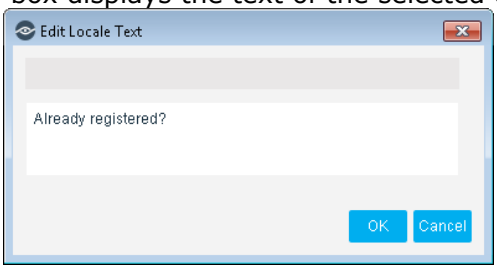
- HTTP Notification
- Windows Self Remediation
- HTTP Login
- Start SecureConnector
- Default Email Messages
- Guest Management Portal

To localize text:

1. Select Tools > Options, and then select Advanced > Language Localization > Endpoint Messages. The table lists text strings that are displayed in various interactions between the eyeSight and a detected endpoint.



2. In the search field of the Endpoint Messages pane, enter any portion of the text that you want to localize. The table displays all entries that include the portion of text, which you provided in the search field.
3. Select a table entry and then select Edit, or double-click a table entry. The Edit Locale Text dialog box displays the text of the selected entry.



4. Modify the text as needed.
5. Select OK.

   Note:

   Select a table entry and then select Default to return to the default text.
6. Select Apply. Your configuration changes are saved.

Display local languages in reports, actions, and other features

The eyeSight supports foreign text entered in reports, action, conditions and other features. No configuration is required to detect or display foreign language text.

The Forescout Research program

By default, your eyeSight devices share selected endpoint and system information with the Forescout Research Program.

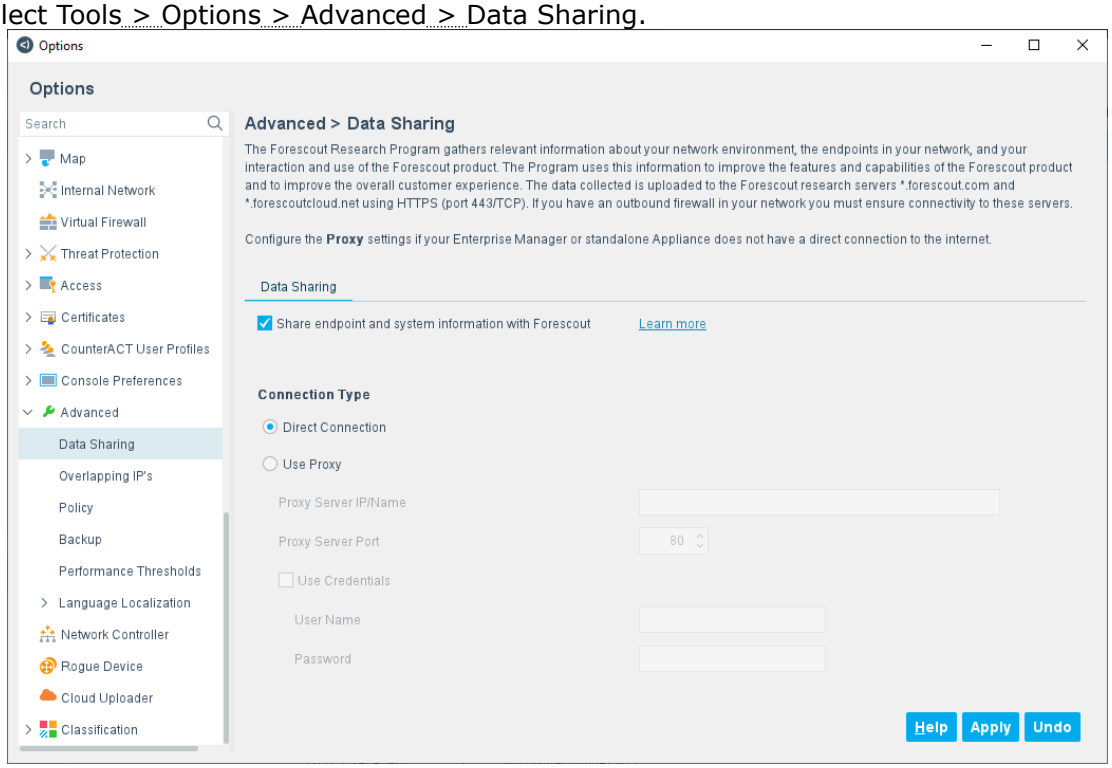
By opting into the Forescout Research Program, your shared data enables Forescout to provide a better security platform to its customers in the long term.

For more information about which data is uploaded and how the data is uploaded, refer to https://www.forescout.com/resources/forescout-research-program-terms-and-conditions/.

Note:
The Enterprise Manager connects to servers named `*.forescout.com` and `*.forescoutcloud.net` using HTTPS (port 443/TCP). Ensure that your firewall is configured to allow this or configure the proxy server settings.

To opt into the Forescout Research Program:

1. Select Tools > Options > Advanced > Data Sharing.



2. By default, your organization is opted into the program:
   - If your Enterprise Manager does not have a direct connection to the Internet, configure the Proxy settings in this window and also in the Cloud Uploader Configuration window. For information about the Cloud Uploader, see Configure and Test the Cloud Uploader in the *Cloud Uploader Configuration Guide*.
   - If you want to opt out, clear the Share endpoint and system information with Forescout option.
3. Select Apply.

If you opt out of the Forescout Research Program, Forescout does not upload any additional data, but data previously uploaded (prior to your opt-out) remains in the program unless you contact Forescout support.

If you need to delete previously uploaded data, contact Forescout support by following the instructions at this link: https://www.forescout.com/resources/support-services-maintenance-and-support-policy/

Manage Forescout eyeSight email notifications

Forescout eyeSight generates alerts/notifications about an assortment of platform processing conditions, including:

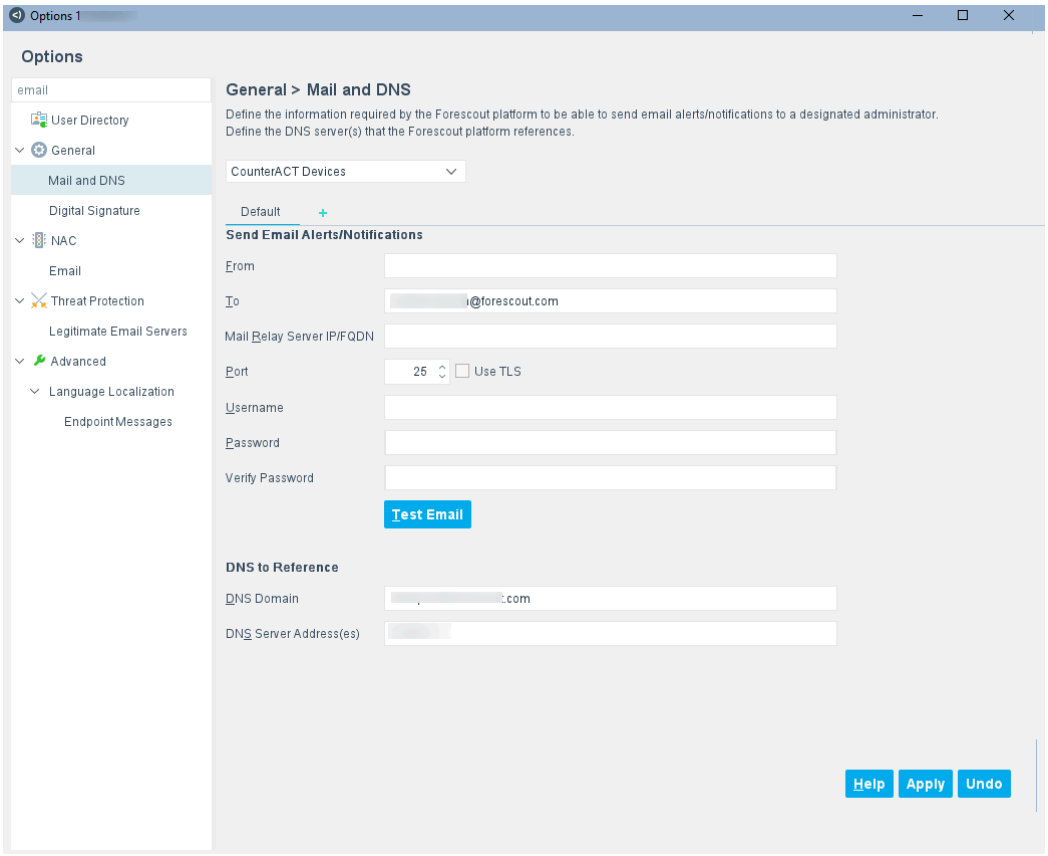
- When specific endpoint events, email worm events and service attacks occur. Not applicable to policy detections.
- License expiration warning notices
- System operation alerts

eyeSight sends these alerts / notifications, via email, to the recipient(s) that you designate.

While setting up an Appliance, you configured the following information in the Mail pane of the Console's Initial Setup Wizard – Mail):

- In the Admin Email field, you defined email address(es). These email addresses are your organization's administrator email address(es) to receive the alerts / notifications that eyeSight generates and sends via email.
- (optional) In the Mail Relay field, you defined the mail relay server to which the Forescout SMTP mail server must send its alerts/notifications. The mail relay server then routes these alerts / notifications to your organization's administrator email address(es)

In the Console's Mail and DNS pane, you manage (update) the options that the Forescout SMTP mail server uses to send its email alerts / notifications, including using SMTP user name /password authentication with TLS (secure communication:



Options are available to configure the mail options differently for different Appliances in your enterprise and to view different configurations per Appliance. See Configure Features for an Appliance or Group of Appliances.

Note:
Threat Protection policies can optionally limit the number of emails delivered to these addresses daily, and to define how many events are listed in each email.

To update the options used to send email alerts / notifications, select Tools > Options > General > Mail and DNS. Update any of the following fields:

From	(optional) In the From field, do any of the following: Enter the Forescout [sender] email address Clear the field of any entry to use the default, Forescout [sender] email address.
To	In the To field, modify the administrator email address(es) to receive the email alerts / notifications that Forescout eyeSight generates. This field must contain a minimum of one email address. Separate multiple addresses using any of the following characters: semicolon (;), blank space or comma (,).
Mail Relay Server IP/FQDN	(optional) If your organization's network security policy requires the routing of incoming email through a mail relay server, enter that server's IP address [IPv4/IPv6] or FQDN.
Port	(optional) In the Port field, modify the mail relay server's port number to which the Forescout SMTP mail server sends its email alerts / notifications. Default field values: 25 - when Use TLS is disabled 587 - when Use TLS is enabled
Use TLS	(optional) Enable/disable the Use TLS option. If enabled (selected), the eyeSight SMTP mail server uses TLS secure communication to send email alerts / notifications to the designated mail

	relay server. If disabled (not selected), the eyeSight SMTP mail server uses unsecured communication to send email alerts / notifications to the designated mail relay server.
Username	(optional) Enter the username that eyeSight uses to access the mail relay server.
Password	(optional) Enter the password that eyeSight uses to access the mail relay server.
DNS Domain	Enter either of the following: • The domain name of the DNS that eyeSight references • localhost
DNS Server Address(es)	(optional) Enter the IP address [IPv4/IPv6] of each DNS server that eyeSight references. Use spaces to separate multiple entries.

Note:
When you enable Use TLS for the sending of email alerts/notifications, you must configure the certificate authority trust chain of the designated mail relay server (Subsystem Trusted for = Send Mail) so that eyeSight can authenticate this server. Use the Console certificate interface to configure the required, certificate authority trust chain. See Configuring the Certificate Interface for information about working with the Console certificate interface.

Property configuration when using TLS to send email alerts/notifications (Option 1)

When Use TLS is enabled in the Console Mail and DNS pane, you must configure the eyeSight property `fs.mail.tls.verify.ocsp` in all your deployed devices (Enterprise Manager and Appliances) as follows:

1. In the Enterprise Manager, log in to the CLI.
2. If the target mail relay server's certificate authority (CA) uses the Certificate Revocation List (CRL) method, run the following fstool commands:
    - To configure the property for all Appliances:

      ```
      fstool oneach -R -c fstool set_property fs.mail.tls.verify.ocsp false
      ```

    - To configure the property for the Enterprise Manager:

```
fstool set_property fs.mail.tls.verify.ocsp false
```

By default, the `fs.mail.tls.verify.ocsp` setting is `false`, which instructs the Forescout eyeSight SMTP mail server that the target mail relay server's certificate authority (CA) uses the Certificate Revocation List (CRL) method.

3. If the target mail relay server's certificate authority (CA) uses the Online Certificate Status Protocol (OSCP) method, run the following fstool commands:
   - To configure the property for all Appliances:

     ```
     fstool oneach –R –c fstool set_property fs.mail.tls.verify.ocsp
     true
     ```

   - To configure the property for the Enterprise Manager:

     ```
     fstool set_property fs.mail.tls.verify.ocsp true
     ```

4. Restart the eyeSight `maild` service by running the following fstool commands:
   - To restart the `maild` service for all Appliances:

     ```
     fstool oneach –R –c fstool service maild restart
     ```

   - To restart the `maild` service for the Enterprise Manager:

     ```
     fstool service maild restart
     ```

   In the above `fstool oneach` command lines, the `–R` parameter ensures that the provided `fstool` commands (`set_property`, `restart`) are executed for the Recovery Manager, if your eyeSight deployment includes a Recovery Manager, in addition to all Appliances.

Property configuration when using TLS to send email alerts/notifications (Option 2)

When Use TLS is enabled and you do not want the eyeSight SMTP mail server's certificate authority (CA) to check the revocation status of presented system certificates (this means that, by default, presented system certificates are considered valid), then you must configure the eyeSight property `fs.mail.tls.no.check.revocation` in all your deployed Forescout devices (Enterprise Manager and Appliances) as follows:

1. On the Enterprise Manager, log in to the CLI.
2. Run the following `fstool` commands:
   - To configure the property for all Appliances:

     ```
     fstool oneach –R –c fstool set_property
     fs.mail.tls.no.check.revocation true
     ```

   - To configure the property for the Enterprise Manager:

     ```
     fstool set_property fs.mail.tls.no.check.revocation true
     ```

   By default, the `fs.mail.tls.no.check.revocation` setting is `false`, which instructs the eyeSight SMTP mail server's certificate authority (CA) to check the revocation

status of presented system certificates.

3. Restart the eyeSight `maild` service by running the following `fstool` commands:
   - To restart the `maild` service for all Appliances:

     ```
     fstool oneach –R –c fstool service maild restart
     ```

   - To restart the `maild` service for the Enterprise Manager:

     ```
     fstool service maild restart
     ```

   In the above `fstool oneach` command lines, the `–R` parameter ensures that the provided `fstool` commands (`set_property`, `restart`) are executed for the Recovery Manager, if your eyeSight deployment includes a Recovery Manager, in addition to all Appliances.

Handle Forescout eyeSight network connectivity failures

Resolve network connectivity failures between an Appliance and your enterprise network.

During installation, a connectivity test is performed to verify that packets are properly injected into the network and that eyeSight eyeSight sees symmetric traffic on the monitoring interfaces. For every session, both incoming and outgoing directions are visible. After installation, the test is run after configuration changes are made to the network (for example, NAC or Active Response range, Ethernet NIC, VLAN).

If this connectivity test is not successful, consider and check these possible reasons.

- A message indicates that the tool did not see enough TCP sessions to make a decision. By default, the test is run until it sees 250 TCP sessions, and (but) no longer than 15 minutes.
    - Configure the switch to mirror both incoming and outgoing traffic.
      Or
    - Verify that the correct port is mirrored.
- When all sessions are asymmetric, the mirroring port may be misconfigured so that only one side (incoming or outgoing) is mirrored. Configure the switch to mirror both incoming and outgoing traffic.
- Some asymmetric sessions are detected.
    -
      Or
    - There is an asymmetric routing of packets going in to and out of the containment cell. Mirror the other port that traffic is going through. This may require additional NICs (for example, if the other port is on a different switch or the bandwidth requirements of both ports exceed the mirror port capacity).
      Or
    - The wrong port is mirrored. Mirror the correct port.
      Or
    - The packet loss rate is high. Make sure the capacity of the mirroring port can accommodate the actual traffic of the mirrored ports. Both incoming and outgoing traffic should be accounted for. Use a higher capacity mirroring port (for example, gigabit) or mirror the incoming and outgoing traffic to different ports (and use an additional NIC).
      Or
    - Some of the traffic in one direction is encapsulated (tunneled). Either mirror traffic after it is de-encapsulated or mirror when both directions are encapsulated (and is ignored).
- Some traffic is tagged with VLAN IDs, which are not defined in the system. Number of "Wrong VLAN ID" packets detected is shown. Define proper VLAN IDs (Channel configuration) or instruct the switch to remove the VLAN ID while mirroring (if only one VLAN is mirrored).

Remote access to endpoints

eyeSight needs remote access to the endpoint's registry service to properly access service pack installations, antivirus installations, and perform other important tasks.

Authentication at the domain level allows the service to make local registry checks while running a remote scan. This allows the service access to additional information in system registry settings that otherwise would not be available. With this information, the service can perform more in-depth vulnerability assessments.

You should create a special domain account that is used by the service for Windows authentication. This domain account needs assigned privileges most suitable for use with the service, not the default privileges. Specifically, the domain account needs privileges that allow read access to remote registries and minimal domain access otherwise.

Remote registry read permissions are controlled by this key:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers\winreg
```

Various methods for setting this registry key on target endpoints are available. The available options depend on the Windows version running on the endpoints.

Define domain credentials

Troubleshoot domain credentials

Use these procedures to test and troubleshoot remote access to endpoints.

Use a domain-wide policy

This is the recommended option to enable remote access for Windows 2000 style domains.

This option is only available to Windows 2000-style domains that support ACL-level control through domain-wide registry policies.

1. Log in to the Domain Controller as Administrator.
2. Open the Active Directory Users and Computers MMC snap-in.
3. Create a new Global group called CA_scanners by selecting New and then Group from the User folder in the Tree tab.
4. Open the properties dialog box for the group.
5. Select the Members Of tab.
6. Remove the Everyone group by selecting Remove. The Members Of section should be empty.
7. Create a new user account called CA_account by selecting New and then User from User folder in the Tree section.
8. Add the new user account to the "CA_scanners" group.
9. Confirm that the user has no unintended permissions on the domain. For example, check the "Member of" section to confirm that it only has the "CA_scanners" group listed.
10. Open the "Domain Security Policy" MMC snap-in, and add the remote access key:
    a. Go to the "Registry" section.

b. Select "Add Key".
c. Add the following key:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\
SecurePipeServers\winreg
```

11. Select the new registry key by selecting Windows Setting and then Registry from the Tree tab.
12. Add the CA_scanners group, and set "Read" and "Execute" permissions only by selecting the read and execute checkbox.
13. Open the Set the Template Security Policy Setting dialog box to configure this key.
14. Select the Propagate inheritable permissions to subkeys option.
15. Select OK. The new registry-key ACL policy is propagated to all Windows endpoints participating in the domain (standalone endpoints are not affected in any way). The time it takes for this configuration to be propagated to endpoints may vary, depending on network configuration and traffic. To set the registry processing options:
16. Open the Group Policy MMC.
17. Select the Default Domain Policy, and then go the Group Policy section.
18. Select Default Domain Policy and then Computer Configuration, Administrative Templates, then System, Group Policy.
19. Set options in Registry Policy Processing Properties dialog box and the Group Policy Refresh Interval for Computers Properties dialog box. Be sure to select the Process even if Group Policy objects have not changed in the Registry Policy Processing Properties dialog box.

Use a Forescout eyeSight administrator group

You can create a new user account in the Global administrator group. This option may be used with Windows NT-style domains.

1. Log in to the Domain Controller as Administrator.
2. Create a new user account called "CA_account".
3. Make the CA_account a member of the Global group Domain Admins.
4. In the Member Of section of the group properties, keep only the Group Domain Admins and remove any other groups. The Global group Domain Admins should be used for access to remote systems as this group is automatically added to the Administrators Local group on each system when it becomes a member of the Windows NT domain.

Working with Windows XP SP2 machines

If your network includes endpoints that run under Windows XP SP2, you will need to change the Windows Firewall Settings so Forescout eyeSight can perform remote inspection on these machines.

To change firewall settings, you should have access to port 137 UDP and port 139/445 TCP, which is closed by default on XP SP2 machines. Allowing access means that Forescout eyeSight can retrieve Windows related information.

It is recommended to allow access from all eyeSight devices to each endpoint. This ensures that no matter where the endpoint is located, it is managed by the system. For example, if the user is roaming with a laptop, the device is properly scanned. To allow this kind of access, the firewall on each endpoint should allow connections from any of the devices.

Using the security configuration wizard

Windows Server 2003 SP1 provides a security configuration wizard to easily manage server lockdown and security settings.

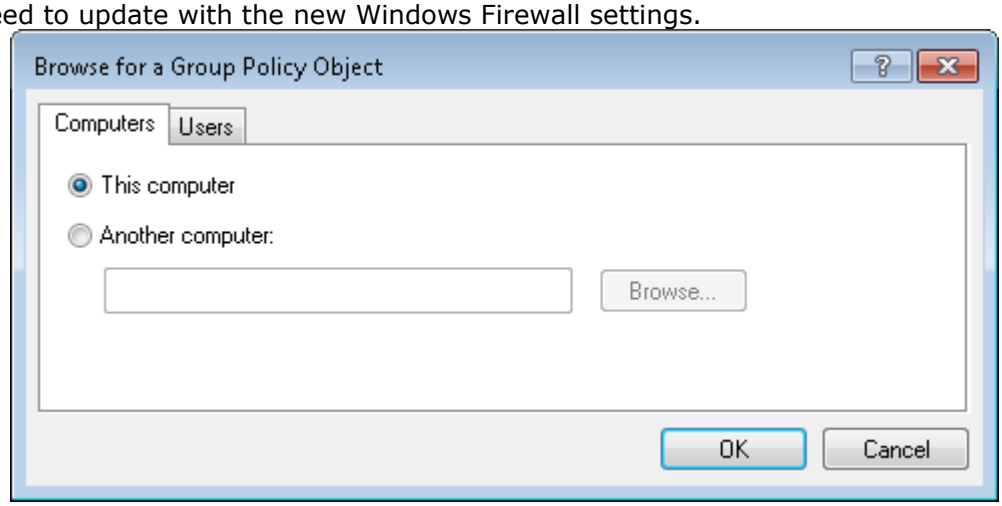
To be sure that the TCP ports used by the scanner for local security checks are available, verify that Remote Windows Administration is enabled in the Select Administration and Other Options.

Update group policy objects with new windows firewall settings

To update your Group Policy objects for network environments using Active Directory and Windows XP SP1, it is recommended that you use the Group Policy Management Console, a free download available from Microsoft. For more information, see *Group Policy Management Console with Service Pack 1*.

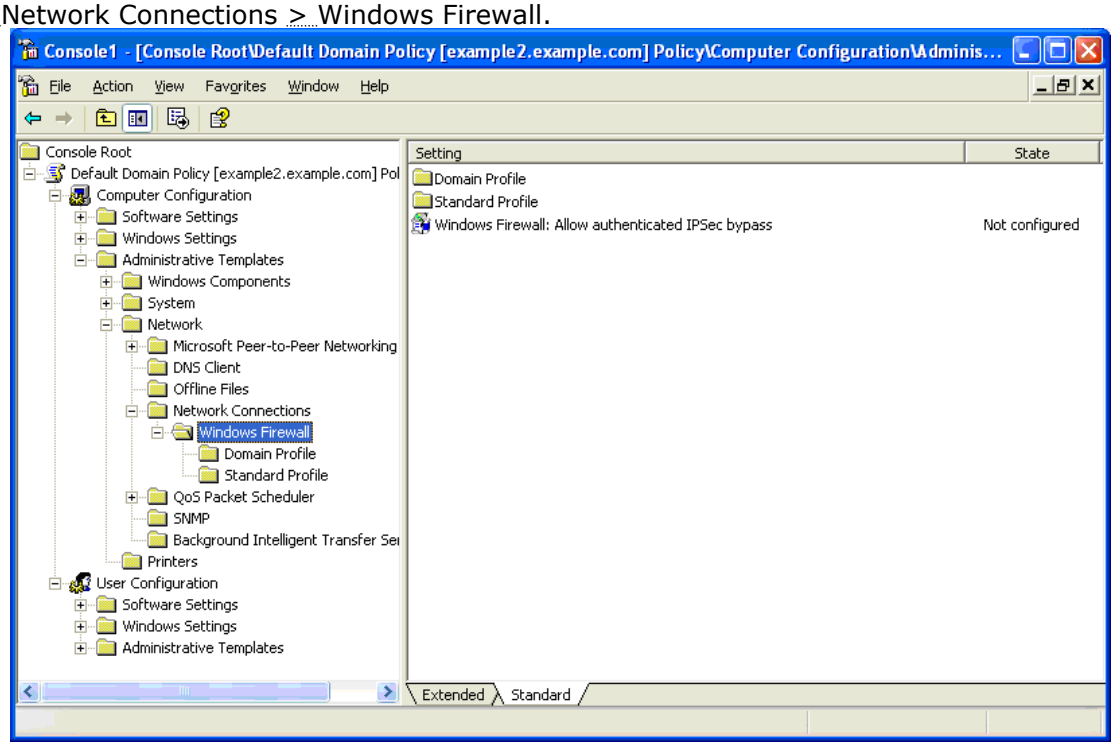
Update your Active Directory Group Policy objects with the new Windows Firewall settings using the Group Policy snap-in (provided with Windows XP SP2).

1. Install Windows XP SP2 on a computer that is a member of the domain that contains the computer accounts of the other computers running Windows XP on which you plan to install Windows XP SP2.
2. Restart the computer and log in to the Windows XP SP2 computer as a member of the Domain Administrators security group, the Enterprise Administrators security group, or the Group Policy Creator Owners security group.
3. From the Windows XP endpoint, select Start, select Run, enter mmc, and then select OK.
4. On the File menu, select Add/Remove Snap-in.
5. In the Standalone tab, select Add.
6. In the Available Standalone Snap-ins list, select Group Policy, and then select Add.
7. In the Select Group Policy Object dialog box, select Browse.
8. In the Browse for a Group Policy Object dialog box, select the Group Policy object that you need to update with the new Windows Firewall settings.



9. Select OK.
10. Select Finish to complete the Group Policy Wizard.
11. In the Add Standalone Snap-in dialog box, select Close.
12. In the Add/Remove Snap-in dialog box, select OK.
13. In the Console tree, select Computer Configuration > Administrative Templates > Network

> Network Connections > Windows Firewall.



14. Select Domain Profile, and then Windows Firewall: Define port exceptions.
15. Select Enabled.
16. Select Show.
17. Select Add.
18. Define the required rule. For example:
    `139:TCP:192.168.10.51:enabled:Port139ForCounterACT` would define a rule allowing the endpoint at 192.168.0.51 to access port 139 on WinXPSP2 computers in the scope controlled by this group policy.
19. Repeat steps 17 and 18 for additional rules.
20. Select OK.

Note:
A restart may be needed on the client machines in order for this definition to take effect.

Test domain credentials

Verify access to endpoints using the domain credentials configured for Remote Inspection.

Test the Domain Credentials

1. Log in to an endpoint using the eyeSight user name and password. If this fails, check the user settings on the Domain Controller.
2. Check that the endpoint is a member of the Domain and is authenticating against the Domain Controller.
3. Check that the login is using the Domain, rather than localhost credentials.

Test Endpoint Credentials Using a Localhost Query

4. Log in to an endpoint using any credentials other than the user. This endpoint should be a member of the domain.

5. Open a command window (Start>Run>"cmd").
6. Run the command: `C:\>net use \\127.0.0.1\C$ /user:<domain>\counteract`
    - <domain> is the fully qualified domain of the network.
7. The command should return the following: If this test fails:

```
Local name
Remote name \\127.0.0.1\C$
Resource type Disk
Status OK
# Opens 0
# Connections 1
The command completed successfully.
```

    - Check the domain syntax. It may need to be more fully qualified. For example, domain, domain.com or hq.domain.com.
    - Check the credentials on the Domain Controller.

Test Endpoint Credentials Using Remote Query

8. Log in to another endpoint that is also a member of the domain.
9. Open a command window (Start>Run>"cmd").
10. Run the command: `net use \\<IP_address>\c$ <password> /user:<domain>\counteract`
    - <IP_address> is the IP address of the target machine
    - <password> is the password for the user

      If this fails, perform the following tests:

Test the credentials on the endpoint using a localhost query

This test ensures that a query can be performed using the domain credentials.

1. Log in to an endpoint using any credentials other than the user. This endpoint should be a member of the domain.
2. Open a command window (Start>Run>"cmd").
3. Run the command: `C:\>net use \\127.0.0.1\C$ /user:<domain>\counteract`

   <domain> is the fully qualified domain of the network.

4. The command should return the following: If this test fails:

```
Local name
Remote name \\127.0.0.1\C$
Resource type Disk
Status OK
# Opens 0# Connections 1
The command completed successfully.
```

    - Check the domain syntax. Perhaps it needs to be more fully qualified. For example, domain, domain.com or hq.domain.com.

- Check the credentials on the Domain Controller.

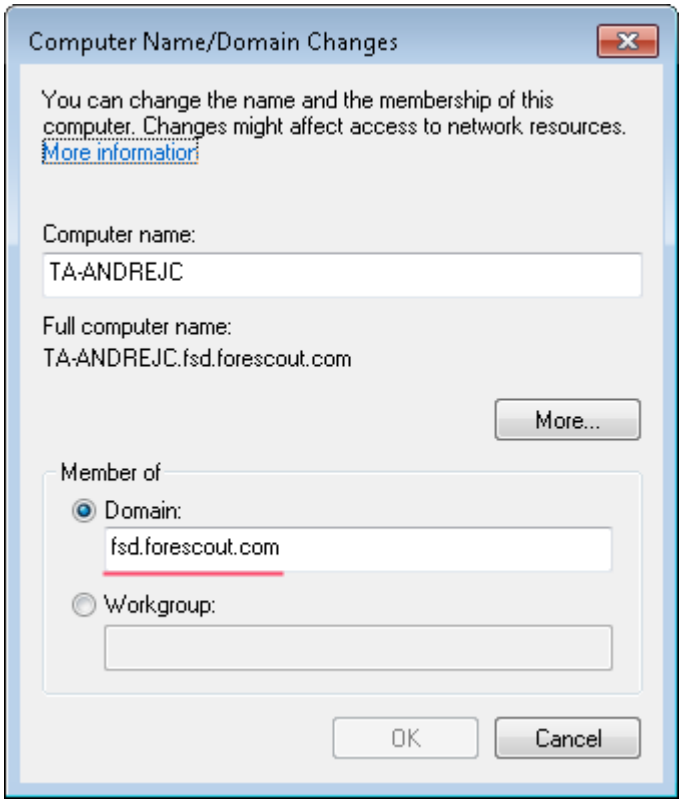
Test the credentials in the endpoint using remote query

1. Log in to another endpoint that is also a member of the domain.
2. Open a command window (Start>Run>"cmd").
3. Run the command: `net use \\<IP_address>\c$ <password> /user:<domain>\counteract`
   - <IP_address> is the IP address of the target machine
   - <password> is the password for the user

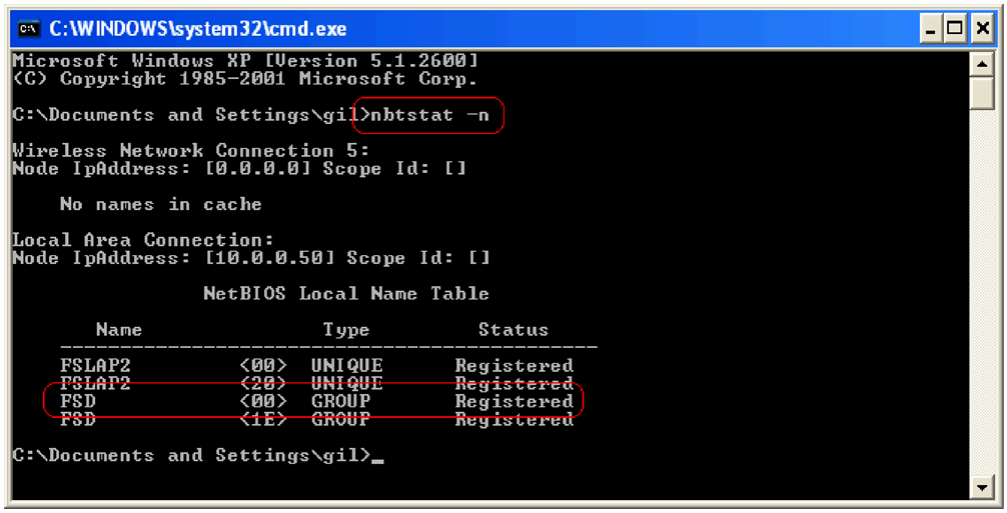
   If this fails, perform the following tests:

Domain configuration test

1. Open the System dialog.
2. Select Start, select Run, enter rename this computer, and then press Enter.
3. Set the domain configuration – in the <Computer_Name> tab, select Change. Verify that the machine is a member of the domain and that the domain is spelled correctly.



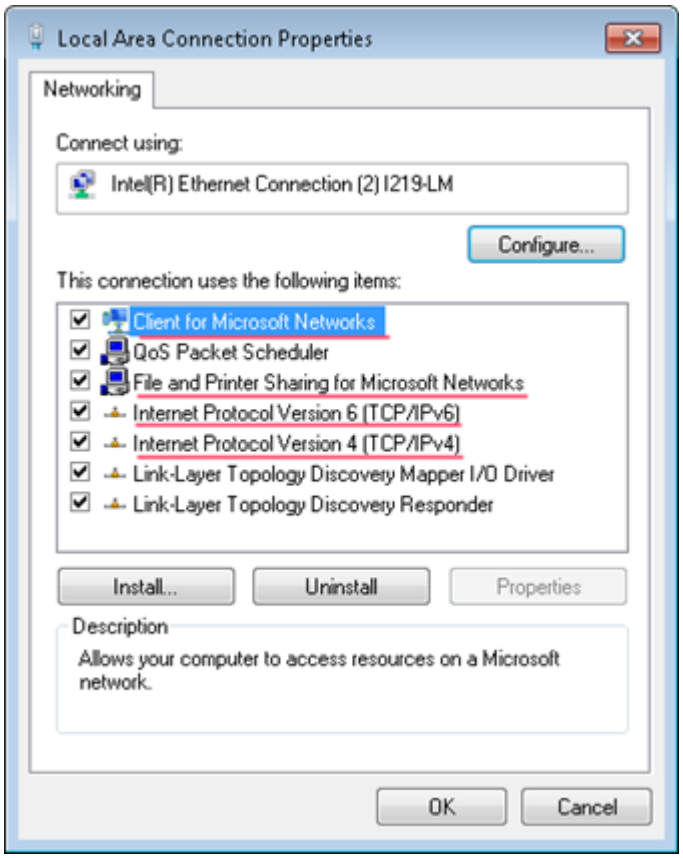
4. Verify that the NetBIOS domain name is identical to the one configured in the Host Properties Scanner Plugin configuration pane. This is done by running the command `nbtstat -n`, which should produce the following output.



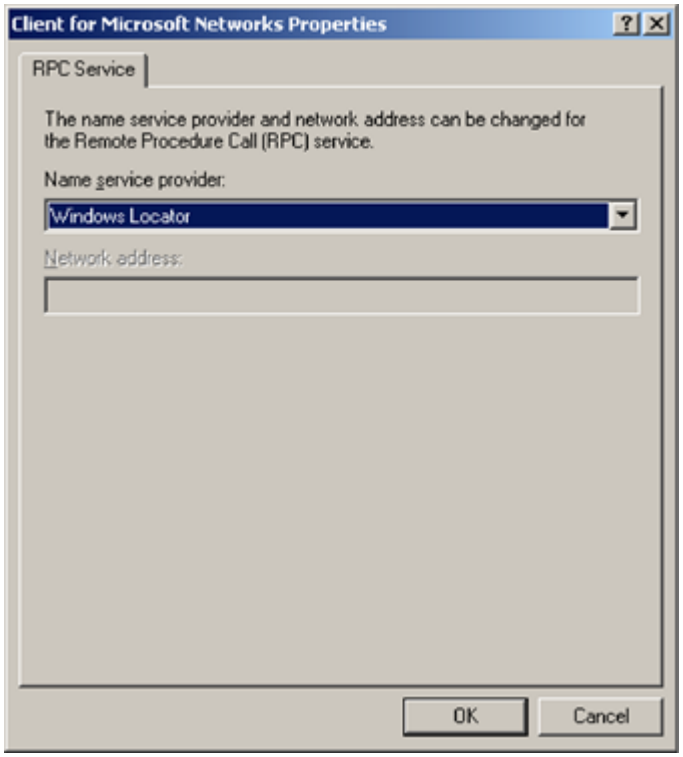
TCP/IP configuration test

Open the properties dialog box of the relevant network connection.

1. Select Start Control Panel Network and Internet View Network Status and Tasks > Change adapter settings, and right-click the Local Area Connection.
2. Select Properties. The following components should be installed (marked in red in the figure below):
    - Client for Microsoft Networks.
    - File and printer sharing for Microsoft network.
    - Internet Protocol Version 4 and Version 6 (TCP/IPv4 and TCP/IPv6).



The "Client for Microsoft Networks" should be configured as follows:



Forescout eyeSightport setup test

The Forescout eyeSight should have access to either one of the following ports: 139/TCP, 445/TCP.

Group policy test

In a Windows XP group policy, the domain can be configured to set the end-system's personal firewall settings. For more details, see Working with Windows XP SP2 Machines.

Local configuration of the firewall

Allow monitored network connections:

1. Select My network > Properties > Change Windows Firewall Settings > Exceptions > File > Printer sharing. Ports TCP 139 and TCP 445 should be set.
2. Select Change Scope, then add the device IP address to the Custom List.

Disable the firewall

For testing purposes, the firewall can be disabled.

1. In the Advanced tab, select Setting from the Windows Firewall group.
2. Disable the firewall by turning it off.

NetBIOS over TCP/IP setup test

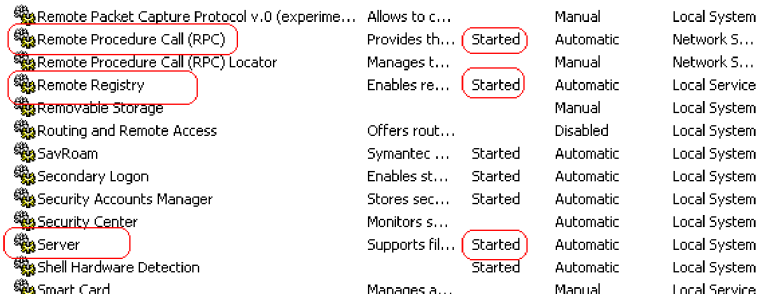
NetBIOS over TCP/IP should be enabled either directly or from the DHCP server. Verify that either the Default or Enable NetBIOS over TCP/IP option is selected.

Services test

Verify that the services listed in step (circled in red) are running.

To verify:

1. Open the services view by selecting Start > Control Page > Administrative Tools > Services. Verify that the following services (in red) are running:
    - Remote Procedure Call (RPC)
    - Remote Registry Service
    - Server



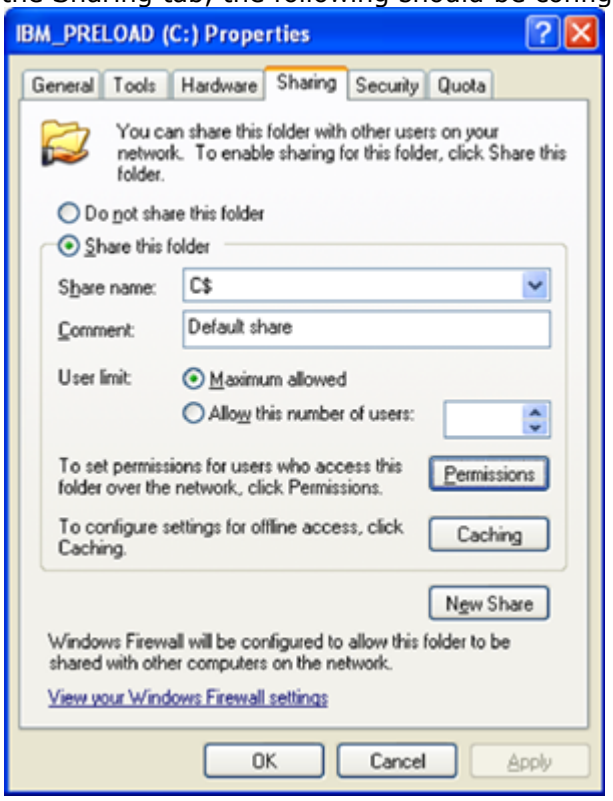
2. If a service is not running, right-click it and select Start to start it.

Shares test

Verify that the default c$ share exists.

To verify:

1. From My Computer, right-click drive "C" and select Properties.
2. In the Sharing tab, the following should be configured:



Troubleshooting deep inspection

Perform these additional checks if you cannot perform deep inspection on supported Windows endpoints.

- For Windows Vista machines, verify that Vista UAC is disabled. For more information see http://www.petri.co.il/disable_uac_in_windows_vista.htm.
- Verify that the following services are enabled: Remote Procedure Call, Server Service, and Remote Registry Service.
- Verify that File & Print Sharing for Microsoft Networks (connection properties) is installed.
- Verify that you have domain-level administrative privileges on each computer being scanned or that you are a member of the Domain Admins Group. This group allows writing to the file system but not to the registry.
- If your network includes endpoints that run under Windows XP SP2, you can change the Windows Firewall Settings so that Forescout eyeSight eyeSight can perform remote inspection on these machines. This means that you should have access to port 137 UDP

and port 139/445 TCP. Allowing access means Forescout eyeSight can retrieve Windows related information. By default, these ports are open on Windows 2000 machines.

- Verify that you have cleared Use Sharing Wizard for the endpoint (for XP systems only.
    1. Double-click My Computer.
    2. Select Folder Options from the Tools menu.
    3. Select the View tab.
    4. Clear the Use Sharing Wizard option and select OK.

Configure HTTP redirection

HTTP Redirection reroutes an HTTP request made by a user to the Appliance for a notification, login, or remediation interaction.

By default, the redirection is sent to the management IP address of the Appliance. In an environment where the management network and the general network are separate you must change this default behavior, or the redirection will fail. To address this situation, a different network card needs to be connected to the network and assigned an IP address so it can process the redirection requests. Unless it is connected to a trunk port on which it handles multiple VLANs, the injection interface can be used for this purpose.

After these changes are applied, the Appliance has IP connectivity to both the general-purpose network and to the isolated management network. Several measures are in place to prevent the Appliance from connecting the two networks:

- The Appliance is configured to not route traffic (net.ipv4.ip_forward = 0). This attribute is monitored periodically, and is reset if found in the wrong state, so as to avoid mistakes made manually.
- The Appliance built-in firewall blocks all forwarding (FORWARD chain policy is DROP). This is also monitored periodically and reset if found in the wrong state.

To enable HTTP Redirection, which reroutes HTTP requests made by users to the Appliance for notification, login, or remediation interactions, follow these configuration steps:

1. Connect a NIC other than the one used for management to the general-purpose network. If the injection interface is not configured to handle VLANs on a switch trunk port, it can be used for this purpose.
2. Configure the NIC with a proper IP address and default gateway by using the `fstool netconfig` command.
3. Test connectivity to and from Forescout eyeControl by pinging various addresses in the network. Invoke the `fstool fw` command to temporarily allow outgoing ICMP traffic prior to these tests.
4. Configure Forescout eyeControl to redirect HTTP requests to the new address by using the following command: `fstool set_property http.server.ip.address <Address>`
5. Restart the Appliance services by using the `fstool service restart` command.
6. Verify that HTTP redirection works with the new address by applying a proper policy rule to an IP address inside the general network.
7. Verify that connectivity with the management station has not been lost (for example, using the device).
8. If you are logged on to a single Appliance:
    - For the Appliance, HTTP redirection can be performed using DNS names, and not just IP addresses. This is desired if a security certificate has been obtained and installed on the Appliance (for more information about certificates see The Certificates pane .
    - The system redirects using the DNS name of an Appliance if its IP address (reversibly) resolves to a name, and the name (forwardly) resolves to the IP address. This behavior can be controlled by setting the fs.redirect.dns.enabled property:

      ```
      fstool set_property fs.redirect.dns.enabled truefstool service restart
      ```

The default setting for this property is false (i.e., redirection using DNS names is not performed).

Sample fstool netconfig Session

Note:
The `fstool netconfig` command supports IPv6 address format.

```
fstool netconfig

fstool netconfig


 CounterACT Machine Network Configuration Options:
 1) Configure network interfaces
 2) Configure default gateway
 3) Restart network service
 4) Quit
 Choice (1-4) : 1


 ------------------------------------------------
 CounterACT Machine Network Interfaces Configuration
 ------------------------------------------------
 eth0 Address: 10.0.4.214 Netmask: 255.255.255.0*
 eth1 Address: unassigned*
 eth2 Address: unassigned*
 eth3 Address: unassigned
 (E)dit,(A)dd VLAN,(D)elete VLAN,(B)ack,(H)elp : e


 Choose interface to configure:
 1) eth0 Address: 10.0.4.214 Netmask: 255.255.255.0
 2) eth1 Address: unassigned
 3) eth2 Address: unassigned
 4) eth3 Address: unassigned
 Choice (1-4) : 2


 IP address for eth1 ('none' for no address) : 1.2.3.4 eth1 network mask
 [255.255.255.0] :
 Update eth1 configuration? (yes/no) : yes
 Updating /etc/sysconfig/network-scripts/ifcfg-eth1...
 Network service should be restarted for changes to take effect.
 Restart network service? (yes/no) : no (do it later)


 ------------------------------------------------
 CounterACT Machine Network Interfaces Configuration
 ------------------------------------------------*
```

```
eth0 Address: 10.0.4.214 Netmask: 255.255.255.0*
eth1 Address: 1.2.3.4 Netmask: 255.255.255.0*
eth2 Address: unassigned*
eth3 Address: unassigned
(E)dit,(A)dd VLAN,(D)elete VLAN,(B)ack,(H)elp : B


CounterACT Machine Network Configuration Options:
1) Configure network interfaces
2) Configure default gateway
3) Restart network service
4) Quit
Choice (1-4) : 2


Default gateway IP address [1.2.3.5] : 1.2.3.5
Default gateway set to 1.2.3.5.Apply change now? (yes/no) : yes
Change applied.
Press ENTER to continue
CounterACT Machine Network Configuration Options:
1) Configure network interfaces
2) Configure default gateway
3) Restart network service
4) Quit
Choice (1-4) : 3


Restart network service? (yes/no) : yes
Restarting network service...
Shutting down interface eth0: [ OK ]
Shutting down interface eth1: [ OK ]
Setting network parameters: [ OK ]
Bringing up loopback interface: [ OK ]
Bringing up interface eth0: [ OK]
Bringing up interface eth1: [ OK ]
net.ipv4.ip_forward = 0
net.ipv4.conf.default.rp_filter = 1
kernel.sysrq = 0
kernel.core_uses_pid = 1
Done restarting network service


CounterACT Machine Network Configuration Options:
1) Configure network interfaces
2) Configure default gateway
3) Restart network service
4) Quit
```

```
Choice (1-4) : 4
```

SNMP support and integration

The Forescout eyeSight hosts an SNMP service. SNMP functionality is supported in IPv4, IPv6, and dual stack device configurations.

The local SNMP service provides the following SNMP support:

- Standard MIBs over SNMPv1, SNMPv2c and SNMPv3
- Trusted notifications using SNMPv3 with USM traps and INFORMs
- SNMPv3 with:
  - Rich authentication (MD5 or SHA-1)
  - Encryption (AES-128 or DES)
  - View of the MIB tree via industry standards

The Forescout eyeSight uses the Net-SNMP suite to support most SNMP functionality. More information about Net-SNMP is available at http://www.net-snmp.org/.

Configure SNMP service settings

Configuration tools for the SNMP Service are based on the configuration model of the View Based Access Control Module (VACM).

The VACM was defined as part of SNMP v3, and is widely supported for SNMP v1/v2 interaction. It provides settings to control user access privileges and to define trap targets and behaviors.

To configure SNMP Service settings, select Tools > Options > General > SNMP Settings.

You can configure different SNMP service settings for groups of Appliances. See Configure Features for an Appliance or Group of Appliances.

Note:
During initial configuration, it is recommended to define the properties in the SNMP Settings tabs in the order in which they appear. For example, it is recommended to define Views before you define Users.

The SNMP Settings pane provides a subset of the most useful settings supported by the VACM model, organized in the following tabs:

General	Enable and disable the SNMP service, and import or export service settings.	
	Run SNMP service	Start and stop the SNMP service on configured devices. When the service is enabled, the firewall on the eyeSight device automatically opens. **Note:** You need an SNMP Engine ID for sending SNMPv3 traps. The Forescout admin user can manually edit or automatically reset the Engine ID to generate a new value.

	Disable TCP timestamps	TCP timestamps are enabled by default. Disable TCP timestamps to prevent attackers from learning system uptime. Disabling these timestamps also prevents system administrators from using this information.
	Import Settings to Console	Import an SNMP conf file. The SNMP Settings pane reflects imported settings. See Import SNMP Service Settings.
	Export Console-Based Configuration	Export current settings to a file. See Export SNMP Service Settings.
	Export Forescout MIB	Export the MIB used by Forescout devices. See SNMP MIB for appliances.
Views	Define and manage inbound Views that restrict user access to the Forescout MIB.	
Users	Define and manage inbound users that can access the Forescout MIB.	
Traps	Define and manage targets that receive outbound traps from the Forescout SNMP service.	
Active Traps	Enable and disable traps defined in the SNMP service.	

Import SNMP Service Settings

Use this procedure to import SNMP service settings from an SNMP `.conf` file. Imported settings overwrite the current settings of the SNMP Settings pane of the Console. After import, the Console-based configuration of the SNMP Settings pane reflects the settings of the imported file. You can use this imported configuration as the basis for further customization.

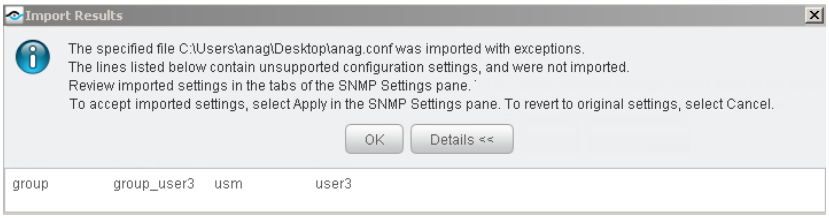
Note:
SNMPv3 Authentication/Privacy credentials will not be imported and must be added manually after the import. SNMPv3 traps will not be sent until these credentials are added.

To import SNMP service settings:

1. In the General tab of the SNMP Settings pane, select Import Settings from File. Browse to an SNMP.conf file. The imported file overwrites the configuration in the SNMP Settings

pane.

A dialog box lists lines of the file that were not imported, if any. For example, if the imported file contains VACM settings not supported by the SNMP Settings pane in the Console, these lines are listed in the results window.



Import Results Dialog

2. Select OK.
3. Review imported settings in the tabs of the SNMP Settings pane, then do one of the following:
    - Select Cancel to roll back the import. Previous settings of the SNMP Settings pane are restored.
    - Select Apply to accept imported settings. The tabs of the SNMP Settings pane reflect imported settings.

Export SNMP Service Settings

Use this procedure to save current settings of the SNMP Settings pane to a `.conf` file.

To export SNMP service settings:

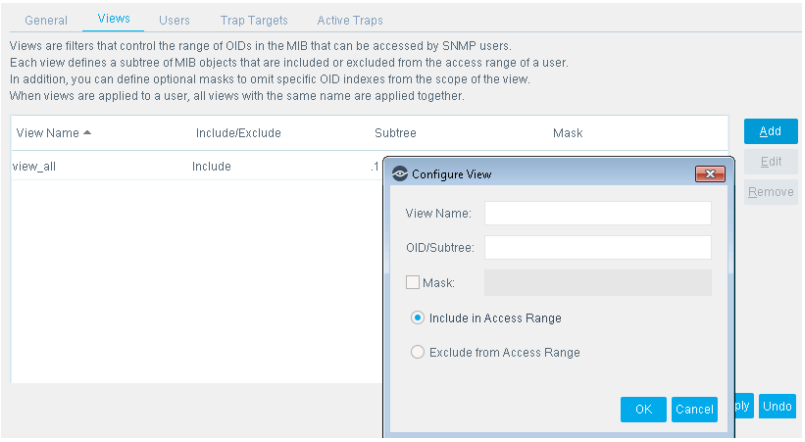
1. In the General tab of the SNMP Settings pane, select Export Settings to File. In the Export dialog box, browse to the desired target directory and enter a name for the .conf file.
2. Select Export. A file is created in the target directory. The file contains the current settings of the SNMP Settings pane.

Configure SNMP Views

Use this procedure to define inbound Views that restrict user access to the Forescout MIB.

To configure Views:

1. In the SNMP Settings pane of the Options tree, select the Views tab. The table lists existing views.



2. Do one of the following:
   - Select Add to create a new view.
   - Select an existing view in the table, and then select Edit to modify it.

   The Configure View dialog box opens.

3. Define the view using the following fields and options:

View Name	This value is not necessarily unique. Several views can have the same name, each of them defining different access range of MIB objects. When a view is applied to a user or group, all access ranges with the same name are applied together.
OID/Subtree	A sub-tree in the eyeSight device MIB, for example: .3.4.5.2.78 Apply the view to an SNMP user to define user access to this sub-tree.
Mask	(Optional) Select this option to mask specific OIDs in the sub-tree. Specify the mask as a colon-separated list of hexadecimal octets.
Include in access range	Exclude from access range Determines how the view affects the access range of users. Include in access range – the sub-tree is permitted to users when this view is applied to them. Exclude from access range – the sub-tree is prohibited to users when this view is applied to them.

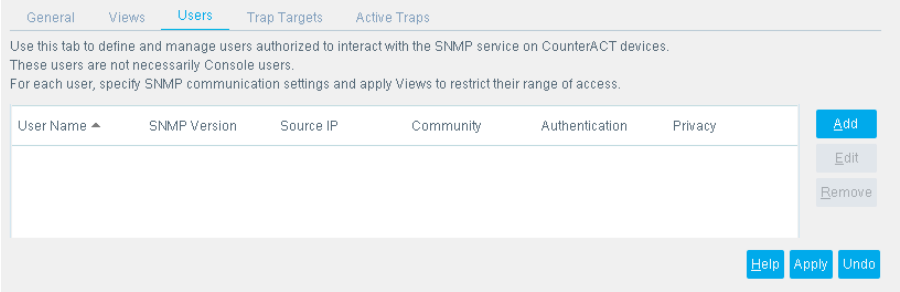
4. To remove a view, select it in the table and select Remove.

Configure SNMP Users

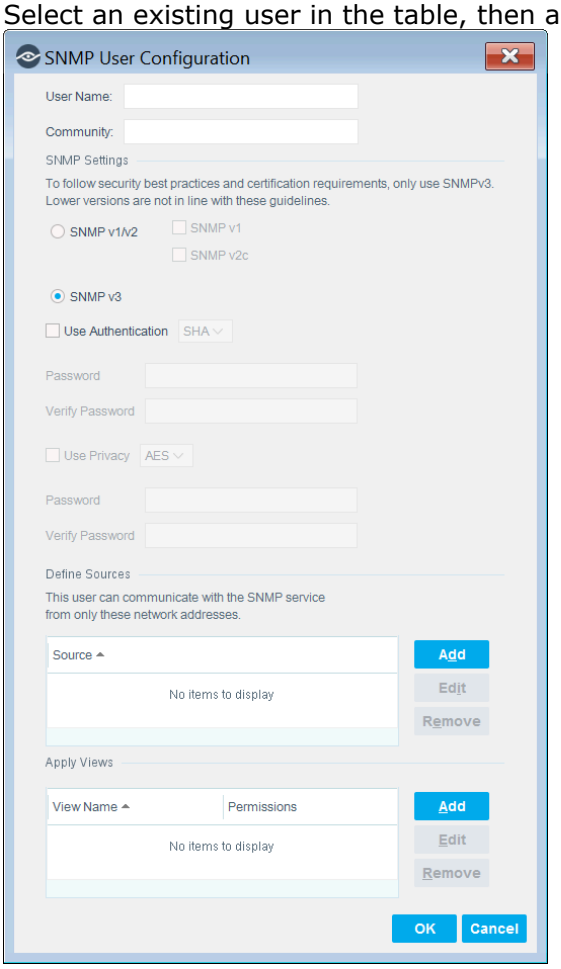
Use this procedure to define inbound users that can access the Forescout MIB. These users are not necessarily Forescout users.

To configure SNMP users:

1. In the SNMP Settings pane of the Options tree, select the Users tab. The table lists users that can interact with the SNMP service on eyeSight devices.



2. Do one of the following:
   - Select Add to create a new user.
   - Select an existing user in the table, then and select Edit to modify it.



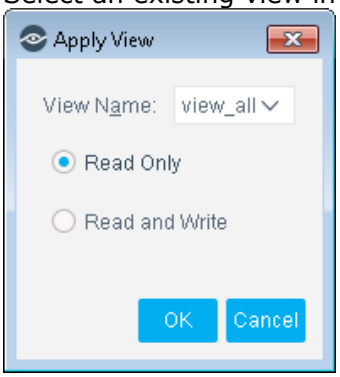
3. In the User Name field, specify a unique name for this SNMP user.
4. In the Community field, specify the community string config with which the user communicates with the Forescout eyeSight (not relevant for SNMP v3).
5. In the SNMP Settings area, select the version of the SNMP protocol that is used to communicate with this user. To follow security best practices and certification requirements, only use SNMP v3 (default). Lower versions are not in line with these guidelines. (Optional) When SNMP V3 is selected, Authentication and Privacy encryption options are available. Specify encryption protocols and passwords. This data is not imported when you Import SNMP Service Settings.
6. In the Define Sources area, define the network addresses from which this user can access the SNMP service. Do one of the following:
    - Select Add to add a source.
    - Select a source in the table and select Edit or Remove.

    Each entry in the list can be a specific FQDN or IP address, or a subnet declared using the IP/MASK or IP/BITS convention. For example:

    ```
    10.10.10.0/255.255.255.0
    ```

    ```
    2001:db8:abcd:3f02::/64
    ```

7. In the Apply Views area, select the views that filter access for this user. Do one of the following:
    - Select Add to apply a view to the user.
    - Select an existing view in the table, and then select Edit to modify it.



In the Apply View dialog box, define how a view is applied using the following fields and options.

View Name	The drop-down menu lists all view names currently defined in the Views tab that have not yet been assigned to this user.
Read Only	Read and Write This setting determines permissions granted to the user for the MIB objects in this view: Read Only (default)– user can only read the MIB objects in this view.

	Read/Write –user can read and write to the MIB objects in this view.

Note:
If you do not configure this option, the user is granted read only permissions.

To remove a view from a user, select it in the table and select Remove. The view still appears in the Views tab, but no longer applies to this user.

Configure Trap Targets

Define and manage targets that receive outbound traps from the Forescout SNMP service.

To configure SNMP Service settings, select Tools > Options > General > SNMP Settings.

1. In the SNMP Settings pane of the Options tree, select the Trap Targets tab.
2. Do one of the following:
   - Select Add to create a new target.
   - Select an existing target in the table, and then select Edit to modify it.

   The Trap Configuration dialog box opens.

   Define a target using the following fields and options. Select OK to save changes.

IP Address or FQDN	The network address to which the traps are sent. This can be a specific FQDN or IP address.
Community	The community string that is used to communicate with this target.
Trap Type	The type of SNMP trap message that is sent to this user.

3. To remove a target, select it in the table and select Remove.
4. Test communication with trap targets
   a. In the SNMP Settings pane of the Options tree, select the Trap Targets tab.
   a. Select Send Test Trap. Select OK to confirm. A test trap is sent to all the targets configured in the Trap Targets table.

Enable and Disable Forescout eyeSight Traps

Configure which Forescout eyeSight-specific outbound traps are sent by devices to external trap targets.

Note:
Standard SNMP traps are always sent and cannot be disabled.

1. In the SNMP Settings pane of the Options tree, select the Active Traps tab.

   The table lists all the Forescout eyeSight-specific traps supported by the SNMP service on devices. By default, all traps are enabled.

2. (Optional) Use the search field to show traps that match a sub-string of any trap identifier fields, or a MIB subtree.
3. Do one of the following:
   - Clear the checkbox next to a trap to disable it. The trap is not sent by Forescout devices.
   - Select the checkbox next to a trap to enable it. The trap is sent when Forescout devices experience triggering events or thresholds.
   - Use the Clear All and Select All buttons to enable or disable all currently displayed traps.
4. Select Apply to save configuration changes.

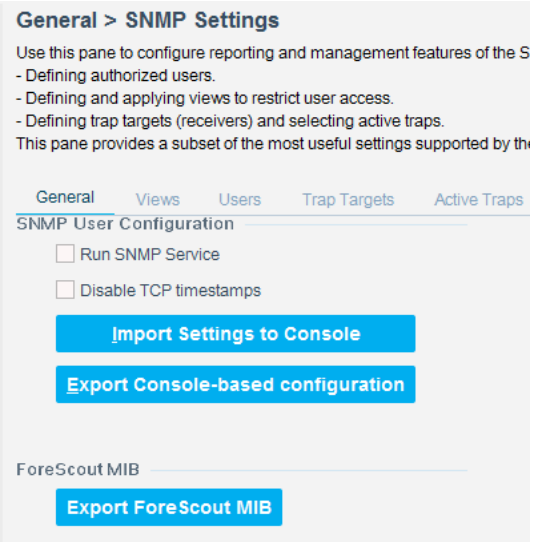
SNMP MIB for appliances

MIB tables for eyeSight Appliances provide objects that report detailed information about status, configuration and performance.

SNMP queries made to an Enterprise Manager return a table containing the MIB attributes of the Enterprise Manager and all its managed Appliances.

SNMP queries made to a specific Appliance return a table containing a single row providing the MIB attributes of the queried Appliance.

To obtain the Forescout SNMP MIB file, select Options > General SNMP Settings. In the Forescout MIB area of the General tab, select Export ForeScout MIB.



Load this file in your external management system.

Note:
eyeExtend for ArcSight also provides SNMP MIB and Trap Notification information about the interaction between eyeSight devices and their peer ArcSight servers. Refer to the eyeExtend for ArcSight documentation.

Note:
For an external network management system to query an Appliance SNMP MIB and receive SNMP trap notifications, you must enable SNMP on the Appliance. By default, the Forescout SNMP agent is disabled. See SNMP Support and Integration for details.

MIB table objects for appliances

The eyeSight Appliance MIB contains the following objects.

ctDeviceTable

OID: .1.3.6.1.4.1.11789.4.3

This object contains a table of MIB object values for all Forescout Appliances managed by this Appliance.

- For an Enterprise Manager (EM) this object contains a table of values for all its managed Appliances. Each row contains the MIB values of a single managed Appliance.
- For a managed or standalone Appliance this table contains a single-row table representing the MIB values of the Appliance.

The following related trap notifications are provided:

- ctDeviceAddedTrapNotification
- ctDeviceRemovedTrapNotification

ctDeviceId

OID:.1.3.6.1.4.1.11789.4.3.1.1

An internally defined unique identifier for the Appliance. The Enterprise Manager assigns a unique Device ID to itself, and to each managed Appliance. The Device ID provides a consistent reference to the Appliance as long as it is associated with the Enterprise Manager.

ctDeviceIpAddress

OID:.1.3.6.1.4.1.11789.4.3.1.2

The IP address of this Appliance.

- For an Enterprise Manager this is the IP address of the device.
- For a managed Appliance this is the IP address of the Appliance as perceived by the Enterprise Manager.

ctDeviceIpAddressType

OID:.1.3.6.1.4.1.11789.4.3.1.3

The type of IP address in the ctDeviceIpAddress object. Valid values are:

ipv4 (1)	Indicates that an IPv4 address is used, as defined by the InetAddressIPv4 textual convention.
ipv6 (2)	Indicates that an IPv6 address is used, as defined by the InetAddressIPv6 textual convention.

ctNumberOfManagedEndpoints

OID:.1.3.6.1.4.1.11789.4.3.1.12

The total number of endpoints currently managed by this Appliance. For an Enterprise Manager, this object contains the total number of endpoints directly managed by the Enterprise Manager.

The following related trap notifications are provided:

- ctDeviceTrapEndpointCapacityExceeded
- ctDeviceTrapEndpointCapacityNormal

ctDeviceCpuUtilization

OID:.1.3.6.1.4.1.11789.4.3.1.5

Percentage of the Appliance's allocated processor resources currently in use. This value is an average taken across all processors.

The following related trap notifications are provided:

- ctDeviceTrapHighCPUUtilization
- ctDeviceTrapNormalCPUUtilization

ctDevicePacketLoss

OID:.1.3.6.1.4.1.11789.4.3.1.13

Packet loss as a percent of received IP packets. This is the fraction of received packets that were not handled by the Appliance over a sliding window of the last 30 seconds. When packet loss is excessive, HTTP Redirection and Virtual Firewall actions may not work consistently. To resolve, upgrade the Appliance or configure the channels to monitor less traffic.

The following related trap notifications are provided:

- ctDeviceTrapHighPacketLoss
- ctDeviceTrapNormalPacketLoss

ctDeviceMemorySwaps

OID:.1.3.6.1.4.1.11789.4.3.1.6

Amount of memory swapped (kbytes) over the last minute. If this value exceeds the recommended threshold, the system may work slowly. To resolve this issue, add physical memory to the Appliance or replace the Appliance with a model that has more physical memory.

The following related trap notifications are provided:

- ctDeviceTrapHighMemorySwapping
- ctDeviceTrapNormalMemorySwapping

ctDeviceConnectionStatus

OID:.1.3.6.1.4.1.11789.4.3.1.4

Indicates the network connectivity status. Possible states are:

---

connectionOK (1) Indicates that the Appliance is up and ready.

connectionFailed (2)	Indicates the connection to the network failed. There may be a network outage, or the Appliance may be down.
connectionStatusUnknown (3)	Indicates that the connection status cannot be verified at this time (for example, if the Appliance is down or unreachable).

The following related trap notification is provided:

ctDeviceConnectionStatusChangedTrap

ctDeviceEngineStatus

OID:.1.3.6.1.4.1.11789.4.3.1.11

Indicates the status of the Packet Engine service, which monitors network traffic and discovers network endpoints. Possible states are:

ready (1)	Indicates that the Packet Engine is up and ready.
initializing (2)	Indicates that the Packet Engine is starting up and currently initializing.
down (3)	Indicates that the Packet Engine is currently down.
statusUnknown (4)	Indicates that the Packet Engine status cannot currently be verified. For example, the Appliance may be down or unreachable.
notApplicable (5)	Indicates that the Packet Engine is administratively disabled.

The following related trap notification is provided:

ctDevicePacketEngineStatusChangedTrap

ctDeviceCurrentBandwidth

OID:.1.3.6.1.4.1.11789.4.3.1.10

Bit-rate consumed by the Appliance communication resources expressed in kilobytes per second; averaged over a sliding window. This value accounts for internal traffic between Appliances and traffic handled by the Packet Engine. If this value exceeds recommended thresholds for each Appliance model, Appliance performance may be affected. To resolve this issue, contact Forescout Customer Care or your sales representative.

The following related trap notifications are provided:

- ctDeviceHighBandwidthUtilizationTrap

- ctDeviceNormalBandwidthUtilizationTrap

ctDeviceHaStatus

OID:.1.3.6.1.4.1.11789.4.3.1.9

Indicates the status of the High Availability (HA) service, which monitors the status of the active and the passive (standby) Appliances in a High Availability pair. Possible states are:

ok (1)	Indicates that the standby device is up, responsive and is in sync with the active eyeSight device.
statusDegraded (2)	Indicates that the standby device is unreachable, down, or currently out of sync with the active CounterACT device.
inMaintenanceMode (3)	Indicates that the active or the standby device is undergoing maintenance operations such as setup or upgrade
notSupported (4)	Indicates that High Availability is not supported or configured on this Appliance.
statusUnknown (5)	Indicates that the High Availability status cannot be determined because the Enterprise Manager cannot connect to the Appliance.

The following related trap notification is provided:

ctDeviceHaStatusChangedTrap

ctDeviceLicenseStatus

OID:.1.3.6.1.4.1.11789.4.3.1.8

Indicates the status of the licensing service. This service monitors the licensed operating capacity of eyeSight relative to the number of managed endpoints, used Appliance bandwidth, software modules and other license terms. Possible states are:

valid (1)	Indicates that the current license status is OK, and usage is within the licensed capacity.
violation (2)	Indicates that there are one or more license violations, for example, services running with usage capacity exceeding the currently deployed licenses.
invalid (3)	Indicates that the currently deployed license is expired or invalid.

statusUnknown (4)	Indicates that the license status cannot be verified at this time (for example, the Appliance is down or unreachable).

The following related trap notification is provided:

ctDeviceLicenseStatusChangedTrap

ctDeviceNtpStatus

OID:.1.3.6.1.4.1.11789.4.3.1.7

Indicates the status of the network time synchronization service, which handles synchronization with the associated NTP server. Possible states are:

syncOk (1)	Indicates the Appliance is synchronized with the NTP server.
syncFailed (2)	Indicates the Appliance failed to connect to the NTP server or failed to get a valid response from the NTP server.
notApplicable (3)	Indicates that the NTP is not configured or that the NTP service is down.
statusUnknown (4)	Indicates that the Appliance is currently unreachable and that the current status cannot be verified.

The following related trap notification is provided:

ctDeviceNTPStatusChangedTrap

ctDeviceActionsOnHoldStatus

OID:.1.3.6.1.4.1.11789.4.3.1.14

Indicates the status of the pending actions queue. This object indicates if there are policy-driven actions that were blocked because the number of pending actions exceeded the queue size defined in the Console at Options > NAC > Action Thresholds. Queue size and action thresholds can be defined per action and/or per device. Possible states are:

ok (1)	Indicates that policy actions are within the defined Action thresholds, and that there are no policy driven actions in a blocked state.
blockedOnExceedingThreshold (2)	Indicates that actions are blocked. One or more policies have created a queue of actions that exceeds the administrator defined threshold. The administrator can review and release blocked actions from the Console at Options > NAC > Action Thresholds.

blockStatusUnknown (3)	Indicates that the queue status cannot be verified (for example, if the device is down or unreachable).

The following related trap notification is provided:

ctDeviceActionOnHoldStatusChanged

ctDeviceChannelStatus

OID:.1.3.6.1.4.1.11789.4.3.1.15

Indicates the status of the network interfaces used by the Appliance to mirror monitored traffic and insert management input. A channel is defined as a pair of monitor and response interfaces. Possible states are:

ok (1)	Indicates that the Appliance is currently monitoring network traffic.
warning (2)	Indicates a significant change in traffic on the channel's monitoring interface. The volume of mirrored traffic may have dropped significantly, indicating that not all traffic is being monitored. A trap with this severity may report a transient effect. If the Appliance does not recover channel function within a minute or two, troubleshooting intervention is typically necessary. Significant, persistent missed traffic prevents eyeSight from reliably implementing detection, prevention, and remediation actions – and may require reconfiguration of the Appliance's channels.
error (3)	Indicates that the Appliance's internal test of the channel's response interface repeatedly fails, and/or traffic on the monitoring interface may be asymmetric. The Appliance cannot reliably track communications or insert response traffic. This effectively prevents the Appliance from implementing detection, prevention, and remediation actions.
unknown (4)	Indicates that the status of channel interfaces cannot be verified at this time (for example, if the Appliance is down or unreachable).
notApplicable (5)	Indicates that channels are not configured or administratively disabled.

The following related trap notification is provided:

ctDeviceChannelStatusChangedTrap

SNMP trap notifications for appliances

These SNMP trap notifications are issued when a configuration, status, or performance attribute of the eyeSight Appliance SNMP MIB changes on an Appliance.

Appliance SNMP trap notifications include varbinds to identify the reporting Appliance and to indicate severity and other information. See Common Trap Notification Varbinds.

Several of the trap notifications described here are threshold crossing alarms (TCA). Trap notification is triggered when MIB values pass configurable performance thresholds. For information about setting these thresholds, see Performance Thresholds for SNMP Notifications.

Note:
eyeExtend for ArcSight also provides SNMP MIB and Trap Notification information about the interaction between eyeSight devices and their peer ArcSight servers. Refer to the eyeExtend for ArcSight documentation.

Note:
For an external network management system to query an Appliance SNMP MIB and receive SNMP trap notifications, you must enable SNMP on the Appliance. By default, the Forescout SNMP agent is disabled.

Appliance trap notifications can contain the following MIB objects:

ctConfigurationChangedTrap

OID:.1.3.6.1.4.1.11789.0.14

Indicates a configuration change on the Appliance. In addition to the common trap notification varbinds, this trap provides the following additional varbinds to identify the configuration change:

fsFieldOid

OID:.1.3.6.1.4.1.11789.3.24

The OID of the changed object. For example, if the eyeSight operator changed the ArcSight server name, this varbind contains the OID of the arcSightServerName object.

fsOldValue

OID:.1.3.6.1.4.1.11789.3.25

The value of the MIB attribute before the configuration change.

fsNewValue

OID:.1.3.6.1.4.1.11789.3.26

The updated value of the MIB attribute after the configuration change.

ctDeviceAddedTrapNotification

OID:.1.3.6.1.4.1.11789.0.15

Indicates that an Appliance was added to Enterprise Manager (EM).

ctDeviceRemovedTrapNotification

OID:.1.3.6.1.4.1.11789.0.16

Indicates that an Appliance was removed from Enterprise Manager (EM).

ctDeviceTrapEndpointCapacityExceeded

OID:.1.3.6.1.4.1.11789.0.25

This trap notification is sent when the ctNumberOfManagedEndpoints MIB attribute crosses the upper bound of the Number of Hosts threshold. Trap severity is warning(6).

This alarm trap is cleared by the ctDeviceTrapEndpointCapacityNormal trap notification.

To set performance thresholds, see Performance Thresholds for SNMP Notifications.

ctDeviceTrapEndpointCapacityNormal

OID:.1.3.6.1.4.1.11789.0.26

This trap notification is sent when the ctNumberOfManagedEndpoints MIB attribute crosses the lower bound of the Number of Hosts threshold. Trap severity is clear(1).

This trap notification is only sent after a ctDeviceTrapEndpointCapacityExceeded alarm trap was sent.

To set performance thresholds, see Performance Thresholds for SNMP Notifications.

ctDeviceTrapHighCPUUtilization

OID:.1.3.6.1.4.1.11789.0.19

This trap notification is sent when the ctDeviceCpuUtilization MIB attribute crosses the upper bound of the CPU Usage threshold. Trap severity is warning(6).

This alarm trap is cleared by the ctDeviceTrapNormalCPUUtilization trap notification.

ctDeviceTrapNormalCPUUtilization

OID:.1.3.6.1.4.1.11789.0.20

This trap notification is sent when the ctDeviceCpuUtilization MIB attribute crosses the lower bound of the CPU Usage threshold. Trap severity is clear(1).

This trap notification is sent only after a ctDeviceTrapHighCPUUtilization alarm trap is sent.

To set performance thresholds, see Performance Thresholds for SNMP Notifications.

ctDeviceTrapHighPacketLoss

OID:.1.3.6.1.4.1.11789.0.28

This trap notification is sent when the ctDevicePacketLoss MIB attribute crosses the upper bound of the Packet Loss threshold. Trap severity is warning(6).

This alarm trap is cleared by the ctDeviceTrapNormalPacketLoss trap notification.

To set performance thresholds, see Performance Thresholds for SNMP Notifications.

ctDeviceTrapNormalPacketLoss

OID:.1.3.6.1.4.1.11789.0.29

This trap notification is sent when the ctDevicePacketLoss MIB attribute crosses the lower bound of the Packet Loss threshold. Trap severity is clear(1).

This trap notification is sent only after a ctDeviceTrapHighPacketLoss alarm trap is sent.

To set performance thresholds, see Performance Thresholds for SNMP Notifications.

ctDeviceTrapHighMemorySwapping

OID:.1.3.6.1.4.1.11789.0.23

This trap notification is sent when the ctDeviceMemorySwaps MIB attribute crosses the upper bound of the MemorySwaps threshold. Trap severity is warning(6).

This alarm trap is cleared by the ctDeviceTrapNormalMemorySwapping trap notification.

To set performance thresholds, see Performance Thresholds for SNMP Notifications.

ctDeviceTrapNormalMemorySwapping

OID:.1.3.6.1.4.1.11789.0.24

This trap notification is sent when the ctDeviceMemorySwaps MIB attribute crosses the lower bound of the MemorySwaps threshold. Trap severity is clear(1).

This trap notification is sent only after a ctDeviceTrapHighMemorySwapping alarm trap is sent.

To set performance thresholds, see Performance Thresholds for SNMP Notifications.

ctDeviceConnectionStatusChangedTrap

OID:.1.3.6.1.4.1.11789.0.33

Indicates a change in the ctDeviceConnectionStatus MIB attribute. The severity of this alarm trap reflects the current value of the MIB attribute, as shown in the following table.

Value of ctDeviceConnectionStatus	Severity of ctDeviceConnectionStatusChangedTrap
connectionOK (1)	cleared(1)
connectionFailed (2)	critical (3)
connectionStatusUnknown (3)	indeterminate(2)

ctDevicePacketEngineStatusChangedTrap

OID:.1.3.6.1.4.1.11789.0.33

Indicates a change in the ctDeviceEngineStatus MIB attribute. The severity of this alarm trap reflects the current value of the MIB attribute, as shown in the following table.

Value of ctDeviceEngineStatus	Severity of ctDevicePacketEngineStatusChangedTrap
engineReady (1)	cleared(1)
engineInitializing (2)	indeterminate(2)
engineDown (3)	critical (3)
engineStatusUnknown (4)	indeterminate(2)
engineNotApplicable (5)	warning (6)

ctDeviceHighBandwidthUtilizationTrap

OID:.1.3.6.1.4.1.11789.0.21

This trap notification is sent when the ctDeviceCurrentBandwidth MIB attribute crosses the upper bound of the Bandwidth threshold. Trap severity is warning(6).

This alarm trap is cleared by the ctDeviceNormalBandwidthUtilizationTrap trap notification.

To set performance thresholds, see Performance Thresholds for SNMP Notifications.

ctDeviceNormalBandwidthUtilizationTrap

OID:.1.3.6.1.4.1.11789.0.22

This trap notification is sent when the ctDeviceCurrentBandwidth MIB attribute crosses the lower bound of the Bandwidth threshold. Trap severity is clear(1).

This trap notification is sent only after a ctDeviceHighBandwidthUtilizationTrap alarm trap is sent.

To set performance thresholds, see Performance Thresholds for SNMP Notifications.

ctDeviceHaStatusChangedTrap

OID:.1.3.6.1.4.1.11789.0.30

Indicates a change in the ctDeviceHaStatus MIB attribute. The severity of this alarm trap reflects the current value of the MIB attribute, as shown in the following table.

Value of ctDeviceHaStatus	Severity of ctDeviceHaStatusChangedTrap
haStatusOK (1)	cleared(1)
haStatusDegraded (2)	major(4)
haInMaintenanceMode(3)	warning(6)
haNotSupported(4)	cleared(1)
haStatusUnknown(5)	indeterminate(2)

ctDeviceLicenseStatusChangedTrap

OID:.1.3.6.1.4.1.11789.0.17

Indicates a change in the ctDeviceLicenseStatus MIB attribute. The severity of this alarm trap reflects the current value of the MIB attribute, as shown in the following table.

Value of ctDeviceLicenseStatus	Severity of ctDeviceLicenseStatusChangedTrap
licenseValid (1)	cleared(1)

Value of ctDeviceLicenseStatus	Severity of ctDeviceLicenseStatusChangedTrap
licenseViolation (2)	warning(6)
licenseInvalid (3)	major(4)
licenseStatusUnknown (4)	indeterminate(2)

ctDeviceNTPStatusChangedTrap

OID:.1.3.6.1.4.1.11789.0.18

Indicates a change in the ctDeviceNtpStatus MIB attribute. The severity of this alarm trap reflects the current value of the MIB attribute, as shown in the following table.

Value of ctDeviceNtpStatus	Severity of ctDeviceNTPStatusChangedTrap
ntpSyncOk (1)	cleared(1)
ntpSyncFailed (2)	major(4)
ntpNotApplicable (3)	indeterminate(2)
ntpStatusUnknown (4)	indeterminate(2)

ctDeviceActionOnHoldStatusChanged

OID:.1.3.6.1.4.1.11789.0.32

Indicates a change in the ctDeviceActionsOnHoldStatus MIB attribute. The severity of this alarm trap reflects the current value of the MIB attribute, as shown in the following table.

Value of ctDeviceActionsOnHoldStatus	Severity of ctDeviceActionOnHoldStatusChanged
actionsOk (1)	cleared(1)

Value of ctDeviceActionsOnHoldStatus	Severity of ctDeviceActionOnHoldStatusChanged
actionsBlockedOnExceedingTreshold (2)	major(4)
actionsBlockStatusUnknown (3)	indeterminate(2)

ctDeviceChannelStatusChangedTrap

OID:.1.3.6.1.4.1.11789.0.31

Indicates a change in the ctDeviceChannelStatus MIB attribute. The severity of this alarm trap reflects the current value of the MIB attribute, as shown in the following table.

Value of ctDeviceChannelStatus	Severity of ctDeviceChannelStatusChangedTrap
channelsOk (1)	cleared(1)
channelsWarning (2)	warning(6)
channelsError (3)	critical(3)
channelsUnknown (4)	indeterminate(2)
channelsNotApplicable (5)	is warning(6)

Common trap notification varbinds

SNMP trap notifications issued by the eyeSight always include a sequence of variable bindings (varbinds).

A varbind is an SNMP key-value attribute pair, composed of the varbind OID (key) and its assigned value. For example, the trap notification ctDeviceChannelStatusChangedTrap always includes the following varbind:

```
.1.3.6.1.4.1.11789.3.21 = 1
```

where:

`.1.3.6.1.4.1.11789.3.21` is the OID of varbind fsTrapSeverity

`1` is the severity value assigned to this OID. For the ctDeviceChannelStatusChangedTrap trap

notification, a varbind severity value of 1 indicates that trap's severity is now cleared, given that the channel status has changed to channelsOk.

The following varbind objects are common to all Forescout trap notifications.

ctDeviceId

OID:.1.3.6.1.4.1.11789.4.3.1.1

An internally defined unique identifier for the Appliance. The Enterprise Manager assigns a unique Device ID to itself, and to each managed Appliance. The Device ID provides a consistent reference to the Appliance as long as it is associated with the Enterprise Manager.

ctDeviceIpAddress

OID:.1.3.6.1.4.1.11789.4.3.1.2

The IP address of the Appliance or Enterprise Manager that issued the SNMP trap notification.

ctDeviceIpAddressType

OID:.1.3.6.1.4.1.11789.4.3.1.3

The type of IP address in the ctDeviceIpAddress varbind object. Valid values are:

ipv4 (1)	Indicates an IPv4 address as defined by the InetAddressIPv4 textual convention.
ipv6 (2)	Indicates an IPv6 address as defined by the InetAddressIPv6 textual convention.

fsTrapSeverity

OID:.1.3.6.1.4.1.11789.3.21

The severity assigned to the trap notification.

Cleared (assigned value = 1)	Indicates that this trap notification clears one or more previously reported alarm traps. This trap clears all alarms for this managed object that have the same Alarm type.
Indeterminate (assigned value = 2)	Indicates that the severity level cannot be determined.
Critical (assigned value = 3)	Indicates that a service-affecting condition has occurred, and immediate corrective action is required. This severity is reported when a managed object goes completely out of

	service and its function must be restored.
Major (assigned value = 4)	Indicates that a service-affecting condition has developed, and urgent corrective action is required. This severity is reported when there is a severe degradation in the capability of the managed object and its full capability must be restored.
Minor (assigned value = 5)	Indicates a fault condition that does not affect service. Corrective action should be taken to prevent a more serious fault that may affect service. This severity is assigned to a detected alarm condition that is not currently degrading the capacity of the managed object.
Warning (assigned value = 6)	Indicates the detection of a potential or impending service-affecting fault, before any significant effects have been felt. Action should be taken to further diagnose (if necessary) and correct the problem before it affects service.
Informational (assigned value = 7)	Provided for informational purposes only. With the exception of the Informational severity, all the other severity levels are defined in the CCITT standard X.733.

fsTrapTime

OID:.1.3.6.1.4.1.11789.3.21

Date and time when the event occurred in the Appliance, provided in the format of the DateAndTime field, as specified in the SNMPv2-Textual Conventions standard.

fsTrapId

OID:.1.3.6.1.4.1.11789.3.21

A unique identifier for each issued trap notification. The ID is an integer based on a counter which increments monotonically until a maximum value is reached, and then begins again from zero.

Based on a corporate network configuration (UDP), it is possible that the trap receiver may receive multiple copies of the same trap notification. In such a case, the Trap ID and Trap Time can be used to identify duplicate trap notifications.

Customizing user interfaces

Work with the User Portal Builder

Use the eyeSight User Portal Builder to create custom skins for HTTP Login, HTTP Notification, and Guest Management user interfaces.

You can work interactively in the User Portal Builder, or download CSS files to edit. You can make more extensive font and design modifications by editing the CSS file.

Note:
The User Portal Builder cannot be used to localize user interface text. To localize the text, see Localize Redirected Web Pages and Messages .

- Access the User Portal Builder.
  - From the Console toolbar select More > User Portal Builder.
    Or
  - From the Console toolbar select Tools > Options > NAC > HTTP Redirection > Open User Portal Builder.
- To work interactively in the User Portal Builder:
  1. Open a working template.
     - Select Add and select the user interaction for which you want to create a skin. An editable copy of the default skin opens.
     - Select a template you already created, and select Edit. An editable copy of the skin opens.
  2. Edit the skin colors and logo as needed and assign a name to the new skin.
     Note:
     Uploaded logo files must be in PNG format and cannot be larger than 1 MB.
  3. In the Preview area, select the laptop/PC, tablet, and mobile device icons to preview the skin on various devices. There is no unique customization for mobile devices.
  4. Name the new skin, then select Save.
- To download skin files and edit them in another application:
  1. Download skin files:Select a skin, then select the Export Skin icon. A zip archive containing the CSS file and bitmaps is downloaded.
  2. Modify the CSS file and replace bitmaps. Save all skin components in a zip archive.
  1. In the User Portal Builder interface, select the Import Skin icon. Specify a name for the new skin, and browse to the zip archive you prepared.
- Only one skin is deployed throughout your eyeSight environment for each type of user interface. Select the skin to be deployed in place of the one currently deployed, and then select Deploy. his skin is distributed and used in your eyeSight deployment

The legacy customization tool

Customize the interface eyeSight presents on PCs and laptops for the end-user interactions of HTTP actions, SecureConnector installation, and other features.

The Legacy Customization tool lets you configure the user interface used for the following end-user interactions.

- Start SecureConnector
- HTTP Localhost Login
- Start Macintosh Updates
- Start Windows Updates
- Windows Self Remediation
- Compliance Center

From the Console toolbar select Tools > Options > NAC > HTTP Redirection > Open Legacy Customization Tool. A table lists all customized templates. A default template is provided.

The following icons indicate which templates are currently used by Forescout.

	Template is used when Forescout Compliance Center (FCC) is enabled.
	Template is used when Forescout Compliance Center (FCC) is disabled.
	Template is used for all general pages.
	Template is not used.
•	Template was published in the past.

The following actions are available.

Add	Create new template based on the default Forescout template.
Edit	Modify customized templates. You cannot modify the default Forescout template.
Duplicate	Copies an existing template.
Delete	Delete a customized template. You cannot delete the default Forescout template.
Publish	Integrate a template and use it for Forescout end user interactions.
Preview	View a sample web page formatted with the template.
Export	Save a custom template to external systems, such as backup servers in Web Developer mode.

Import	Imports a custom template from external systems, such as backup servers in Web Developer mode.

Create or edit a template

Create custom skin templates for HTTP interactions in the Legacy Customization Tool.

1. From the Console toolbar select Tools > Options > NAC > HTTP Redirection > Open Legacy Customization Tool.
2. Select Add to create a new template, or select an existing template and select Edit. The Customization Tool page opens.
3. If the template will use custom image files, style sheets, or scripts, scroll to the bottom of the page and import these files in the File Manager area.
4. Configure template settings.

Name	A unique name for the template. and a short description of its use.
HTML Head Tag Elements	Specify additional tags that are inserted in the header of HTML files formatted with the template. The following HTML tags can be added: <title>, <base>, <link>, <meta>, <script> and <style>. **Note:** To work with this feature prior HTML knowledge is required.
Header and Footer	Specify the header and footer of HTML pages formatted with the template. To directly edit HTML tags used for headers and footers, select Advanced Customization. **Note:** To work with the Advanced Customization feature, prior HTML knowledge is required.

Image	The drop-down shows image files that were uploaded to Forescout. Select Left-Center-Right to specify the horizontal alignment of the image on the web page.
Text	Enter text for the header or footer. Select Left-Center-Right to specify the horizontal alignment the text on the web page.

Page Properties	Define the main body of the HTML pages formatted with the template.

Page Background color	The value of the HTML background-color property. Select the color swatch to edit the color. In the color

	dialog, select the color-wheel icon to save the color.
Page Background image	The drop-down shows image files that were uploaded to Forescout.
Use Forescout Style Sheet	The default Forescout style sheet configures three customization areas, Header, Footer and background. To implement more extensive page customization, clear this option to remove this page configuration.
File Manager	Upload, preview, and delete image, style sheet, and script files used by your template. Uploaded files appear in the list, and in image drop-downs on this page. A check mark ✔ indicates files that are currently used in the template.

5. Select Save. Select OK. The template is saved, and the page preview opens.
6. Select Return to Customize menu. The HTTP Redirection Page: Customization Tool page opens.

Publish a customized template

When you publish a template, eyeSight uses it for the HTTP interactions you specify.

Published templates you create are used for the following interactions:

- Start SecureConnector
- HTTP Localhost Login
- Start Macintosh Updates
- Start Windows Updates
- Windows Self Remediation
- Compliance Center

When the Forescout Compliance Center (FCC) is enabled, two templates are used - one for compliant endpoints, and one for non-compliant endpoints. This lets you use warning icons and colors to alert users on non-compliant endpoints. See Working with the Forescout Compliance Center for details.

1. Select Publish.
2. In the Publish Type drop-down menu, select a publishing option.

General	Use the template for all pages.
Comply (FCC mode)	When the Forescout Compliance Center is enabled, use the template for all compliant pages.

Not Comply (FCC mode)	When the Forescout Compliance Center is enabled, use the template for all non-compliant pages.

3. Select Publish. Forescout uses the template for the HTTP interactions you specified.

Localize text for HTTP interactions

Edit or localize text labels and messages for HTTP interactions.

To localize/customize text strings used in HTTP Redirect actions, go to Options > Advanced > Language Localization > Endpoint Messages.

You can apply HTML formatting code to texts, for example, bold and underlines. A new line <Enter> in text areas is automatically translated to a <br> tag.

Tip:
Enter the word 'mobile' in the Search field to find strings used only in mobile interfaces.

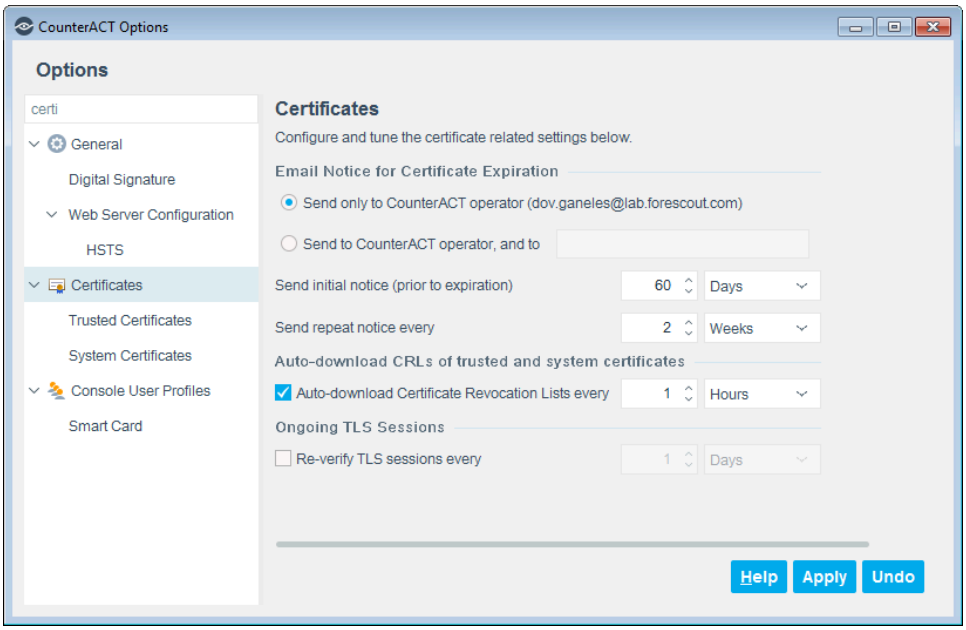
The Certificates pane

The Certificates pane simplifies handling of trusted and system certificates in Forescout.

The Certificates pane replaces previously used `fstools` features. Certificates used in earlier versions of eyeSight are automatically migrated, along with their scopes, to the System Certificates and Trusted Certificates tables.

Each certificate is associated with one or more Forescout services, or with applications running on one or more eyeSight devices. This allows different certificates to be used for different Forescout sub-systems running on different devices.

Access the Certificates pane at Tools > Options > Certificates.



Certificate general settings

Configure general options for certificates defined in Forescout at Tools > Options > Certificates.

Email Notice for Certificate Expiration

Enable and configure automatic emails when certificates near expiration. Select one of the following options.

Send only to CounterACT Operator	Send email only to the eyeSight operator at the email shown.
Send to CounterACT Operator and to	Send email to the eyeSight operator, and to the specified email address.

Specify time intervals for email notification.

Send initial notice (prior to expiration)	The time of the first reminder email, relative to the certificate expiration date. The default is 60 days.
Send repeat notices every	The time interval at which additional reminders are sent. The default is two weeks.

Auto-download CRLs of trusted and system certificates

Auto-download Certificate Revocation Lists every	The time interval at which Forescout downloads updated certificate revocation lists (CRLs) for installed certificates. The default is one hour. You must have Crypto Administration permissions to modify this setting.

Ongoing TLS sessions

Re-verify TLS sessions every	The time interval at which Forescout verifies the certificate of existing TLS sessions. Ongoing TLS sessions may be kept alive for performance reasons - for example, the User Directory plugin connection to the Active Directory server is used more many requests. By default, this option is disabled.

Certificate scope settings

Scope settings determine which eyeSight sub-systems and devices can accept or present a certificate.

There are two certificate scope settings in eyeSight:

- Restrict the sub-systems, components, or services in your eyeSight deployment that accept/present the certificate.
- Restrict the eyeSight devices that accept/present the certificate.

These scope settings are applied together to determine the scope of a certificate.

For Trusted Certificates:

- In the Trusted for Subsystems field, specify the Forescout components or services that accept certificates signed by the CA of the certificate.
- In the Trusted for Devices field, specify the eyeSight devices that accept certificates signed by the CA of the certificate.

The intersection of these scope settings determines certificate usage. Certificates signed by this CA are accepted only by the specified sub-systems, and only when they run on the specified devices.

This CA is not accepted by instances of the specified sub-systems that run on other devices. This

CA is not accepted by other subsystems running on the specified devices.

For System Certificates:

- In the Used for Subsystems field, specify the eyeSight components or services that can present the certificate.
- In the Used for Devices field, specify the eyeSight devices that can present the certificate.

The intersection of these scope settings determines certificate usage. Only the specified sub-systems can present the certificate, and only when they run on the specified devices.

Instances of the specified sub-systems that run on other devices cannot present the certificate. Other sub-systems running on the specified devices cannot present the certificate.

Certificate precedence between Appliance and Enterprise Manager

When you add an Appliance to an Enterprise Manager, the certificates of one may take precedence over the other.

When the first Appliance is added to an Enterprise Manager, you can copy the full Appliance configuration, including certificates, to the Enterprise Manager, or define certificates from scratch.

When another Appliance is added to an Enterprise Manager:

- Typically the Enterprise Manager has no certificates with a scope that includes the Appliance. The Appliance certificates are pushed to the Enterprise Manager and scoped for the Appliance.
- When the Enterprise Manager has certificates whose scope covers the Appliance (for example, when the configured scope is All Devices) , the Enterprise Manager certificates take precedence, and the Appliance certificates are removed. To retain the Appliance certificates, export them to a file before you add the Appliance to the Enterprise Manager, and import them after the Appliance is added.

Manage trusted certificates

eyeSight components and services use the trusted certificates defined in Forescout to authenticate certificates presented by external applications.

Certificates are trusted only if the issuer chain they present ends with a trusted certificate authority (CA). You can define the scope of services or devices in your eyeSight deployment for which each certificate is accepted.

Manage system certificates

Forescout presents system certificates to external services and applications.

Ensure that each subsystem is scoped to the correct certificate on every device on which it runs.

Import and Configure Trusted Certificates

Import trusted certificates and specify the scope for which they are trusted.

You must have Crypto Administration privileges to perform this procedure.

1. In the Console, navigate to Tools > Options > Certificates > Trusted Certificates.
2. Select Add and use the Add a Trusted Certificate wizard to import and configure a certificate.
   a. In the Import CA Certificates pane, configure these settings. Then select Next..

Certificate File	The certificate file you want to import. Most standard certificate archive formats are supported.
Enable Trusting this Certificate	By default this option is enabled. Clear this option to import certificates before you enable them, or to disable an existing certificate without removing it from Forescout.

   b. In the Issuer Chain pane, review certificate details. Then select Next.
   c. In the Trusted for Subsystems pane, specify which components and services trust peers presenting certificates signed by this CA.

All subsystems	All subsystems in your Forescout deployment trust peers presenting a certificate signed by this CA.
Subsystems selected below	Certificates signed by this CA are only trusted by the subsystems you specify. Select this option, then select or deselect items from the list of components and features in your Forescout deployment. **Note:** Subsystems must run on a device that is configured to trust the certificate.

   d. In the Trusted for Devices pane, specify the devices on which the CA certificate is trusted. Then select Next..

All CounterACT devices	The CA certificate is trusted on all CounterACT devices.
CounterACT devices selected below	The CA certificate is trusted only on specific CounterACT devices. Select this option, then select or clear items from the list of devices in your deployment. **Note:** On a device that accepts the certificate, the certificate is only accepted by subsystems that were configured to trust the certificate.

   e. Select Finish.

   The imported certificates appear in the Trusted Certificates table.
3. Use the Add/Import wizard to import more certificates.

4. Apply changes, distribute certificates, and restart Forescout components.
   Select Apply. A dialog box displays the changes to be applied. If the changes are correct, select OK. eyeSight restarts plugins and product components in the scope of the certificate.

Edit Trusted Certificate Entries

Edit the scope of Forescout systems that accept a CA chain, or replace the CA certificate for the defined scope.

You must have Crypto Administration privileges to perform this procedure.

1. In the Console, navigate to Tools > Options > Certificates > Trusted Certificates.
2. Select an entry in the table and select Edit. Use the Edit the Trusted Certificate dialog to review and modify certificate settings.

3. To import a different CA certificate for the scope defined in this table entry, select the Import button, browse to and select the CA certificate file to be imported, and select Apply. The file is imported.
4. Select or clear the checkbox to enable or disable the certificate for the defined scope. A CA certificate is trusted only when enabled for the scope.
5. To change the subsystem scope, select the Trusted for Subsystems tab.
6. To set the scope of Forescout subsystems that trust this CA certificate, do one of the following:
    - To trust this certificate for all Forescout subsystems verifying external certificates, select All subsystems.
    - To trust this certificate for specific Forescout subsystems verifying external

certificates, select Subsystems selected below. In the table, select the relevant subsystems.

Note:

The CA certificate scope also includes the Forescout device on which the subsystem runs. See step 7 .

7. To change the device scope, select the Trusted for Devices tab.
8. To set the scope of devices on which Forescout subsystems can run when presenting the system certificate signed by this certificate, do one of the following:
   - To allow subsystems running on all devices, select All CounterACT devices.
   - To allow subsystems running on only specific devices, select CounterACT devices selected below. In the table, select the relevant devices.

     Note:

     The CA certificate scope includes also the subsystem that presents the signed certificate. See step 7 .
9. Select OK.
10. Select Apply. A dialog box displays all the changes to be applied. If the changes are correct, select OK. eyeSight restarts plugins and product components in the scope of the CA certificate.

Remove Trusted Certificate Entries

When you remove a trusted certificate definition, certificates signed by that CA are no longer accepted by Forescout.

You must have Crypto Administration privileges to perform this procedure.

1. In the Console, navigate to Tools > Options > Certificates > Trusted Certificates.
2. Select the table entry to be removed, and then select Remove.
3. Select Apply. A dialog box displays all the changes to be applied. If the changes are correct, select OK. eyeSight restarts plugins and product components in the scope of the CA certificate.

Generate and Import a Trusted Certificate for Web Portals

Generate and import a trusted certificate for Forescout web portal interactions.

A browser security warning opens when you try to access Forescout Web Portals such as the Assets Portal or the Reports Portal. The Appliance runs a web server to operate these portals. Access to them requires a secured connection (HTTPS), because the information provided is sensitive.

During installation of an Appliance or Enterprise Manager, a default self-signed certificate is created for this purpose. However, this certificate is not signed by a 3rd party Certification Authority. Web browsers do not trust the self-signed certificate, and display a security warning each time you connect to a Forescout portal.

Note:

If you set up the HTTP Login action so that credentials sent to the Appliance are transmitted, you may also want to generate the certificate.

To prevent this message from appearing, the certificate that the web server is using needs to be

signed by a known CA, and the web server should be accessed using its DNS name (and not its IP address).

Use the tools of the Certificates pane to generate a CSR and import a trusted certificate. Scope the certificate to include web portal interaction.

Import and Configure System Certificates

Import system certificates into Forescout and specify which Forescout components present the certificate to external applications.

You must have Crypto Administration privileges to perform this procedure.

1. In the Console, navigate to Tools > Options > Certificates > System Certificates.
2. Select Add from PKCS#12 to import a certificate. The Manage System Certificate wizard opens. wizard opens.
3. In the Import pane browse to the PKCS#12 file to be imported.
4. Select Next. In the Private Key Password dialog, enter the password for the signed certificate file and select OK. The file is imported.
5. Select Next. The Certificate Details pane displays the details of the imported certificate.
6. Select Next. The Issuer Chain pane opens.
7. To add a certificate into the issuer chain, select Add, browse to and select the certificate file to be imported to the chain, and select Apply. The file is imported.
8. Select Next, the Scope pane opens.
9. Set the scope of Forescout subsystems that present the system certificate to external services and applications.

   Note:
   Subsystems scope and device scope overlap. See Certificate scope settings.

Used for Subsystems	Specify the component or service of your Forescout deployment that presents this certificate. Select All to allow all services of your deployment to present the certificate.
Used for Devices	Specify the device in your Forescout deployment that present this certificate. Select All to allow all devices of your deployment to present the certificate.

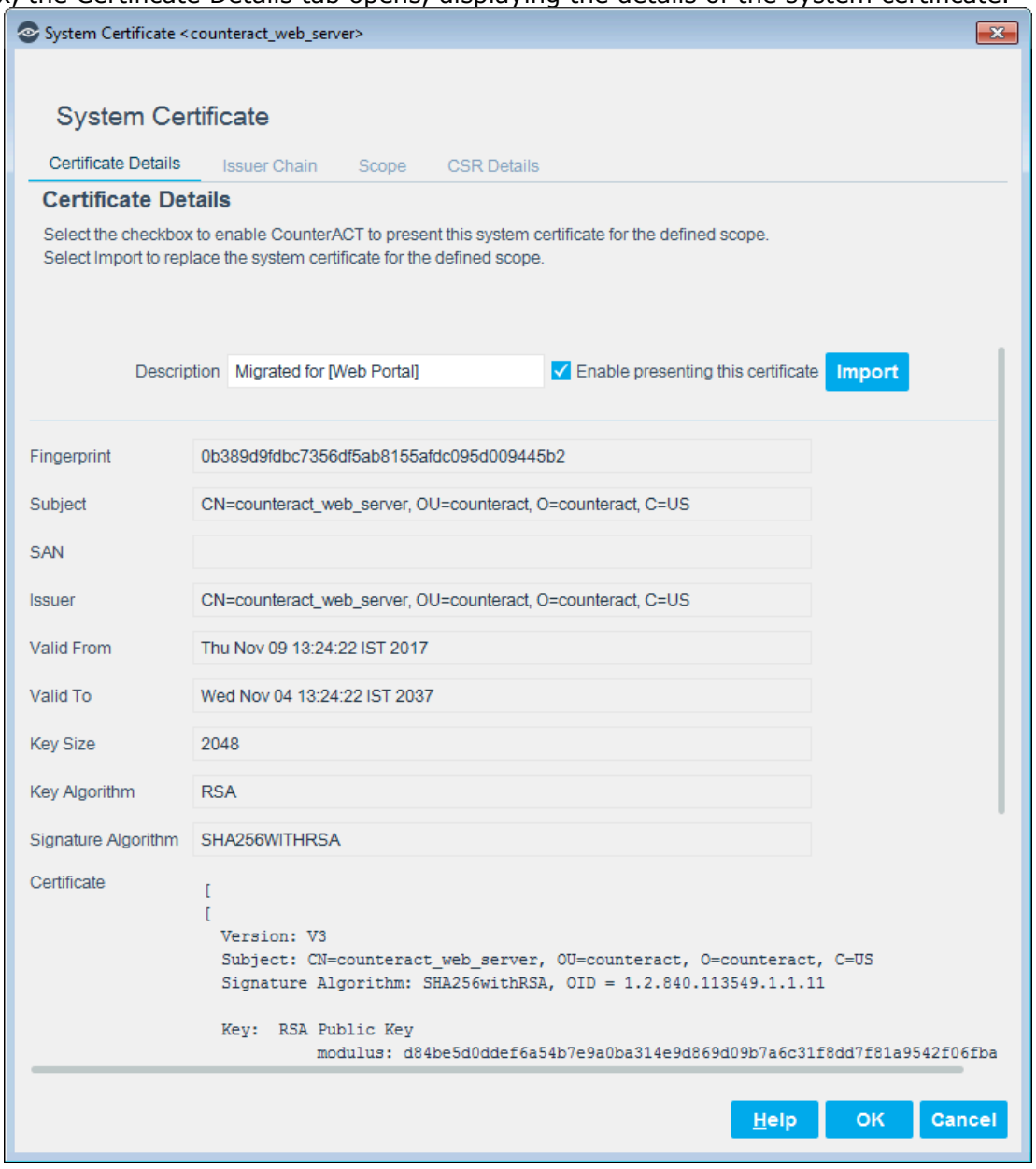
10. Select Next. The Description pane opens.
11. Enter a user-friendly description to identify this certificate and its scope in the System Certificates table.
12. Select or clear the checkbox to enable or disable the imported certificate for the defined scope. Certificates are presented only when enabled for the scope.
13. Select Finish. The certificate is displayed in the System Certificates pane.
14. Select Apply. A summary of the changes to be applied is displayed. If the changes are correct, select Yes. eyeSight restarts plugins and product components in the scope of the certificate.

Edit System Certificate Entries

Edit the certificate scope or replace the certificate for the defined scope.

To edit a certificate entry:

1. Log in to the Console using an account that has CounterACT Crypto Administration permissions.
2. Select Options, and then navigate to Certificates > System Certificates. The System Certificates pane opens.
3. Select the table entry to be edited, and then select Edit. In the System Certificate dialog box, the Certificate Details tab opens, displaying the details of the system certificate.



4. To import a replacement certificate for the scope defined in this table entry, select the Import button, browse to and select the certificate file to be imported, and select Apply. The file is imported.
5. Select or clear the checkbox to enable or disable the certificate. A certificate is presented to external services and application only when it is enabled for the scope.
6. To manage the certificate issuer chain, select the Issuer Chain tab.
7. To add a certificate file to the issuer chain, select Add, browse to and select the certificate file to be imported to the chain, and select Apply. The file is imported.

8. To change the certificate scope, select the Scope tab.
9. To set the scope of Forescout subsystems that present the system certificate to external services and applications, do one of the following in the Used for Subsystem field:
    - To present the system certificate for all subsystems, select All.
    - To select a specific subsystem for which the certificate is presented, select the relevant subsystem.

    Note:
    You can select either All or one specific subsystem. To use the same certificate for some, but not all, Forescout subsystems, duplicate the certificate and edit the new certificate's scope. See Duplicate System Certificate Entries.
10. To set the scope of devices on which subsystems can present the system certificate, do one of the following in the Used for Device field:
    - To allow subsystems running on all devices to present the certificate, select All.
    - To allow subsystems running on only a specific device to present the certificate, select the relevant device.

    Note:
    You can select either All or exactly one specific device. To use the same certificate for some, but not all devices, duplicate the certificate and edit the new certificate's scope. See Duplicate System Certificate Entries.
11. To review the certificate signing request (CSR) used for creating this certificate, select the CSR Details tab.
12. Select OK.
13. Select Apply. A summary the changes to be applied is displayed. If the changes are correct, select Yes. eyeSight restarts plugins and product components in the scope of the certificate.

Generate a New System Certificate

Generate a certificate signing request (CSR) and import the signed certificate.

You must have Crypto Administration privileges to perform this procedure.

1. In the Console, navigate to Tools > Options > Certificates > System Certificates.
2. Select Generate CSR . The Manage System Certificate wizard opens to the CSR Form pane. For your convenience, most of the fields are automatically populated with the values used during the last CSR. You can set the certificate validity from 30 days to 10 years. The default validity is three years.
3. Complete the fields and select Next. When the CSR generation completes, the details of the generated CSR are displayed.
4. Copy the CSR text and send it to an external certificate authority (CA).
5. Select Next. Do one of the following:
    - If you have not yet received the signed certificate from the external CA, select Import certificates later. When the certificate becomes available, you can download it to the local file system and then use the Edit feature to import it to this certificate table entry. See Edit System Certificate Entries.
    - If you have access to the certificate file created by the external CA, select Import certificates from selected PKCS#7 file, and browse to and select the signed certificate file to import.
    - If you can view the text of the PEM certificate created by the external CA, select Import certificates from the PEM text below, and paste the text of the signed certificate into the Import pane.
6. Complete the Issuer Chain pane, the Scope pane, and the Description pane as described in Import and Configure System Certificates.
7. Select Finish. The certificate is displayed in the System Certificates pane.

8. Select Apply. A summary of the changes to be applied is displayed. If the changes are correct, select Yes.

Self Signed Certificates

If you need a temporary certificate until a permanent one is issued, or if a "dummy" certificate will suffice for lab environments , you can create a new system certificate that is self-signed.

- Add the self-signed system certificate as trusted to the services that need to verify it.
- Disable certificate validation at the verifying end.

Duplicate System Certificate Entries

To use the same certificate for different scopes, duplicate the certificate and modify it.

You must have Crypto Administration privileges to perform this procedure.

1. In the Console, navigate to Tools > Options > Certificates > System Certificates.
2. Select the table entry to be duplicated, and then select Duplicate. In the System Certificate dialog box, the Certificate Details tab opens, displaying the details copied from the existing system certificate.
3. Edit the scope of the new certificate or replace the certificate. See Edit System Certificate Entries.

Export System Certificate Entries

Export System Certificates as a PKCS#12 file.

You must have Crypto Administration privileges to perform this procedure.

1. In the Console, navigate to Tools > Options > Certificates > System Certificates.
2. Select the table entry to be exported, and then select Export to PKCS#12.
3. In the Export system certificate dialog provide the following information.

Export system certificate	The pathname of the export certificate.
Private key password	The password for the exported certificate file.
Alias name	The alias of the exported certificate file.

4. Select OK to export the certificate.

Remove System Certificate Entries

When you remove a system certificate Forescout components can no longer present it to external applications.

You must have Crypto Administration privileges to perform this procedure.

1. In the Console, navigate to Tools > Options > Certificates > System Certificates.
2. Select the table entry to be removed, and then select Remove.
3. Select Apply. A summary of the changes to be applied is displayed. If the changes are correct, select Yes. eyeSight restarts plugins and product components in the scope of the certificate.

Security deployment hardening best practices

Use these options to harden your Forescout security stature and protect your Forescout deployment.

Maintain Up-To-Date Versions

Ensure that your Forescout software is up-to-date and that you are using the latest releases. See Check for Updates for more information.

Backup Forescout Settings

It is recommended to schedule automatic backups of the Forescout system or component settings to a remote server, via SFTP or SCP. Scheduled backups provide extra safety and protection against data loss.

With SFTP and SCP protocols, public-key authentication achieves a higher level of security and is preferable to password authentication. With password-based authentication, use strong passwords.

You must configure a backup server and an encryption password to perform system or component backup.

If you have logged in to the Console via an Enterprise Manager, the Enterprise Manager and all registered Appliances are backed up to individual files.

Sync High Availability Connectivity

Forescout eyeRecover enables synchronization of data to the High Availability pair for recovery purposes. When adding the High Availability secondary node to the primary node, verify that you pair a legitimate Appliance. To do this, use a direct network connection between the two nodes (not over the LAN).

Refer to the *Forescout Resiliency and Recovery Solutions User Guide* for more information about High Availability pairing and other eyeRecover functionality.

Restrict Access to the Management Interface

Forescout management interfaces provide privileged admin access, and should be protected to reduce the attack surface of eyeSight.

Dedicated Management Segment

When possible, connect management interfaces to an out-of-band management network segment. The management network can be physically isolated from the corporate LAN and detached from external networks.

Limit Access to the Console

Define a list of IP addresses that can access the Console to limit access to specific endpoints. See Define Console Access for more information about configuring this option.

Limit Access to Web Portals

Define a list of IP addresses that can access Forescout web portals to limit access to specific endpoints. See *Web Server Settings* for more information.

Restrict Workstation Access to Management Interfaces

Workstations that access the Forescout management interfaces should be well protected against malicious events, by use of segmentation and endpoint security mechanisms.

Protect iDRAC Interfaces

By default, when Appliances are shipped, the iDRAC component is not configured with an IP address, and all services (except the web interface) are disabled. If you don't intend to use remote management via iDRAC, verify that the dedicated network interface labeled "iDRAC" is not connected to any network.

When using iDRAC for remote management, verify that:

- The iDRAC network interface is connected to a dedicated out-of-band management network
- IP-based access restrictions are configured to allow access only from trusted network sources
- Strong authentication schemes are used when authenticating to iDRAC
- When accessing iDRAC web interfaces, use a valid SSL certificate

Refer to Remote System Management Integration in theForescout eyeSight *Installation Guide* for more information about configuring this option.

Define Secure Configuration Settings

Change default settings to more secure options, unless network or functionality constraints prevent it.

Password and Sessions Policy Settings

Define a secure password policy for Console users, as well as secure session timeout and expiration settings.

Configure Permissions and Scope for Console and Portals

These settings provide powerful calibration of user access. For example:

- Allow access to the entire network range, but never allow access to certain high security features, such as the Appliance configuration or Action Threshold features.
- Allow access to a specific network range, such as a particular building, and grant permission to all Forescout tools.
- Use the Scope pane to grant and limit access to specific ranges or segments in the Console or Assets Portal. Users can only see and work with endpoints in ranges in their Scope. See Access to Network Endpoints – Scope

In addition, you can create users or user groups that have access to only the Console or only to

web portals, or both.

Smart Card Authentication Settings

If your organization uses smart cards for authentication, enable smart card authentication to the Console and web portals. See Using Smart Card Authentication for more information about configuring this option.

HTTPS Redirection Settings

Enable redirect only via HTTPS. See Globally Redirect via HTTPS for information on how to configure this setting. It is strongly recommended that HTTPS redirect is only done with a certificate that is trusted by the endpoints. Either globally trusted or organization-wide trust via a local CA. See The Certificate Pane for more information about this option.

User Directory Settings

Secure LDAP communications with Active Directory to protect and eavesdropping and man-in-the-middle (MitM) attacks.

- Enable Active Directory authentication using TLS and port 636.
- Define a long and complex password as the Directory password on Active Directory. Use these credentials only for the Forescout authentication against the User Directory.

Web Server Settings

Define strict access lists for web access, allowing only specific IP addresses or narrow subnets. Define a range of IP addresses allowed to access the web. IP addresses in this range have access to Forescout web features. See Define Web Access for information about how to configure this option.

Disable access to unused web portals, and to one or more portals or web-based services under relevant security scenarios. See Disable Web Portals

Secure HPS Inspection Engine Settings

Where possible, change default configuration settings with more secure options.

Refer to the HPS Inspection Engine Configuration Guide for information about these options.

Authentication Method

Kerberos is considered the most secured authentication method for Remote Inspection, and is recommended. When using Kerberos, verify the following:

- Before enabling Kerberos, make sure that the Kerberos protocol is operational on the network.
- When eyeSight uses Kerberos authentication, define a dedicated user in the domain controller for interaction with the endpoints. In accordance with Kerberos best practices, it is recommended that delegation permissions be disabled for this user.

If Kerberos is not available, use NTLMv2. It is more secure than NTLM v1.

SMB Version

Select the highest available SMB version. Earlier versions of SMB are known to be vulnerable to various network-based attacks.

SMB Signing

SMB Signing secures SMB communications by use of a digital signature. SMB Signing helps identify SMB Injection attacks and prevent man-in-the-middle (MitM) attacks. As a good security practice in Windows-based environments, system administrators should require SMB signing on endpoints on their networks (for example, via GPO).

To reduce the risk of malicious users (such as in the case of MitM attackers) leveraging Forescout RPC-based Remote Inspection (using SMB), eyeSight can verify that SMB signing is required (or at least enabled) on endpoints and remotely inspect endpoints only with SMB signing.

SNMP Settings

Configure Forescout to use SNMP v3. SNMP v3 encrypts the communications and protects the credentials from eavesdropping. See Configure SNMP Users.

FIPS Support

eyeSight can run in FIPS 140-2 mode, as required by the US Federal Government. This mode is disabled by default. Forescout recommends enabling FIPS mode. In FIPS mode eyeSight uses only FIPS-140 approved cryptographic ciphers. Refer to FIPS mode in the *Forescout eyeSight CLI Commands Reference Guide* for information about enabling FIPS mode.

TLS Settings

Forescout eyeSight v8.5.3 introduces TLS 1.3 support for console-to-backend and inter-appliance communications (IAC).

Important: FIPS compliance is not yet supported by TLS 1.3. This functionality will be supported in a future release.

Configure SecureConnector to support TLS 1.2 only.

Set the Minimum Supported TLS version to TLS v1.2.

When you configure SecureConnector to require TLS version 1.1 or 1.2 to connect to an Appliance, legacy versions of Windows (Windows XP/ Vista/ Windows 2008 server pre-R2) cannot be managed by SecureConnector due to their TLS support limitations.

Disable Password Login

Disable password login to Forescout devices, and configure more secure access in with an SSH key.

On each Appliance, first configure and enable SSH key-based access. Then disable password-based access.

This procedure requires you to login as the cliadmin with sudo permission.

1. Log in to the target Appliance as cliadmin.
2. Run the command `user ssh-passwd status` to view the status of SSH and password login options.
3. If no SSH key has been installed, generate an SSH RSA key pair for your SSH login client and install it on the target Appliance.
   Run the command `User auth setkey` to create the key. Run the command `User auth getkey` to check the key.
4. Configure login using SSH keys for users and verify they work.
5. Run the command `user ssh-passwd status` to verify that SSH key-based login is enabled.
6. Run the command `User ssh-passwd disable` to disable password login.

Regenerating the SSH key

Use this procedure to regenerate the root SSH key on each Appliance.

1. Verify that the `pwd` command executes successfully on all Appliances managed by your Enterprise Manager.
   Log in to the Enterprise Manager command-line interface (CLI) and run the command `fstool oneach pwd`
2. Log in to the CLI on each Appliance and verify the following settings.
   - Run the command `echo $SSH_AUTH_SOCK`. Verify that the environment variable is set to `SSH_AUTH_SOCK=/run/ssh-agent.socket`.
   - Run the following commands to verify High Availability status and integrity.

     ```
     fstool ha status

     fstool ha verify
     ```

3. Regenerate the SSH Key.
   - For an standalone Appliance, log in to the CLI using root credentials and run the command `fstool ssh -k regen`.
     Or
   - For an Enterprise Manager or Recovery Enterprise Manager deployment, log in to the CLI of each Appliance with root credentials and run the command `fstool ssh -k regen`.
4. Synchronize keys of any High Availability pairs.
   In the CLI of the passive device, access the miniroot with the command `ssh -p 2222 him` . Submit the command `fstool ha ssh_key_sync` to synchronize with the key on the active device.
5. Verify that the `pwd` command executes successfully on all Appliances managed by your Enterprise Manager.
   Log in to the Enterprise Manager command-line interface (CLI) and run the command `fstool oneach pwd`
6. Run the following commands on each Appliance to verify High Availability status and integrity.

   ```
   fstool ha status

   fstool ha verify
   ```