ForeScout CounterACT®

Administration Guide

Version 8.0

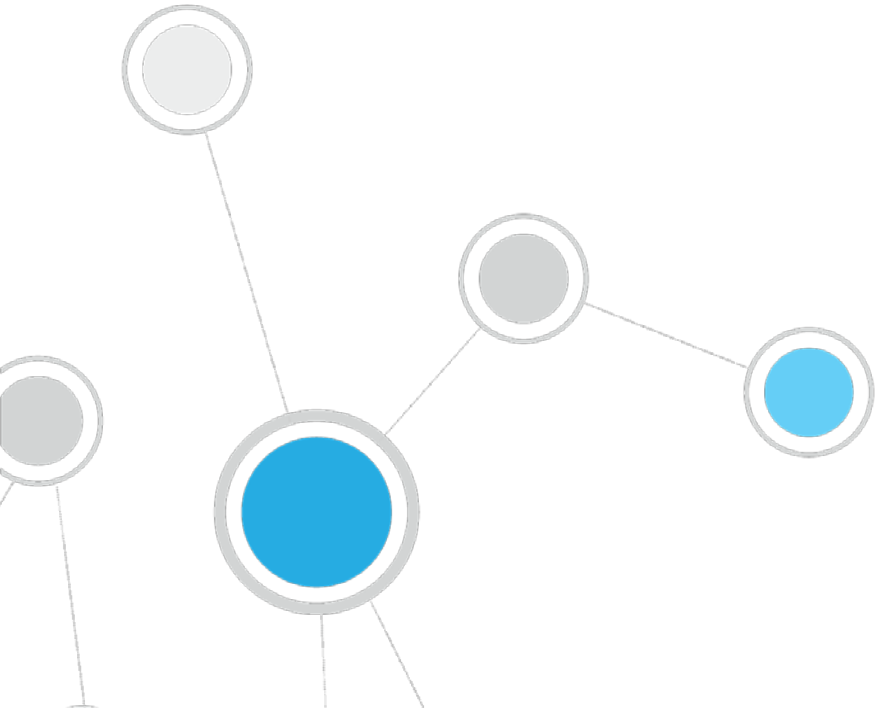


Table of Contents

Preface **16**
About This Guide 17
Additional CounterACT Documentation 19
Documentation Downloads 20
Documentation Portal 20
CounterACT Help Tools 21

Chapter 1: Welcome to CounterACT **22**
About CounterACT 23
Real-Time Network Visibility 23
Policy-Initiated or Manual Control 24
Comprehensive Third-Party Orchestration 25
On-Demand Asset Intelligence 25
CounterACT Components 26
The Appliance 27
The Enterprise Manager 28
The Console 28
Virtual Systems 29
Help Tools 29
Console Help Buttons 30
CounterACT Help 30
Feature Dialog Box Descriptions 30
On-Screen Troubleshooting 31
Documentation Portal 32
Plugin/Module Configuration Help 33

Chapter 2: Working with the Initial Setup Wizard **34**
About the Initial Setup Wizard 35
Before You Begin 35
Logging In to CounterACT 35
Forgot Your Password? 38
Updating Wizard Settings 39
Setup Scenarios 39
Set Up an Appliance from Scratch 39
Welcome 39
License (CounterACT Virtual Systems Only, Per-Appliance Licensing Mode) 40
Time 42
Mail 43
User Directory 44
Domain Credentials 46
Authentication Servers 47
Internal Network 48
Enforcement Mode 49
Channels 49
Switch 53

Policy 55
Asset Inventory 56
Finish 58
Set Up an Appliance with Enterprise Manager Settings 59
Assign IP Addresses 60
Finish 61
Set Up an Enterprise Manager from Scratch 62
Set Up an Enterprise Manager with Appliance Settings 62
Finish 64
When You Are Done 64
Review Console and Assets Portal Access Assignments 64
Set Up Segments 64
Set Up Segment Properties 65
Set Up Ignored IPs 65
Review, Run and Edit Pre-Defined Template Policies 65
Set Up HTTP Redirection for Policies 66
Set Up a Threat Protection Policy and Define Legitimate Traffic for Threat Protection Policies 66
Review Asset Inventory Items and Create Lists 66
Set Up Map Locations 67
Opt In to ForeScout Research and Intelligent Analytics Program 67

Chapter 3: Working in the Console 69
About the Console 70
Title Bar, Menu Bar, Toolbar and Status Bar 70
Title Bar 70
Menu Bar 71
Toolbar – Console Views 71
Status Bar 75
Console Searches 76
Wildcard Searches 76
Working in the Site Map 76
Enable or Disable the Map 78
Set Up the Map – Create Site Locations 78
Customize Display Thresholds for Map Indicators 81
Map Tools 82
Working with CounterACT Detections 85
Home Views 88
Working in the Detections Pane 91
Tracking Endpoints Using the Detections Pane Filter 91
Controlling the Detections Pane Columns 91
Viewing Mouse-Over Table Information 94
Controlling Endpoints from the Detections Pane 94
Working in the Filters Pane 101
Working with Asset Inventory Detections 102
How the Asset Inventory Is Learned 104
Filtering the View 105
Asset Inventory View Panes 106
Customizing the Asset Inventory 110

View Lists and Values Associated with an Asset Inventory Item 113
Use Inventory Detections to Create Powerful Policies 114
Working with CounterACT Segments 114
Working with Organizational Units 120
Adding and Removing Segments from Organizational Units 121
Working with CounterACT Groups 122
Creating an Ignored IP List 126
Restricting Endpoint Inspection 126
Getting More Information about Endpoints 127
Details Pane 127
Host Log 134
Assets Portal 136
Working with the ForeScout Compliance Center 136
Using the Compliance Center vs. Policies 137
What the Endpoint Users See 137
Accessing the Compliance Center from the Endpoint 139
Exiting the Console 140

Chapter 4: CounterACT Policy Templates 141
Working with Policy Templates 142
Creating Policies Using Templates – Basics 142
Tips for Rolling Out Templates 145
Template Structure 146
Asset Classification and Primary Classification Templates 147
About Classification 147
Template Classification Groups 148
Properties Resolved by a Primary Classification Policy 150
Prerequisites 151
Using the Template 151
Which Devices Are Inspected – Policy Scope 152
How Devices Are Classified – Policy Condition 155
Handling Discovered Devices – Policy Actions 156
Replacing Asset Policies 156
Using an Action to Assign a Classification 156
Fine-Tuning the Classification Mechanism 158
Classification Upgrade Impact Analysis Template 159
Prerequisites 160
Using the Classification Upgrade Impact Analysis Template 160
Which Devices Are Inspected – Policy Scope 161
How Devices Are Classified and Compared – Policy Condition 162
Compare Classification Results 163
Stop the Migration Classification Policy 164
Upgrade the Classification Version 164
Mobile Classification Template 164
About the Mobile Classification Template 164
Prerequisites 165
Using the Mobile Classification Template 165
Which Devices Are Inspected – Policy Scope 166
How Mobile Devices Are Detected – Policy Condition 166

How CounterACT Handles Discovered Devices – Policy Actions 168
Manually Assigning a Classification 168
External Device Classification Template 168
About the External Device Classification Template 168
Prerequisites 169
Using the External Device Classification Template 170
Which Devices Are Inspected – Policy Scope 170
When Are Endpoints Removed from Groups? 171
How CounterACT Handles Discovered Devices – Policy Actions 171
Virtual Machine Classification Template 171
About the Virtual Machine Template 172
Using the Virtual Machine Template 172
Which Devices Are Inspected – Policy Scope 172
How Virtual Machines Are Detected – Policy Condition 173
How Virtual Machines Are Handled – Policy Actions 175
Passive Learning Mode Template 175
Passive Learning Sub rules 176
Corporate/Guest Control Template 177
About the Corporate/Guest Control Template 177
Deploying a Corporate/Guest Control Policy 177
Prerequisites 178
About Corporate/Guest Classification 178
Using the Corporate/Guest Control Policy Template 179
Which Devices Are Inspected – Policy Scope 180
Handling Guests – Guests Page 180
Working with Guest Registration Options 182
What Happens When the Authentication Values Are Changed? 184
External Disk Drive Compliance Template 184
About the External Disk Drive Compliance Template 184
Prerequisites 185
Using the External Disk Drive Compliance Template 185
Which Endpoints Are Inspected – Policy Scope 186
Detecting Authorized External Disk Drives 186
Detecting External Disk Drives – Policy Sub-Rules 188
Handling Noncompliant External Disk Drives – Policy Actions 188
Overall Endpoint Compliance Template 189
About the Overall Endpoint Compliance Template 189
Prerequisites 190
Using the Overall Endpoint Compliance Template 190
Which Endpoints Are Inspected – Policy Scope 190
Required and Restricted Applications Pages 191
Detecting Compliance Status – Policy Condition 192
How CounterACT Handles Noncompliant Devices – Policy Actions 195
Compliance Notification at Endpoint 198
Individual Compliance Templates 198
Windows Update Compliance Template 199
About Windows Update Compliance Template 199
Prerequisites 199
Using the Windows Update Compliance Template 199
Which Endpoints Are Inspected – Policy Scope 199

Detecting Noncompliant Windows Endpoints – Policy Condition 200
Handling Windows Hosts – Policy Actions..... 201
Macintosh Update Compliance Template..... 202
About Macintosh Update Compliance Template..... 202
Prerequisites..... 202
Using the Macintosh Update Compliance Template..... 202
Which Endpoints Are Inspected – Policy Scope 203
Detecting Noncompliant Macintosh Endpoints – Policy Condition..... 203
Handling Macintosh Hosts – Policy Actions 204
Threats Templates..... 204
About the Threats Templates 205
Prerequisites..... 205
Using the Threats Templates..... 205
Which Endpoints Are Inspected – Policy Scope 205
Malicious Hosts Template 206
ARP Spoofing Template 208
Impersonation Template 210
Dual Homed Template..... 212
Track Changes Templates..... 215
Prerequisites..... 215
Using the Track Changes Templates 215
Which Hosts Are Inspected – Policy Scope 216
How Frequently Are Endpoints Inspected – Change Time..... 216
How a Change Is Detected – Policy Condition..... 217
How a Change Is Handled – Policy Actions..... 218
How to Modify a Condition – Advanced Settings 218
New TCP/IP Port Template..... 218
About the New TCP/IP Port Template 219
Prerequisites..... 219
Using the New TCP/IP Port Template 219
Which Endpoints Are Inspected – Policy Scope 219
Handling Endpoints with New TCP/IP Ports – Policy Actions..... 221

Chapter 5: Policy Management 222
What Is a Policy?..... 223
How Policies Are Structured 223
Working with Policies 224
When Are Policies Run?..... 224
What You See in the Console in the Home view..... 225
Using Groups 230
Broaden the Scope – Plugins and Extended Modules 230
Basic Policy Rollout Tips 230
CounterACT Policy Priorities..... 231
Handling Endpoint Identity Changes 232
Stopping the Policy from the Appliance 232
Viewing and Managing Endpoints..... 233
The Policy Manager..... 235
Policy Manager Tools 235
Working with the Policy Manager 236
Creating Custom Policies 241

Defining a Policy Name and Description 242
Defining a Policy Scope 243
Defining a Policy Main Rule 246
Defining Policy Sub-Rules 248
Advanced Policy Options 250
Main Rule Advanced Options 250
Sub-Rule Advanced Options 255
Policy Preferences 258
Defining Authentication Servers 259
HTTP Preferences 260
Customizing HTTP Pages 266
Email Preferences 267
Customizing Endpoint Identity Change Thresholds and Detection Mechanisms 268
Time Settings 270
HTTP Login Attempts 272
Property Lists 273
Categorizing Policies 273
Policy Reports and Logs 276
Policy Reports 276
Policy Logs 277
Policy Safety Features 280
Working with Action Thresholds 280
Handling Irresolvable Criteria 287
Handling Criteria Defined as Empty Lists 288
Misconfigured Add to Group Policy 289

Chapter 6: Working with Policy Conditions 290

About Policy Conditions 291
What Is a Policy Condition? 291
Meeting Condition Criteria 292
Condition Shortcuts 292
Irresolvable Criteria 292
Case Sensitivity 292
Properties 292
Property Expression Types 293
Properties and Scripts 293
Windows Endpoint Applications Vendor Support 293
Working with Properties 294
Properties Delivered with Plugins and Extended Modules 294
Querying for Property Values 295
Authentication Properties 296
Classification Properties 297
Advanced Classification Properties 298
Device Information Properties 300
Event Properties 305
External Devices Properties 307
Guest Registration Properties 307
Linux Properties 308
Macintosh Properties 309

Remote Inspection Properties 310
SNMP Properties 310
Switch Properties 311
Track Changes Properties 314
User Directory Properties 314
Windows Properties 315
Windows Application Properties 318
Windows Security Properties 319
Detecting New Vulnerabilities and Newly Supported Vendor Applications 320
Defining Custom Conditions 322
Using Custom Conditions 324
Comparing Property Results 324
Defining and Managing Lists 326
Use a Wizard to Create Lists 326
Create Lists Based on Endpoint Detections 329
Using the Lists That You Create 330

Chapter 7: Working with Actions 333

About Actions 334
Actions Delivered with Modules and Extended Modules 334
Gradual Action Enforcement 335
Action Tools 335
Enabling and Disabling Actions 335
Action Schedules 335
Property Tags in Actions 336
Action Thresholds 336
Scripts and Interactive Actions 336
Accessing Console Actions 337
Working with Actions 337
Audit Actions 338
Send Message to Syslog 338
Authenticate Actions 339
HTTP Login 339
HTTP Sign Out 361
Classify Actions 362
Set Function Classification 362
Set OS Classification 363
Set Network Function 365
Manage Actions 366
Add to Group 366
Add Label Action 367
Delete Label Action 368
Delete Host 369
Delete Properties 369
Disable Remote Inspection 370
HTTP Localhost Login 370
Recheck Host 373
Start SecureConnector / Stop SecureConnector 373
Upgrade OS X SecureConnector 377
Set Counter Action 378

Notify Actions 379
HTTP Notification 379
HTTP Redirection to URL 382
Send Balloon Notification 382
Send Email 383
Send Email to User 384
Send Notification (OS X) Action 385
Remediate Actions 385
Disable Adapters on Dual Homed Devices 386
Disable External Devices 386
Expedite IP Discovery 387
Kill Instant Messaging 388
Kill Cloud Storage 389
Kill Peer-to-Peer 390
Kill Process on Linux and Kill Process on Macintosh 391
Kill Process on Windows 391
Run Script on CounterACT 392
Run Script on Linux and Run Script on Macintosh 393
Run Script on Windows 394
Set Registry Key on Windows 396
Start Antivirus 397
Start Macintosh Updates 398
Start Windows Updates 399
Update Antivirus 404
Windows Self Remediation 405
Restrict Actions 408
Switch Restrict Actions 408
Virtual Firewall 411
Action Tools 415
Creating Action Schedules 416
Enabling and Disabling Actions 417
Working with Property Tags 418
Action Icon Display Tool 420
Policy Action Log 420
About HTTP Actions 421
Transmitting Actions via HTTPS 423
Captive Portal Detection Exceptions 424
Action Thresholds 425

Chapter 8: Base, Content and Extended Modules 426
About Base, Content and Extended Modules 427
Base Modules 427
Content Modules 430
Extended Modules 431
Centralized Module Management 434
Installing a Module 434
Plugin Configuration Management 435
Plugin and Module Security 436
Check for Updates 436
How Do You Know if a New Software Version Is Available? 436
Configuring Check for Updates 437

Roll Back to Previous Module Versions 438
Designing Customized Plugins 438

Chapter 9: Assets Portal 440
About the Assets Portal 441
Search Tools 441
Search Status 441
Expanding Information Discovered by the Assets Portal 442
Importing and Exporting Information 443
Assets Portal User Management 443
Defining Assets Portal Users and Permissions 443
Accessing the Assets Portal 444
Add the Assets Portal to Your Web Browser 446
Performing an Assets Portal Search 446
Host-Based Ticket Results 448
User-Based Ticket Results 449
Viewing Additional Information 449
Page Display 449
Clearing Event Detections 449

Chapter 10: Generating Reports and Logs 451
About Reports 452
On-Screen Threat Protection Reporting 452
Executive Reports 453
Operational Reports 454
Generating On-Screen Threat Protection Reports 457
Customizing Reports 458
Viewing Multiple Reports 461
Viewing Report Definitions 462
Working with On-Screen Report Management Tools 462
Generating Scheduled Reports 463
Report Scheduler Management Tools 467
Opening Saved Reports 469
Opening a Scheduled Report 471
Reports Portal 471
Working with System Event Logs 474
Viewing Block Events 475
Refreshing the List of Events 477
Viewing a History of Monitored and Blocked Services 477

Chapter 11: Managing Your Virtual Firewall Policy 479
Defining a Virtual Firewall Policy 480
What You See on Your Screen 480
Policy Priorities 481
Defining Block Rules 481
TCP versus UDP Blocking 481
Working with Block Rules 482
Viewing Block Events 483

Defining Allow Rules 484
Removing and Editing Allow Rules 486

Chapter 12: Threat Protection 487

About Threat Protection 488
Detecting Threats – How It Works 488
Basic Terminology 489
About the Threat Protection Policy 493
About Advanced Policy Tools 493
Viewing Threat Detections 494
High Activity Mode 494
Viewing and Updating the Policy 495
Blocking Worms Using Plugins 497
Customizing Basic Policy Settings 498
Customizing Scan Settings 498
Customizing Bite Settings 501
Bite Type Details 504
Customizing Email Worm Settings 505
Configuring the Block Method 507
Handling Service Attacks 508
Managing Threat Protection Mail Alert Deliveries 513
Working with Manually Added Endpoints 516
Manually Adding an Endpoint 516
Defining the Active Response Range 520
Viewing Endpoint Activity Details 521
Events Tab 521
Managing Enterprise Lockdown Alerts 527
Legitimate Traffic 529
Handling Legitimate Activity of Malicious Sources 530
Defining Legitimate Traffic 531
Automatically Defining Legitimate Scanning Activity – Wizard 532
Manually Defining Legitimate Scanning Applications 533
Manually Defining Removed Servers 535
Creating Customized Legitimate Traffic 536
Editing and Removing Legitimate Traffic 539

Chapter 13: Threat Protection, Advanced Tools 540

Defining Mark Naming Conventions 541
Defining Mark Rules 541
Editing and Removing Mark Naming Rules 545
Defining Lists 545
Applying Mark Naming Rules 546
Defining Virtual Site Endpoint Operating System Parameters 546
Parsing Event Information Displayed in Email Alerts 547

Chapter 14: Managing Users 549

About CounterACT Users 550
Creating Users and User Groups 551
Working with Permission and Scope Options 551

Access to Network Endpoints – Scope 557
Modifying User Details 559
Removing Users 559
Password Protection 560
Audit Logs 562
Login Preferences 562
Login Notice and Consent Message Before Login 562
Login Notice and Consent Message After Login 563
Log in to Each CounterACT Web-Based Portal 564
Session Handling Preferences 564
Support for One-Time Password Authentication 564
Disconnecting Inactive Console Users 565
Allowing One Login Session per Console User 565
Manual User Password Change 566
Using Smart Card Authentication 568
Setting Up Smart Card Authentication 569
Smart Card Configuration 569
Smart Card User Setup 571
Monitoring User Activity 572

Chapter 15: Managing Appliances, Enterprise Managers and Consoles..... 575

About Management 576
CounterACT Device Management Overview 576
Console Management 576
Defining Console Access 577
Multiple Console Logins 578
Defining Web Access 578
Disabling Web Portals 579
Configuring HTTP Strict Transport Security 581
Configuring the Time Zone 581
Customizing Alarm Indicators 582
Configuring Console Memory Settings 582
Configuring Console View Settings 583
Standalone Appliance Management 583
Enterprise Manager Management 583
Upgrading the Enterprise Manager Software 584
Viewing Enterprise Manager System Health Information 586
Stopping and Starting the Enterprise Manager 587
Appliance Management 587
Viewing Appliance Health Information 588
Registering Appliances with the Enterprise Manager 589
Upgrading Appliance Software 591
Upgrading the Console 593
Starting and Stopping Appliances 593
Working with Appliance Folders 594
Managing Groups of Appliances 599
Appliance Endpoint Performance Capacity 601
Working with Appliance Channel Assignments 601
Viewing Information about CounterACT Devices 609

Viewing Appliance Traffic Statistics 612
Configuring Features for an Appliance or Group of Appliances 613
Apply Uniform Configuration Settings to All Appliances 613
Define a Configuration for a Single Device or Group of Devices 614
Editing and Updating a Configuration 614
Limiting User Access to Appliances 615
Viewing Limitations 616
Controlling Command-line Access to CounterACT Devices 616
Configure Session Security Features for Command-Line Interaction 616
Configure Password Protection for the Boot Loader 617

Chapter 16: The Dashboard 619
About the Dashboard 620
Accessing the Dashboard 620
What You See in the Dashboard 621
Dashboard Layout 621
Before You Begin 623
How the Dashboard is Populated 623
Run the Dashboard Policy Template 623
Working with Dashboard Widgets 625
Selecting the Reporting Interval 625
Expanding a Widget 626
Adding a Widget 627
Dashboard Feature Updates 631

Chapter 17: License Management 632
About License Management 633
Default Licensing Modes in CounterACT 634
Centralized Licensing Mode 635
Per-Appliance Licensing Mode 635
Per-Appliance CounterACT Device License 635
Per-Appliance Extended Module License 647
Switch Licensing Mode from Per-Appliance to Centralized 654
Receiving License Alerts 655

Chapter 18: Additional Options 656
Working with the Internal Network 657
Working with Hosts without IPv4 Addresses 658
Working with Hosts Whose IPv4 Address Is Used by Another Host 659
Managing Email Notification Addresses 660
Signing Emails with an S/MIME Certificate 660
Generating CSRs and Importing Signed Certificates 661
Working with Digitally Signed Emails 661
Defining Endpoint Discovery Rules 662
Working with the Enforcement Mode 667
Backing Up System and Component Settings 667
Scheduling Automatic Backups of CounterACT Settings to External Servers . 668

Performing a One-Time System Backup 674
Backing Up and Restoring the rSite for Your Appliances..... 675
Recovering an Enterprise Manager..... 675
Language Support 675
Displaying Endpoint Information in a Local Language 676
Localizing CounterACT Redirected Web Pages and Messages 677
Displaying Local Languages in Reports, Actions and Other Features 681
Localizing Guest Management Portal Texts 682
Pre-Registration and Guest Registration Management 682
Guest Management Portal 682
Guest Registration Pane 683
Registered Guests 685
Password Policy..... 693
User Policy 694
Sponsors..... 694
Terms and Conditions 695
Guest Notifications 696
Sponsor Notifications 697
The ForeScout Research and Intelligent Analytics Program 698
Sharing Additional Endpoint Properties..... 699
Opting In or Out of Data Sharing..... 699

Appendix 1: Handling Network Connectivity Failures 702

Appendix 2: Remote Access to Endpoints 704
When Is Remote Access to Endpoints Needed?..... 705
Domain Account Requirements 705
Using a Domain-Wide Policy 705
Using an Administrator Group 706
Using the Security Configuration Wizard..... 707
Working with Windows XP SP2 Machines 707
Updating Group Policy Objects with New Windows Firewall Settings 707
Troubleshooting Domain Credentials..... 709
A. Test the Domain Credentials 709
B. Test the Credentials on the Endpoint Using a Localhost Query 710
C. Test the Credentials in the Endpoint Using Remote Query..... 710
Troubleshooting Deep Inspection..... 715

Appendix 3: Generating and Importing a Trusted Web Server Certificate 717

Appendix 4: HTTP Redirection 719
About HTTP Redirection..... 720
HTTP Redirection Procedure..... 720
Security Considerations..... 721
Sample fstool netconfig Session 721

Appendix 5: SNMP Support and Integration 724
SNMP Integration 725
About SNMP Service Settings..... 725

Configure SNMP Service Settings 725
Performance Thresholds for SNMP Notifications 733

Appendix 6: SNMP MIB for CounterACT Appliances 735
About the SNMP MIB for CounterACT Appliances 736
MIB Table Objects for CounterACT Appliances 737
SNMP Trap Notifications for CounterACT Appliances 742

Appendix 7: Customizing User Interfaces 749
The CounterACT User Portal Builder 750
Opening the User Portal Builder 751
Using the User Portal Builder to Customize Skins 752
Deploying a Skin for a User Interface 754
The Legacy Customization Tool 755
Opening the Legacy Customization Tool 755
Using the Customization Tool to Customize Skins 759
Saving and Integrating a Customized Page 763
Customized ForeScout Compliance Center (FCC) Pages 764
Customize Text and Labels 766

Appendix 8: Configuring the Certificate Interface 769
About the Certificate Interface 770
Configure Certificate-Related Settings 770
Configure Certificate Expiration Monitoring 771
Auto-download CRLs 771
Verify Ongoing TLS Sessions 772
Configure the Trusted Certificates Table 772
Import and Configure Trusted Certificates 772
Edit Trusted Certificate Entries 775
Remove Trusted Certificate Entries 778
Configure the System Certificates Table 778
Certificate Precedence between Appliance and Enterprise Manager 778
Import and Configure System Certificates 779
Generate a New System Certificate 781
Generate a CSR for a New System Certificate 782
Duplicate System Certificate Entries 786
Export System Certificate Entries 786
Edit System Certificate Entries 786
Remove System Certificate Entries 788

Preface

This section provides the following information:

- **About This Guide**
- **Additional CounterACT Documentation**

About This Guide

This guide is a manual for new users and a reference tool for experienced users. It is designed for users who have logged in to the Console from a ForeScout CounterACT® Enterprise Manager or Appliance. Instructions and explanations in the guide refer to both login scenarios, unless specifically noted.

Refer to the *CounterACT Installation Guide* for information on software installation, post-installation and other installation procedures for CounterACT components, including the Enterprise Manager, Appliance and Console. See Additional CounterACT Documentation for information on how to access the Installation Guide.

This Administration Guide consists of the following chapters:

Chapter 1: Welcome to CounterACT	This chapter presents general information about CounterACT functionally and components.
Chapter 2: Working with the Initial Setup Wizard	This chapter details the initial steps required to configure CounterACT. The Initial Setup wizard provides critical configurations to ensure that you get your system up and running quickly and efficiently.
Chapter 3: Working in the Console	This chapter details the basic Console tools that you should be familiar with before you begin working.
Chapter 4: CounterACT Policy Templates	CounterACT provides a full range of templates to help you create NAC policies quickly and effectively using default settings. This chapter instructs you how to work with templates in general and then provides step-by-step procedures for creating template-based policies that cover important network security tasks, for example: ▪ Primary classification and asset classification ▪ Antivirus, Peer-to-Peer ▪ Corporate and guest control ▪ Windows and Macintosh update compliance ▪ Mobile device classification ▪ External disk drive compliance ▪ Virtual machine classification
Chapter 5: Policy Management	This chapter describers how to create and manage custom policies.
Chapter 6: Working with Policy Conditions	This chapter describes how to work with CounterACT policy conditions.
Chapter 7: Working with Actions	This chapter describes how to work with CounterACT policy actions, used to control network endpoints.
Chapter 8: Base, Content and Extended Modules	This chapter describes Base Modules, Content Modules, and Extended Modules.

Chapter 9: Assets Portal	This chapter describes how to set up and work with the Assets Portal. The Assets Portal is a web-based search and discovery tool that allows you to leverage extensive network information collected and correlated by CounterACT and plugins. This includes not only endpoint information, but also Policy violations, login histories, User Directory details, organizational mapping details and endpoint device connections. The information is useful across your organization, especially for: ▪ Security teams ▪ IT departments ▪ Help Desk
Chapter 10: Generating Reports and Logs	This chapter describes CounterACT report generation tools. These tools provide you with important compliance information, as well as detailed information about malware and self-propagating code. Reports about policy compliance, inventory and vulnerabilities can be generated from the Reports site. In addition, user audit trail and system event logs can also be generated.
Chapter 11: Managing Your Virtual Firewall Policy	This chapter contains information about working with Virtual Firewall rules. Network Virtual Firewall protection allows you to easily create network security zones to give you more control over network traffic and provides all the benefits of an inline firewall without being located inline.
Chapter 12: Threat Protection	CounterACT's Active Response technology fights worms and other self-propagating malware by: ▪ Pinpointing threats at the earliest stage of the infection process ▪ Providing real-time protection against zero-day worms ▪ Protecting your network against infection methods known and unknown to the security community This chapter provides basic information about the Active Response malicious endpoints technology, including how CounterACT defines, detects and handles threats. It also describes how to define legitimate traffic as part of your Threat Protection policy, i.e., traffic to be ignored for requirements that compel you to grant full access to specific addresses.
Chapter 13: Threat Protection, Advanced Tools	This chapter provides information regarding advanced tools available for handling threats including: defining naming conventions for marks, defining virtual site endpoint operating system distribution and density, and parsing event information displayed in email alerts.
Chapter 14: Managing Users	This chapter describes how to: ▪ Create and manage CounterACT users. ▪ Define user permissions. ▪ Create password protection policies. ▪ Audit user activity.
Chapter 15: Managing Appliances, Enterprise Managers and Consoles	Use the tools described in this chapter to update settings defined during your setup. Additional options, such as upgrading your software version are also detailed.

Chapter 16: The Dashboard	This chapter describes how to set up and use the Dashboard.
Chapter 17: License Management	This chapter describes how to acquire and manage CounterACT and Extended Module licenses.
Chapter 18: Additional Options	This chapter describes additional CounterACT options.
Appendix 1: Handling Network Connectivity Failures	This appendix details how to handle network connectivity failures between the Appliance and your network.
Appendix 2: Remote Access to Endpoints	This appendix details how to gain remote access to an endpoint's registry service. You must perform these steps to take advantage of the policy scanning processes.
Appendix 3: Generating and Importing a Trusted Web Server Certificate	This appendix describes how to generate and import a trusted certificate and remove the browser security warning that opens when trying to access the CounterACT Web Portals.
Appendix 4: HTTP Redirection	For browser notification, login and remediation actions the Appliance must see traffic going to the web. This appendix details how to make these actions work properly, including how to set the IP address used by the HTTP redirection features; for example, the Assets Portal or the Reports Portal.
Appendix 5: SNMP Support and Integration	This appendix describes CounterACT SNMP support.
Appendix 6: SNMP MIB for CounterACT Appliances	This appendix describes: ▪ About the SNMP MIB for CounterACT Appliances ▪ MIB Table Objects for CounterACT Appliances ▪ SNMP Trap Notifications for CounterACT Appliances
Appendix 7: Customizing User Interfaces	This appendix describes customizations that can be made to the user interface: ▪ The CounterACT User Portal Builder ▪ The Legacy Customization Tool ▪ Customize Text and Labels
Appendix 8: Configuring the Certificate Interface	This appendix details how to use the Certificates Interface for handling trusted and system certificates.

Additional CounterACT Documentation

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

- Documentation Downloads
- Documentation Portal
- CounterACT Help Tools

Documentation Downloads

Documentation downloads can be accessed from the ForeScout Resources Page, or one of two ForeScout portals, depending on which licensing mode your deployment is using.

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

Software downloads are also available from these portals.

To identify your licensing mode:

- From the Console, select **Help > About ForeScout CounterACT…**.

ForeScout Resources Page

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

To access the ForeScout Resources Page:

1. Go to https://www.forescout.com/company/resources/.
2. Select **Technical Documentation** and search for documents.

Product Updates Portal

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

To access the Product Updates Portal:

1. Go to https://updates.forescout.com/support/index.php?url=counteract.
2. Select the CounterACT version you want to discover.

Customer Portal

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

To access documentation on the ForeScout Customer Portal:

1. Go to https://forescout.force.com/support/.
2. Select **Downloads** or **Documentation**.

Documentation Portal

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

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

To access the Documentation Portal:

1. Go to https://updates.forescout.com/support/files/counteract/docs_portal/.
2. Use your customer support credentials to log in.
3. Select the CounterACT version you want to discover.

CounterACT Help Tools

Access information directly from the CounterACT Console.

Console Help Buttons

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

CounterACT Administration Guide

Select **CounterACT Help** from the **Help** menu.

Plugin Help Files

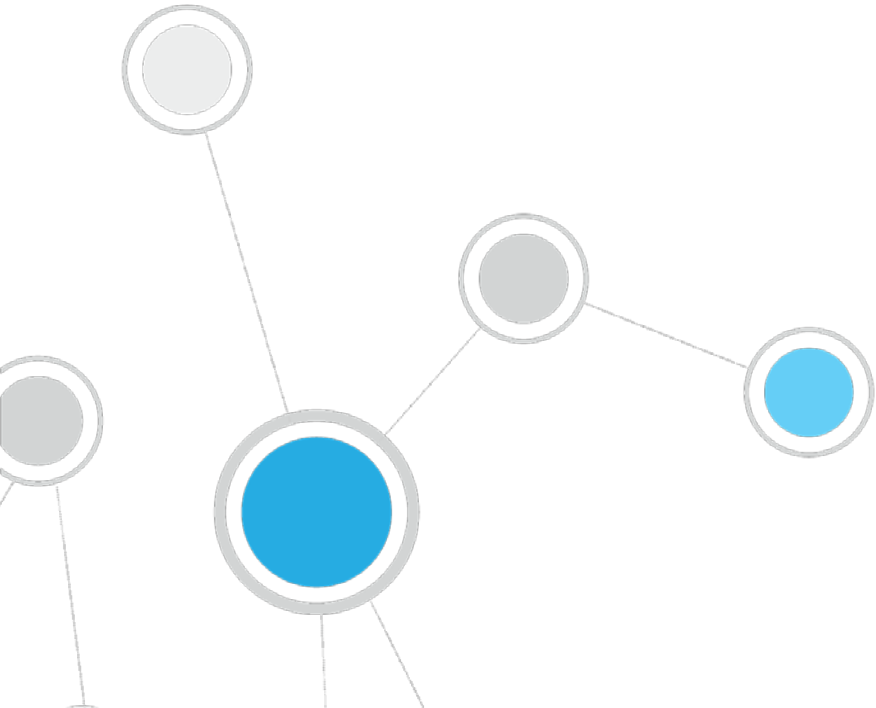
1. After the plugin is installed, select **Options** from the **Tools** menu and then select **Modules**.
2. Select the plugin and then select **Help**.

Documentation Portal

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

Chapter 1: Welcome to CounterACT

- About CounterACT
- CounterACT Components
- Help Tools



About CounterACT

The CounterACT platform provides infrastructure and device visibility, policy management, orchestration and workflow streamlining to enhance network security. CounterACT provides enterprises with real-time contextual information of devices and users on the network. Policies are defined in CounterACT using this contextual information that help ensure compliance, remediation, appropriate network access and streamlining of service operations. This is delivered by providing:

- Real-Time Network Visibility
- Policy-Initiated or Manual Control
- Comprehensive Third-Party
- On-Demand Asset Intelligence

Real-Time Network Visibility

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

- Desktops, laptops and servers
- Mobile devices such as smartphones and tablets
- Personal vs. corporate devices
- On-premise virtual machines and off-premise 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 device

CounterACT 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 in device types connected, software and configurations, compliance requirements and the internal and external threat landscape. Controls from notification, remediation and restriction are needed based on enterprise policies enacted by CounterACT to secure the network.

Some examples of CounterACT's 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 devices 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

CounterACT allows 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 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
- Enterprise Mobility Management systems
- Almost any third-party product using a web API, SQL or LDAP

When integrating with third-party systems, use the CounterACT 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 CounterACT to third-party systems
- Set up third-party systems to trigger CounterACT actions

Integration is carried out by working with *ForeScout Extended Modules*. See Chapter 8: Base, Content and Extended Modules for more information about modules.

On-Demand Asset Intelligence

Use CounterACT 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.

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 network activity at multiple levels; for example, processes and services currently running, vulnerabilities currently detected, ports currently open or users currently logged in. 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 an Assets Portal

The Assets Portal is a web-based search and discovery tool that allows you to leverage extensive network information collected and correlated by CounterACT and its plugins. This includes not only endpoint information, but also network policy violations, current login information, User Directory identity details, organizational mapping details and endpoint device connections. The accumulated information makes the portal valuable across organizational teams.

- Security teams can use the IP address provided by the Assets Portal to quickly locate and shut down switch ports and eliminate a security threat.
- IT departments can use the IP address provided by the Assets Portal to locate and contact users when maintenance is required at the endpoint.
- The Help Desk can effortlessly link IP addresses, computer hardware addresses and switch ports to employees in real time.

CounterACT Components

CounterACT is comprised of the following components:

- The Appliance
- The Enterprise Manager
- The Console

Sample CounterACT Device

Virtual systems are also available. See Virtual Systems for more information.

Connections between CounterACT devices use fingerprints for verification purposes. When a connection is established, the fingerprints of the two CounterACT devices are compared. If they match, the connection is accepted. This ensures that only trusted CounterACT devices are connecting 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, CounterACT Technical Note* for information regarding Enterprise Manager/Appliance communication. See Additional CounterACT Documentation for information on how to access this guide.

The Appliance

A CounterACT appliance (Appliance) is a dedicated device that monitors traffic going through your corporate network. It protects 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 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 feature, refer to the *ForeScout CounterACT Resiliency Solutions* guide. For more information about Appliance installation, Appliance specifications and deployment, refer to the *CounterACT Installation Guide*. See Additional CounterACT Documentation for information on how to access these guides.

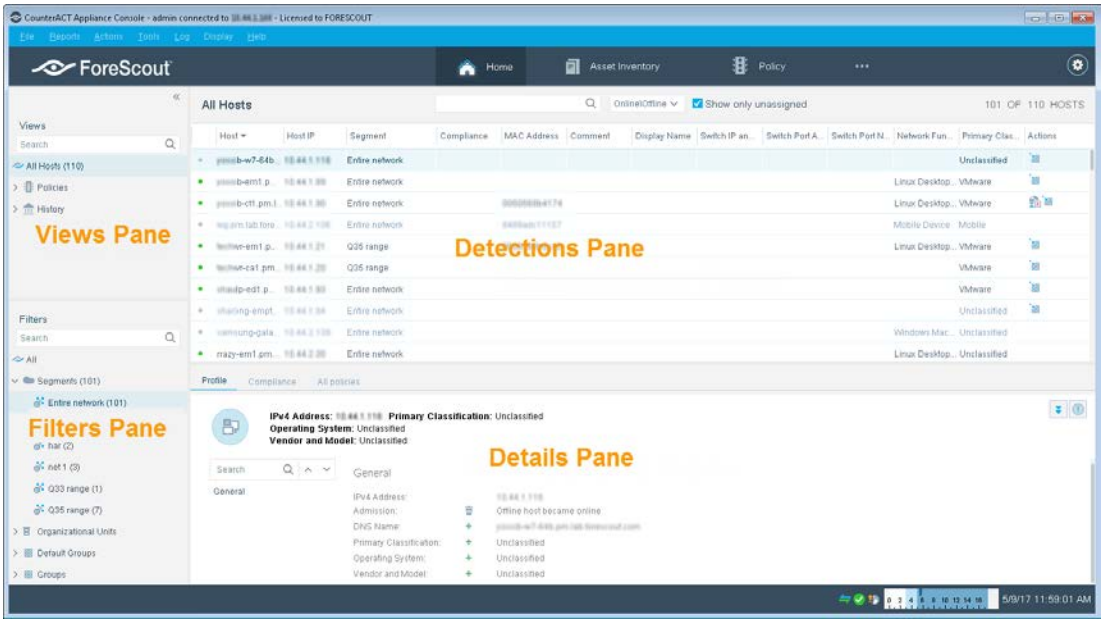
The Enterprise Manager

The Enterprise Manager is an aggregation device that communicates with multiple CounterACT 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.

The Console

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



Console

About the Console

Detection information is displayed in the Console, your unified information, management and control center. Key features include:

- An integrated display of endpoints detected by your NAC, Threat Protection, Compliance and Corporate/Guest Control policies, as well as other endpoints discovered by CounterACT.
- 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 currently running, vulnerabilities currently detected, ports currently open or users currently logged in.
- 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 endpoints 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 CounterACT's response to these activities.
- Control tools allow you to start and stop CounterACT devices and update the configuration defined during installation; for example, the network range CounterACT is protecting or the time zone setting. Other control tools allow you to communicate with your network management application and work with third-party applications.

Virtual Systems

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

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

Using CounterACT virtual devices lets you:

- 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.

If your deployment is operating in Per-Appliance Licensing Mode, installing and working with licenses differs slightly for virtual systems and physical systems. Refer to Virtual Licenses for details about working with virtual licenses.

Hybrid Deployments

Hybrid deployments are also supported. This means that a physical Enterprise Manager can manage both physical and virtual Appliances, and a virtual Enterprise Manager can manage both physical and virtual Appliances.

Help Tools

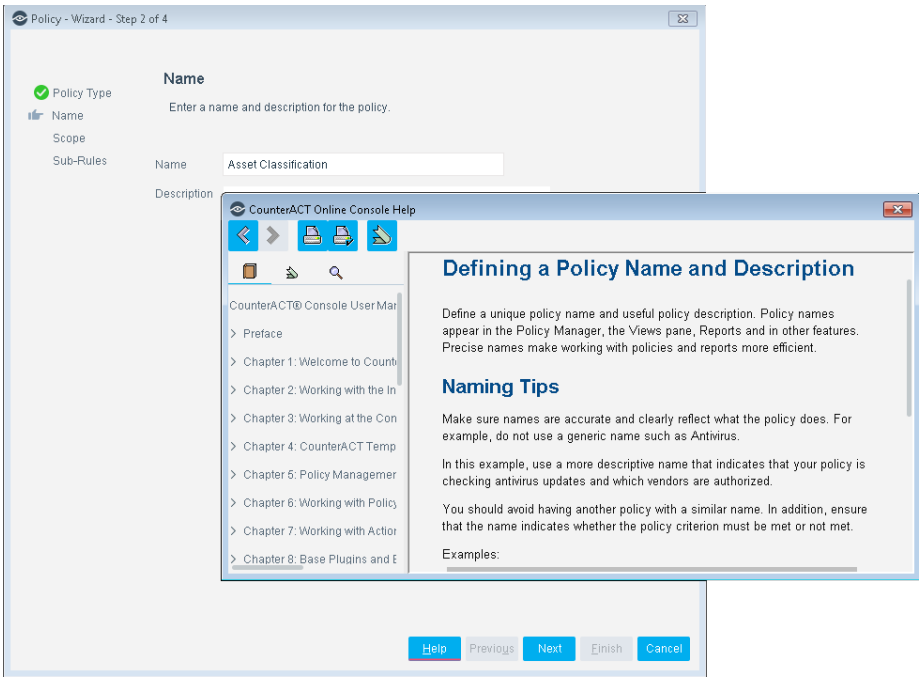
CounterACT provides a range of Help tools to assist first-time users in gaining proficiency and an understanding of the CounterACT Console. Help tools also guide

veteran users in working with more advanced Console options. This section describes help tools available and how to access them.

- Console Help Buttons
- CounterACT Help
- Feature Dialog Box Descriptions
- On-Screen Troubleshooting
- Documentation Portal
- Plugin/Module Configuration Help

Console Help Buttons

You can quickly access specific information about the tasks and topics that you are working with by using Help buttons that appear in Console dialog boxes, panes and wizard pages.



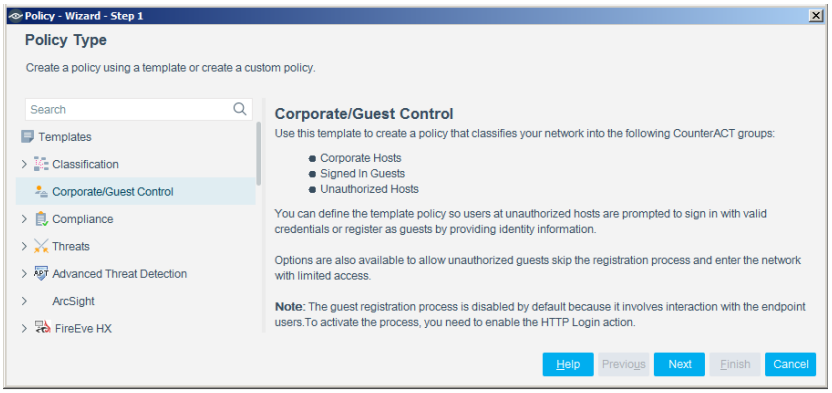
Help Button Example

CounterACT Help

Select **CounterACT Help** from the **Help** menu to open the CounterACT online help.

Feature Dialog Box Descriptions

CounterACT dialog boxes are designed with text that is automatically displayed to provide helpful descriptions about various Console features.



Example of Description in Dialog Box

On-Screen Troubleshooting

Two types of on-screen troubleshooting are available:

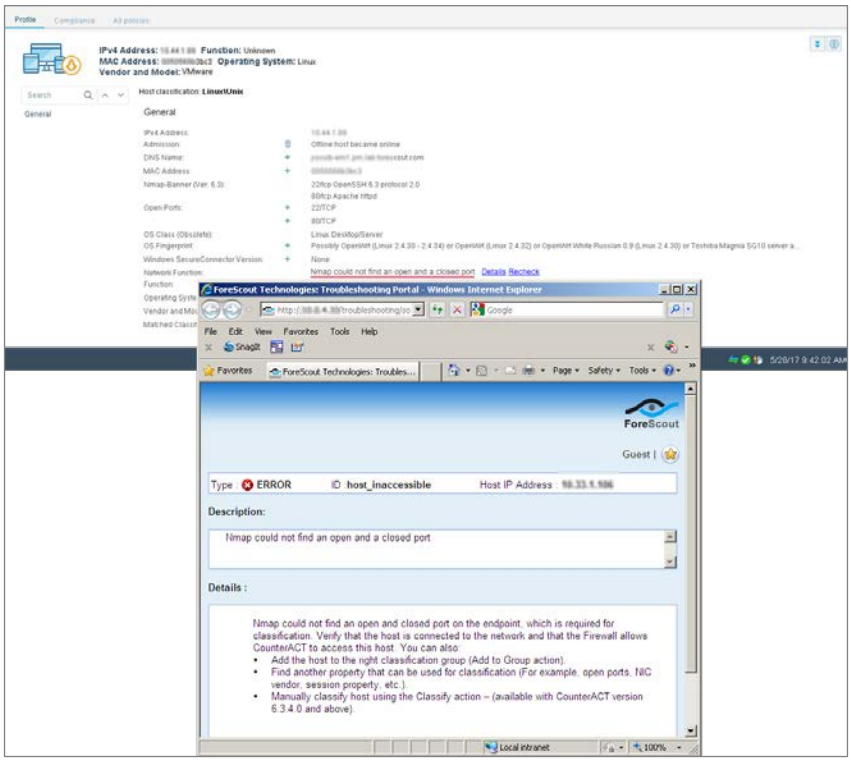
- Troubleshooting Messages
- Troubleshooting Endpoint Policy Matches

Troubleshooting Messages

Troubleshooting messages about irresolvable issues, failed actions and other errors can be displayed in the Detections pane for a selected endpoint. Information is also available about resolving these issues.

To view troubleshooting tips for these messages:

1. From the Home view, select (**Show troubleshooting messages**) at the top right corner of the Details pane.
2. In the Details pane, select the **Details** link that is displayed after the red text. The link may appear in any tab where an unresolved event occurred. A window opens with troubleshooting tips.



Example of On-Screen Troubleshooting

Troubleshooting Endpoint Policy Matches

You can quickly troubleshoot an endpoint policy match by viewing member-of-group assignments per policy. This information is graphically displayed in a *Policy flow* diagram accessed from the *All Policies* 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.

Documentation Portal

The Documentation Portal is an online library containing a comprehensive range of information about CounterACT tools, features and functionality. The portal includes the following sets of documents:

- CounterACT Administration Guide (this document)
- CounterACT Installation Guides
- CounterACT How-to Guides
- CounterACT Plugin and Module Configuration Guides
- FStool Command Reference Guide
- CounterACT Glossary Reference Guide
- CounterACT Console Features Shortcuts Reference Guide
- Advanced Technical Notes

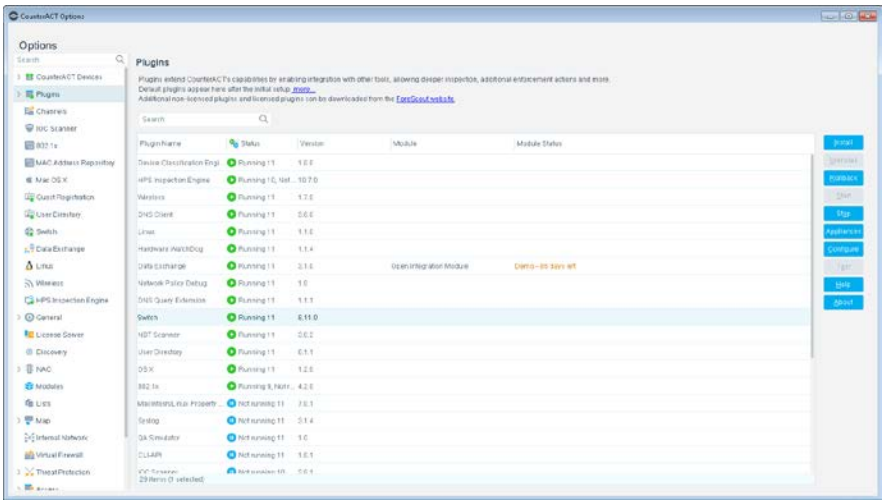
Access the Documentation Portal:

- At the Console, select **Help** and then select **Documentation Portal**.
- From your Internet browser at http://www.forescout.com/kb (use Product Updates Portal login credentials).

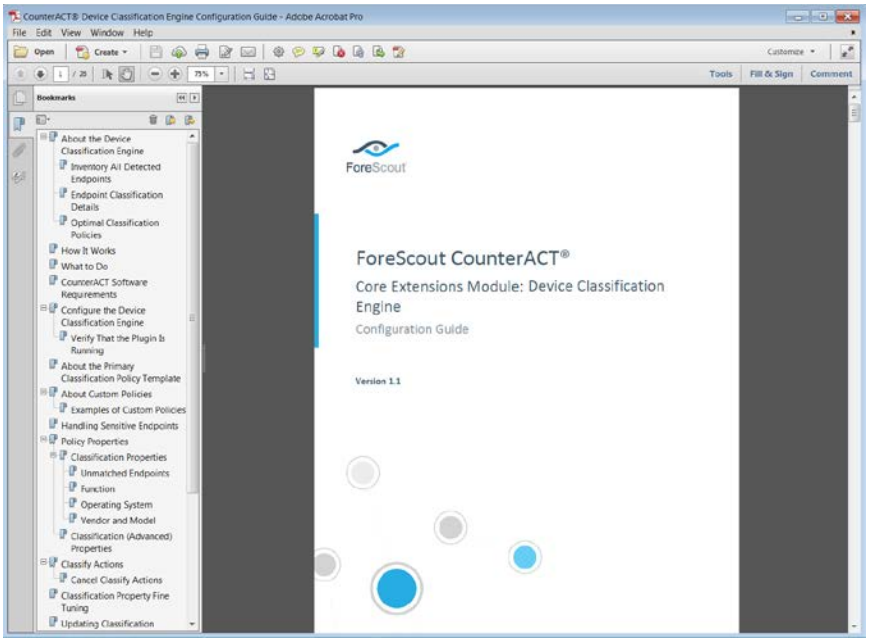
If your deployment is using Centralized Licensing Mode, you may not have credentials to access this portal.

Plugin / Module Configuration Help

When configuring CounterACT's various components, you can access the Configuration Guides directly from the Modules pane by selecting **Help**.



Accessing Online Help



Help File Sample

Chapter 2: Working with the Initial Setup Wizard

- About the Initial Setup Wizard
- Setup Scenarios
- Set Up an Appliance from Scratch
- Set Up an Appliance with Enterprise Manager Settings
- Set Up an Enterprise Manager from Scratch
- Set Up an Enterprise Manager with Appliance Settings
- When You Are Done

About the Initial Setup Wizard

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

Proceed as follows:

1. Review the Before You Begin section.
2. Run the Initial Setup wizard.
3. Review the When You Are Done section for information regarding additional basic setup tasks.

Before You Begin

Prepare the following information regarding the CounterACT device that you want to configure:

- 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.
- CounterACT 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 CounterACT 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 CounterACT can analyze which endpoints have successfully authenticated.
- Core switch IP address, vendor and SNMP parameters.

This information is tested and saved by the wizard at each stage of the setup. A verification message is displayed, indicating if the settings are valid or not.

Logging In to CounterACT

Access to the CounterACT device via the Console is authenticated by verifying the appropriate CounterACT IP address, user name and password. Make sure that you have this information before attempting to log in.

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

To access the CounterACT Console:

1. Select **ForeScout CounterACT**>**CounterACT Console** from the **Start** menu.

   The CounterACT Login dialog box opens.

CounterACT Login Dialog Box

2. Type the CounterACT device IP address or host name in the **IP/Name** field.
3. Select a login method.

   These login authentication methods are available:

   – Select **Password** to perform standard authentication. Enter your user name and password.

   – Select **Smart Card** to allow authentication using a smart card. Enter your PIN code. If the **Dll Location** field is empty, enter the location where the Smart Card driver is installed on your computer. See Using Smart Card Authentication for more information.

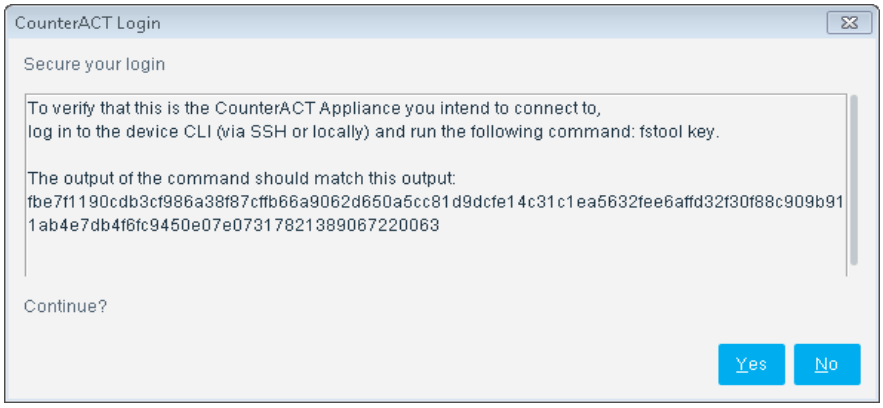
Smart Card Login

4. Select **Save address and user name** to instruct CounterACT to remember these credentials when you next log in.
5. Select **Login**.
6. If prompted with a Notice and Consent dialog box, read the message and then select **Accept**.

Verifying the CounterACT Device

When logging in to the Console for the first time, a dialog box opens asking you to verify that you are connecting to a trusted CounterACT device. This is done by comparing the output of an fstool command with the string that appears in the dialog box. Verifying ensures that you are logging in to a secured CounterACT component with protected Console credentials.

Select **Yes** to proceed with login *only after you have followed the instructions that appear in the dialog box*.



CounterACT Device verification

To verify:

1. Log in to the CounterACT device CLI.
2. Run the following command:

   `fstool key`

3. Verify that the output of the command matches the value displayed in the CounterACT Login dialog box.

Forgot Your Password?

If you are a CounterACT operator and forgot your password, contact your System Administrator or another user authorized to create a new one. If you are the *admin* user and forgot your password, you can update it remotely.

Update the Admin password from the CounterACT device. This tool is designed for administrators with root privileges.

To update the password:

1. Log in to the CounterACT device CLI.
2. Run the following command:

   `fstool passwd`

   The following message opens:

   ```
   Current Admin password:
   ```

3. Type your current Admin password.

   The following message opens:

   ```
   New Admin password:
   ```

4. Type a new password. Use between six and fifteen characters, including at
5. least one non-alphabetic character.
6. Press **Enter**.

   The following message opens:

   ```
   New Admin password (confirm):
   ```

7. Retype the password and press **Enter**.
8. The following message opens:

```
User 'admin' password updated.
```

Updating Wizard Settings

Most of the options defined here can be modified from the CounterACT Options dialog box.

To access the Options window:

1. Select **Options** from the **Tools** menu.

Setup Scenarios

The following sections describe the various setup scenarios available when installing CounterACT Enterprise Manager or Appliances.

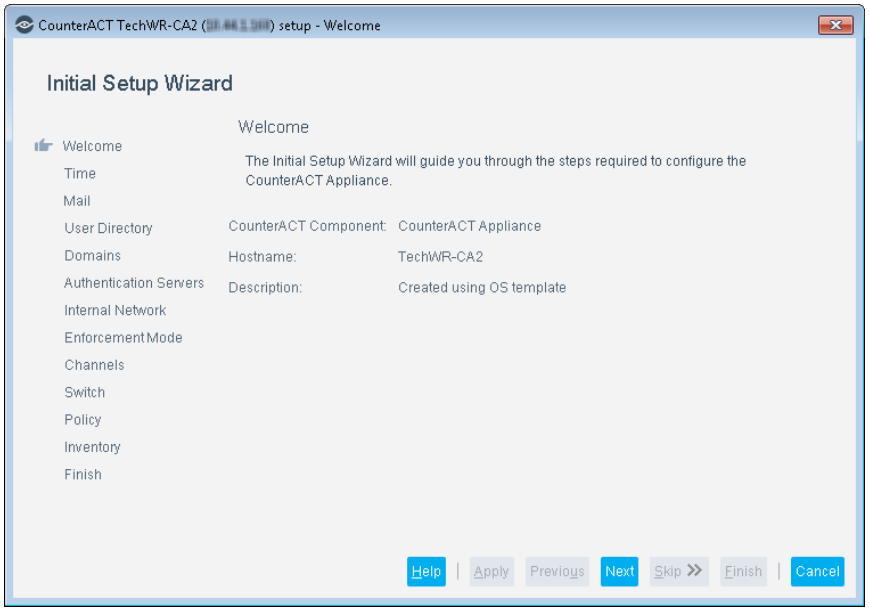
- Set Up an Appliance from Scratch
- Set Up an Appliance with Enterprise Manager Settings
- Set Up an Enterprise Manager from Scratch
- Set Up an Enterprise Manager with Appliance Settings

Set Up an Appliance from Scratch

After logging in to the Console for the first time, you are prompted to follow the on-screen wizard instructions described in the following sections.

Welcome

The Welcome page displays the CounterACT 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 from the CounterACT Options window.



Welcome Page, Appliance

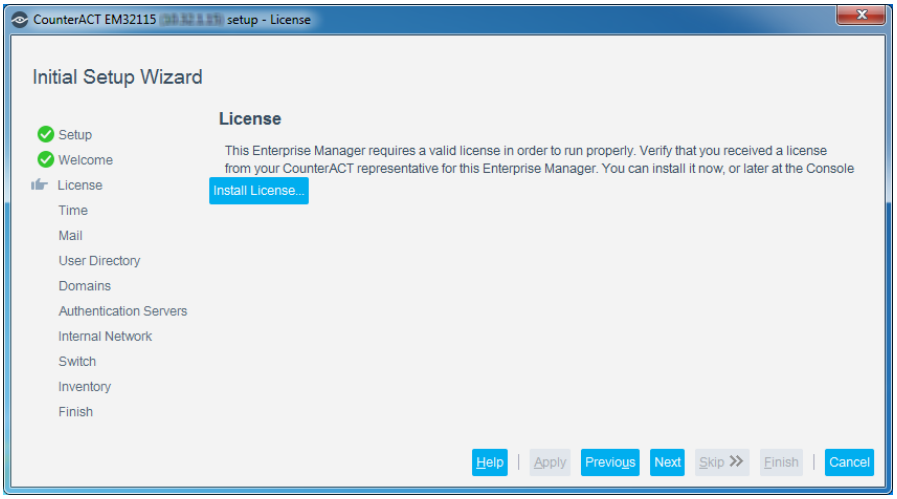
License (CounterACT Virtual Systems Only, Per-Appliance Licensing Mode)

If you are working with a CounterACT virtual system operating in Per-Appliance Licensing Mode, the License page appears.

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.

Refer to the CounterACT Installation Guide *for information about installing CounterACT virtual systems.*

The License page allows you to install the virtual demo license that was provided by your CounterACT representative by email. The license is valid for 30 days from the time it was generated by the ForeScout representative. When installing the license, you are presented with the license's expiration date. You must request and install a permanent license before this period expires. See Virtual Licenses for details.



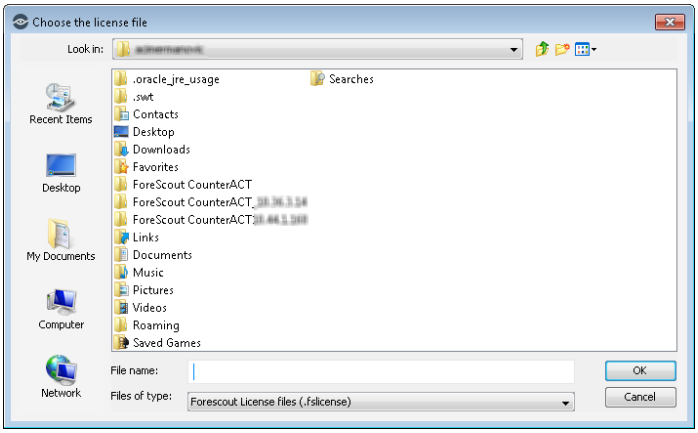
License Page

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 Viewing License Alerts for more information.

Virtual licenses are authenticated daily by the ForeScout License Server (at https://license.forescout.com). Licenses that cannot be authenticated for a month are revoked. If this happens, significant CounterACT functionality will stop. See Virtual Licenses for information about working with the License Server.

To install a virtual license:

1. Select **Install License** and then select the required license. The Choose the license file dialog box opens.



Choose the License File Dialog Box

2. Navigate to the license and then select **OK**. The Install License from File dialog box opens.

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 tailored for a specific device.

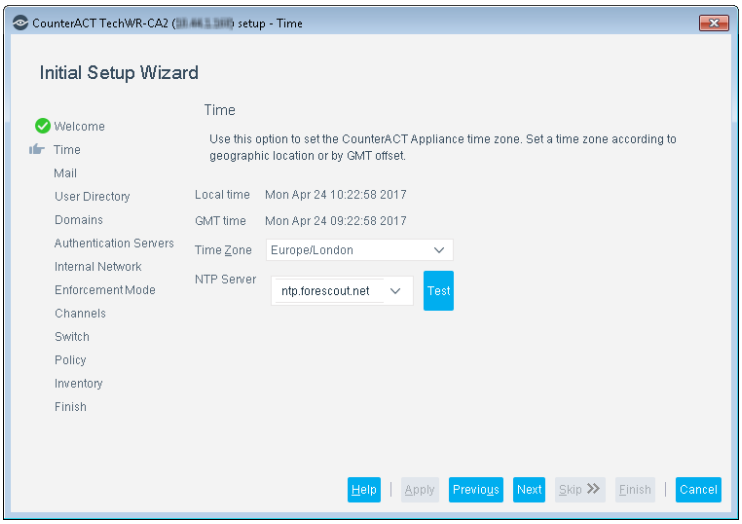
3. Select the device and then select **Install**.

   A dialog box opens with information about the start and end date for installing the license, as well as other license information.

4. Complete the wizard.

Time

Define time settings for this Appliance.



Time Page

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.

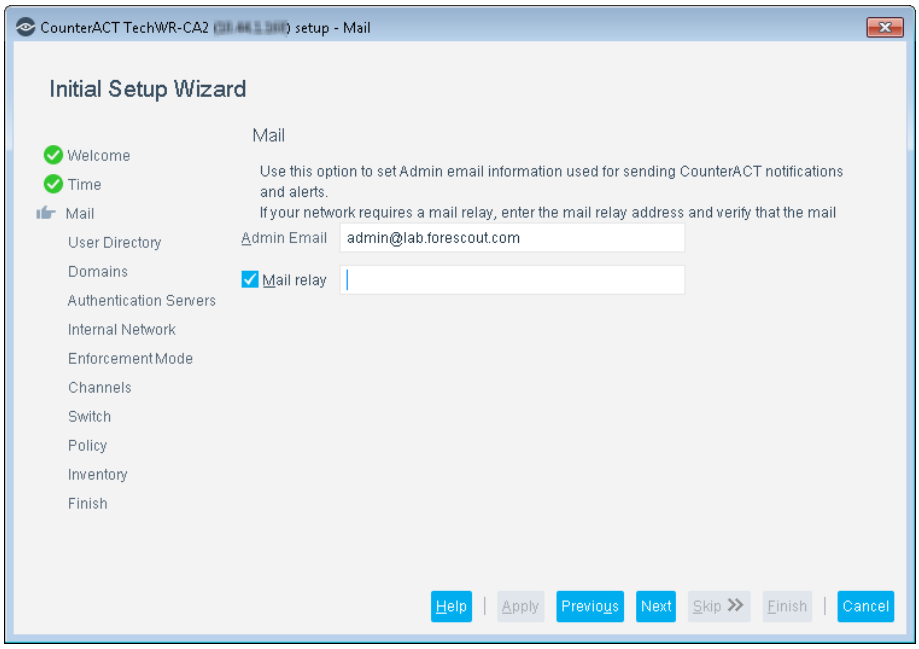
NTP Server	CounterACT devices require NTP connectivity (port 123 UDP) to an NTP server. Enter an NTP server that your organization connects to or use the ForeScout default (ntp.foreScout.net). Select **Test**. If the test fails, contact your IT professional. Use the **`fstool ntp setup`** command to define additional NTP servers: **1.** Log in to the Enterprise Manager CLI. **2.** Run the following command: **`fstool ntp setup`** <servers> where <servers> is a comma-separated list of IP addresses of NTP servers you prefer (local or remote). CounterACT will use these servers for time synchronization.

Mail

CounterACT generates email messages regarding:

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

Mail relay and Admin email addresses are defined here.



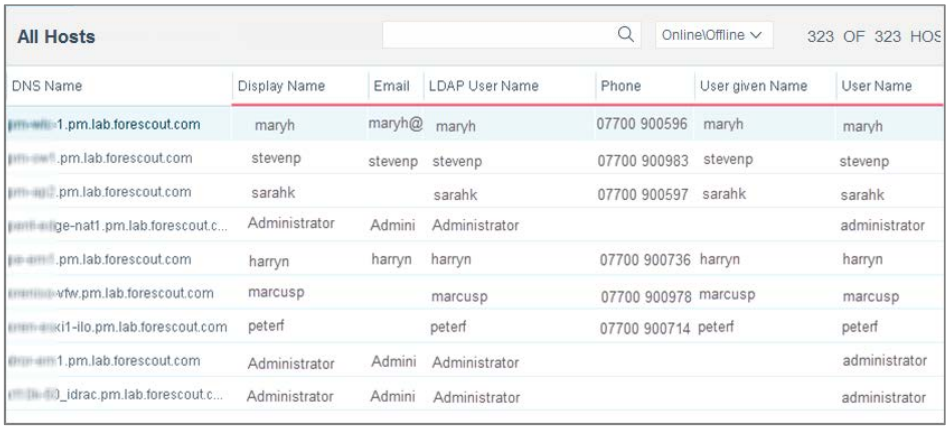
Mail Page

Admin Email (Required)	The CounterACT administrator address or another address that should receive CounterACT 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 (port 25) traffic is not allowed from CounterACT to the Internet. This must be the fully qualified host name. For example, mail-relay.example.com. If you type an incorrect address you will not receive CounterACT alerts.

You can change these addresses from the CounterACT Options window by selecting **General** and then **Mail**.

User Directory

Use this option to define credentials for a User Directory server. These credentials are used to validate network authentication and resolve user details. For example, the endpoint user's User Directory display name, department name or email address.



User Credentials in the Console

CounterACT allows you to define various types of User Directory servers.

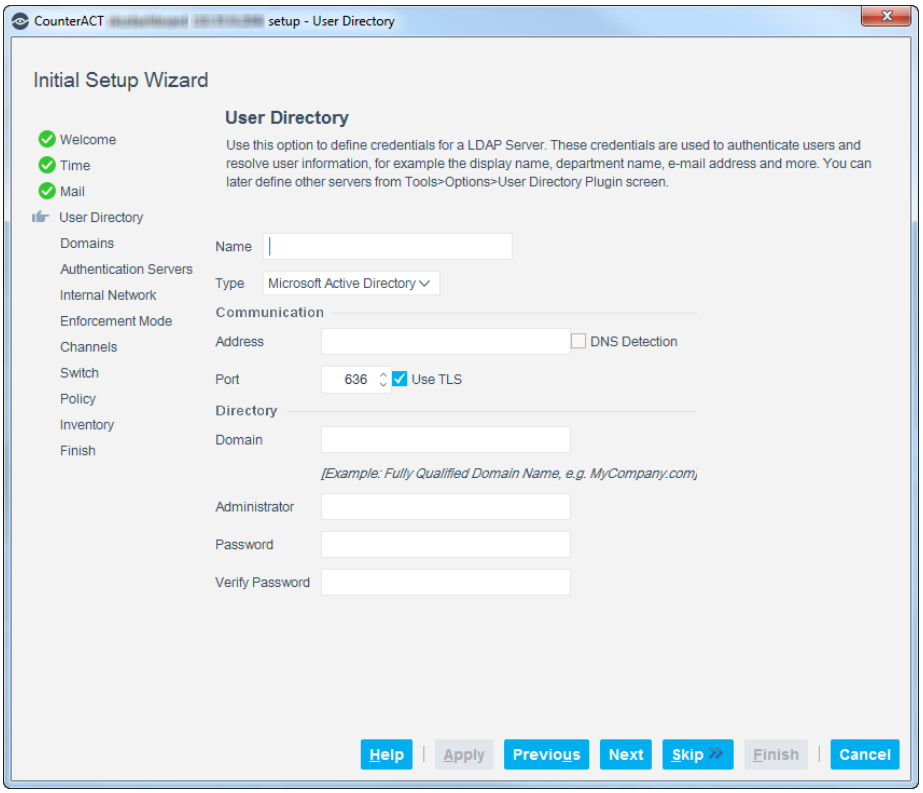
The following user directory and authentication servers are supported:

- 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.

You cannot configure RADIUS or TACACS authentication servers using the Initial Setup Wizard.

You can define additional User Directory servers from the CounterACT Options window by selecting **User Directory** and then **Add**.



User Directory Page

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:

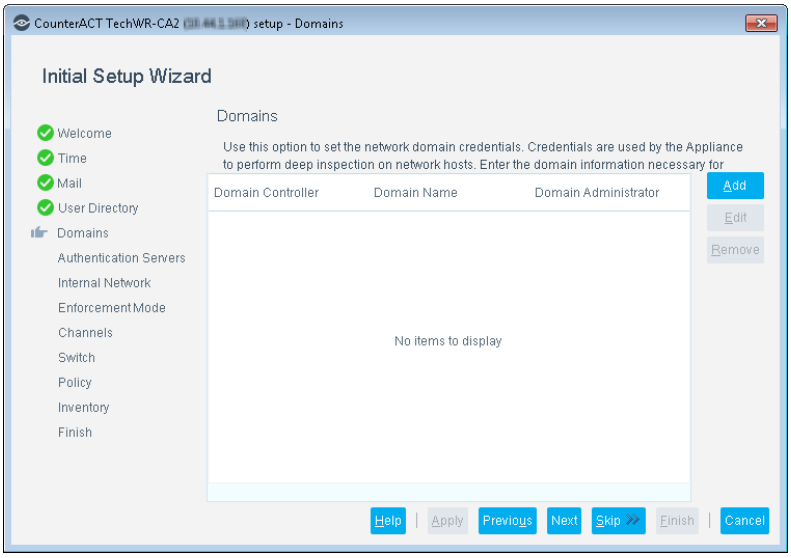
Name	Enter the hostname of the server. ***Note:*** *This value cannot be edited later.*
Type	Select a server type: ▪ Microsoft Active Directory ▪ Novell eDirectory ▪ Oracle Directory ▪ IBM Lotus Notes ▪ OpenLDAP Server ***Note:*** *This value cannot be edited later.*

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 the **DNS Detection** checkbox to instruct CounterACT to learn directory servers based on the domain name that you configure 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 to instruct CounterACT 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**. User details and authentication status are displayed in the Console, Detections pane. For more information about User Directory server setup, refer to the *User Directory Plugin Configuration Guide*.

Domain Credentials

Network domain credentials are used by the Appliance to perform deep inspection on endpoints. 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.



Domains Page

Select **Add** and define the following:

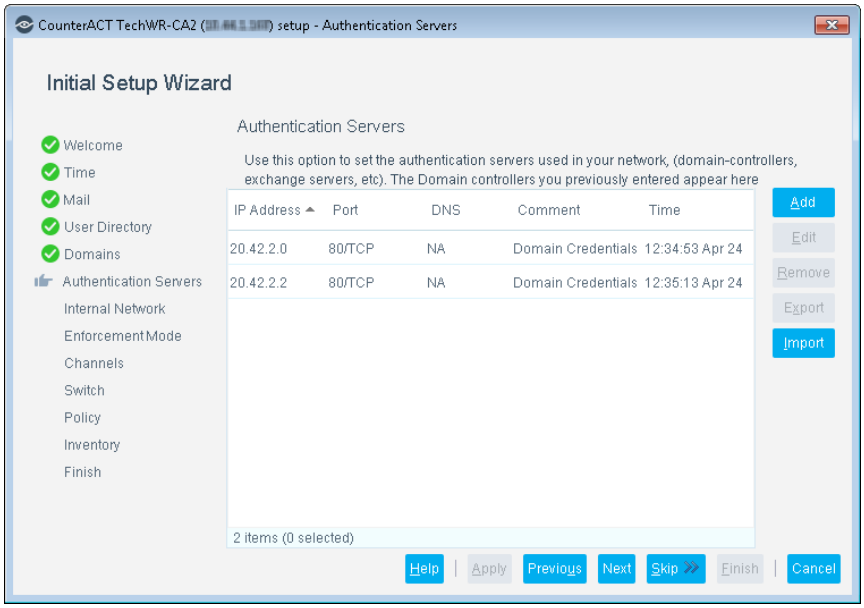
Domain Controller	The Domain Controller IP address. This information is used to test password validity and provide defaults for the authentication servers defined later.
Domain Name	The domain name. The domain should include all endpoints that you want to inspect via the policy. Endpoints in this domain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

Additional domain options let you fine-tune certain inspection process definitions and perform other testing. Refer to the "Configuration" section of the HPS Inspection Engine Configuration Guide*. See Additional CounterACT Documentation for information on how to access this guide.*

If the verification test fails, you may need to perform troubleshooting tasks. See Appendix 2: Remote Access to Endpoints for more information.

Authentication Servers

Policies can be created to verify that endpoints have authenticated successfully. Use this option to define the authentication servers used in your network (domain controllers, exchange servers, etc.). The domain controllers that you previously entered appear here automatically.



Authentication Servers Page

Select **Add** and define authentication servers.

CounterACT supports the following services for authentication:

- HTTP (80/TCP)
- Telnet (23/TCP)

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

Internal Network

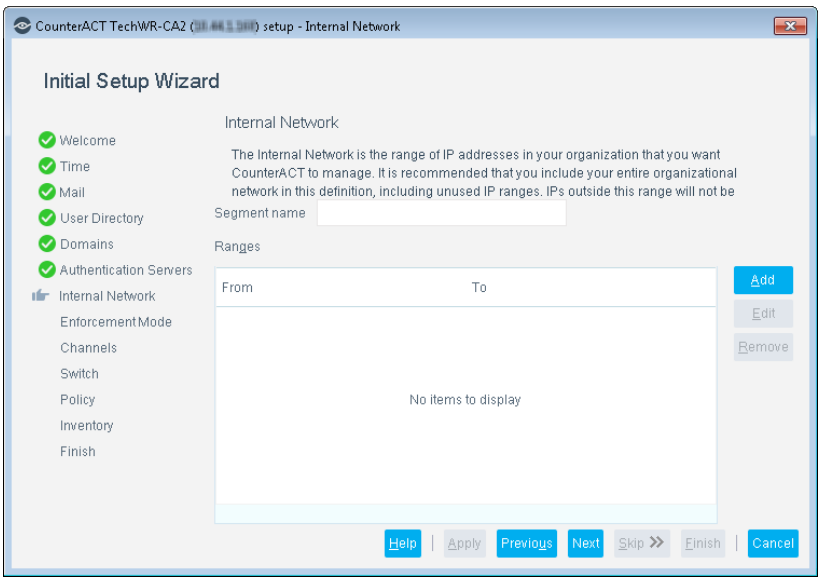
The ***Internal Network*** is a set of network segments or IP ranges that defines your network in CounterACT. When CounterACT detects endpoints with IP addresses within the Internal Network, they are assumed to be in your network.

The Internal Network defines the extent of CounterACT's management activity - for example, when a CounterACT 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 CounterACT's Internal Network definition, are not managed by CounterACT. In addition, endpoints in the Internal Network must be visible to CounterACT Appliances.

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

Several CounterACT 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 CounterACT Segments for more information.

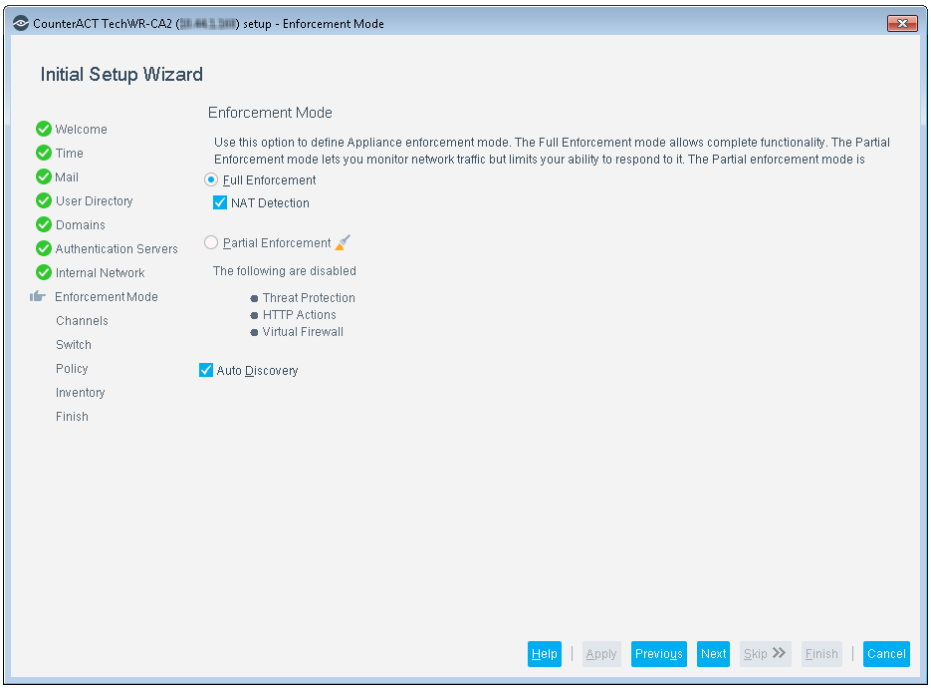


Internal Network Page

Enforcement Mode

Use this option to define Appliance enforcement mode. The Full Enforcement mode allows complete functionality. 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 in Partial Enforcement mode. This mode is recommended for evaluation purposes only.

Select the NAT detection checkboxes to detect NAT devices.



Enforcement Mode Page

The **Partial Enforcement Mode** icon is displayed on the status bar if your system is set to this mode.

By selecting **Auto Discovery**, you allow CounterACT to resolve and display endpoint properties; for example, NetBIOS names Nmap and domain information. See Defining Endpoint Discovery Rules for more information.

Channels

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) and the other interface generates traffic back into the network (response interface). Response traffic is used to:

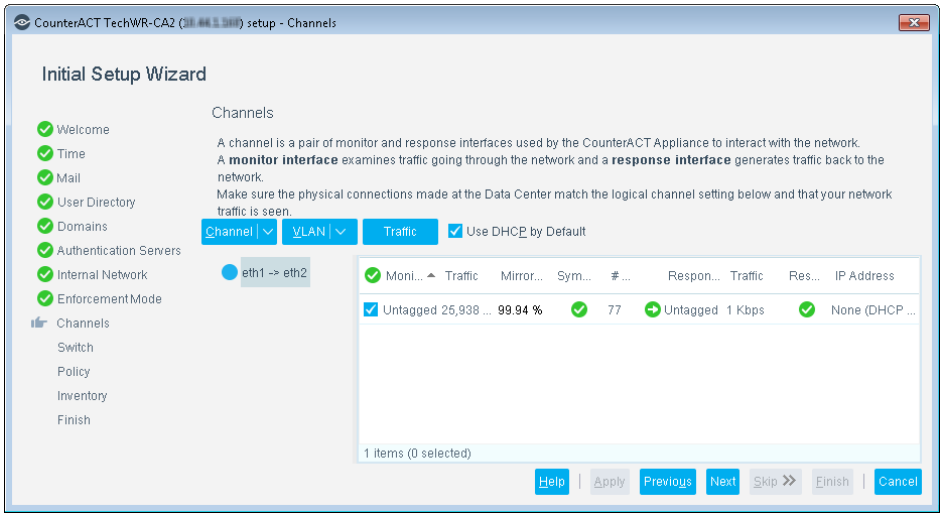
- Protect against self-propagating malware, worms and hackers.
- Carry out Virtual Firewall blocking.
- Perform policy *actions*. These actions may include, for example, redirecting web browsers or carrying out Virtual Firewall blocking.

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

You should have defined monitoring and response interfaces and made the appropriate physical connections in the Data Center when installing the Appliance and connecting it to the network switch.

Use the Channels page to complete interface assignments made in the Data Center

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



Channels Page

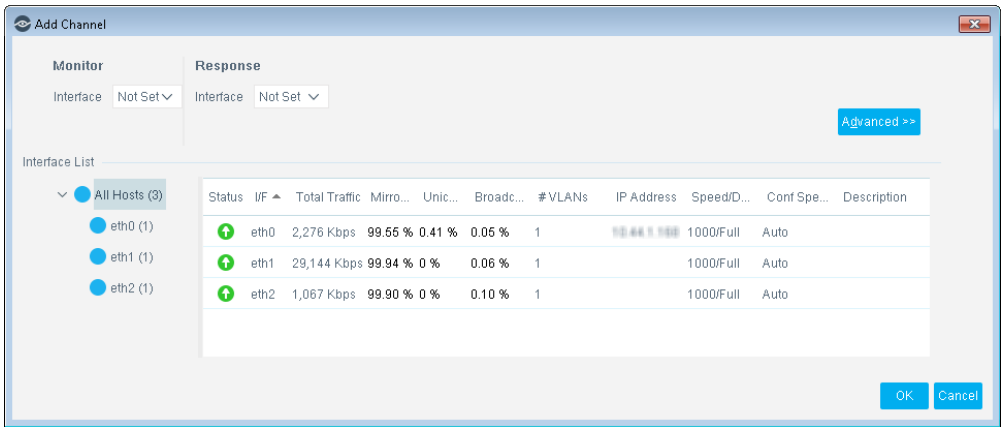
If your network architecture is set up to work with VLANs, the Appliance will automatically detect them. These VLANs are displayed in the Channels page.

Add Channels

You must define channel definitions to match Appliance interface connections in order to detect and respond to traffic on network interfaces.

To add channels:

1. Select the **Channel** drop-down list and then select **Add**. The Add Channel dialog box opens.



Add Channel Dialog Box, Basic Setup

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.

Review the interfaces and related information to verify that traffic is being seen 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 readjust the physical interface connections.

The information in the following table is displayed.

VLAN ID	The VLAN name or number.
Total Traffic	Total VLAN traffic monitored by the interface.
Broadcast	The percentage of broadcast traffic detected on the VLAN.
Mirrored	The percentage of total traffic that is not broadcast and not directed at the Appliance. This information allows you to 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 will show with a high percentage of broadcast traffic.
Unicast	The percentage of traffic sent to and from the Ethernet address on the interface.

Troubleshooting information will appear at the bottom of the dialog box if traffic detection is exceptionally low or high.

2. Select the **Monitor** drop-down list and assign the interface connected in the Data Center.
3. Select the **Response** drop-down list and assign the interface connected in the Data Center.
4. Select **OK**. The Channels pane displays the channel setup that you defined. (Alternatively, you can select **Advanced** to modify VLAN tagging definitions. See Customizing VLAN Tagging Definitions for more information.)

The dialog box contains the following additional information:

Enabled	Activates the channel configuration. 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, the 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 is 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, CounterACT cannot respond to ARP requests. In this case, manually define the address. Addresses are defined per VLAN, if required. See Manually Adding a VLAN for more information.

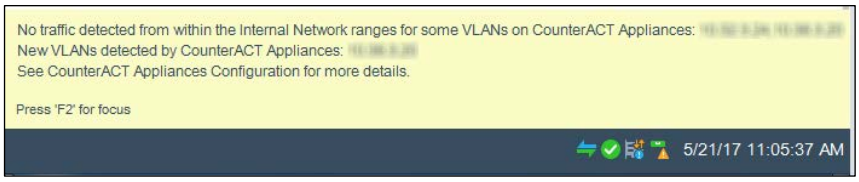
5. Select **Use DHCP by Default** if a DHCP address is used by CounterACT for monitored traffic. Clear **Use DHCP by Default** to manually configure the IP address.
6. Select the **Enabled** checkbox for each VLAN that you want to activate.
7. Select **Apply**. Symmetric and Response tests are performed. If the tests fail, you can review related troubleshooting information at the bottom of the dialog box.

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.

A tooltip provides details about the event that occurred.

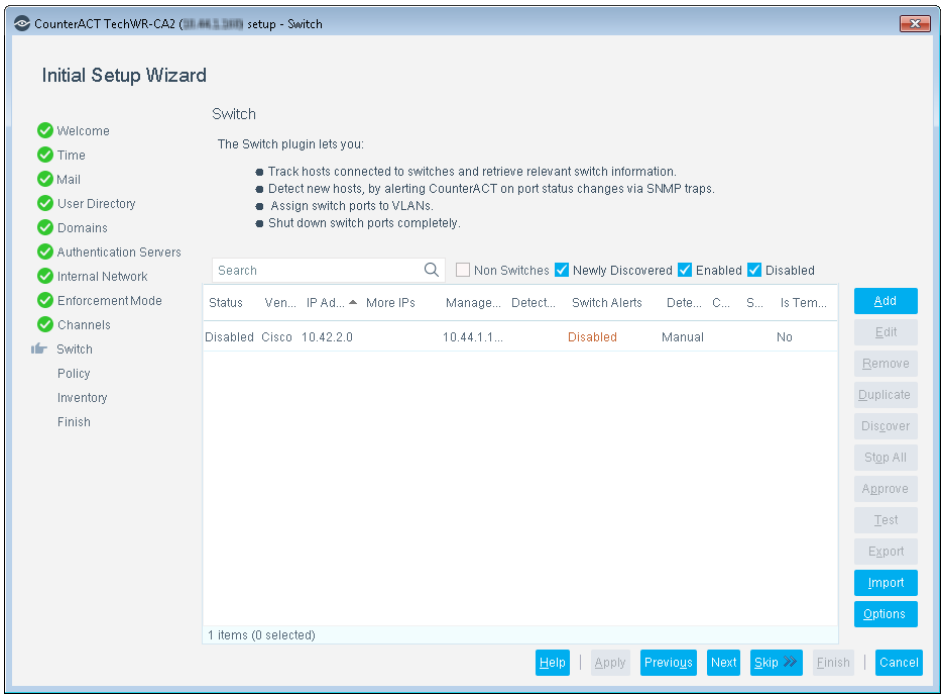


Indicator and Tooltip

Switch

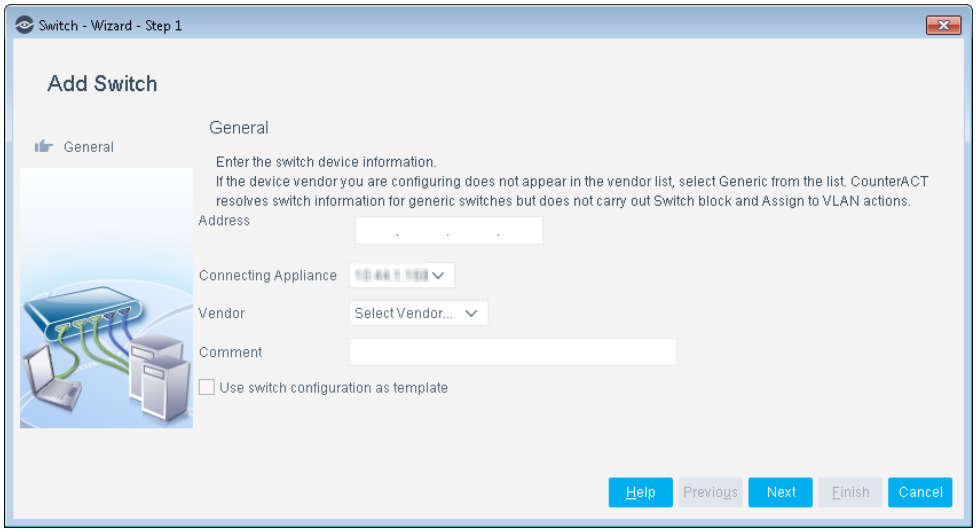
For switches that are managed by the Switch Plugin, CounterACT switch tools let you:

- 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 CounterACT on 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.



Switch Page

From the Switch page of the wizard, configure a switch that exists in your network by selecting **Add** and stepping through the Add Switch wizard.



Add Switch, General

Select **Help** to open the *Switch Plugin Configuration Guide* if you need help configuring the switch.

You can configure the switch that you are configuring here to add other switches in your network to CounterACT 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.

Note that 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.

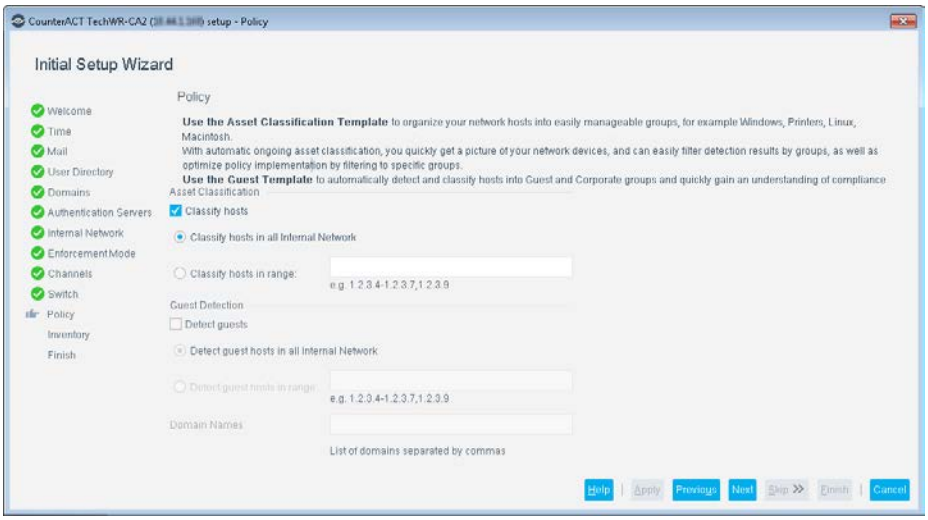
- Use the switch configuration as a template for other switches: When an unmanaged switch (that is, a switch that is not managed by the CounterACT Switch Plugin) sends an SNMP trap and the community string of the unmanaged switch matches the community string of this switch, then all the settings of this switch (except its IP address) are applied to the unmanaged switch. Switches detected in this manner are automatically added to CounterACT.

You can also add additional switches here. After configuring switches here, select **Switch** in the CounterACT Options window to edit switch configurations and use additional Switch Plugin features.

Refer to the Switch Plugin Configuration Guide *for information about additional switch configuration features. To open this file, select* ***Options*** *from the* ***Tools*** *menu, select* ***Switch*** *and then select* ***Help****.*

Policy

You can use this option to classify endpoints into easily manageable groups of network assets and corporate/guest users. Network asset classification is carried out by a CounterACT Primary Classification Policy or an Asset Classification Policy. Corporate/guest user classification is carried out by a Corporate/Guest Control Policy. These policies are created using core CounterACT policy templates.



Policy Page

Asset Classification Policy

The Asset Classification policy template creates CounterACT groups according to the following device categories:

- NAT devices: Devices that may hide other devices
- Mobile devices
- Windows
- Printers
- Linux/Unix
- Macintosh
- VoIP devices
- Network devices: For example, routers and switches
- Unclassified: If CounterACT does not know to which category an endpoint is associated.

To take advantage of more precise classification profiles, it is recommended to create and run Primary Classification policies instead of Asset Classification policies.

To create the groups:

1. Select the **Classify hosts** checkbox.
2. Insert the range of IP addresses to be classified.

Primary Classification Policy

For an encompassing classification of devices connected to the network, it is recommended to create and run a policy based on the *Primary Classification* policy template after the Appliance has been set up.

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 the set of properties which includes the hostname of the device revealed by DHCP traffic, the HTTP banner, the NIC vendor and Nmap scan results. A *Primary Classification* policy can create the same groups as an *Asset Classification* Policy. See Asset Classification and Primary Classification Templates for details.

Corporate/Guest Control Policy

The Corporate/Guest Control policy template lets you detect:

- endpoints known to be part of the corporate network
- endpoints that may be *guests*, i.e. not part of the corporate network

The policy organizes endpoints into *Corporate Hosts*, *Signed-in Guests* and *Guest Hosts* groups. If CounterACT cannot evaluate the status of an endpoint, that endpoint is classified as a guest host.

Corporate Hosts are endpoints that either:

- Are currently signed in as a Domain User
- Have authenticated recently to an approved authentication server

To create the groups:

1. Select the **Detect guests** checkbox.
2. Insert the range of IP addresses to be categorized.

Asset Inventory

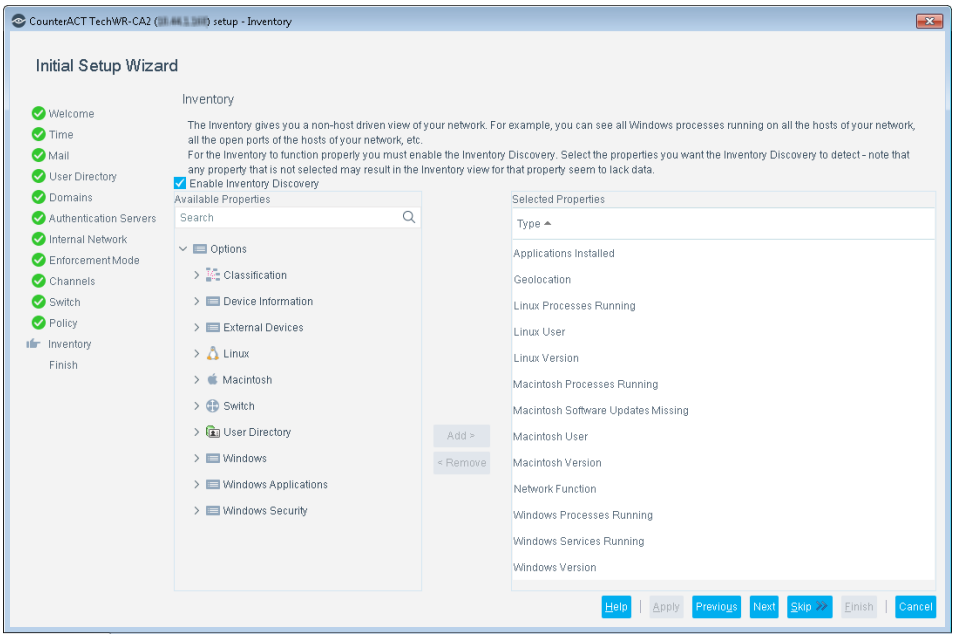
The Asset Inventory presents a live display of network activity in the Console; for example, processes and services currently running, vulnerabilities currently detected, ports currently open or users currently logged in.

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.

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

Use the wizard to select items that will appear in the Asset Inventory.



Inventory Page

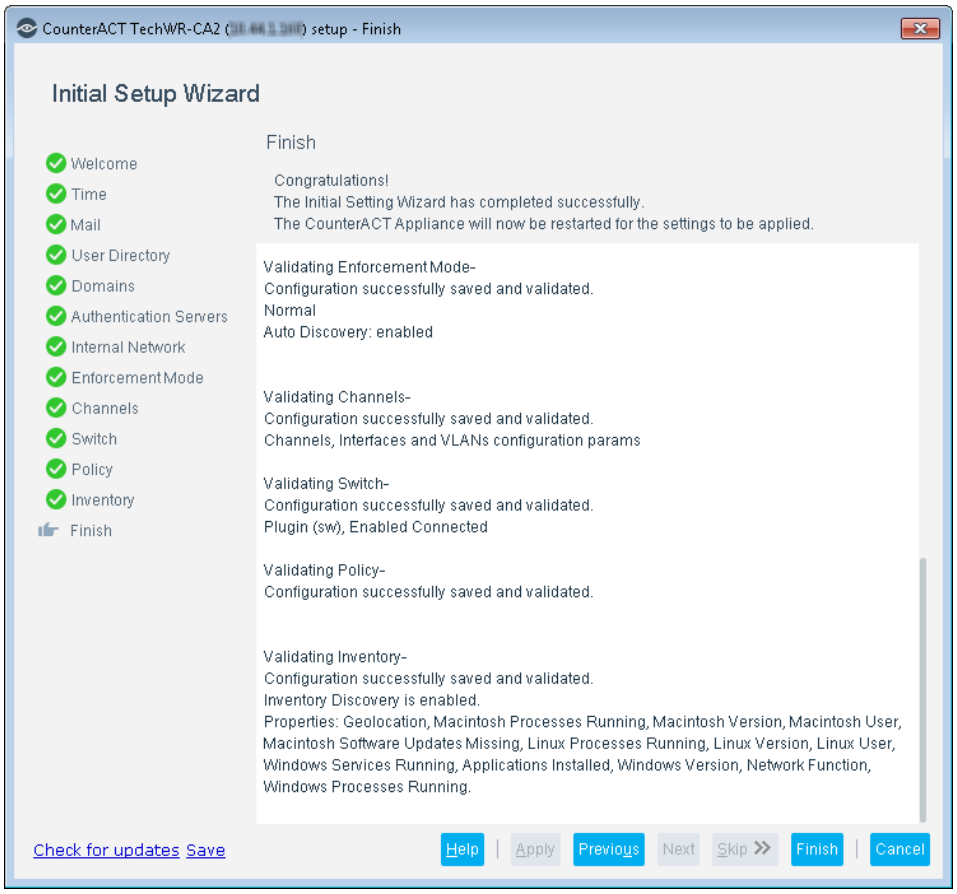
The following network activities are selected by default:

- Users
- OS Class types running
- Switches integrated with CounterACT
- Windows Applications installed
- Processes and services running
- Windows machines
- Operating system versions running
- Linux machines
- Logged-in users
- Operating systems running
- Processes running
- Macintosh machines
- Users logged-in
- Operating systems running
- Processes running
- Updates missing

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 however by updating the Inventory rules. See [How the Asset Inventory Is Learned for details.

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. It is not generated from this pane.*

Finish



Finish Page

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

Select **Save** to save the configuration to an external file.

Use the Check for Updates feature to automatically update your system with the most current version of all currently installed CounterACT plugins. See [Chapter 8: Base, Content and Extended Modules] for more information about working with Check for Updates.

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

Set Up an Appliance with Enterprise Manager Settings

You can import the settings of an Enterprise Manager to new Appliances. This saves you the trouble of redefining configuration values, and ensures that each Appliance is configured uniformly.

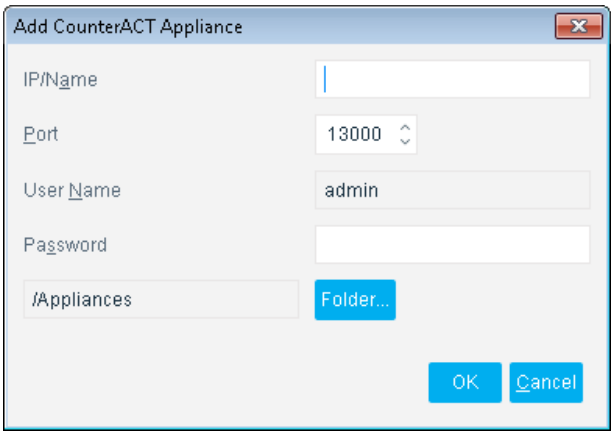
In addition to the Enterprise Manager wizard settings, plugin versions are synchronized and the following Enterprise Manager definitions are imported:

- 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. This means that when Enterprise Manager settings are changed, the settings are applied to the Appliance as well. See Chapter 15: Managing Appliances, Enterprise Managers and Consoles for more information about CounterACT device management.

To set up an Appliance:

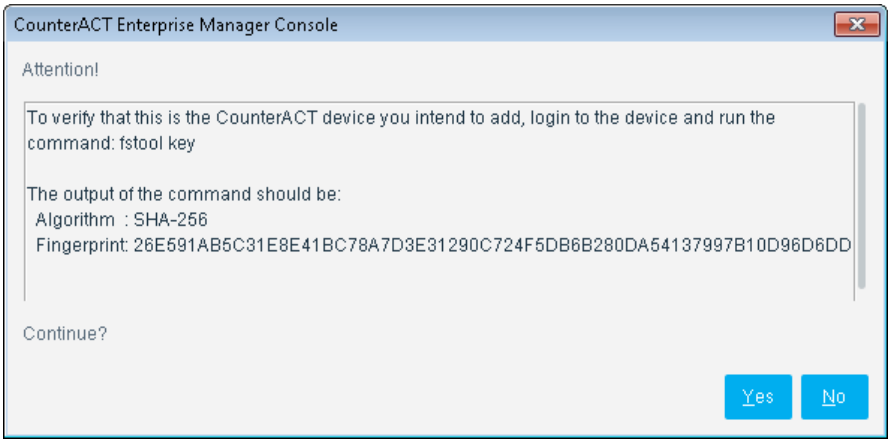
1. Log in to the Enterprise Manager via the Console.
2. Select **Options** from the **Tools** menu and then, if necessary, select **CounterACT Devices**.
3. Select **Add**.



Add Appliance Dialog Box

4. Type the IP address of the Appliance that you want to add.

5. The default port is 13000. It is recommended to not change this value.
6. Type the Admin password created during the Appliance installation in the Data Center.
7. Select **OK** until CounterACT connects to the Appliance. Messages indicate that the components are connecting and that the Appliance is being registered with the Enterprise Manager. You are prompted to verify that the CounterACT Appliance public key signature is valid.



Public Key Dialog Box

8. To verify, log in to the CounterACT Appliance CLI. Run the following command: **`fstool key`**. A message opens with the key ID.
9. You are prompted to complete the wizard with Appliance-specific definitions. These include:
   - Enforcement Mode (See the description in Set Up an Appliance from Scratch.)
   - Channels (See the description in Set Up an Appliance from Scratch.)
   - Assign IP addresses
   - Run Appliance Script

Assign IP Addresses

All endpoints in your Internal Network should be assigned to an Appliance.

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**.

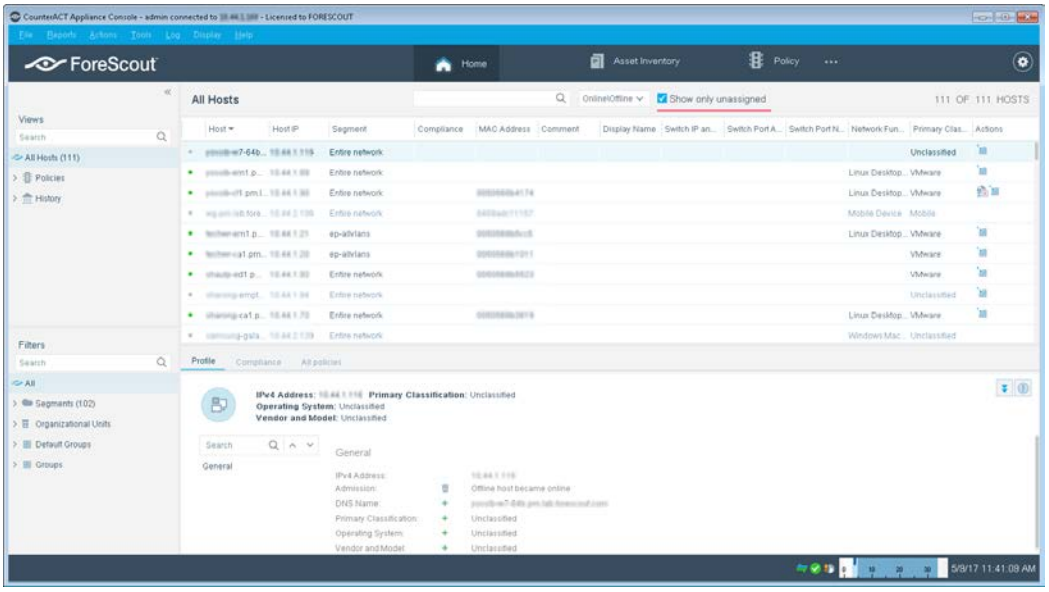
Distributing the work load among various Appliances:

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

The dialog box includes the Appliance that you are adding as well as others Appliances. Edit as required.

All endpoints in your Internal Network should be assigned to an Appliance. Assignments must be unique to each Appliance. This means IP ranges or segments cannot overlap between Appliances.

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



Show Hosts Unassigned with IP Addresses

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.

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 CounterACT Options window.

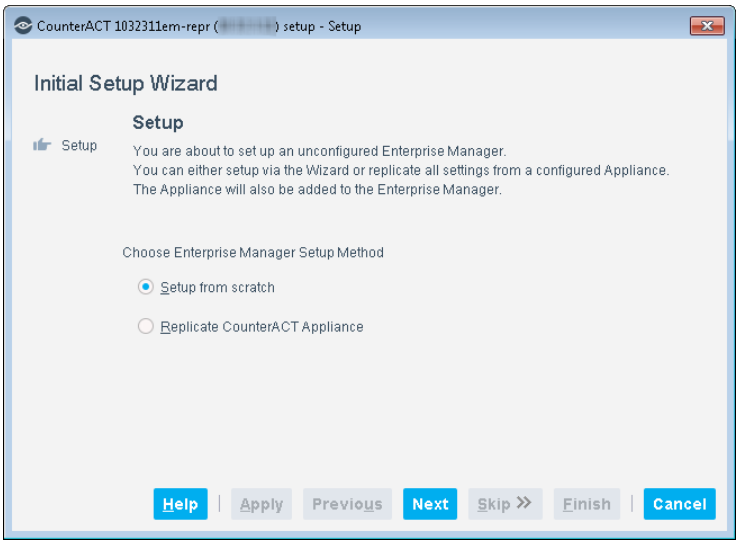
1. Select **Check for Updates** to automatically update your system with the most current versions of all installed CounterACT plugins/modules. See Check for Updates for more information.
2. Select **Save** to save the configuration to an external file.

Set Up an Enterprise Manager from Scratch

This section describes how to set up an Enterprise Manager from scratch.

To perform the Initial Setup:

1. Log in to the Enterprise Manager via the Console. The initial setup page opens.



Initial Setup Page, Enterprise Manager, Setup from Scratch

2. Select **Setup from scratch** to run the 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
   - Inventory

   See Set Up an Appliance from Scratch for more information about the items.

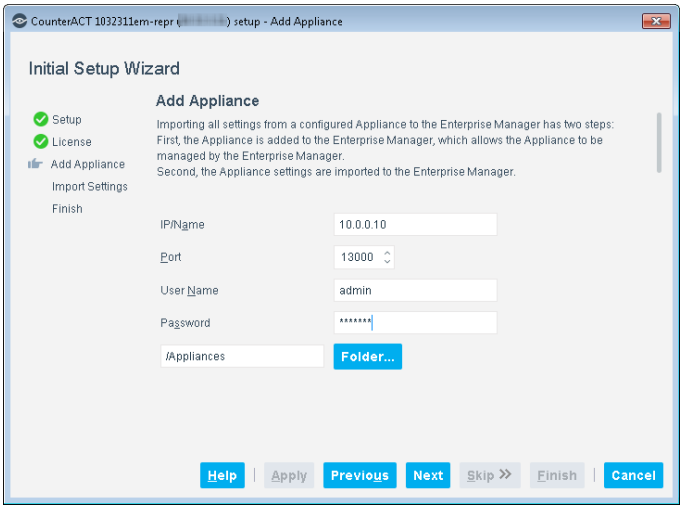
Set Up an Enterprise Manager with Appliance Settings

Use this option to replicate settings from a configured Appliance to an Enterprise Manager and register the Appliance with the Enterprise Manager. In addition, plugin versions are synchronized and the following CounterACT definitions are imported 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 CounterACT device
- Internal Network
- Legitimate Traffic rules

To replicate settings:

1. Log in to the Enterprise Manager via the Console. The initial setup page opens.
2. Select **Replicate CounterACT Appliance** and then select **Next**.



Add Appliance

3. Type the Appliance IP address.
4. The default port is 13000. It is recommended to keep this value.
5. Type the Admin password created during the Appliance installation in the Data Center.
6. Select **Next**. Messages indicate that the components are connecting and that the Appliance is being registered with the Enterprise Manager.
7. Select **Next**. You are prompted to verify that the CounterACT 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 CounterACT Options window.

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

Plugins and modules significantly broaden CounterACT's 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 Chapter 8: Base, Content and Extended Modules for more information about this and other plugins.

Select **Save** to save the configuration to an external file.

When You Are Done

After completing the Initial Setup wizard, it is recommended to perform the following:

- Review Console and Assets Portal Access Assignments
- Set Up Segments
- Set Up Segment Properties
- Set Up Ignored IPs
- Review, Run and Edit Pre-Defined Template Policies
- Set Up HTTP Redirection for Policies
- Set Up a Threat Protection Policy and Define Legitimate Traffic for Threat Protection Policies
- Review Asset Inventory Items and Create Lists
- Set Up Map Locations
- Opt In to ForeScout Research and Intelligent Analytics Program

Review Console and Assets Portal Access Assignments

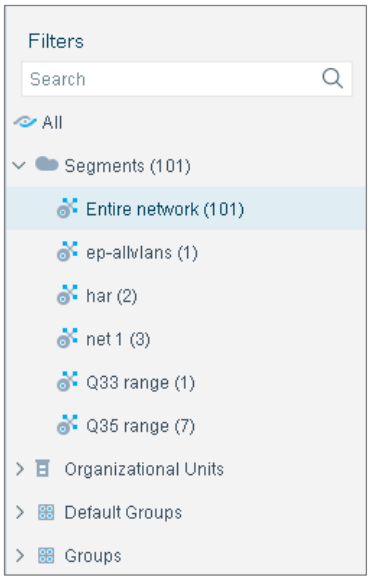
By default, Console and Assets Portal access is open to all users with IP addresses in the Internal Network. To change these defaults see:

- Defining Console Access
- Assets Portal User Management

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 CounterACT 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 that you define also appear for other features. For example, when creating an accounting segment, the defined range is available when using the VA tool (i.e. a user wants to scan accounting), or the Virtual Firewall Policy (i.e. accounting cannot use FTP).



Sub-Segments Defined

See Working with CounterACT 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 Properties for a description of each property.

Set Up Ignored IPs

You can define endpoints that should be ignored by all policy and Discovery rules; for example, a set of servers that should not be included in policy inspection. Endpoints that you add to this group are inspected by Threat Protection and Virtual Firewall policies. See Creating an Ignored IP List for more information.

Review, Run and Edit Pre-Defined Template Policies

CounterACT 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 CounterACT's major capabilities.
- Rollout 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 – instructions regarding how to handle endpoints – are generally disabled by default. You should only enable actions after testing and fine-tuning the policy. See Chapter 4: CounterACT Policy Templates for details.

Set Up HTTP Redirection for Policies

CounterACT HTTP actions let you redirect endpoint web sessions and replace them with important messages or tasks. For example, 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 Appendix 4: HTTP Redirection for more information.
- If your organization uses a proxy for web connection, you must define the proxy ports to be used. See Policy Preferences for more information.
- An option is available to redirect user Intranet sessions. See Defining HTTP Redirect Exceptions and Appendix 4: HTTP Redirection for more information.
- To disable HTTP redirection, see Disabling Web Portals.

Set Up a Threat Protection Policy and Define Legitimate Traffic for Threat Protection Policies

Your Threat Protection Policy lets you define how CounterACT handles malware, worms and other malicious endpoints that attempt to infect your network.

See Chapter 12: Threat Protection or more information.

You may also need to ignore legitimate scanning activity detected by CounterACT; for example, when you are performing vulnerability assessments, when there is traffic 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.

Review Asset Inventory Items and Create Lists

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

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*. This means you can use the inventory to discover that network guests are 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 are running the process.

See 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. Use the map to get at-a-glance, high-level status reports across sites for:

- Total number of devices per site
- Non-compliant devices per site
- Unmanaged devices per site
- Devices without policies deployed per site
- Blocked devices per site
- Malicious devices per site
- Number of online and offline devices per site
- Number of corporate and guest devices per site

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

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

Opt In to ForeScout Research and Intelligent Analytics Program

ForeScout continually attempts to provide better services to customers. Customers who voluntarily opt in to the ForeScout Research and Intelligent Analytics Program allow anonymous information from their environment to be shared with ForeScout researchers for improving the product.For information about the program, including how to view an up-to-date list of the shared properties and how the properties are anonymized, see The ForeScout Research and Intelligent Analytics Program.

Following the CounterACT installation, you are prompted to accept the ForeScout Research and Intelligent Analytics Program participation terms.

ForeScout Research and Intelligent Analytics Program Participation Terms

- If you ask to be prompted later, the prompt will be displayed the next time you log in to CounterACT.
- If you do not accept the terms, nothing will be shared with ForeScout.
- If you accept the terms, a selection of endpoint properties will be shared with ForeScout.

Chapter 3: Working in the Console

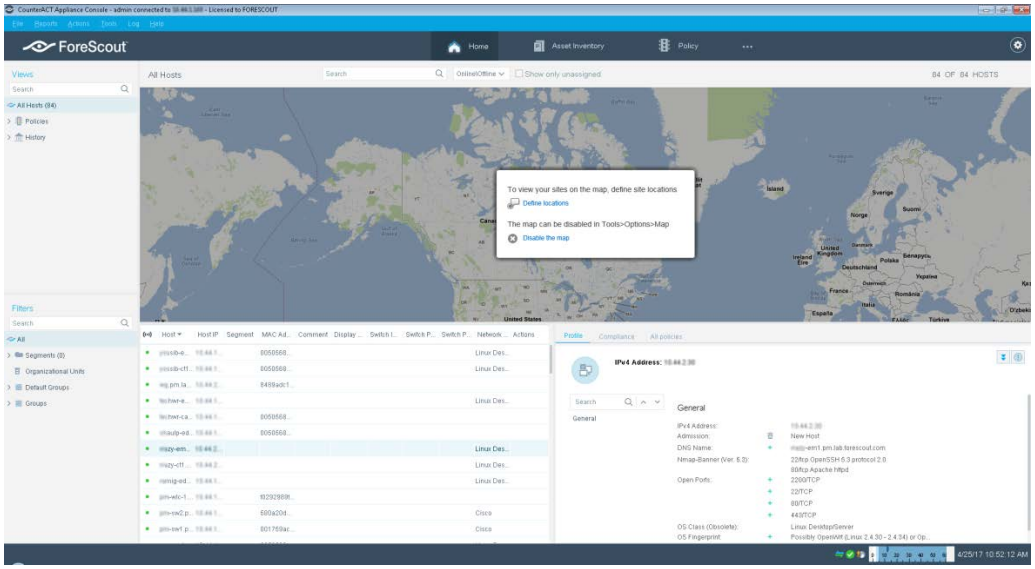
- About the Console
- Title Bar, Menu Bar, Toolbar and Status Bar
- Console Searches
- Working in the Site Map
- Working with CounterACT Detections
- Working in the Detections Pane
- Working in the Filters Pane
- Working with Asset Inventory Detections
- Working with CounterACT Segments
- Working with Organizational Units
- Working with CounterACT Groups
- Creating an Ignored IP List
- Restricting Endpoint Inspection
- Getting More Information about Endpoints
- Working with the ForeScout Compliance Center
- Exiting the Console

About the Console

The Console is the CounterACT management application used for viewing information about endpoints and devices; for example, NAC compliance status, malicious intrusions, vulnerable endpoints, real-time network inventories, and more. In addition, the Console offers an extensive range of tools used to analyze and manage these endpoints.

To access the Console, see Logging In to CounterACT.

For an explanation of the Console, see Title Bar, Menu Bar, Toolbar and Status Bar.



Console after Login

Title Bar, Menu Bar, Toolbar and Status Bar

The following sections describe the Console title bar, toolbar, icons and Console indicators:

- Title Bar
- Menu Bar
- Toolbar – Console Views
- Status Bar

Title Bar

The title bar displays the following information:

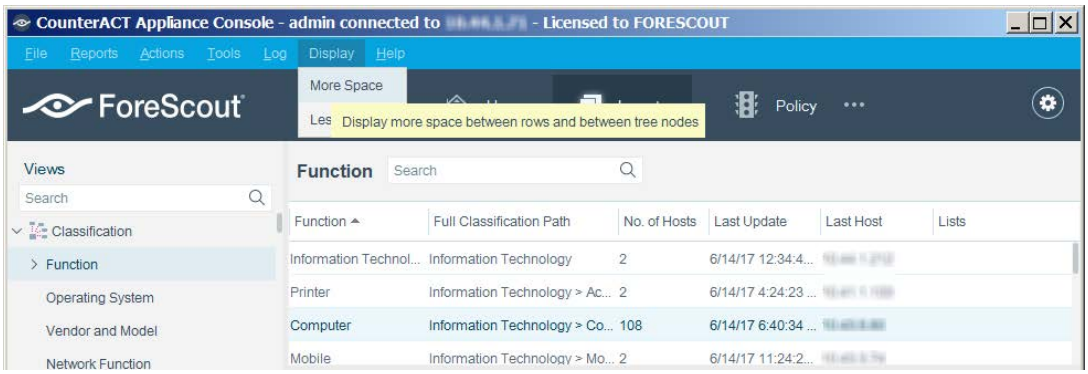
- CounterACT device IP address or host name.
- Login user name.
- CounterACT device connection status with the Console.

- 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. See Access to Network Endpoints – Scope for details.

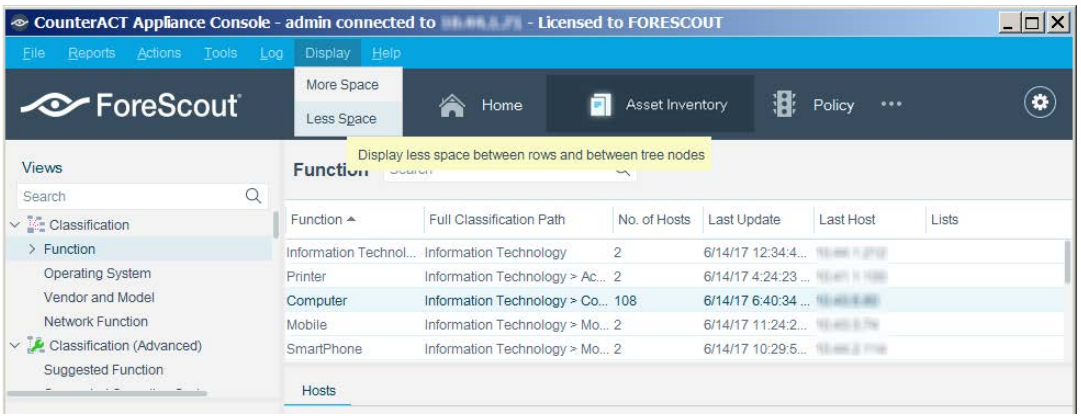
Menu Bar

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.



Display - More Space



Display - Less Space

Toolbar – Console Views

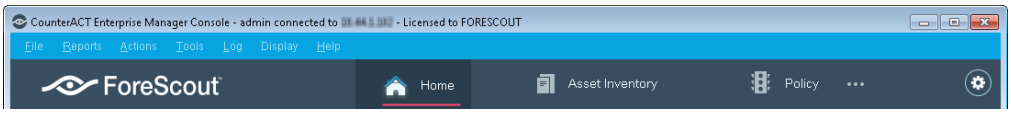
Toolbar items allow you quick access to important CounterACT information and tools. Select a toolbar tab to view the following:

- CounterACT Detections
- Asset Inventory Detections
- Threat Detections
- Policy Management
- Dashboard
- Additional Functionality

CounterACT Detections

The Home view displays:

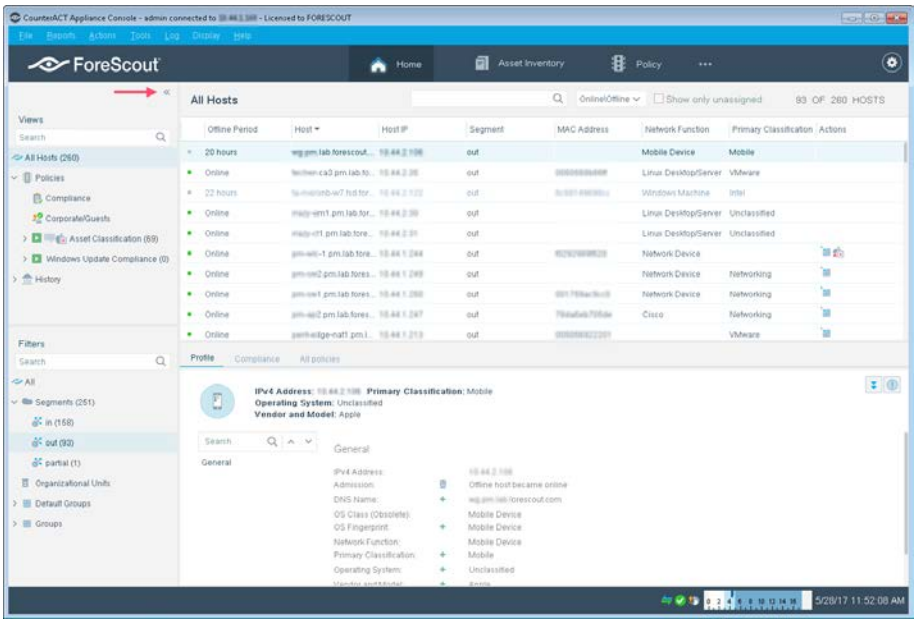
- Extensive real-time information about endpoints detected on your network; for example, endpoint details learned by CounterACT information about endpoint policy status, CounterACT actions applied to endpoints, and more. See Working with CounterACT Detections for details.
- The CounterACT site map. The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



Home View Tab

Customize the Home view

Adjust the view to meet your viewing preferences by using the toggle arrow located on the perimeter of the Console pane.



Toggle Arrow

Asset Inventory Detections

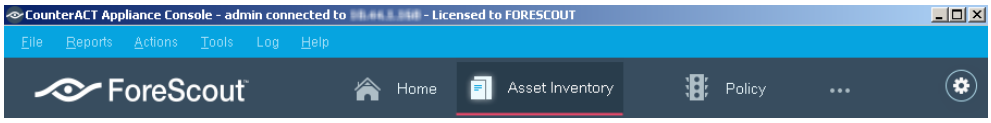
The Asset Inventory presents a live display of network activity at multiple levels; for example, processes and services currently running, vulnerabilities currently detected, ports currently open and users currently logged in.

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, create a policy that detects and halts these processes on guest machines.

See Working with Asset Inventory Detections.



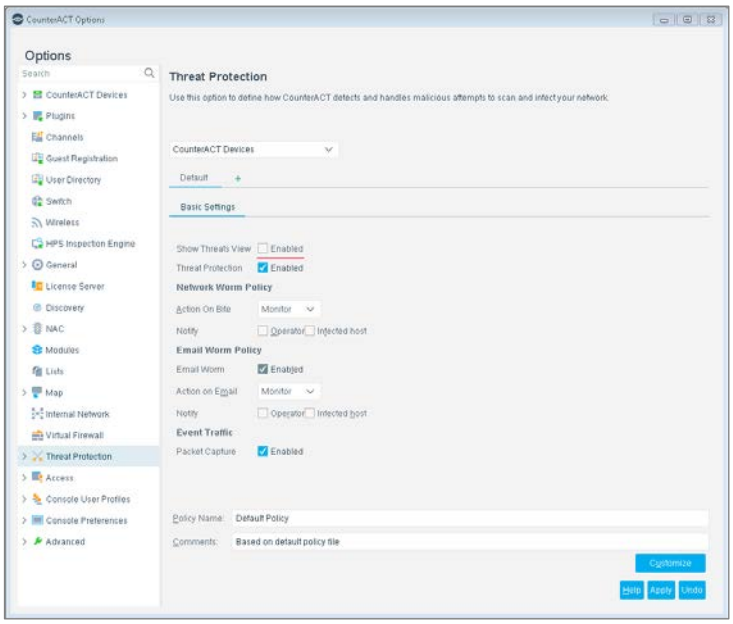
Asset Inventory View Tab

Threat Detections

The Threats view displays endpoints detected via Threat Protection policies. Create and edit Threat Protection Policies from this view. See Chapter 12: Threat Protection for more information. The Threats tab can be displayed or hidden.

To display or hide the Threats tab on the Toolbar pane:

1. Select **Options** from the **Tools** menu.
2. Select **Threat Protection** from the dropdown menu. The Threat Protection pane opens.
3. To display the tab, select the **Show Threats View** checkbox.
4. To hide the tab, clear the **Show Threats View** checkbox.
5. Select **Apply** to save the changes.



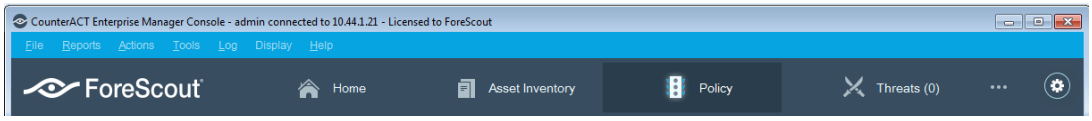
Threats View Tab

Customize the Threats View

Adjust the view to meet your viewing preferences by using the toggle arrows located on the perimeter of the Console pane.

Policy Management

Use the tools in the Policy view to create, edit and manage policies. See Chapter 5: Policy Management for details.



Policy Tab

Dashboard

Access the Dashboard – a web-based information center that delivers dynamic at-a-glance information about:

- Device compliance
- Device classification
- Device management status
- Network overview

To access the Dashboard:

1. Select the **Ellipsis icon** from the **Toolbar**, and Select **Dashboard** from the dropdown menu. The Dashboard opens in a new browser window.

Additional Functionality

You can also access the Reports Portal, the CounterACT Dashboard, Assets Portal from the toolbar.

Toolbar Ellipsis Icon	Access additional options from the ellipsis: ▪ Dashboard, a web-based information center that delivers dynamic at-a-glance information about network compliance, threats and guests. See Chapter 16: The Dashboard for more information. ▪ Assets Portal, a web-based search and discovery tool that allows you to leverage extensive network information regarding network assets. See Chapter 9: Assets Portal for more information. ▪ 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 CounterACT User Portal Builder for more information.
Options Icon	Use the Options window to define a wide range of system parameters and update parameters configured during the Appliance installation and initial setup.

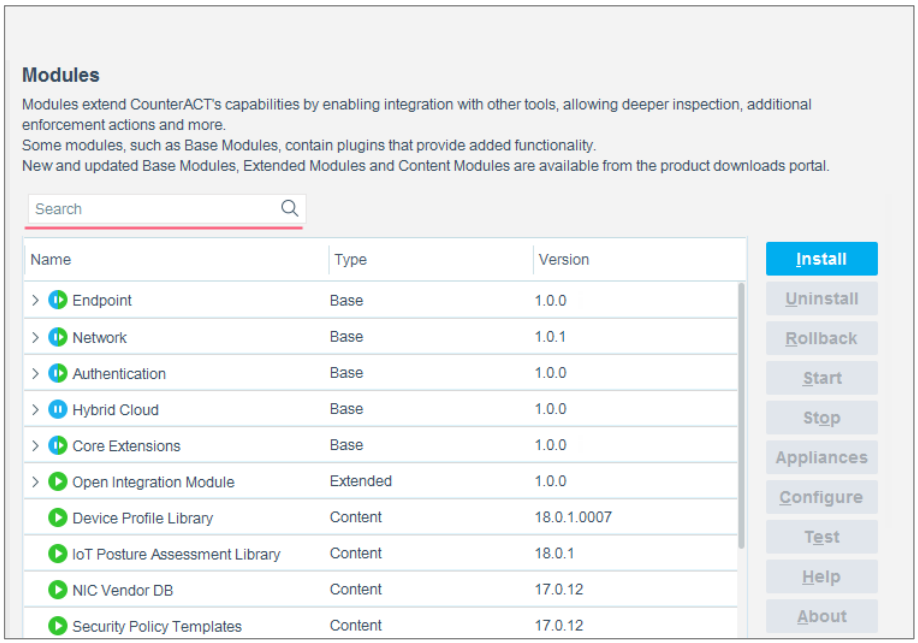
Status Bar

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. CounterACT 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 CounterACT detects a service attack at your network. The indicator blinks until the service attack is viewed in the Current Service Attack dialog box. See Handling Service Attacks for more information.
Connection Status Indicator	Indicates the connection status between Appliances and the Enterprise Manager. If an Appliance is disconnected the red checkmark is displayed.
Enforcement Mode	If you have 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 will be disabled. This mode is recommended for evaluation purposes only. See Working with the Enforcement Mode for more information about this mode. If the indicator reads High Activity Mode, CounterACT is responding to an extensive amount of traffic. See High Activity Mode for more information.
Updates	This icon is displayed when new updates of installed plugins and modules are available. CounterACT detects versions installed on your CounterACT devices and notifies you when new updates are available. Select the icon to view and install newer versions. See Chapter 8: Base, Content and Extended Modules for more information.
High Availability Cluster Status	Indicates the status of a High Availability pair. Refer to the *ForeScout CounterACT Resiliency Solutions User Guide* for more information about High Availability. See Additional CounterACT Documentation for information on how to access this guide.
Date and Time Indicator 4/24/17 1:50:07 PM	Represents the current date and time according to your local time zone setting.

Console Searches

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



Search Tool – Modules Pane

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 on the pane header; for example, the Filters pane.

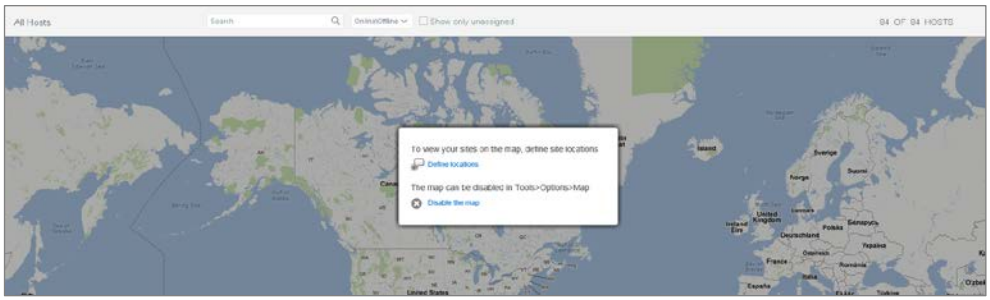
Wildcard Searches

You can use the following wildcard characters in searches throughout the CounterACT Console:

- **** (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.

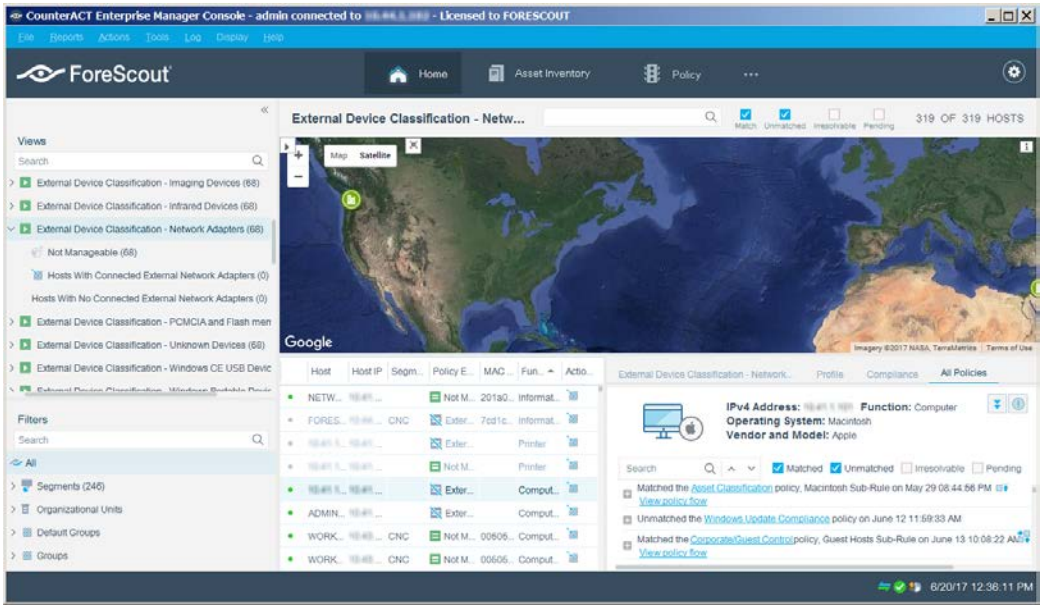
Working in the Site Map

The CounterACT 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.



Site Map

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

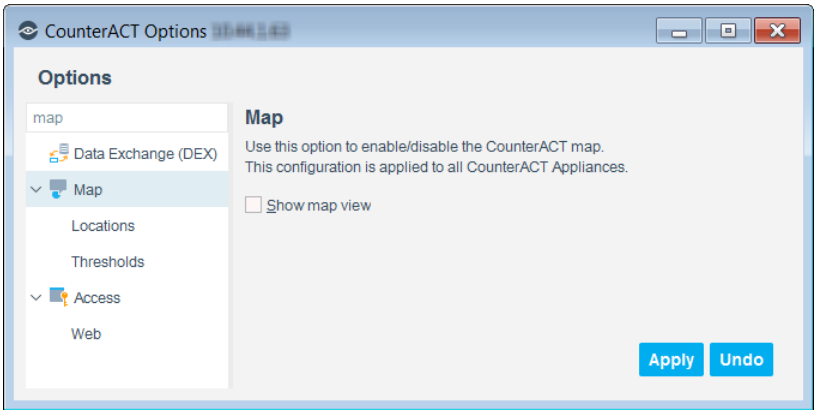
The map runs on Internet Explorer 8 and above.

Enable or Disable the Map

You can enable or disable the CounterACT site map. This configuration is applied to all CounterACT Appliances.

To enable or disable the map:

1. Select **Options** from the **Tools** menu and then select **Map**.



Map Option

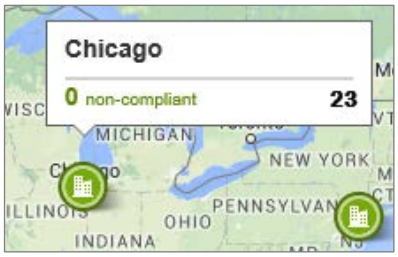
2. Select or clear **Show map view**.
3. Select **Apply**.

Set Up the Map – Create Site Locations

To work with the 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.

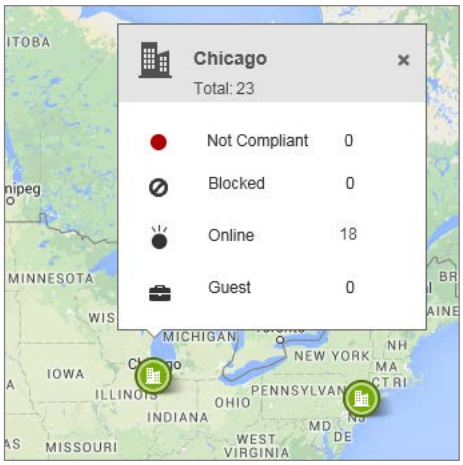
Each location is represented on the map by a location indicator .The indicator size is based on the number of detections at the site, i.e., when there are more detections the site indicator is larger.

After locations are created, the map displays information about detections at each site when you hover the mouse over a site.



Map with Site Locations

When you click on a site, the map displays detailed site information.



Map with Site Location Details

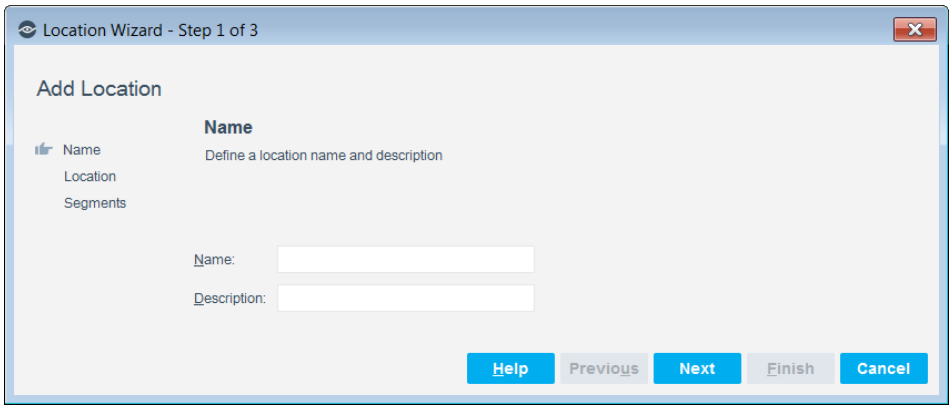
When you double-click a site, the endpoints at that site are displayed in the Detections pane below the map. A blue highlight appears around the site icon to indicate that the site is selected. You can deselect the site by clicking anywhere on the map.

Map with Selected Site Location

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

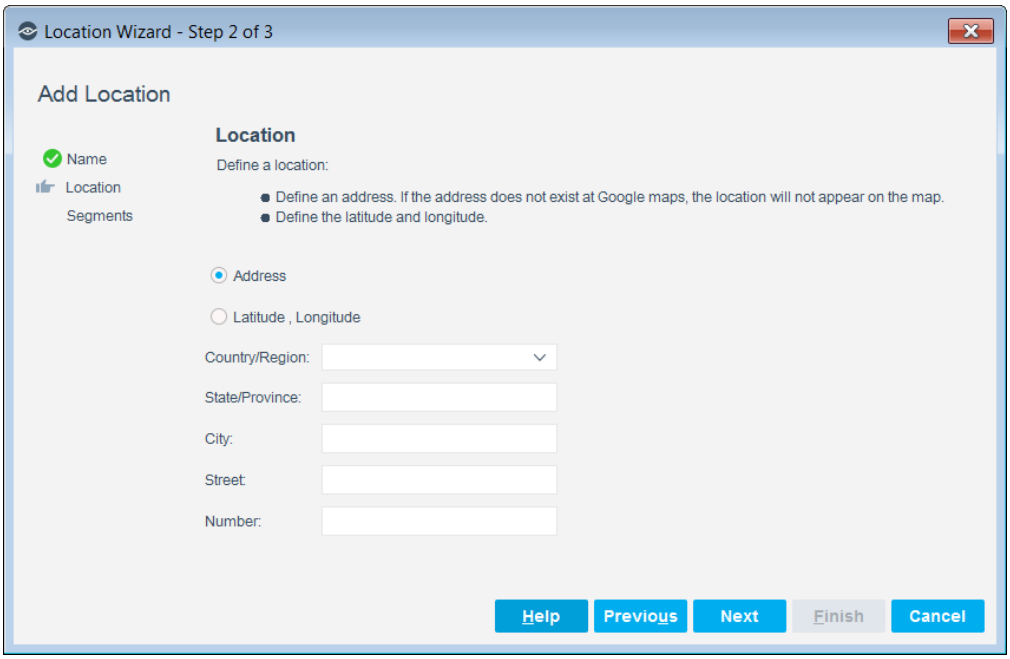
To define locations:

1. Select **Options** from the **Tools** menu.
2. Select **Map** and then select **Locations**. The Locations pane opens.
3. Select **Add**. The Add Location wizard opens.



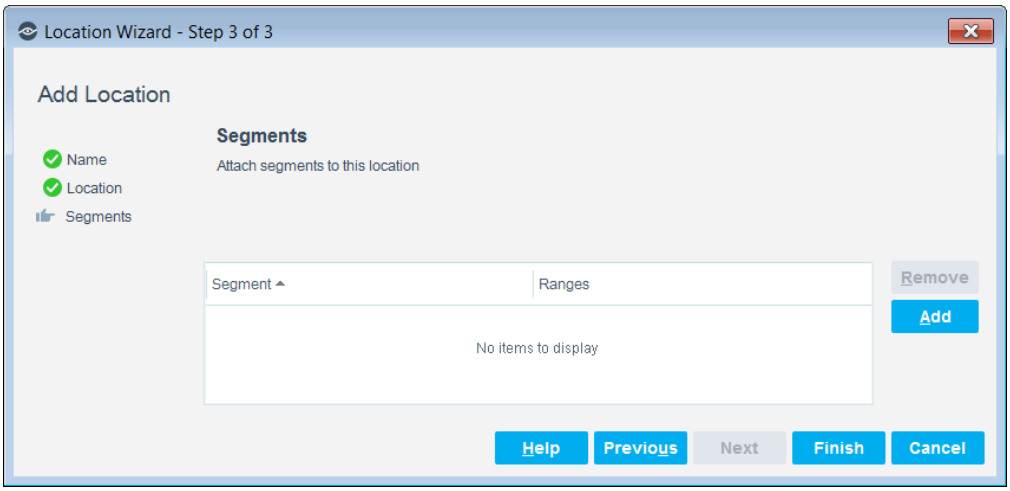
Locations Wizard – Name

4. Enter a location name and description. Select **Next.** The Location page opens.



Locations Wizard – Location

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**. The Segments page opens.



Locations Wizard – Segment

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

Customize Display Thresholds for Map Indicators

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

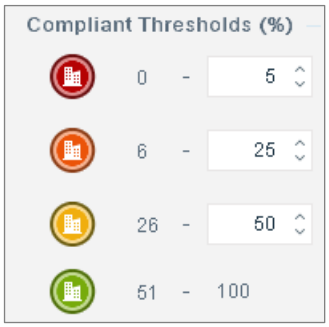
- Customize Compliant Threshold Settings
- Customize Cluster Size Settings
- Customize Cluster Grid Size Settings

Customize Compliant Threshold Settings

Customize the Compliant Thresholds (%) settings to adjust the display color of location icons according to the percentage of compliant endpoints at locations. 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 **Options** from the **Tools** menu.
2. Select **Thresholds** from the **Maps** folder. The Thresholds pane opens.



Map Icon Compliant Threshold

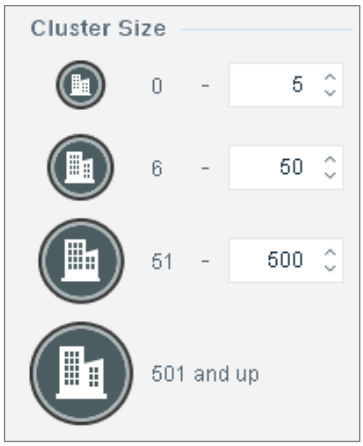
3. Use the spin controls to define the compliance display thresholds.

Customize 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 on the map for sites with 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 **Options** from the **Tools** menu.
2. Select **Thresholds** from the **Maps** folder. The Thresholds pane opens.

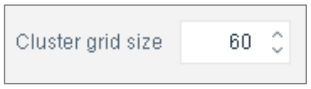


Map Icon Cluster Size

3. Use the spin controls to define the icon display sizes.

Customize Cluster Grid Size Settings

The **Cluster grid size** field determines how nearby offsite locations are clustered together at differing zoom levels. The CounterACT 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, CounterACT groups geographically close offsite endpoint locations together and displays only one offsite indicator. When you zoom in, you will see each location independently.



Cluster Grid Size

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 **Options** from the **Tools** menu.
2. Select **Thresholds** from the **Maps** folder. The Thresholds pane opens.
3. Adjust the **Cluster grid size** value.

Map Tools

Use map tools to:

- Access Map Legend
- View Grid-Based Clustering of Endpoints
- Drill Down for 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 Map Legend

You can select the Information icon on the top right of the map to display the map legend.

Map Legend Icon

Map Legend

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

View Grid-Based Clustering of Endpoints

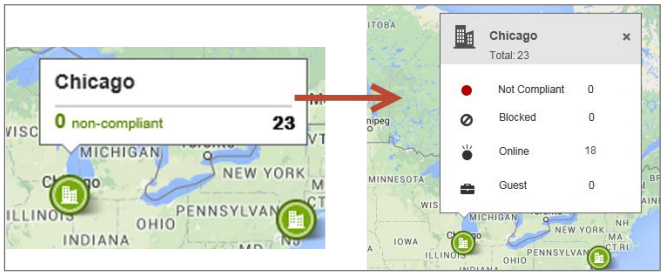
The CounterACT site map uses grid-based clustering to divide the map into squares of a certain size. When viewing the map from a higher zoom level, CounterACT groups geographically close endpoint locations together and displays only one indicator. When you zoom in, you will see each location independently.

Grid-Based Clustering

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

Drill Down for Site-Specific Statistics

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, blocked, and more.



Site Specific Information

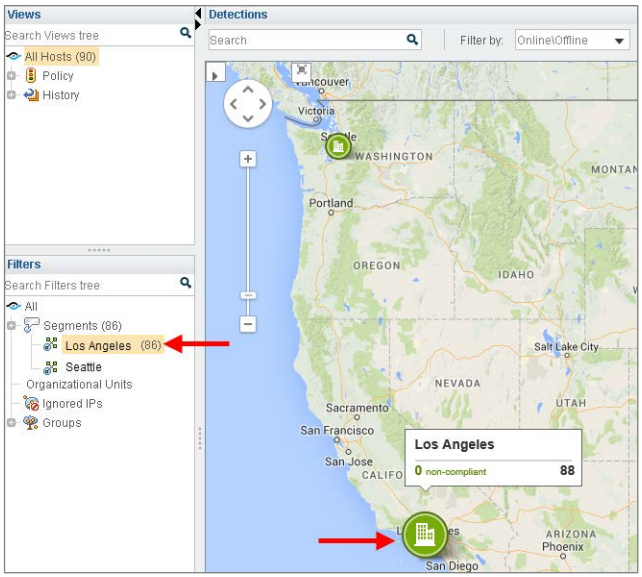
Filter Map Display

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

- Filter by Online/Offline/Unassigned Endpoints
- Group, Segment and Policy Searches
- Filter by Online/Offline/Unassigned Endpoints

Group, Segment and Policy Searches

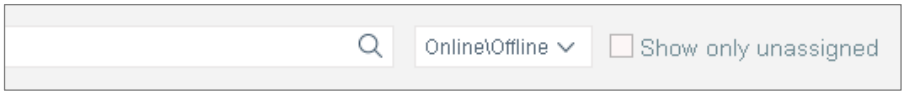
Focus the map display based on location or segments and groups that you select from the Filters pane.



Filter by Group / Segment / Policy

Filter by Online / Offline / Unassigned Endpoints

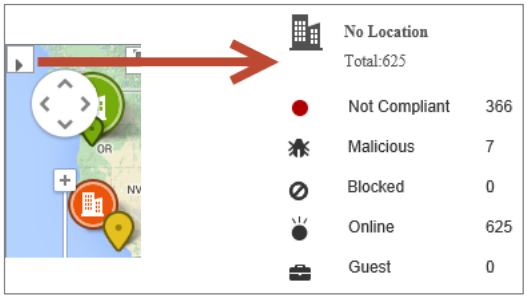
The default map filter lets you filter by online/offline or unassigned endpoints.



Filter by Online / Offline / Unassigned Endpoints

Display Information about Endpoints Not Assigned to a Location

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



No Location Form

Working with CounterACT Detections

The Console Home tab displays important details about endpoints detected by CounterACT 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, switch port to which the endpoint is connected
- Endpoint and user identity information, for example, User Directory user name, email address, department, etc.
- Information related to actions taken at the endpoint and notification sent to network users

If you have installed plugins/modules, related information will also appear; for example, if you installed the VPN Plugin, you will see VPN user information. See About Base, Content and Extended Modules for more information about plugins.

Deriving Unique Endpoints from Observed Addresses

CounterACT learns 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, additional information sources such as NetFlow are used

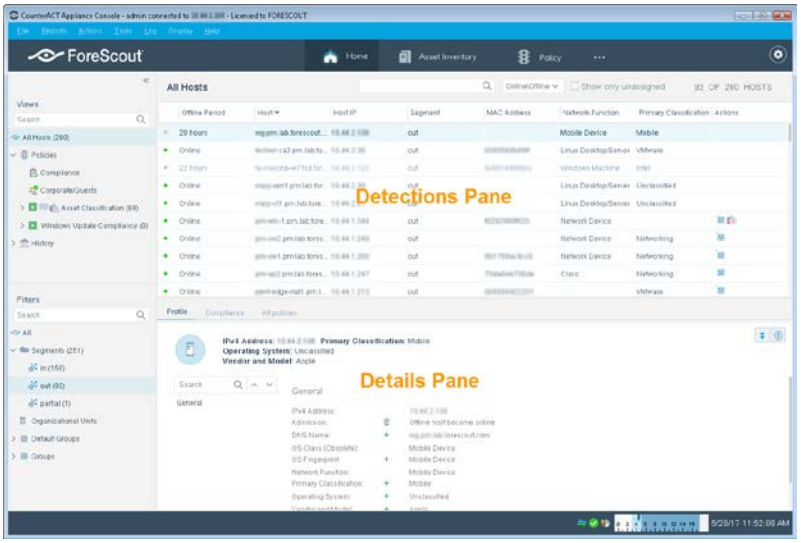
CounterACT analyzes this information to identify unique endpoints, and to correlate IP and MAC addresses to each endpoint. Note that:

- CounterACT 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, CounterACT 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 Working with Hosts without IPv4 Addresses.



Detections Pane

Two panes are available for displaying detection information from the Home tab.

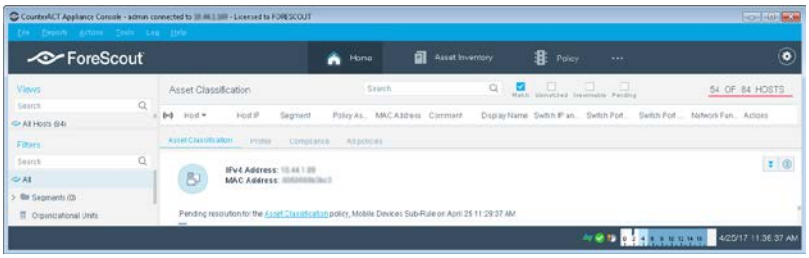
- About the Detections Pane
- About the Details Pane

About the Detections Pane

You can use an extensive range of Detections pane tools to help you find endpoints of interest and control them. For example:

- Controlling Endpoints from the Detections Pane.
- Tracking Endpoints Using the Detections Pane Filter.
- Viewing Mouse-Over Table Information.
- Filter the view in the Detections pane. See Working in the Filters Pane.
- Filter the view based on policy status; for example, only display endpoints that did not match a policy, or only display endpoints that are offline.

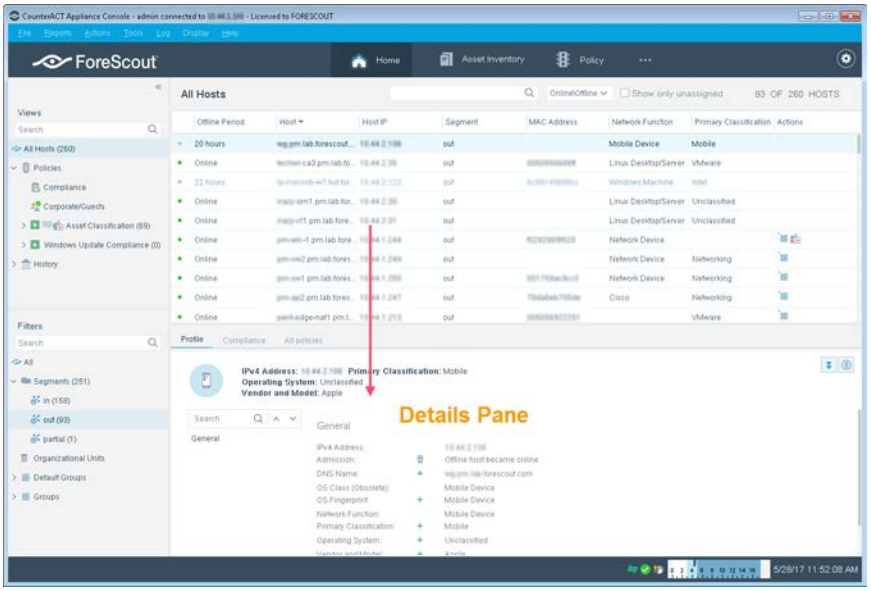
The **Hosts** indicator at the top right corner of the Detections pane displays the total number of endpoints detected for the folder or sub-folder you select. When there are a large amount of endpoints and it takes a long time to load the information to the Console, this indicator is updated to **Showing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



Showing Counter

About the Details Pane

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



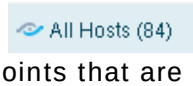
Details Pane

Home Views

The information displayed in the Detections pane varies depending of the Home view that you select. The following views may be chosen:

- All Hosts View
- Policy View
- Real-Time Policy Status Summary
- Compliance View
- Corporate/Guests View
- History View

All Hosts View

The All Hosts view 

displays all endpoints that CounterACT 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 that you created in the Policy Manager. Important detection statistics are provided. For example:

- The policy that the endpoint matched and the time that it was detected

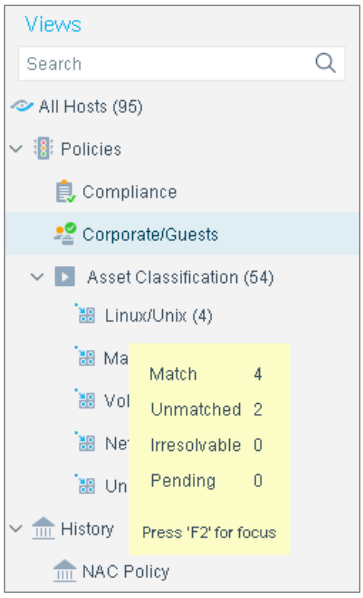
- Machine information such as the IP address, MAC address, NetBIOS name and DNS name
- Actions taken at the endpoint; for example, if the endpoint was blocked or if access was prevented to the Internet
- User Directory information
- Automated notifications sent to endpoint users
- Information about endpoints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

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.

To review a summary:

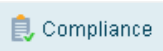
1. Mouse-over a policy folder.



Policy Summary

See Chapter 5: Policy Management for more information about working with policies.

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.

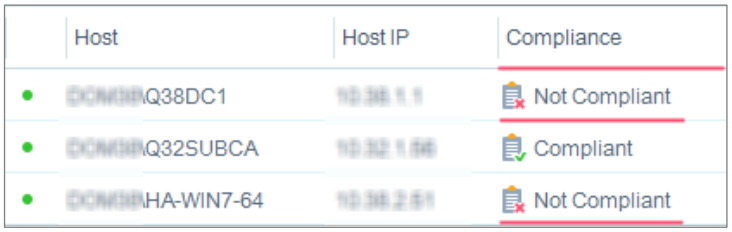
Compliance categorization can also be configured in the Policy Manager. See Working with the Policy Manager for details.

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

Compliance Summary

Select a specific endpoint and view a compliance summary for Compliance policies at which the endpoint was inspected.

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.



Compliance Entry

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. Categorization is performed in the Policy Manager. See Working with the Policy Manager for details.

These include policies generated from the Corporate/Guest Control template.

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

History View

The History view

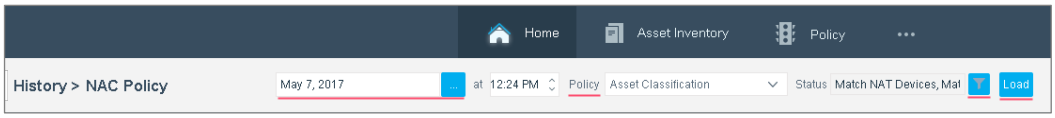
lets you display a snapshot of detection and action information from a previous period. You can view information about malicious endpoints, Service Attacks and policy detections.

You can perform the following from the History view:

- Use right-click action tools on selected endpoints.
- View details about endpoint events that you see in the Detections pane.

To open the history view:

1. Select the Home tab.
2. Select an entry under **History** in the Views pane. The policy history filters are displayed at the top of the Detections pane.



3. Select required values for the filters. The following filters are available:
   - ***Date filter:*** Select a search date
   - ***Time filter:*** Select a search time
   - ***Policy filter:*** Select a policy to view
   - ***Status filter*** **:** Select endpoints to view based on status
4. Select **Load** to load the information.

   The Detections pane is updated with new information according to the filters that you specified.

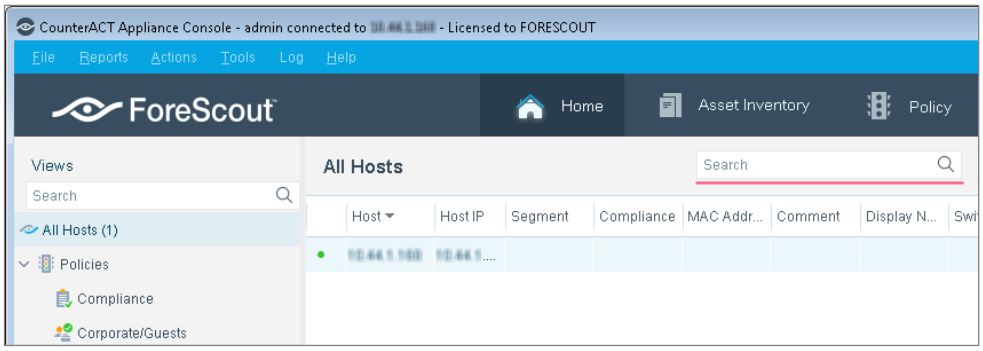
Working in the Detections Pane

You can perform a variety of tasks from the Detections pane, including:

- Tracking Endpoints Using the Detections Pane Filter
- Controlling the Detections Pane Columns
- Viewing Mouse-Over Table Information
- Controlling Endpoints from the Detections Pane

Tracking Endpoints Using the Detections Pane Filter

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



Detections Pane Filter

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 items that you are searching for.

Controlling 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 will vary, depending on the Home view that you choose. For each view, default information is displayed.

Several options are available for working with Detections pane columns, including:

- Adding, Removing and Reorganizing Columns in the Detections Pane
- Viewing the "Best Fit" for Columns
- Sorting the Pane Columns
- Exporting Detections Pane Data

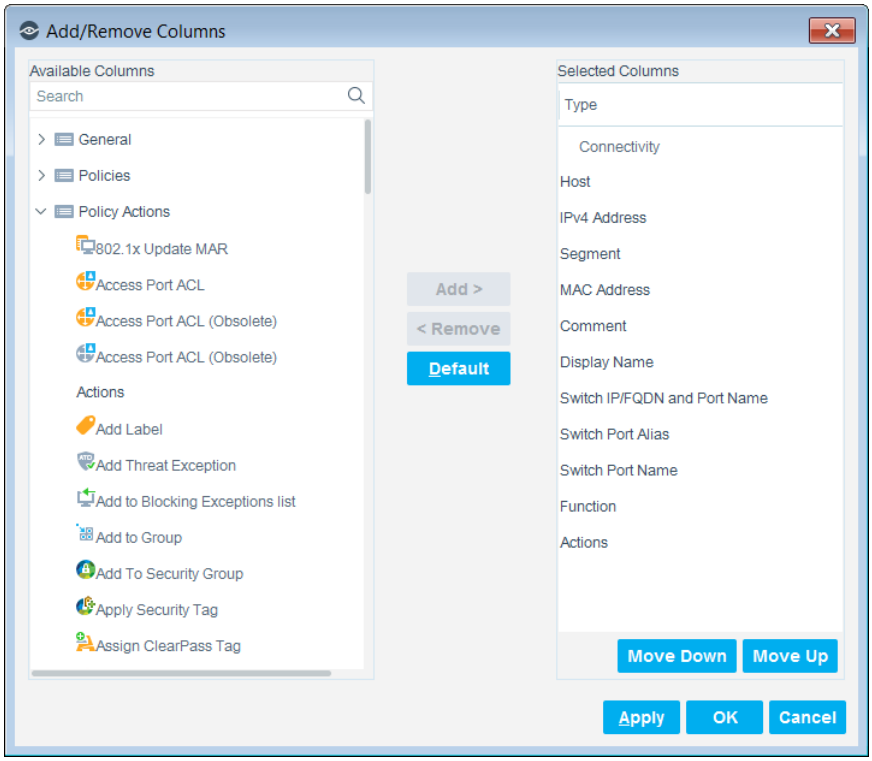
Adding, Removing and Reorganizing Columns in the Detections Pane

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 cluttered.

*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 Working with Hosts without IPv4 Addresses.*

To add, remove and reorganize columns:

1. In the Detections pane, right-click a header and then select **Add/Remove Columns**. The Add/Remove Columns dialog box opens.



Add/Remove Columns Dialog Box

2. In the Available Columns area, select the columns that you want to add and then select **Add**.

3. In the Selected Columns area, select the columns that you want to remove and then select **Remove**.
4. The topmost column in the Selected Columns area is displayed in the leftmost position in the Detections pane. To change this order, use **Move Down** and **Move Up**.
5. Select **OK**.

To remove columns directly from the Detections pane:

1. Right-click a column and select **Remove Column**.

Viewing the "Best Fit" for Columns

You can improve the readability of the Detections pane by working with the Best Fit Column option. When using this feature, a selected column is automatically adjusted to display the column text in its "best fit."

To work with the Best Fit Column option:

1. In the Detections pane, right-click a column title and select **Best Fit Column** or double-click the separator line in between columns.

Sorting the Pane Columns

Detections pane columns can be sorted in ascending or descending alphabetical, chronological or numerical order, as appropriate for each column.

To sort the columns:

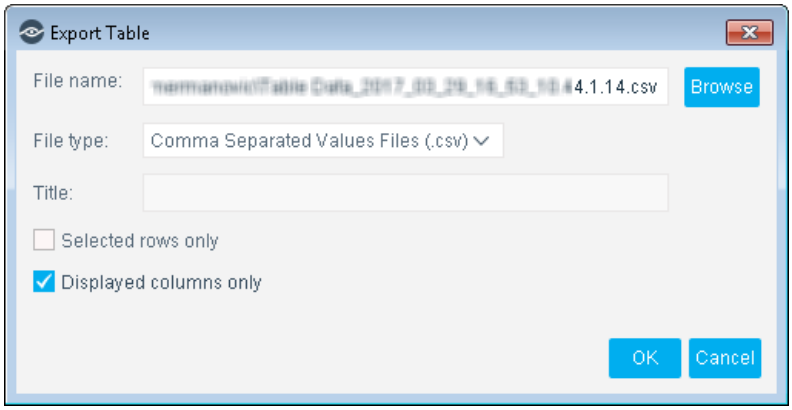
1. Click any column header. A triangle at the top of the column indicates the sorting order (pointing downwards = descending, pointing upwards = ascending).

Exporting Detections Pane Data

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

To export the Detections pane data:

1. Select **Export Current Table** from the **Reports** menu or right-click an endpoint and select **Export Table**. The Export Table dialog box opens.



Export Table Dialog Box

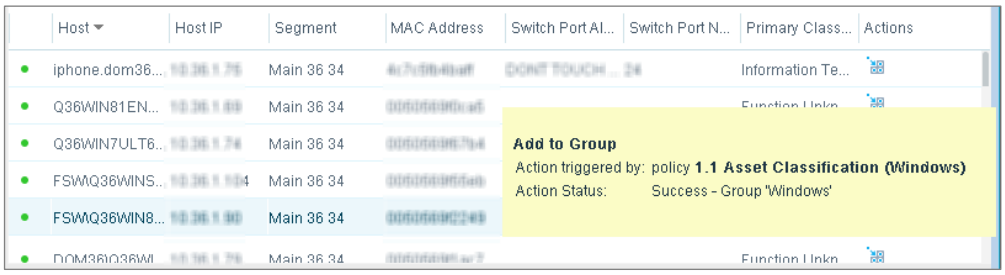
2. Browse to the location to save the file.
3. Configure an export option:

Export all information for all current detections	Clear all checkboxes.
Export displayed information for all current detections. (That is, do not export information in hidden columns.)	Select **Displayed columns only**.
Export all information but from selected rows only.	Select **Selected rows only**.
Export displayed information from selected rows only. (That is, do not export information in hidden columns.)	Select **Selected rows only** and **Displayed columns only**.

4. Select **OK**.

Viewing Mouse-Over Table Information

When you point to an item in the table with your mouse, a tooltip appears displaying information regarding that item. For example, if you drag your mouse over the **Action** field, a tooltip appears displaying 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.



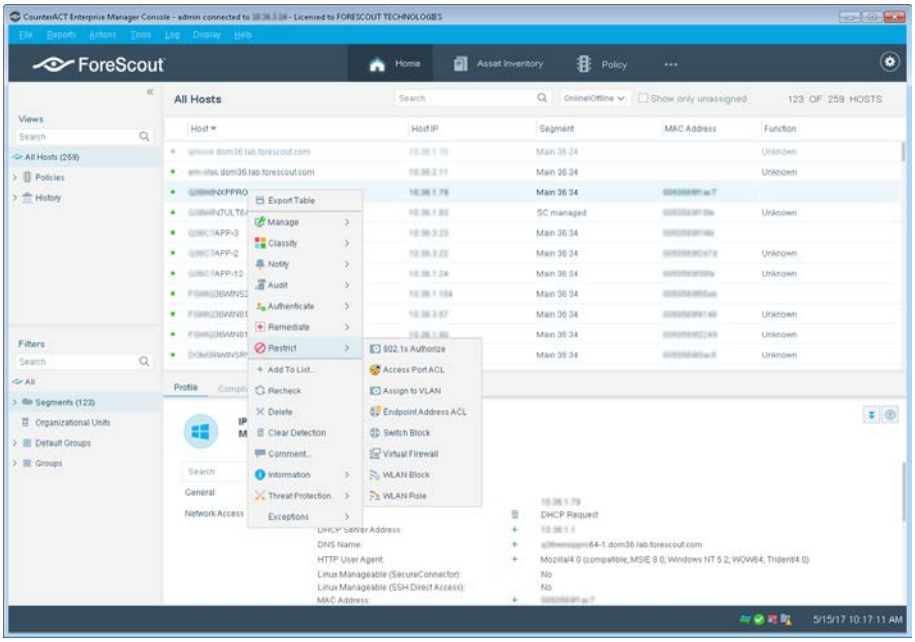
Tooltip Information (Mouse-over)

Controlling Endpoints from the Detections Pane

A variety of options are available for controlling endpoints from the Detections pane. For example:

- Start and cancel CounterACT 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

This section describes the tools available for controlling endpoints from the Detections pane.



Control Options, Detections pane

Starting Actions on Selected Endpoints

Perform manual 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 Chapter 7: Working with Actions for details about all actions.

To start an action:

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

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

Cancelling Actions on Selected Endpoints

You can manually cancel actions currently carried out on detected endpoints. The action remains cancelled 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. You can also cancel manual actions listed in the Assets Portal by selecting *Undo*, see Manual Actions.

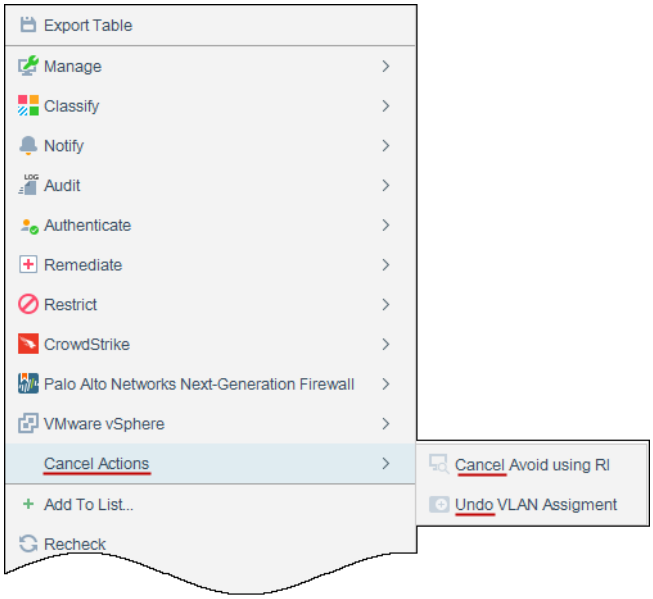
Can all action types be cancelled?

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

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 have 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 cancelled?

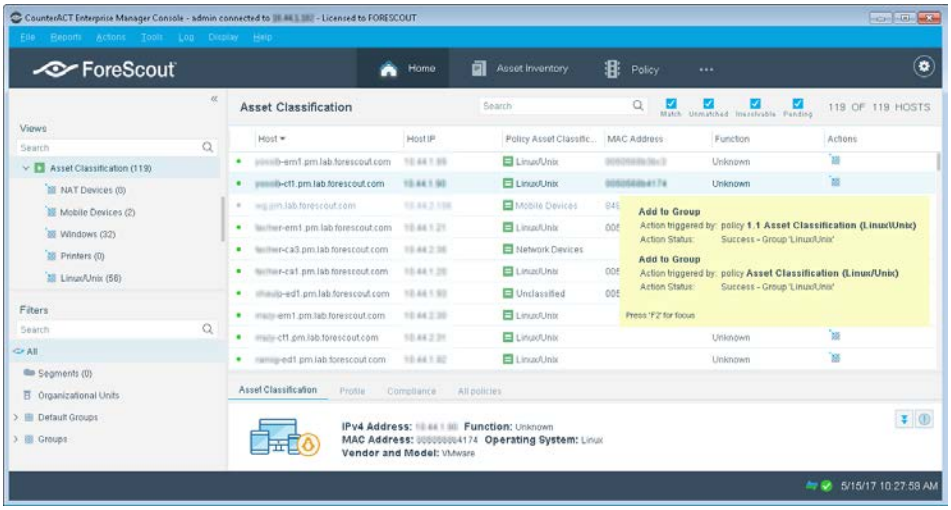
You'll know if an action can be cancelled if you right-click the endpoint in the Detections pane and the *Cancel Actions* options is displayed.



Cancel Actions

How do I know how an action was applied?

Use the Action tooltip to review information about how the action was applied or stopped.



Action Tooltip

To cancel actions:

1. Right-click an endpoint from the Detections pane that has an action that you want to cancel and then select **Cancel Actions**.

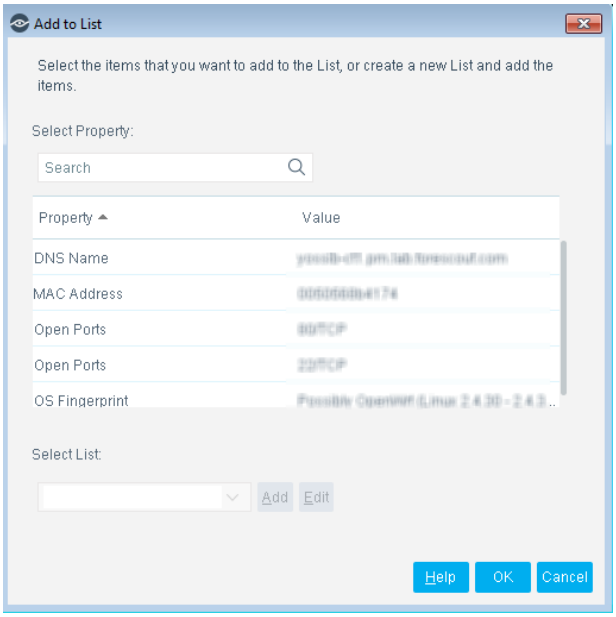
Adding Endpoint Properties to a List

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 from the Detections pane.
2. Select **Add to List**. The Add to List dialog box opens.

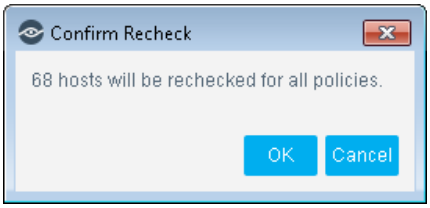
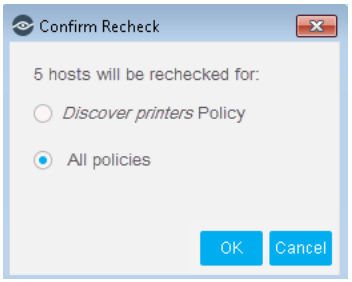


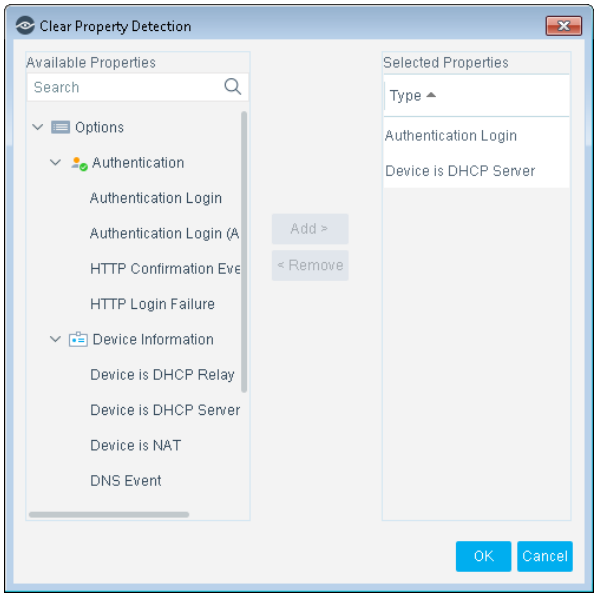
Add to List Dialog Box

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

Additional Controls

Additional controls are also available from the Detections pane.

Exception	Exclude selected endpoints from policy inspection. See Creating Policy Endpoint Exceptions for more information.
Delete	Release 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	Recheck 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.  **When a policy is not selected**  **When a policy is selected**

Clear Detection	Clear *Event* property detections; for example, admission or authentication login events. Clearing will cancel 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 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 Chapter 10: Generating Reports and Logs for more information. Events can also be cleared from the Assets Portal. See Chapter 9: Assets Portal for more information.

Comment	Make endpoint management easier with user-defined comments. Create a comment by right-clicking an endpoint or group of endpoints, and then either use the search box to look for endpoints with the comment text or create a policy that detects endpoints based on your comment. The comment is retained for the life of the endpoint in CounterACT. Use the Device Information>Comment property to create policy that detect endpoints with a comment. See Device Information Properties for details.

Malicious Host Actions

Set State / Time	Change the malicious host state and expiration time. See Changing the Host State for more information.
Add to Legitimate Email Servers	Define the endpoint as a legitimate email host. CounterACT will ignore email traffic detected at this endpoint.
Add to Legitimate Traffic	Define as a Legitimate Traffic host. Endpoints that perform legitimate scans are ignored. Specifically, they will not be counted in the scan count by CounterACT when attempting to access defined services and endpoints. See Defining Legitimate Traffic for more information.

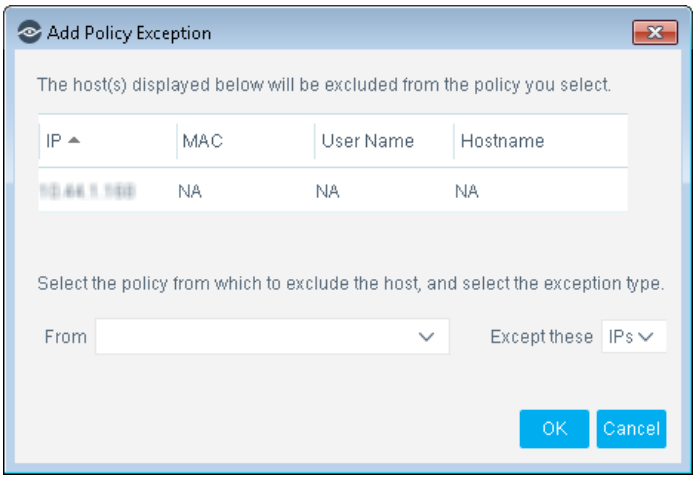
Creating Policy Endpoint Exceptions

You can select endpoints from the Detections pane and remove them from further inspection for the policy at which they were detected. The exceptions that you create here are added to the policy, Exceptions parameters.

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

To create exceptions:

1. From the Detections pane, right-click an endpoint or group of endpoints and select **Add Policy Exception**. The endpoints that you select appear in the Add Policy Exception dialog box that opens.



Add Policy Exception

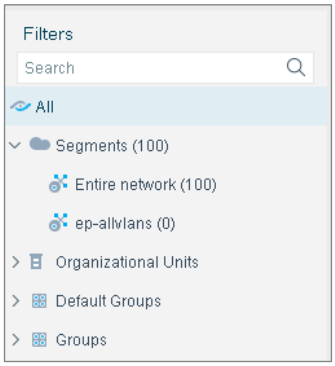
2. Select a policy or sub-rule from which to exclude the endpoint and define the exception type.
3. In the **Except these** drop-down list, select an identifier by which to detect the endpoint. Options may include the IP address, host name, and MAC address or user name of the endpoint. Select the identifier that you think is least likely to change.
4. Select **OK**.

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.

Working 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.



Filters Pane

Several filter categories can be created:

- ***Segments:*** Segments feature lets you organize your endpoints into logical categories—for example, Sales or Finance departments. Sub-segments can also be created—for example, create a Sales category and, under that, a Local Sales and International Sales category. Define segments to create a visual representation of your network that closely represents your organizational structure. See Working with CounterACT Segments for details.
- ***Organizational Units:*** An organizational unit reflects a group of CounterACT segments that have something in common; for example, the *East*, *West* and *Central Management* segments can be organized into the *Management Organizational Unit*. See Working with Organizational Units for details.
  - ***Properties - Passive Learning:*** Define endpoints that CounterACT does not actively inspect. See Restricting Endpoint Inspection for details.

– ***Groups:*** A group is a collection of endpoints with something in common, such as endpoints that run Windows systems or guest endpoints. Groups help you view and manage CounterACT detections, make it easier to define policies, and make policy implementation easier to track. See Working with CounterACT Groups for details.

Use the Filters pane search option to display segments, organizational units ignored IPs, or groups of interest to you. Items that meet the filter string appear as you type. Collapsed folders expand if the search item you entered is found in the folder. The search bar can be hidden or displayed by clicking on the Filters pane header.

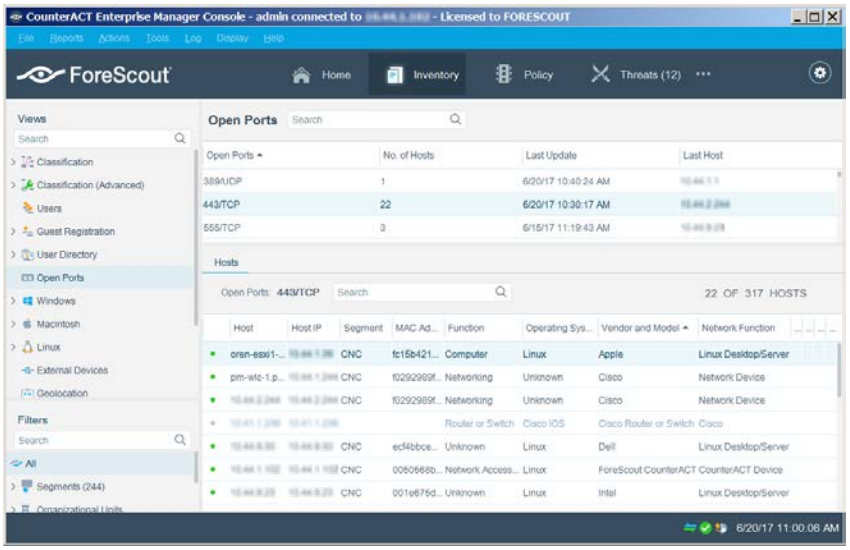
Select an item from the Filters pane and view related endpoint detection in the Detections pane. For example, view endpoint detections from Sales or Finance segment.

Working with Asset Inventory Detections

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

Use this 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.



Asset Inventory View

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

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

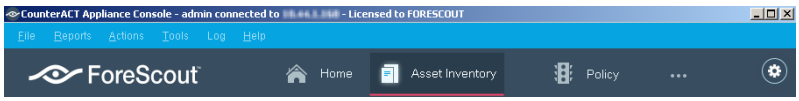
You can maximize smooth tracking of this activity by customizing the inventory categories into sub-categories. For example, you may discover via the Asset Inventory that your network is working with a variety of authorized and unauthorized processes. If this is the case, you could create lists of authorized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

To access the Asset Inventory:

1. Select the Asset Inventory tab.



Asset Inventory Tab

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 allows you to 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 from the following CounterACT tools:

- Inventory Discovery Rules
- Detection Policies

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

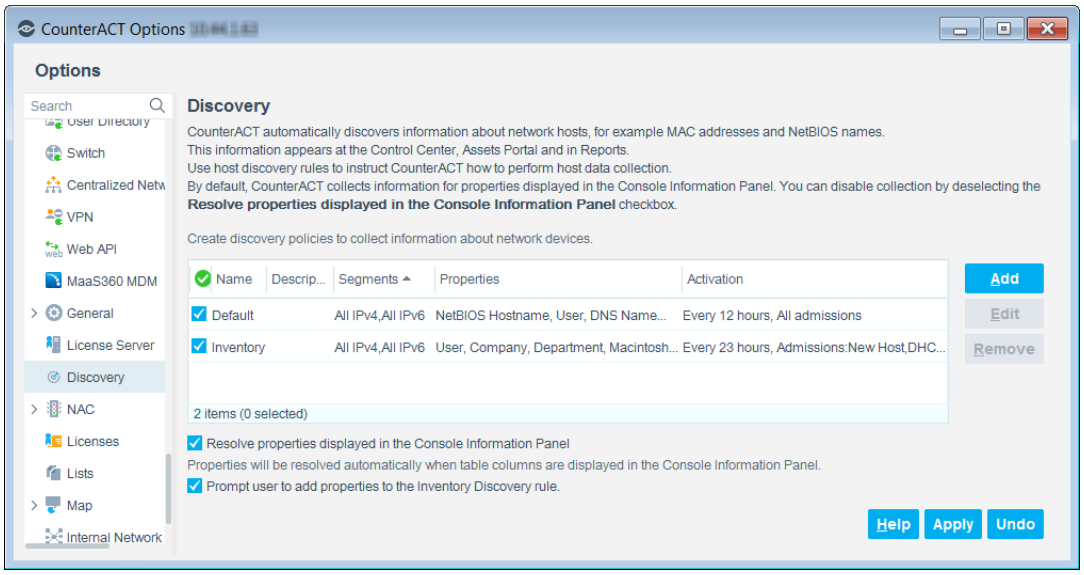
Inventory Discovery Rules

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

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

To enable Inventory Discovery:

1. Select **Options** from the **Tools** menu and then select **Discovery**.



Inventory Discovery Rules

2. Enable the rules by selecting the **Inventory** checkbox ☑.
3. Select **Apply** and **Close**.

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, described below.

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.

Viewing and Updating 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 Defining Endpoint Discovery Rules for details about working with the wizard.

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

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* property in the Inventory Discovery rule but select it in another discovery rule, installed applications are displayed in the Asset Inventory view.

Detection Policies

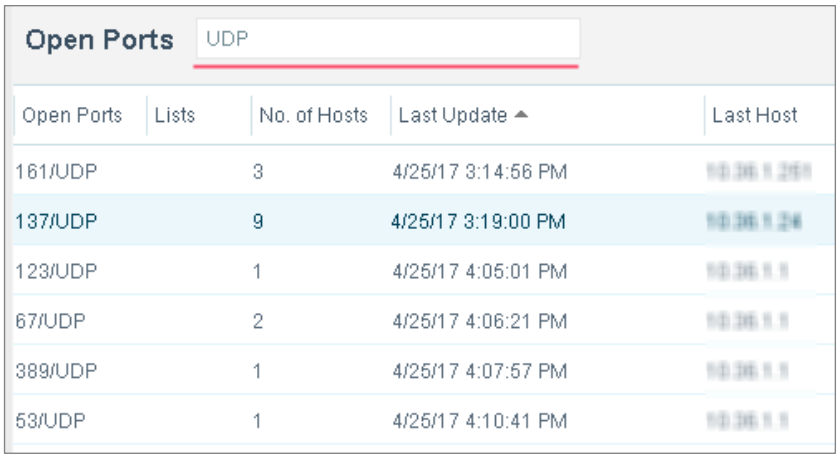
Inventory properties can also be discovered via your policies. For example, if you run a policy that detects running processes, the detected processes will appear in the Asset Inventory. Specifically, if you want to discover and display Open Ports in the Asset Inventory, you should create a policy that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

Filtering the View

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

Quick Search for Asset Inventory Data

Use the Search tool to filter the Asset Inventory display. The filtering is done 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.



Open Ports UDP

Open Ports	Lists	No. of Hosts	Last Update	Last Host
161/UDP		3	4/25/17 3:14:56 PM	[illegible]
137/UDP		9	4/25/17 3:19:00 PM	[illegible]
123/UDP		1	4/25/17 4:05:01 PM	[illegible]
67/UDP		2	4/25/17 4:06:21 PM	[illegible]
389/UDP		1	4/25/17 4:07:57 PM	[illegible]
53/UDP		1	4/25/17 4:10:41 PM	[illegible]

Text Filter – Asset Inventory

Filter per Asset Inventory List

You can customize the Asset Inventory into sub-categories. 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, filter the Asset Inventory view according to Lists of interest.

See Customizing the Asset Inventory for details.

Asset Inventory View Panes

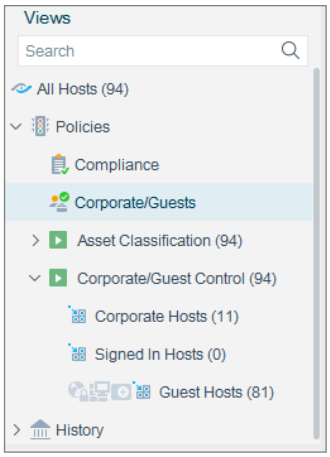
The Asset Inventory is divided into the following sections:

- 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 that are running a certain process.
- The Hosts Pane displays all endpoints that are detected with the inventory item that is currently selected. For example, the endpoint IP address, MAC address, connected switch port or User Directory name.

Inventories only show information detected at endpoints that are online.

Views Pane

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



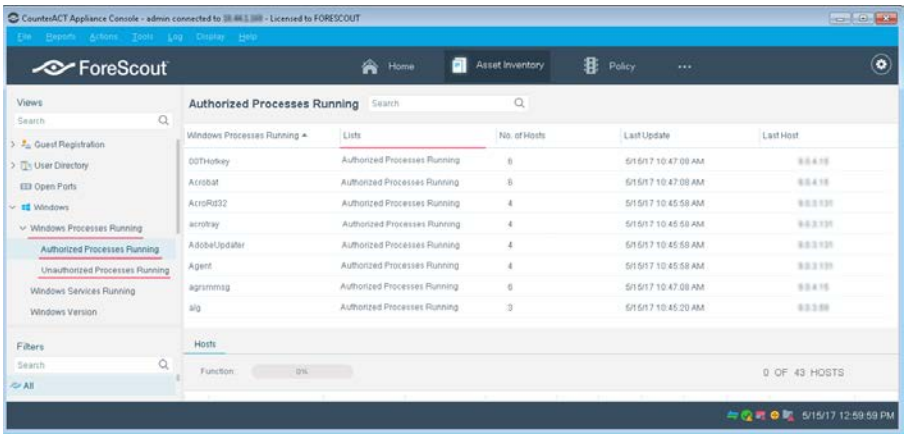
Views Pane

The following items are displayed. If non-bundled plugins, plugins or Extended Modules are installed, items related to the following items may appear.

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

- Services Running
- Operating system versions running
- Macintosh machines
- Users logged-in
- Operating system versions running
- Processes Running
- Software Updates Missing
- Applications Installed

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.



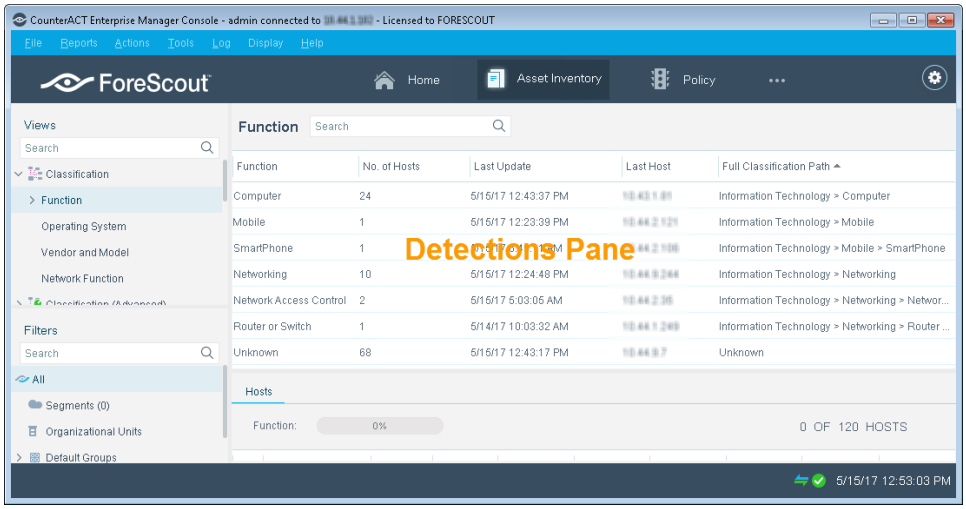
Lists

Detections Pane

The Detections pane displays information about the property that you selected from the Views pane.

Inventory Property (for example, Processes Running)	The property that you selected from the Views pane. Information in this column will include all the values for the related property. For example, if you selected the Process Running property, this column will show all the processes currently running.
No. of Hosts	The number of endpoints currently detected with the selected property. For example, the number of endpoints currently 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 that the detection was made.
Last Host	The last endpoint at which the activity was detected.

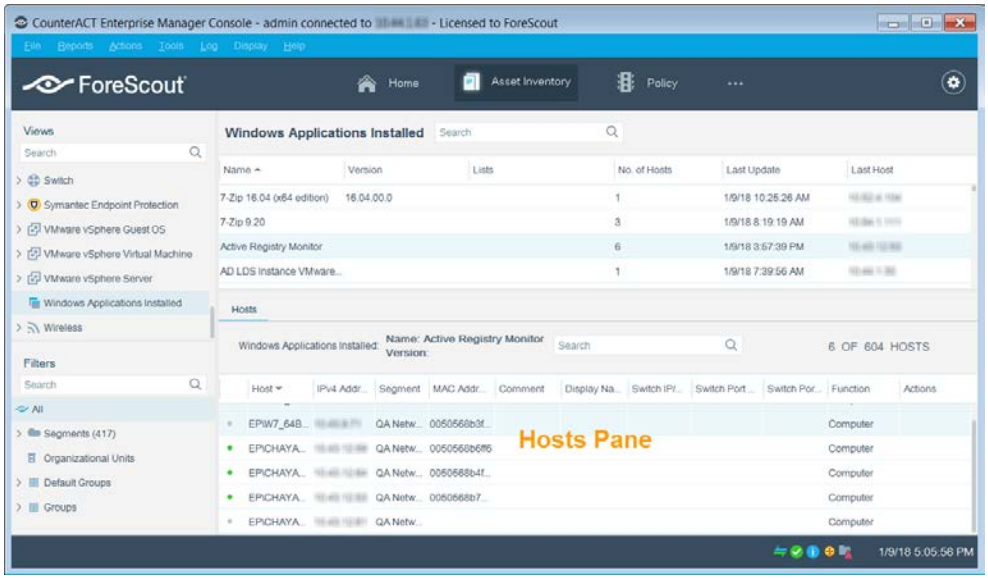
Lists	The lists to which the live inventory property was assigned. For example, the *iexplore.exe* process may be part of the *White listed Server Processes* list and the *White listed Endpoint Processes* list. See Customizing the Asset Inventory for more information about creating lists.



Detections Pane

Hosts Pane

The Hosts pane displays the endpoints that have been detected for the Asset Inventory item selected. Use the tools available when working with endpoint detections to handle these endpoints; for example, 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 Controlling Endpoints from the Detections Pane and Getting More Information about Endpoints for details.



Hosts Pane

Customizing 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.

Two methods are available for working with lists:

- Create Lists Based on Inventory Detections
- Plan Lists Ahead of Time

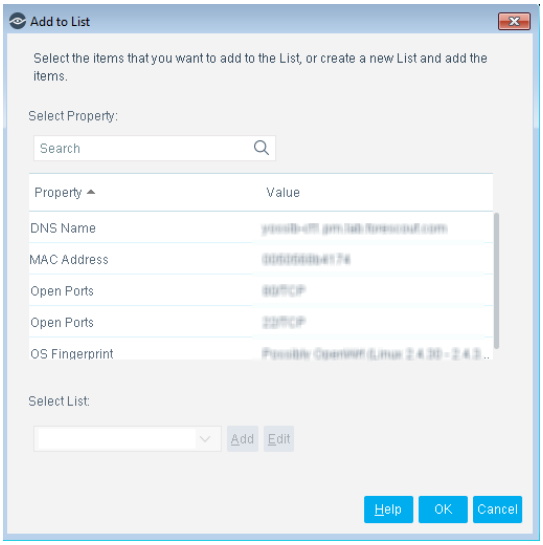
Create Lists Based on Inventory Detections

Create lists based on Inventory detections – for example, if you see that CounterACT 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:

1. Select an Asset Inventory category from the Views pane; for example, **Open Ports**.
2. Right-click one or more property values from the Detections pane.
3. Select **Add to List**.

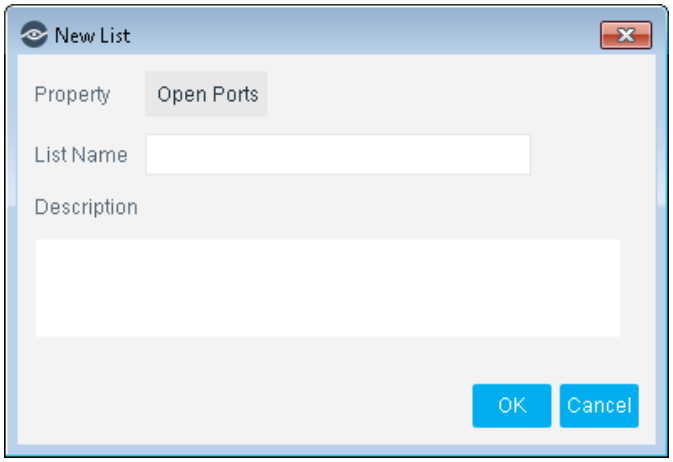
   The Add to List dialog box opens.



Add to List Dialog Box

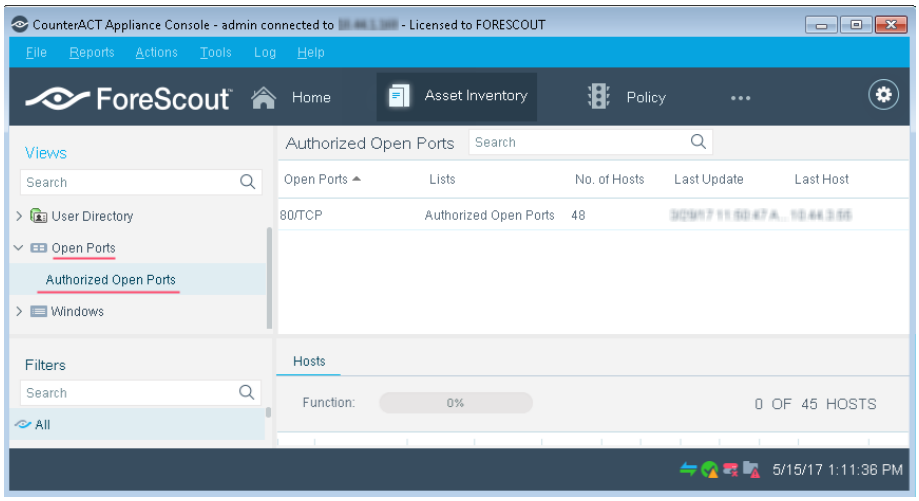
4. Add the value to an existing list by selecting the required list from the drop-down list.

5. Select **OK**. Alternatively, add the value to a new list.
   a. Select Add. The New List dialog box opens.



New List

   b. Type a list name in the List Name field; for example, Authorized Open Ports.
   c. Type a list description in the Description field. The description is displayed in the Lists dialog box, where lists are managed.
6. Select **OK**. The list is added to the Add to List dialog box.
7. Select **OK**.
8. The list is displayed in the Views pane when you select the parent Asset Inventory item.

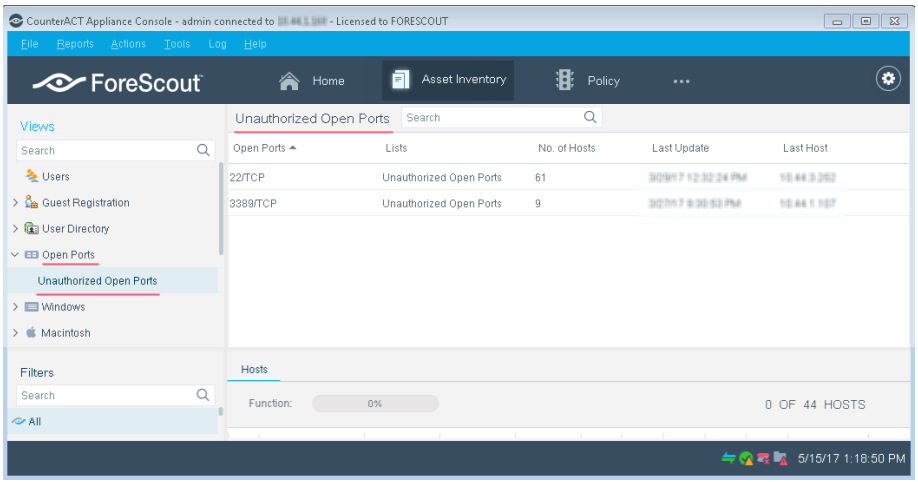


Asset Inventory List

Plan Lists Ahead of Time

You can create inventory Lists for items not yet detected on your network. 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 black lists of open

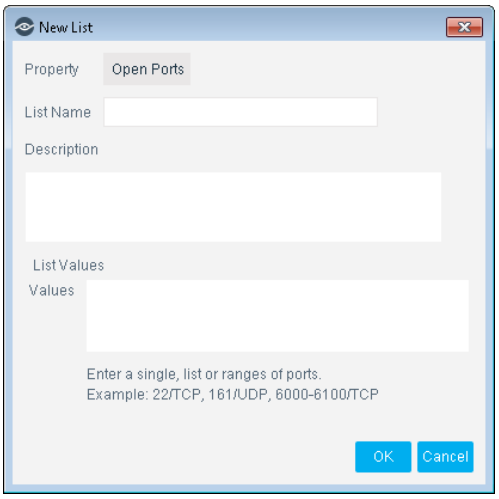
ports. When endpoints start working with these ports, they will appear in the Detections pane>Lists column. Information about endpoints working with these ports is included in the Hosts Pane.



Asset Inventory List

To create lists:

1. Right-click a property folder from the Views pane. For example, right-click Open Ports.
2. Select **Add List**. The New List dialog box opens.



New List Dialog Box

3. In the **List Name** field, type a list name; for example, *Unauthorized Open Ports*.
4. In the **Description** field, type a description of the list. The description is displayed in the Lists pane.
5. In the **Values** field, type the property values; for example, the names of the ports that are not authorized.

6. Select **OK**.

   The values that you enter will 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. 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 more details.

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 items that were previously detected and are currently offline.

To view lists:

1. Right-click the Asset Inventory folder whose sub-items you want to view.
2. Select **View Lists**.
3. The Lists pane opens with all lists related to this item.

See Defining and Managing Lists for information about working with feature.

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 being used in policies. Lists that are currently being used in policies can be edited, but the changes may immediately affect the policy behavior.

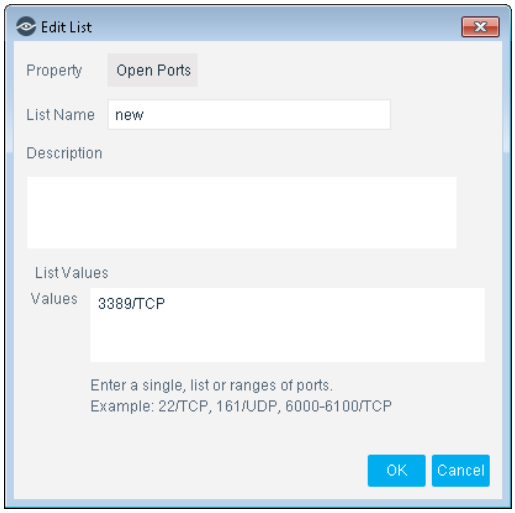
To remove a list:

1. Right-click a list from an Asset Inventory folder.
2. Select **Remove List**.
3. Select **OK**.

To edit a list:

1. Right-click a list from an Asset Inventory folder.
2. Select **Edit List**.

   The List dialog box opens, showing all the values for the list.



Edit List

3. 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.

Use the following 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 CounterACT list or create 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 Using the Lists That You Create for details.

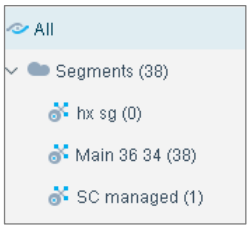
Working with CounterACT Segments

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

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 CounterACT definitions used to specify sub-sections of your network within CounterACT.

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

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



Segments Defined in the Console

After you define segments, you can use them to:

- Filter the Console, Detections pane. For example, display endpoints in the Sales department that match a specific policy.
- Specify IP addresses for CounterACT 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 Chapter 10: Generating Reports and Logs for details.

When you work with segments, note that:

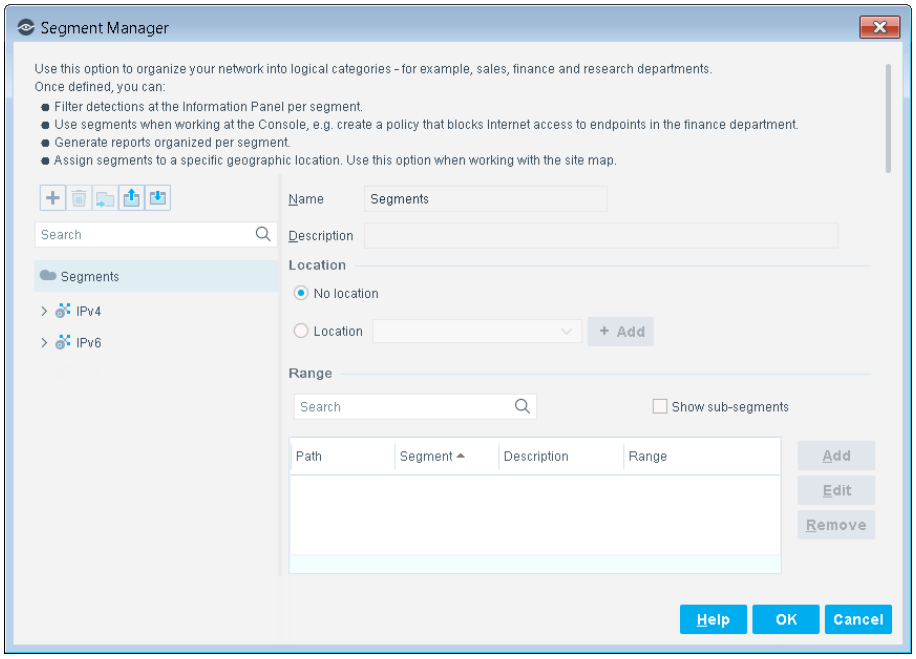
- When you modify an existing segment, this changes the IP addresses that are referenced by the segment wherever it is used in CounterACT. For example, the scope of policies may change, or the CounterACT Appliance that handles certain IP addresses may change.
- One set of segments is shared among all Console users. If one user creates, edits, or deletes a segment all users see the change.
- Use the Audit Trails reports to search for information about users who have modified segment definitions. See Audit Logs for more information.

To work with segments:

1. 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.

   The Segment Manager opens.

   - The left-hand pane shows the tree of segments. Use the search tool in this pane to find existing segments.
   - The right-hand pane shows information for the segment that is currently selected. 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.



Segment Manager

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

2. To modify the segment tree, use the following actions.

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. ***CounterACT may still manage the IP addresses associated with the segment.*** See Removing 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.

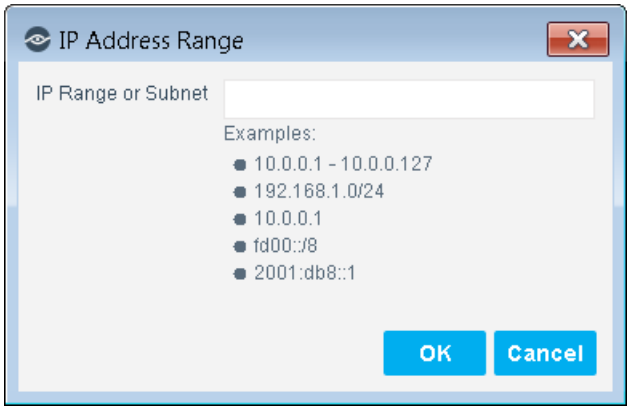
Moving segments in the hierarchy can change the IP addresses they contribute to parent segments. This can change the IP addresses that are referenced by the parent segment.

Import or export a sub-tree of segment definitions to the selected location. Segment definitions are expressed in a XML file structure. See Importing and Exporting the Segment Tree.

3. Select a segment from the Segment tree. In the right-hand pane:

– Edit the **Name** and **Description** fields.

– If you are working with the Console map, select **Location** and enter location information. See Set Up the Map – Create Site Locations for more information.
– To assign IP addresses to the segment, select **Add**. The IP Address Range dialog box opens.



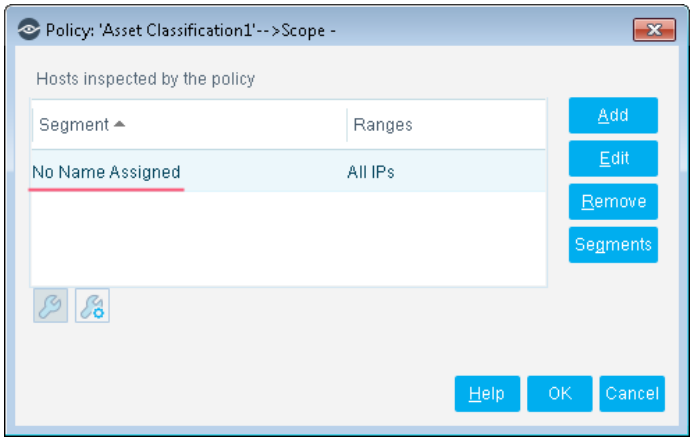
IP Address Range Dialog Box

Enter an IP address range or subnet and select **OK**. The specified IP addresses are added to the segment.

Removing Segments from the Tree

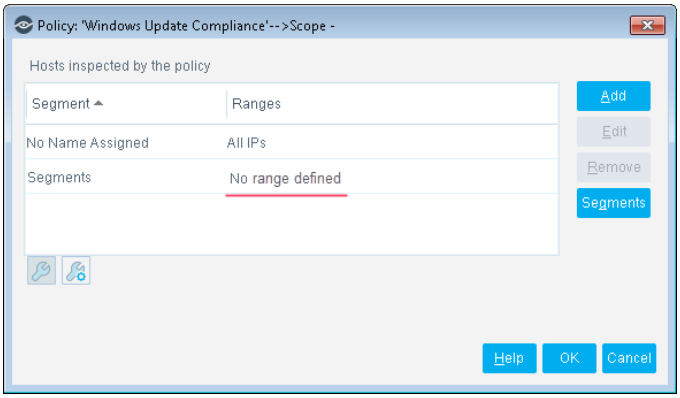
Removing segments from the Segment tree only deletes the segment *name*. If you have already assigned IP addresses to this segment, CounterACT will *still* handle endpoints with those IP addresses.

If you remove the segment, the feature indicates that no segment name is assigned.



Segment Name Removed

Conversely, if you remove IP assignments from the **Ranges** section, those IPs will no longer be included in the segment.



No Range Defined

Importing and Exporting the Segment Tree

You can export or import the entire segment tree or a specific segment. Segment data (segment names and address ranges) is imported or exported as an XML file.

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.

Exporting a Structure

To export a segment:

1. Select **Segment Manager** from the Tools menu. The Segment Manager opens.
2. Right-click the segment that you want to export from the segment tree.
3. Select **Export**.
4. Select XML file format.
5. Locate the file and then select **Export**. The data is exported.

Importing a Structure

You can import your segment structure from an XML file. These files can be created using any standard editing tool.

To create a structure using CSV file format:

1. Define your segment structure using an editing tool. Use the following format:

Segment ID	A unique ID number assigned to each segment.
Parent Segment ID	The parent ID of each segment.
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.

2. Apply the following rules:

- Each segment ID must be a unique number.
- Each segment must have a parent.
- The parent ID for the root segment must be –1.
- If there are a number of ranges within the segment, those ranges must have the same segment ID, parent ID, and name.

3. Save as a CSV file.

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

Sample CSV File Structure for Import

To create a structure using an XML file format:

1. Define your structure using an editing tool. Use the following format:

Entity	Attribute	Description
Group	Name	The name of the segment
Range	Ranges	The ranges included in the segment

The hierarchy defined in the file should represent the hierarchy of the Internal Network.

2. Save as an XML file.

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<NODES>
  <NODE ID="465524609423655971">
    <SEGMENT ID="2066676187115598614" NAME="0.0.0.0-222.222.222.222">
      <RANGE FROM="0.0.0.0" TO="222.222.222.222"/>
    </SEGMENT>
    <RESERVED FROM="224.0.0.0" TO="224.1.134.160"/>
  </NODE>
  <NODE ID="139067896579767066">
    <RESERVED FROM="224.3.13.66" TO="224.4.147.226"/>
  </NODE>
  <NODE ID="6825920946265064143">
    <SEGMENT ID="8094255731330093995" NAME="all ipv6">
      <SUBNET address="::" prefix="0"/>
    </SEGMENT>
    <RESERVED FROM="224.1.134.161" TO="224.3.13.65"/>
  </NODE>
</NODES>
```

Sample XML File Structure for Import

To import the structure:

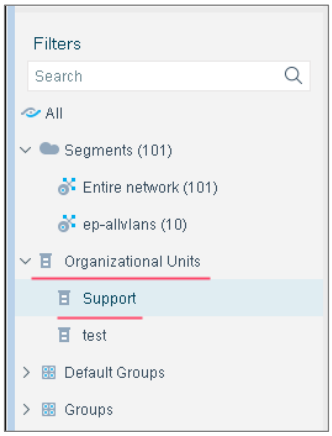
1. Select **Segment Manager** from the Tools menu. The Segment Manager opens.

2. Right-click a segment from the segment tree and select **Import**. An Import dialog box opens.
3. Select a file format and the file name.
4. Select **Import**. The structure is updated to reflect the data in the file.

Working with Organizational Units

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

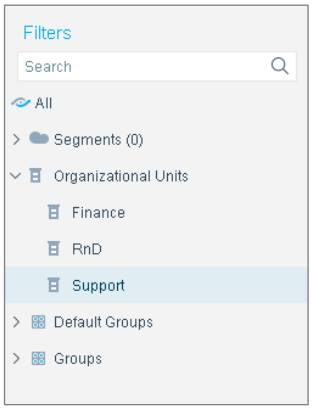
You can filter the view in the Console, Detections pane according to a specific organizational unit. This makes it easier for you to locate problematic network areas.



Console View Filtered per Organizational Unit

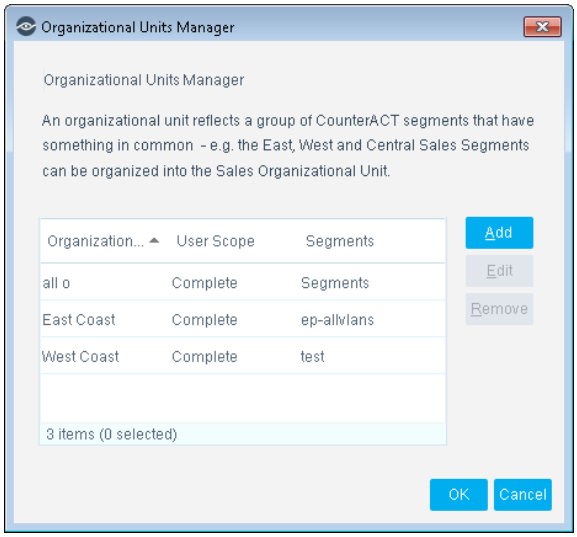
To create organizational units:

1. Right-click **Organizational Units** from the Console, Filters pane.



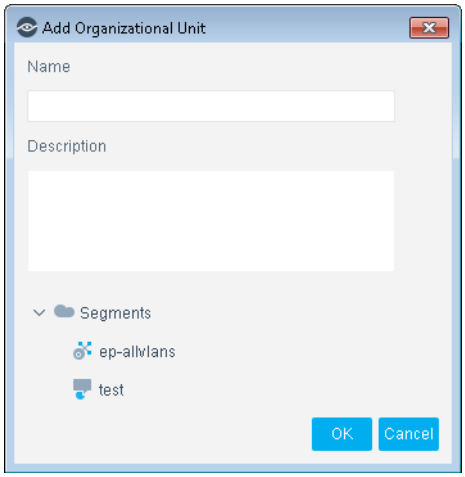
Organizational Units

2. Select **Organizational Units Manager**. The Organizational Units Manager opens.



Organizational Units

3. Select **Add**. The Add Organizational Unit dialog box opens.



Add Organizational Unit

4. Type a unit name in the **Name** field.
5. Type a description in the **Description** field.
6. In the Segments tree, select the segments that you want to include in the unit.
7. Select **OK**.

Adding and Removing Segments from Organizational Units

This section describes how to add and remove segments from Organizational Units.

To add/remove segments:

1. Select the Organizational Unit from which you want to add or remove a segment.

2. Select **Edit**. All defined segments appear. Segments already in the unit you selected are highlighted.
3. Select the **Ctrl** key and then select the segments you want to include in the Organizational Unit. Unselected segments are not included.
4. Select **OK** then **Yes** to save your changes.

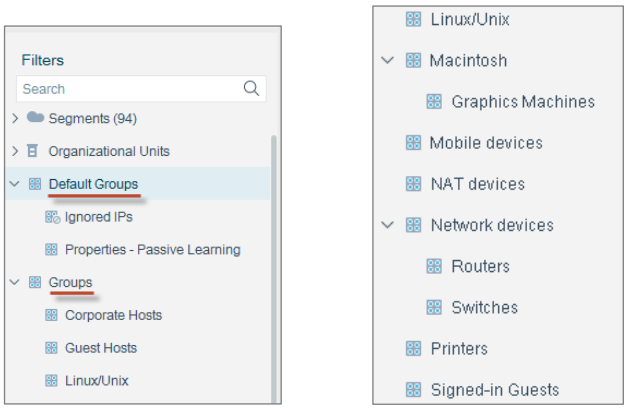
Working with CounterACT Groups

A group is a collection of endpoints with something in common, such as endpoints that run Windows systems or guest endpoints. Groups help you view and manage CounterACT 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.

CounterACT provides some groups by default. For example, asset classification and corporate/guest groups may have been automatically created when your Console was set up. See the About the Initial Setup Wizard and Policy sections for more information. In addition, optional plugins and policy templates may create groups.



Console Groups

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

To add endpoints to a group:

- Specify 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 CounterACT evaluates a policy 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 at a later time if their IP addresses change.

The Audit Trails reports provide information about users who have modified group definitions. See Audit Logs for more information.

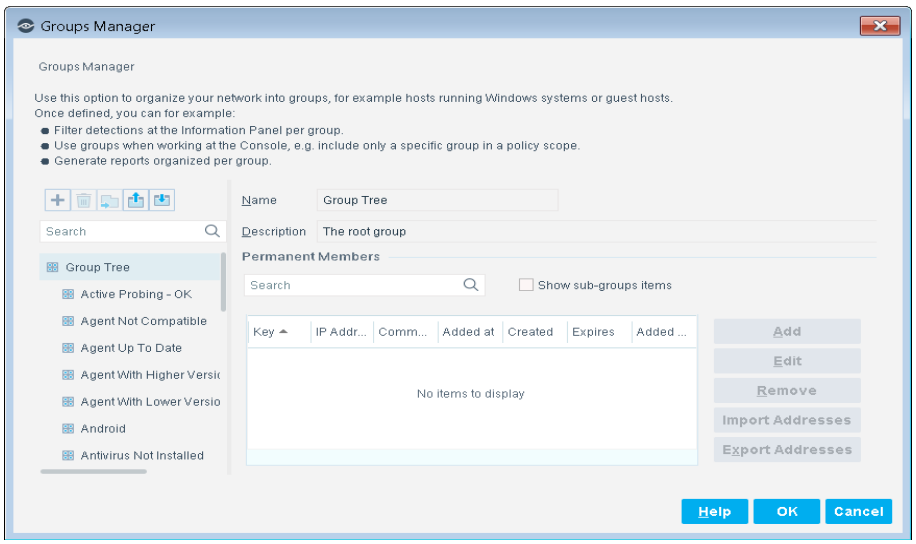
Not all users have access to the Group features. See Access to Console Tools – Permissions for details.

To work with groups:

1. Do one of the following:
   - Right-click a group node in the Filters pane in the Console, and select **Group Manager**.
   - Select **Group Manager** from the Tools menu.

   The Group Manager opens. The group you right-clicked is selected.

   - The left-hand pane shows the tree of groups. Use the search tool in this pane to find existing groups.
   - The right-hand pane shows information for the group that is selected. 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*.



Groups Manager

The table lists the following information for IP addresses assigned to the group:

Key	The value by which the endpoint is associated with the group (IP address or MAC address) CounterACT 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 CounterACT user that added the member (if the was added manually). ▪ The name of the policy that added the member (if added by a policy).
Expires	This is relevant only if the endpoint was added by a policy. It indicates whether the **Expires when host no longer matches policy** option was used, which automatically removes the endpoint from the group when it no longer meets the policy condition.

2. To modify the group tree, use the following actions.

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.

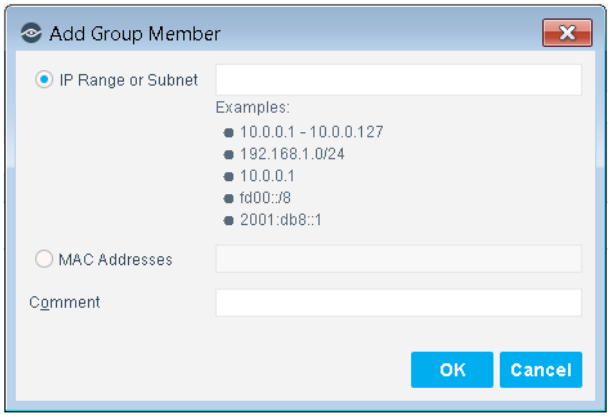
You can also drag and drop nodes of the tree.

Moving group 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.

Import or export a sub-tree of group definitions to the selected location. Group definitions are expressed in a XML file structure. See Import and Export Group Trees.

3. Select a group from the tree. In the right-hand pane, edit the **Name** and **Description** fields.

4. To assign MAC/IP addresses to the group, select **Add**. The Add Group Member dialog box opens.



Add Group Member Dialog Box

Do one of the following:

– To add endpoints to the group by their IP address, enter an IP address, address range, or subnet that is included in the group.

– To add endpoints to the group by their MAC address, enter a MAC address block definition that is included in the group.

Select **OK**. The specified addresses appear in the table.

*To work with groups of IP addresses, use the **Import** and **Export** options. See Import and Export Group Members.*

Import and Export Group Trees

You can export to or import group information from external files. You may want to export groups if you are doing extensive editing and want to use an external tool.

To export Group Trees:

1. In the Groups Manager dialog box, right-click a group and select **Export**.
2. Choose the file location and then select **Export**. The data is exported in an xml file, including any sub-groups.

To import Group Trees:

1. In the Groups Manager dialog box, right-click a group and select **Import**.
2. Browse to an xml file containing group tree information and select **Import**.
3. The group tree described in the file is a subtree at the import location.

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 type a title that will appear in the file header.
5. Use the checkboxes to select the information that is exported.

To import group member details:

1. In the Groups Manager dialog box, select a group.

   The table shows endpoints or MAC/IP addresses assigned to the group.
2. Select Import Addresses. The Import Group Members box opens.
3. Browse to a text file listing addresses. Each address should be on a new line of the file. Select **Import**.
4. The addresses are added to the group.

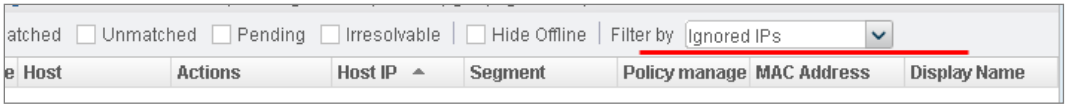
Creating an Ignored IP List

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.

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

Endpoints that you add to this group are included in Threat Protection and Virtual Firewall policy inspections.

You can filter the view in the Detections pane according to ignored IPs.



Ignored IP Filter

How do I create 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 more information.

Restricting Endpoint Inspection

Some devices, such as critical IoT devices can be adversely affected if CounterACT repeatedly connects to resolve properties or run Nmap scans. This is referred to as active scanning.

If you know which devices on your network may be adversely impacted by active scanning, assign these endpoints to the **Properties - Passive Learning** group to limit CounterACT's active inspection of specified endpoints or IP ranges. CounterACT never contacts endpoints in this group to resolve properties, even for policy evaluation. Properties that are learned passively from monitored traffic or third parties may be used for property evaluation, but properties that require endpoint inspection remain *Irresolvable* for endpoints in this group.

SecureConnector still contacts CounterACT from managed endpoints even if they are placed in this group. This means that properties resolved using SecureConnector still are 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 more information.

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.

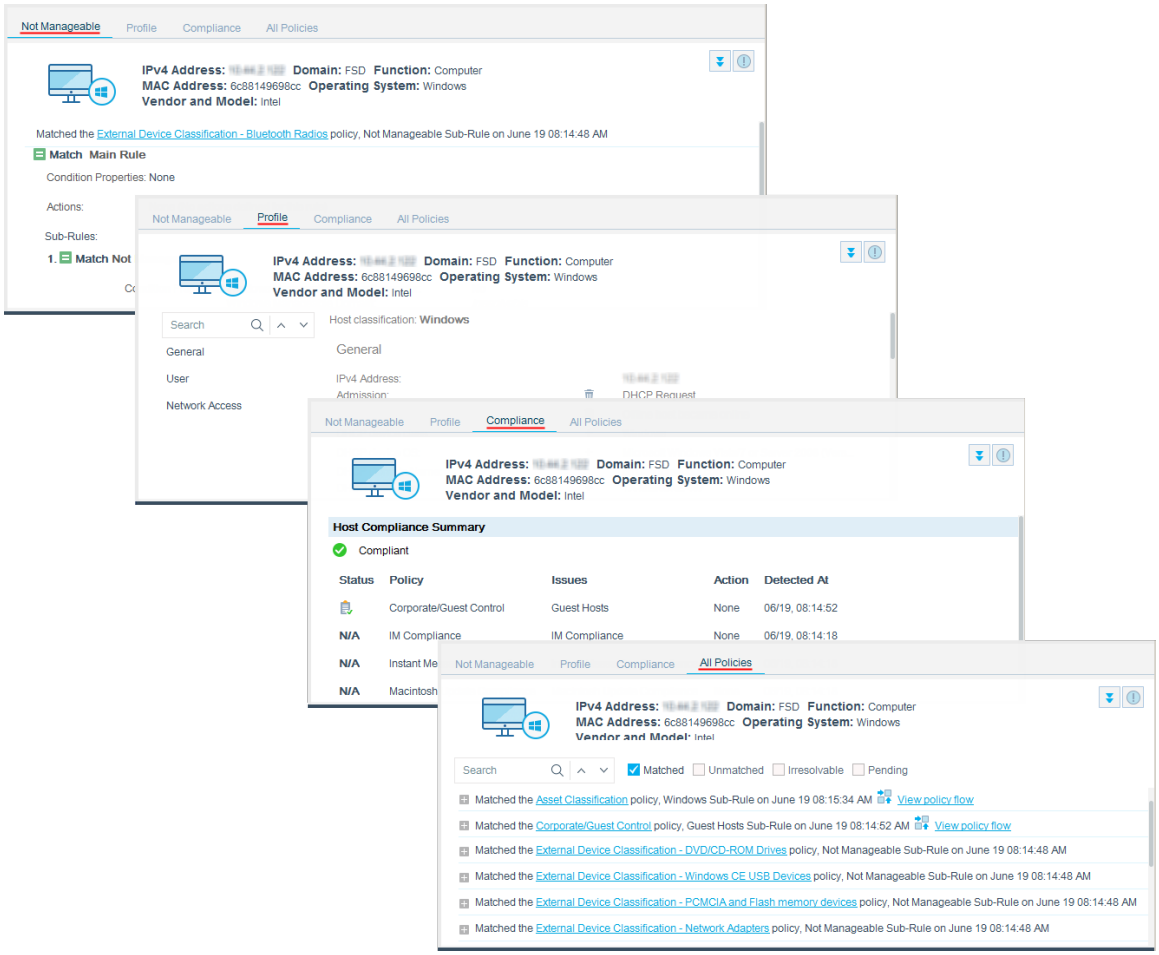
Getting More Information about Endpoints

This section describes how to access detailed information about endpoints from the Detections pane. There are a number of options to view information:

- Details Pane
- Host Log
- Assets Portal

Details Pane

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



Details Pane Tabs

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 from 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.

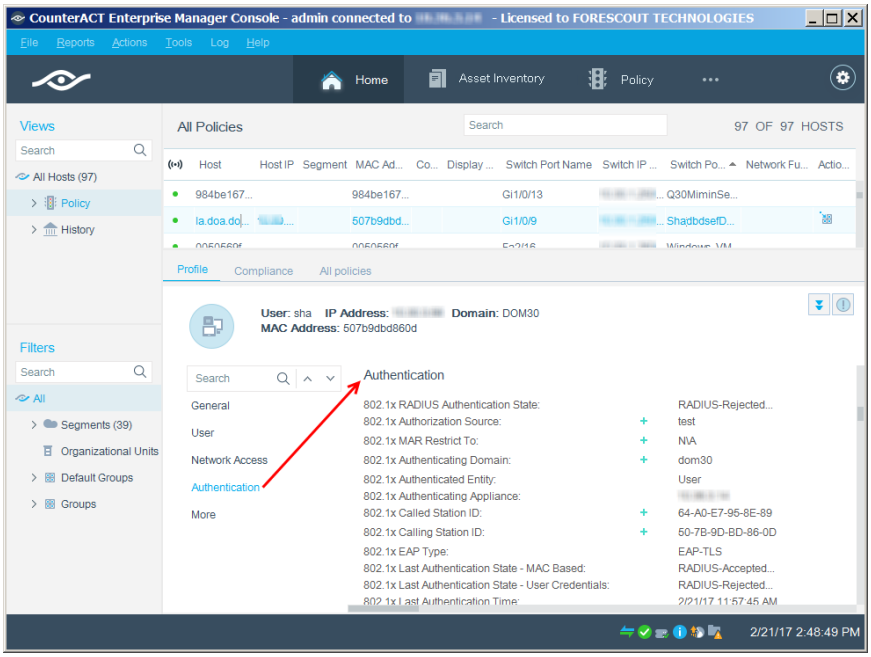
Details Pane Search Options

The Details pane provides the following powerful search options:

- Profile Tab Categories
- Details Pane Search
- Filter by Policy Match Status

Profile Tab Categories

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



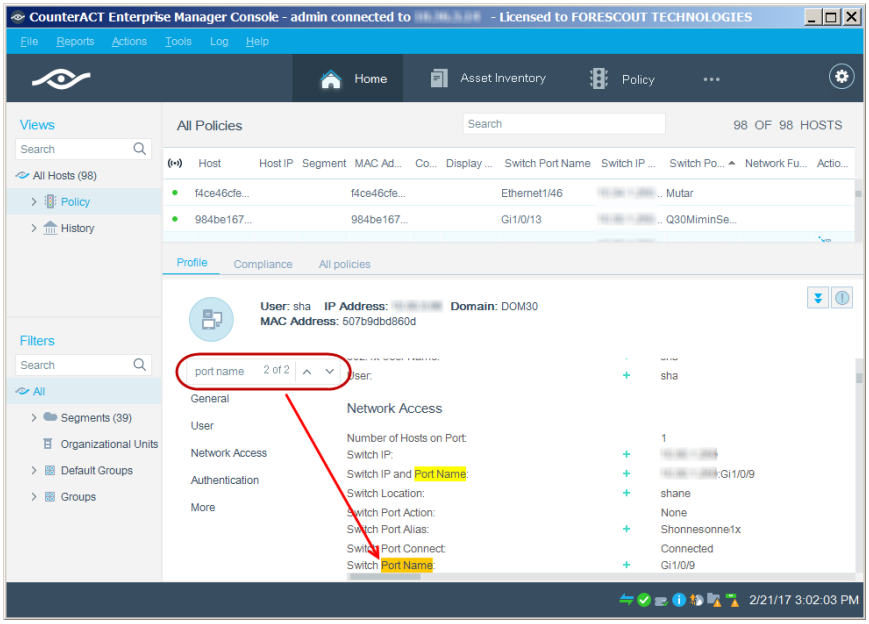
The categories include:

- General (displays widely-used host information)
- User
- Network Access
- Peripherals
- Applications
- Security
- Authentication
- More

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

Details Pane Search

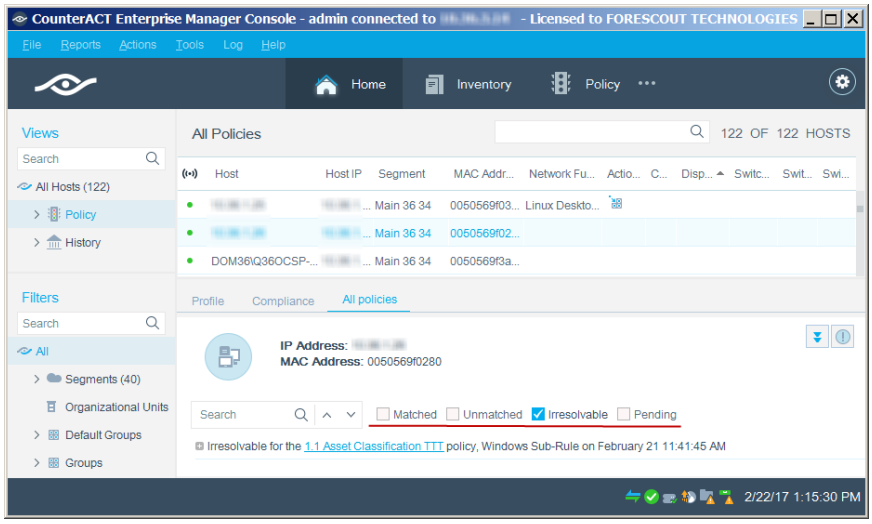
Use the search option in the Profile tab and the All Policies tab to locate specific information displayed in the tab. You can proceed forward and backward through the search results.



Filter by Policy Match Status

You can filter policies by selecting one or more match statuses:

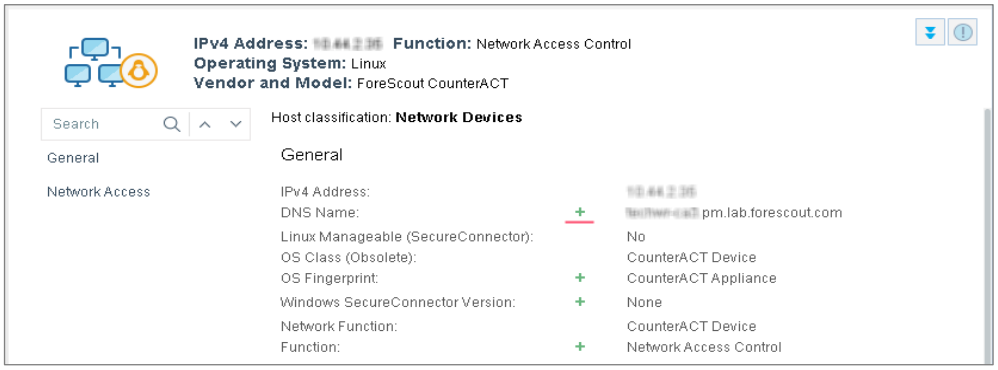
- Matched
- Unmatched
- Irresolvable
- Pending



Details Pane Tools

Options are available to:

- View troubleshooting information by selecting (**Show troubleshooting messages**). See Troubleshooting Messages for more details.
- View all details or a summary. To toggle between details and summary, select (**Show all details**) from the pane.
- Add a property to a CounterACT List by selecting in the Details pane.



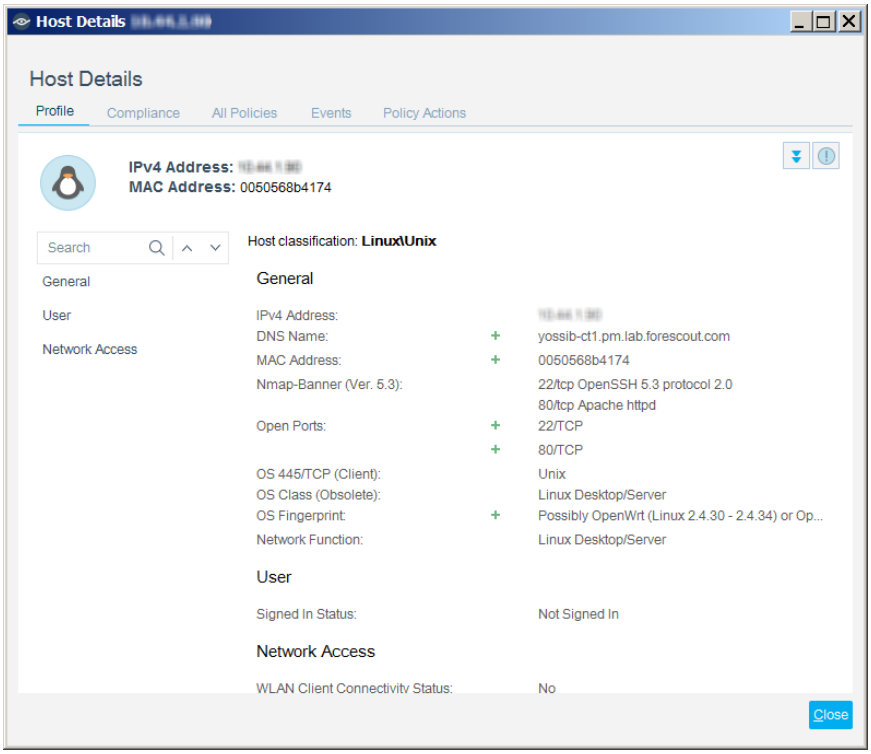
Add to List Link

Viewing Endpoint Details

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:

1. Double-click the endpoint. The Host Details dialog box opens.



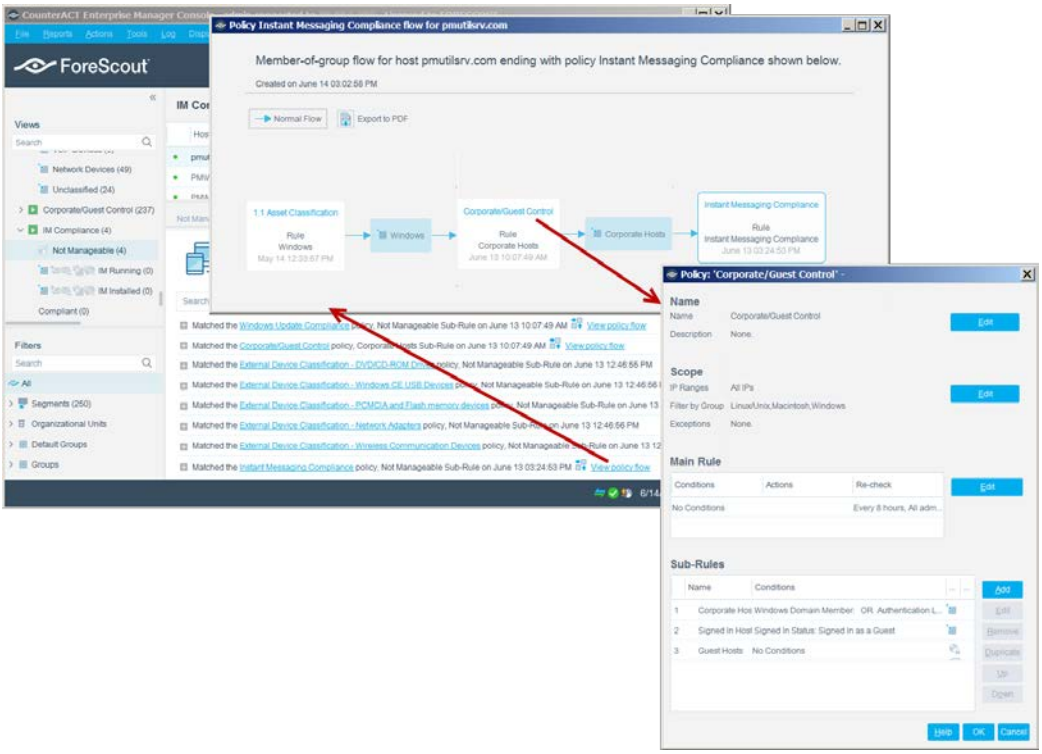
Host Details

Information in the Policy Actions tab can be exported. See Policy Action Log for more information.

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. The diagram shows the flow of policies in 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 information is graphically displayed in a *Policy flow* diagram 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.

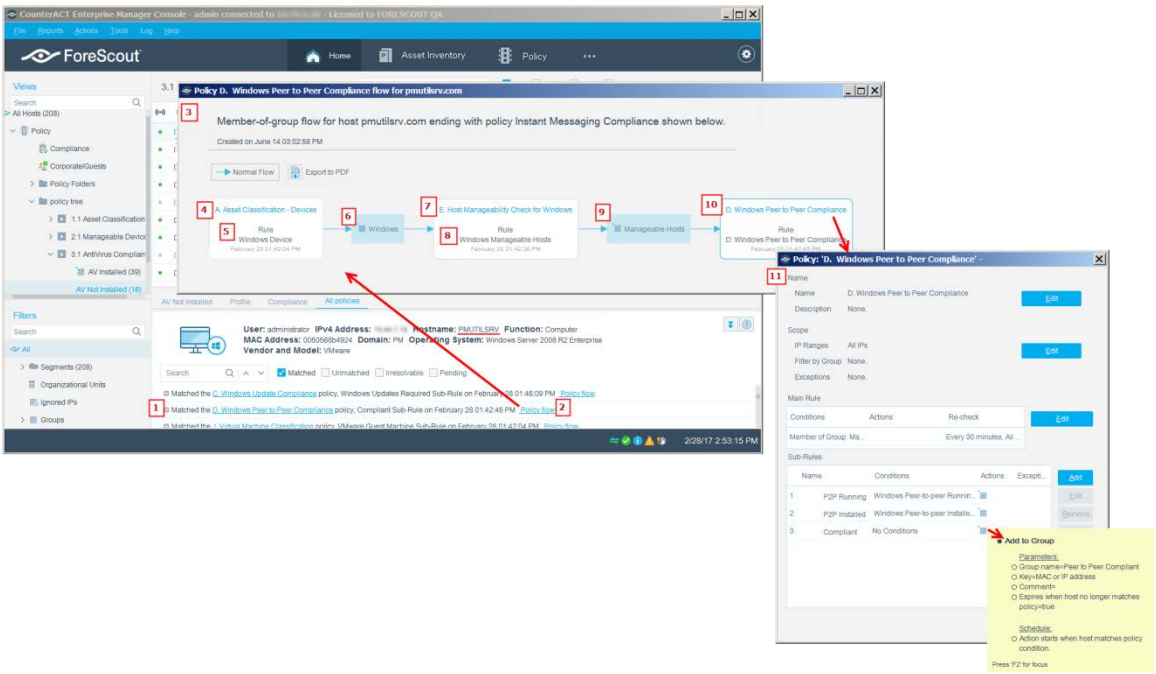


Policy flows are displayed only for policies that meet at least one of the following conditions:

- 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.

Detailed Example of a Policy Flow Diagram



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 policy rule named *Windows Device*.
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 policy rule named *Windows Manageable Hosts*.
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.

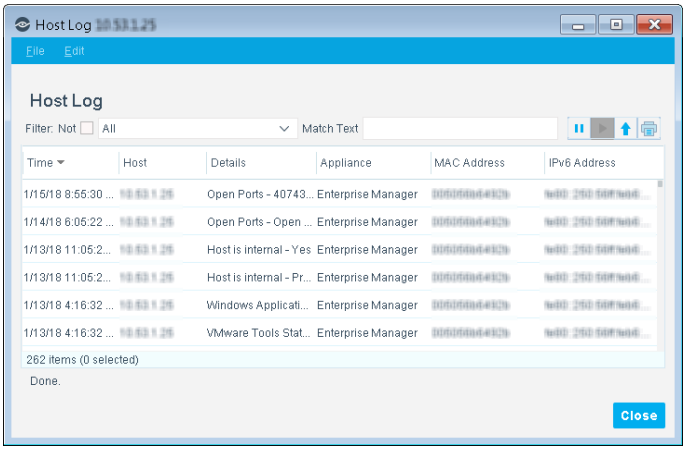
Host Log

Use the Host Log to investigate the activity of specific endpoints, and display information about how CounterACT 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.

To access the Host Log:

1. Right-click an endpoint from the pane and select **Information > Host Log**.
2. Enter a time range and then select **OK**.



Host Log

The following information is available for each entry:

Appliance	The CounterACT 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.
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, rechecked property that was learned regarding the selected IP address ranges.

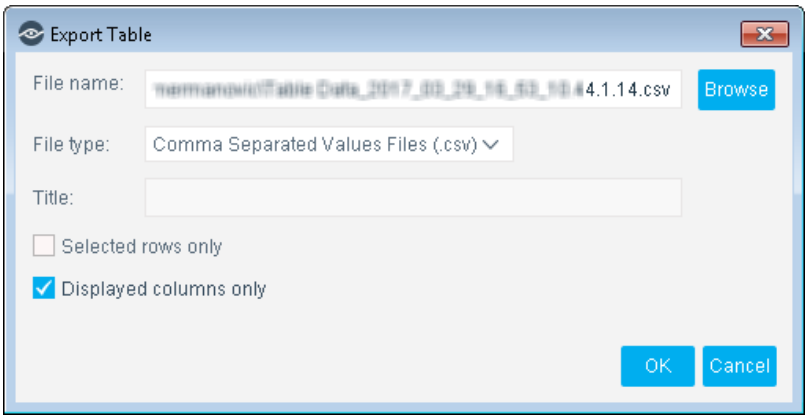
Policy	The name of the Network Integrity policy or sub-policy.
Property	Changes to Network Integrity Policy properties; for example, when authentication changes status.
System	Important CounterACT system events, including Console/Enterprise Manager initialization time, Appliance status, plugin/module 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 Working with System Event Logs.

Exporting the Log

You can export the log data or sections of it to a CSV file.

To export the data:

1. Right-click an endpoint from the pane and select **Information**.
2. Select **Host Log**.
3. Type a time range and then select **OK**.
4. Select **Export** from the **File** menu. The Export Table dialog box opens.



Export Table Dialog Box

5. Browse to the location where you want to save the file.
6. Configure the export options.

Export all information.	Clear all checkboxes.
Only export information displayed in the log. (This does not include information hidden via the Hide/Display column feature.)	Select **Displayed columns only**.
Select rows to export and export all related data. (This includes information hidden via the Hide/Display column feature.)	Select **Selected rows only**.

Select rows to export but only export data displayed. (This does not include information hidden via the Hide/Display column feature.)	Select **Selected rows only** and **Displayed columns only**.

7. Select **OK**.

Assets Portal

The Assets Portal displays information about the endpoint in a web-based search and discovery tool. For example, view information about endpoint properties, policy violations, login information, User Directory user identity details, organizational mapping details, endpoint device connections and more. You can perform Google-like searches from the portal. See Chapter 9: Assets Portal for more information.

To access the portal:

1. Right-click an endpoint from the pane and select **Information**.
2. Select **Show in Assets Portal**.

Working 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 on their compliance level with your corporate security policies.
- Offering users instructions for performing self-remediation by following links that you provide.

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.

The ForeScout Compliance Center is not accessible whenever HTTP Redirection is disabled. For more information, see Disabling 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 open the compliance wizard manually from their endpoint to view their compliance status as well.

Customizing Page Design

The design of the ForeScout Compliance Center may be customized. In addition to customizing the look and feel of the page, i.e. 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 by using CounterACT 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 and educate your users as to security requirement at your organization, and force them to bring their machines to compliance. This may be useful, for example, at universities or organizations where guests may be required to self-remediate.

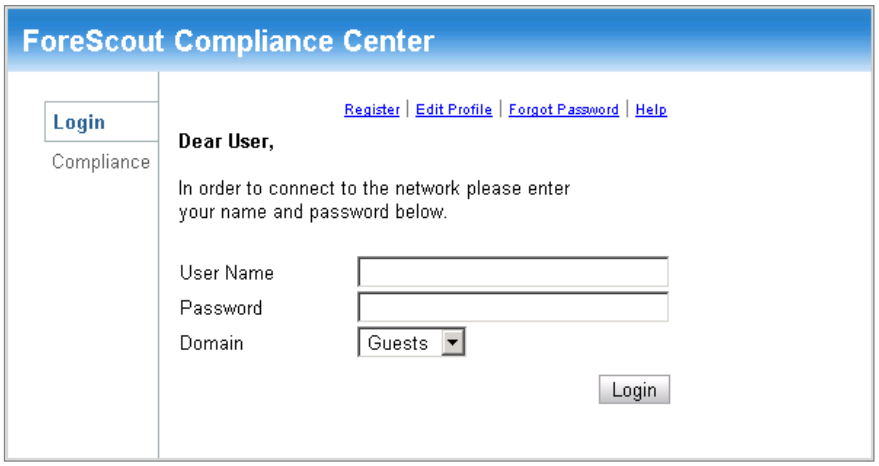
What the Endpoint Users See

The ForeScout Compliance Center dialog box is comprised of two tabs:

- Login Tab: For entering the user name and password to gain access to the network.
- Compliance Tab: For viewing the user compliance status and for providing links to help self-remediate in the event of noncompliance.

Login Tab

The Login tab prompts users to enter their login credentials to sign in to your network. See the HTTP Login action for more information about when the Login tab is activated.



ForeScout Compliance Center Dialog – Login Tab

After users have successfully signed in, the Compliance tab opens.

Compliance Tab

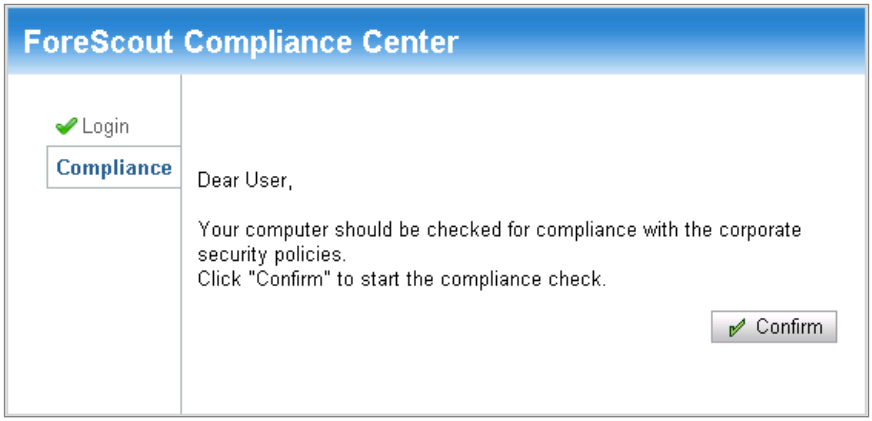
The Compliance tab:

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

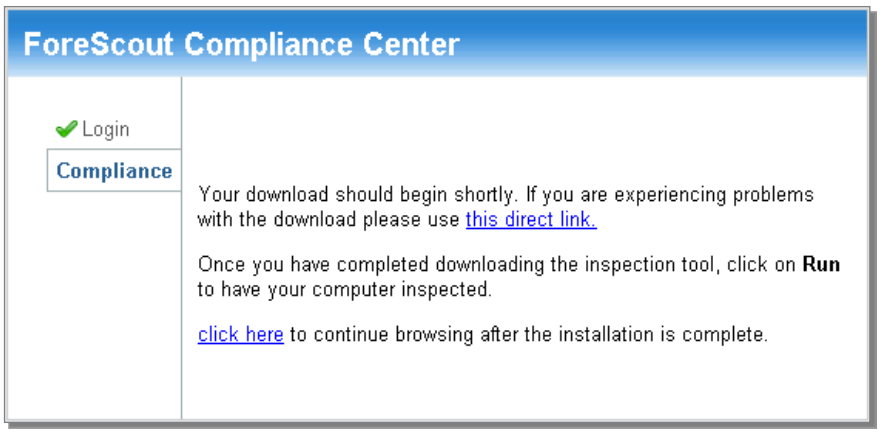
You can add additional comments to this tab by using the HTTP Notification action. Messages entered using these actions are also displayed in the tab.

Installing SecureConnector

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



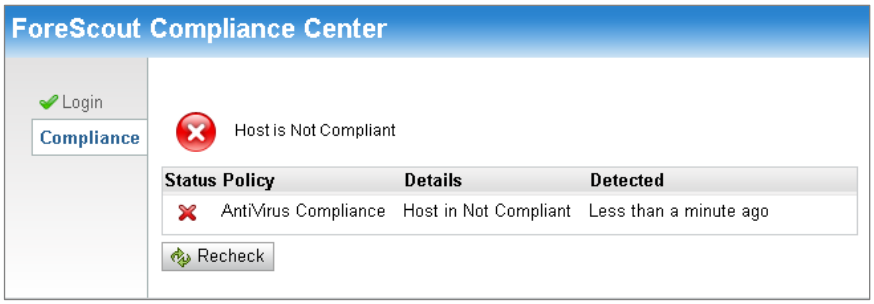
Initial SecureConnector Page



Secondary SecureConnector Page

Achieving Compliance

The Compliance tab displays the endpoint compliance status.



ForeScout Compliance Center Dialog – Noncompliance

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

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.

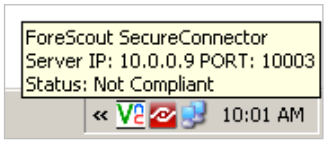
Users can select **Recheck** to verify their compliance status. All categorized policies are rechecked against the GUI Policy Editor options. Categorization is configured in the Policy Manager. See Working with the Policy Manager for details.

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

ForeScout Compliance Center Dialog – Compliance

Compliance Notification at Endpoint

If there is noncompliance at the endpoint, CounterACT notifies the user. On the Windows Notification Bar at the bottom of the window, the **CounterACT** icon is displayed as red. Placing the cursor over the icon, the endpoint details are displayed.



Noncompliance Indication

Accessing the Compliance Center from the Endpoint

Users can access the Compliance Center if SecureConnector is running on their endpoints.

To access the Compliance Center from an endpoint:

1. Move the cursor over the **ForeScout** icon in the system tray to view compliance status.
2. Right-click the icon to open the ForeScout Compliance Center dialog box.

Exiting the Console

When you exit the Console, CounterACT continues to protect your network. System and user events that occurred during logout can be viewed. See Chapter 10: Generating Reports and Logs for more information.

To exit the Console:

1. Select **Exit** from the **File** menu.

Chapter 4: CounterACT Policy Templates

- Working with Policy Templates
- Asset Classification and Primary Classification Templates
- Classification Upgrade Impact Analysis Template
- Mobile Classification Template
- External Device Classification Template
- Virtual Machine Classification Template
- Passive Learning Mode Template
- Corporate/Guest Control Template
- External Disk Drive Compliance Template
- Overall Endpoint Compliance Template
- Individual Compliance Templates
- Windows Update Compliance Template
- Macintosh Update Compliance Template
- Threats Templates
- Track Changes Templates
- New TCP/IP Port Template

Working with Policy Templates

CounterACT templates are predefined policies. Templates 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 CounterACT's major capabilities.
- Rollout 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 – instructions regarding how to handle endpoints – are generally disabled by default. You should only enable actions after testing and fine-tuning the policy.

Creating Policies Using Templates – Basics

The following table provides a brief description of available CounterACT templates.

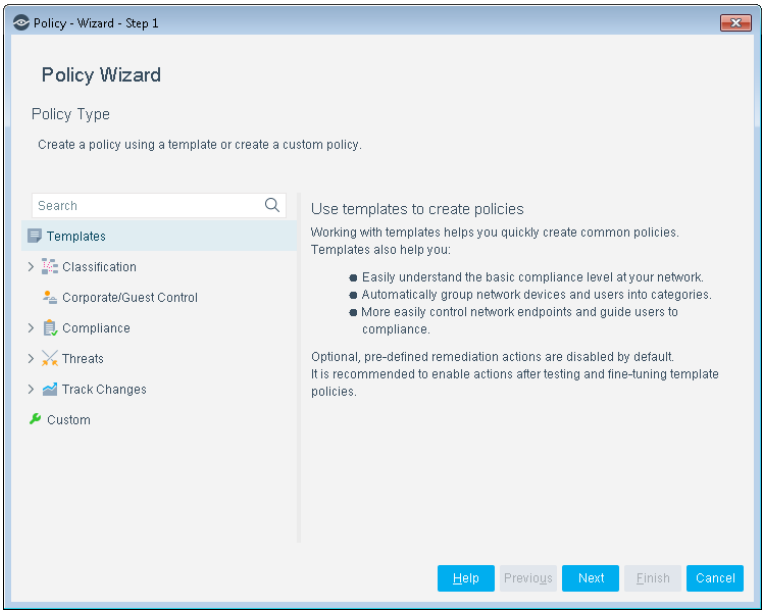
Category	Policies	Description
Classification	Asset Classification and Primary Classification Templates Classification Upgrade Impact Analysis Template Mobile Classification Template External Device Classification Template Virtual Machine Classification Template	Create policies that detect network devices according to these categories. Discovered endpoints are placed in CounterACT groups that are displayed in the Console, Filters pane.
Corporate/ Guest Control	Passive Learning Mode Template	Create a policy that detects and classifies your network into the following CounterACT 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.

Category	Policies	Description
Compliance	Individual Compliance Templates ▪ External Disk Drive ▪ Antivirus ▪ Peer-to-Peer ▪ Personal Firewall ▪ Instant Messaging ▪ Windows Update ▪ Macintosh Update ▪ Overall Endpoint	Generate compliance policies, understand the compliance level at your network, guide users to compliance and remediate endpoints.
Threats	Malicious Hosts Template ARP Spoofing Template Impersonation Template Dual Homed Template	Detect and remediate threats to your network by enforcing policies against a range of widely used techniques.
Track Changes	Track Changes Templates ▪ Application ▪ Hostname ▪ Operating System ▪ Shared Folder ▪ Switch ▪ User ▪ Windows Service ▪ New TCP/IP Port	Track changes within your network to identify unauthorized changes and remediate possible threats.
PCI Compliance (available after the PCI Kit Plugin is installed)	Selected PCI policies	Implements over 20 PCI policies and generates related report to help you during a PCI audit. The template includes predefined actions for automatic remediation of endpoints that do not comply with the PCI specification. Refer to the *ForeScout CounterACT PCI Guide* for more information about this template and about PCI compliance.

If you installed plugins or modules, related templates may also be available. See Chapter 8: Base, Content and Extended Modules for details.

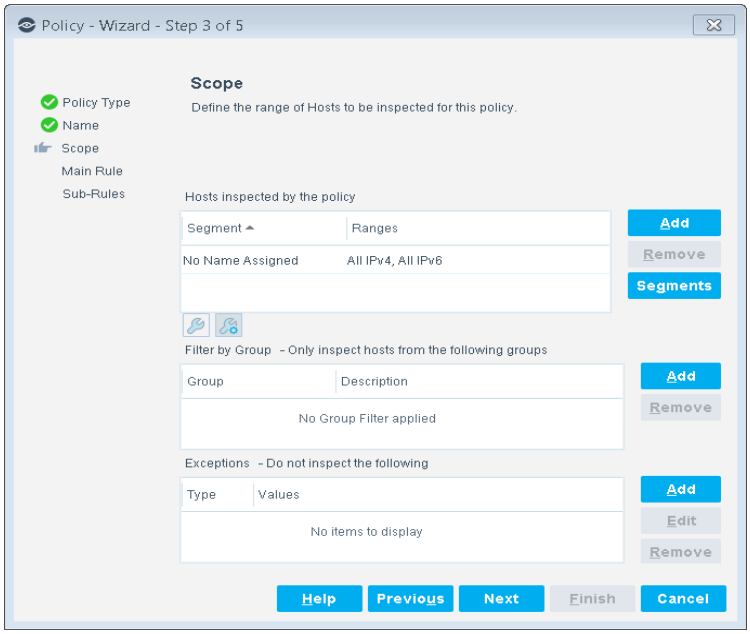
To create policies from templates:

1. Select the Policy tab. The Policy Manager opens.
2. Select **Add**. The Policy Wizard opens.



Policy Wizard – Templates

3. Select a policy template. The Asset Classification and Corporate/Guest Control policies may have been run during the initial Console setup. Run either the Asset Classification or the Primary Classification policy wizard to create network asset classification groups, and then the Corporate/Guest Control policy wizard, before defining other policies.
4. Select **Next**.
5. In the Scope page, 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.



Policy Wizard – Sample Scope

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 and Edit Policies and Rules.
9. When you are satisfied with the policy results, run the policy again and, if necessary enable predefined actions. See Starting Actions on Selected Endpoints for information about enabling actions.

How Often Are Endpoints Rechecked?

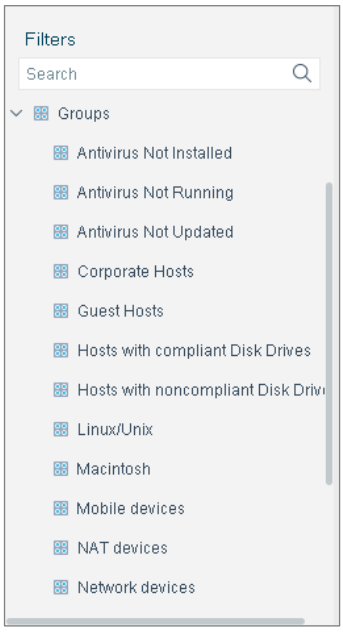
By default, policies are rechecked:

- Every eight hours.
- On all admission events. For example, when an endpoint physically connects to a switch port, when its IP address changes or when it sends out a DHCP request. For more information, see Updating a Recheck Policy for Unmatched and Matched Endpoints.
- When new information is learned about an endpoint being inspected by the policy.

Tips for Rolling Out Templates

To create policies that classify the network into CounterACT groups, use either the Asset Classification or the Primary Classification template to create network asset 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 CounterACT from scratch, then the Asset 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.



Template Groups in the Console Filter

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. See Edit Policies and Rules for more information.
- 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. The rollout should be handled 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. CounterACT 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 Creating Custom Policies.

Detections and actions resulting from the template policies appear in the Home view, and can be managed from there.

Asset Classification and Primary Classification Templates

The section covers:

- About Classification
- Template Classification Groups
- Properties Resolved by a Primary Classification Policy
- Prerequisites
- Using the Template
- Which Devices Are Inspected – Policy Scope
- How Devices Are Classified – Policy Condition
- Handling Discovered Devices – Policy Actions
- Replacing Asset Policies
- Using an Action to Assign a Classification
- Fine-Tuning the Classification Mechanism

About Classification

Classification is an objective assessment of what a device is, from a functionality, operating system and manufacturer & model point of view. CounterACT uses all the data discovered about each device to intelligently figure out what the device is.

Two classification policy templates are available:

- The Asset Classification template is a legacy CounterACT template that provides limited information about endpoints.
- The Primary Classification template, a feature of the Device Classification Engine, uses a vast array of information provided by various CounterACT components in order to determine the function, operating system and vendor & model of each endpoint. The policy template then uses this classification information as conditions for sub-rules to broadly classify the endpoints.

To take advantage of more precise classification profiles, it is recommended to create and run Primary Classification policies instead of Asset Classification policies.

Template Classification Groups

Policies created based on the Asset Classification template or the Primary Classification template can create CounterACT groups for the following device categories, and automatically place each endpoint in the appropriate device group.

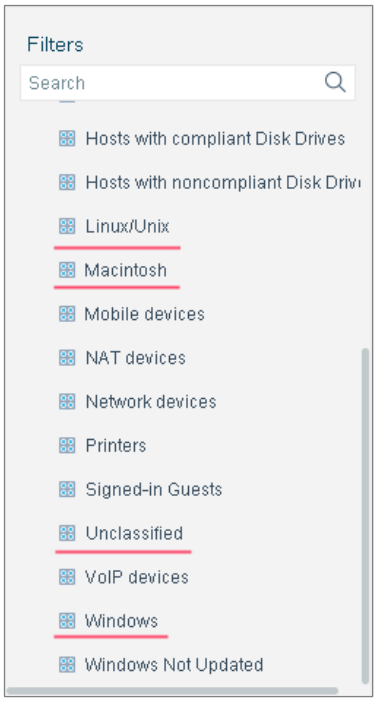
Groups That Can Be Created by Primary Classification Policies	Groups Created by Asset Classification Policies
CounterACT Devices	
Storage	
NAT devices: Devices that may hide other devices.	**NAT devices**: Devices that may hide other devices.
Mobile devices	**Mobile devices**
Windows	**Windows**
Printers	**Printers**
Linux/Unix	**Linux/Unix**
Macintosh	**Macintosh**
VoIP devices	**VoIP devices**
Network devices: Networking equipment, such as WLAN controllers, routers, switches, and wireless controllers.	**Network devices**: Networking equipment, such as WLAN controllers, routers, switches, and wireless controllers, as well as CounterACT devices and network storage devices.
Unclassified: If CounterACT does not know to which category an endpoint is associated. This may happen, for example, if network devices are new.	**Unclassified**: If CounterACT does not know to which category an endpoint is associated. This may happen, for example, if network devices are new.

Primary Classification policies create separate groups for CounterACT devices and network storage devices. Asset Classification policies include all these devices in the Network devices *group.*

If a device does not meet the criteria for any group or if CounterACT cannot evaluate the endpoint, it is placed in an Unclassified group. The operator may then choose to manually classify the device. See Using an Action to Assign a Classification.

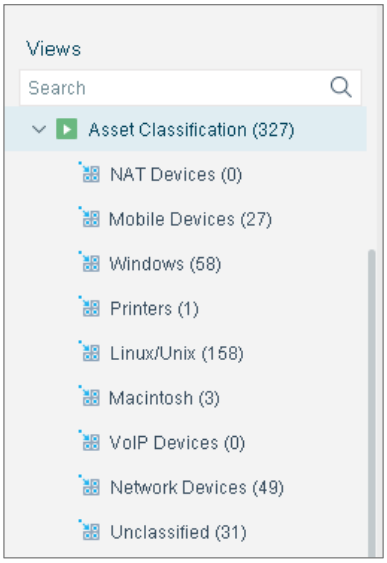
The Primary Classification template includes a sub-rule that indicates if a member of the Exempt-Approved Misc Devices *group does not meet the criteria for a classification category. It is recommended to add to this group all the endpoints that CounterACT does not classify, but that you know about and specifically do not want to fall into the Unclassified group.*

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.

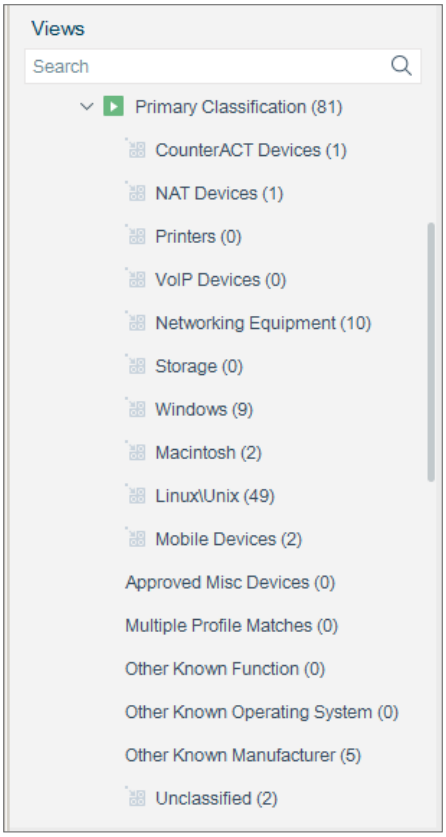


Groups Created by an Asset or Primary Classification Policy

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.



Asset Classification Policy Sub-Rules



Primary Classification Policy Sub-Rules

Properties Resolved by a Primary Classification Policy

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

These properties are *not* resolved by Asset Classification policies.

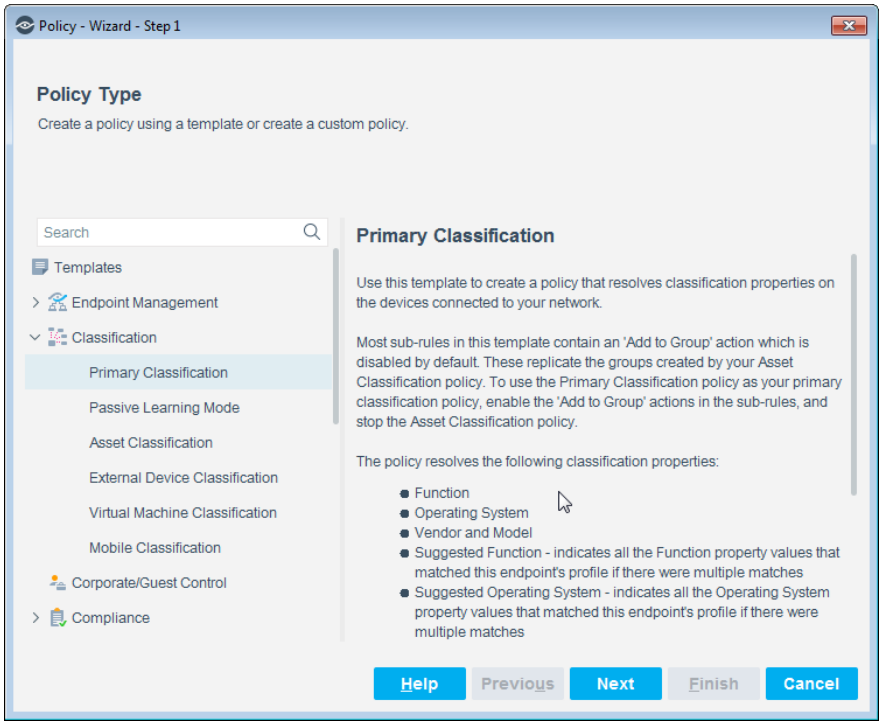
Prerequisites

- Consider which endpoints you want to inspect. See Which Devices Are Inspected – Policy Scope. The policy does not handle endpoints outside of the Internal Network.
- Verify that either an Asset Classification policy or a Primary Classification policy using the *Add to Group* action is run before any other policy.
- Groups created by these policies are used when working with policies created by other templates. Check the Console Home tab, 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.

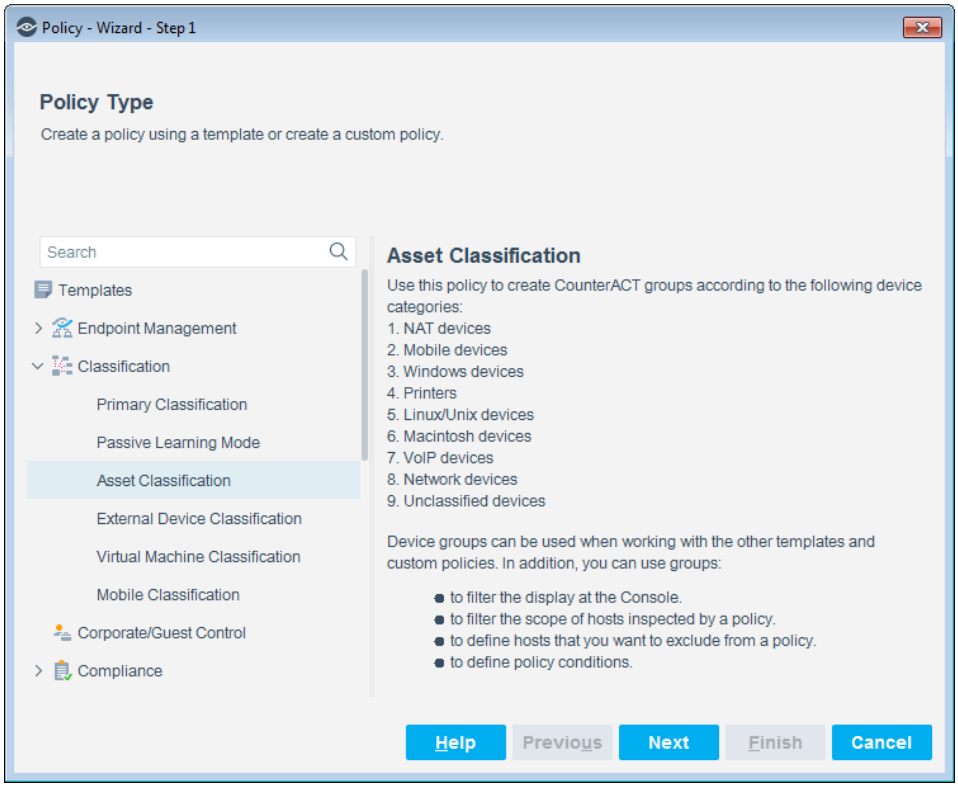
Using the Template

To use the template:

1. Select **Add** from the Policy Manager, and expand the Classification folder.
2. Do one of the following:
   - To create a policy using the Primary Classification template, select Primary Classification.



   - To create a policy using the Asset Classification template, select Asset Classification.



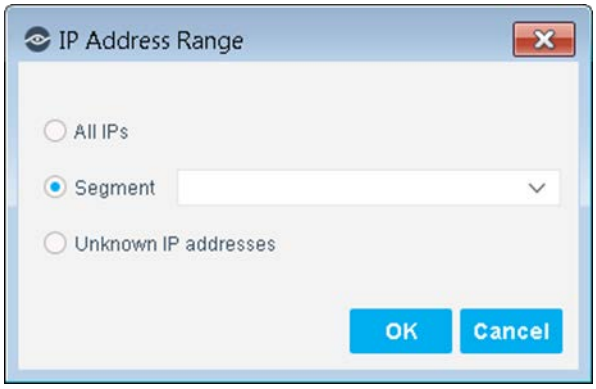
3. Select **Next**. The Name page opens.
4. Edit the name if required and add a description. See Naming Tips for guidelines about creating effective names.
5. Select **Next**. The Scope page opens.

Which Devices Are Inspected – Policy Scope

Classification policies instruct CounterACT to 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 Asset Classification or Primary Classification policies. For details about excluding sensitive endpoints, see Restricting Endpoint Inspection

To set the policy scope:

1. Use The IP Address Range dialog box to define which endpoints are inspected.

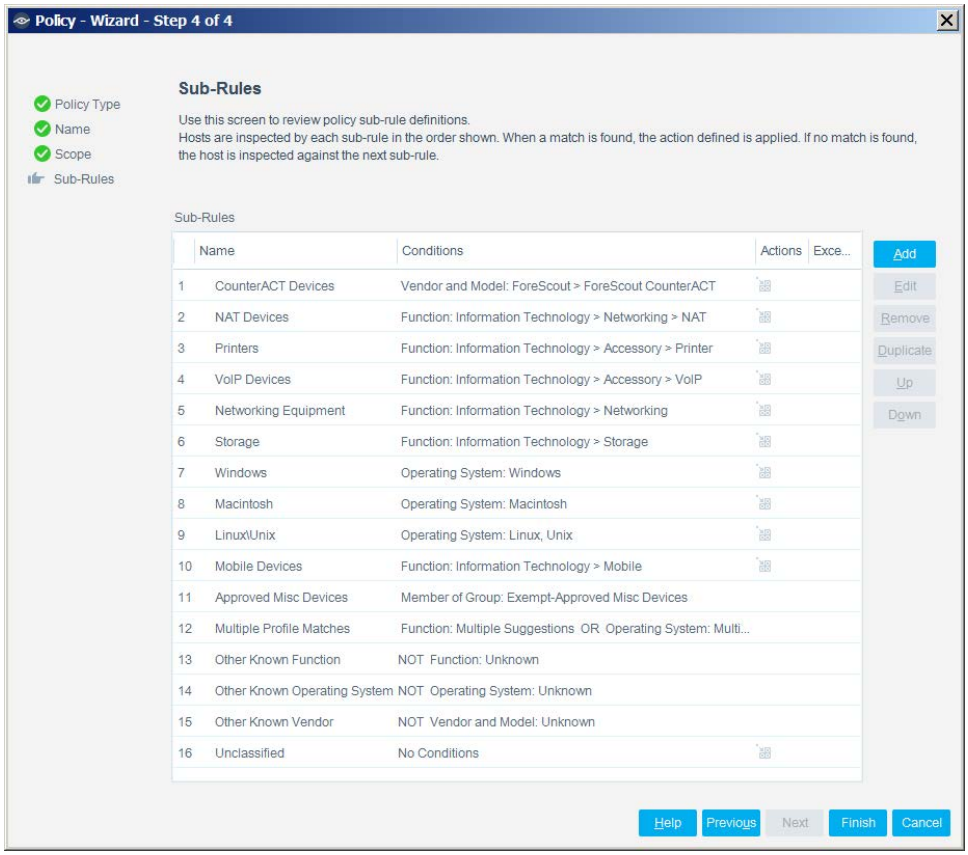


The following options are available:

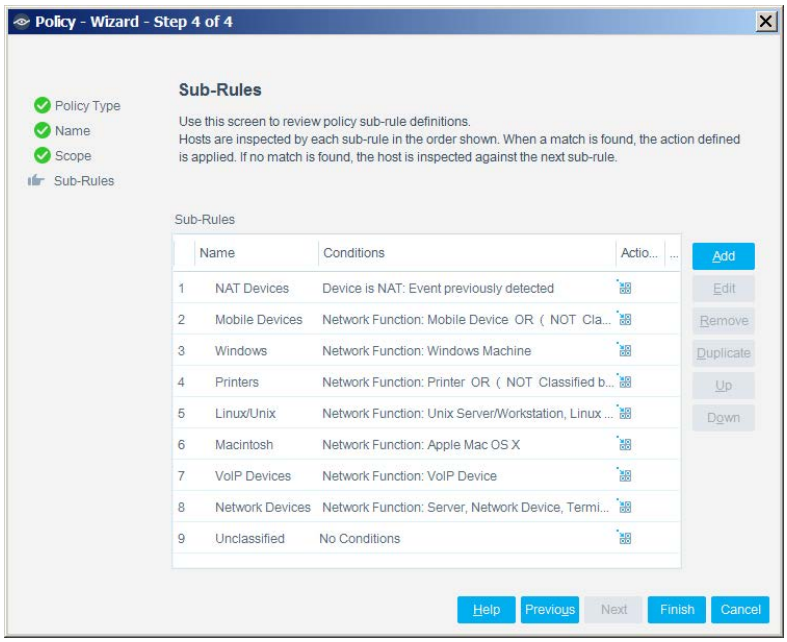
– **All IPs**: Include all IP addresses in the Internal Network.
– **Segment**: Select a previously defined segment of the network. To specify multiple segments, select **OK** or **Cancel** to close this dialog box, and select **Segments** from the Scope page.
– **Unknown IP addresses**: Apply the policy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

The Asset Classification policy template requires endpoints to have known IP addresses. Do not select the Unknown IP addresses option when using the Asset Classification policy template.
The Primary Classification policy template can resolve classification properties for endpoints even when their IP addresses are unknown.

2. Select **OK**. The added range appears in the Scope page.
3. To filter the specified ranges or add exceptions, select (**Advanced**).
4. Select **Next**. The Sub-Rules page opens. This page lets you review sub-rule conditions and actions.



Primary Classification, Sub-Rules



Asset Classification, Sub-Rules

How Devices Are Classified – Policy Condition

Properties used by these classification policies can be resolved on all endpoints within the policy range.

Refer to the HPS Inspection Engine Configuration Guide *for more information about classification methods. Select* ***Options*** *from the* ***Tools*** *menu. Select* ***Modules****. Select this plugin and then select* ***Help****.*

Device Classification Using an Asset Classification Policy

An Asset Classification policy attempts to resolve each connected endpoint's Network Function property.

The Device is NAT property resolves if the device is a NAT device.

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

These properties are not resolved by an Asset Classification policy.

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'.

Viewing Policy Conditions

You can learn more about how the detection mechanism is defined by viewing policy *conditions*.

To view policy conditions:

1. Select an item from the Sub-Rules page.

2. Select **Edit**.

   The Sub-Rules dialog box opens for the condition that you chose.
3. Select a criterion from the **Condition** section and select **Edit**.
4. The Condition dialog box opens, displaying the parameters.

Handling Discovered Devices – Policy Actions

Policy *actions* instruct CounterACT how to respond to device detections.

The policy can create CounterACT groups according to the device categories.

- In an Asset Classification policy, these actions are enabled by default.
- In a Primary Classification policy, these actions are disabled by default to avoid possible conflicts with the Asset Classification Policy.

When Are Endpoints Removed from Groups?

Endpoints are removed from groups if CounterACT discovers, during policy recheck, that the device function or type has changed, or if the policy has been stopped.

Replacing Asset Policies

If you find that the *Primary Classification* policy provides more comprehensive classification in your environment than an existing *Asset Classification* policy, it is recommended to use it as your primary classification policy. To do this, ensure that the *Add to Group* actions are enabled in the *Primary Classification* policy, and use the Policy Manager to stop the *Asset Classification* policy.

Using an Action to Assign a Classification

You can use the *Classify* actions to override an endpoint classification property set by an *Asset Classification* or *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 will be added to the appropriate group.

It is useful to manually assign a classification in the following situations:

- The classification resolved by CounterACT is not correct or CounterACT was not able to resolve a classification.
- You are able to refine the device's classification. For example, CounterACT 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.

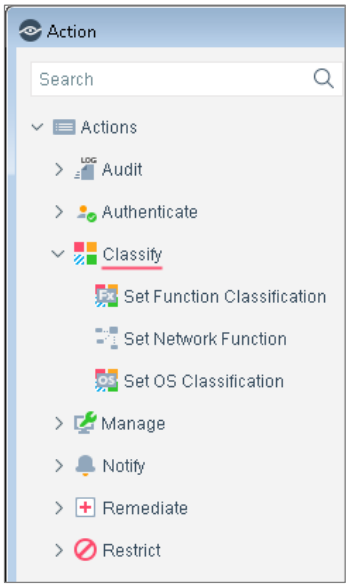
You can use the Cancel Actions action to easily revert your manual classification assignments to those set by your classification policy.

When using a Primary Classification policy to add endpoints to groups, the *Set Network Function* action is not relevant. After a *Set Function Classification* or *Set OS 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 will be added to the appropriate group.

When using an Asset Classification policy and not a Primary Classification policy, run the *Set Network Function* action as needed. The *Set Function Classification* and *Set OS Classification* actions are not relevant.

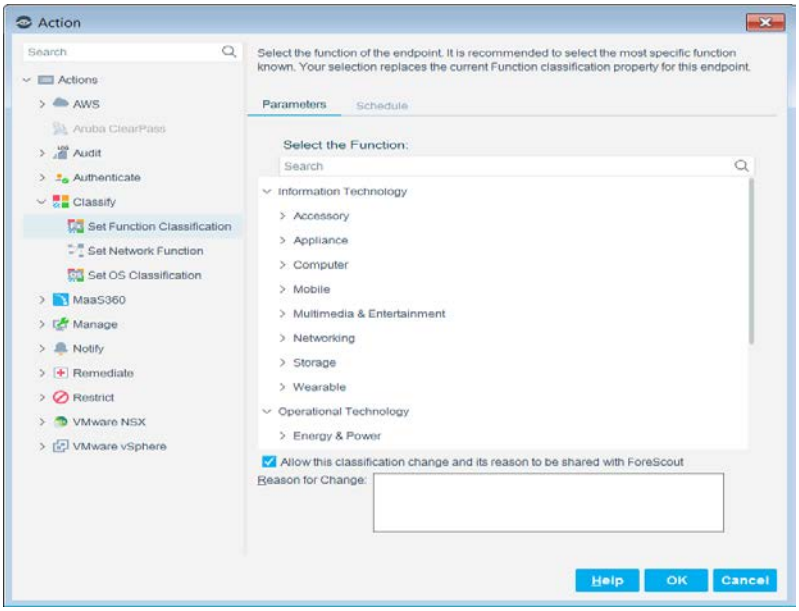
To use CounterACT actions to classify devices:

1. 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.



Classify, Actions

2. Expand the Classify folder, and select the classification property to be set:
   - Set Function Classification
   - Set Network Function
   - Set OS Classification



Classify Device by Function

3. Select the appropriate property value.
4. If you have opted in to data sharing, the classification change will be uploaded to ForeScout. If you agree to also provide ForeScout with additional information regarding 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

   The feedback that you enter in the field will be sent to ForeScout to help provide better classification services.

   This feature is enabled for Function and OS Classifications only. To ensure that your changes are shared with ForeScout, first go to Tools > Options > Advanced > Data Sharing, and select ***Allow selected endpoint properties to be shared with ForeScout****. See The ForeScout Research and Intelligent Analytics Program.*
5. Select **OK**.

Fine-Tuning the Classification Mechanism

Several methods for retrieving classification information are used; for example, Nmap tools, domain credentials, information resolved on devices managed by SecureConnector, or switches configured to work with CounterACT. Nmap tools are used if other mechanisms could not resolve the endpoint classification.

You can fine-tune the Nmap classification, if required.

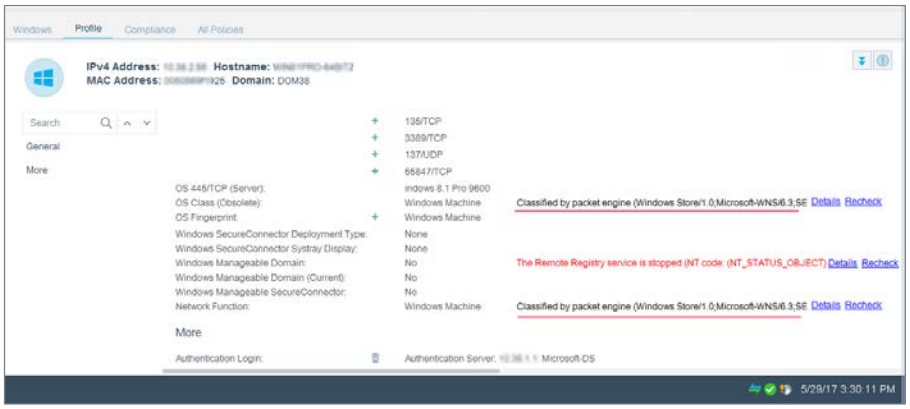
You can prevent Nmap fingerprinting of endpoints that are sensitive to network traffic. See Restricting Endpoint Inspection.

To fine-tune Nmap classification:

1. Select **Options** from the **Tools** menu and then select **HPS Inspection Engine**.
2. Select the Classification tab.
3. Update Nmap settings as required.
4. Select **Apply**.
5. Refer to the *HPS Inspection Engine Configuration Guide* for details about these options. In the HPS Inspection Engine pane, select **Help**.

Troubleshooting Tip

To view the classification method used by CounterACT to resolve the *Network Function* properties, select the **Show troubleshooting messages** icon in the Profile tab of the Details pane.



Classification Type

Classification Upgrade Impact Analysis Template

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 CounterACT. 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 CounterACT Classification tools, including changes in how endpoints are handled by Asset Classification policies.

When Should You Use This Template

When you change the set of classification methods used by CounterACT, 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 CounterACT from Classification version 2 to Classification version 3.

Before you change the Classification version, it is highly recommended to follow this procedure:

1. Create and run a policy based on this template. This policy detects endpoints for which the new and old classification methods yield different results.
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.

How to Proceed

To compare the classification results and perform the upgrade, perform the following in the order specified:

1. How Devices Are Classified and Compared – Policy Condition
2. Compare Classification Results
3. Using an Action to Assign a Classification
4. Stop the Migration Classification Policy
5. Upgrade the Classification Version

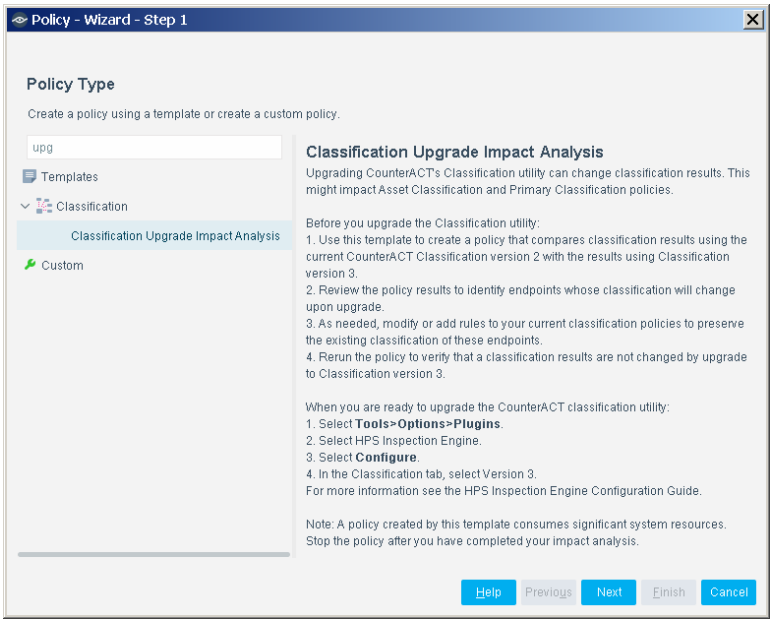
Prerequisites

- Classification version 2 is currently configured.
- Consider which endpoints you want to inspect. The policy does not handle endpoints outside of the Internal Network.

Using the Classification Upgrade Impact Analysis Template

This section describes how to use the template to create a policy.

1. Select **Add** from the Policy Manager.
2. Open the Classification folder.
3. Select **Classification Upgrade Impact Analysis**.

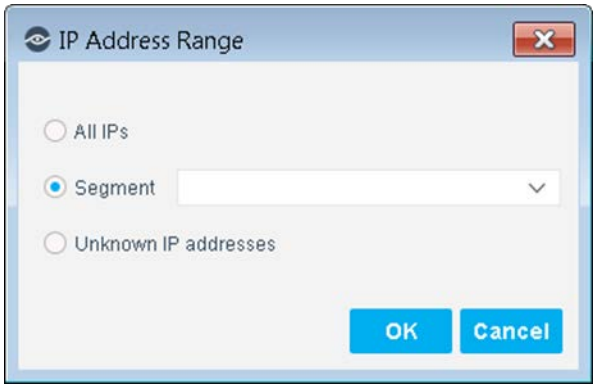


Policy Wizard – Classification Upgrade Impact Analysis

4. Select **Next**. The Name page opens.
5. Edit the default name if required and add a description. See Naming Tips for guidelines about creating effective names.
6. Select **Next**. The Scope page opens. Define which endpoints are inspected.

Which Devices Are Inspected – Policy Scope

1. Use The IP Address Range dialog box to define which endpoints are inspected.

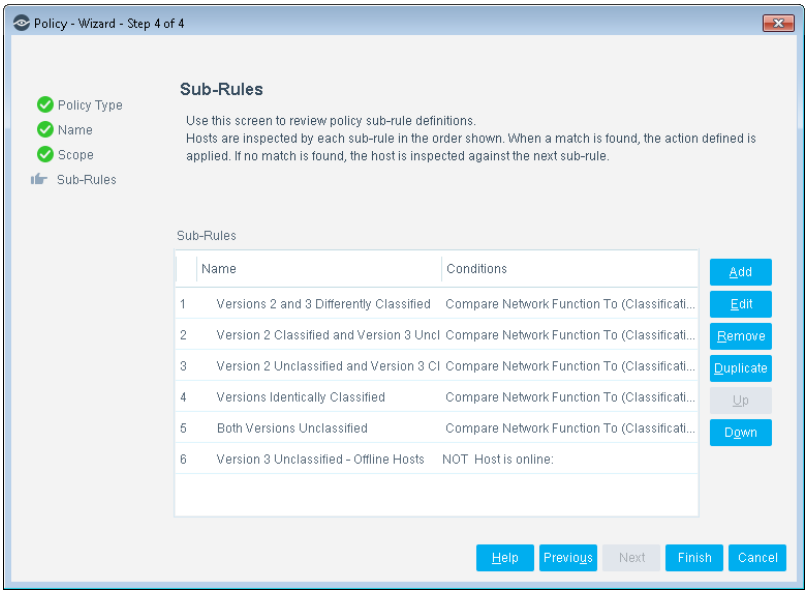


The following options are available:

– **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 select **Segments** from the Scope page.
– **Unknown IP addresses**: Apply the policy to endpoints whose IP addresses are not known. Endpoint detection is based on the endpoint MAC address.

The **Unknown IP addresses** option is not applicable to this template. This policy is applicable only to endpoints with IP addresses.

2. Select **OK**. The added range appears in the Scope list, and is inspected by the policy.
3. To filter the specified ranges or add exceptions, select (**Advanced**).
4. Select **Next**. The Sub-Rules page opens. This page lets you review the sub-rules predefined with this policy.



Classification Upgrade Impact Analysis, Sub-Rules

How Devices Are Classified and Compared – Policy Condition

You can learn more about how the classification comparison is carried out by viewing policy *conditions*.

To view policy conditions:

1. Select an item from the Sub-Rules page.
2. Select **Edit**.

   The Sub-Rules dialog box opens for the condition that you selected.
3. Select a criterion from the **Condition** section and select **Edit**. The dialog box for the condition opens, displaying the parameters.

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 an asset classification, if required. See Using an Action to Assign a Classification. This is optional.

Sub-Rule Result	Description
Version 2 Classified and Version 3 Unclassified	CounterACT did not classify the asset using classification version 3. These assets were previously classified using version 2. Manually assign an asset classification if the number of unclassified devices is minimal. See Using 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	CounterACT 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	CounterACT did not classify the asset in either version. Manually assign an asset classification if the number of unclassified devices is minimal. See Using 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	CounterACT classified the assets in version 2. In version 3, they are unclassified because the assets are offline.

4. Close the Sub-Rule dialog boxes and return to the wizard.
5. Select **Finish**.

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 asset 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 Using an Action to Assign a Classification.

Stop the Migration Classification Policy

The Classification Upgrade Impact Analysis policy utilizes 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.

To stop the policy:

1. Select the Classification Upgrade Impact Analysis policy from the Policy Manager.
2. Select **Stop**.

Upgrade the Classification Version

You are ready to upgrade the Classification tools used by CounterACT 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 Using 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. In the HPS Inspection Engine pane, select **Help**.

Mobile Classification Template

This section covers:

- About the Mobile Classification Template
- Prerequisites
- Using the Mobile Classification Template
- Which Devices Are Inspected – Policy Scope
- How Mobile Devices Are Detected – Policy Condition
- How CounterACT Handles Discovered Devices – Policy Actions
- Manually Assigning a Classification

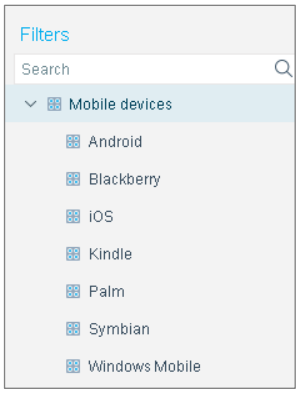
About the Mobile Classification Template

This template creates a policy that classifies devices in the Mobile asset group into the following mobile device type sub-groups:

- iOS
- Kindle Fire
- Android

- Kindle
- Windows Mobile
- Blackberry
- Symbian
- Palm
- Other

These sub-groups automatically appear under the Mobile devices group in the Filters pane>Groups. When you select a sub-group, its members appear in the Detections pane, where you can view information about them.



Mobile Device Classification into Groups

Prerequisites

Use the Mobile Classification policy template in environments running an Asset Classification policy.

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 the Asset Classification policy template before running this policy template. This is required because the Asset Classification policy creates device groups, including the *Mobile* 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.

Using the Mobile Classification Template

This section describes how to use the template to create a policy.

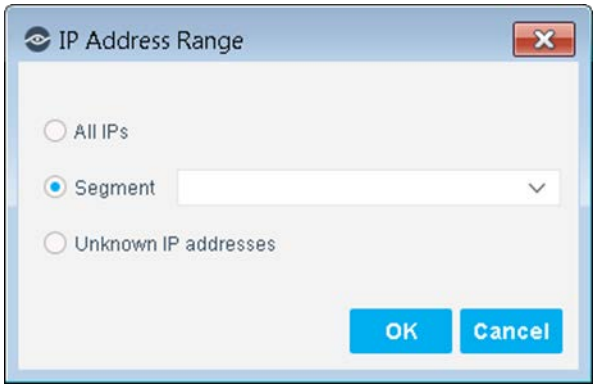
To use the template:

1. Select **Add** from the Policy Manager.
2. Open the Classification folder.

3. Select **Mobile Classification**.
4. Select **Next**. The Name page opens.
5. A default policy name appears in the **Name** field. Accept the default name or create a new name and add a description. See Naming Tips for guidelines about creating effective names.
6. Select **Next**. The Scope page opens.

Which Devices Are Inspected – Policy Scope

1. Use The IP Address Range dialog box to define which endpoints are inspected.



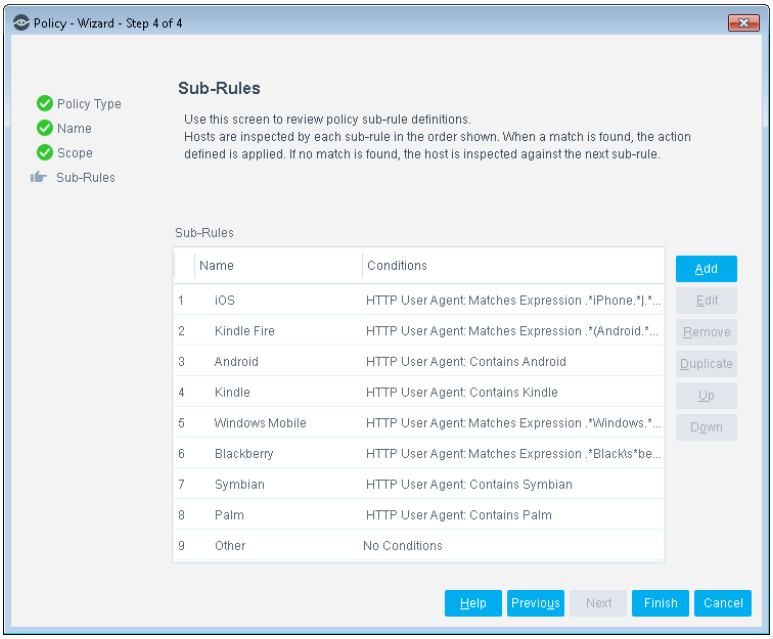
The following options are available:

– **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 select **Segments** from the Scope page.
– **Unknown IP addresses**: Apply the policy to endpoints whose IP addresses are not known. Endpoint detection is based on the endpoint MAC address.

2. Select **OK**. The added range appears in the Scope page.
3. To filter the specified ranges or add exceptions, select (**Advanced**).
4. Select **Next**. The Sub-Rules page opens.

How Mobile Devices Are Detected – Policy Condition

1. The Sub-Rules page lets you review the conditions and actions used to classify mobile devices.



Mobile Classification, Sub-rules

CounterACT classifies mobile devices by using the classification techniques described below. If none of the techniques are successful the device will be classified as Unclassified:

- HTTP User Agent: Requires packet engine and CounterACT version 2 classification.
- Passive banners: Requires engine server banner traffic and CounterACT Classification version 2.
- Active banners: Requires server banner traffic and CounterACT Classification version 2.
- Passive TCP/IP fingerprint: Requires a unique device fingerprint
- Nmap banners: Requires that endpoint to have accessible services with unique banners (not available in Android devices)
- Active TCP/IP fingerprint (Nmap): Requires that the device replies to network traffic requests, and requires a unique Nmap fingerprint
- Open ports: Only available for iPhone, iPad and iPod

To ensure that all mobile devices are identified, you may need to refine the conditions in the Mobile Classification template or the Asset Classification template as follows:

- By default, CounterACT must detect HTTP traffic (browsing) on the device to classify it. Alternatively, you can add the NIC Vendor condition to device sub-rules, with the names of mobile NIC vendors. The devices are detected based on the vendor name, without the need to wait for browsing.
- Mobile devices are detected when the access point is configured as a bridge. By default, the template does not detect mobile devices when their access point is configured as a gateway or router. You can use the Device is NAT condition to detect mobile devices that use gateway or router access points.

2. Select **Finish**. The policy is listed in the Policy Manager.
3. Select the policy and select **Apply**. CounterACT will now detect mobile assets in the specified scope, and add them to their appropriate group in the **Home view**, Filters pane.

How CounterACT Handles Discovered Devices – Policy Actions

Policy *actions* instruct CounterACT how to respond to device detections.

By default, the policy creates CounterACT sub-groups according to the mobile device categories. This action is enabled by default.

When Are Endpoints Removed from Groups?

Endpoints are removed from groups if CounterACT discovers, during policy recheck, that the device function or type has changed.

Manually Assigning a Classification

You can use the *Classify* actions to classify network devices manually. You may need to do this if devices were not properly classified by the Mobile Classification template or if you would like to reclassify them.

External Device Classification Template

This section covers:

- About the External Device Classification Template
- Prerequisites
- Using the External Device Classification Template
- Which Devices Are Inspected – Policy Scope
- When Are Endpoints Removed from Groups
- How CounterACT Handles Discovered Devices – Policy Actions

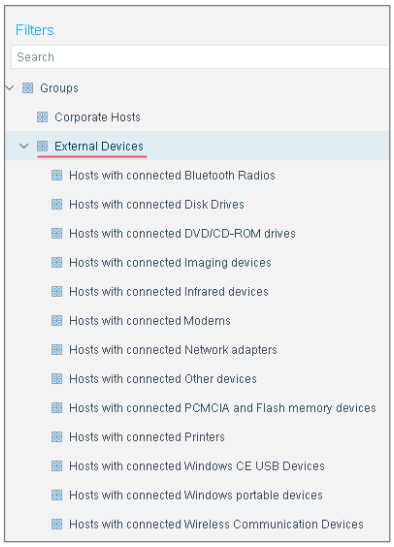
About the External Device Classification Template

This template creates a policy that detects external devices connected to Windows endpoints. The policy creates a CounterACT External Devices group that includes a sub-group for each external device class that you instruct CounterACT to detect. The following device classes can be detected:

- Wireless communication devices
- Windows portable devices
- Windows CE USB devices
- Printers
- PCMIA and flash memory devices

- Other devices
- Network adapters
- Modems
- Infrared devices
- Imaging devices
- Disk drives
- DVD/CD-ROM drives
- Bluetooth radios

These sub-groups automatically appear under the Groups tree in the Console, Filters pane. When you select a sub-group, associated endpoints appear in the Console, Detections pane, where you can view information about endpoints that have connected to these devices.



External Device Classification, Groups

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 CounterACT 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.

Using the External Device Classification Template

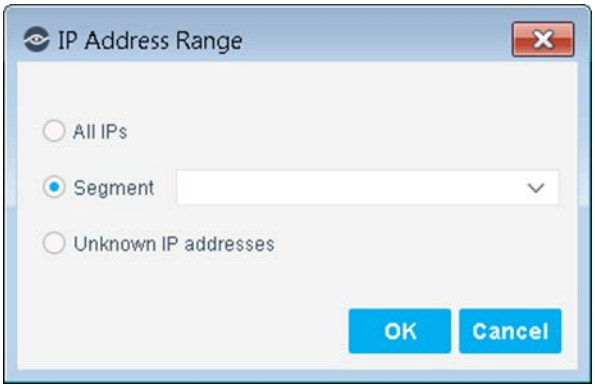
This section describes how to use the template to create a policy.

To use the template:

1. Select **Add** from the Policy Manager.
2. Open the Classification folder.
3. Select **External Device Classification**.
4. Select **Next**. The Scope page opens. Use this page to define which endpoints are inspected.

Which Devices Are Inspected – Policy Scope

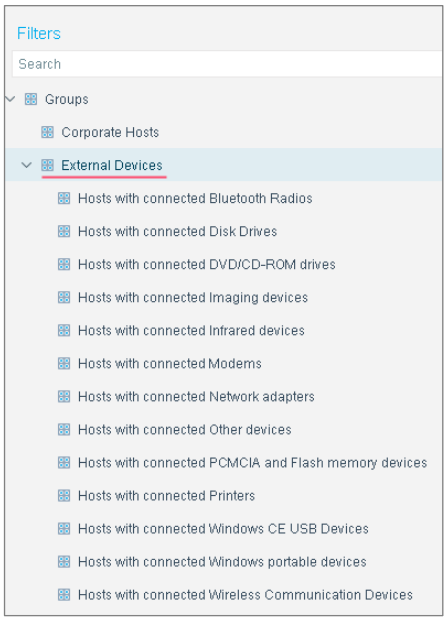
1. Use The IP Address Range dialog box to define which endpoints are inspected.



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 select **Segments** from the Scope page.
– **Unknown IP addresses**: Apply the policy to endpoints whose IP addresses are not known. Endpoint detection is based on the endpoint MAC address.

2. Select **OK**. The added range appears in the Scope page.
3. To filter the specified ranges or add exceptions, select (**Advanced**).
4. Select **Next**. The External Device Classification page opens. This page lets you select the types of external devices for which you want to create policies.



External Device Classification, Device Types

5. Select **Next** and then **Finish**.

When Are Endpoints Removed from Groups?

Endpoints are removed from groups if CounterACT discovers, during policy recheck, that the device function or type has changed. See Updating a Recheck Policy for Unmatched and Matched Endpoints.

How CounterACT Handles Discovered Devices – Policy Actions

Policy *actions* instruct CounterACT how to respond to device detections.

By default, devices that are discovered are added to a sub-group named by device types. This action is enabled by default.

Virtual Machine Classification Template

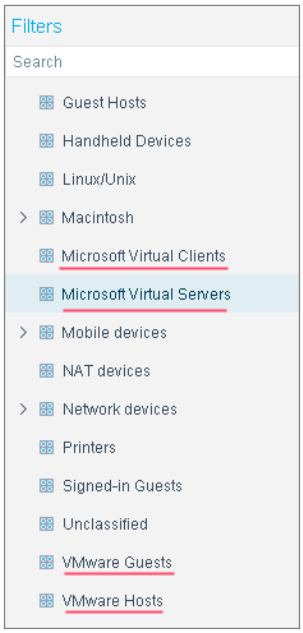
This section covers:

- About the Virtual Machine Template
- Using the Virtual Machine Template
- Which Endpoints Are Inspected – Policy Scope
- How Virtual Machines Are Detected – Policy Condition
- How Virtual Machines Are Handled – Policy Actions

About the Virtual Machine 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.



Virtual Machine Classification, Groups

Using the Virtual Machine Template

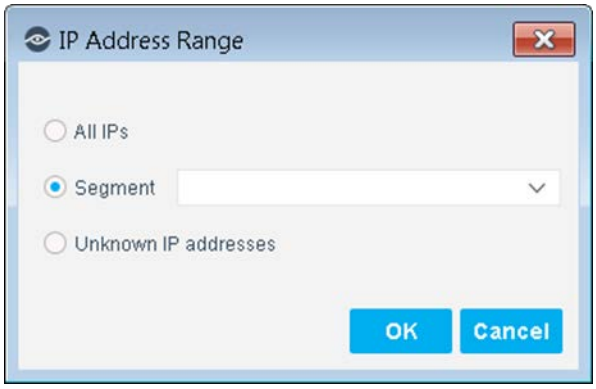
This section describes how to use the template to create a policy.

To use the template:

1. Select **Add** from the Policy Manager.
2. Open the Classification folder.
3. Select **Virtual Machine Classification**.
4. Select **Next**. The Name page opens.
5. Edit the folder name that is used for saving policies for virtual machines that you select, and add a description. See Naming Tips for guidelines about creating effective names.
6. Select **Next**. The Scope page opens. Use this page to define which endpoints are inspected.

Which Devices Are Inspected – Policy Scope

1. Use The IP Address Range dialog box to define which endpoints are inspected.



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 select **Segments** from the Scope page.
– **Unknown IP addresses**: Apply the policy to endpoints whose IP addresses are not known. Endpoint detection is based on the endpoint MAC address.

2. Select **OK**. The added range appears in the Scope page.
3. To filter the specified ranges or add exceptions, select (**Advanced**).
4. Select **Next**. The Sub-Rules page opens. This page lets you review sub-rule conditions and actions.

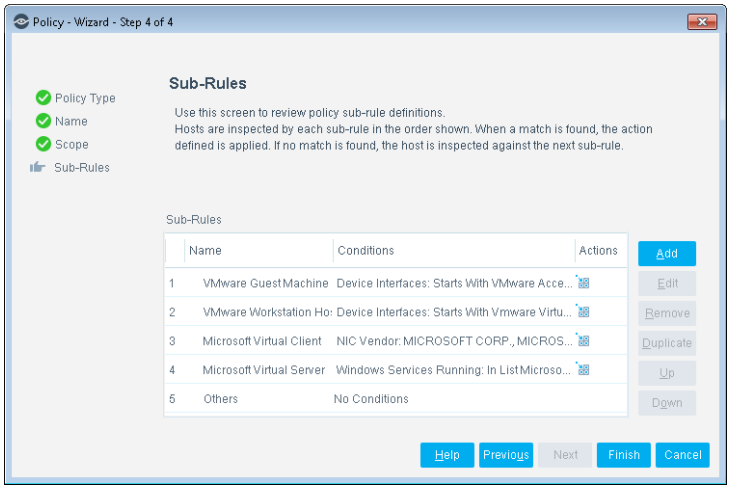
How Virtual Machines Are Detected – Policy Condition

VM activity is detected by CounterACT in a number of 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.

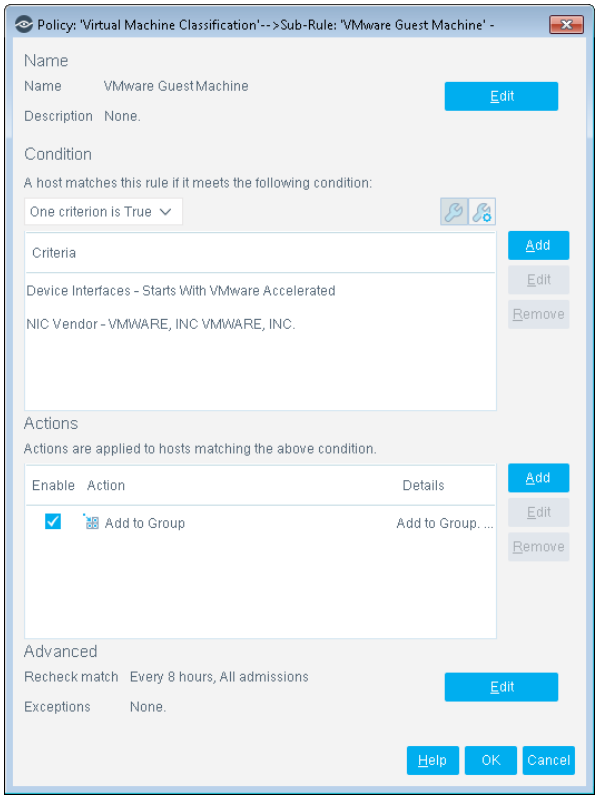
To view and edit conditions:

1. Select a sub-rule in the Sub-Rules page.



Virtual Machine Classification, Sub-Rules

2. Select **Edit** to view the condition and default actions.



Virtual Machine Classification, Criteria

3. Select **OK**. The Sub-Rules page reopens.
4. Select **Finish**.

How Virtual Machines Are Handled – Policy Actions

Policy *actions* instruct CounterACT how to respond to endpoints on which virtual machines have been detected. One action is available by default:

- Detected virtual machines are added to the appropriate Virtual Machine group. This action is enabled by default. Select the checkbox to disable it.

To view this action:

1. Select it from the Sub-Rules page.
2. Select **Edit**. The action definition is displayed.
3. Select the checkbox to enable it and then select **OK**. The Main Rule page appears.
4. Select **Finish**.

Passive Learning Mode Template

Passive Learning mode restricts CounterACT 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.

*If you know ahead of time which devices on your network may be adversely impacted by active probing, assign these endpoints to the **Properties - Passive Learning** group to limit CounterACT's active inspection of them. CounterACT never contacts endpoints in this group to resolve properties, even for policy evaluation. See Restricting Endpoint Inspection for details.*

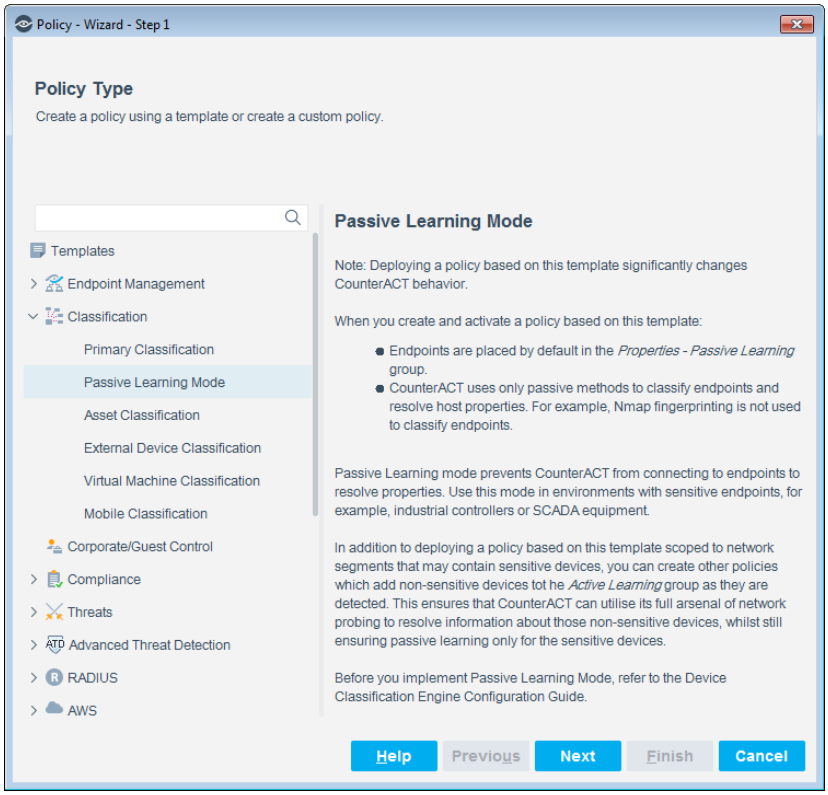
Deploying a policy based on this template significantly changes CounterACT behavior. When you create and activate a policy based on this template:

- Endpoints are placed by default in the **Properties - Passive Learning** group.
- CounterACT 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 template and scoped to network segments that contain sensitive devices, you can create policies which add non-sensitive devices to the **Active Probing - OK** group as they are detected (or add them to the group manually). This allows you to focus Passive Learning on sensitive devices only. The Active Probing - OK group is created and added to the list of CounterACT Groups when you create a new policy using the Passive Learning Mode template.

To use the template:

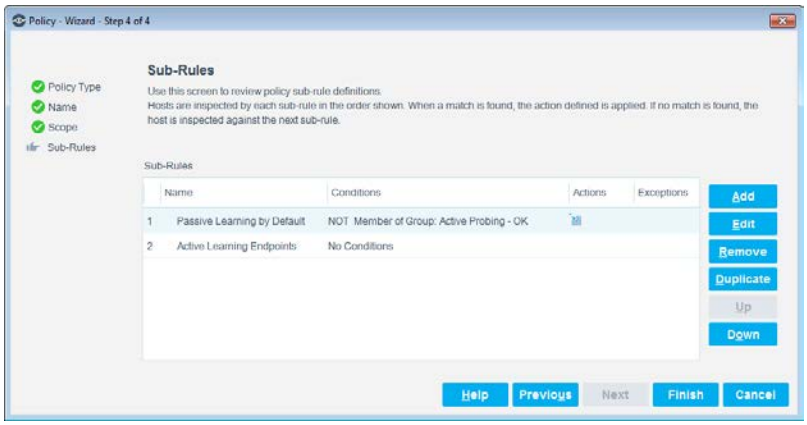
1. Select **Add** from the Policy Manager, and expand the Classification folder.
2. Select **Passive Learning Mode**.



3. The **Passive Learning Mode** template opens.
4. Select **Next**. The Name page opens.
5. Edit the name if required and add a description. See Naming Tips.
6. Select **Next**. The Scope page opens. Use this page define which endpoints are inspected.
7. Select **Next**. The Sub-Rules page opens.

Passive Learning Sub rules

This section describes Passive Learning sub-rules.



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 in CounterACT.

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.

Corporate/Guest Control Template

This section covers:

- About the Corporate/Guest Control Template
- Deploying a Corporate/Guest Control Policy
- Prerequisites
- About Corporate/Guest Classification
- Using the Corporate/Guest Control Policy Template
- Which Devices Are Inspected – Policy Scope
- Handling Guests – Guests Page
- Working with Guest Registration Options
- What Happens When the Authentication Values Are Changed?

About the 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

Deploying a Corporate/Guest Control Policy

Deploy the policy created by this template as follows:

Stage 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 About Corporate/Guest Classification.

Stage 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.

Stage 3

Enable the policy action used to register guests. See Activating the Registration Process.

Stage 4

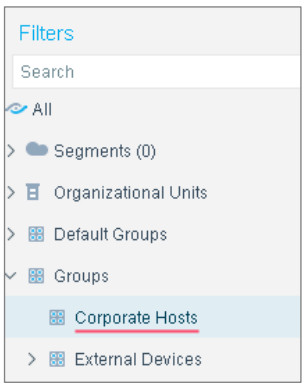
Enable the policy action used to restrict guest access. See Defining Network Access Restrictions to Guest Hosts.

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 the Primary Classification or Asset Classification policy. Verify that you have run and fine-tuned the Primary Classification or Asset Classification policy.
- Verify that the Primary Classification or Asset Classification policy is applied to the network segment or IP address range on which you want to apply the Corporate/Guest Control policy.

About Corporate / Guest Classification

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.



Guest Groups

When you select a group, associated endpoints appear in the Console, Detections pane.

Criteria for Corporate Hosts

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 instructs CounterACT to verify that the endpoint authenticated with an approved authentication server within the last four weeks.

Authentication servers should have been defined during the initial setup. Select **Options** from the **Tools** menu and then select **NAC**>**Authentication**. The authentication servers that appear were defined during the initial setup.

For information about working with the policy when these parameters change see What Happens When the Authentication Values Are Changed?

The Endpoint Is Currently Signed In as a Domain User

This criterion instructs CounterACT to verify that the endpoint is signed in as a domain user.

Signed-In Guests

Hosts that were not categorized as *Corporate Hosts* are evaluated to see if they are *Signed-in Guests*.

This sub-rule instructs CounterACT to evaluate 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

A *Signed-in Guest* is a user who was not authorized to enter the network as a corporate user but later received a valid user name and password. These credentials were successfully used in a Login page when the *Signed-in Guest* attempted to access the Internet.

Criteria for Guest Hosts

Hosts that do not meet the criteria as *Signed-in Guests* are categorized as *Guest Hosts*.

Using the Corporate/Guest Control Policy Template

This section describes how to use the template to create a policy.

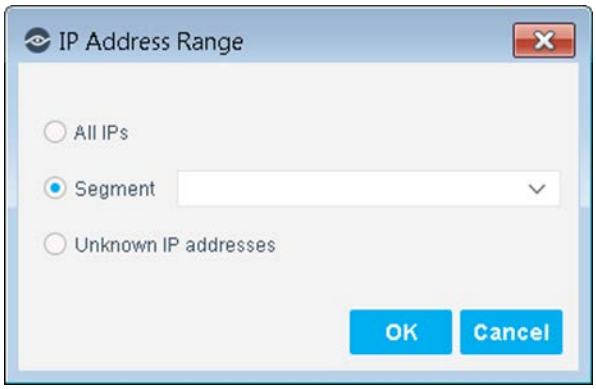
To use the template:

1. Select **Add** from the Policy Manager.
2. Select **Corporate/Guest Control**.
3. Select **Next**. The Name page opens.
4. Edit the name if required and add a description. See Naming Tips.

5. Select **Next**. The Scope page opens. Use this page define which endpoints are inspected.

Which Devices Are Inspected – Policy Scope

1. Use The IP Address Range dialog box to define which endpoints are inspected.



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 select **Segments** from the Scope page.
– **Unknown IP addresses**: Apply the policy to endpoints whose IP addresses are not known. Endpoint detection is based on the endpoint MAC address.

2. Select **OK**. The added range appears in the Scope page.
3. To filter the specified ranges or add exceptions, select (**Advanced**).
4. Select **OK** and then select **Next**. The Guests page opens.

Handling Guests – Guests Page

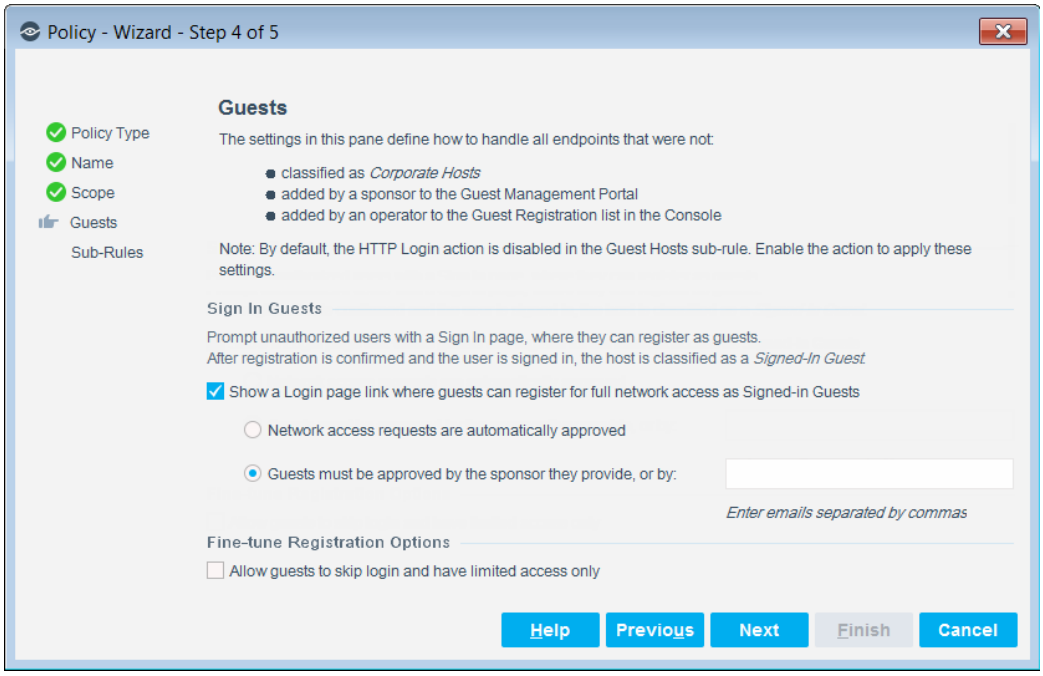
Endpoints that do not meet the criteria as *Corporate Hosts* or *Signed-in Guests* are classified as *Guest Hosts*, and users at these endpoints are called *guests*. These may include, for example, visiting professionals, contractors or university students, or corporate members using personal devices that are not currently known to CounterACT.

Use the options here to define how you want to handle guests. *These options are disabled by default*. The template is set up this way so that you can first review endpoint classification, perform fine-tuning, and then enable sub-rule actions to easily activate a registration process that meets your corporate needs.

Select the **Show a Login page link where guests can register for full network access as Signed-in Guests** checkbox to require unauthorized users not yet registered as guests to request network access using the *Guest Registration form* in a web browser. CounterACT can share the registration information submitted by the guest with designated corporate contacts, called *sponsors*, who can be designated by

the guest. If the checkbox is cleared, guest registration must be initiated by a sponsor in the Guest Management Portal or by a CounterACT operator in the Guest Registration Pane. See Pre-Registration and Guest Registration Management.

Sponsor email addresses must be included in the Guest Registration, Sponsors tab. For more information about sponsors, see Sponsors.



Corporate / Guest Control, Guest

The following are examples of ways to handle unauthorized users:

- ***Network access requests are automatically approved***

  Allow users to enter identity information on a Guest Registration form in a web browser and then receive login credentials. To use this option, select **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 Working with Guest Registration Options for details.

- ***Pre-approve guests using the Guest Management Portal***

  Users designated as corporate sponsors in the Console Guest Registration settings can add guests to the Guest Management Portal. These guests are automatically approved, and login credentials are emailed to them. To use this option, select **Guests must be approved by the sponsor...**, and clear **Allow guests to skip login and have limited access only**. Refer to the *Guest Management Portal for Sponsors How-to Guide* for information about adding guests. See Additional CounterACT Documentation for information on how to access this guide.

- ***Pre-approve guests in the Console***

Operators can define identity information and login credentials for guests at the Console. When these guests log in to your network, the credentials they submit are checked against the credentials that the operator defined. It is the responsibility of your organization to forward the credentials to the guests. CounterACT does not do this for you. To use this option, clear **Allow guests to skip login and have limited access only**. See Adding Guests Using the Console for information about manually adding guests.

- ***Let guests skip the both the registration and the login process***

  All unauthenticated users are able to enter the network with limited access. There are no login requirements for limited access. To use this option, clear **Show a Login page link where guests can register for full network access as Signed-in Guests**, and select **Allow guests to skip login and have limited access only**.

- ***Let users sign in with credentials, without registration***

  Force users to sign in with valid credentials, with no option to register as a guest. Until they sign in, users at these endpoints will not able to enter the network at all. 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**.

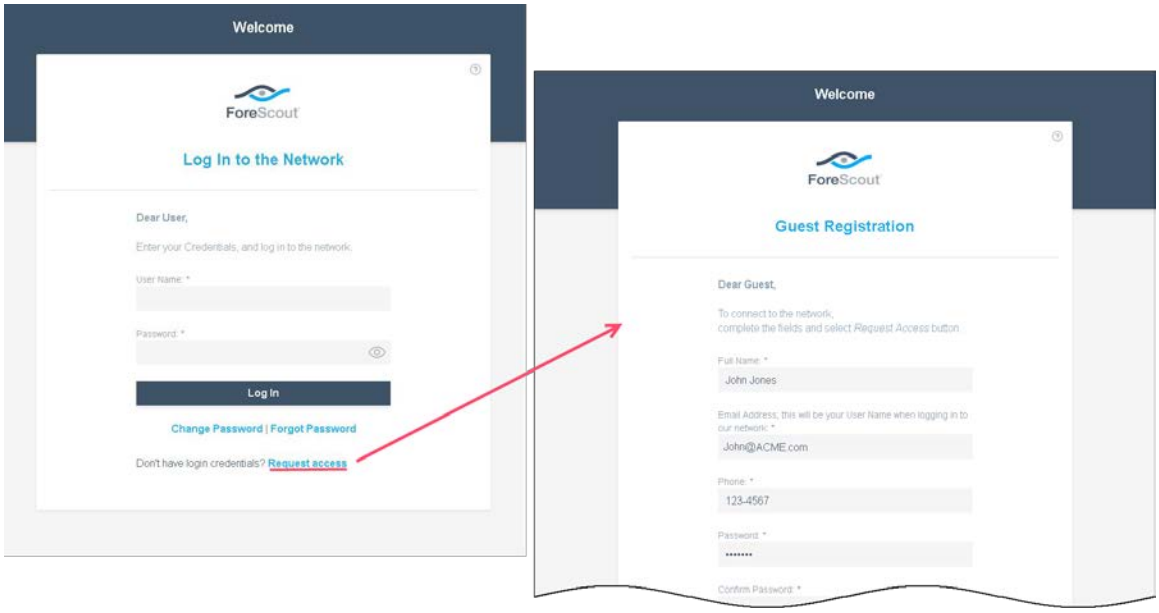
- ***Let users enter the network with limited access***

  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 Signed-in Guests** and select **Allow guests to skip login and have limited access only**. See Defining Network Access Restrictions to Guest Hosts.

Working with Guest Registration Options

This section provides information about the guest registration options and about activating the guest registration process. The process should be activated after you have run the policy template and approved the groups generated by the Corporate/Guest Control policy.

When guest registration is enabled, unauthorized users are prompted to either sign in 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. 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.



Login Page and Guest Registration Form

Automatically approve guest registrations

For guests to be automatically approved after completing the Guest Registration form, select **Network access requests are automatically approved** in the Guests page of the policy wizard. 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. Guests fill out a registration form with identity information, including an email address. 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 CounterACT operator in the Guest Registration Pane. See Pre-Registration and Guest Registration Management. Guests log in using their email address as their user name, together with a password that 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. 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 that is automatically generated by CounterACT. When guests log in to the network, their credentials are checked against the credentials that were approved. 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 CounterACT operator in the Guest Registration Pane. See Pre-Registration and Guest Registration Management.

Activating the Registration Process

By default, the HTTP Login policy action used to activate the Guest Registration form and other web pages or emails used for the guest registration process is disabled. This means that if you choose to enable guest registration from the policy template, you still must activate the registration process from the policy sub-rule.

The template is designed this way so that you can run the policy once to get a sense of how your endpoints are classified, fine-tune the policy, and then activate the corporate log in and guest registration process.

To activate this process:

1. Right-click the **Guest Hosts** sub-rule for this policy from the Policy Manager.
2. Select **Quick Edit**.
3. Select **Actions** and enable the *HTTP Login* action.
4. Select **OK** and then **Apply**.

Defining Network Access Restrictions to Guest Hosts

After you have run the policy, classified your endpoints and registered them, you can assign access restrictions to unauthorized endpoints. Two options are available to restrict guest access from this template. These options are disabled by default.

- *Assign to VLAN* action: Move guest hosts to a predefined VLAN from which network access can be restricted. A Guest VLAN must be included in the IP address range defined for this policy. The VLAN must be defined on all switches on which guest hosts can be found.
- *Virtual Firewall* action: Block guests from your network.

What Happens When the Authentication Values Are Changed?

If authentication values are changed after running the template, the policy values must be updated manually. Specifically, parameters defined in the template are not linked to authentication settings. You can update policy credentials via a property *List* – an editable list of these credentials that is automatically generated with the template.

External Disk Drive Compliance Template

This section covers:

- About the External Disk Drive Compliance Template
- Prerequisites
- Using the External Disk Drive Compliance Template
- Which Endpoints Are Inspected – Policy Scope
- Detecting Authorized External Disk Drives
- Detecting External Disk Drives – Policy Sub-Rules
- Handling Noncompliant External Disk Drives – Policy Actions

About the External Disk Drive Compliance Template

This template lets you analyze the compliance level at your network for external disk drives connected to Windows endpoints. The policy categorizes endpoints with

connected drives into compliant and noncompliant CounterACT 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

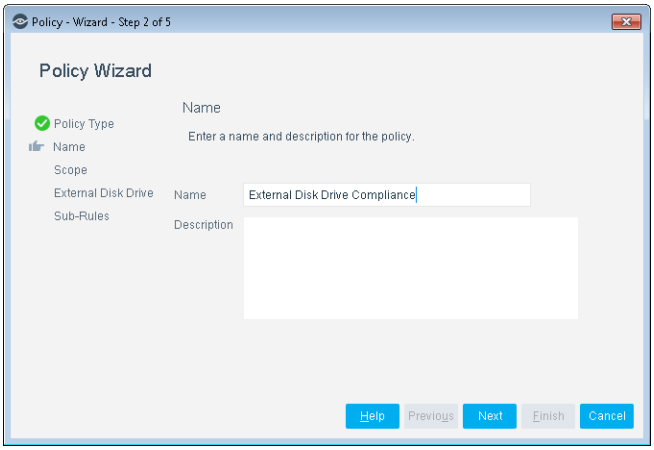
- Consider which endpoints you want to inspect. CounterACT does not handle endpoints outside the Internal Network.
- Verify that you have run and fine-tuned policies created from a Primary Classification or Asset Classification template, and a Corporate/Guest Control template. The External Disk Drive 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 Windows Group Policy to allow access from all CounterACT Appliances to port 445/TCP on domain endpoint devices.

Using the External Disk Drive Compliance Template

This section describes how to use the template to create a policy.

To use the template:

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**. The Name page opens.

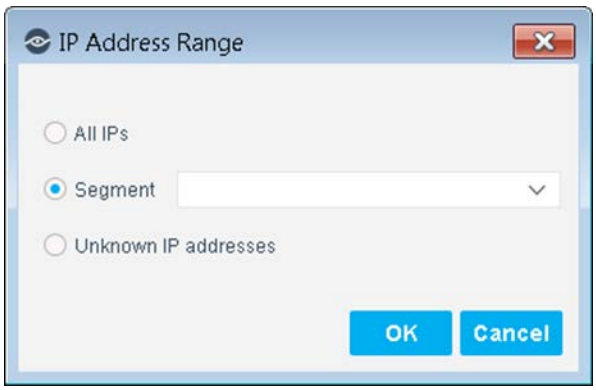


External Disk Drive Compliance, Policy Name

6. Edit the name, and if required add a description. See Naming Tips for guidelines about creating effective names.
7. Select **Next**. The Scope page appears. Use this page to determine which endpoints are inspected by the policy.

Which Endpoints Are Inspected – Policy Scope

1. Use The IP Address Range dialog box to define which endpoints are inspected.



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 select **Segments** from the Scope page.
– **Unknown IP addresses**: Apply the policy to endpoints whose IP addresses are not known. Endpoint detection is based on the endpoint MAC address.

2. Select **OK**. The added range appears in the Scope page.
3. To filter the specified ranges or add exceptions, select (**Advanced**).
4. Select **Next**. The External Disk Drive page opens. This page lets you define which external disk drives are acceptable.

Detecting Authorized External Disk Drives

You instruct CounterACT which external disk drives are authorized by applying a user-defined whitelist of authorized external disk drives to the policy. Endpoints using these drives are placed in the *Hosts with compliant Disk Drives* group.

Endpoints not using these drives are placed in the *Hosts with noncompliant Disk Drives* group.

The list is based on external device disk IDs group.

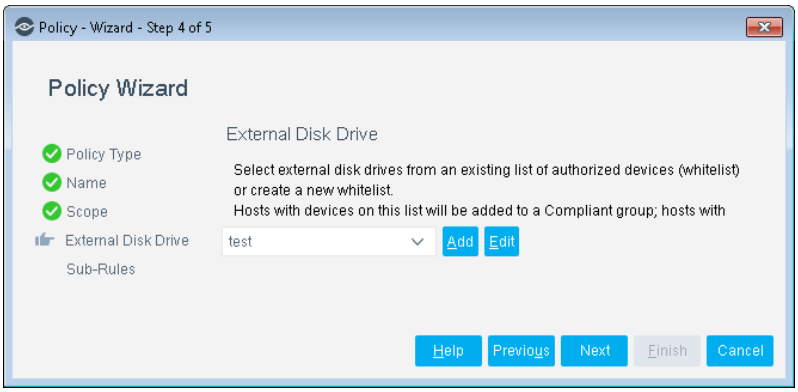
Lists are created from the Asset Inventory or by using the List option. See Working with Asset Inventory Detections and Defining and Managing Lists for details.

If no list exists, the wizard lets you create one here. It is important to note that the device ID name entered must exactly match the actual name of the device ID, including character spacing, and is case-sensitive.

You can create an empty list and add compliant ID numbers later.

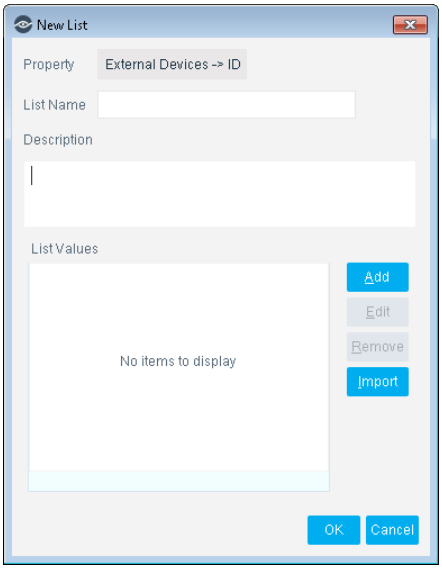
To select or create a whitelist:

1. If you are using an existing whitelist, select it from the drop-down list.



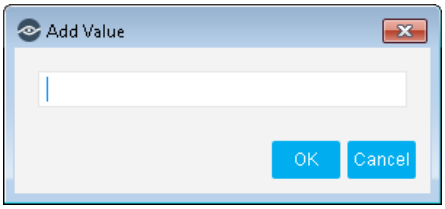
External Disk Drive Compliance, Whitelist

2. To create a new List, select **Add**. The New List dialog box opens.



External Disk Drive Compliance, Whitelist – Add Value List

3. The property displayed is *External Devices>ID*. This instructs CounterACT to looks for external disk drives based in their ID number. Type a list name; for example, *Authorized External Disk Drives*.
4. Select **Add**. The Add Value dialog box opens.

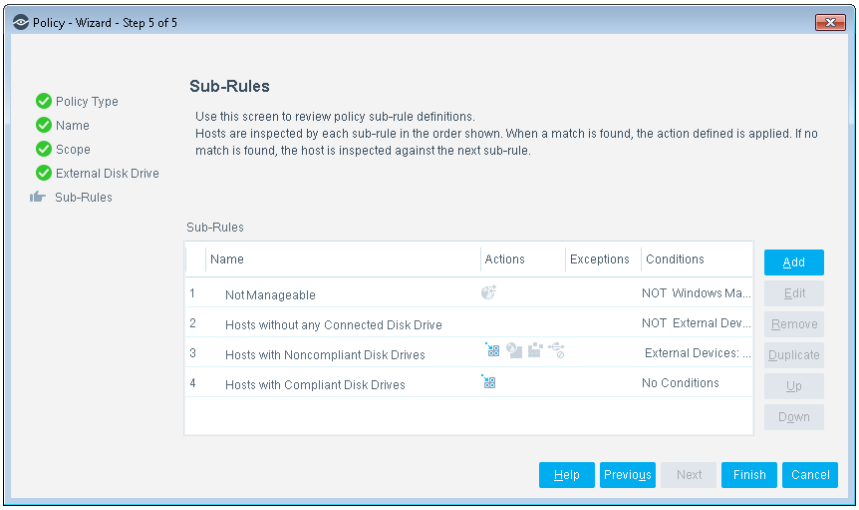


External Disk Drive Compliance, Whitelist – Add Value

5. Enter the authorized external disk drive ID. It is important to type the exact device ID. This ID is what CounterACT detects when an external device is connected to an endpoint.
6. Select **OK**. The added value is displayed on the New List dialog box.
7. Select **Next**. The Sub-Rules page opens.

Detecting External Disk Drives – Policy Sub-Rules

The policy finds endpoints that have external disk drives connected whether compliant or noncompliant. You can view the sub-rules used by the policy.



External Disk Drive Compliance, Sub-Rules

To view sub-rules:

1. Select a sub-rule and then select **Edit**.
2. View the sub-rule details and select **OK**.

Handling Noncompliant External Disk Drives – Policy Actions

Policy *actions* instruct CounterACT how to respond to endpoints that have noncompliant disk drives connected.

- *Add to Group*: Noncompliant disk drives are added to a group called **Hosts with noncompliant Disk Drives**, a subgroup of the **Hosts with connected Disk Drives** group under **External Devices**. This action is enabled by default.

- *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.

To view these actions:

1. Select Sub-Rule 3, **Hosts with Noncompliant Disk Drives**, from the Sub-Rules dialog box.
2. Select **Edit**.
3. Review the actions in the **Actions** section.
4. Select **OK**. The Sub-Rules page appears.
5. Select **Finish**.

When an external device is detected by CounterACT, 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 section covers:

- About the Overall Endpoint Compliance Template
- Prerequisites
- Using the Overall Endpoint Compliance Template
- Which Endpoints Are Inspected – Policy Scope
- Required and Restricted Applications Pages
- Detecting Compliance Status – Policy Condition
- How CounterACT Handles Noncompliant Devices – Policy Actions
- Compliance Notification at Endpoint

About the 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 CounterACT 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.

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. CounterACT does not handle endpoints outside the Internal Network.
- Verify that you have run and fine-tuned policies created from a Primary Classification or Asset 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.
- 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 CounterACT Appliances to port 445/TCP on domain endpoint devices.

Using the Overall Endpoint Compliance Template

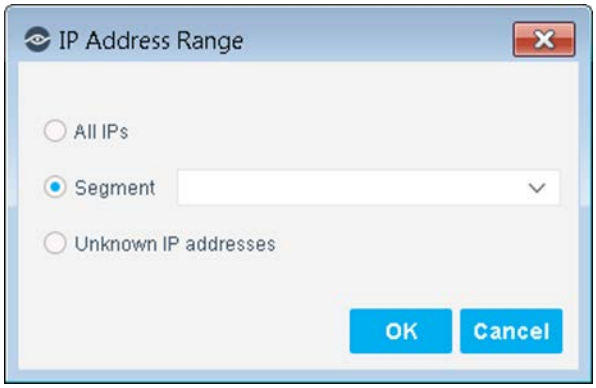
This section describes how to use the template to create a policy.

To use the template:

1. Select **Add** from the Policy Manager.
2. Select the Compliance folder.
3. Select the **Overall Endpoint Compliance** template.
4. Select **Next**. The Scope page opens. Use the page to define which endpoints are inspected.

Which Endpoints Are Inspected – Policy Scope

1. Use The IP Address Range dialog box to define which endpoints are inspected.



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 select **Segments** from the Scope page.
- **Unknown IP addresses**: Apply the policy to endpoints whose IP addresses are not known. Endpoint detection is based on the endpoint MAC address.

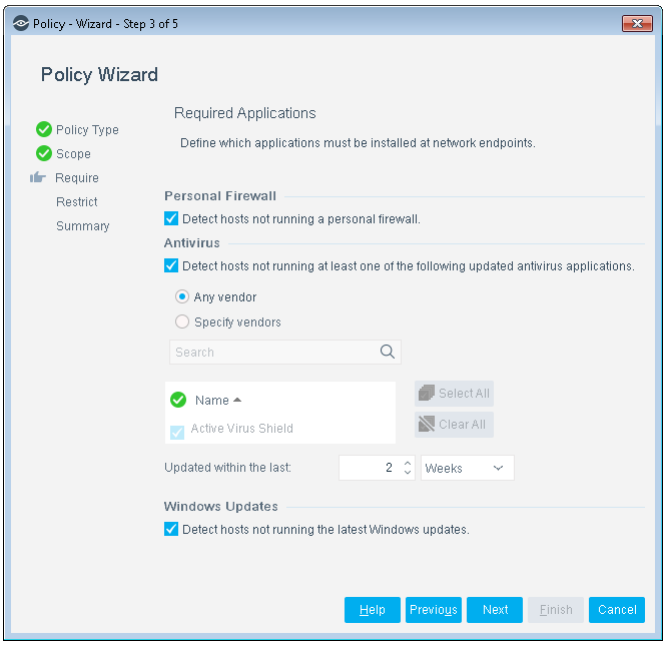
2. Select **OK**. The added range appears in the Scope page.
3. To filter the specified ranges or add exceptions, select (**Advanced**).
4. Select **Next**. The Required Applications page opens.

Required and Restricted Applications Pages

The Required/Restricted Applications pages display the compliance tests that you can perform.

Required Applications

Define which applications must be installed at endpoints.

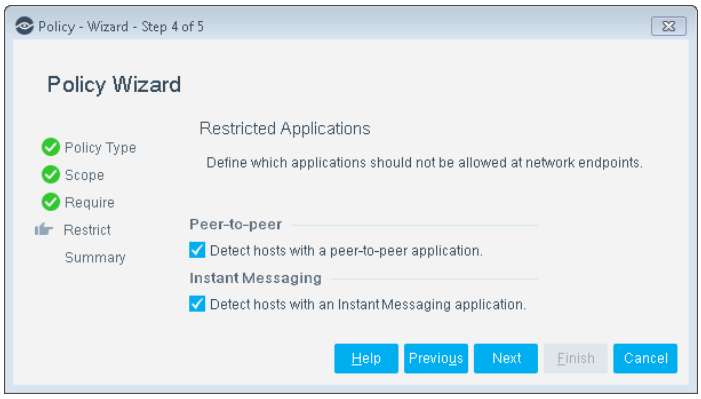


Overall Endpoint Compliance, Required Applications

- Verify that a personal firewall is running.
- Verify that at least one antivirus application is running and has been updated within the past two weeks. Select the antivirus vendors that you want the policy to find.
- Verify that the endpoint is patched with the most current Microsoft published vulnerability updates.

Restricted Applications

Define which applications should not be allowed at endpoints.



Overall Endpoint Compliance, Restricted Applications

- Verify that no peer-to-peer application is installed on the endpoint.
- Verify that no instant messaging application is installed on the endpoint.

To define tests:

1. Select the tests that you want to perform.
2. Select **Next**. The Summary page opens. It displays the list of policies that have been set using the Overall Endpoint Compliance template.

Overall Endpoint Compliance, Summary

Detecting Compliance Status – Policy Condition

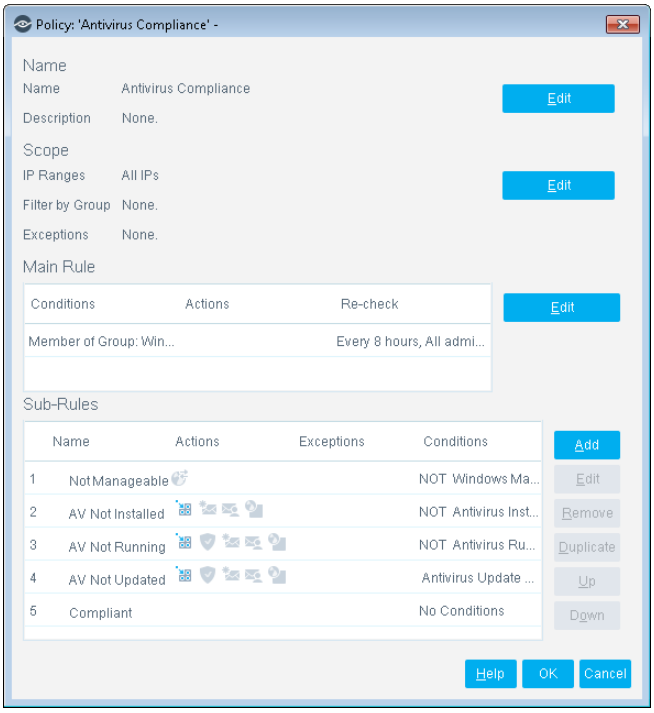
Inspection Sequence

Endpoints are inspected in the order shown in the dialog box. Select the compliance tests that you want to perform. When the policy verifies that an endpoint meets a compliance requirement, that endpoint is moved to the next compliance test. For example, if CounterACT discovers that the antivirus installed is compliant, the

endpoint is next checked for personal firewall compliance. If compliance is not met, inspection is halted and the endpoint is placed in a noncompliant group.

To change the order:

1. Select a compliance test and then select **Edit**. The Compliance dialog box opens for the test that you have selected.



Antivirus Compliance, Sub-Rules

2. Use the **Up** and **Down** buttons to change the endpoint inspection order.

Before Inspection

Before inspecting endpoints defined in the Scope page, the policy verifies that CounterACT can perform deep inspection. This means that either:

- CounterACT can access the endpoint via TCP ports 139/445 and is able to inspect it using domain credentials. When this happens, the endpoint is *manageable (domain)*. Unmanageable endpoints are usually foreign to the domain.
- The endpoint is accessible to CounterACT via *SecureConnector*. SecureConnector is a lightweight, small-footprint executable that runs at the endpoint so that CounterACT can inspect it. SecureConnector opens an encrypted tunnel to CounterACT, allowing remote endpoint inspection; similar to how a domain member endpoint would be inspected. Endpoint users at unmanageable endpoints can be prompted via a template *action* to run SecureConnector and allow deep inspection, i.e. become manageable.

Corporate windows endpoints that are not manageable are displayed as *matched* for the *Not manageable* sub-rule.

To view this condition:

1. Select the **Not Manageable** sub-rule from the Sub-Rules page.
2. Select **Edit**.
3. Select the **NOT Manageable (Domain)** or the **NOT Windows Manageable (SecureConnector)** criterion from the **Condition** section of the Sub-Rules dialog box that opens.
4. Select **Edit**. The condition values appear.

To view or enable the SecureConnector action:

1. Select the **Not Manageable** sub-rule from the Sub-Rules page.
2. Select **Edit**.
3. From the **Actions** section, select **Start SecureConnector**.
4. Select **Edit**. The action definition is displayed. Review the information about SecureConnector if needed.
5. Select **OK**.
6. Select **Enable** from the **Actions** section to run SecureConnector on unmanageable endpoints.

Inspection Details

Sub-rule *conditions* criteria define how CounterACT detects endpoint compliance status.

- The policy finds endpoints that are not running one of the personal firewalls listed in the page. For example:
  - ZoneAlarm
  - Windows Firewall
  - Symantec Firewall
  - Sygate
  - Sophos Firewall
  - McAfee Personal Firewall
  - Internet Connection Firewall (ICF)

  See the Personal Firewall property for more information. Additional applications may become recognizable in between version updates. These changes are documented in the *Windows Applications Content Module Release Notes*. Refer to the *Windows Applications Configuration Guide* for more information about the module. Select **Options** from the **Tools** menu. Select **Modules**. Select **Windows Applications** and then select **Help**.
- The policy finds endpoints that have NOT installed any of the antivirus applications selected in the Compliance page. See the Antivirus Installed property for more information.
- The policy finds endpoints that have installed required antivirus applications, but are NOT running them. See the Antivirus Running property for more information about the detection mechanism.

- The policy finds endpoints that are running out-of-date antivirus applications. By default, antivirus applications should be updated every two weeks. If the update is older than this period, the endpoint is considered noncompliant. You can change the update period if required. See the Antivirus Update Date property for more information about the detection mechanism.
- The policy finds endpoints that have not updated with the most current Microsoft published vulnerability patches. See Microsoft Vulnerabilities for more information about the detection mechanism.
- The policy finds endpoints that have installed at least one of the peer-to-peer applications listed in the page. For example:

Shareaza	Twister	LimeWire	FolderShare
iMesh	TrustyFiles	Warez	BitComet
gnutella	Soulseek	Kazaa	BitTorrent
eMule	Morpheus	Jubster	BearShare
FrostWire	MP3 Rocket		

  Additional applications may become recognizable in between version updates. These changes are documented in the *Windows Applications Content Module Release Notes*. Refer to the *Windows Applications Configuration Guide* for more information about the module. Select **Options** from the **Tools** menu. Select **Modules**. Select **Windows Applications** and then select **Help**.

- The policy finds endpoints that have installed at least one of the instant messaging applications listed in the page. For example:

Yahoo! Messenger	MSN Messenger	AOL Instant Messenger
Trillian	ICQ	Camfrog
Skype	Google Talk	PaltalkScene

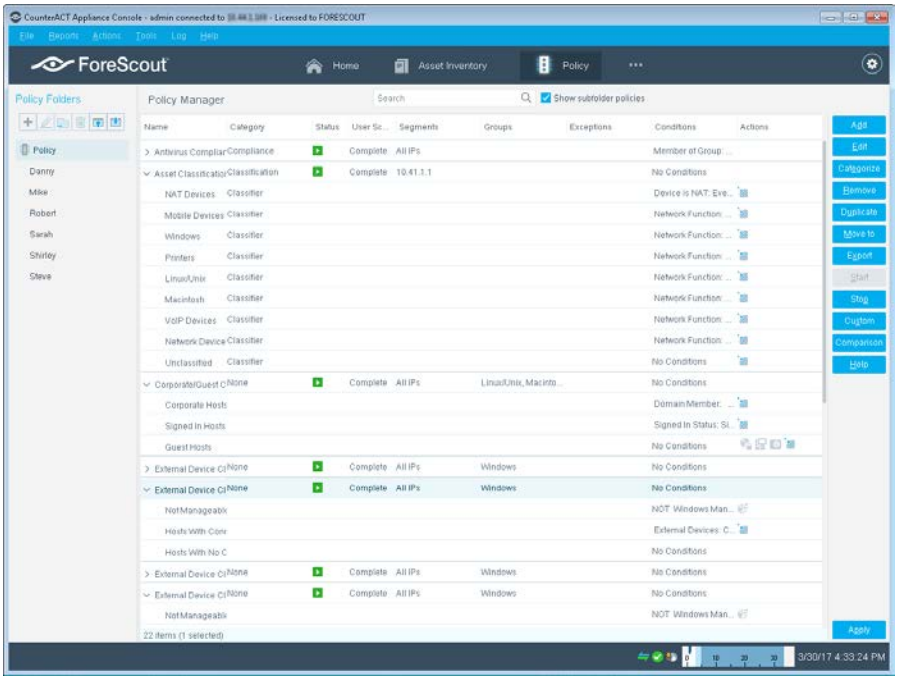
  Additional applications may become recognizable in between version updates. These changes are documented in the *Windows Applications Content Module Release Notes*. Refer to the *Windows Applications Configuration Guide* for more information about the module. Select **Options** from the **Tools** menu. Select **Modules**. Select **Windows Applications** and then select **Help**.

How CounterACT Handles Irresolvable Endpoints

If CounterACT cannot resolve the status of the endpoint, it will not be placed in a relevant compliance group, i.e. **Personal FW Inactive** group. Irresolvable endpoints can be displayed by selecting the policy and selecting **Irresolvable** in the Detections pane. An exception is the Antivirus Update rule, which, if irresolvable, is evaluated by CounterACT as compliant.

How CounterACT Handles Noncompliant Devices – Policy Actions

Template *actions* instruct CounterACT how to respond to endpoints that are not compliant. This template creates separate policies for each endpoint, which are listed one by one in the Policy pane.



Overall Endpoint Compliance, Listings

Antivirus Applications Not Installed, Running or Updated

- The endpoint is added to the appropriate group: *Antivirus Not Installed*, *Antivirus Not Running* or *Antivirus Not Updated*. The action is enabled by default.
- Email notification is sent to the CounterACT operator. The generic messages 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. Users are asked to contact IT and the Helpdesk for instructions. The generic messages can be modified from the template Sub-Rule dialog box. The action is disabled by default.
- Stopped antivirus applications are automatically restarted. The action is disabled by default.

Personal Firewall Not Active

- The endpoint is added to the **Personal FW Inactive** group. The action is enabled by default.
- Email notification is sent to the CounterACT operator. The action is disabled by default.
- Email and web notification are sent to noncompliant users, indicating that their computers are not running the authorized applications. The action is disabled by default.

Peer-to-Peer or Instant Messaging Applications Running

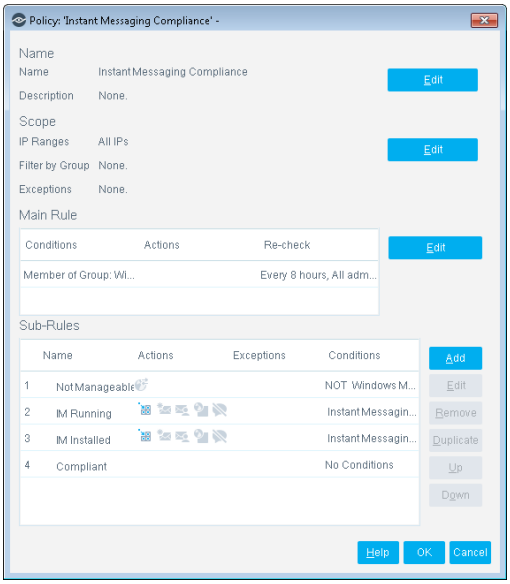
- The endpoint is added to the appropriate group: *P2P Installed*, *P2P Running*, *IM Installed* or *IM Running*. The action is enabled by default.
- Email notification is sent to the CounterACT operator. The action is disabled by default.
- Email and web notification are sent to the noncompliant users, indicating that their computers are not running the authorized applications. Users are asked to contact IT and the Helpdesk for instructions. The action is disabled by default.

Endpoints with Microsoft Vulnerabilities

- The endpoint is added to the **Windows Not Updated** group. This action is enabled by default.
- Two remediation actions are available. These actions are disabled by default. The two are related and should be enabled simultaneously.
- *Automatic Remediation*: This 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. See Start Windows Updates for more information about this action.
- *Self-Remediation*: This action prompts the user to perform remediation. It is scheduled to start one hour after the *Automatic Remediation* action. Only if automatic remediation fails or is taking too long will the self-remediation occur. When using this action, CounterACT 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 accessed in order to patch vulnerabilities. The endpoint cannot access the web until it 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. See Windows Self Remediation for more information about this action.

To view, customize and enable these actions:

1. Select an action from the **Sub-Rules** section of the Compliance page.
2. Select **Edit**.



Instant Messaging Compliance, Sub-Rules

3. From the **Actions** section, select an action and select **Edit**. The action definition is displayed.
4. Select **OK**. The Compliance page reopens.
5. From the **Actions** section, select an action and then select **Enable** to run it.
6. Select **OK**. The Main Rule page reopens.
7. Select **Finish**.

Compliance Notification at Endpoint

If there is noncompliance at the endpoint, CounterACT notifies the user. On the Windows Notification Bar at the bottom of the window, the **CounterACT** icon is displayed in red. Placing the cursor over the icon, the endpoint details are displayed.

Noncompliance Indication

Individual Compliance Templates

You can create individual compliance templates for any of the entries listed in the *Overall Endpoint Compliance* template – including Instant Messaging, Antivirus, Peer-to-Peer and Windows Updates – instead of running the policies together. Refer to the templates located under the Compliance folder for details about each option.

The policies created using the individual compliance templates inspect only Windows machines. To inspect Macintosh machines, use the Macintosh Update Compliance template.

Windows Update Compliance Template

- About Windows Update Compliance Template
- Prerequisites
- Using the Windows Update Compliance Template
- Which Endpoints Are Inspected – Policy Scope
- Detecting Noncompliant Windows Endpoints – Policy Condition
- Handling Windows Hosts – Policy Actions

About Windows Update Compliance Template

This policy allows you to detect hosts that have not updated with the latest Microsoft-published vulnerability patches, and to create 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

- An Asset Classification or Primary Classification policy must have already been run, and a Corporate/Guest Control policy must have already been run. Detected endpoints must already 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 information regarding the SecureConnector connection.

Using the Windows Update Compliance Template

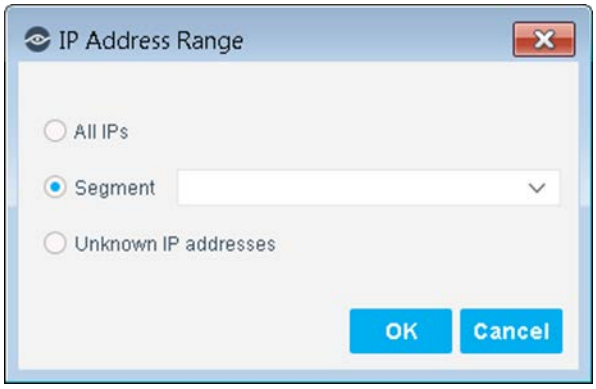
This section describes how to use the template to create a policy.

To use the template:

1. Select **Add** from the Policy Manager.
2. Select the Compliance folder and then select **Windows Update Compliance**.
3. Select **Next**.
4. Edit the name if required and add a description. See Naming Tips for guidelines about creating effective names.
5. Select **Next**. The Scope page opens. Use the page to define which endpoints are inspected.

Which Endpoints Are Inspected – Policy Scope

1. Use The IP Address Range dialog box to define which endpoints are inspected.



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 select **Segments** from the Scope page.
– **Unknown IP addresses**: Apply the policy to endpoints whose IP addresses are not known. Endpoint detection is based on the endpoint MAC address.

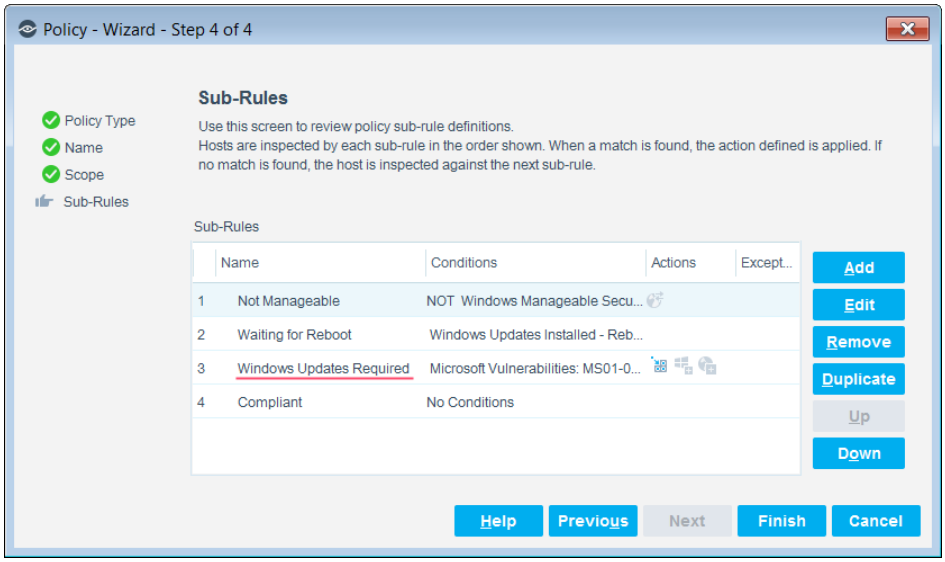
2. Select **OK**. The added range appears in the Scope page.
3. To filter the specified ranges or add exceptions, select (**Advanced**).
4. Select **Next**. The Sub-Rules page opens. This page lets you review policy conditions and actions.

Detecting Noncompliant Windows Endpoints – Policy Condition

The policy finds endpoints that have not been updated with the most current Windows updates. This requires that the endpoint is managed by CounterACT, either via SecureConnector or remotely. Endpoints waiting for a reboot following the installation of a previous patch updated until after the reboot.

To view this condition:

1. Select the **Windows Updates Required** sub-rule from the Sub-Rules page.



Windows Update Compliance, Sub-Rules

2. Select **Edit**.
3. From the **Condition** section of the Sub-Rules dialog box, select **Microsoft Vulnerabilities** and select **Edit** to view the criteria.

Handling Windows Hosts – Policy Actions

Policy *actions* instruct CounterACT how to respond to endpoints that meet certain conditions. You can add additional policy actions as required.

The policy template provides four sub-rules.

- *Not Manageable:* The provided action installs the SecureConnector tool, making the Windows machine manageable by CounterACT. This action is disabled by default.
- *Waiting for Reboot:* The updates successfully downloaded and installed on the Windows machine. CounterACT is now waiting for the endpoint to reboot so as to complete the update process. There are no actions provided by default.
- *Windows Updates Required:* The sub-rule provides three actions.
  - The endpoint is added to the **Windows Not Updated** group for processing. This action is enabled by default.
  - You can Start Windows Updates to update the endpoints. Using this action, you have the option of informing the user that a reboot is required, or forcing the endpoint to reboot automatically. This action is disabled by default.
  - You can run Windows Self Remediation. This action sends the user links to the updates and patches that must be downloaded and installed to correct the 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, nor are any actions performed.

To view or enable these actions:

1. Select a rule from the Sub-Rules page.
2. Select **Edit**.
3. In the **Actions** section, select the action entry, and select **Edit**. The action definition is displayed.
4. Select **OK**. The Sub-Rules page appears.
5. In the **Actions** section, select the action and select **Enable** to run it.
6. Select **OK**.

Macintosh Update Compliance Template

This section covers the following:

- About Macintosh Update Compliance Template
- Prerequisites
- Using the Macintosh Update Compliance Template
- Which Endpoints Are Inspected – Policy Scope
- Detecting Noncompliant Macintosh Endpoints – Policy Condition
- Handling Macintosh Hosts – Policy Actions

About Macintosh Update Compliance Template

This template lets you verify that endpoints have installed the most current Macintosh software updates.

Prerequisites

- An Asset Classification or Primary Classification policy must have already been run, and a Corporate/Guest Control policy must have already been run. 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 information regarding the SecureConnector connection.

Using the Macintosh Update Compliance Template

This section describes how to use the template to create a policy.

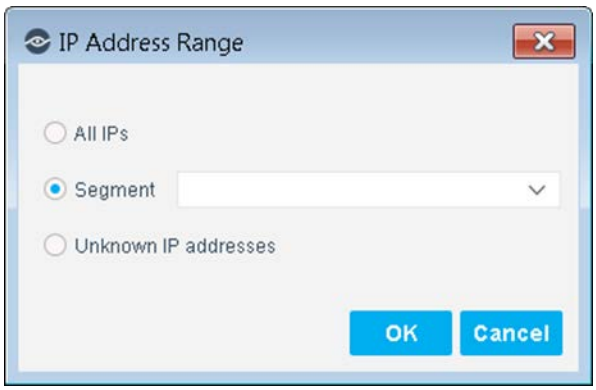
To use the template:

1. Select **Add** from the Policy Manager.
2. Select the Compliance folder and then select **Macintosh Update Compliance**.
3. Select **Next**.

4. Edit the name if required and add a description. See Naming Tips for guidelines about creating effective names.
5. Select **Next**. The Scope page opens. Use the page to define which endpoints are inspected.

Which Endpoints Are Inspected – Policy Scope

1. Use The IP Address Range dialog box to define which endpoints are inspected.



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 select **Segments** from the Scope page.
– **Unknown IP addresses**: Apply the policy to endpoints whose IP addresses are not known. Endpoint detection is based on the endpoint MAC address.

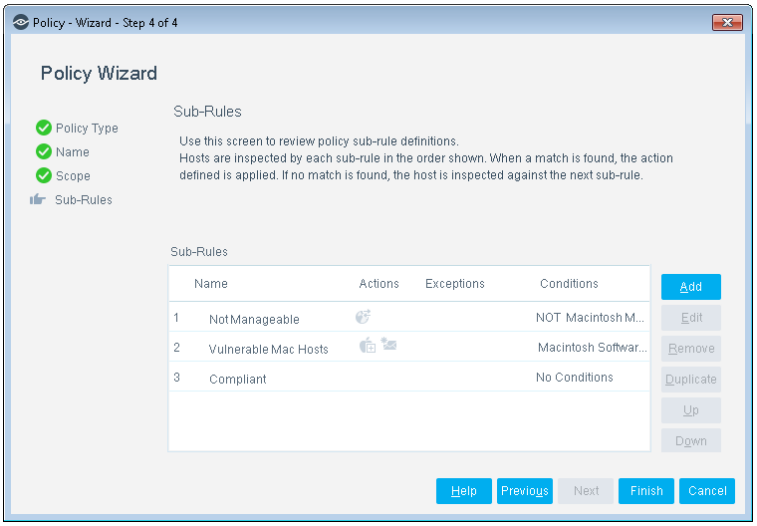
2. Select **OK**. The added range appears in the Scope page.
3. To filter the specified ranges or add exceptions, select (**Advanced**).
4. Select **Next**. The Sub-Rules page opens. This page lets you review policy conditions and actions.

Detecting Noncompliant Macintosh Endpoints – Policy Condition

The policy finds endpoints that have not updated with the most current Macintosh updates. This requires that the endpoint be managed by CounterACT, either via SecureConnector or remotely.

To view this condition:

1. Select rule **2**, **Vulnerable Mac Hosts**, from the Sub-Rules page.



Macintosh Update Compliance, Sub-Rules

2. Select **Edit**.
3. From the **Condition** section of the Sub-Rules dialog box, select **Macintosh Software Updates Missing** and select **Edit** to view the criteria.

Handling Macintosh Hosts – Policy Actions

Policy *actions* instruct CounterACT how to respond to endpoints that are not updated.

- *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.

To view or enable these actions:

1. Select rule **2**, **Vulnerable Mac Hosts**, from the Sub-Rules page.
2. Select **Edit**.
3. In the **Actions** section, select the **Start Macintosh Updates** entry and select **Edit**. The action definition is displayed.
4. Select **OK**. The Sub-Rules page appears.
5. In the **Actions** section, select the action and select **Enable** to run it.
6. Select **OK**.

Threats Templates

This section describes general guidelines for using all of the Threats templates. It covers:

- About the Threats Templates
- Prerequisites

- Using the Threats Templates
- Which Endpoints Are Inspected – Policy Scope
- Malicious Hosts Template
- ARP Spoofing Template
- Impersonation Template
- Dual Homed Template

About the Threats Templates

CounterACT 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 enable you to neutralize malicious threats.

The following Threats templates are available:

- Malicious Hosts Template
- ARP Spoofing Template
- Impersonation Template
- Dual Homed Template

Prerequisites

There are no prerequisites for any of the Threats templates.

Using the Threats Templates

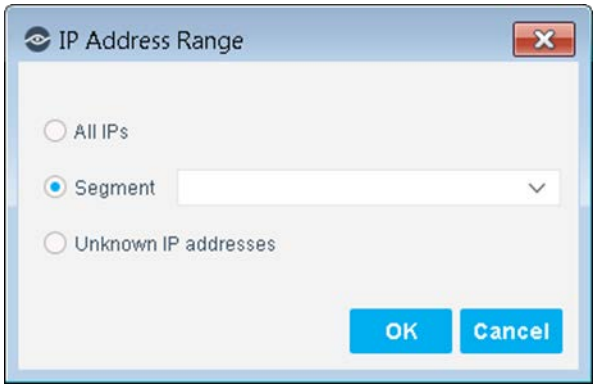
This section describes how to use the template to create a policy.

To run the various templates:

1. Select **Add** from the Policy Manager.
2. Select the Threats folder.
3. Select the appropriate template for the policy that you want to create.
4. Edit the name if required and add a description. See Naming Tips for guidelines about creating effective names.
5. Select **Next**. The Scope page opens. Use this page to define which endpoints are inspected.

Which Endpoints Are Inspected – Policy Scope

1. Use The IP Address Range dialog box to define which endpoints are inspected.



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 select **Segments** from the Scope page.
– **Unknown IP addresses**: Apply the policy to endpoints whose IP addresses are not known. Endpoint detection is based on the endpoint MAC address.

2. Select **OK**. The added range appears in the Scope page.
3. To filter the specified ranges or add exceptions, select (**Advanced**).
4. Select **Next**. Either the Main Rule or Sub-Rules page opens. These pages lets you review policy conditions and actions.

Malicious Hosts Template

This section covers:

- About the Malicious Hosts Template
- How Malicious Hosts Are Detected – Policy Condition
- How Malicious Hosts Are Handled – Policy Actions

About the 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 Malicious Hosts Are Detected – Policy Condition

Malicious endpoint activity is detected using CounterACT's 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 Chapter 12: Threat Protection for more information.

The policy conditions instruct CounterACT to detect a wide range of scan, bite and email anomaly events. If an endpoint has performed one of these events, CounterACT evaluates it as malicious.

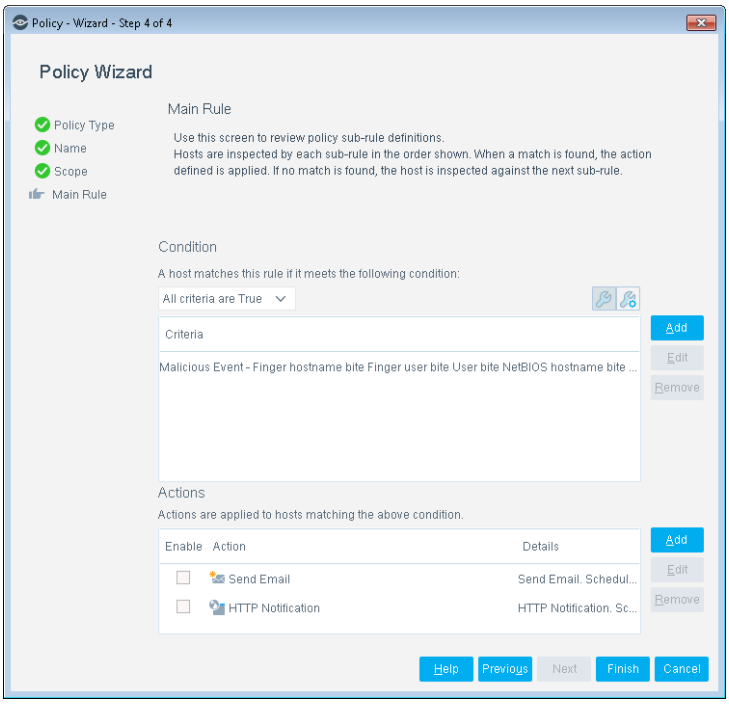
What are these events?

Scan event	A Threat Protection event indicating that an endpoint performed a configurable number of network probes within a certain time period.
Bite event	An event in which a malicious endpoint tries to gain access to the protected network using CounterACT bait.
Email anomaly event	Unusual email activity; for example, endpoints that send more than a certain number of emails within a specified time period. The default is ten mails within one minute.

For more information about these events, see About Threat Protection and Basic Terminology.

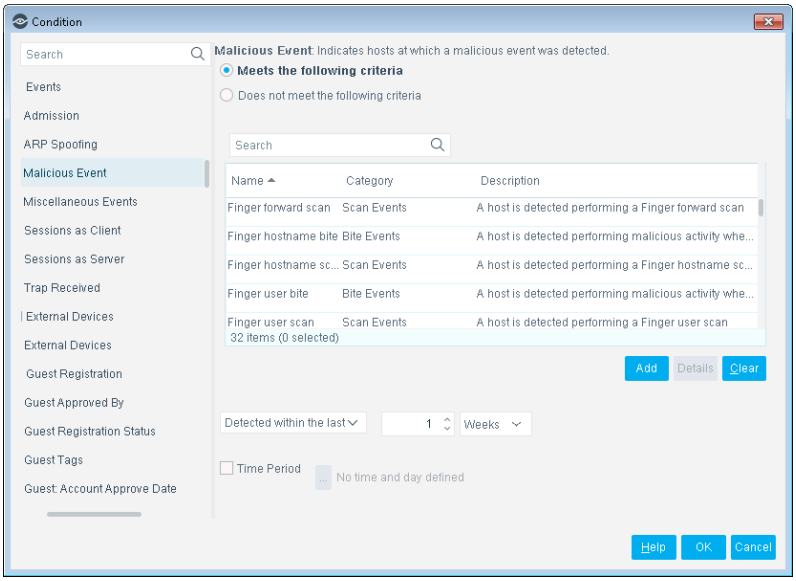
To view conditions:

1. Select the **Malicious Event** entry from the **Condition** section of the Main Rule page.



Malicious Hosts, Main Rule

2. Select **Edit** to review details about the condition.



Malicious Hosts, Main Rule Properties

3. Select **OK**. The Main Rule page reopens.
4. Select **Finish**.

How Malicious Hosts Are Handled – Policy Actions

Template *actions* instruct CounterACT how to respond to endpoints that are malicious.

- *Send Email*: A predefined action lets you send email to the CounterACT administrator indicating that a malicious event was detected at an endpoint. The email provides information about the endpoint; for example, the IP address, the user logged in 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.

To view or enable actions:

1. Select an entry from the **Actions** section of the Main Rule page.
2. Select **Edit**.
3. Review action details.
4. Select **OK**. The Main Rule page reopens.
5. Select an action and then select the associated checkbox to enable it.
6. Select **Finish**.

ARP Spoofing Template

This section covers:

- About the ARP Spoofing Template

- How ARP Spoofing Is Detected – Policy Condition
- How ARP Spoofing Is Handled – Policy Actions

Refer to the *Port Mirroring in CounterACT Technical Note* for more information about configuring your environment for detecting ARP spoofing. See Additional CounterACT Documentation for information on how to access this guide.

About the ARP Spoofing Template

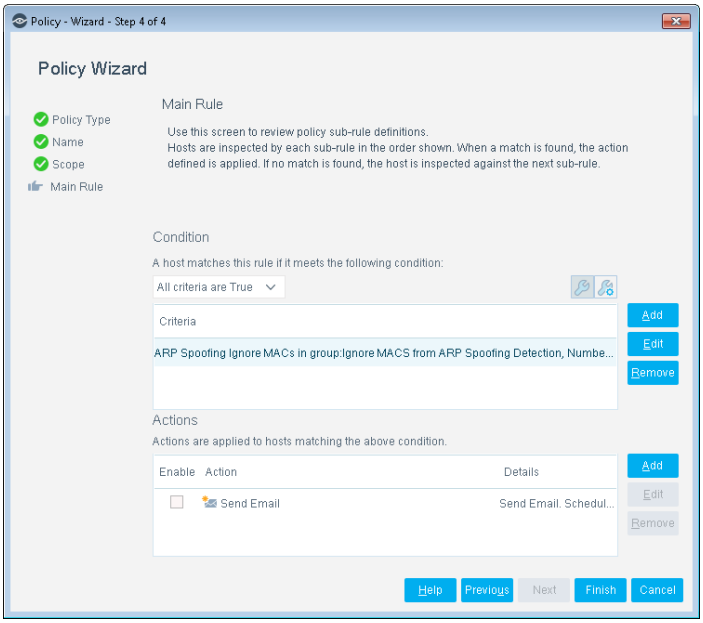
Use this template to create a policy that tracks and remediates attempts to maliciously direct network traffic. ARP spoofing is a technique used to attack an Ethernet network that may allow an attacker to sniff data frames on a Local Area Network (LAN), modify the traffic, or completely halt it. The aim is to associate the attacker's MAC address with the IP address of another node. Any traffic meant for that IP address would be 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.

How ARP Spoofing Is Detected – Policy Condition

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 CounterACT to indicate if the number of different MAC addresses reported for an IP address over a specific time period exceeds a certain limit. You can define the number of MAC address and the time period.

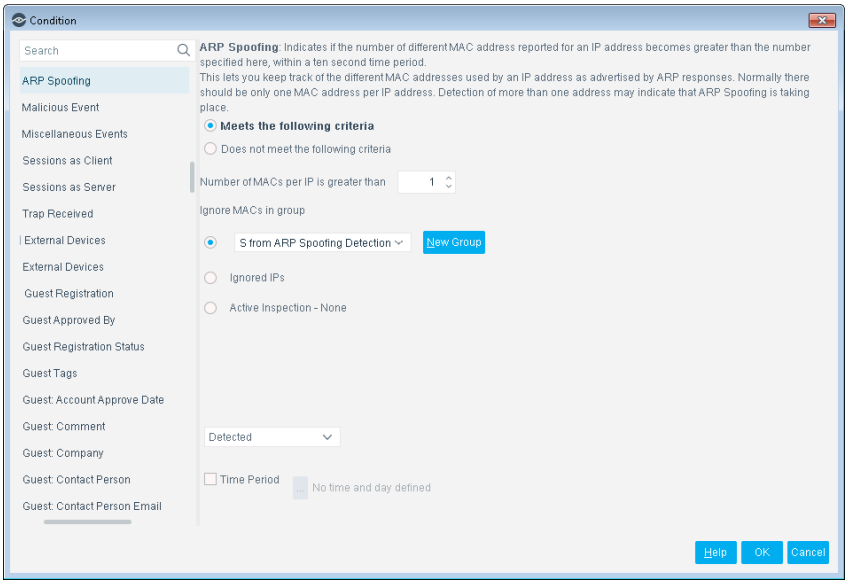
To view conditions:

1. Select the **ARP Spoofing** entry from the **Condition** section of the Main Rule page.



ARP Spoofing, Main Rule

2. Select **Edit** to view the criteria.



ARP Spoofing, Criteria

3. Select **OK**. The Main Rule page reopens.
4. Select **Finish**.

How ARP Spoofing Is Handled – Policy Actions

Template *actions* instruct CounterACT how to respond to endpoints on which ARP Spoofing activities have been detected.

- Send Email: A predefined action lets you send email to the CounterACT 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 user logged in and User Directory information. You must provide an email address recipient. This action is disabled by default.

To view or enable this action:

1. Select it from the **Actions** section of the Main Rule page.
2. Select **Edit**.
3. Review action details.
4. Select **OK**. The Main Rule page reopens.
5. Select the checkbox to enable it and then select **Finish**.

Impersonation Template

This section covers:

- About the Impersonation Template
- How Impersonation Is Detected – Policy Condition
- How Impersonation Is Handled – Policy Actions

About the Impersonation Template

This template allows you to 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.

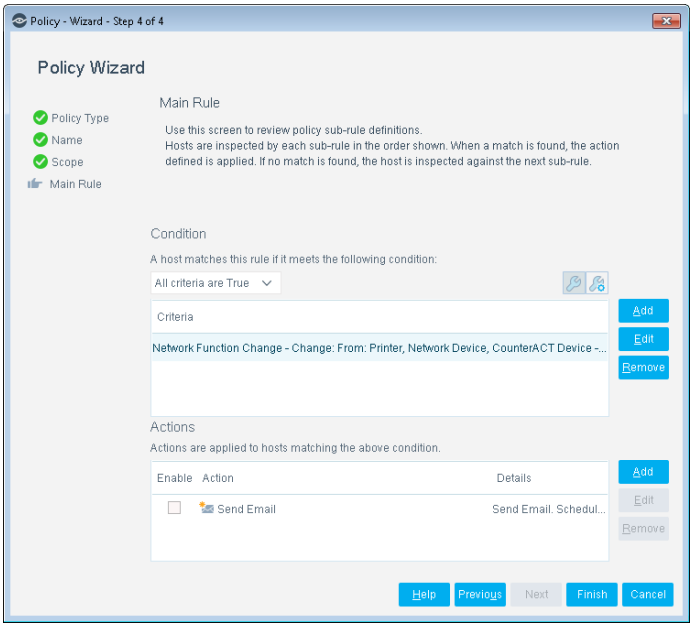
How Impersonation Is Detected – Policy Condition

Impersonation activity is detected by tracking a change in the Nmap-Network function of the endpoint.

The template *conditions* instruct CounterACT to detect a change in the Nmap-Network function of the endpoint as indication of impersonations attempts.

To view and edit the condition:

1. Select the entry from the **Condition** section of the Main Rule page.



Impersonation, Main Rule

2. Select **Edit** to view the criteria.
3. Select **OK**. The Main Rule page reopens.
4. Select **Finish**.

How Impersonation Is Handled – Policy Actions

Template *actions* instruct CounterACT how to respond to endpoints on which impersonation activities have been detected.

- *Send Email*: A predefined action lets you send email to the CounterACT administrator indicating that an impersonation activity was detected at an endpoint. The email provides information about the endpoint; for example, the IP address, the user logged in and User Directory information. You must provide an email address recipient. This action is disabled by default.

To view or enable this action:

1. Select the action from the **Actions** section of the Main Rule page.
2. Select **Edit**.
3. Review action details.
4. Select **OK**. The Main Rule page reopens.
5. Select the checkbox to enable it and then select **Finish**.

Dual Homed Template

This section covers:

- About the Dual Homed Template
- How Dual-Homed Threats Are Detected – Policy Condition
- How Threats to Dual-Homed Hosts Are Handled – Policy Actions

About the 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 to 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 – Policy Condition

Threats from dual-homed endpoints are detected in the following ways:

- SecureConnector Manageable Sub-Rule
- Detect Windows endpoints managed by SecureConnector. These endpoints will have one at least 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. See How Threats to Dual-Homed Hosts Are Handled – Policy Actions.

- Domain Manageable Sub-Rule
- Detect Windows endpoints managed remotely, i.e. if CounterACT 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.

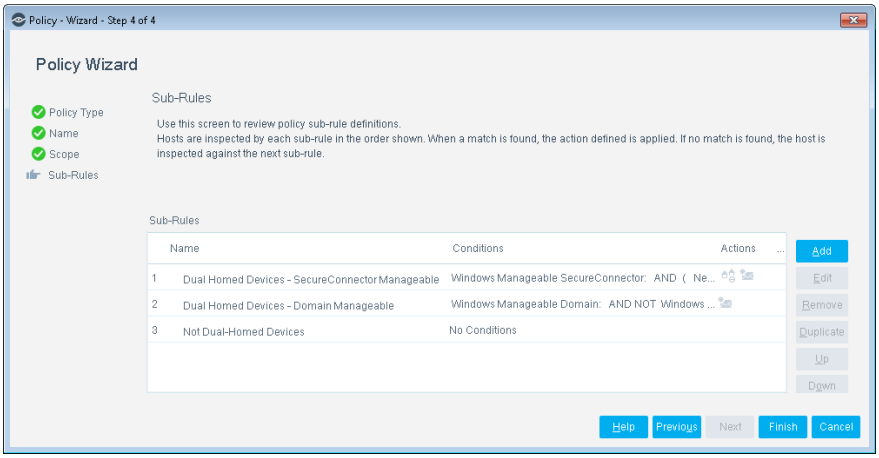
You can fine-tune the template policy by defining the IP addresses that are to be ignored when calculating using the Number of IP Addresses *property. For details see "Tuning" in the* HPS Inspection Engine Configuration Guide*.*

If endpoints meet these criteria they are considered dual-homed. You can manage these endpoints by notifying your IT or Security team. See How Threats to Dual-Homed Hosts Are Handled – Policy Actions.

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 will be automatically detected by the SecureConnector Manageable Sub-Rule.

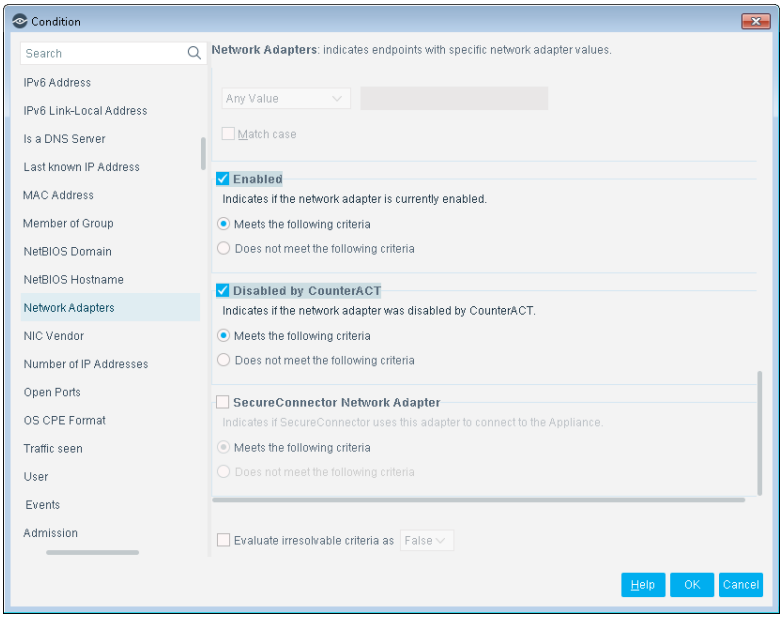
To view and edit conditions:

1. Select a Dual Homed entry from the Sub-Rules page.



Dual Homed, Main Rule

2. Select **Edit** to view the sub-rule and its criteria.



Dual Homed, Criteria

3. Select **OK**. The Sub-Rules Rule page reopens.
4. If required, repeat the previous steps for another Dual Homed entry.
5. Select **Finish**.

How Threats to Dual-Homed Hosts Are Handled – Policy Actions

Template *actions* instruct CounterACT 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 email to the CounterACT 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 user logged in 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 view or enable these actions:

1. Select an action from the **Actions** section of a Sub-Rule page.
2. Select **Edit**.
3. Review action details.
4. Select **OK**. The Sub-Rule page reopens.
5. Select the checkbox to enable it and then select **Finish**.

Track Changes Templates

Track Changes templates help you create policies for monitoring the following changes in your network:

- Application Change
- Hostname Change
- Operating System Change
- Shared Folder Change
- Switch Change
- User Change
- Windows Service Change
- New TCP/IP Port

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.

This section describes the guidelines for using all of the templates except for New TCP/IP Port template. This section covers:

- Prerequisites
- Using the Track Changes Templates
- Which Hosts Are Inspected – Policy Scope
- How Frequently Are Endpoints Inspected – Change Time
- How a Change Is Detected – Policy Condition
- How a Change Is Handled – Policy Actions
- How to Modify a Condition – Advanced Settings

For details about using the New TCP/IP Port template, see About the New TCP/IP Port Template.

Prerequisites

There are no prerequisites for any of the Track Changes templates.

Using the Track Changes Templates

This section describes how to use the template to create a policy.

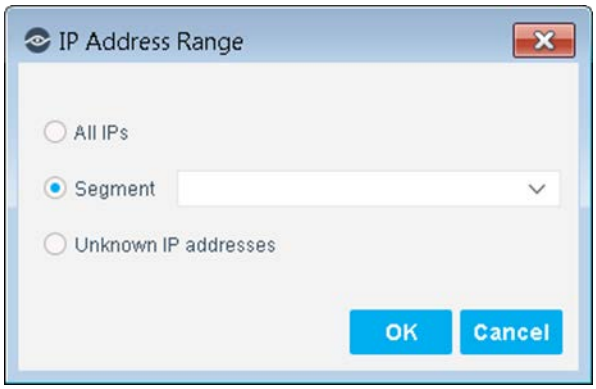
To run the various Track Changes templates:

1. Select **Add** from the Policy Manager.
2. Select the Track Changes folder.
3. Select the appropriate template for the policy that you want to create.

4. Edit the name if required and add a description. See Naming Tips for guidelines about creating effective names.
5. Select **Next**. The Scope page opens. Use the IP Address Range dialog box to define which endpoints are inspected.
6. Select **Next**. The Change Time page opens. Use this page to set the detection interval and time period.
7. Select **Next**. The Main Rule or Sub-Rules page opens. Review policy conditions and actions.

Which Hosts Are Inspected – Policy Scope

1. Use The IP Address Range dialog box to define which endpoints are inspected.



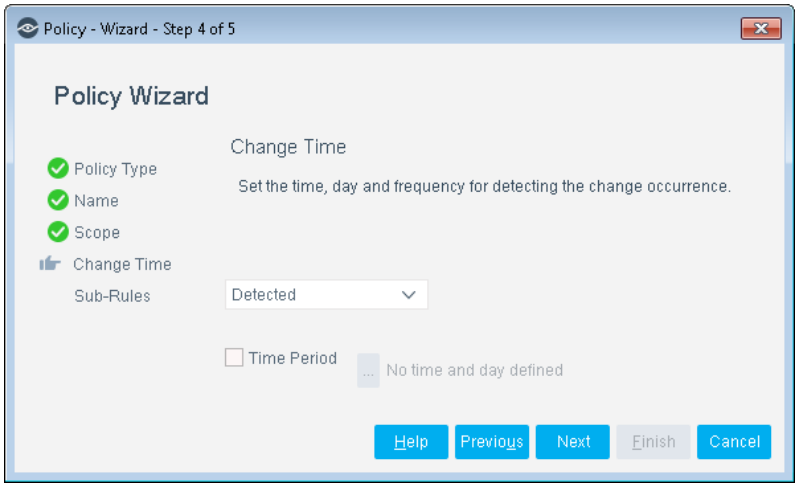
The following options are available:

– **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 select **Segments** from the Scope page.
– **Unknown IP addresses**: Apply the policy to endpoints whose IP addresses are not known. Endpoint detection is based on the endpoint MAC address.

2. Select **OK**. The added range appears in the Scope page.
3. To filter the specified ranges or add exceptions, select (**Advanced**).
4. Select **Next**. The Change Time page opens.

How Frequently Are Endpoints Inspected – Change Time

You must define the frequency at which to inspect endpoints for changes. Define this setting in the Change Time dialog box.



Track Changes, Change Time

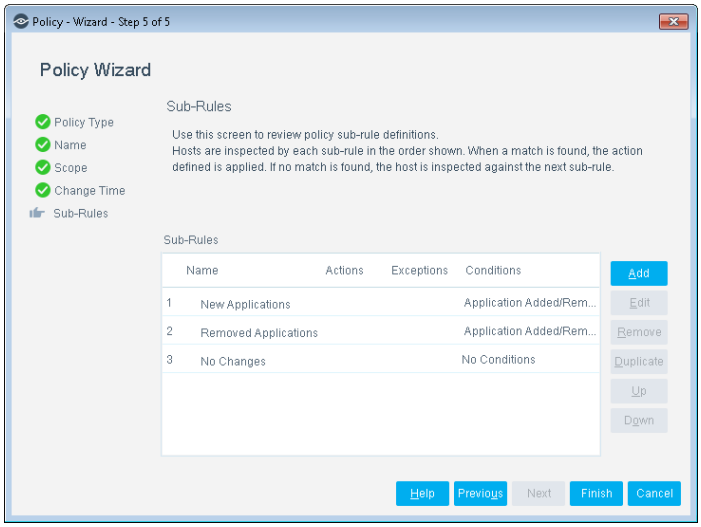
1. Select **Next**. The Main Rule or Sub-Rules page opens. This page lets you review policy conditions and actions.

How a Change Is Detected – Policy Condition

The template *condition* instructs CounterACT to detect the addition or removal of any element that you are tracking.

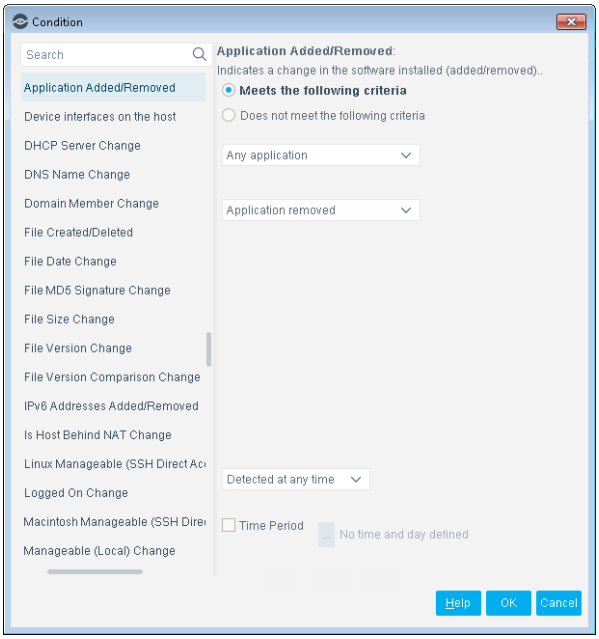
To view and edit conditions:

1. Select the tracked element in the Main Rule or Sub-Rules page.



Track Changes, Sub-Rules

2. Select a sub-rule.
3. Select **Edit** to review the entry. The Sub-Rules Condition dialog box opens.
4. Select an entry in the **Condition** section of the Sub-Rules Condition dialog box.
5. Select **Edit** to review the entry. The Condition dialog box opens.



Track Changes, Criteria

6. Select **OK**.

How a Change Is Handled – Policy Actions

There are no default actions for any of the Track Changes templates.

How to Modify a Condition – Advanced Settings

The bottom section in the Sub-Rules dialog box lets you view and edit the conditions that you have selected, and apply any exceptions.

To view or modify a condition:

1. Select **Edit** in the **Advanced** section of the Sub-Rules page.
2. Select **OK**.

New TCP/IP Port Template

- About the New TCP/IP Port Template
- Prerequisites
- Using the New TCP/IP Port Template
- Which Endpoints Are Inspected – Policy Scope
- Handling Endpoints with New TCP/IP Ports – Policy Actions

About the New TCP/IP Port Template

The New TCP/IP Port template lets you track the addition of a new TCP/IP port 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.

Prerequisites

There are no prerequisites for using this template.

Using the New TCP/IP Port Template

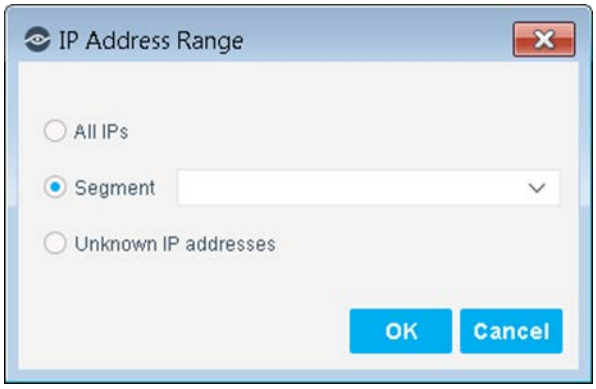
This section describes how to use the template to create a policy.

To use the template:

1. Select **Add** from the Policy Manager.
2. Select the Track Changes folder and then select **New TCP/IP Port**.
3. Select **Next**.
4. Edit the name if required and add a description. See Naming Tips for guidelines about creating effective names.
5. Select **Next**. The Scope page opens.

Which Endpoints Are Inspected – Policy Scope

1. Use The IP Address Range dialog box to define which endpoints are inspected.



The following options are available:

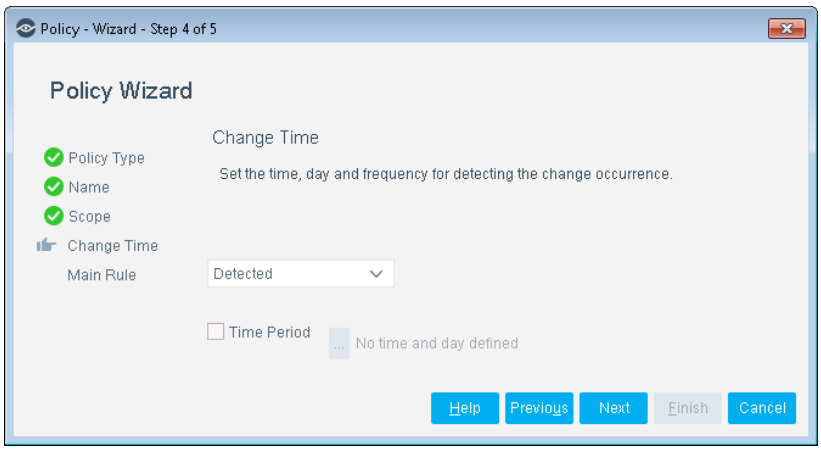
– **All IPs**: Include all IP addresses in the Internal Network.
– **Segment**: Select a previously defined segment of the network. To specify multiple segments, select **OK** or **Cancel** to close this dialog box, and select **Segments** from the Scope page.

– **Unknown IP addresses**: Apply the policy to endpoints whose IP addresses are not known. Endpoint detection is based on the endpoint MAC address.

2. Select **OK**. The added range appears in the Scope page.
3. To filter the specified ranges or add exceptions, select (**Advanced**).
4. Select **Next**. The Change Time page opens. This page lets you set the time period and interval for new TCP/IP port detection.
5. Select **Next**. The Main Rule page opens. This page lets you set conditions for new TCP/IP port detection.

How Frequently Are Endpoints Inspected – Change Time

You must define the frequency at which to track endpoints for changes. Define this setting in the Change Time page.



New TCP/IP Port, Change Time

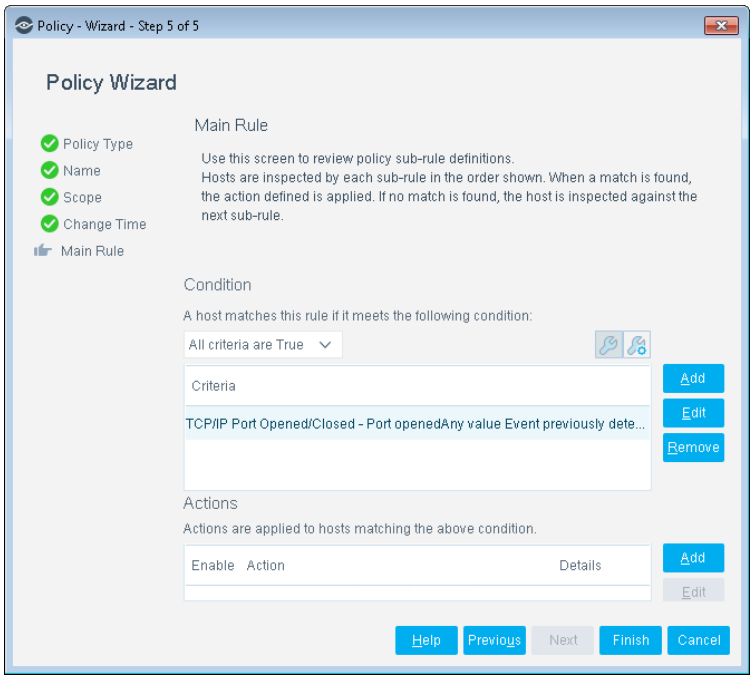
1. Select **Next**. The Main Rule page reopens and lets you review policy conditions and actions.

Detecting Endpoints with New TCP/IP Ports – Policy Condition

CounterACT detects endpoints with new TCP/IP ports when their status changes between opened and closed. This section describes how to view the condition for detecting new TCP/IP ports.

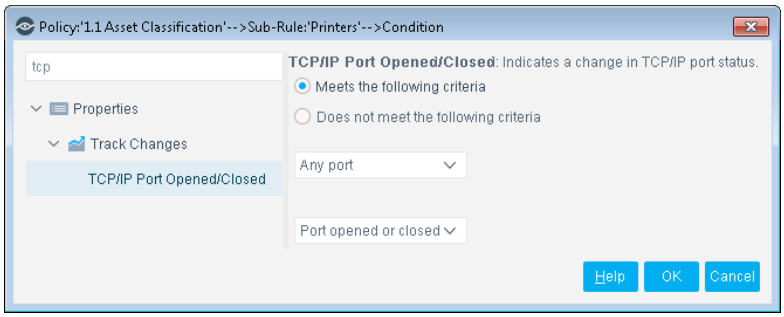
To view the condition:

1. Select the criterion from the **Condition** section of the Main Rule page.



New TCP/IP Port, Condition

2. Select **Edit**.
3. After viewing the criteria and timeframe for new TCP/IP port detection, select **OK**.



New TCP/IP Port, Criteria

4. The Main Rule page reopens. Select **Finish**.

Handling Endpoints with New TCP/IP Ports – Policy Actions

There are no default actions for the New TCP/IP Port template.

Chapter 5: Policy Management

- What Is a Policy?
- Working with Policies
- The Policy Manager
- Creating Custom Policies
- Advanced Policy Options
- Policy Preferences
- Property Lists
- Categorizing Policies
- Policy Reports and Logs
- Policy Safety Features

What Is a Policy?

Most networks consist of complex topologies and architectures; a multitude of events, users, vendors and devices; continuously changing downloads and patches; new vulnerabilities; extensive compliance requirements, and more.

CounterACT policies let you automate and simplify the intricate and time-consuming tasks involved in dealing with these realities. For example:

- 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 *Dashboard*. The Dashboard is a web-based information center that delivers dynamic at-a-glance information about network compliance, threats and guests.

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

Specifically, you use policies to initiate endpoint inspection, specify conditions under which CounterACT 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.

In addition to creating your own policies, you can also use policy templates – CounterACT-supplied templates that help you quickly create important policies based on predefined policy parameters.

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 CounterACT regarding what properties to look for on endpoints. For example, detect endpoints running Windows XP and an outdated Symantec Antivirus application. See About Policy Conditions for more information.

- 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. See About Actions for more information.

About Templates for Policy Creation

CounterACT is delivered with ready-to-use *templates*. Using them helps you quickly create commonly used policies. See Working with Policy Templates for more information.

About Custom Policy Creation

CounterACT lets you 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 Creating Custom Policies.

Working with Policies

This section describes basic information that you will need to know when working with policies and templates.

- When Are Policies Run?
- What You See in the Console in the Home view
- Using Groups
- Broaden the Scope – Plugins and Extended Modules
- Basic Policy Rollout Tips
- CounterACT Policy Priorities
- Handling Endpoint Identity Changes
- Stopping the Policy from the Appliance
- Viewing and Managing Endpoints

When Are 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.

Scheduled Rechecks

You can define a time-based recheck schedule for a policy, or for a specific sub-rule of the policy. For more information, see Updating a Recheck Policy for Unmatched and Matched Endpoints 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 to CounterACT. This triggers re-evaluation of all policies which include the host property that changed. 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. For more information about event driven monitoring this feature, refer to the *HPS Inspection Engine Configuration Guide*. Select **Options** from the **Tools** menu. Select **Modules**. Select this plugin and then select **Help**.

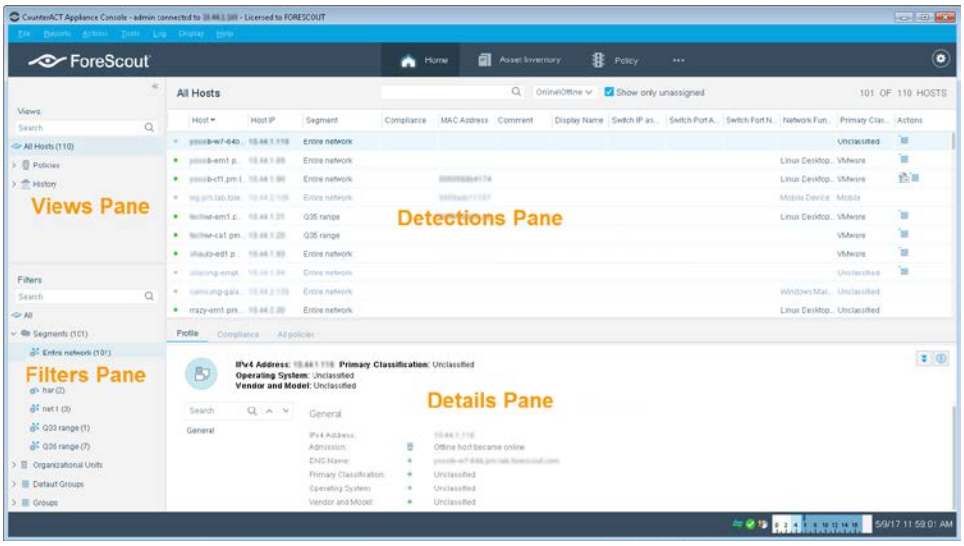
Working with Policy Results

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

What You See in the Console in the Home view

Endpoints detected as a result of your policies and templates appear in the Home view, Detections pane. Select a policy of interest from the Policy folder to view detection information. The folder is located in the Console, Views pane.

An extensive range of detection information can be added and hidden from the Detections pane by using the Add/Remove Columns feature. See Adding, Removing and Reorganizing Columns in the Detections Pane for more information.



What You See in the Console

Information about endpoints inspected by the policy is provided. For example:

- Endpoints that match the policy, and the detection time. You can also view information about unmatched endpoints, endpoints pending inspection and more.
- Machine statistics 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.
- Switch related information.

Viewing Detection Information per Group or Segment

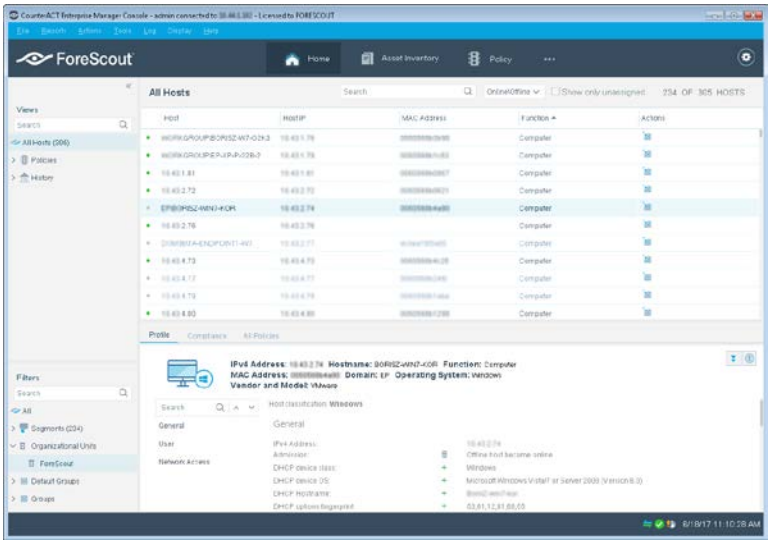
You can display detections associated with a specific network *segment* or *group*.

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 CounterACT Groups for more information.

Segments are network subdivisions; for example, a finance department or East coast regional office, created by users. See Working with CounterACT Segments for more information.

To filter the view:

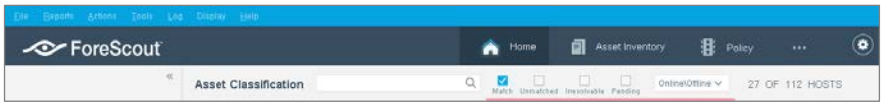
1. Select a Segment or Group filter from the Filters pane of the Console. Endpoints associated with the group or segment are displayed in the Detections pane.



Filtering View per Group

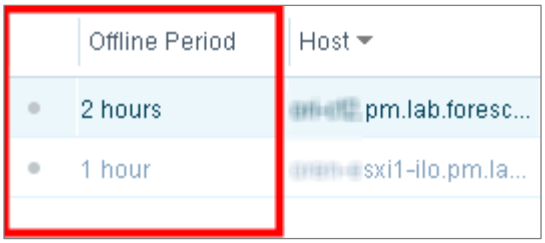
Viewing Detection Information by Endpoint Status

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.



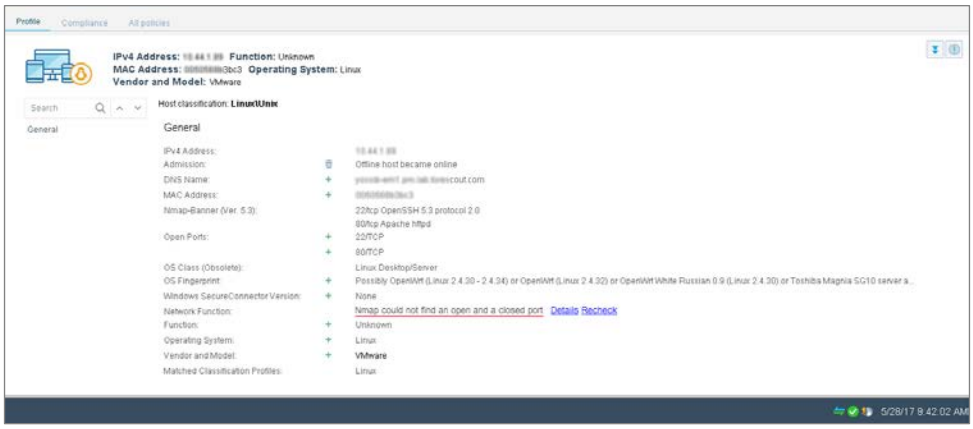
Example of Endpoint Statuses

Matched	Endpoints that matched the conditions defined in the policy.
Unmatched	Endpoints that did 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 CounterACT 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 endpoints that were previously discovered but are no longer connected to the network. If an endpoint is connected to a network switch that is managed by the Switch Plugin, CounterACT 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. Select **Options** from the **Tools** menu. Select **Modules**. Select this plugin and then select **Help**. If an endpoint is not connected to a managed switch, CounterACT can discover that the endpoint is disconnected up to one hour after disconnection. You can change this time period. See Inactivity Timeout 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 a CounterACT Appliance. Each endpoint in your network must be assigned to an Appliance. See Working with Appliance Folders for more information.

Troubleshooting Messages

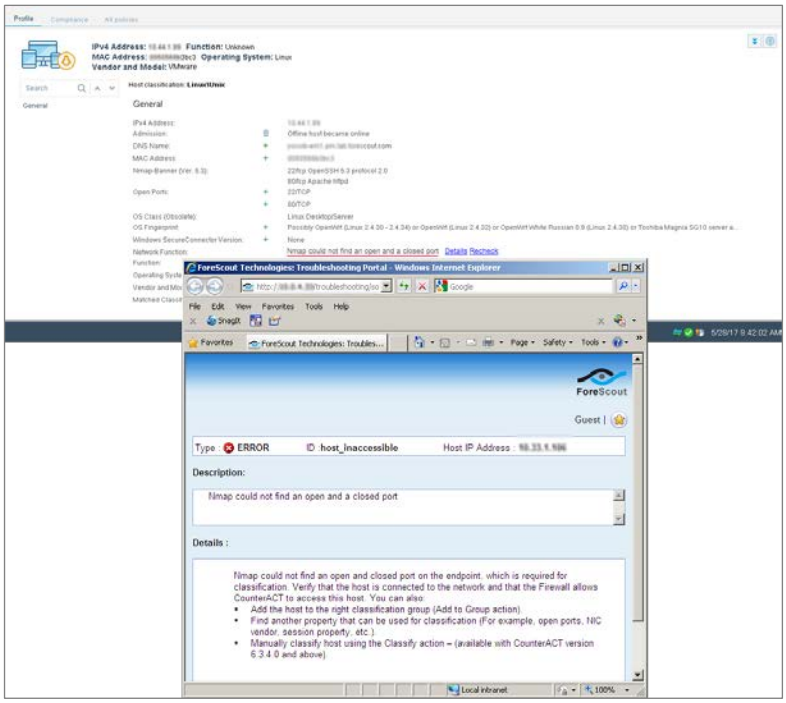
Messages about irresolvable issues, failed actions and other errors can be displayed in the Console. You can also open linked troubleshooting pages that offer suggestions for handling these issues.



Troubleshooting Display

To view troubleshooting:

1. Select (**Show troubleshooting messages**), located at the top right corner of the Details pane.
2. In the Details pane, review the relevant troubleshooting information. Select the **Details** link that appears after the text. The link may appear in any tab that an unresolved event occurred. A window opens with troubleshooting tips.



Example of Online Troubleshooting

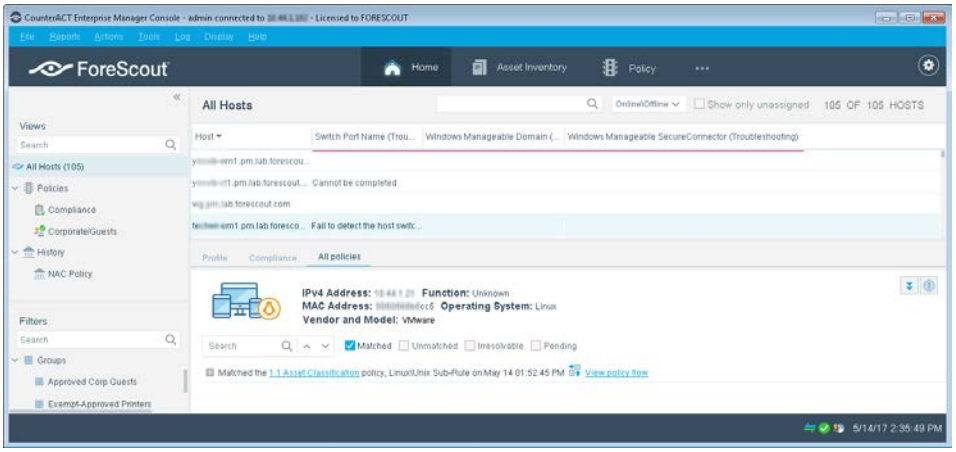
Hiding and Displaying Troubleshooting Messages

You can toggle troubleshooting messages by selecting the **Show troubleshooting messages** icon from the Details pane.

Quickly Access Endpoints with Troubleshooting Issues

View endpoints with troubleshooting issues in the Detections pane.

1. Right-click a Detections pane column and select **Add/Remove Columns**.
2. In the Add/Remove columns dialog box, search field, type *troubleshooting* and add the items for display.
3. Select **OK**. The endpoints with these troubleshooting issues appear in the Detections pane.



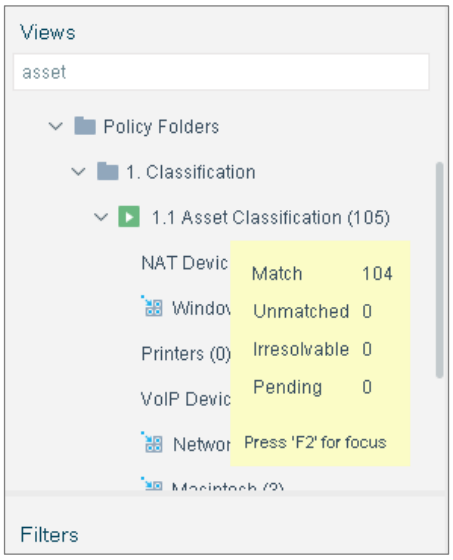
Detections Pane Troubleshooting

Real-Time Policy Status Summary

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.

To display real-time endpoint statistics:

1. From the Views pane, move your cursor over a policy or right-click a policy and select **Show Summary**.



Policy Status Summary

Using 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 perform policies on 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. See About Policy Conditions for details.
- 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*.

There is an additional option to automatically remove 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 will automatically remove the endpoint from the *USB Attached* group.

Broaden the Scope – Plugins and Extended Modules

CounterACT is delivered with predefined policy detection criteria and actions that you can work with. 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 Extended Modules. For example, the McAfee ePolicy Orchestrator Extended Module allows you to integrate with McAfee ePO, access related information, synchronize with related servers, and more.

See Chapter 8: Base, Content and Extended Modules and refer to the related configuration guide for more information.

Basic Policy Rollout Tips

- Make Good Policy Choices
- Test Your Policy

Make Good Policy Choices

Smart policies allow you to reliably and automatically handle an extensive range of network events and tasks. To ensure that you make maximum use of the 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 that such endpoints were 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 actually 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.

CounterACT 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

Handling 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 cancelled on the older address – thus protecting the correct machine. The new IP address is updated in the Detections pane. The following message is displayed in the Host Log when such a change occurs: **`IP Change: IP Changed from...`**
IP transferred from one machine to another	Under certain circumstances, a specific IP address is detected on one machine, and discovered later 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, CounterACT activates the Admission-based activation for the IP address. The following message is displayed in the Host Log when such a change occurs: **`IP Change: IP Changed from...`**

You can customize the mechanism by which CounterACT 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 more information.

Stopping the Policy from the Appliance

If required, you can use the **`fstool nphalt`** command to stop the policy. 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 Console but need to stop the policy.

To stop the policy:

1. Log in to the CounterACT device and run the following command:

   `fstool nphalt`

Viewing and Managing Endpoints

Endpoints detected as result of your policy appear in the Home view in the Console.

To display this view:

1. Select the Home tab.
2. Select the Policy or Compliance folder from the Views pane.

Important detection information is displayed. For example:

- Endpoint information such as the endpoint IP address, DNS name and MAC address.
- User information, such as user name, email address and phone number.
- Action information taken on the endpoint as a result of the policy, i.e., blocking, notification or remediation actions.

Endpoints can be further managed from this view.

Endpoints appear in the view until:

- You release the endpoint. To do this, right-click the endpoint and select **Remove**.
- The endpoints are cleared. To do this, right-click the policy and select **Clear**.
- The endpoint is removed as a result of the automatic recheck mechanism.

Stop and Start Actions for Endpoints in Policies and Sub-Rules

You can stop and start specific actions for all endpoints detected in a policy and sub-policy.

This means:

- Actions currently affecting endpoints are stopped.
- Actions will not be applied to endpoints that are later detected and match the policy.

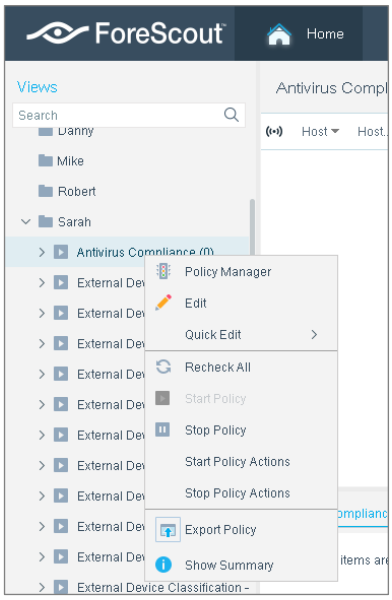
You may want to stop actions to test a policy before enforcing sanctions, i.e., only detect endpoints that match a policy.

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 cancelled if they were defined in Actions schedules.

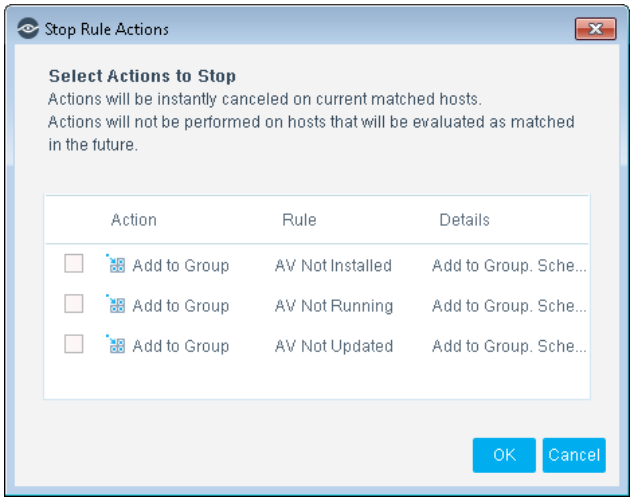
To stop or start an action:

1. Select a policy or sub-rule from the Views pane>Policies folder.
2. Right-click the appropriate listing.



Views Pane

3. Select **Stop Policy Actions** or **Start Policy Actions**. The Stop Action or Start Action dialog box opens.



Stop Policy Action

4. Select the actions that you want to stop or start. You can edit the action definitions from here.

How do I know if actions have been stopped for a policy?

You can check to see if an action is stopped by:

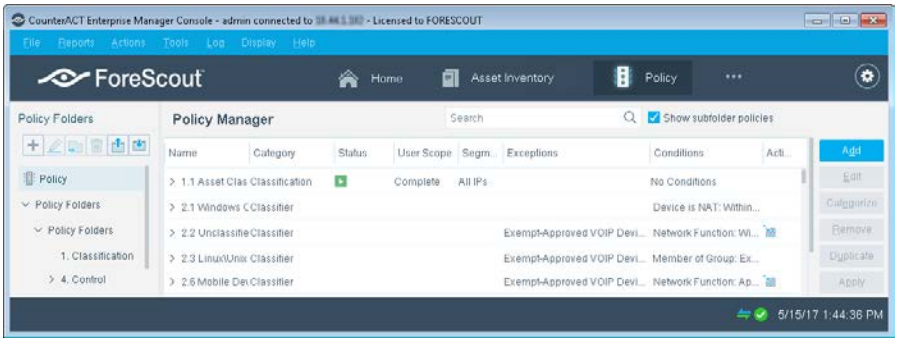
- ***Looking at the action icon***: Action icons are grayed out if cancelled.
- ***Checking the Start or Stop Rule Actions dialog box***: Select the policy or sub-policy and then select Start or Stop Policy Actions to see the stopped and started actions.

The Policy Manager

Your policies are defined and managed from the Policy Manager.

To open the Policy Manager:

1. Select the Policy tab. The Policy Manager opens.



Policy Manager

Policy Manager Tools

The Policy Manager provides the following tools:

Add	Create a new policy.
Edit	Edit a policy.
Remove	Remove a policy.
Duplicate	Duplicate a policy, and edit as required.
Categorize	Categorize policies to help you organize and view them in the Policy Manager. For example, only display policies that have been 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 the: ▪ ForeScout Compliance Center ▪ Site Map ▪ Compliance Status property ▪ Corporate/Guest Status property See Categorizing Policies 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 about creating folders.

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.

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

In addition, the following policy management tools are available in the Policy Manager:

Custom	Create custom reusable policy conditions. Select **Custom** from the **Tools** menu. See Authentication Properties for more information.
Generate Policy Report	Generate a report listing all your policies, and policy definitions. Select **Policies Summary Report** from the **Reports** menu on the Console.
Import **Export** **Policy Folders**	By default, policies are imported as XML files. Select the **Import** icon from the **Policy Folders** pane or right click 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 subfolder of the folder in the original location (**Add folder to the target**) or as a subfolder of the target itself (**Add folder content to the target**). ▪ **File name** is the name of the policy that you want to import. ***Import limitations*** If you import a policy that refers to groups not defined on the Appliance, these groups will automatically be created. Note that 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.

Working with the Policy Manager

Policy Information

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

Item	Description
Name	The name assigned to the policy.
Status	Indicates whether the CounterACT detection mechanism is paused or running. When paused, new detection events are ignored.
Category	The category assigned to the policy.

Item	Description
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	CounterACT groups included in the policy inspection. See Working with CounterACT Groups for details.
Segments	The range of IP addresses to be inspected for the policy. See Defining a Policy Scope for details.
Exceptions	The range of IP addresses excluded from policy inspection.
User Scope	The range of endpoints a CounterACT 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).

Apply Your Policies

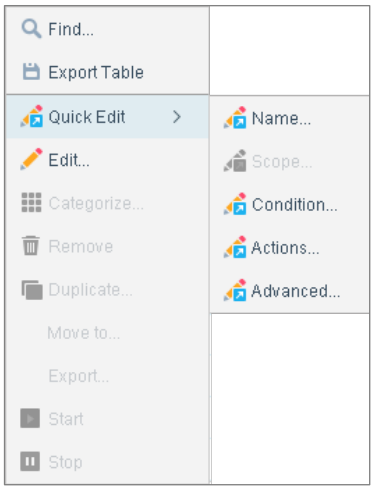
After creating and editing policies, you must apply them in the Policy Manager by selecting **Apply**.

Edit Policies and Rules

Use the Quick Edit option to easily access the policy or sub-rule parameters that you want to update. Changes made to policy definitions are implemented immediately.

To edit:

1. Right-click a policy or sub-rule from the Policy Manager and select **Quick Edit**.
2. Select an editing option.

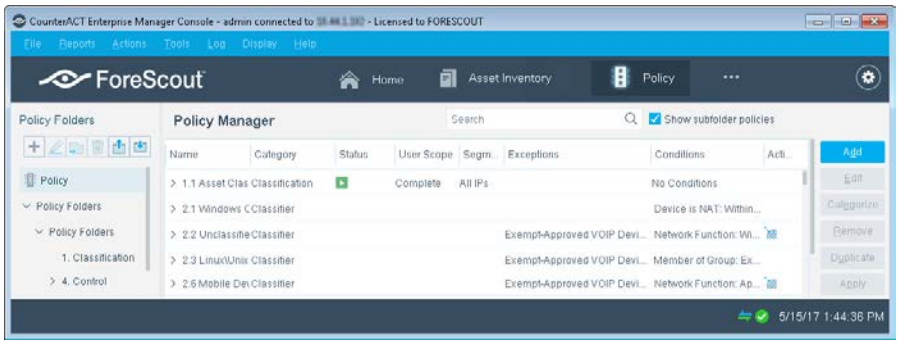


Quick Edit Tools

Manage Policy Folders

You can organize your policies into logical folders for easier navigation and management. For example, create East Coast Finance and West Coast Finance folders and place the appropriate policies in these folders, which also appear in the Views pane.

If you create and then delete a folder, any policies in the folder will also be deleted.



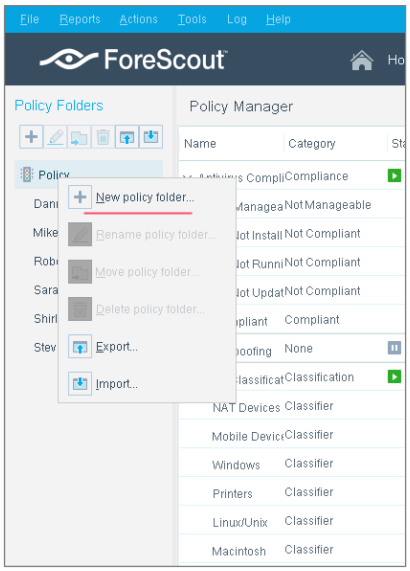
Policy Manager

You can hide and display policies associated with a subfolder by using the **Show subfolder policies** checkbox in the Policy Manager.

To see all policies and sub-rules, select the **Policy** icon in the tree root and then select the checkbox.

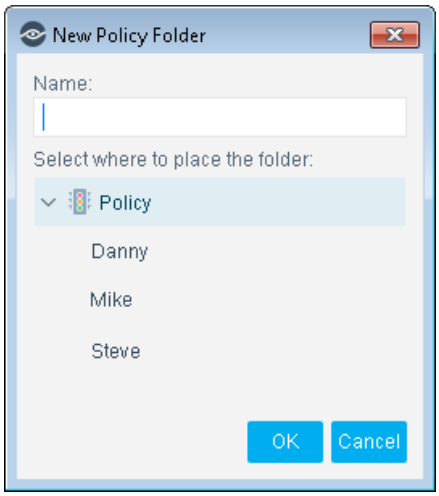
To create folders:

1. Right-click an item in the Policy Folders pane of the Policy Manager.
2. Select **New Policy Folder**.



New Policy Folder Option

The New Policy Folder dialog box opens.



New Policy Folder Dialog Box

3. Type a folder name.
4. Select a location to place the folder.
5. Select **OK**.
6. Use the **Edit**, **Delete** and **Move** buttons or right-click options to manage these folders.

Add Policies to Folders

Add your policies to policy folders that you created. You cannot copy a policy to more than one folder.

To add a policy to a folder:

1. Select a policy from the Policy Manager.

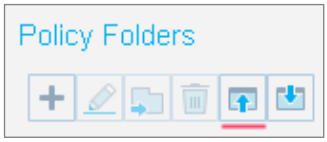
2. Select **Move to**. The Move To Policy Folder dialog box opens.
3. Select a folder in which to place the policy and select **OK**.

Export and Import Policies

It is often convenient to copy policies to Appliances using the export/import tools of the Console.

To export a policy or policy folder:

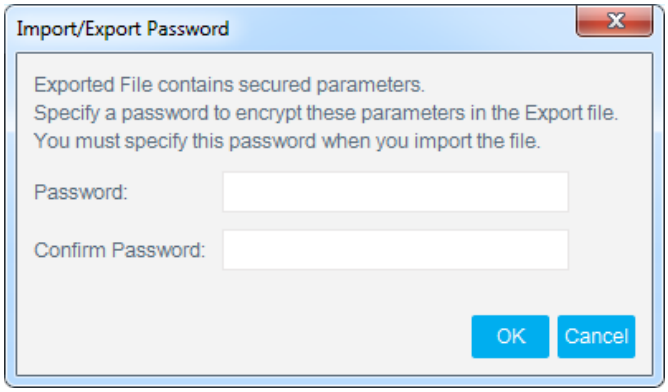
1. In the Policy view, do one of the following:
   - Right-click a policy in the Policy Manager pane or a folder in the Policy Folders pane, and select **Export**.
   - Select a policy from the Policy Manager pane, and select **Export**.
   - Select a folder from the Policy Folders pane, and select the Export Folder icon.



Export Folder Icon

2. When policy conditions or actions include login credentials for network devices, servers, or services, CounterACT encrypts the exported policies. When you export policies, CounterACT prompts you for a password that is used to encrypt the exported file. Enter an encryption password and select **OK**.

This password must be used to import the file.



Policy Export Password

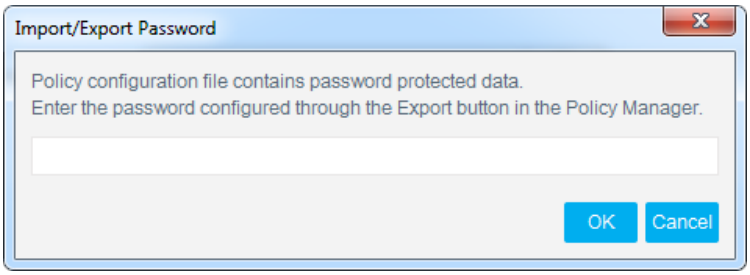
3. Policies and policy folders are exported and imported as XML files. In the Export dialog box, specify the location of the exported XML file and select **OK**. The selected policy or folder is exported.

To import a policy or policy folder:

1. In the Policy Folders pane, do one of the following:

- Right-click the target folder to which the policy or folder will be imported, and select Import. To import a policy or folder into the top level of the policy tree, right-click the Policy icon.
- Select the target folder to which the policy or folder will be imported. Then select the Import Folder icon.

2. In the Import dialog box, specify the location of the XML file you want to import and select **OK**.
3. When policy conditions or actions include login credentials for network devices, servers, or services, CounterACT encrypts the exported policies. When you import these policies, CounterACT prompts you for the password that was used to encrypt the exported file.



Policy Import Password

4. Enter the password and select **OK**. The policy or folder is imported to the location you specified in the Policy Folders tree.

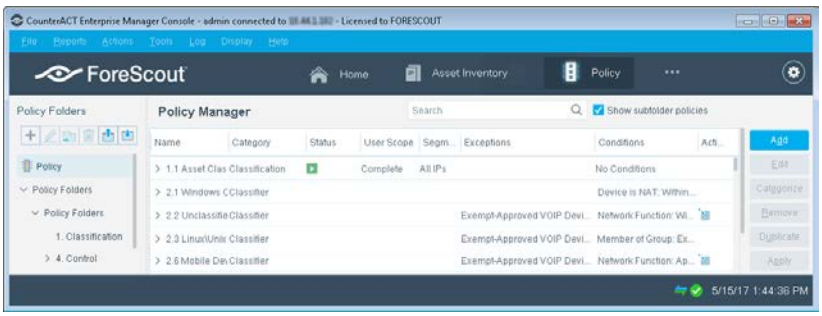
Creating Custom Policies

The following sections detail the procedure for creating a custom policy. You may choose to create a 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. For information about policies, see What Is a Policy?

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

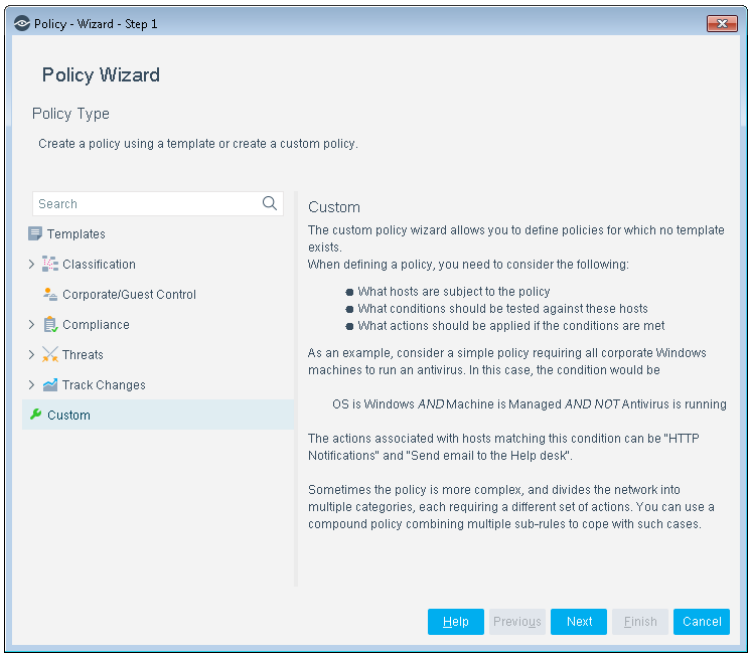
To create a policy:

1. Select the Policy tab. The Policy Manager opens.



Policy Manager

2. Select **Add** from the Policy Manager. The Policy wizard opens.
3. Select **Custom**.

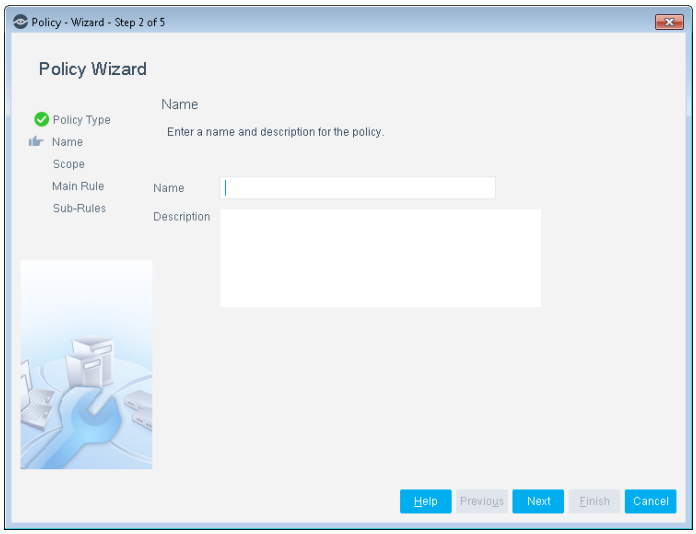


Policy Wizard

4. Select **Next**.

Defining a Policy Name and Description

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.



Custom, Name

Naming Tips

Make sure names are accurate and 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

1. Type a unique name and description.
2. Select **Next**. The Scope page opens.

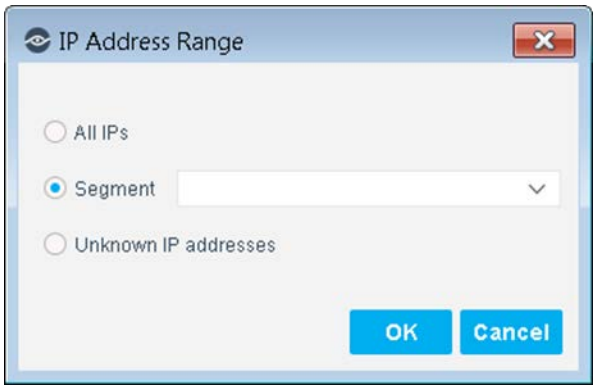
Defining a Policy Scope

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

- Including only certain CounterACT 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 a scope:

1. Use The IP Address Range dialog box to define which endpoints are inspected.



The following options are available:

– **All IPs**: Include all IP addresses in the Internal Network.

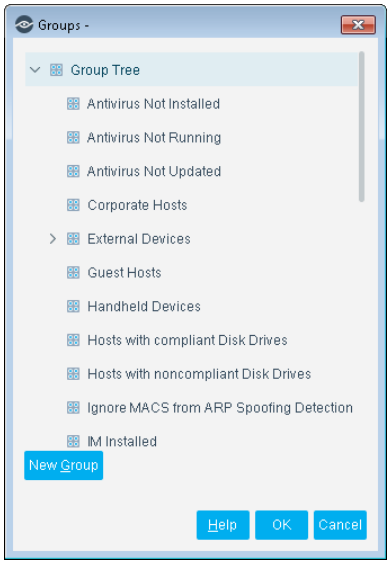
– **Segment**: Select a previously defined segment of the network. To specify multiple segments, select **OK** or **Cancel** to close this dialog box, and select **Segments** from the Scope page.

– **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 detection of MAC-only endpoints, see Working with Hosts without IPv4 Addresses.

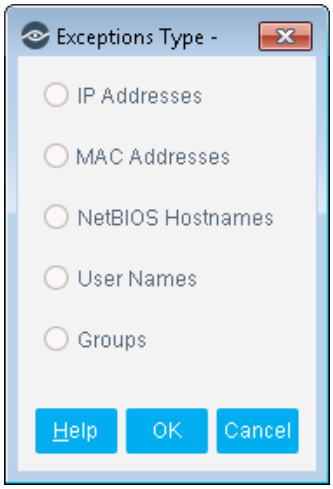
2. Select **OK**.
3. Select **Advanced** to fine tune the scope. Two options are available:
   – Only include some CounterACT groups in the inspection. If you select several groups, and an endpoint is detected in at least one, that endpoint is included in the policy inspection.
   – Select **Add** from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

   The Policy Group dialog box opens.



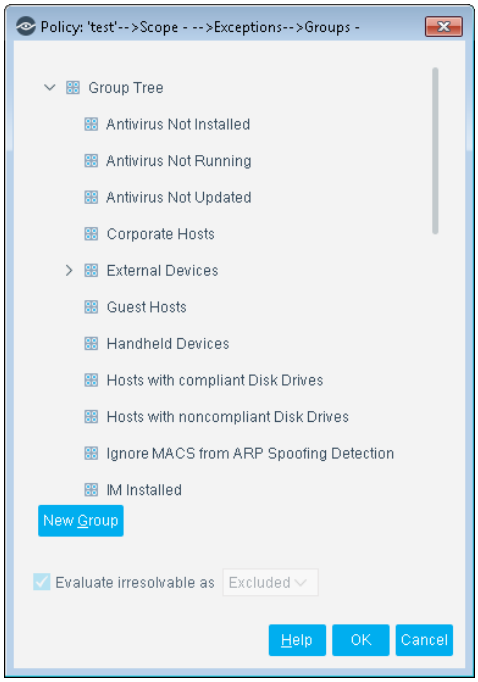
Group Dialog Box

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** section, to *exclude* endpoints from inspection. For example, ignore groups of VIP users from inspections. The Exception Type dialog box opens.



Exceptions Dialog Box

8. Select an exception type and then select **OK**. An Exception dialog box opens. Exception dialog boxes vary depending on the exception that you selected. 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).



Sample – Exceptions Dialog Groups Box

9. Select **OK**.

10. Use the **Evaluate Irresolvable As** checkbox to instruct CounterACT how to evaluate the endpoint if the exception value cannot be resolved; for example, CounterACT 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 Rule page 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: CounterACT measures taken at endpoints. For example, provide automatic remediation at endpoints without up-to-date Symantec Antivirus installations.

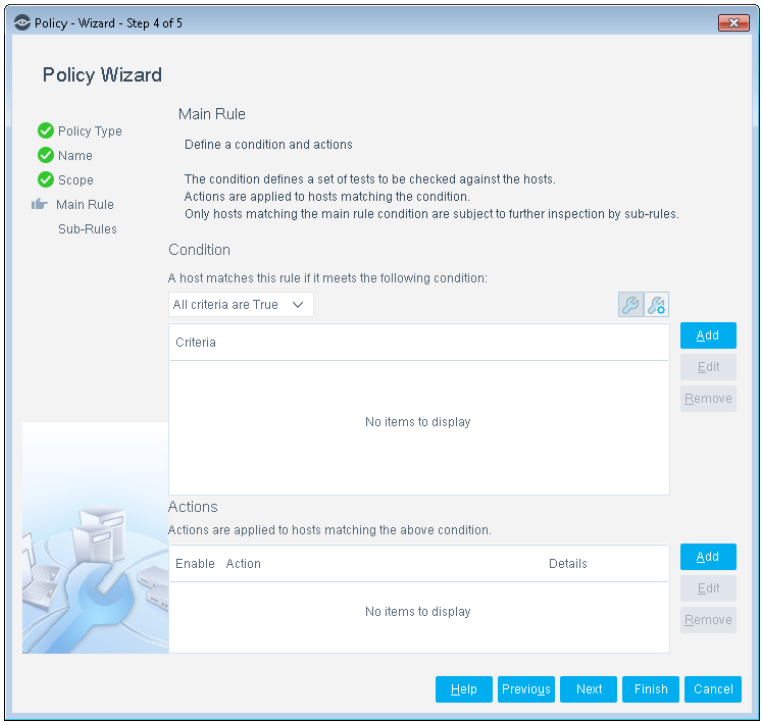
In general, it is recommended to define conditions and actions in Main Rules when your policy deals with a single policy purpose or problem and solution. For example, consider a policy requiring all corporate Windows machines to run an antivirus application. In this case, the Main Rule would be:

- ***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.

In such cases, you should use policy sub-rules to create *several* conditions and related actions. Sub-rules allow you to automatically follow up with endpoints after initial detection and handling. Creating sub-rules lets you streamline separate detection and actions into one automated sequence. See Defining Policy Sub-Rules for more information.



Custom, Main Rule

To define Main Rule conditions and actions:

1. Select **Add** from the **Condition** or **Actions** section of the Main Rule dialog box as required.

   See Chapter 6: Working with Policy Conditions and Chapter 7: Working with Actions for details about conditions and actions.

2. When you are done, select **Next**. The Sub-Rules dialog box opens. Use the dialog box to review and update Main Rule definitions and advanced policy settings, as well as to define sub-rules.

How Often Are Policies Run?

By default, policies are run every eight hours and on any *admission event*—a network event that indicates the admission of an endpoint into the network, such as when it physically connects to a switch port.

You can update the default setting; for example, according to a set schedule. You can also configure several activation settings to work simultaneously; for example, when an endpoint IP address changes, and every five hours.

You can update defaults and work with advanced Main Rule settings from the Advanced Settings dialog box.

To open the Advanced dialog box:

1. Right-click a policy from the Policy Manager.
2. Select **Quick Edit**.
3. Select **Advanced**.

See Main Rule Advanced Options and Sub-Rule Advanced Options for more information.

Defining Policy Sub-Rules

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

Sub-rules are performed in order until a match is found. When a match is found, the corresponding action is applied to the endpoint. If the endpoint does not match the requirements of the sub-rule, the endpoint is checked against the next sub-rule. This means that the order in which the sub-rule is displayed is significant.

For example:

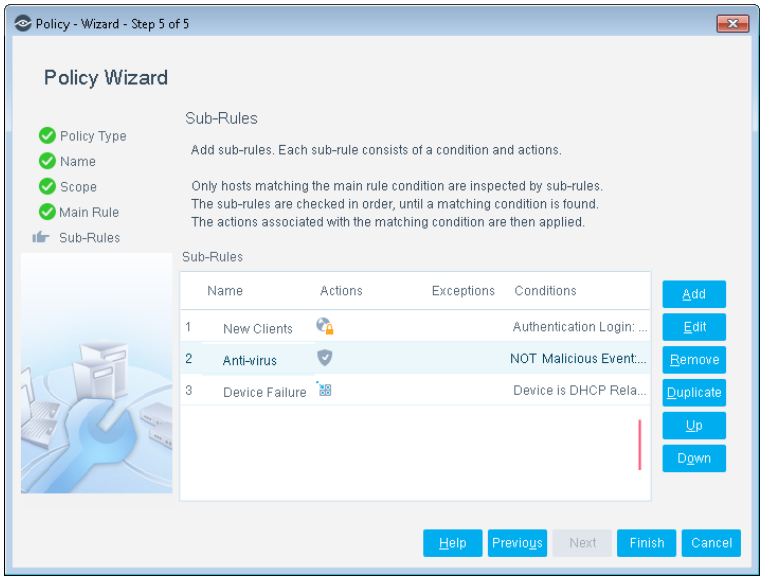
- Assign endpoints to different VLANs based on their security compliance:
- *If* non-corporate endpoints are detected, block access to the production network, but allow limited network Internet access.
- *If* corporate unmatched endpoints are detected, but are VIP users, *then* remediate in a separate 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.

Sub-rules consist of the following elements:

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

Rearranging the Order of Sub-Rules

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

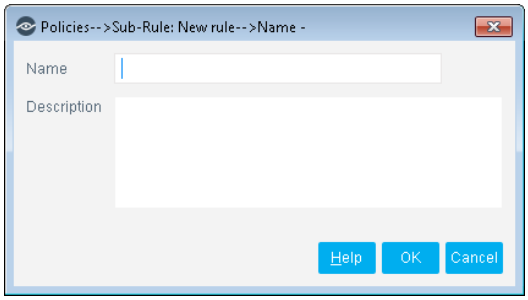


Up and Down Buttons

To define a sub-rule name and description:

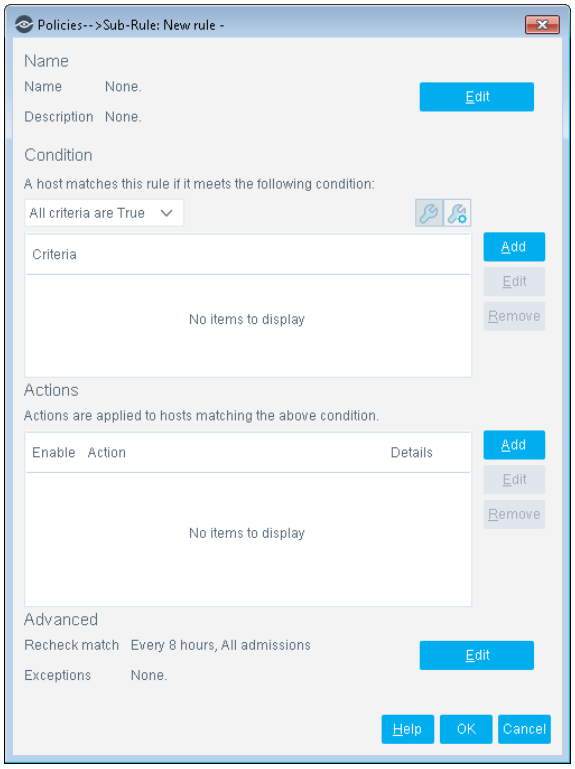
1. Select **Add** from the Sub-Rules dialog box.

   The New rule>Name dialog box opens.



Name and Description

2. Type a unique policy and description. See Defining a Policy Name and Description for details.
3. Select **OK**. The name is displayed in the New Sub-Rule dialog box that opens. Use the dialog box to define sub-rule conditions and actions. See Chapter 6: Working with Policy Conditions and Chapter 7: Working with Actions for details.



New Sub-Rule Dialog Box

Advanced Policy Options

The following advanced policy options are available:

- Main Rule Advanced Options
- Sub-Rule Advanced Options

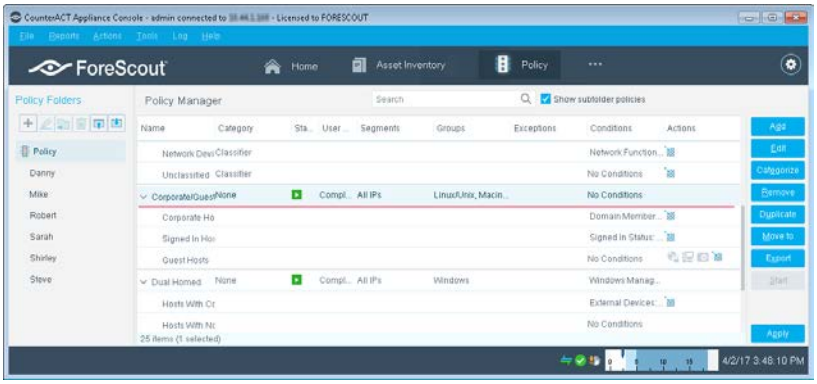
Main Rule Advanced Options

The following advanced Main Rule options are available:

- Updating a Recheck Policy for Unmatched and Matched Endpoints
- Handling Dated Information – General Tab
- Ignoring Dated Information
- Updating the Network Admission Resolve Delay
- Setting and Incrementing Counters

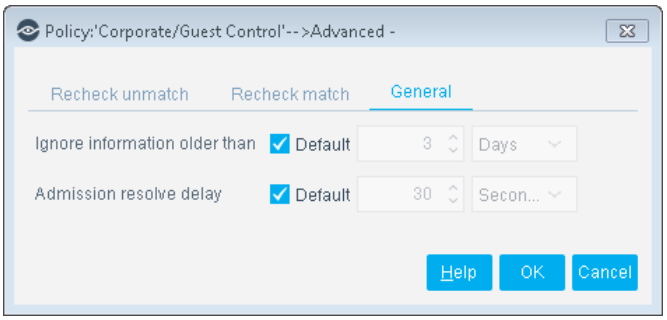
To view Main rule advanced options:

1. Right-click a Main Rule from the Policy Manager.



Main Rule Selected from Policy Manager

2. Select **Quick Edit**>**Advanced**.



Advanced, General

Updating a Recheck Policy 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:

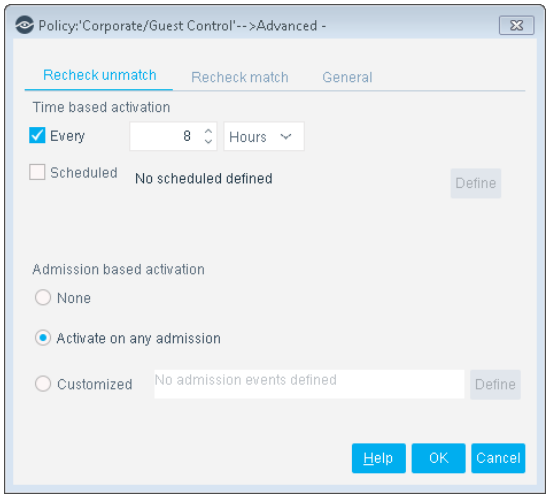
- How often endpoints that match a policy are rechecked
- Under what conditions to perform recheck

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 select **Quick Edit**>**Advanced**.
2. Select the **Recheck unmatch** or **Recheck match** tab.



Advanced, Recheck Unmatch Tab

Time Based Activation

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

Every	Use this option to run a policy at short 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 want 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 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 will initiate the activation. The default time period can be changed. See Policy Preferences for more information. ▪ 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, *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.

A delay time 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 more information.

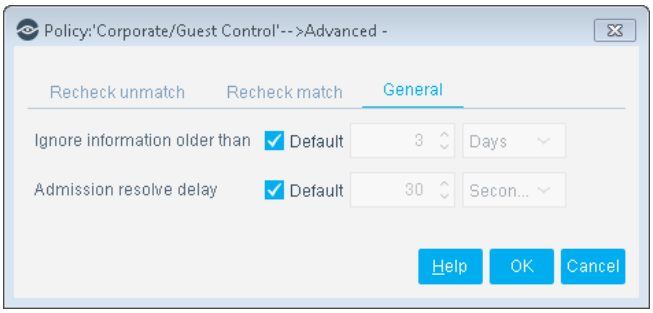
Handling Dated Information – General Tab

Several options are available for handling dated information.

- Ignoring Dated Information
- Updating the Network Admission Resolve Delay

To handle dated information:

1. Right-click a rule from the Policy Manager and select **Quick Edit**.
2. Select **Advanced**.
3. Select the General tab.



General Tab

Ignoring Dated Information

This value applies to information stored and used between activation evaluations. For example, if you defined an activation schedule that evaluates endpoints every two days, the information stored for two days are used for evaluation. You can define a value here that applies an absolute time information should be stored and used. The value set here is applied per policy. You can also set the value globally for all policies. When you use global values, the policy setting still applies. See Policy Preferences for more information.

Updating the Network Admission Resolve Delay

A default delay time exists between the detection of network admission events and the onset of the policy evaluation. This time is allotted because 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 rule evaluation will start when more details can be learned about the endpoint (after all services have loaded). You can update the delay default time.

This delay is only applied to properties that are reported directly from the endpoint; for example, Processes Running, Windows Applications, Windows Domain Member or File version. The delay is not applied to properties that are reported from other

sources; for example, switch properties, Active Directory group membership or properties related to Extended Modules.

The value set here is applied per policy. You can also set the value globally for all policies. When you use global values, the per-policy setting still applies.

TIP: If you set this value too high, your machines will not be checked immediately after admission. If you set the value too low, discovered information may not be accurate.

Setting and Incrementing Counters

This section describes properties and actions that let you set and evaluate counters in policies. Policies can trigger actions based on counters assigned and incremented previously by other policies. This allows you to use endpoint history in policies.

For example, if an endpoint repeatedly installs pluggable memory devices, you can invoke actions on the endpoint after this behavior is repeated a number of times. The use of counters lets you accommodate occasional use of hot-swappable memory, and identify problematic repeat users.

When using counters in policies, note that:

- Counters are incremented each time an endpoint *returns* to the conditions of a policy, as follows:
  - 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 CounterACT evaluates other policy conditions. However, counter values are *retained* even when the endpoint no longer satisfies the conditions of the policy.

Counters are maintained per endpoint – and like a host property, the same counter can have a different value for each endpoint.

Using Counters in Policy Rules

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:
  - **a.** 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 newly created counter.
  - **b.** Then the rule uses the Set Counter action to increment the counter on endpoints that match the condition.

Sub-Rule Advanced Options

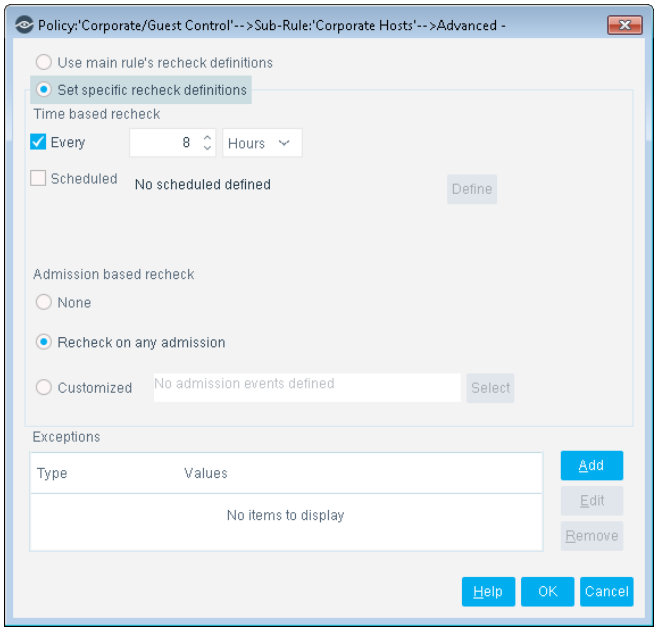
The following advanced Sub-Rule options are available:

- Inherit Main Rule Recheck
- Sub-Rule Recheck Policy

To view Sub Rule advanced options:

1. Right-click a Sub-Rule from the Policy Manager.
2. Select **Quick Edit**.
3. Select **Advanced**.

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



Sub-Rule Advanced Dialog

Inherit Main Rule Recheck Definitions

Instruct CounterACT to automatically apply main rule recheck definitions to all sub-policies, rather than defining the recheck value for each sub-rule.

To use main rule definitions:

1. Select **Use main rule recheck definitions**.

Sub-Rule Recheck Policy

Sub-rule *Recheck* tools let you define:

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

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

To define the recheck policy:

1. Right-click a sub-rule from the Policy Manager.
2. Select **Quick Edit** and then select **Advanced**.

   The Advanced dialog box opens.
3. See Updating a Recheck Policy for Unmatched and Matched Endpoints for information about how to work with this feature.

Define Sub-Rule Exceptions

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

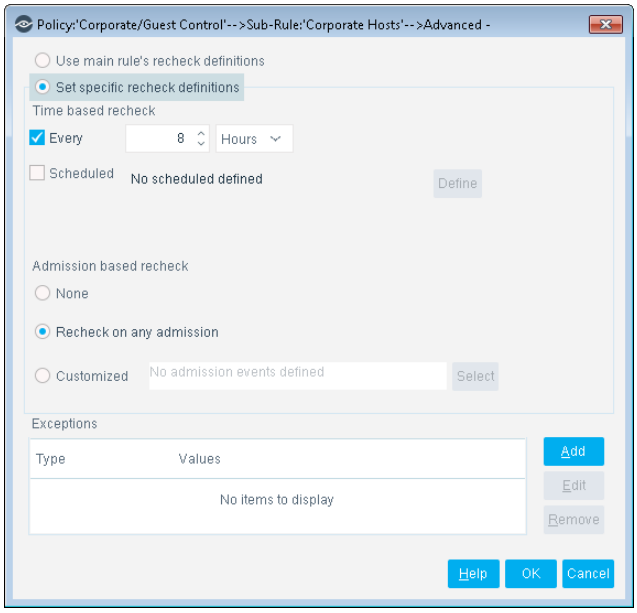
- Scope
- Windows hosts
- Sub-Rule 1
- Condition: Vulnerable to MS-08-xxx
- Action: Browser Notification
- Exception: Windows Servers
- Sub-Rule 2
- Condition: Symantec AntiVirus not installed
- Action: Browser Notification
- Exception: none

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

To define sub-rule exceptions:

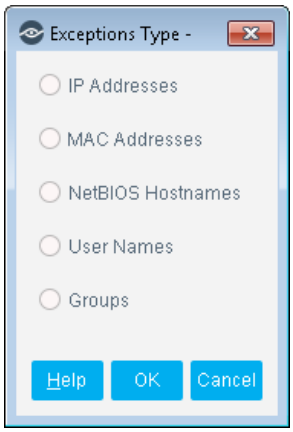
1. Right-click a sub-rule from the Policy Manager.
2. Select **Quick Edit** and then select **Advanced**.

   The Advanced dialog box opens.



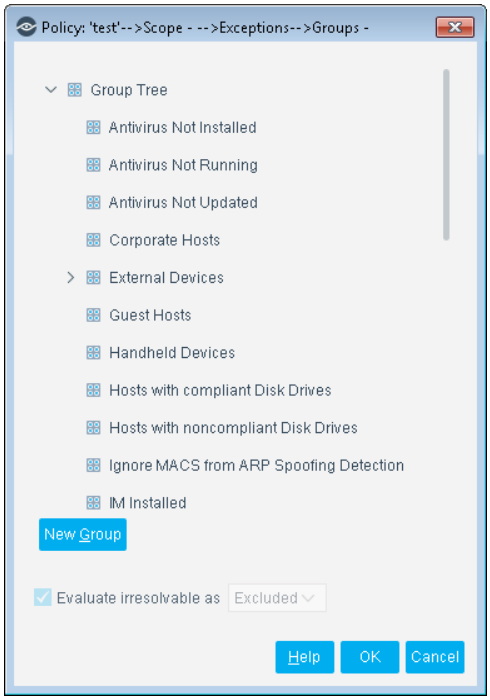
Sub-Rule Advanced Dialog Box

3. In the **Exceptions** section, select **Add**. The Exception Type dialog box opens.



Exception Type Dialog Box

4. Select an exception type and then select **OK**. An Exception dialog box opens. This dialog box varies depending on the exception that you selected. 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 information about lists.



Sample Exceptions Dialog Box

5. Select **OK**.
6. Use the **Evaluate Irresolvable As** checkbox to instruct CounterACT how to evaluate the endpoint if the exception value cannot be resolved; for example, CounterACT 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*.
7. After defining each exception, select **OK**.

Policy Preferences

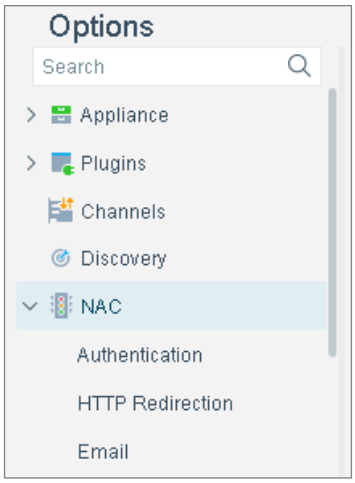
The following policy preferences are available:

- Defining Authentication Servers
- HTTP Preferences
- Customizing HTTP Pages
- Email Preferences
- Customizing Endpoint Identity Change Thresholds and Detection Mechanisms
- Time Settings
- HTTP Login Attempts

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

To access the NAC options:

1. Select **Options** from the **Tools** menu and then select **NAC**.



NAC Folder

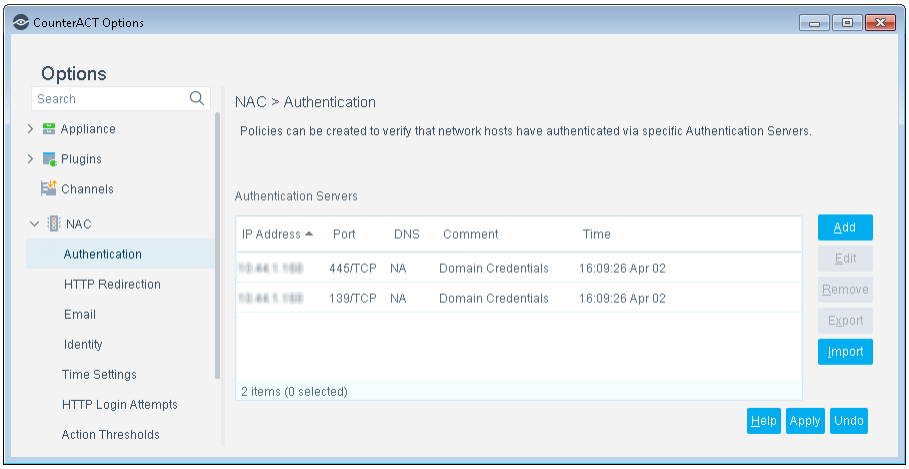
Defining Authentication Servers

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

CounterACT supports the following authentication servers:

- HTTP (80/TCP)
- Telnet (23/TCP)
- NetBIOS (139/TCP)
- FTP (21/TCP)
- IMAP(143/TCP)
- POP3(110/TCP)
- rlogin (513/TCP)

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

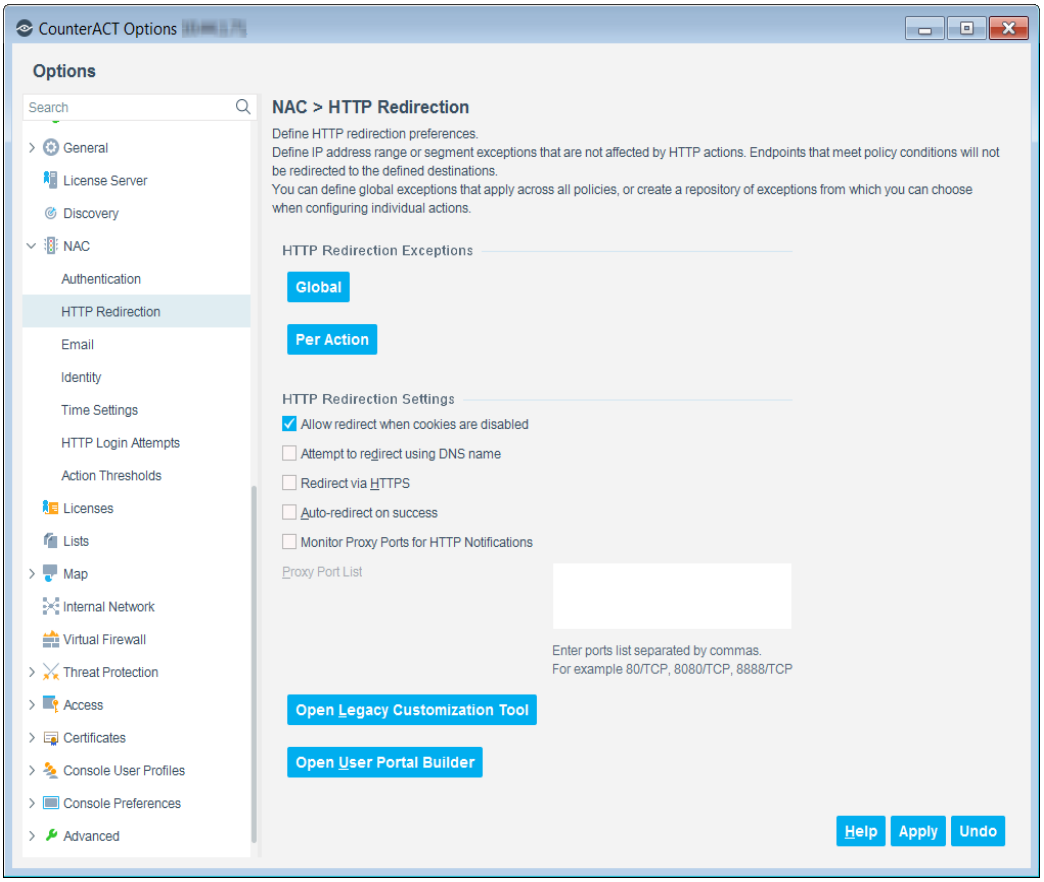


NAC>Authentication Pane

HTTP Preferences

Various preferences are available for handling HTTP traffic.

- Defining HTTP Redirect Exceptions
- Disable Redirection When Cookies Are Disabled
- Redirect Using Web Server DNS Name
- Globally Redirect via HTTPS
- Skip HTTP Redirect Confirmation Message
- Defining Proxy Ports for HTTP Notification



HTTP Redirection Pane

To access the HTTP Redirection pane:

1. Select **Options** from the **Tools** menu and then select **NAC**>**HTTP Redirection**.

Defining HTTP Redirect Exceptions

You may want 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 across all actions.
- IP Address Exceptions per Action. IP address exceptions that can be applied to individual actions.

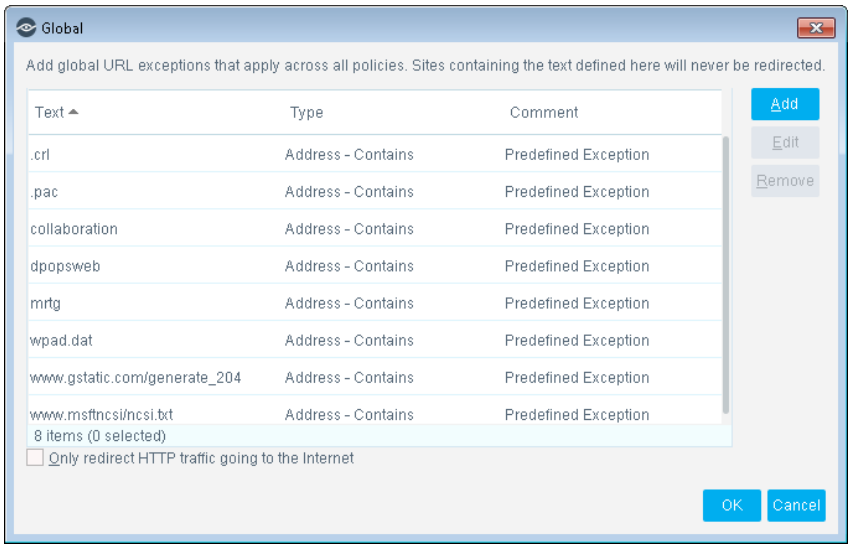
Global URL Exceptions

Endpoint users who browse to URLs in this list will not be redirected by CounterACT even when a CounterACT 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, if needed.

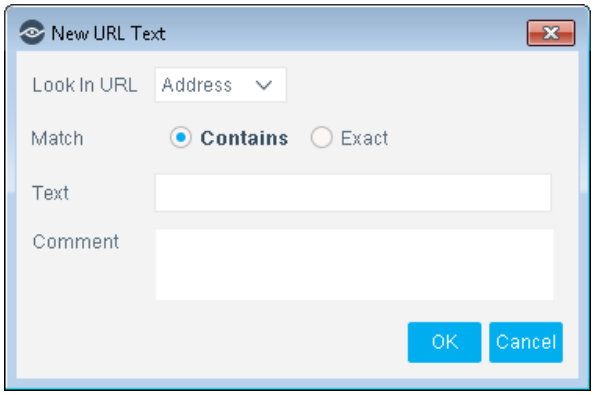
To create exceptions:

1. Select **Tools**>**Options** and then select **NAC**>**HTTP Redirection**.
2. Select **Global...** in the HTTP Redirection Exceptions section. The Global dialog box opens.



Global Dialog Box

3. Select **Add**. The URL Text dialog box opens.



URL Text Dialog Box

4. Two options are available:
   - Look in URL for filename
   - Look in URL for address
5. Select **Contains** or **Exact**.
6. In the **Text** field, type the URL address or filename to search for.
7. Select **OK**.

By default, the following URLs are never redirected:

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

This allows 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.

If the address contains one string from the following 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.

To redirect web sessions to the Internet only:

1. 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 will not be 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 unless the endpoint IP address is 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*

To apply an HTTP Redirection exception per action, perform the following:

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

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

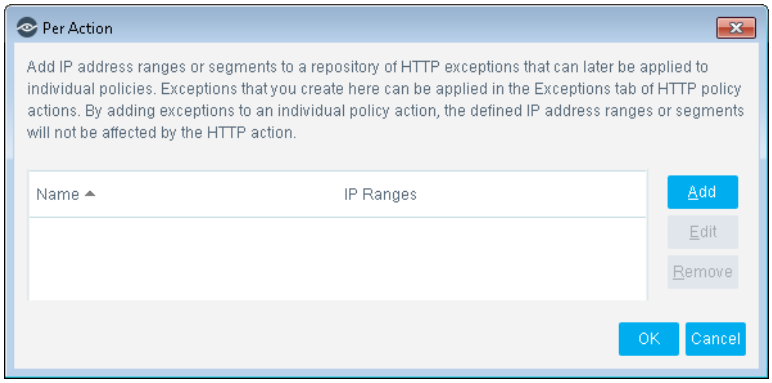
When multiple HTTP actions, each containing HTTP Redirection Exceptions, are simultaneously applied to an endpoint, only the exceptions of the first HTTP action received by CounterACT are applied. Additional HTTP Redirection Exceptions are only applied when there are no other HTTP actions applied to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

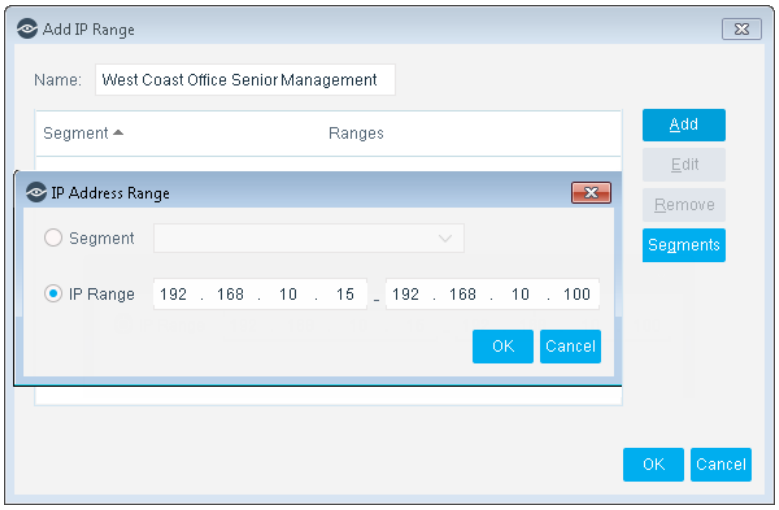
To add an exception to the repository:

1. Select **Options > NAC > HTTP Redirection**.
2. Select **Per Action...** in the HTTP Redirection Exceptions section.



Per Action Dialog Box

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 select **OK**.



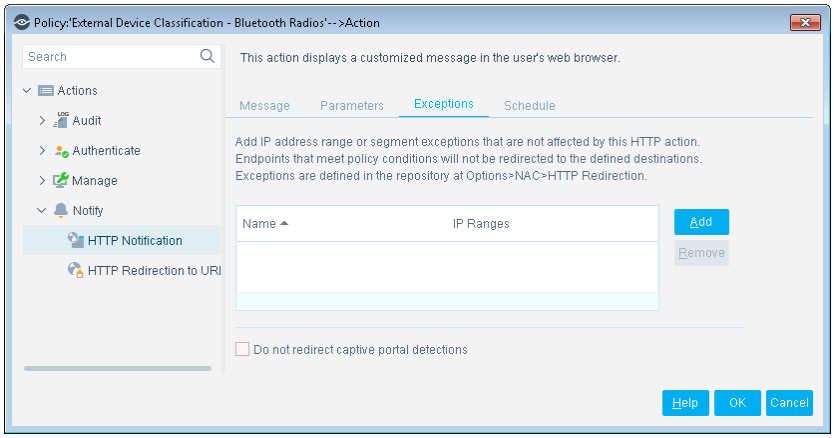
Add IP Address Range Exception

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

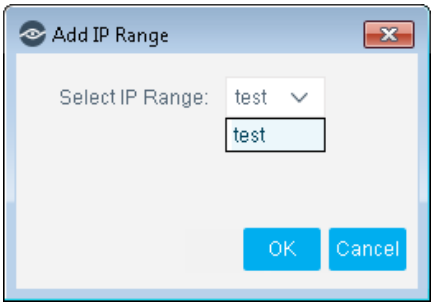
To apply an exception:

1. In the relevant HTTP action configuration, navigate to the Exceptions tab.



HTTP Action Exceptions tab

2. Select **Add**. The Add IP Range dialog box opens.



HTTP Action Exceptions Add IP Range dialog box

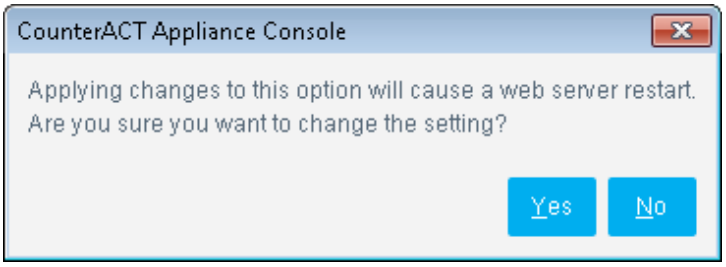
3. Select the name of an HTTP exception from the Select IP Range dropdown list and select **OK**. The exception is displayed in the Exceptions table.

Disable Redirection When Cookies Are Disabled

By default, HTTP redirection actions also apply when cookies are disabled on the end user browser. You can instruct CounterACT to disable these actions when cookies are disabled as an added security measure to prevent passing the session ID via the URL. Applying changes to this option will cause a web server restart.

To disable redirection when cookies are disabled:

1. Select **Tools>Options** and then select **NAC>HTTP Redirection**.
2. Clear the **Allow redirect when cookies are disabled** option. A warning message opens.



Web Server Restart warning message

3. Select **Yes**. When you apply changes, the CounterACT web server will restart.

Redirect Using Web Server DNS Name

When CounterACT 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.

To redirect using the web server DNS name:

1. Select **Tools**>**Options** and then select **NAC**>**HTTP Redirection**.
2. Select **Attempt redirect using the DNS name** to redirect using the DNS name.

Globally Redirect via HTTPS

You can configure the connection method used for transmitting all redirected traffic to HTTP, or to HTTPS, i.e. encrypted over a secured connection (HTTP over TLS).

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 will 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 Appendix 3: Generating and Importing a Trusted Web Server Certificate and Appendix 4: HTTP Redirection for more information.

To globally redirect using HTTPS:

1. Select **Tools**>**Options** and then select **NAC**>**HTTP Redirection**.
2. Select **Redirect via HTTPS** to redirect using HTTPS. Alternatively, you can define individual HTTP actions to transmit via HTTPS.

Skip HTTP Redirect Confirmation Message

You can instruct CounterACT 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.

To configure the skip option:

1. Select **Tools**>**Options** and then select **NAC**>**HTTP Redirection**.
2. In the HTTP Redirection Settings section, 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.

To define:

1. In the HTTP pane, select **Monitor Proxy Ports for HTTP Notifications**.
2. Type the ports in the **Proxy Ports List** field. Use the following format: 80/TCP, 8080/TCP, 8888/TCP.
3. Select **Apply**.

Customizing HTTP Pages

Redirected web pages are generated by CounterACT users to interact with endpoints when specific actions are performed. At the endpoint, a default or customized web page replaces the page currently being displayed. The content inside the page is

configured when defining policy actions. See Chapter 7: Working with Actions for details.

Use the User Portal Builder when customizing the web pages displayed by the following CounterACT actions:

- HTTP Login
- HTTP Notification

For more information, see The CounterACT User Portal Builder.

When CounterACT is upgraded from versions earlier than 8.0.0, customizations created using the legacy CounterACT Customization Tool are preserved for these interfaces and are upgraded to the User Portal Builder. However, customization files that were configured manually and then copied to the CounterACT 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 CounterACT 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 CounterACT is upgraded 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.

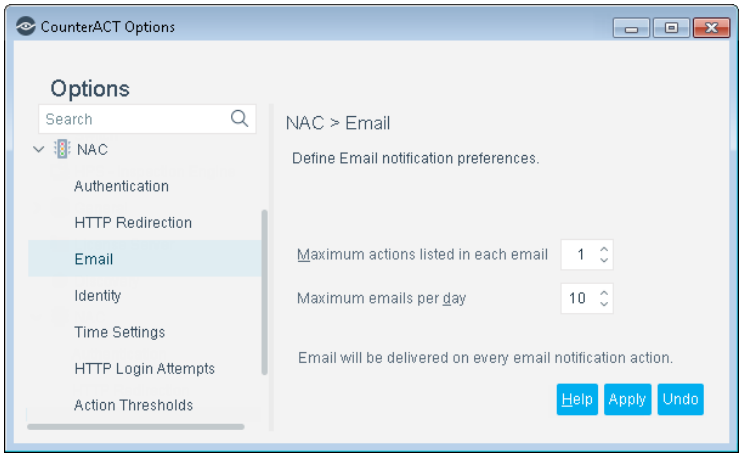
Default Settings

By default, up to ten emails can be sent within 24 hours, and one message is displayed in each email. This means, for example, that if there is activity early in the day and ten 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.

To update email delivery parameters:

1. Select **Options** from the **Tools** menu and then select **NAC**>**Email**.
2. Enter a value for **Maximum actions listed in each email** or use the spin controls to adjust the value. For example, to receive an email alert each time an events occurs, type **1** in the **Maximum actions listed in each email** field.
3. Type a value in the **Maximum emails per day** field or use the spin controls to adjust the value.
4. Select **Apply**.



Email Pane

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.

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. CounterACT 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 5-minute period specified on the same MAC address.

What happens 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, CounterACT activates the Admission based activation option for the IP address.

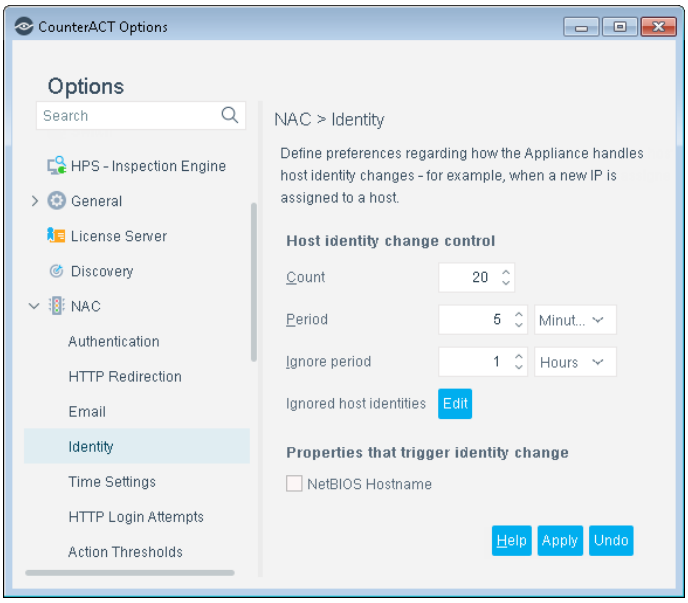
  The detection is displayed in the Detections pane with the same MAC addresses and the most current IP address detected.

What happens to the endpoint 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.

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.



Identity Pane

To update the threshold:

1. Select **Options** from the **Tools** menu and then select **NAC**>**Identity**.
2. Define any of the following options:

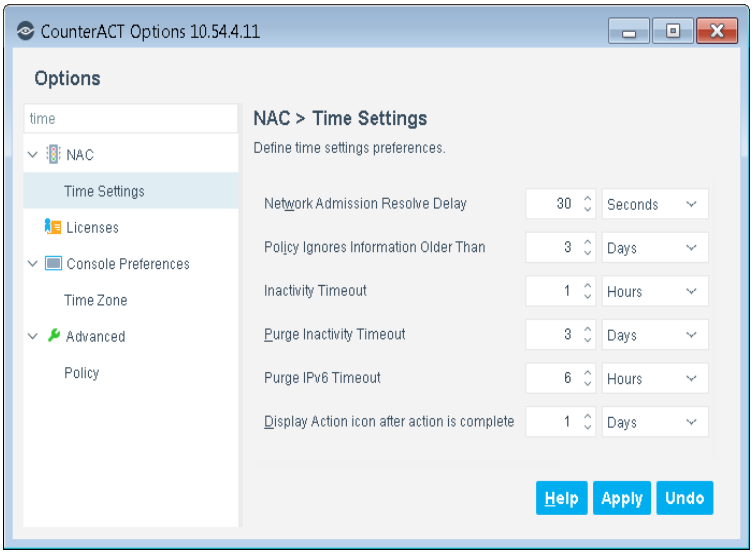
Count	The number of IP address changes that can occur before the threshold is passed.
Period	The time period during which identity changes can occur before the threshold is passed.
Ignore period	Endpoint identity change will be ignored for this period.

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.
NetBIOS Hostname	Apply the ignore mechanism and threshold definitions to NetBIOS names that change on the same IP address.

Time Settings

To access the Time Settings pane and update values:

1. Select **Options** from the **Tools** menu and then select **NAC**>**Time Settings**.
2. Use the spin controls for each time settings to select the desired value.



Time Settings Pane

Network Admission Resolve Delay

A delay time 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 rule evaluation will start when more details could be learned about the endpoint (after all services have loaded). You can update the delay default time.

If you set this value too high, your machines will not be checked immediately after admission. If you set the value too low, discovered information may not be accurate.

You can also set this value per policy. See Updating the Network Admission Resolve Delay in Main Rule Advanced Options for details.

Policy Ignores Information Older Than

This value is a specific time period that CounterACT *does not* see traffic at endpoints that were previously discovered by a policy. 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 CounterACT Switch Plugin, CounterACT uses the **Inactivity Timeout** option to resolve offline status. This is the time period that endpoints should be disconnected from the network in order for CounterACT 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 allows you to view and work exclusively with online endpoints.

If endpoints are connected to a switch that is managed by the CounterACT Switch Plugin, by default CounterACT detects offline status within one minute. Refer to the *Permissions Configuration* section of 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 CounterACT *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. This means, for example, the 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 CounterACT associates an IPv6 address with an endpoint. This timeout is measured from the time CounterACT learns the IPv6 address. If CounterACT 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 from CounterACT.

Display Action Icon after Action Is Complete

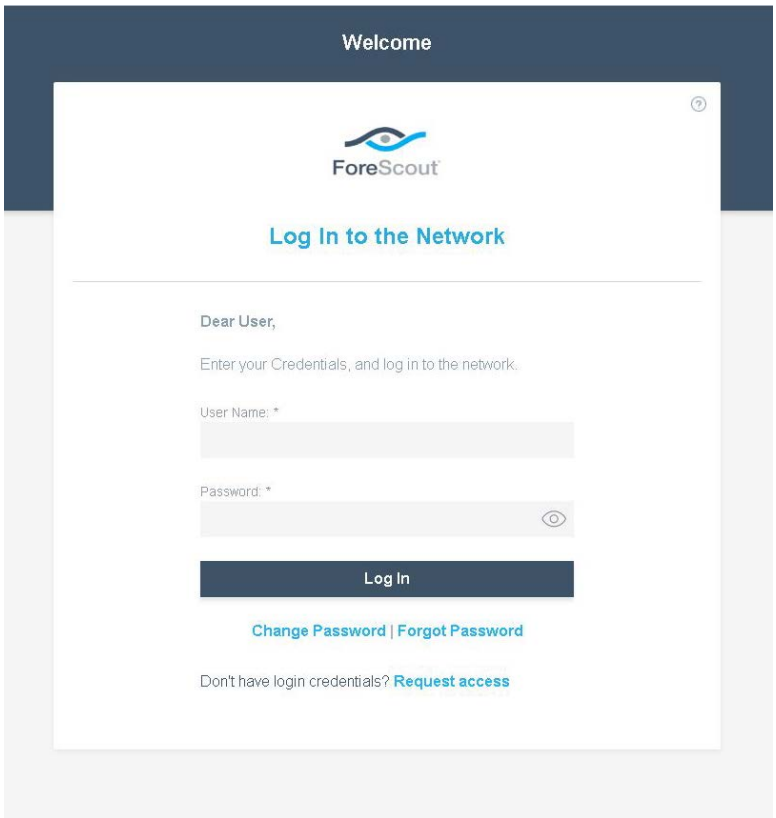
You can choose a time period to display an Action icon after a one-time action is complete. For example:

- After an email action is delivered
- After network users confirm reading redirected pages
- After users perform redirecting tasks

This feature helps you more quickly understand the endpoint status.

HTTP Login Attempts

Define a failed login limit for endpoint users attempting to log in via the CounterACT HTTP Login page. This page is triggered via the HTTP Login action.

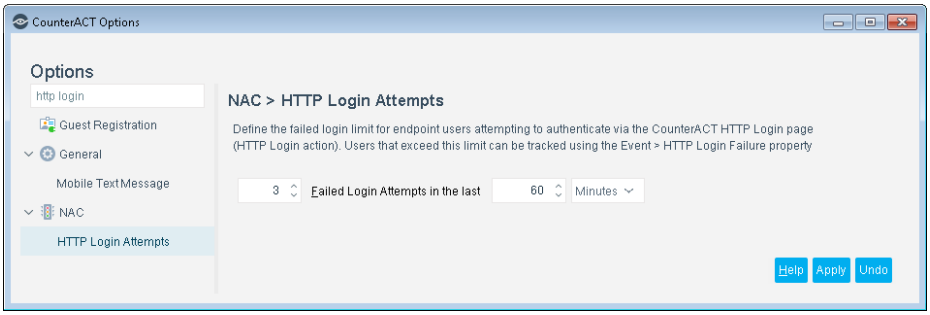


Login Page

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.

To define a limit:

1. Select **Options** from the **Tools** menu and then select **NAC > HTTP Login Attempts**.



HTTP Login Attempts Pane

2. Type 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 Lists for details.

Categorizing Policies

Assign policies to policy categories to:

- Help you organize and view policies in the Policy manager. For example, only display policies that have been labeled as Compliance policies. See Working with the Policy Manager.
- 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 Compliance and Corporate/Guest Control templates.

This section describes how to categorize other policies as either Compliance or Corporate/Guest.

Follow these guidelines:

1. Create a policy whose results you want to display in the Dashboard.
2. Categorize the policy as either *Compliance* or *Corporate/Guest*.
3. Label endpoints that *match* the policy sub-rules as follows:
   - Matched endpoints are Compliant / Not Compliant / Unlabeled
   - Matched endpoints are Authorized Guest / Unauthorized Guest / Corporate / Unlabeled

When working with policies that only have a Main Rule, label endpoints that either match or do not match the policy. For example, consider a policy detecting endpoints that have installed uTorrent – an unauthorized peer-to-peer application. Endpoints that match the policy can be labeled *Not Compliant* and endpoints that do not match the policy can be labeled *Compliant* or *Unlabeled*.

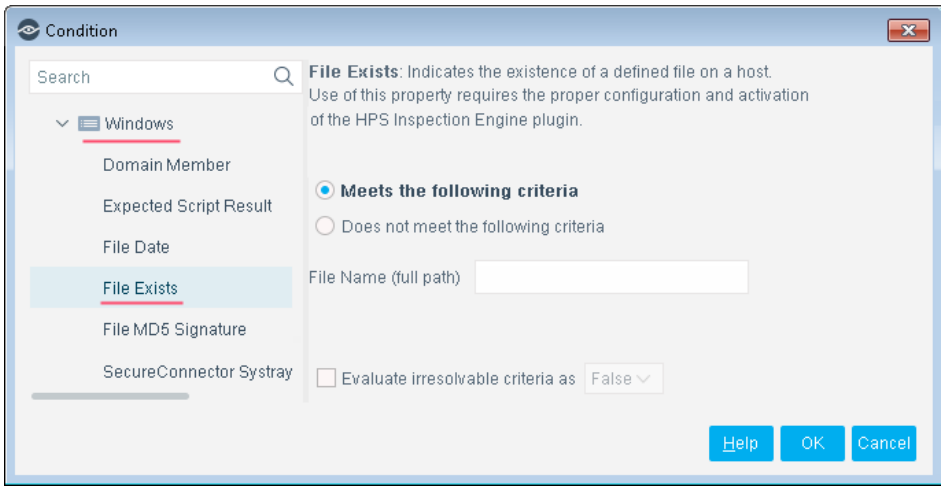
Working with Unlabeled Rules

Endpoints that are marked *Unlabeled* are not calculated. Endpoints may be unlabeled, for example, if they are defined as a necessary part of a rule or policy but do not fall into a useful category.

Sample Categorization and Labeling – Running Vital File on Windows Endpoint Policy

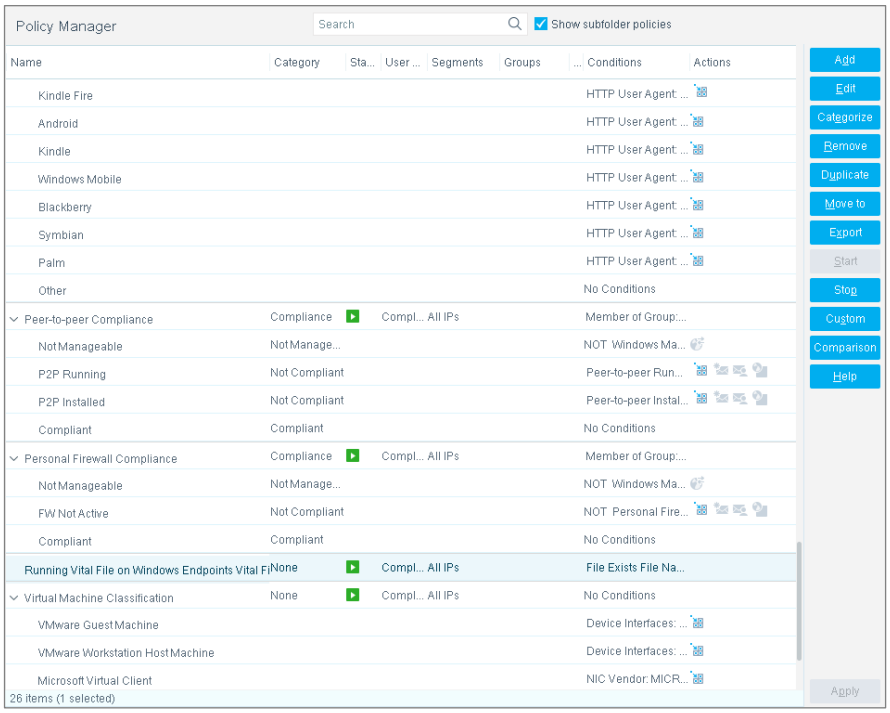
To categorize and label a policy:

1. Create a policy that verifies that a vital file is installed on endpoints Running Windows XP applications. Name the policy *Running Vital File on Windows Endpoints*.
2. Configure the Main Rule to discover endpoints running any Windows XP application.
3. Configure the sub-rule to verify that a certain file exits on these endpoints. Define the property so that endpoints with the file meet the property criteria.



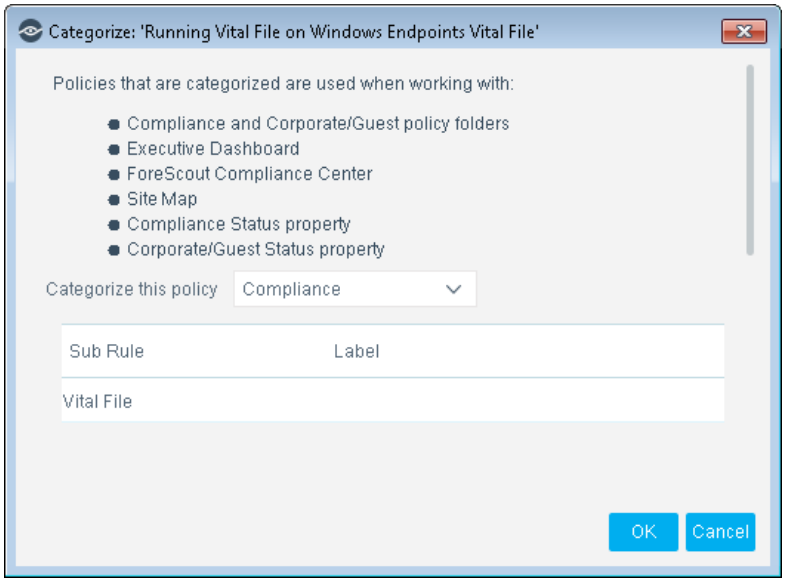
Rule Definitions

4. Finish creating the policy and select it from the Policy Manager.



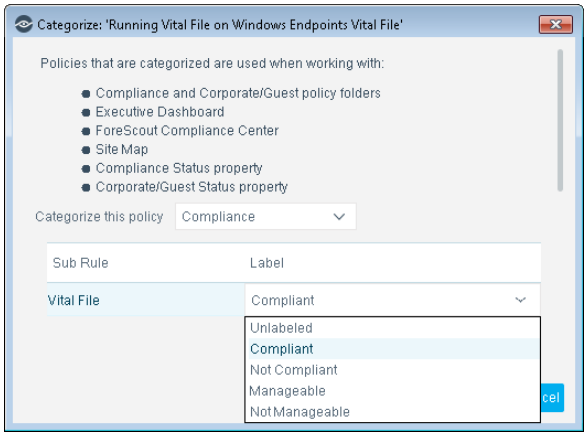
Policy Main Rule Selected

5. Select **Categorize**. The Categorize dialog box opens.
6. Select **Compliance** from the **Select a policy category** drop-down list.



Classify Dialog Box

7. Select the **Label** header and then select **Compliant**.



Sample Label

This means that endpoints with the vital file are calculated as compliant. Other endpoints are unlabeled.

8. Select **Unlabeled** if you do not want results to be calculated.

Policy Reports and Logs

This section describes:

- Policy Reports
- Policy Logs

Policy Reports

Two categories of reports are available:

- Policies summary
- Reports portal

Policies Summary

You can generate a report listing your policies and policy definitions.

To generate a summary of your policies:

1. Select **Policies Summary Report** from the **Reports** menu.

Reports Portal

The Reports Plugin lets you generate reports with 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 be used, for example, to help you understand:

- Long-term network compliance progress and 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.

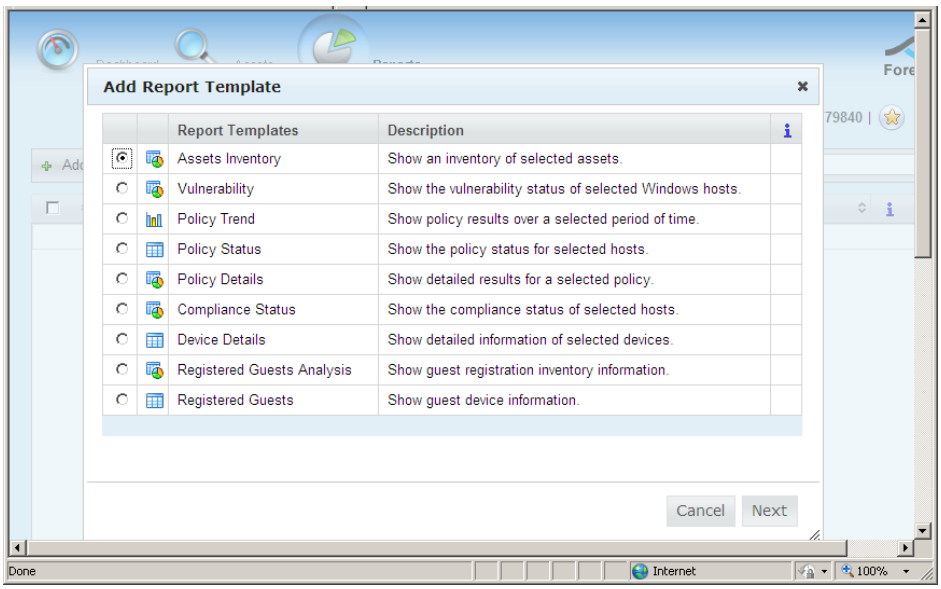
In addition, you can use any language supported by your operating system to generate reports. Reports can be viewed and printed as either PDF or CSV files.

To learn more about reports:

1. Select **Options** from the **Tools** menu.
2. Select **Modules** and then select **Reports**.
3. Select **Help**.

To generate reports:

1. Select **Reports** from the **Reports** menu. The Login page opens.
2. Enter the credentials that you use to log in. The home page opens. A variety of reports are available; for example, compliance and guest status reports or device and policy detail reports.



Reports

The Reports Portal is provided by the CounterACT Reports Plugin. Plugin updates may be available in between CounterACT version releases.

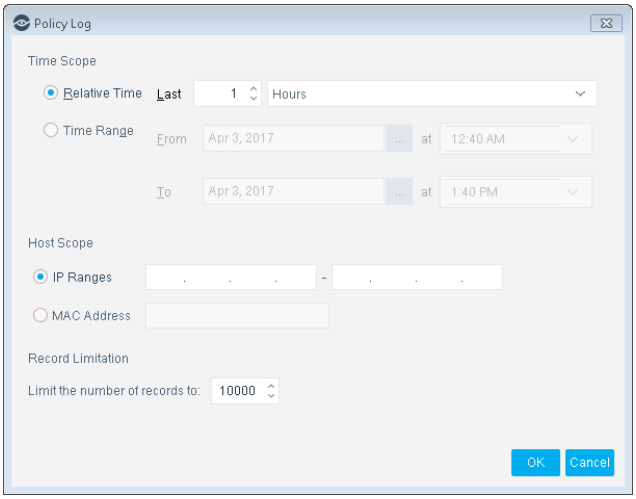
Policy Logs

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.

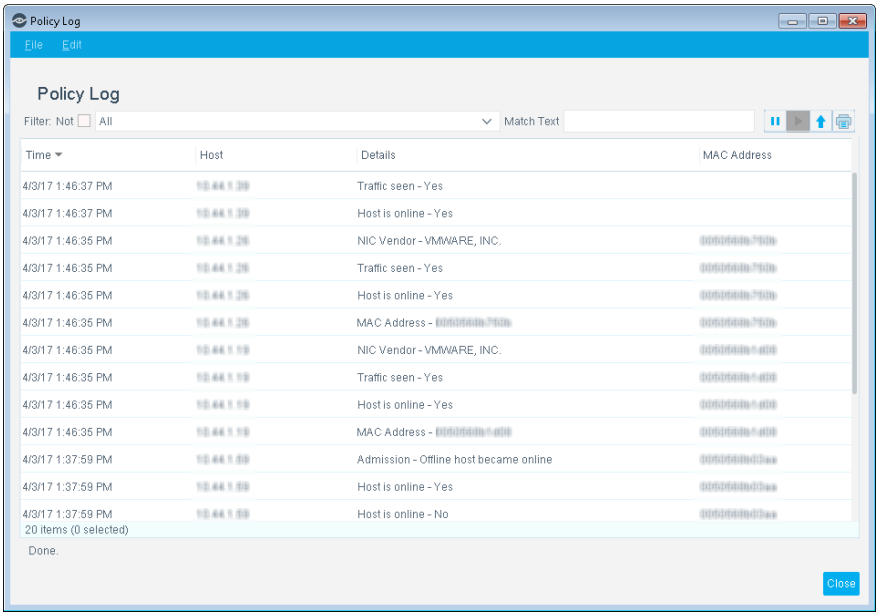
To open the log:

1. Select **Policy Log** from the **Log** menu.



Main Policy Log Dialog Box

2. Define a time scope and address range and select **OK**. A Log dialog box opens according to the range that you selected.



Policy Log Dialog Box

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 CounterACT device that detected the event.
MAC Address	The MAC address of the detected endpoint.

The following filter options are available:

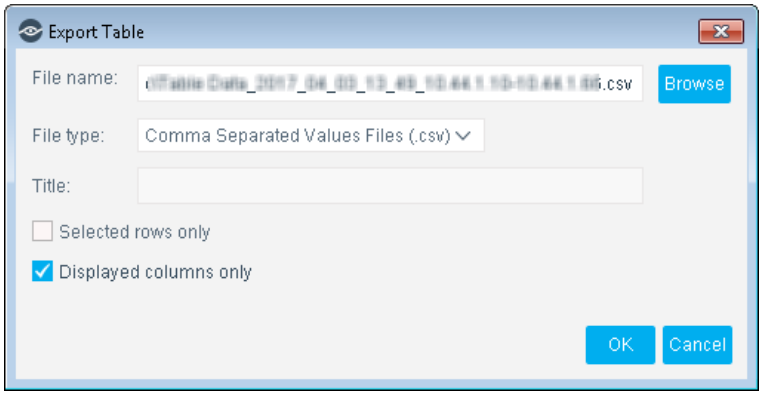
All	Display all log events.
Log	Contains detections, action execution and additional information.
Threat Protection	Displays endpoints detected via the Threat Protection Policy.
Only Changes	New, changed, rechecked property that was learned regarding to the selected IP address ranges.
Policy	The name 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 Working with System Event Logs for details.

Exporting the Log

You can export the log data or sections of it to a CSV file.

To export the data:

1. From the Policy Log dialog box, select **Export** from the **File** menu. The Export Table dialog box opens.



Save as CSV Dialog Box

2. Browse to the location for saving the file.
3. Configure the export options.

Export all information.	Do not select any checkbox.
Only export information displayed in the log. (This does not include information hidden via the Hide/Display column feature.)	Select **Displayed columns only**.
Select rows to export and export all related data. (Including information hidden via the Hide/Display column feature.)	Select **Selected rows only**.
Select rows to export but only export data displayed. (This does not include information hidden via the Hide/Display column feature.)	Select both checkboxes.

4. Select **OK**.

Policy Safety Features

Several safety features are available to help ensure that your policies efficiently handle endpoints.

- Working with Action Thresholds
- Handling Irresolvable Criteria
- Handling Criteria Defined as Empty Lists
- Misconfigured Add to Group Policy

Working with Action Thresholds

There are scenarios in which 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 anticipated.

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.

How It Works

1. CounterACT sets default thresholds for an action type.
2. CounterACT puts 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. See Managing Actions On-Hold on a Specific Device for details.
5. When the situation is remediated and the blocking limit falls below the threshold, you can cancel the on-hold status and continue blocking or remediating.
6. You can also manually select endpoints and cancel on-hold status.

You can also create threshold policy exceptions, i.e., policies that you would like to exclude from action threshold calculations. You can, for example, exclude all thresholds when working with policies that handle outside contractors.

How On-hold Calculations Are Made

Actions 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 Actions Covered and Threshold Percentages for details.
- The number of endpoints with an action assigned to them must be equal to or more than the minimal number of endpoints CounterACT is instructed to detect before calculating the threshold. By default, this number is ten. See Controlling the Counting Mechanism for details.

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 ten 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
VPN Block	1%
Wireless Host Block	1%
Kill Process on Windows	2%
Add to Blocking Exceptions list	2%
ACL	2%

Action	Default Threshold
Disable External Device	2%

To change a default:

1. Select the Configuration tab from the Options > NAC > Actions Thresholds pane.
2. Select **Custom** and type a value in the field.
3. Select **Apply**.

How Do I Know When a Threshold Violation Occurred?

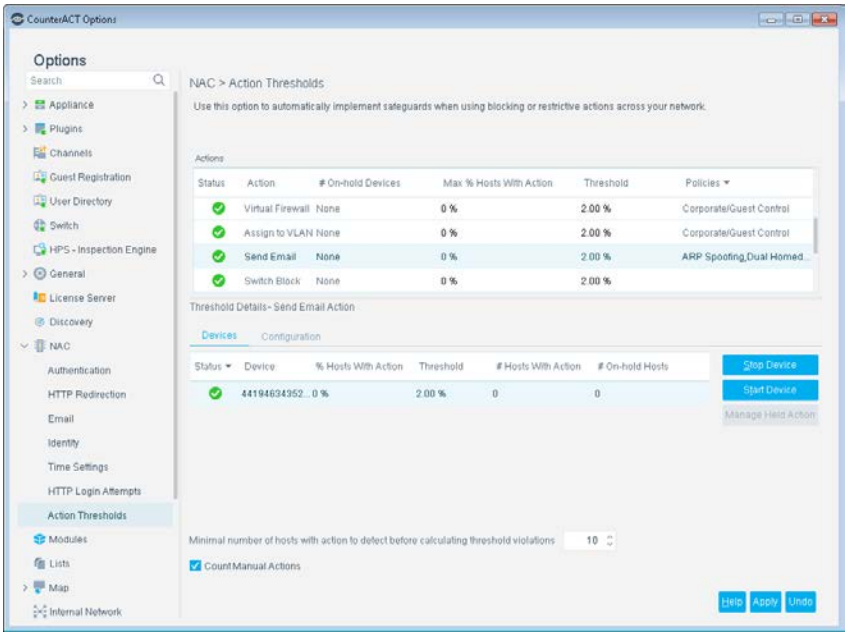
The action threshold indicator flashes if a threshold violation occurred.

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.

To work with action thresholds:

1. Select **Options** from the **Tools** menu and then select **NAC** > **Action Thresholds**.



Action Thresholds Pane

Actions Section

This section lists all the actions defined in your enterprise and provides related information.

Description	Action Name
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 checkmark 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** section.

Threshold Details Section

This section displays threshold information for an action that you selected in the **Actions** section; for example, the current number of endpoints that are 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 that you would like 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.

Devices Tab

Display threshold information for an action that you selected in the **Actions** section; for example, the current number of endpoints on hold at a specific device for the *Send Email* action.

Devices Tab

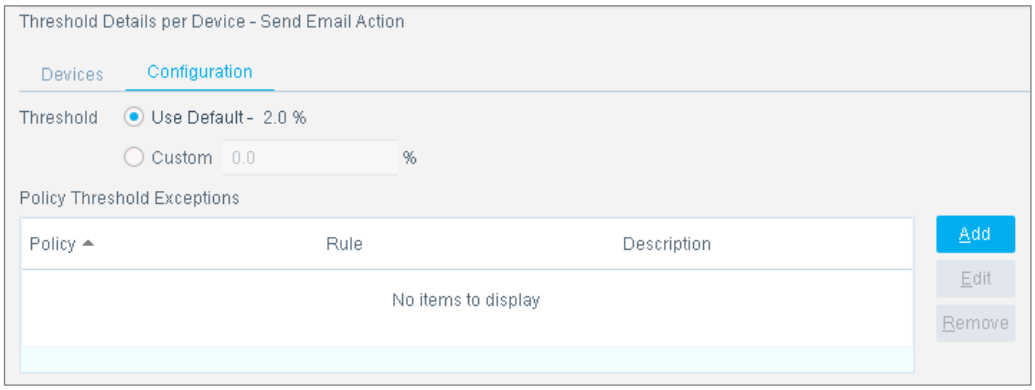
Item	Description
Status	The On-hold status for the action on the selected device. A green checkmark means that the action is *not* On-hold at this device. A blue icon indicates that it is.
Device	The device IP address.
Threshold	The current threshold for this action. Note that it is identical on all 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 CounterACT activity on endpoints is halted. You may decide to do this if you feel that the action is causing unexpected results.

Configuration Tab

Use the Configuration tab from the Options > NAC > Actions Thresholds pane to change the default configuration for the threshold and to create threshold policy exceptions – policies that you would like 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.

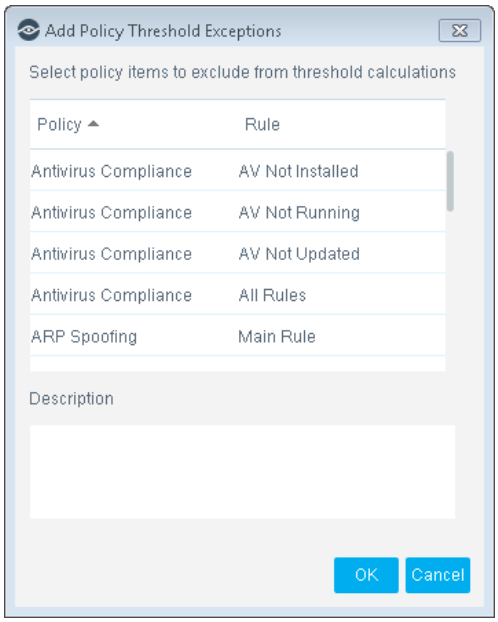


Configuration Tab

To create exceptions:

1. Select **Add**.

The Add Policy Threshold Exceptions dialog box opens.



Add Policy Threshold Exception

2. Select the policy items that you want to exclude from the threshold calculations.
3. Select **OK**.

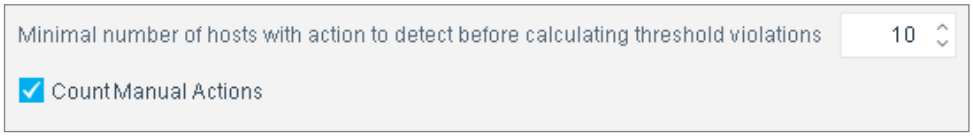
Controlling the Counting Mechanism

You can define the minimum number of endpoints that should be counted for an action before enforcing a threshold. For example, wait until 20 endpoints have been detected with a certain action before calculating the threshold. The number applies to all devices. The calculation is done by each device separately. The default is 10 endpoints.

In small enterprises where there are very few 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 be needed to be lowered.

To change the default:

1. Select the number that you want from the **Minimal number of hosts** field at the bottom of the NAC > Actions Thresholds pane.



Minimal Number of Hosts Setting

2. Select **Apply**.

Include or Exclude Endpoint Manually Assigned an Action

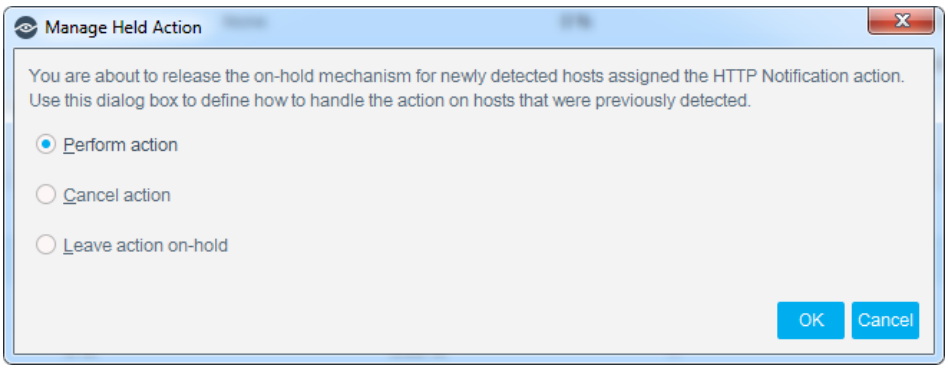
By default, endpoints that have manually been assigned actions are included in the endpoint count. To exclude these endpoints, clear **Count Manual Actions** from the bottom of the Actions Thresholds pane.

Managing Actions On-Hold on a Specific Device

If too many actions are not being carried out, you can perform a procedure to release the On-hold mechanism on endpoints that were previously detected.

To release the On-hold mechanism:

1. Perform one or more of the following:
   - 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 the Options > NAC > Actions Thresholds pane.
2. Select a device from the **Threshold Details** section of the Options > NAC > Actions Thresholds pane.
3. To cancel the On-hold mechanism for the action on the device, select **Manage Held Action**. A dialog box opens letting you instruct CounterACT to handle the action on endpoints that were previously detected. Three options are available:
   - Perform the action.
   - Cancel the action. The action remains cancelled until it is either deleted or unmatched to a policy and then matched.
   - Leave the action on-hold.



Manage Held Action Dialog Box – Switch Block Action

After releasing the on-hold mechanism, you can continue blocking or restricting newly detected endpoints.

Approve Actions on Specific Endpoints

You can release the On-hold status for specific endpoints and approve the action.

To approve:

1. Sort the Detections pane via the Actions column.
2. 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.
3. Right-click the endpoint and select **Approve Actions**. Select the action that you want to release from On-hold.

Handling Irresolvable Criteria

In some situations, CounterACT cannot properly resolve endpoint property criteria. Such criteria are considered *irresolvable criteria*.

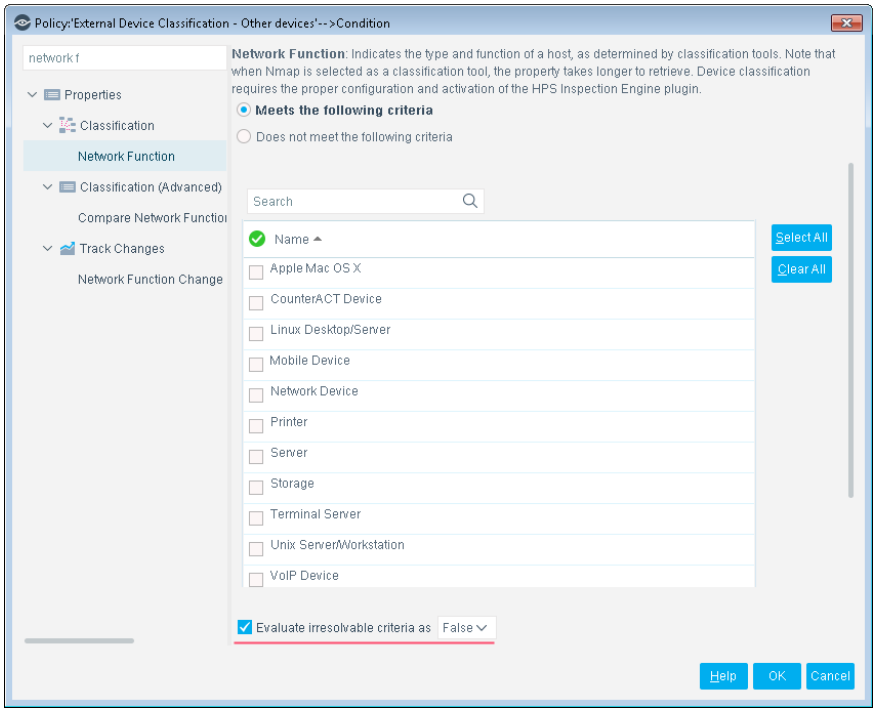
What Causes Criteria to Be Irresolvable?

Property criteria can have a status of Irresolvable for one of two reasons:

- CounterACT failed to resolve the criteria.
- A system error caused CounterACT not to respond to the resolve request (e.g. a plugin is not running, or experienced a timeout).

How Are Irresolvable Criteria Handled?

Many properties provide an option for handling *irresolvable criteria*. If CounterACT cannot verify a property, you can choose how to resolve that endpoint.



Irresolvable Criteria

You can instruct CounterACT to handle irresolvable criteria as follows:

True	The endpoint will match the criteria defined for the property.
False	The endpoint will not match the criteria defined for the property.

*If you do not select the **Evaluate irresolvable criteria as** option, the criteria will be handled as irresolvable. This means that the endpoint will not be further analyzed. The endpoint is not checked to see if it matches additional condition* criteria.

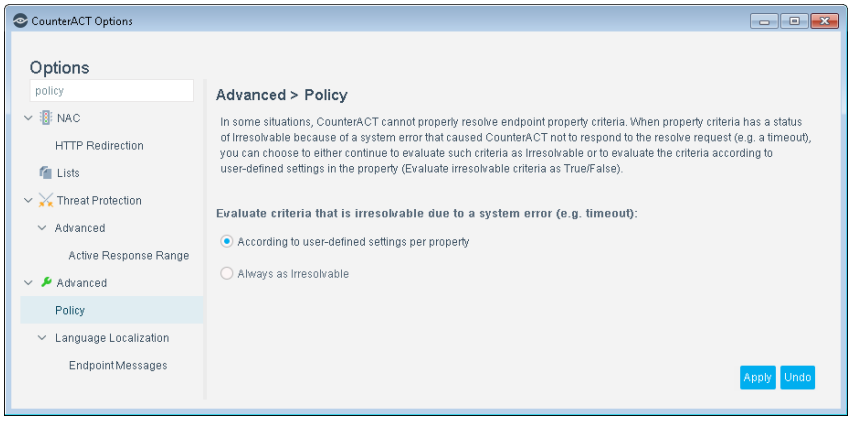
Irresolvable Criteria: System Errors

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 choose to change this default setting. Because this status did not stem from an actual failure to resolve, but rather because 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. This means that the endpoint will not be further analyzed and the endpoint is not checked to see if it matches additional condition criteria.

To evaluate criteria that is irresolvable due to a system error:

1. Select **Options > Advanced > Policy.**



Advanced > Policy Pane

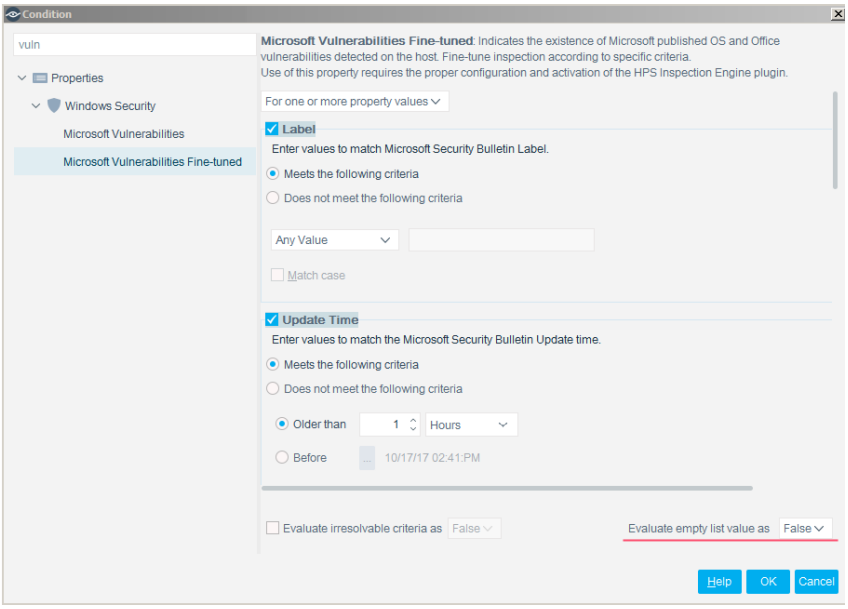
2. Select **Always as Irresolvable** to continue to evaluate Irresolvable criteria as such when the evaluation was caused by a system error.

   By default, *According to user-defined settings per property* is selected. When this is selected, all irresolvable criteria are evaluated according to the user-defined settings configured in the property.

Handling Criteria Defined as Empty Lists

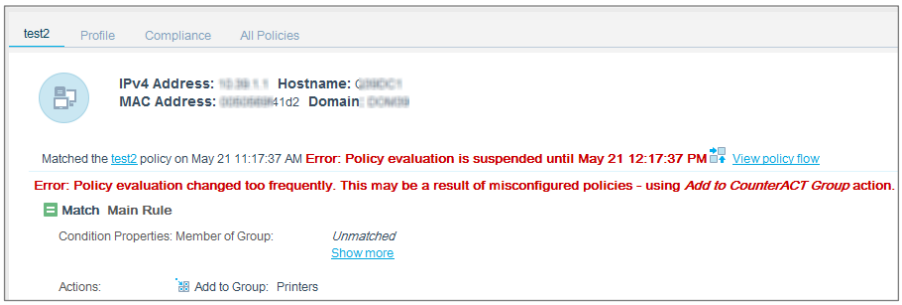
Properties are used to evaluate specific information on an endpoint. If a property must evaluate information that is not contained on the endpoint, CounterACT evaluates the property as an *empty list*. You can choose to evaluate properties with empty list values as either true or false.

For example, the *Microsoft Vulnerabilities Fine-tuned* property detects all the Microsoft vulnerabilities on an endpoint and evaluates them. If the endpoint has no Microsoft vulnerabilities, the property has nothing to evaluate. This situation, known as an *empty list*, returns an evaluation of *False* by default. You can change the *Evaluate empty list value as* option to *True*.



Misconfigured Add to Group Policy

Users may unknowingly create invalid policies. For example, when the *Not a Member of Group* condition and the *Add to Group* action are configured in the same policy. A policy error message is displayed in the Details pane when CounterACT detects this kind of misconfiguration.



Invalid Policy Notification

Chapter 6: Working with Policy Conditions

- About Policy Conditions
- Working with Properties
- Detecting New Vulnerabilities and Newly Supported Vendor Applications
- Defining Custom Conditions
- Comparing Property Results
- Defining and Managing Lists

About Policy Conditions

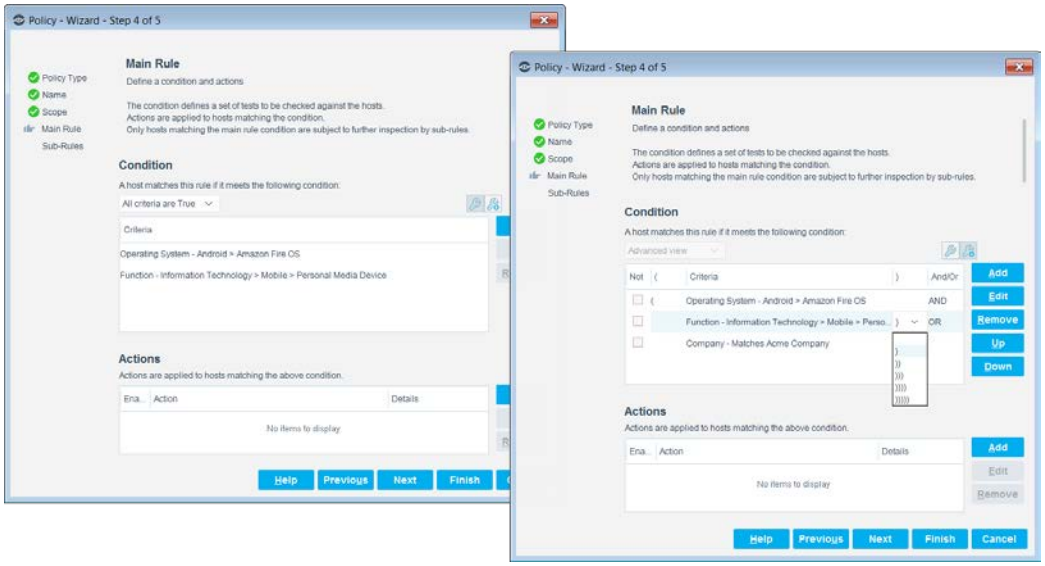
This section describes what policy conditions are and how to work with them. The following subjects are covered:

- What Is a Policy Condition
- Meeting Condition Criteria
- Condition Shortcuts
- Irresolvable Criteria
- Case Sensitivity
- Properties
- Property Expression Types
- Properties and Scripts
- Windows Endpoint Applications Vendor Support

What Is a Policy Condition?

A policy condition is a predefined set of endpoint properties and Boolean logic (***AND***, ***OR***, ***NOT***) connecting them; for example, endpoints running Windows XP with outdated Symantec AntiVirus applications. You can instruct CounterACT to apply a policy action to endpoints that match (or do not match) criteria that you choose for the condition. If the Boolean expression that you create is too complex, CounterACT issues a warning and does not follow through with it.

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.



Standard and Advanced View of Condition Settings

Meeting Condition Criteria

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. 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.

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 more information.
- 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 more information.

Irresolvable Criteria

In some situations, CounterACT cannot properly resolve endpoint property criteria. Many properties provide an option for handling such *irresolvable criteria*. If CounterACT cannot verify a property, you can choose how to treat that endpoint. See Handling Irresolvable Criteria for more information.

Case Sensitivity

Select **Match case** if you want the condition property value to be case sensitive.

Properties

A property is an attribute detected on the endpoint; for example, device and operating system information or information about switch connections or user directly information. CounterACT supports an extensive range of endpoint and network device properties. If you have installed a Module (including Content Modules and Extended Modules), related properties are also available. For example, if you installed the ForeScout Extended Module for McAfee ePolicy Orchestrator, related properties and actions are available.

Using properties lets you quickly and efficiently pinpoint endpoint and network devices.

See Working with Properties for a complete list of properties.

Property Expression Types

You may want to detect certain properties on endpoints, but may not be certain of the precise property values; for example, the exact spelling of a vendor or precise version information. To help you deal with these situations, several *property expression* options are available.

- Contains
- Starts or Ends with
- Greater than
- Matches
- Matches expression
- In List (See Defining and Managing Lists)
- Any Value

Properties and Scripts

The following properties use scripts:

- Windows Expected Script Result
- Device Interfaces
- Number of IP Addresses
- External Devices
- Windows File MD5 Signature
- Windows Is Behind NAT
- Microsoft Vulnerabilities

Scripts are not required if the endpoint is managed by SecureConnector.

Refer to the *HPS Inspection Engine Configuration Guide* for details about working with scripts. Select **Options** from the **Tools** menu, select **HPS Inspection Engine** and then select **Help**.

Windows Endpoint Applications Vendor Support

In addition to general endpoint discovery capabilities, CounterACT provides specialized tools for in-depth discovery and management of the following Windows application types:

- Windows Antivirus vendors
- Windows Peer-to-Peer vendors
- Windows Instant Messaging vendors
- Windows Anti-Spyware vendors
- Windows Personal Firewall vendors

Use CounterACT policies to discover endpoints running these applications, and to apply remediation actions.

Refer to the *Windows Applications Configuration Guide* for more information about the module. Select **Options** from the **Tools** menu. Select **Modules**. Select **Windows Applications** and then select **Help**. Vendor application support may be updated with new Windows Applications releases. See Detecting New Vulnerabilities and Newly Supported Vendor Applications for details.

Working with Properties

Conditions include one or more *properties*. A property is an attribute detected on the endpoint. The following categories of properties are available by default with CounterACT:

- Authentication Properties
- Classification Properties
- Advanced Classification Properties
- Device Information Properties
- Event Properties
- External Devices Properties
- Guest Registration Properties
- Linux Properties
- Macintosh Properties
- Remote Inspection Properties
- SNMP Properties
- Switch Properties
- Track Changes Properties
- User Directory Properties
- Windows Properties
- Windows Application Properties
- Windows Security Properties

Properties Delivered with Plugins and Extended Modules

In addition to the properties delivered with your CounterACT system, other properties may become available when you install modules and Extended Modules. For example, if you are working with the CounterACT Wireless Plugin or the CounterACT FireEye HX Extended Module, properties delivered with these components will be available. Properties are described in related Configuration Guides, and not in this chapter.

To read about properties delivered with plugins and Extended Modules:

1. Select **Options** from the **Tools** menu.

2. Select **Modules** and select the plugin you are working with.
3. Select **Help**. The configuration guide for your plugin opens.

Refer to the related plugin or Extended Module Configuration Guide for details about these properties. See Additional CounterACT Documentation for information on how to access this guide.

See Chapter 8: Base, Content and Extended Modules for information about working with plugins and Extended Modules.

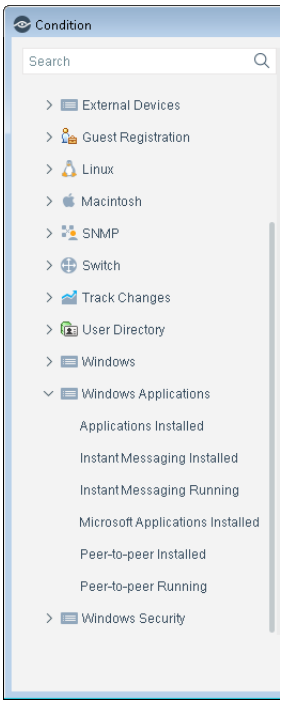
Querying for Property Values

CounterACT Appliances must regularly query endpoints to keep property values up to date. This can generate significant network traffic. The following methods are provided to minimize traffic:

- In general, endpoints are polled for property values only when the a policy that includes the property is being 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 CounterACT, and significantly reduces redundant network traffic.

To define properties:

1. Select **Add** from the **Condition** section of the Sub-Rules dialog box.



Condition Dialog Box

2. Select a property type from the **Select Property** section and define the property value. When defining properties, indicate if the endpoint meets the criteria defined or does not meet the criteria. The properties are detailed below.
3. Select **OK**. The Conditions dialog box reopens.

Authentication Properties

Property	Description
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	The value of the Valid To field of the certificate installed on the endpoint for certificate-based authentication.
Authentication Certificate Issuer	The value of the Issuer field of the certificate installed on the endpoint for certificate-based authentication.
Authentication Certificate Root CA Subject	The value of the Subject field of the certificate installed on the endpoint for certificate-based authentication.
Authentication Certificate Serial Number	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	The value of the Subject field of the certificate installed on the endpoint for certificate-based authentication.
Authentication Certificate Subject Alternate Name	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. CounterACT supports the following authentication services: HTTP(80/TCP), Telnet(23/TCP), NetBIOS(139/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 more information.

Property	Description
Authentication Login (Advanced)	Indicates endpoints that logged in to the network using a specific protocol or against a specific server. Type the protocol name or the server IP address. Servers referenced here must be defined in the Authentication pane. See Defining Authentication Servers for more information.
HTTP Confirmation Events	Indicates whether the end user confirmed an HTTP notification message generated by CounterACT. Confirmation is discovered via the Confirmation Identifier name, defined in the *HTTP Notification* action. Type 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 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. ▪ Are signed-in as guests. ▪ Are signed-out or never signed in.

Classification Properties

Property	Description
Function	Indicates the most specific function in the CounterACT 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. Note that 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 Notes* for more information.

Property	Description
Operating System	Indicates the most specific operating system in the CounterACT 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' checkbox.
Vendor and Model	Indicates the most specific vendor and model in the CounterACT 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' checkbox.

Advanced Classification Properties

Property	Description
Service Banner	Indicates the service and version information, as determined by Nmap. Note that 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 if the *Function* classification property was determined by the Device Classification Engine, or was set by an action.
Operating System Classified By	Indicates if the *Operating System* classification property was determined by the Device Classification Engine, or was set by an action.
Function Classification Update	Indicates if 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 Options > Device Profile Library window.

Property	Description
Operating System Classification Update	Indicates if 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 Options > Device Profile Library window.
Vendor and Model Classification Update	Indicates if 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 Options > Device Profile Library window.
Suggested Function	If there are multiple candidates for the endpoint's *Function* classification, then this property indicates all the profiles in the CounterACT Device Profile Library that match this endpoint. These values were 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, then this property indicates all the profiles in the CounterACT Device Profile Library that match this endpoint. These values were 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. Note that 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 Fingerprint to (Classification Version 3)	Indicates the difference between current OS Fingerprint and OS Fingerprint 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

Property	Description
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

Property	Description
Access IP	Indicates the endpoint IP address that CounterACT 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 allows you to 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. CounterACT matches only endpoints that satisfy the matching condition during the specified time period.
Comment	Indicates devices that contain device *Comment* text defined by the CounterACT user. (Right-click an endpoint from the Detections pane to add a comment. The comment is retained for the life of the endpoint in CounterACT.)
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.

Property	Description
Counter	This property 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.
CounterACT Script Result	This condition runs a script or command on the CounterACT appliance, and examines the result. CounterACT 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 CounterACT 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 CounterACT 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 set CounterACT to the Partial Enforcement mode, this condition will not work. See Working with the Enforcement Mode for more information.
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 CounterACT, 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 Classifier Plugin Configuration Guide. Select **Options** from the **Tools** menu. Select **Modules**. Select this 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.

Property	Description
IPv4 Address IPv6 Address	Indicates one or more IP addresses of an endpoint. Matching criteria include: ▪ Any IP address ▪ Addresses in a named CounterACT 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 CounterACT 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 Working with Hosts Whose IPv4 Address Is Used by Another Host
MAC Address	Indicates the MAC address of the endpoint.
Member of Group	Allows you to investigate endpoints that are part of a group.
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 CounterACT based on the MAC prefix. The HPS NIC Vendor DB updates vendor information used to resolve this property. CounterACT can automatically add newly supported vendors to a policy condition that you create with this property. For more information about this plugin, select **Options** from the **Tools** menu. Select **Modules**. Select this 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. CounterACT can automatically add newly supported vendors to a policy condition that you create with this property. For more information about this plugin, select **Options** from the **Tools** menu. Select **Modules**. Select this plugin and then select **Help**
Number of IPv4 Addresses Number of IPv6 Addresses	Indicates the number of IP addresses of each type that CounterACT detected for an endpoint. You can specify IPv4 addresses to ignore when calculating the Number of IPv4 Addresses property. See "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.

Property	Description
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 CounterACT 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	This property 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	This property 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. CounterACT 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, CounterACT 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 CounterACT 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 CounterACT to ignore the parameter.

Property	Description
SSH Command Output	▪ SSH Username/SSH Password - Specify credentials used to log in and establish an SSH session on the endpoint. Note that 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 CounterACT 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. Note that 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 CounterACT waits after submission of each command for an output response. ▪ Login timeout - The maximum interval, in seconds, that CounterACT 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 CounterACT establishes an SSH session on the endpoint, it submits the first command listed in the **Interactive Session Script** field. CounterACT 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, CounterACT ends the interactive session. ▪ If the output matches the expected response, CounterACT submits the next command in the session script. CounterACT 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.

Property	Description
	NOTE: Enter *UNUSED* in a field if you want CounterACT to ignore the parameter
Traffic seen	Indicates the most recent time network traffic was 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 page 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 CounterACT 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 CounterACT 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

Property	Description
ARP Spoofing	Indicates whether the number of different MAC address reported for an IP address becomes greater than 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. ARP spoofing 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 in CounterACT Technical Note* for more information about configuring your environment for detecting ARP spoofing. See Additional CounterACT Documentation for information on how to access this guide.

Property	Description
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 will initiate the activation. The default time period can be changed. See Policy Preferences for more information. ▪ 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	Refers to 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 Chapter 12: Threat Protection for more information.
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 will be displayed in the Console without an IP address, until it reconnects.
Sessions as Client / Sessions as Server	*Sessions* let you run policies based on real-time identification of network traffic patterns between servers and clients, allowing you to pinpoint: ▪ When session 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

Property	Description
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

Property	Description
Guest Account Approve Date	Indicates when the guest network access was approved.
Guest Approved By	For users who were 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 detailed information about administering guest tags.

Property	Description
Guest Registration Information	For users who were 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.

Linux Properties

Property	Description
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. Type 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 the existence of a defined file on an endpoint.
Linux File Size	Indicates the size (in bytes) of a defined file on a Linux device. Type a single file size or a range of sizes; for example, 1-100. Use a dash when defining a range.
Linux Hostname	Indicates the Linux host name.
Linux Manageable (SSH Direct Access)	Indicates whether the endpoint is connected to CounterACT via SSH.
Linux Manageable (SecureConnector)	Indicates whether the endpoint is connected to CounterACT via SecureConnector.
Linux Processes Running	Indicates whether a process is currently running on detected endpoints.

Property	Description
Linux User	Indicates whether the user is directly logged in to the Linux console.
Linux Version	Indicates the specific version of the Linux OS running on the endpoint. Use of this property requires that the endpoint be managed via SecureConnector.

Macintosh Properties

The OS X Plugin supports the following properties for Mac OS X endpoints.

Property	Description
Macintosh Applications Installed	Indicates whether a specified application is installed on an OS X endpoint. It parallels the Windows Applications Installed host property for Windows endpoints. This property is only reported for Mac OS X endpoints managed by the OS X Plugin.
Macintosh Expected Script Result	Use this property to run a command or file that will 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. 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 File Date	Indicates the last modification date and time of a defined file on an endpoint.
Macintosh File Exists	Indicates the existence of a defined file on an endpoint.
Macintosh File Size	Indicates the size (in bytes) of a defined file on a Macintosh device. Type a single file size or a range of sizes; for example, 1-100.
Macintosh Hostname	Indicates the Macintosh host name.
Macintosh Manageable (SSH Direct Access)	Indicates whether the endpoint is connected to CounterACT via SSH.
Macintosh Manageable (SecureConnector)	Indicates whether the endpoint is connected to CounterACT via SecureConnector.
Macintosh Processes Running	Indicates whether a process is currently running on the detected endpoints.
Macintosh SecureConnector Version	Indicates the version of the SecureConnector package that is running on the endpoint.
Macintosh Software Updates Missing	Indicates Macintosh security and other updates that are missing on the detected endpoint.
Macintosh User	Indicates whether the user is directly logged in to the Macintosh console.

Property	Description
Macintosh Version	Indicates the specific version of the Macintosh OS running on the endpoint. Use of this property requires that the endpoint be managed via SecureConnector.

Remote Inspection Properties

The following properties indicate which management services are available on the endpoint that CounterACT can use to perform Remote Inspection.

Property	Description
MS-RRP Reachable	Indicates whether CounterACT can use the Remote Registry Protocol for Remote Inspection tasks on the endpoint.
MS-SMB Reachable	Indicates whether CounterACT can use the SAMBA protocol for Remote Inspection tasks on the endpoint.
MS-WMI Reachable	Indicates whether CounterACT 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:

-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).

Property	Description
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, type 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, type 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, type 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, type 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, type 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 CounterACT. 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:

Property	Description
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.
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.
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 actions (*Blocked* or *Assign to VLAN*) that are 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 Configurations	*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.
Switch Port Connect	The physical connectivity between the endpoint and the switch port.
Switch Port PoE Connected Device	*For use with Cisco devices only*. Description of the PoE device that is connected to the PoE-enabled switch port, as provided by the managed Cisco switch. For example, Cisco IP Phone 6921.

Property	Description
Switch Port PoE Power Consumption	*For use with Cisco devices only*. Power consumption of the PoE device that is connected to the PoE-enabled switch port, as provided by the managed Cisco 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)`**.

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:

Property	Description
Running Config	*For use with Cisco devices only.* Detects *running config* information of switches managed by CounterACT, 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.

Property	Description
Running Config Time	*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	*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 CounterACT detects if 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
- Company
- Department
- Display Name
- Distinguished Name
- Email
- Employee Number
- Initials
- Last Name
- LDAP User Name

- Member Of
- Mobile Phone
- Password Last Set
- Phone
- Street Address
- Title
- User Given Name

Windows Properties

Property	Description
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	Use this property to run a command or file that will 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, type 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. This property may be used on managed Windows machines only. Running a script is performed 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. Select **Options** from the **Tools** menu. Select **Modules**. Select this plugin and then select **Help**. 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 the specific file, from a specific date, to exist 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 to endpoints with specific MD5 signatures.

Property	Description
Windows File Size	Indicates to a file name and size (in bytes). Use this property to check that endpoints on the network have a specific file, and 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.
NetBIOS Membership Type	Indicates whether the endpoint is a domain or workgroup member.
Windows Registry Key Exists	Indicates the existence of a specified Windows registry key. Note that 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. Note that 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 SecureConnector Systray Display	Indicates the SecureConnector visible mode installed on the endpoint.

Property	Description
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 CounterACT users stop unwanted data from propagating across the network. This property returns the name of the directory.
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 Manageable Domain	Indicates whether CounterACT 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 CounterACT 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 CounterACT SecureConnector is running on the endpoint. See Start SecureConnector / Stop SecureConnector for more information. When an endpoint with multiple interfaces connects to CounterACT through one NIC, only that host (NIC) is reported by this property. When CounterACT policies apply an action 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	Refers to Windows processes running on inspected endpoints.
Windows Services Installed	Indicates whether a specific Windows service is installed on a Windows endpoint. This property resolves the name of the service.
Windows Services Running	Indicates whether a specific service is currently running on a Windows endpoint. This property returns the name of the service. Note that this property relates to Windows services, not regular processes.

Property	Description
Windows Version	Refers 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_edition>:<target_sw>:<target_hw>:<other>** 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 of these properties.

To create policy conditions based on these properties, choose from the list of supported third-party applications. ForeScout 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 configure. CounterACT to automatically add newly supported vendor applications to a policy condition that you create with these properties. See Detecting 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.

Use other host properties to create conditions that inspect endpoints and detect files or processes of unsupported applications.

Property	Description
Windows Applications Installed	Indicates which applications are installed on the Windows endpoint via Add/Remove Programs. This property resolves the name of the applications, and their version number if available.

Property	Description
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 configure CounterACT to automatically add newly supported vendors to a policy condition that you create with these properties. See Detecting New Vulnerabilities and Newly Supported Vendor Applications for details.

Property	Description
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	Refers to 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:

Property	Description
	▪ 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. CounterACT can automatically add newly supported vulnerabilities to a policy condition that you create with this property. See Detecting 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	Indicate 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.

Detecting New Vulnerabilities and Newly Supported Vendor Applications

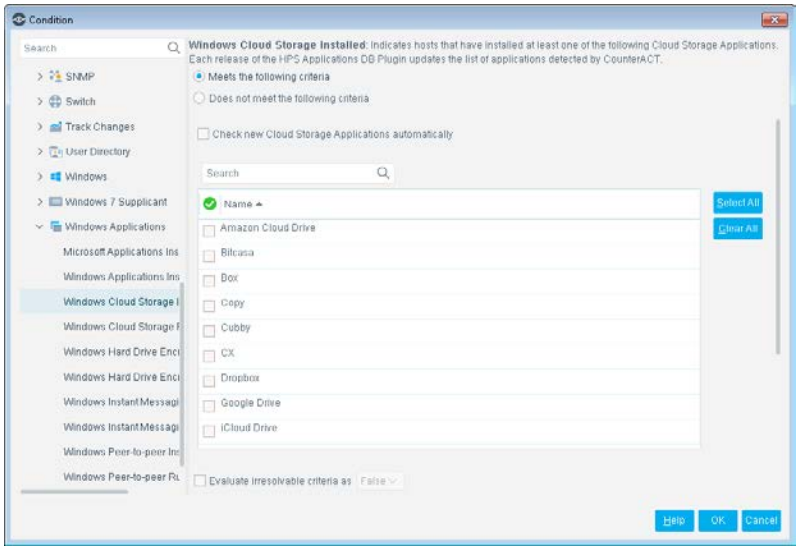
You can instruct CounterACT to automatically detect new Microsoft vulnerabilities and newly supported vendor applications on your network endpoints.

For example:

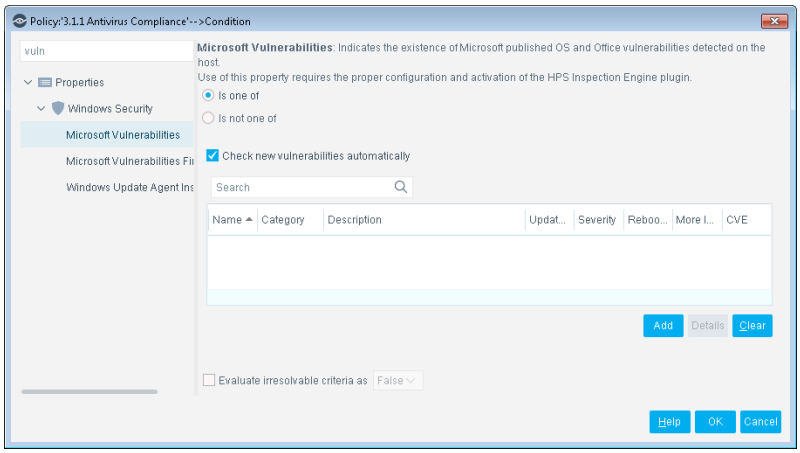
- When working with the *Windows Applications>Cloud Storage Installed* property in your policies, CounterACT will automatically detect any Cloud storage applications of newly supported vendors.
- When working with the *Windows Security >Microsoft Vulnerabilities* property in your policies, CounterACT will automatically detect new Microsoft published OS and Office vulnerabilities.

To detect new vulnerabilities and newly 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. See Additional CounterACT Documentation for information on how to access this guide.
2. Select the Microsoft Vulnerabilities property or a Windows application property that includes the **Check new...** option.



Cloud Storage Installed - Check New...



Microsoft Windows Vulnerabilities - Check New...

3. Select the **Check new…** checkbox.
4. Select **OK**.

Windows Applications Content Module Release Notes. Refer to the *Windows Applications Configuration Guide* for a complete list of supported vendors. Select **Options** from the **Tools** menu. Select **Modules**. Select **Windows Applications** and then select **Help**.

Defining Custom Conditions

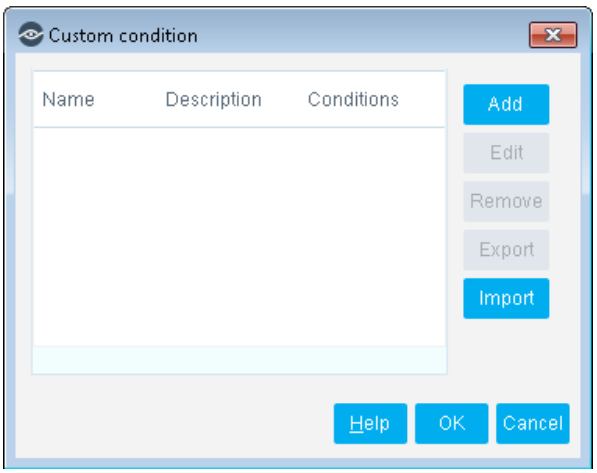
Customized, user-defined conditions are sets of conditions that you create and can reuse in any of your policies. This saves you the trouble of redefining complex conditions.

They can be created and used in any of your policies. Conditions can be imported and exported as XML files.

Defining customized conditions cannot be used in the middle of other wizard actions.

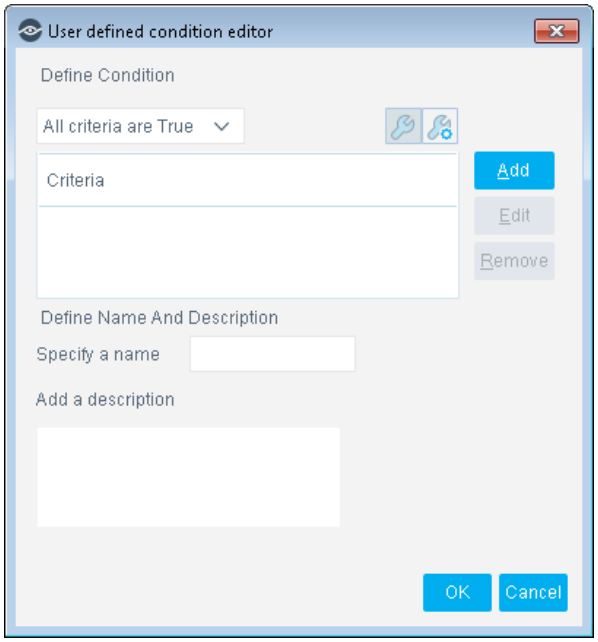
To create custom conditions:

1. Select **Custom** in the Policy Manager. The Custom Condition dialog box opens.



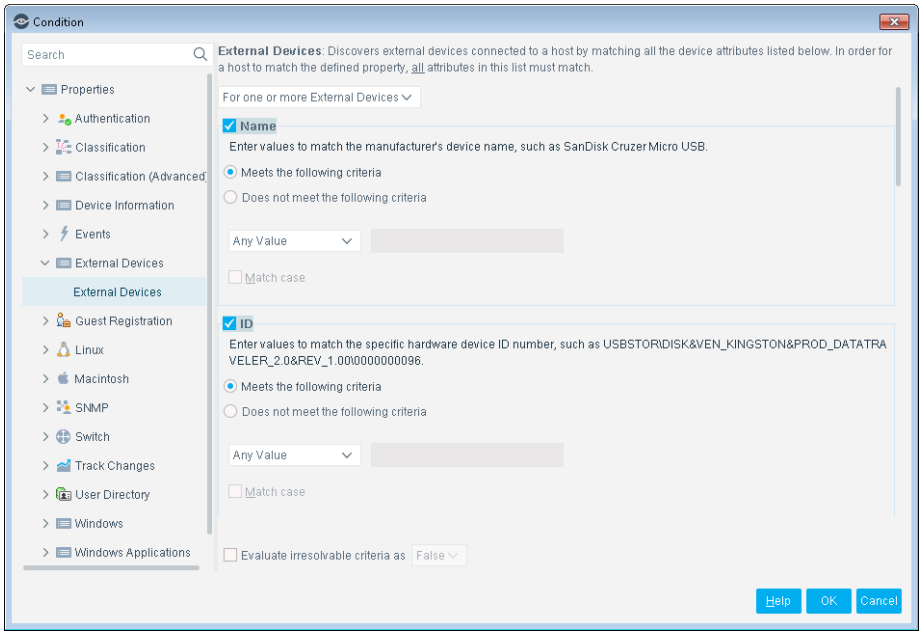
Custom Condition Dialog Box

2. Select **Add**. The User defined condition editor opens.



User Defined Condition Editor Dialog Box

3. Select **Add**. The Condition dialog box opens.



Condition Dialog Box

4. Define properties as required and select **OK**.
5. Define and name and description for the condition and select **OK**.

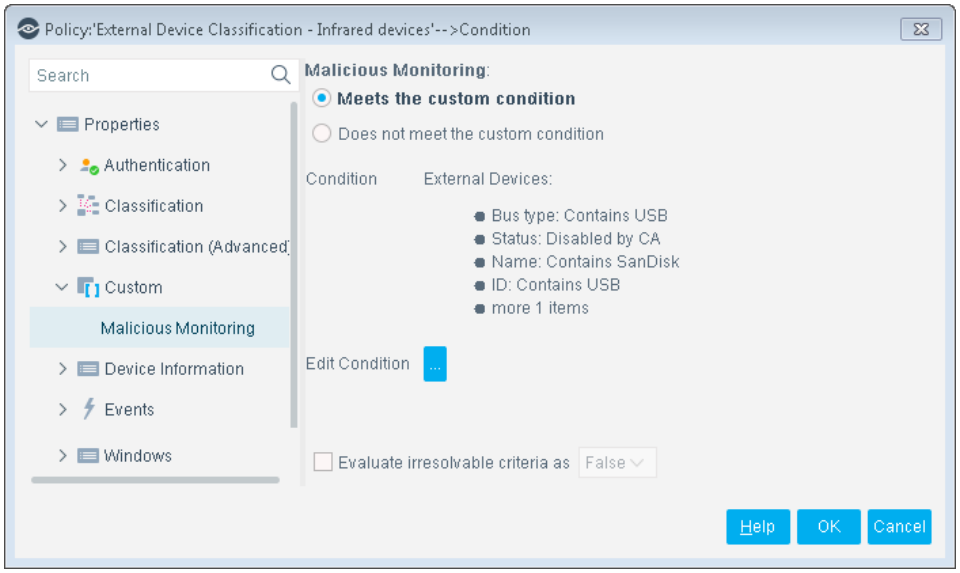
   The Condition that you created is displayed in the Custom Condition dialog box. Use this dialog box to manage your created conditions.

Using Custom Conditions

You can use the conditions that you create for any policy.

To use conditions:

1. Select the Custom folder from the **Select Property** section of the Condition dialog box.



Condition Dialog Box, Custom

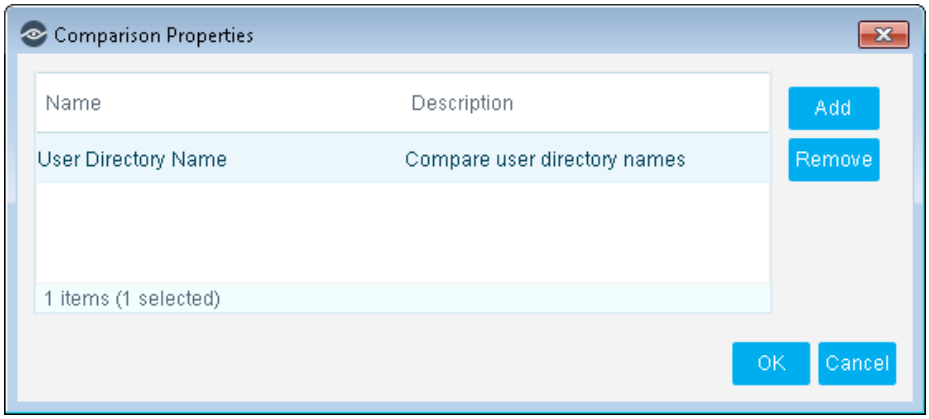
2. Work with the custom condition as you would any other.

Comparing Property Results

You can create a property that indicates differences, if any, 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 at which that the property was used.

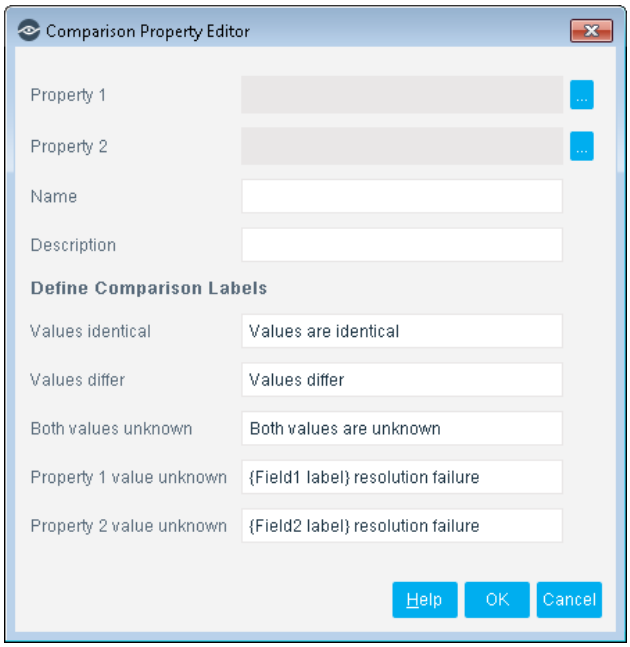
To create a comparison property:

1. Select **Comparison** in the Policy Manager. The Comparison Properties dialog box opens.



Comparison Properties Dialog Box

2. Select **Add**. The Comparison Property Editor opens.



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. Define the Comparison labels.

   Use the labels to customize the names of the property comparison results; for example, change the *Values Identical* result label to *User Directory Names Identical*.
5. Select **OK**.
6. The new property appears in the Comparison Properties dialog box.

7. Select **OK** to save.

To use a comparison property:

1. Edit or create a policy.
2. Navigate to the Condition>Properties list and select the Comparison properties folder.
3. Incorporate your comparison property into your policy.

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 is comprised 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.

The Corporate/Guest Control template automatically generates a list of corporate domains.

The following options are available for creating property lists:

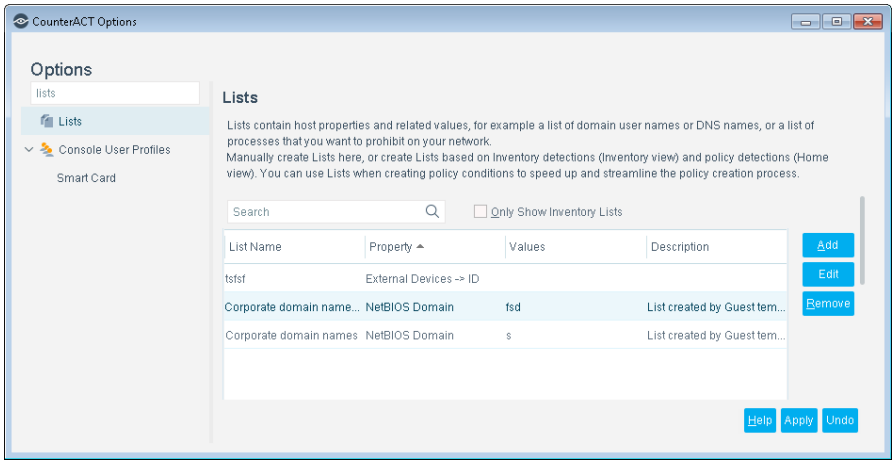
- Use a Wizard to Create Lists.
- Create Lists Based on Endpoint Detections.
- Create lists from properties discovered via the Asset Inventory and policies. See Create Lists Based on Inventory Detections and Adding Endpoint Properties to a List for details.

Use a Wizard to Create Lists

Use the Property Value List wizard to generate lists.

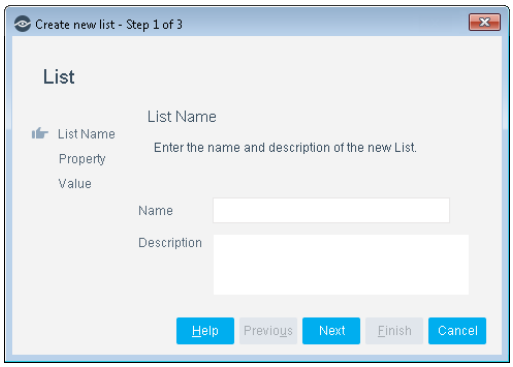
To generate a list:

1. Select **Options** from the **Tools** menu and then select **Lists**.



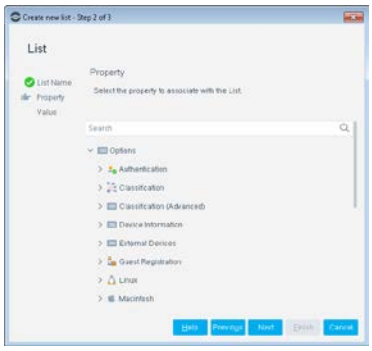
Lists Pane

2. Select **Add**. The wizard opens in the List Name page.



List Name

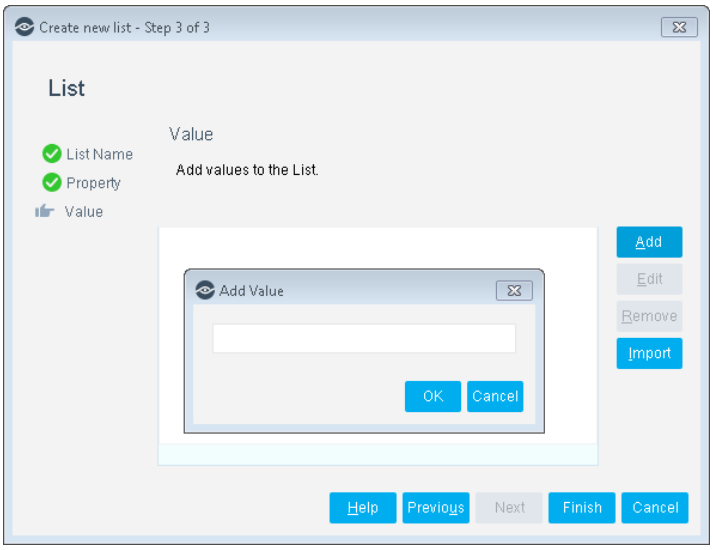
3. Type a name for your list and add a description.
4. Select **Next**. The Property page opens.



Properties

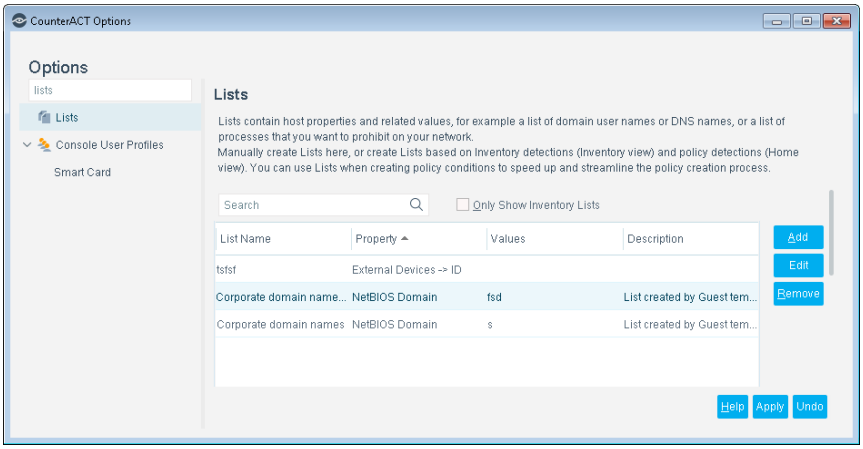
5. Select the property for which you want to make a *List*. See Working with Properties for more information about the properties shown. You can use this option for any property that is comprised of free text and for the Device Information>Open Ports property. Other properties, for example, installed software, peer-to-peer applications or properties indicating endpoint manageability, cannot be included in lists.

6. Select **Next**. The Values page opens.



Values Windows

7. Select **Add** and enter a value.
8. Add additional values as required.
9. 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.
10. Import values from external programs. Type one value per line. A value can contain spaces. Files should be imported in TXT format.
    - Select Import.
    - Navigate to your file and import.
11. Select **Finish**. Your value list is displayed Lists pane.



Lists Pane

12. Select **Apply** and then **Close**.

Lists added here will appear in the Asset Inventory view if the list includes properties detected in the network.

Managing Lists

Perform the following tasks from the Lists pane.

Edit and Remove Lists

You cannot remove lists that are used in policies.

To edit a list:

1. Select an entry from the Lists pane and select **Edit**. The required dialog box opens.
2. Edit the value and select **Apply**.

To remove a list:

1. Select an entry from the Lists pane and select **Remove**.
2. Select **Apply**.

Only Show Lists Generated from the Asset Inventory View

You may have generated lists based on Inventory detections. You can filter the view in the Lists pane to only display these lists. See Working with Asset Inventory Detections for details.

To filter the view:

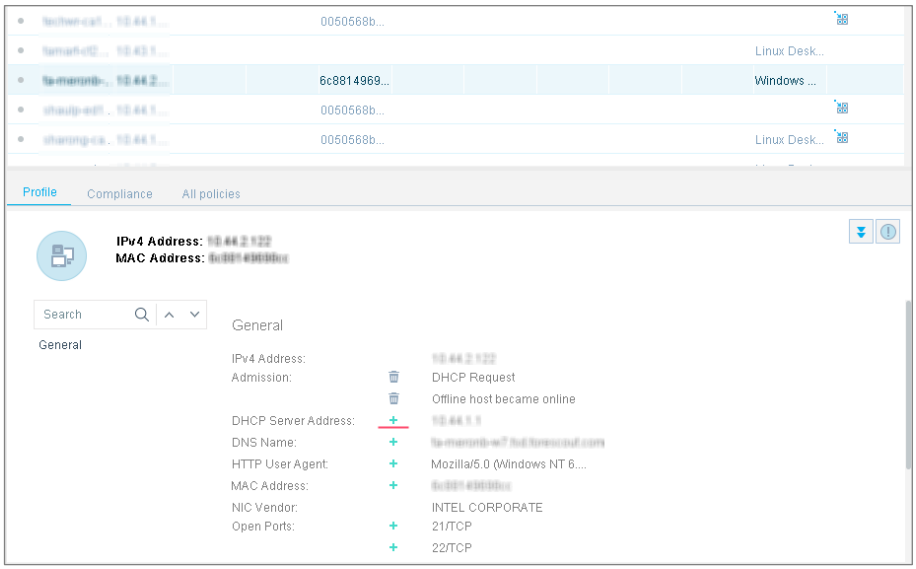
1. Select **Only Show Inventory Lists** in the Lists pane.

Create Lists Based on Endpoint Detections

The Home view, Details pane provides information about endpoint properties detected as a result CounterACT detections. You can navigate to these properties and automatically assign them to lists or add them to new lists.

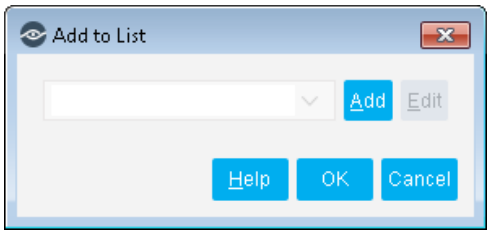
To create a list:

1. Select an endpoint from the Home view, Detections pane.
2. Navigate to the Console, Details pane, Profile tab.



Add to List

3. Select ✚ adjacent to the properties shown in the Details pane, Info tab. The Add to List dialog box opens.



Add to List Dialog Box

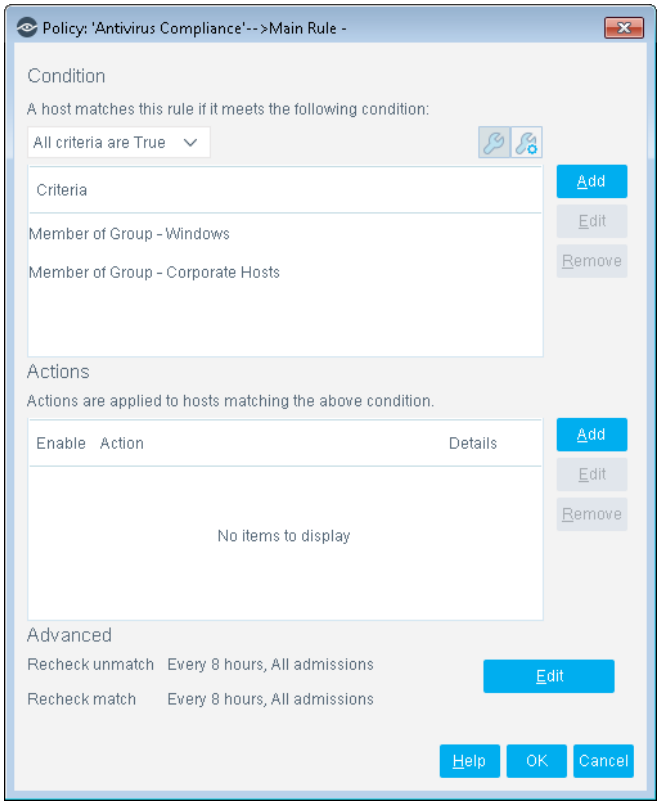
4. Select a list from the drop-down list or select **Add** to add the property to a new list.
5. Select **OK**.

Using the Lists That You Create

You can use property value Lists when defining policies. Using lists speeds up and streamlines the policy creation process, and minimizes mistakes that made be made when defining policy property values.

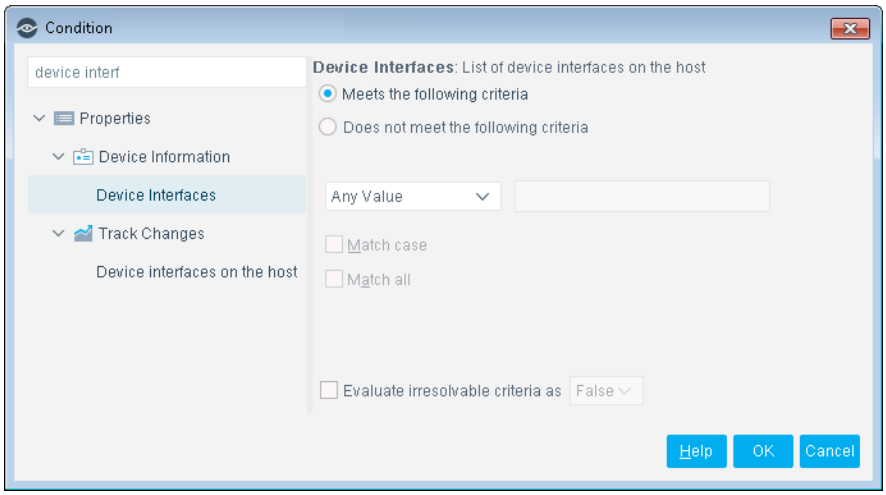
To use value lists:

1. In the Policy manager, select a policy and select **Edit**. The Policy Properties dialog box opens.
2. Next to the **Main Rule** section, select **Edit**. The Policy Conditions dialog box opens.



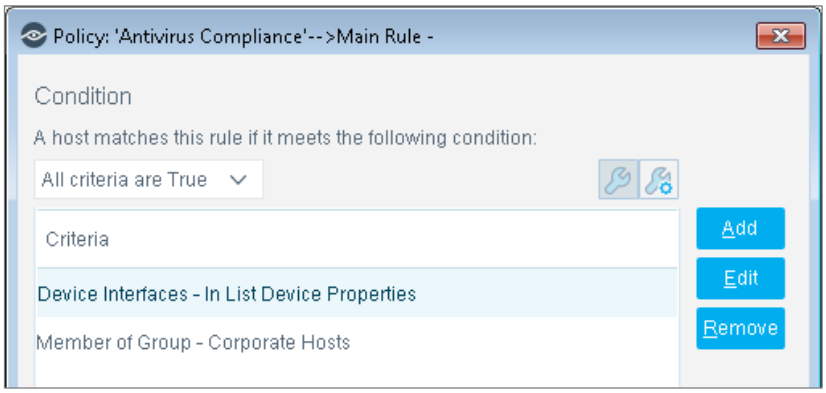
Rules Dialog Box

3. Select **Add** or **Edit** in the **Condition** section.
4. Select the property for which you created a list.
5. Select **Edit**. The Condition dialog box opens.
6. From the Properties tree in the left pane select the condition to add. The condition properties are displayed in the right pane.
7. Select the *In List* option from the drop-down list and select the list. You can create a new list or edit a list from this location.



Condition>Property Value List Option

8. Select **OK**.
9. The list is displayed as part of your policy condition. You cannot remove lists that are used in policies.



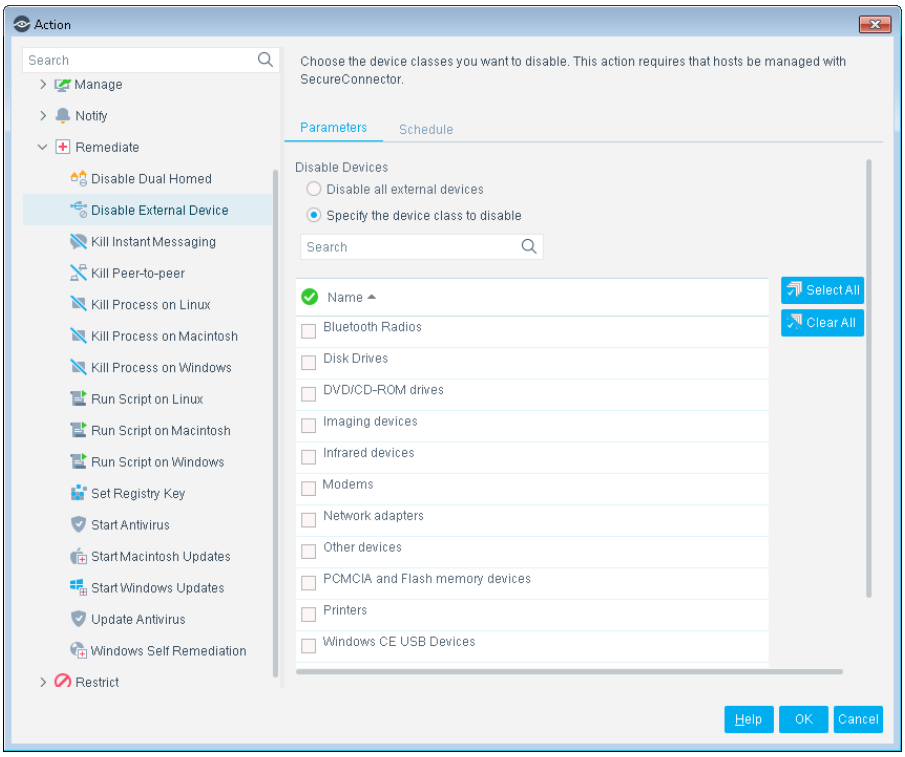
List Incorporated in Condition

Chapter 7: Working with Actions

- About Actions
- Working with Actions
- Audit Actions
- Authenticate Actions
- Classify Actions
- Manage Actions
- Notify Actions
- Remediate Actions
- Restrict Actions
- Action Tools

About Actions

Actions are measures taken at endpoints; ranging from notices, warnings and alerts to remediation, network and web access restrictions and complete blocking.



Actions

Actions Delivered with Modules and Extended Modules

In addition to the actions delivered with your CounterACT system, other actions may become available when you install modules and Extended Modules. For example, if you are working with the CounterACT Wireless Plugin or the CounterACT FireEye HX Extended Module, actions delivered with these components will be available. Actions are described in related Configuration Guides, and not in this chapter.

To read about actions delivered with modules and Extended Modules:

1. Select **Options** from the **Tools** menu.
2. Select **Modules** and select the plugin you are working with.
3. Select **Help**. The configuration guide for your plugin opens.

Refer to the related plugin or Extended Module Configuration Guide for details about these actions. See Additional CounterACT Documentation for information on how to access this guide.

See Chapter 8: Base, Content and Extended Modules for information about working with plugins and Extended Modules.

Gradual Action Enforcement

CounterACT actions enable gradual policy enforcement; for example, initially only notifying endpoint users or IT regarding noncompliance and later, if required, taking more severe measures, such as preventing endpoint users from accessing the Internet or blocking access to the production network.

Actions are organized into the following categories:

- Audit Actions
- Authenticate Actions
- Classify Actions
- Manage Actions
- Notify Actions
- Remediate Actions
- Restrict Actions

Action Tools

This section provides information about Action tools, including:

- Enabling and Disabling Actions
- Action Schedules
- Property Tags in Actions
- Action Thresholds
- Scripts and Interactive Actions
- Accessing Console Actions

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. Policies can be enabled or disabled from:

- Home view, Detections pane.
- Home view, Views pane. See Stop and Start Actions for Endpoints in Policies and Sub-Rules for details.
- A policy. See Enabling and Disabling Actions for details.

Action Schedules

Action schedules can be assigned to each policy action. This allows you to control when actions are carried out and for what duration. 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. See Creating Action Schedules for more information.

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 on to the detected machine. See Working with Property Tags for more information.

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. 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.

Scripts and Interactive Actions

Several actions require that CounterACT 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 **Options** from the **Tools** menu. Select **Modules**. Select this 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. CounterACT 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 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.

Accessing Console Actions

Actions can be incorporated into policies to be carried out when certain conditions are met. For example, create a policy that detects users working with unauthorized instant messaging applications, and use a CounterACT actions that kills those applications.

Alternatively, you can manually apply an action on selected endpoints.

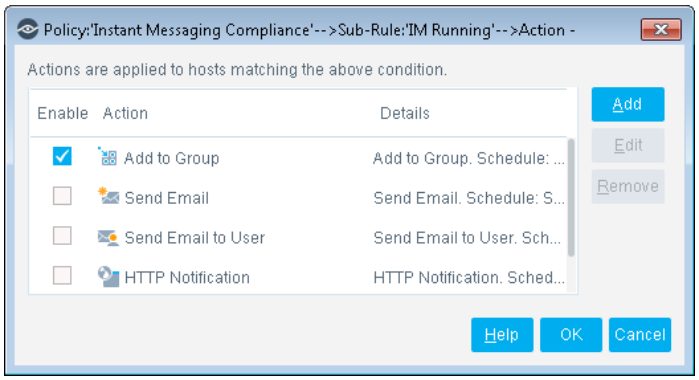
For each installed module, additional actions may be available. See Chapter 8: Base, Content and Extended Modules for details.

Access actions:

- From the Home view, Detections pane.
- When creating and editing a policy. See Defining a Policy Main Rule.
- When editing a policy as described here.

To access actions from a policy:

1. Right-click a policy Main Rule or Sub-Rule from the Policy Manager.
2. Select **Quick Edit** and then select **Actions**. The Policy Action dialog box opens.



3. Enable or disable the action.
4. Select **OK**.

Working with Actions

This section describes how to define CounterACT actions.

- Audit Actions
- Authenticate Actions

- Classify Actions
- Manage Actions
- Notify Actions
- Remediate Actions
- Restrict Actions

In addition to the actions delivered with your CounterACT system, plugin and module-specific actions may appear. For example, if you are working with the CounterACT Wireless Plugin or the McAfee ePolicy Orchestrator Extended Module, related actions will be available. See Chapter 8: Base, Content and Extended Modules for information about working with plugins and Extended Modules.

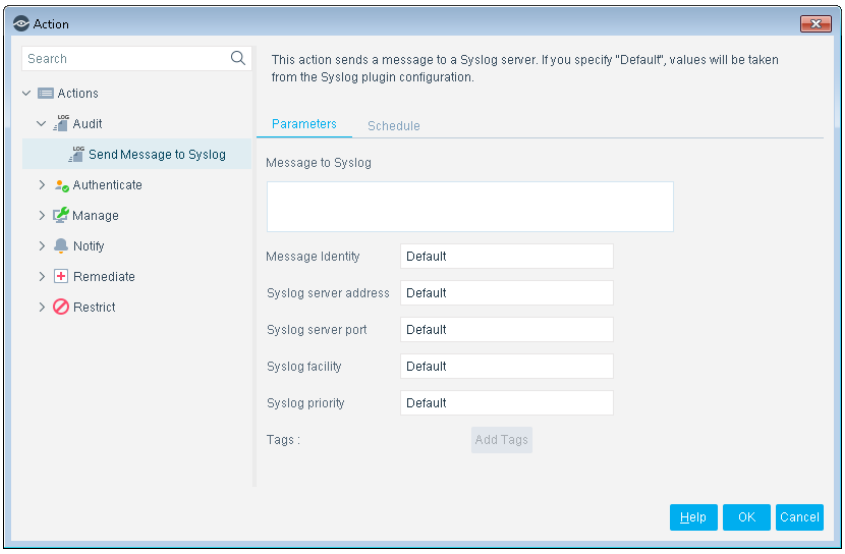
Audit Actions

The *Send Message to Syslog* action is included by default as an Audit action.

Send Message to Syslog

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.

1. In the Policy manager, select a policy and select **Edit**. The Policy Properties dialog box opens.
2. Next to the **Main Rule** section select **Edit**. The Policy Conditions dialog box opens.
3. Next to the **Actions** section select **Add**. The Action dialog box opens.
4. In the left pane expand the Audit folder.
5. Select **Send Message to Syslog**.



Send Message to Syslog Action

6. Specify the following or use **Default** where applicable to apply the default configuration.

Message to Syslog	Type a 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 is 514)
Syslog Facility	Syslog messages facility (default is local4)
Syslog Priority	Syslog messages priority (default is info)
Use TLS	Instruct CounterACT 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.

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 Working with Property Tags for more information.

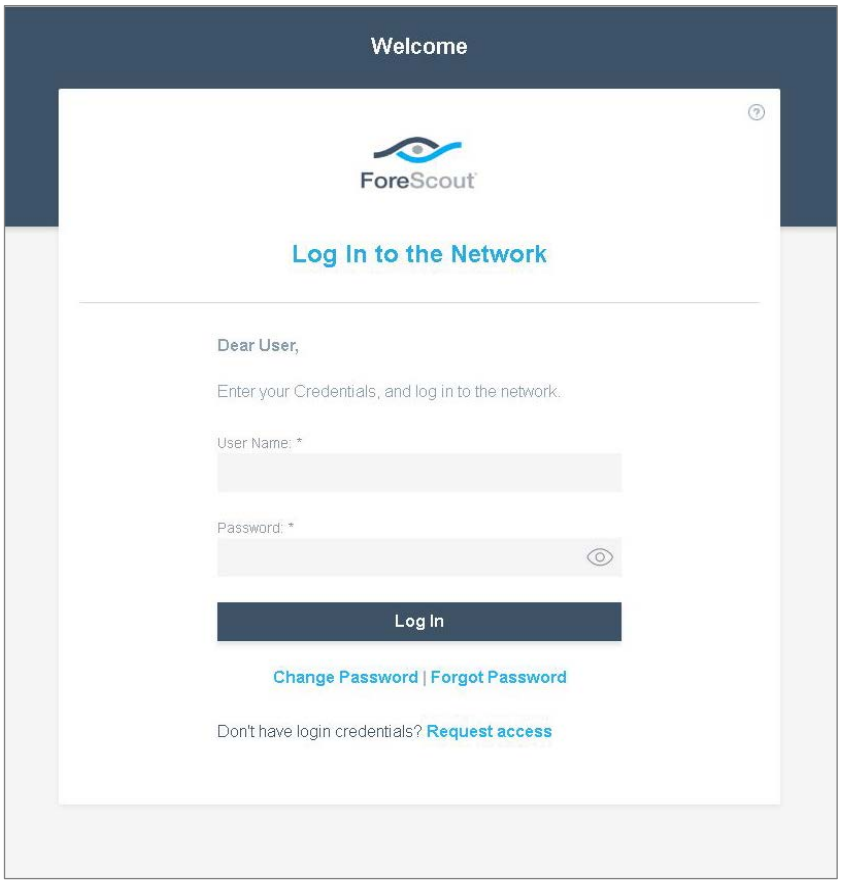
Authenticate Actions

This section describes actions that allow the CounterACT operator to control the access of corporate and guest users to a corporate network. These actions are provided by the User Directory Plugin.

- HTTP Login
- HTTP Sign Out

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 are presented with a Login page and must enter valid credentials.



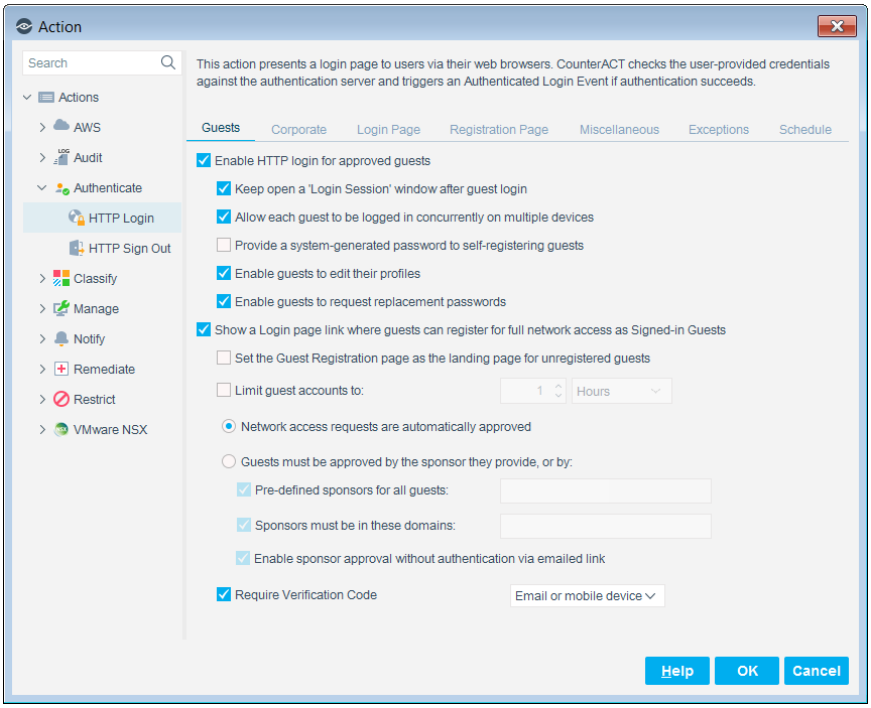
Login Page

The action can be configured to handle:

- Guests: See Handling Guests
- Corporate users: See 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.



HTTP Login Action Configuration

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 cancelled, removing all limitations imposed. In this example, the user is removed from the isolated VLAN and can join the network and browse.

- *Web messages and emails used in this action can be changed and localized. See Localizing CounterACT Redirected Web Pages and Messages.*

- *Login failures can be easily tracked. See HTTP Login Attempts for details.*

- *You can customize the text that the* HTTP Login *action displays at the user's endpoint. For details, see Customize HTTP Login Action Text.*

- *HTTP Login is disabled whenever HTTP Redirection is disabled. For more information, see Disabling Web Portals.*

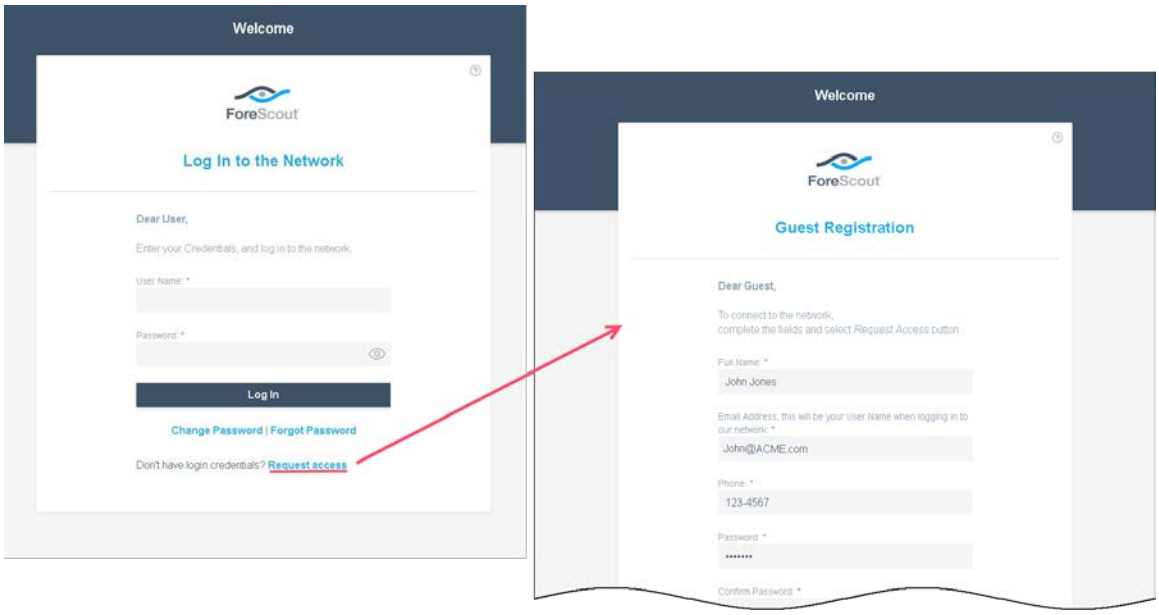
Depending on the endpoint operating system, and how the endpoint is managed, this action is implemented by the HPS Inspection Engine, the Linux Plugin, or the OS X Plugin.

Handling Guests

This section describes how to work with the *HTTP Login* action when handling network guests. For example, create policies that deal with visiting professionals, contractors, etc.

Guests are authenticated against the CounterACT 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.



Login Page and Guest Registration Form

To configure the *HTTP Login* action for guest login, use 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

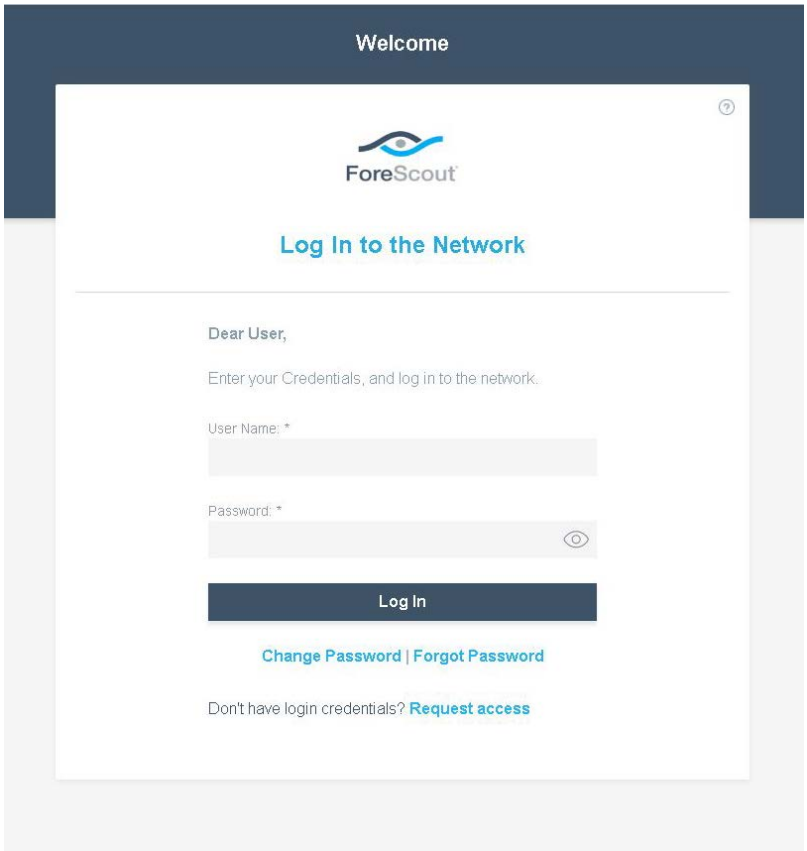
Use the *Corporate* options to enable corporate authentication.

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

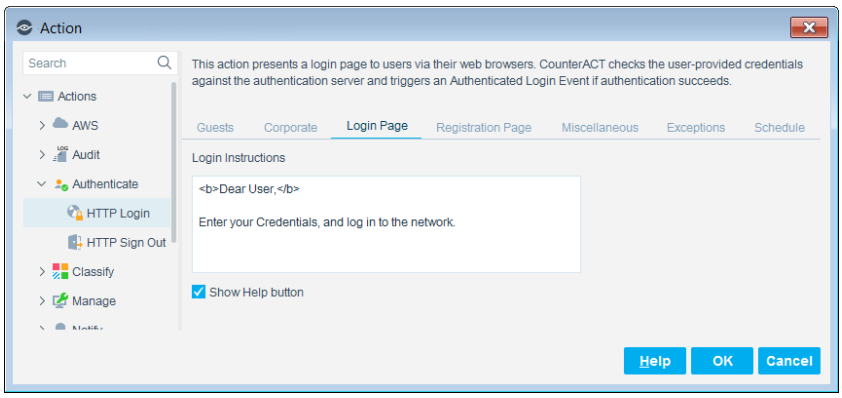
The Login Page tab is used to define what is displayed on the Login page. This page appears for both guest and corporate users.



Login Page

After the user successfully logs in, the endpoint *Authentication, Signed In Status* property is resolved by CounterACT 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 here will be used when resolving the *Device Information > User Name* property. If necessary, you can instruct CounterACT 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 more information. Select **Options** from the **Tools** menu. Select **Modules**. Select this plugin and then select **Help**.



HTTP Login Action, Login Page Tab

The following Login Page tab options are available:

Login Instructions

In the text box of the Login Page tab, define the Login page message that is presented to both guests and corporate users.

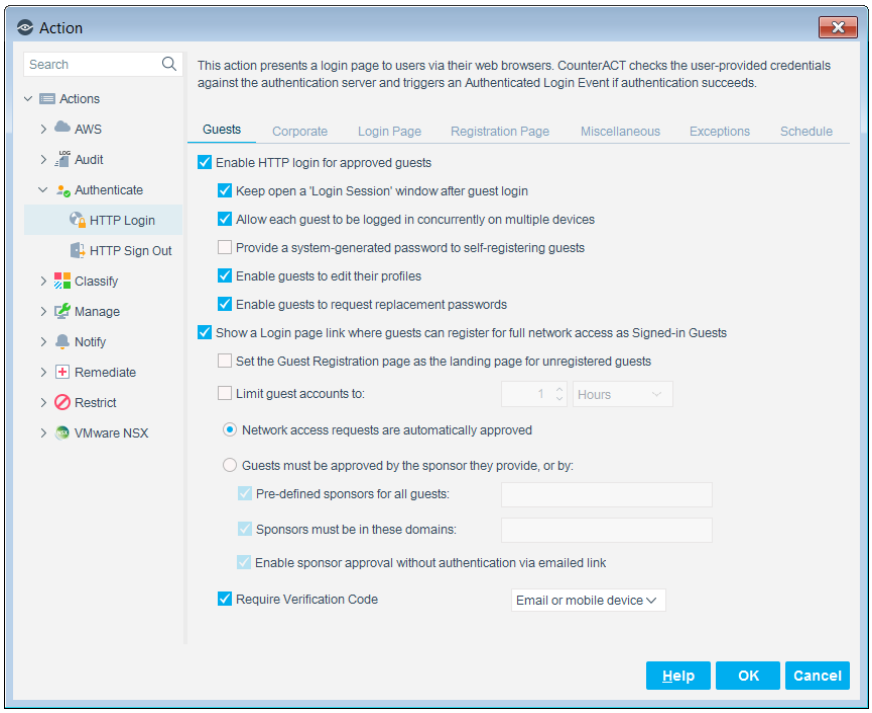
Show Help Button

Help instructions are available on the Login page to assist users.

If you do not want to give users access to the Help page for any reason, hide the **Help** button on the Login page by clearing the **Show Help button** checkbox.

Guests Tab

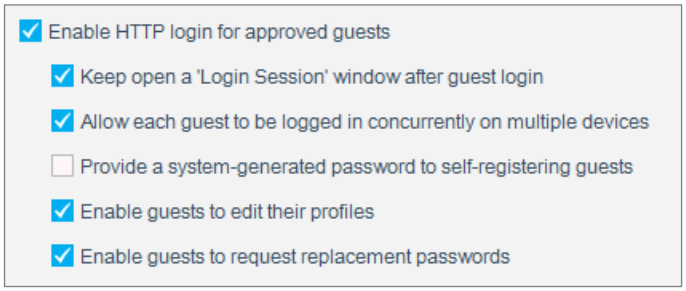
Use the Guests tab to define guest login session options, as well as a registration strategy.



HTTP Login Action, Guests Tab

Guest Login Session Options

These options let you control the guest login experience.



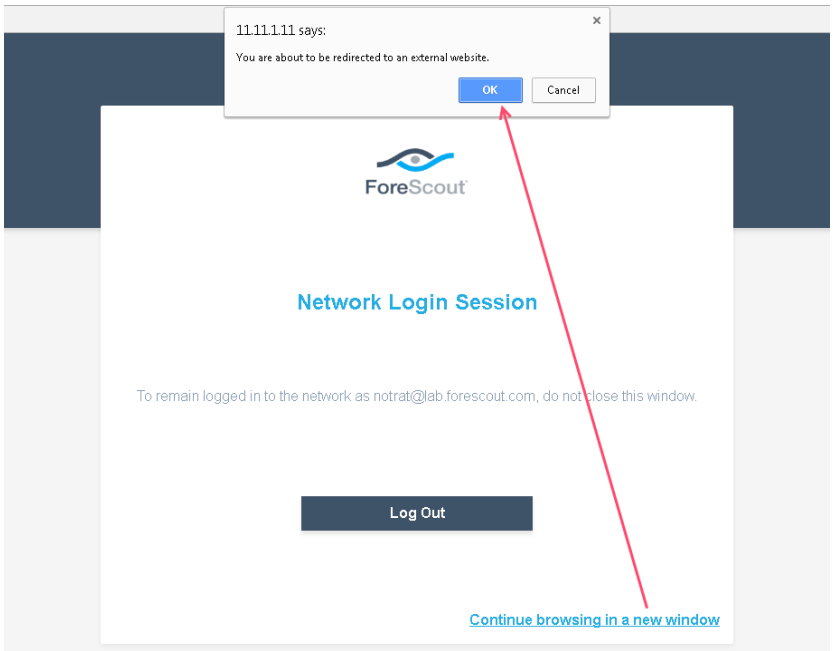
HTTP Login Action, Guest Login Session Options

Enable HTTP login for approved guests

Select this option to enable login for approved guests. Authentication is validated against a CounterACT server database after the guest is approved.

Keep open a 'Login Session' window after guest login

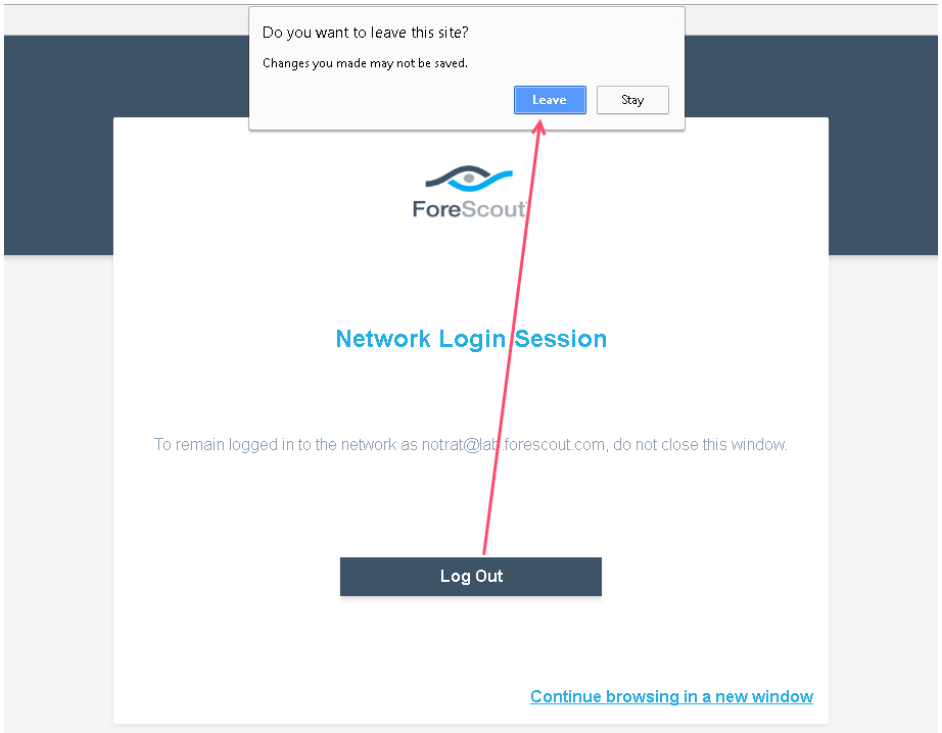
Select this option to display a CounterACT Login Session window for guests. To browse as a registered guest, the user selects **Continue browsing in a new window** and then **OK**.



CounterACT Login Session Window

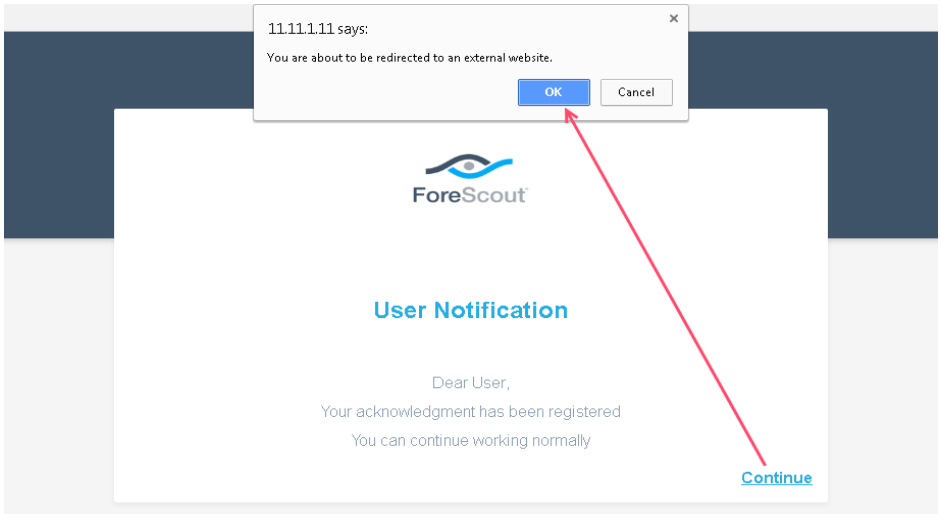
The user must keep the Login Session window open to maintain a network to Internet connection, provided this access was granted in the policy. During this time, CounterACT resolves the *Authentication, Signed In Status* property for the endpoint as *Signed In as a Guest*.

To leave the network, the user selects **Log Out** and then **Leave**:



Logout Window

If the **Keep open a 'Login Session' window after guest login** checkbox is not selected, the CounterACT 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**. CounterACT resolves the *Authentication, Signed In Status* property for the endpoint as *Not Signed In*.



User Notification Window

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 instruct CounterACT to generate a password for the guest to use in the Password field of the Login page. 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, CounterACT generates a password 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.

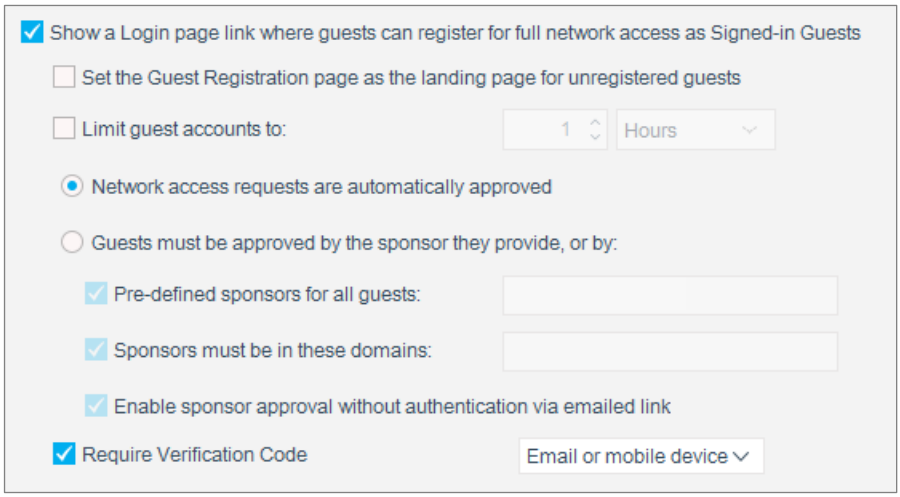
Enable guests to edit their profiles

Select this option to instruct CounterACT to display the Edit Profile link in 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 passwords

Select this option to instruct CounterACT to display the Forgot Password link in the Login page that is presented to guest users. Selecting this link displays the Forgot Password page, where approved guests can request a new password for login.

Guest Registration Options



Define Guest Registration Strategy

Allow only pre-approved guests

Clear the **Show a Login page link where guests can register for full network access as Signed-in Guests** checkbox if all guests must be pre-approved for network access. Information about pre-approved guests is saved on the CounterACT 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 CounterACT operator in the Guest Registration Pane. It is the responsibility of your organization to forward login credentials to these pre-approved guests. CounterACT does not do this. See Guest Registration Pane.

Enable guest registration

To enable not-yet-approved guests to self-register, select the **Show a Login page link where guests can register for full network access as Signed-in Guests** checkbox. This prompts new guests to complete a Guest Registration form on which they provide information such as their identity details and the name of the individual who invited the guest to the network. A link to the Guest Registration form is provided on the corporate login page.

Landing page prompt

Select **Set the Guest Registration page as the landing page for unregistered guests** if you want to prompt the guest to complete the Guest Registration form.

Guest account expiration

To set a maximum time for which guests can request network access, select **Limit guest accounts to** and enter the time limit. By default, this field is unselected, making the maximum network access approval period *unlimited*. In the Guest Management Portal, sponsors can further limit the network access of their self-registering guests to less than this value. When the time period elapses, the guest account expires and the guest is required to register again.

Automatic approval of registered guests

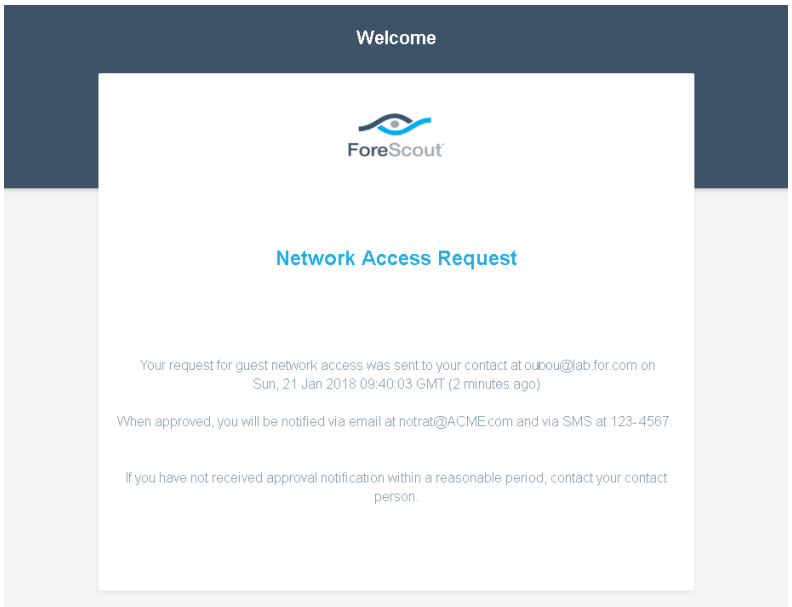
For guests to be automatically approved after submitting a Guest Registration form, select **Network access requests are automatically approved**. You may want to do this if you anticipate many guests and do not have the resources to accept or reject each one, but do want to keep track of who is registered. Approved guests are displayed in the following CounterACT locations:

- In the Guest Management Portal where sponsors can view the registered guests that specified them as their corporate contact.
- In the Guest Registration 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 their guests awaiting approval.

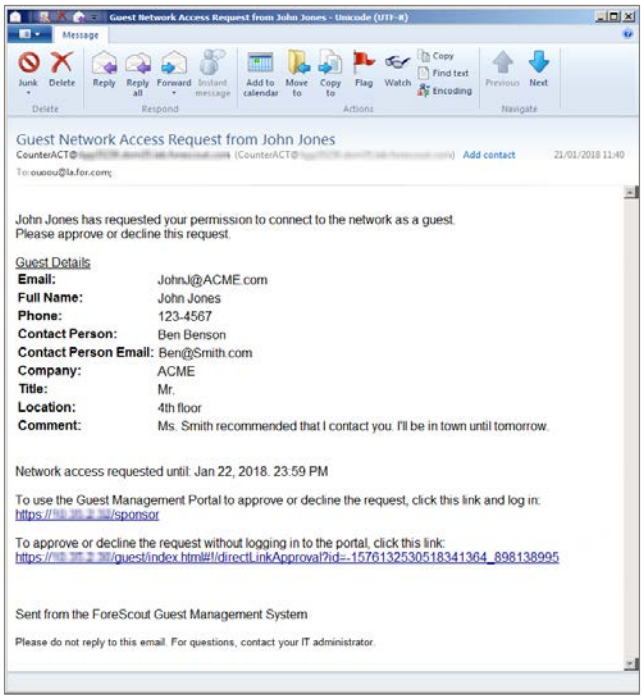
Before sponsor approval is completed, a notification page opens for the guest.



Guest Registration Request Pending Page

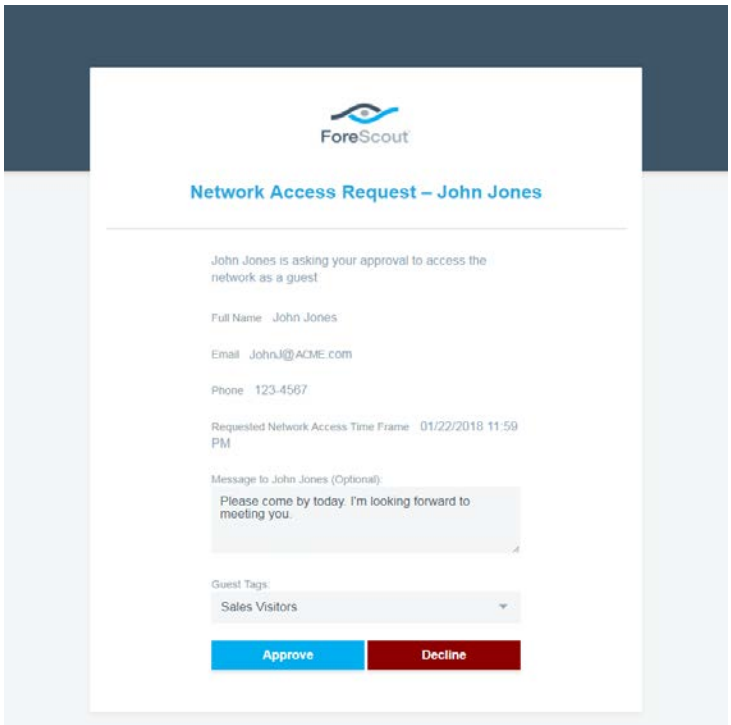
Enable sponsor approval without authentication via emailed link

The guest registration request notification email that is sent to sponsors always includes a link to the corporate Guest Management Portal. Select this option to include an additional link in the notification email to a Network Access Request page containing the specific guest registration request.



Guest Registration Request Email

- 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 CounterACT 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.



Network Access Request - Sponsor Approval Page

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.

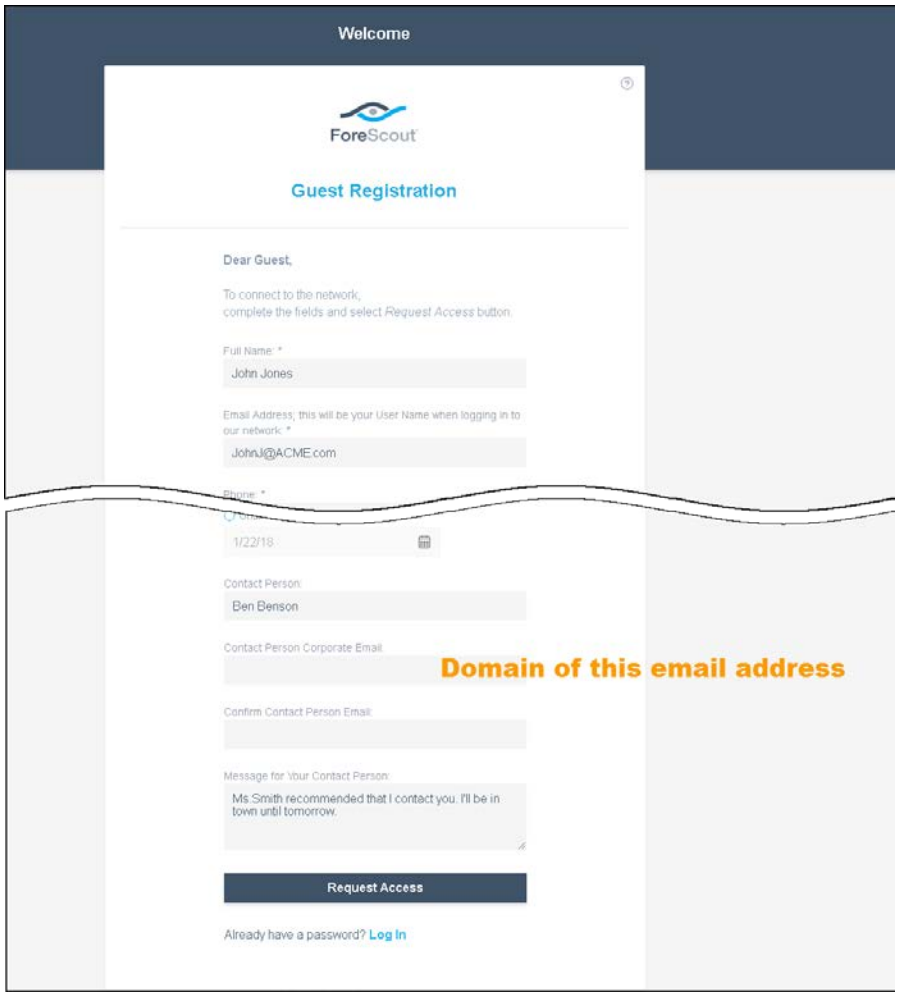
*If **Enable sponsor approval without authentication via emailed link** is selected, it is recommended to select **Sponsors must be in these domains** to ensure that only corporate employees receive the emailed link.*

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.

Sponsors must be in these domains

To make the approval process more scalable, your network guests can be approved by individuals in your organization, based on the domain address of the *Contact Person Email* that they entered in the *Guest Registration* form.

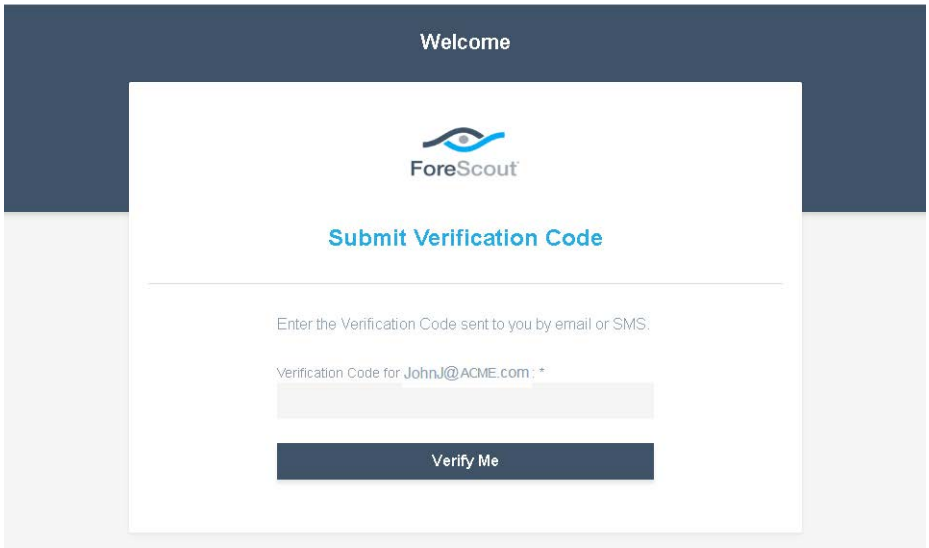


Guest Registration Form

Select this option to provide a comma-separated list of corporate domains. The entries specified in this field limit the allowed domain(s) in the Contact Person Email field of the Guest Registration form submitted by a registering guest. For example, if the field contains the entries **`finance.my-company.com`**, **`marketing.my-company.com`**, **`sample.com`**, then only an email address that ends with one of these domains, such as jane@marketing.my-company.com, is valid for use in the Contact Person Email field.

Require 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. CounterACT 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 CounterACT.



Guest Verification Code Form

Verification codes are automatically generated and validated by CounterACT.

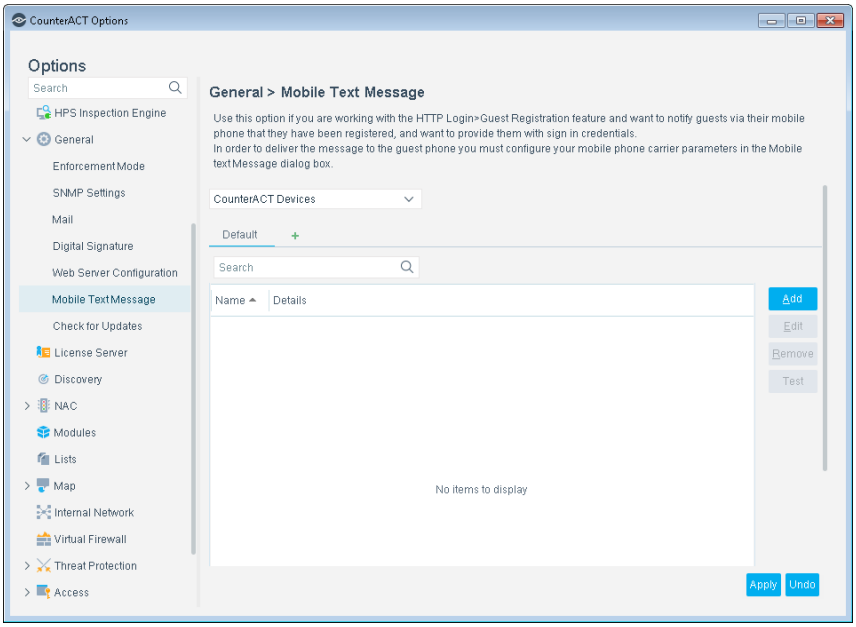
To work with verification codes:

1. Select **Require Verification Code** in the Guests tab.
2. From the drop-down list, select whether the verification code will be sent via email only, via mobile phone only, or via both email and mobile phone. The email messages 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 CounterACT submits the message to the mobile carrier.

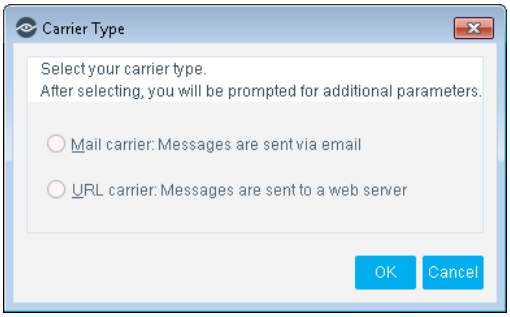
To define text messaging through a mobile carrier:

1. Select **Options** from the **Tools** menu and then select **General**>**Mobile Text Message**.



Mobile Text Message Pane

2. Select **Add**. The Carrier Type dialog box opens.

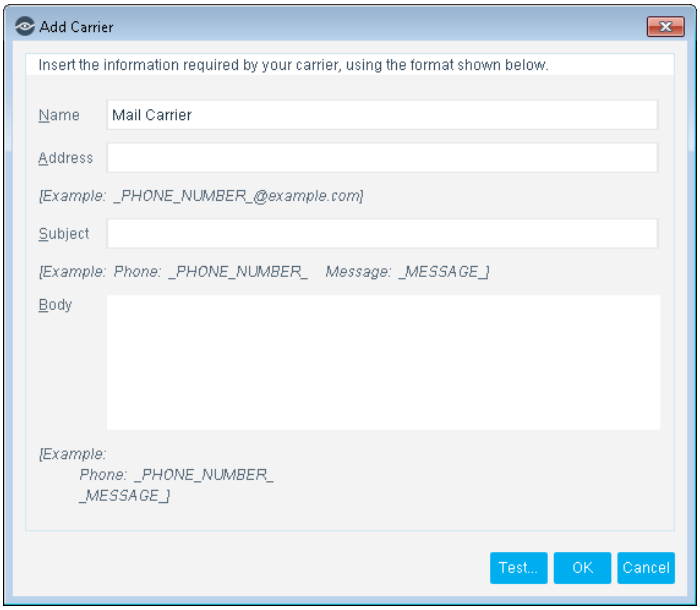


Mobile Text Message Carrier Type

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.

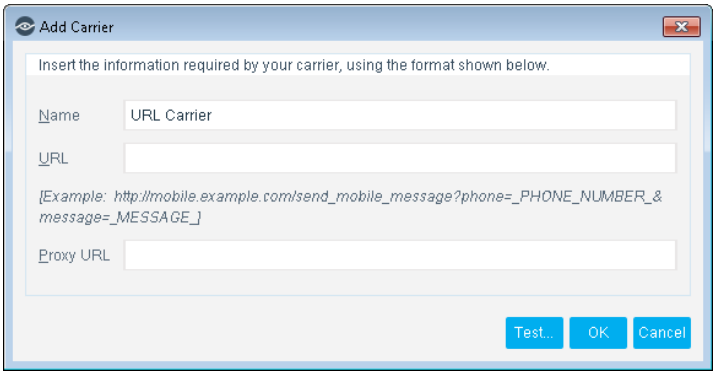
3. Select **OK**. In the Add Carrier dialog box, enter a name that identifies this carrier in the **Name** field. In the other fields of the dialog box, enter string patterns that define the format used to submit message requests.

   – For message requests in email format, the fields correspond to the Address, Subject, and Message fields of an email message.



Mobile Text Message Request, Email Format

– 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.



Mobile Text Message Request, URL Format

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.

4. 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.

5. 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 Registration 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.

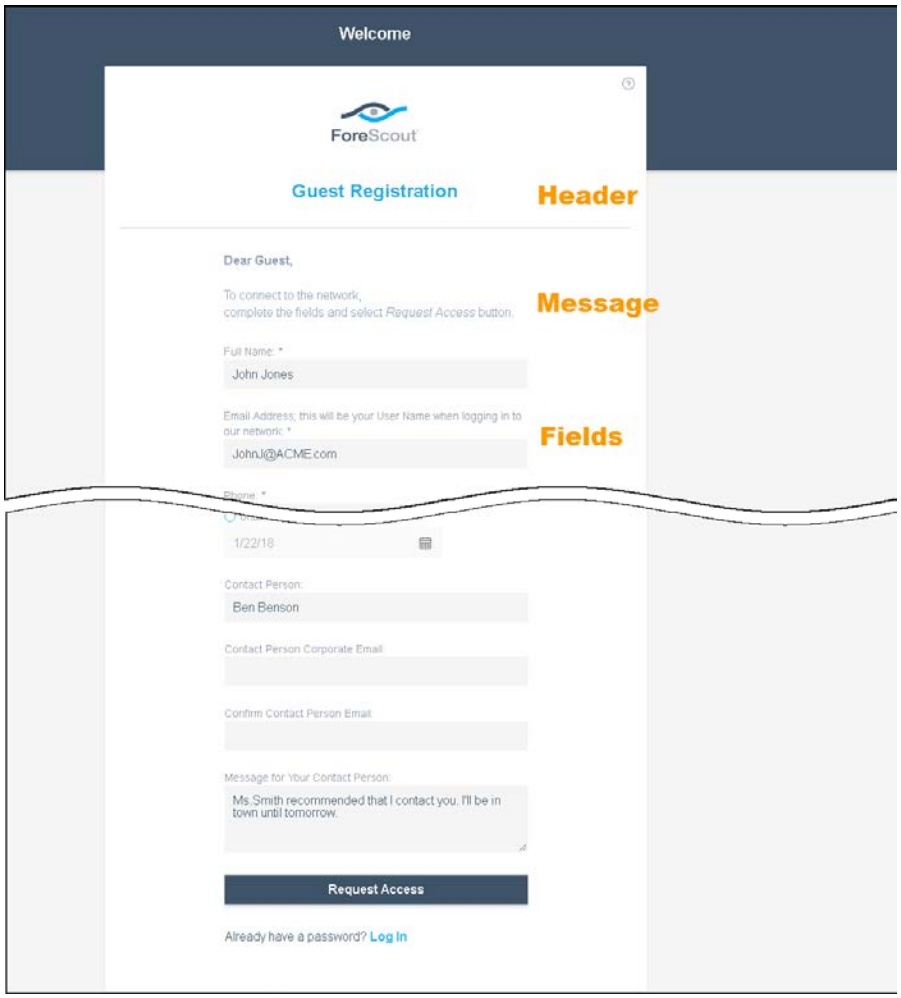
You can create policies that evaluate guests for their guest tag assignments. For example, create a policy that detects *Building A*-tagged guests and assigns them to a specific VLAN or allows them minimum network access.

See Managing Guest Tags for detailed information about administering guest tags.

Registration Page Tab

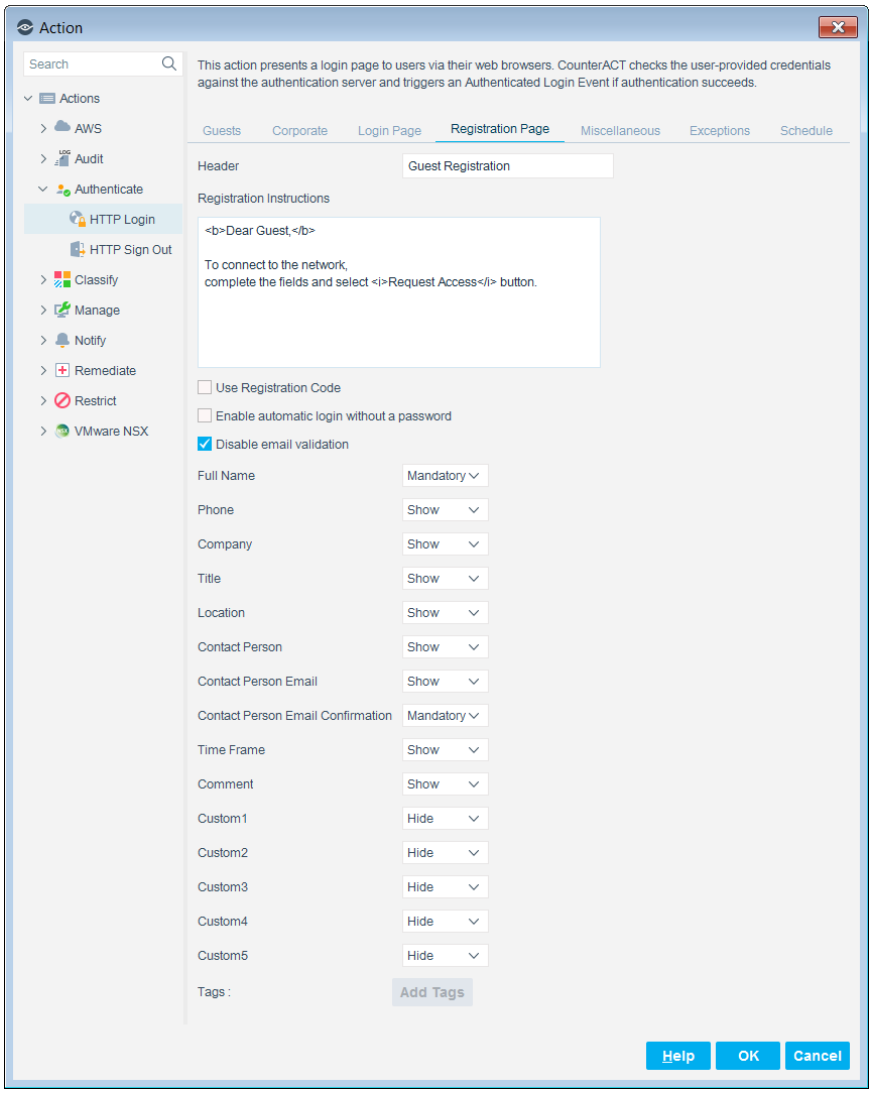
The information in the Registration Page tab is only used if guest registration is enabled in the Guests tab.

Use the Registration Page options to design the Guest Registration form.



HTTP Login, 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.
- Require guests to enter a registration code to begin the registration process. (optional)



HTTP Login, Registration Page Tab

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 that will appear in 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 by CounterACT, 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 checkbox is selected, there is no authentication.
5. The *Email* field is always mandatory, and guests are identified by its contents.
   - Clear the **Disable email validation** 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 the **Disable email validation** checkbox so that no validation is done on the field. Any value will be accepted in the *Email* field.

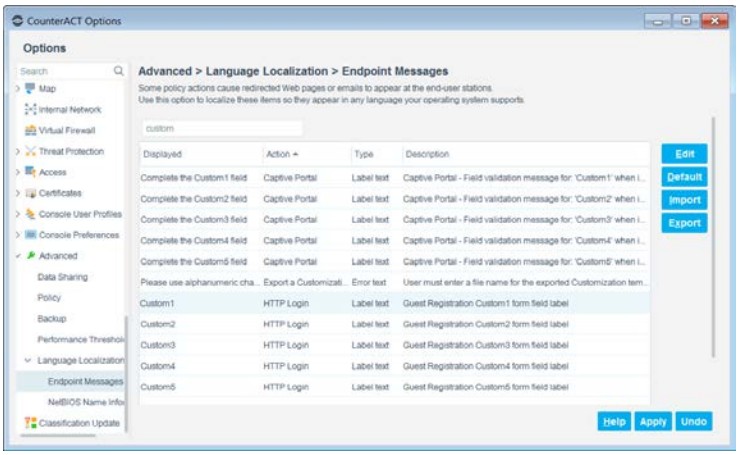
   *To ensure that only one guest identification field is displayed in the Guest Registration form, it is recommended to set the **Full Name** dropdown menu to **Hide** whenever the **Disable email validation** checkbox is selected.*

6. 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.
7. If tags are defined in your environment, you can select tags to be added to the registration form.

The list of fields includes 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:

1. Select **Options** from the **Tools** menu and then select **Advanced** > **Language Localization** > **Endpoint Messages**.
2. Type the word *Custom* in the search field.



Localization

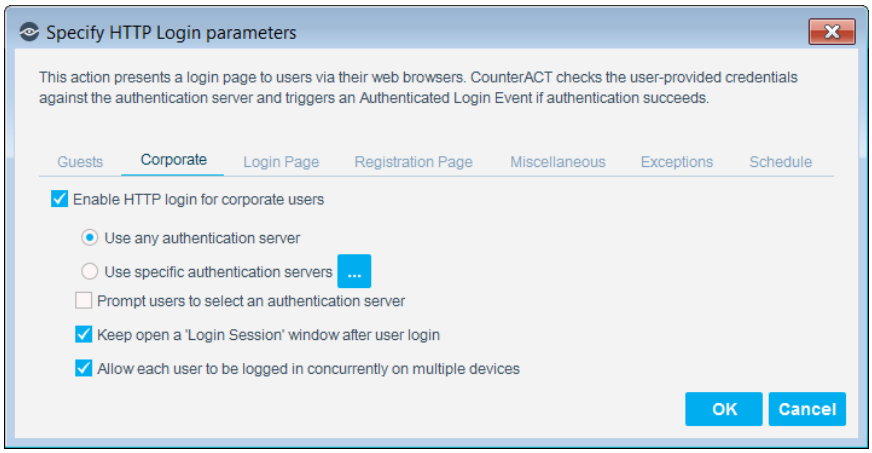
3. Edit the fields as required, select **Close**, and then select **Apply**.

Corporate Tab

Use the Corporate tab to define which servers will be used for domain authentication, as well as other authentication settings.

Before configuring corporate users, you must have already configured User Directory servers. Under most circumstances this configuration was performed when setting up the Console using the Initial Setup wizard.

To see which servers are defined, select **Options** from the **Tools** menu and then select **User Directory**. For more information about configuring User Directories see User Directory.

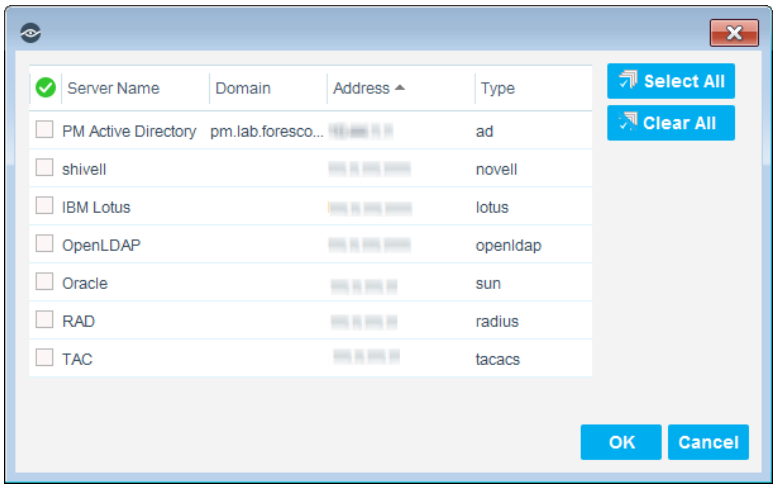


HTTP Login, Corporate Tab

To enable corporate user authentication against an authentication server, select **Enable HTTP login for corporate users**.

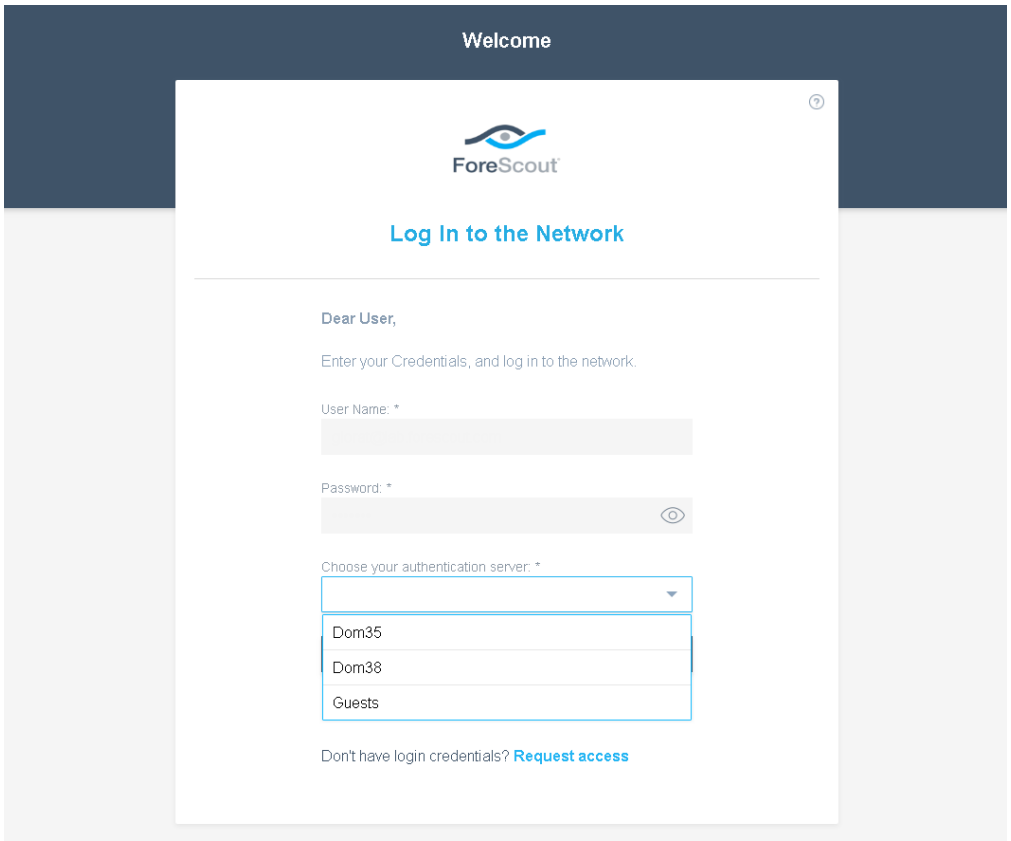
To allow authentication against any of the authentication servers that you defined in the User Directory Plugin, select **Use any authentication server**.

To authenticate users against specific servers, select **Use specific authentication server** and then select the browse button to choose servers.



HTTP Login, Defined Authentication 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 field, from which the endpoint user can select a domain.



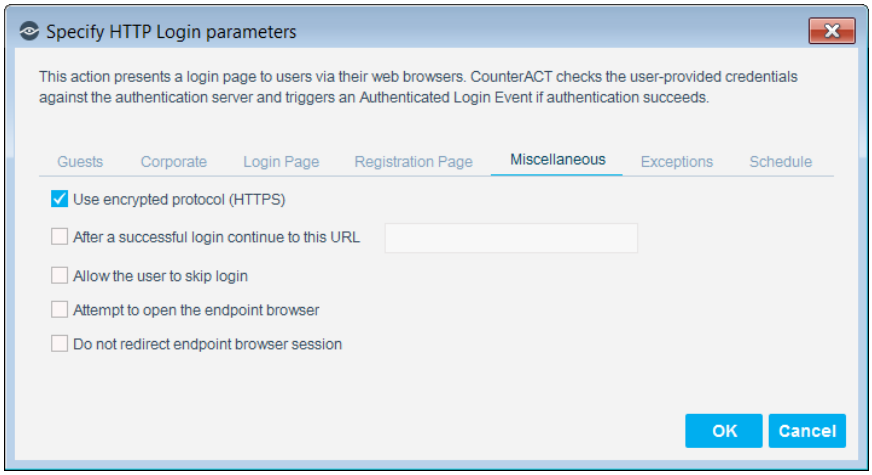
Login Page with Domain

To display a CounterACT 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, CounterACT resolves the *Authentication, Signed In Status* property for the endpoint 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.

Miscellaneous Tab

Use the Miscellaneous tab to configure additional user login parameters.



HTTP Login, Miscellaneous Tab

Use encrypted protocol (HTTPS)

It is recommended to select the **Use Encrypted protocol (HTTPS)** checkbox 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 more information about this transmission method.

Direct user to a predestinated 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**. 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.) CounterACT uses a script when this option is selected.

Refer to the *HPS Inspection Engine Configuration Guide* for details about how scripts work.

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

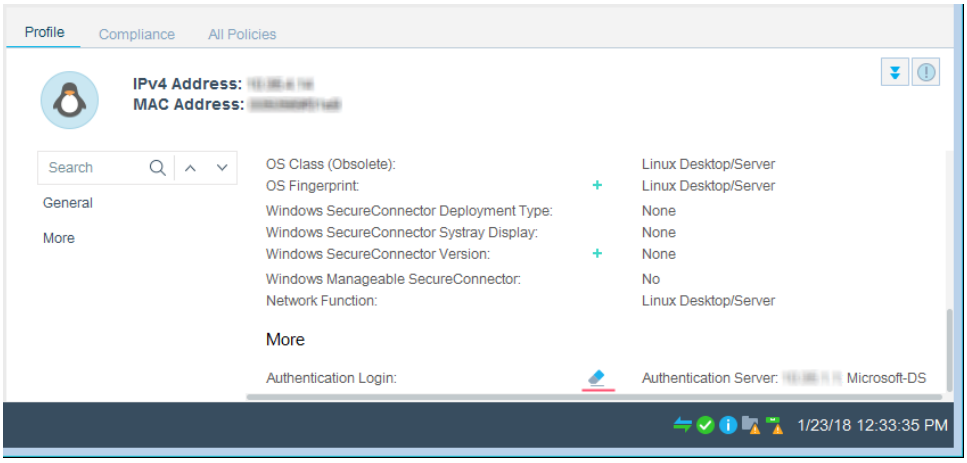
For details about customizing texts that CounterACT processing generates in a user's endpoint, see Localizing CounterACT Redirected Web Pages and Messages.

HTTP Sign Out

The *HTTP Sign Out* action signs out detected endpoints that meet the following criteria:

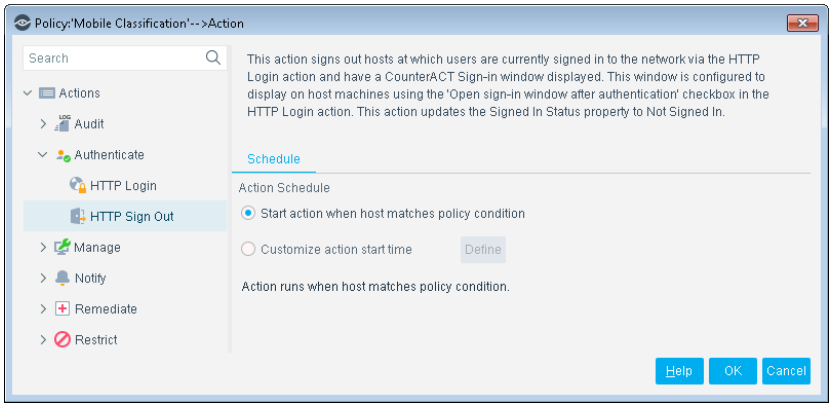
- The endpoint user is currently signed in to the network via the *HTTP Login* action.
- The endpoint displays a CounterACT Login Session window.
- The *Signed In Status* condition is tested to resolve the endpoint's login status.

The HTTP Sign Out *action can be used when running policies created using the Corporate/Guest Control policy template in CounterACT versions earlier than 8.0. These policies test the Signed In Status condition to determine if the user is currently signed in.*
Corporate/Guest Control policies created using the template provided in 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.*



Profile Tab, 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).



HTTP Sign Out Action, Configuration Window

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.

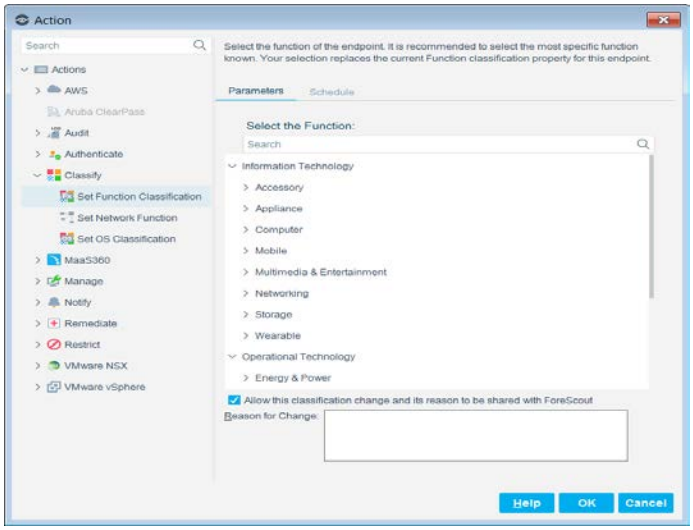
Classify Actions

This section describes actions that classify endpoints:

- Set Function Classification
- Set OS Classification
- Set Network Function

Set Function Classification

This action lets you override a *Function* property value set by Primary Classification policies.



Classify Device by Function

This is useful in the following situations:

- The classification resolved by CounterACT is not correct or CounterACT was not able to classify the endpoint based on its function.
- You are able to refine the device's classification. For example, CounterACT classified the device function as 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.

If the Primary Classification template was deployed with the 'Add to Group' actions enabled, the classified device is added to the related classification group.

If you agree to upload classification changes from your environment to ForeScout, 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

The feedback that you enter in the field will be sent to ForeScout to help provide better classification services.

To ensure that your changes are shared with ForeScout, first go to Tools > Options > Advanced > Data Sharing, and select ***Allow selected endpoint properties to be shared with ForeScout****. See The ForeScout Research and Intelligent Analytics Program.*

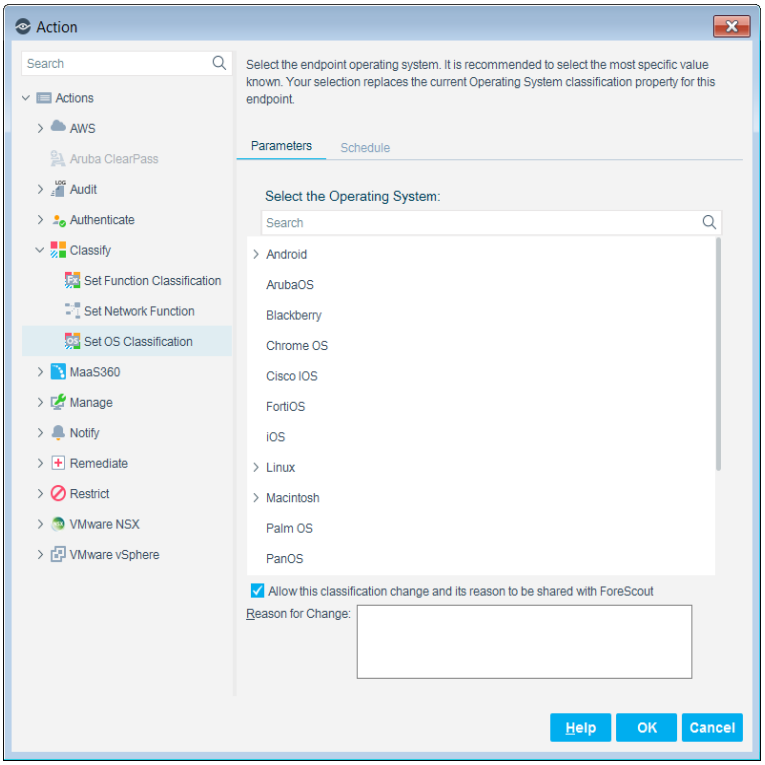
See Asset Classification and Primary Classification Templates for details about the Primary Classification template.

You can easily reset a manual classification assignment to that set by the Device Classification Engine. Under the Cancel Actions action, select **Revert to Suggested Function Classification**.

Revert to Suggested Function

Set OS Classification

This action lets you override an *Operating System* property value set by Primary Classification policies.



Classify Device by Operating System

This is useful in the following situations:

- The classification resolved by CounterACT is not correct or CounterACT was not able to classify the endpoint based on its operating system.
- You are able to refine the device's classification. For example, CounterACT classified the operating system as Macintosh, but you know it's 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.

If you agree to upload classification changes from your environment to ForeScout, 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

The feedback that you enter in the field will be sent to ForeScout to help provide better classification services.

To ensure that your changes are shared with ForeScout, first go to Tools > Options > Advanced > Data Sharing, and select ***Allow selected endpoint properties to be shared with ForeScout****. See* *The ForeScout Research and Intelligent Analytics Program.*

See Asset Classification and Primary Classification Templates for details about the Primary Classification template.

You can easily reset a manual classification assignment to that set by the Device Classification Engine. Under the Cancel Actions action, select **Revert to Suggested Operating System Classification**.

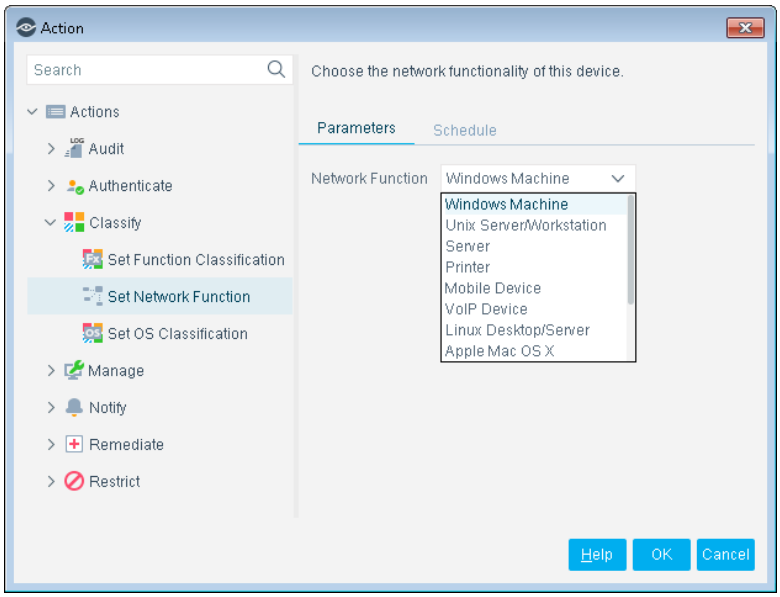
Revert to Suggested OS Classification

Set Network Function

This action lets you set a *Network Function* property value manually. You may need to do this if devices could not be classified by an Asset Classification policy or if you would like to reclassify them.

After a device is classified, it is added to the related Asset Classification group, provided that the Asset Classification template was deployed.

Primary Classification policies do not use the Network Function *property.*



Classify Device by Network Function

See Asset Classification and Primary Classification Templates for details about the Asset Classification policy template.

You can easily reset a manual classification assignment to that set by the Device Classification Engine. Under the Cancel Actions action, select **Cancel Manual Network Function Classification**.

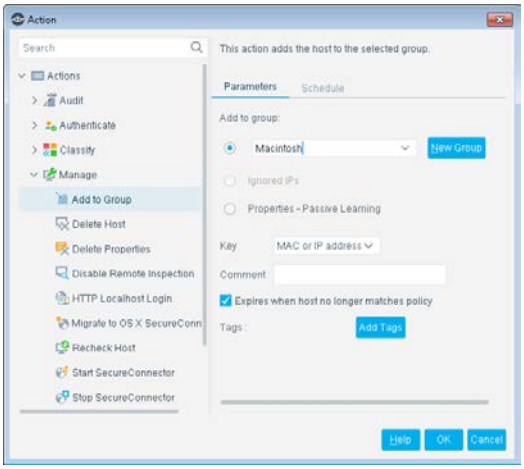
Manage Actions

This section describes actions that manage endpoints:

- Add to Group
- Add Label Action
- Delete Label Action
- Delete Host
- Delete Properties
- Disable Remote Inspection
- HTTP Localhost Login
- Recheck Host
- Start SecureConnector / Stop SecureConnector
- Upgrade OS X SecureConnector
- Set Counter Action

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.



Add to Group Action

Specify the group to which endpoints are added:

- To add endpoints to an existing group, select the first radio button 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 List.
- Select **Properties - Passive Learning** to add endpoints to the *Properties - Passive Learning* group; CounterACT never contacts endpoints in this group to resolve properties, even for policy evaluation. See Restricting Endpoint Inspection for more information.

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 CounterACT Groups.

  When the action adds endpoints to the Ignored IPs *group, policies ignore members of this group, and the* ***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. CounterACT detects group association based on this value.

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.

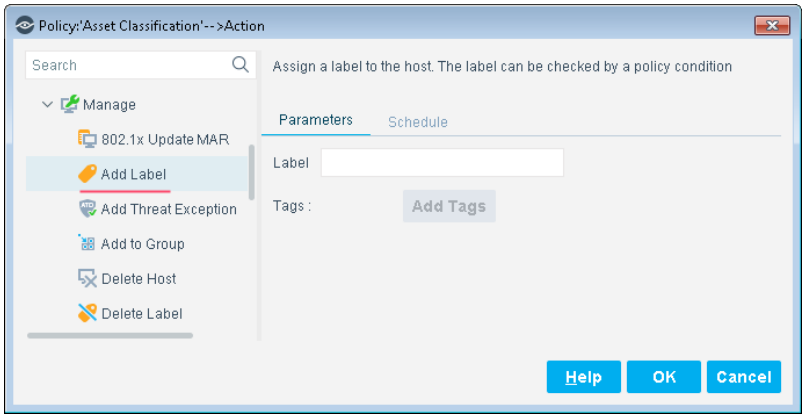
View Member-of-group Assignments to Troubleshoot Policy Matches

You can quickly troubleshoot an endpoint policy match by viewing member-of-group assignments per policy. This information is graphically displayed in a *Policy flow* diagram accessed from the *All Policies* 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.

Add Label Action

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 allows you to construct complex policy behaviors that track endpoint history.

This 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.

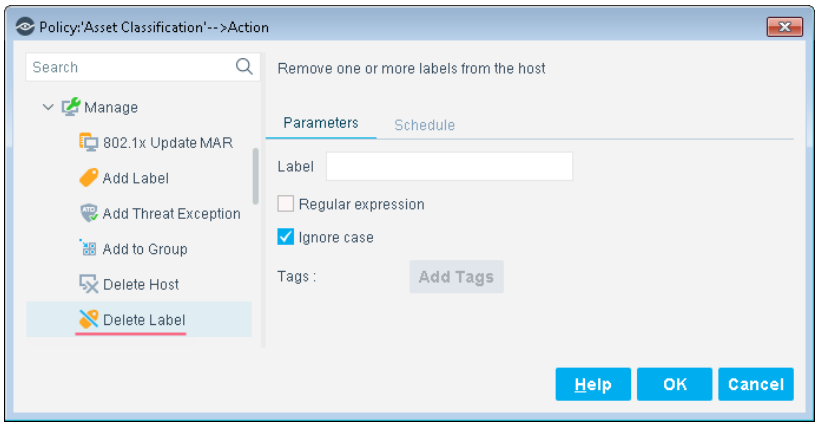


In the Label field, define the label text. The label can combine static text strings and endpoint-specific information. Select **Add Tags** to insert data tags that resolve to host property values. Labels are listed with other endpoint details in Home and Asset Inventory views.

Delete Label Action

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 allows you to construct complex policy behaviors that track endpoint history.

This 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.



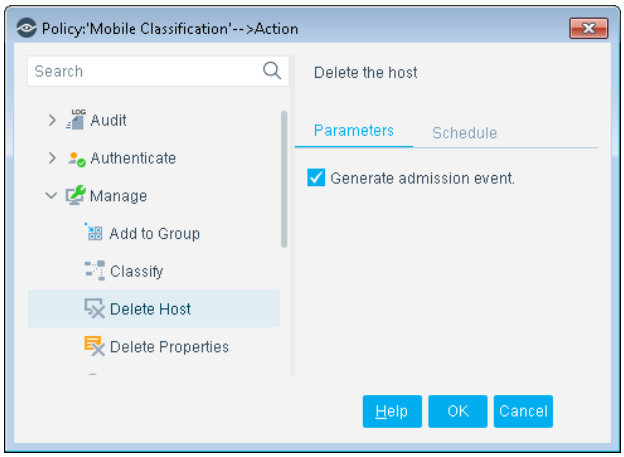
In the Label field, define the label text. The label can combine static text strings and endpoint-specific information. Select **Add Tags** to insert data tags that resolve to host property values.

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 labels only by spelling.

Delete Host

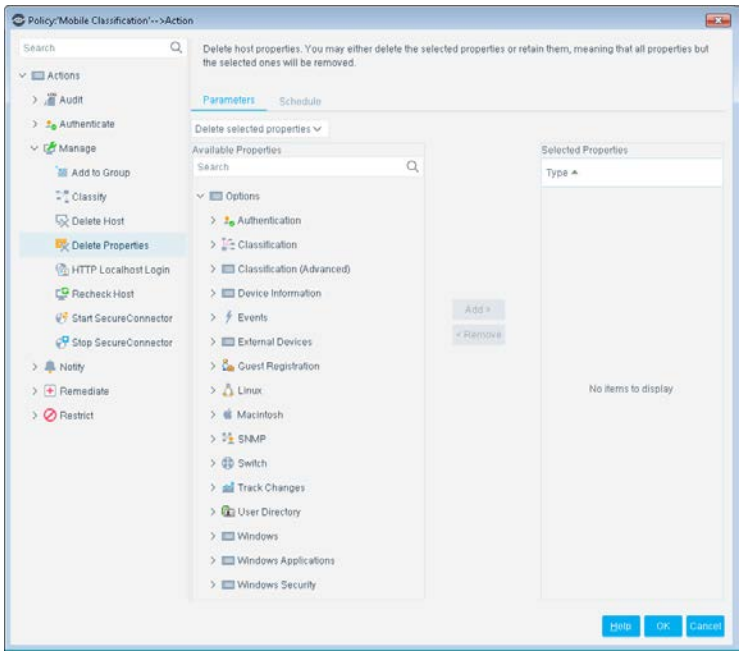
This action lets you instruct CounterACT to delete endpoints detected in a policy. Select **Generate admission event** to rediscover endpoints immediately after they are deleted. When you clear the checkbox, endpoints will be rediscovered after they generate traffic.



Delete Host Action

Delete Properties

This action lets you instruct CounterACT 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 will be evaluated after an endpoint generates traffic.



Delete Properties Action

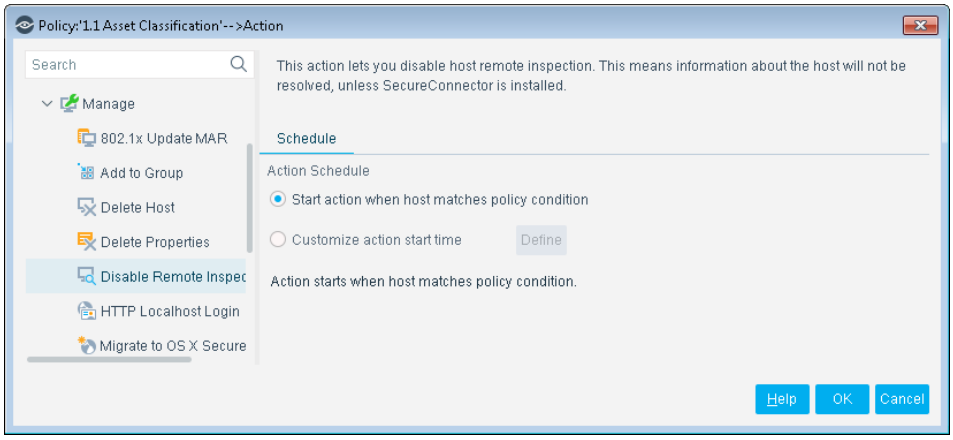
Disable Remote Inspection

This action instructs CounterACT 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 cancelled for the endpoint.

This action may be useful in situations where administrators want to minimize traffic to and deep inspection of sensitive computers at sensitive times.

For example, CounterACT 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 that are managed using SecureConnector are not affected by this action.



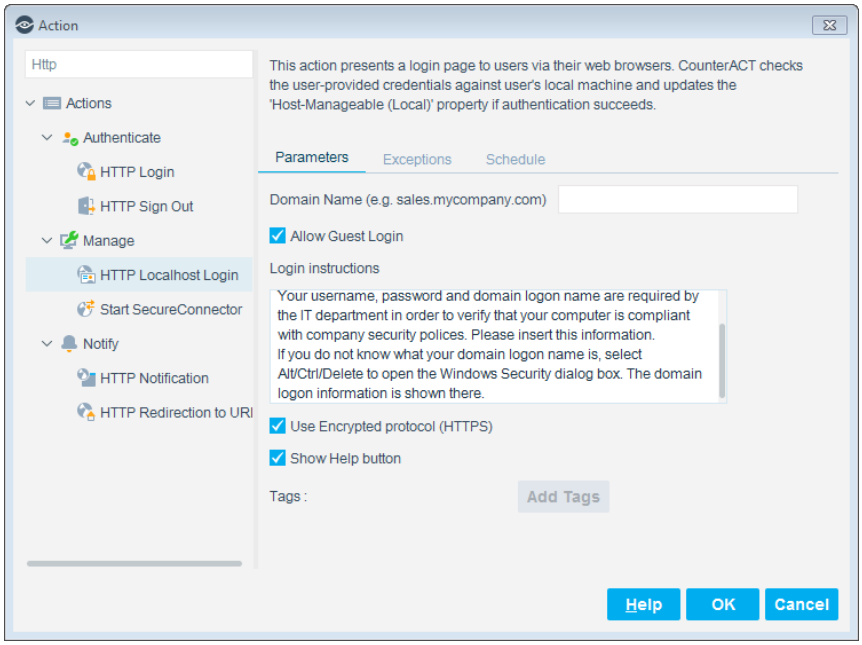
Disable Remote Inspection Action

HTTP Localhost Login

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.

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.

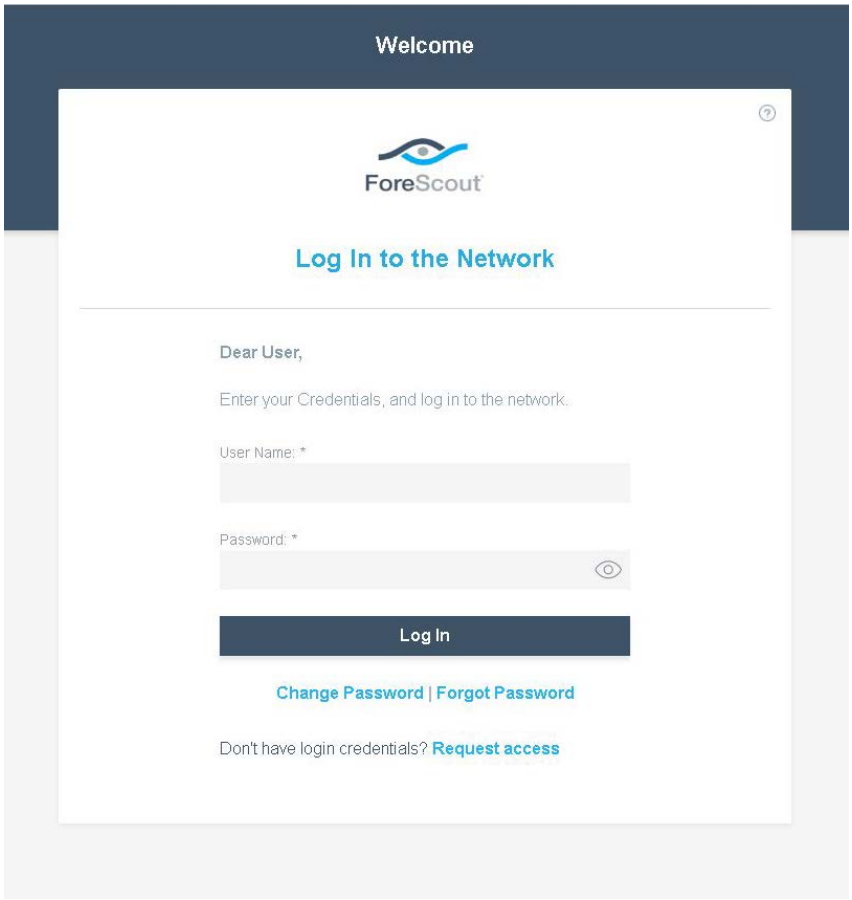
HTTP Localhost Login is disabled whenever HTTP Redirection is disabled. For more information, see Disabling Web Portals.



HTTP Localhost Login Action

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 cancelled, removing all the limitations imposed.

If you think login credentials may not be available to users and do not want to limit their access, you can allow guest login to the web. To do this, select **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 as such is blocked from your network, but allowed web access.



Login Page Displayed at the Endpoint

The network user is prompted with a Login page at 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 the **Use Encrypted protocol (HTTPS)** checkbox 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 more information about this transmission method.

Recommended Conditions

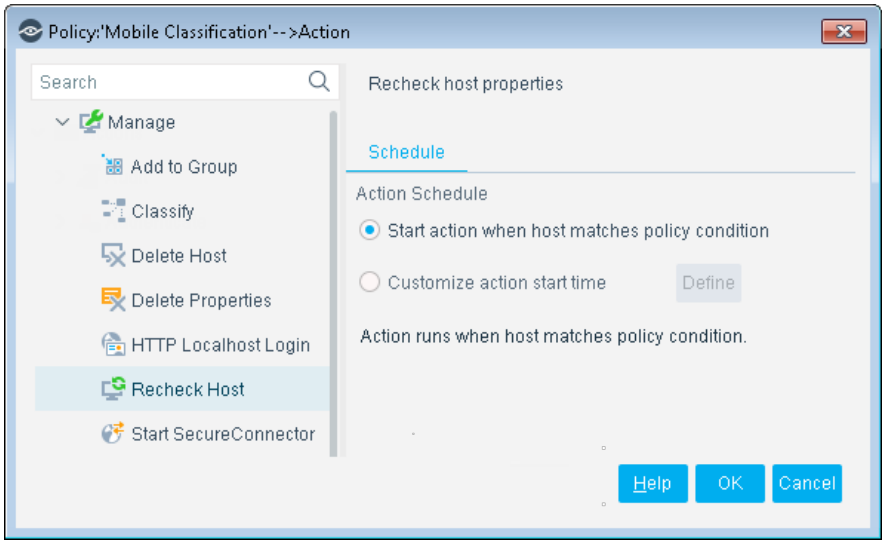
When using this action, you should configure the following condition properties. Use the ***AND*** value between both properties.

- 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 this action to instruct CounterACT to recheck endpoints against conditions defined in a policy, i.e. if the endpoints match or do not match the policy conditions.

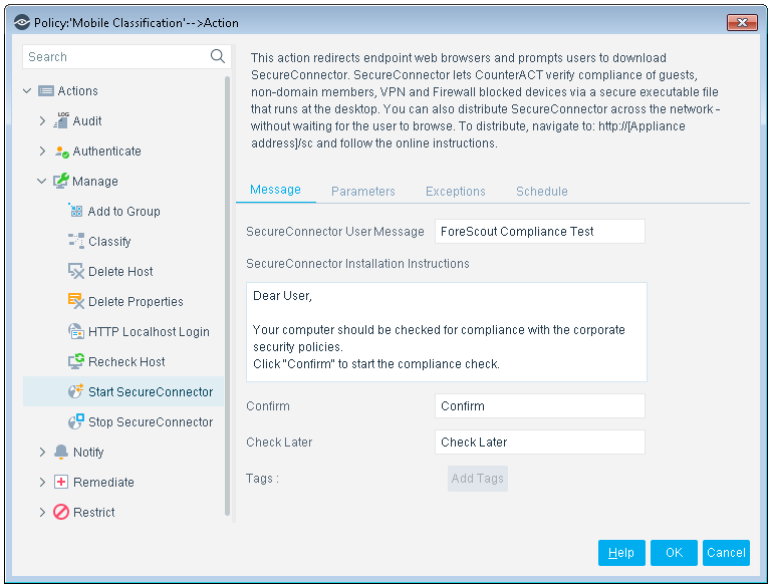


Recheck Host Action

Start SecureConnector / Stop SecureConnector

The *Start SecureConnector* and *Stop SecureConnector* actions let you install or stop CounterACT's SecureConnector, a light footprint executable that runs at the endpoint for the purpose of making endpoints manageable and for performing or optimizing certain actions.

The Start SecureConnector *action is disabled whenever HTTP Redirection is disabled. For more information see* [Disabling Web Portals].



Start SecureConnector Action

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 CounterACT. If neither criterion is met, the endpoint cannot be managed. This occurs typically for:

- Endpoints that are guests on the network
- Domain credentials that do not work or are not available
- Endpoints that are not part of the domain
- VPN users or wireless networks

Several policy properties are available for detecting *unmanageable* endpoints.

SecureConnector is also available when working with macOS/OS X and Linux endpoints. Depending on the endpoint operating system, this action is implemented by the HPS Inspection Engine, the Linux Plugin, or the OS X Plugin. Refer to the relevant plugin configuration guide for details.

Performing or Optimizing Certain Actions

Manageable endpoints can use SecureConnector for the following actions:

- *Assign to VLAN* on VoIP action (required)
- *Disable External Device* action (required)
- *Send Balloon Notification* action (required)
- *Disable Dual Homed* action (required)
- Improve kill frequency when working with the *Kill Process* , *Kill Instant Messaging* and *Kill Peer-to-peer* actions.

These actions detect and halt specific Windows processes. If the endpoint has SecureConnector installed the process is killed once per second; if not, the process is killed once per minute (recommended).

To improve frequency, you should run the *Start SecureConnector* action described here and also make the required configuration in the HPS Inspection Engine. For details, select **Options** from the **Tools** menu, select **HPS Inspection Engine** and then select the SecureConnector tab.

More about SecureConnector

For details about how SecureConnector works; supported operating systems, and installation methods other than the ones described here, see the *HPS Inspection Engine Configuration Guide*. For information about SecureConnector support for macOS/OS X and Linux endpoints, see the *Configuration Guides* for the Linux Plugin, and the OS X Plugin.

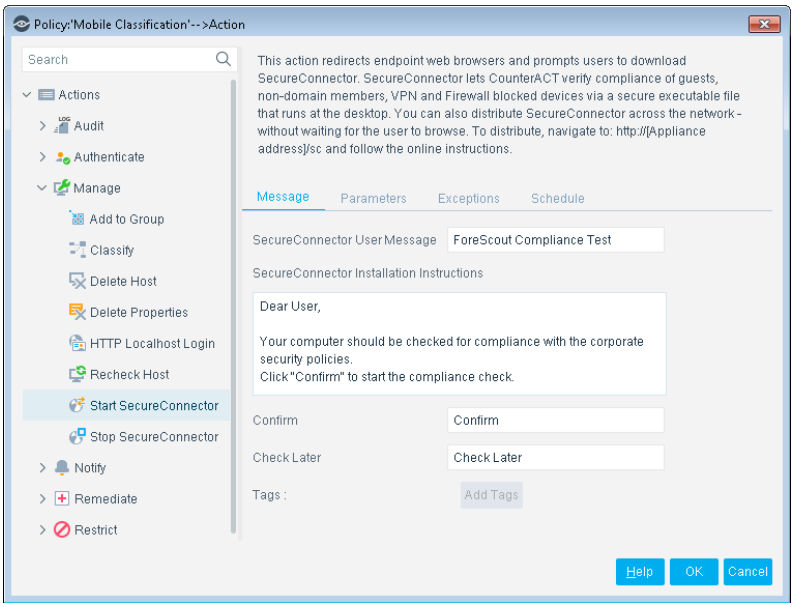
Select **Options** from the **Tools** menu. Select **Modules**. Select this plugin and then select **Help**.

Working with the Action

This section describes how to run SecureConnector via the *Start SecureConnector* action.

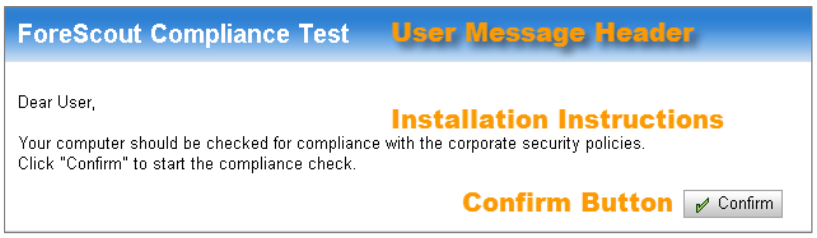
Message Tab

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*.



Message Tab

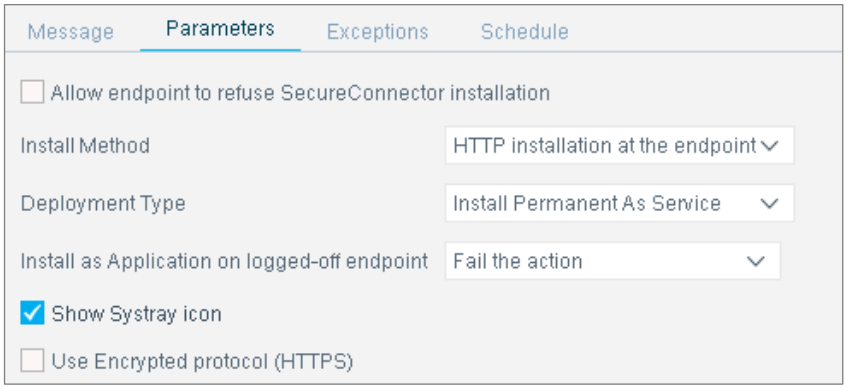
SecureConnector User Message	Text displayed as the page header.
(Message Text)	Body text of the message.
Confirm	Text displayed on the Confirm button. When users select this button, SecureConnector installation proceeds immediately.
Check Later	Text displayed on the Check Later button. When users select 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.



SecureConnector Notification and Buttons

Parameters Tab

Use this tab to define Start SecureConnector installation and deployment parameters.



Start SecureConnector Action – Parameters Tab

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 either the *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 Localizing CounterACT Redirected Web Pages and Messages for details. ▪ *Remote installation*: Perform remote installation on manageable endpoints using domain credentials. CounterACT uses a script when this option is selected. ▪ *Both*: Both methods are activated simultaneously. If an 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 always be removed via the uninstall option in the Start>Programs menu. ▪ *Install Permanent as Application/Service*: Install SecureConnector permanently as an endpoint application or service on the endpoint. Using the service option provides the following advantages: - Enhances SecureConnector performance, especially when working with interactive actions, such as *Run Script on Windows*. - The service can be run before login and after logout. Refer to the *HPS Inspection Engine Configuration Guide* for details. Select Options from the **Tools** menu. Select **Modules**. Select this plugin and then select **Help**.

Install as application on logged-off endpoint	When the Deployment Type is set to *Install Permanent as Application* this setting determines how CounterACT proceeds if the user is not logged in to the endpoint when CounterACT attempts to install SecureConnector. ▪ *Fail the action* – When the user is not logged in, SecureConnector is not installed. ▪ *Install with system permissions* – when the user is not logged in, SecureConnector is installed using system account permissions, and runs on the endpoint under these permissions. When the user logs on after system restart, SecureConnector installs itself under the user account.
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 more information.

Schedule Tab

Define an action schedule. See Creating Action Schedules for details.

Recommended Conditions

You can use the following properties to help you identify unmanageable endpoints:

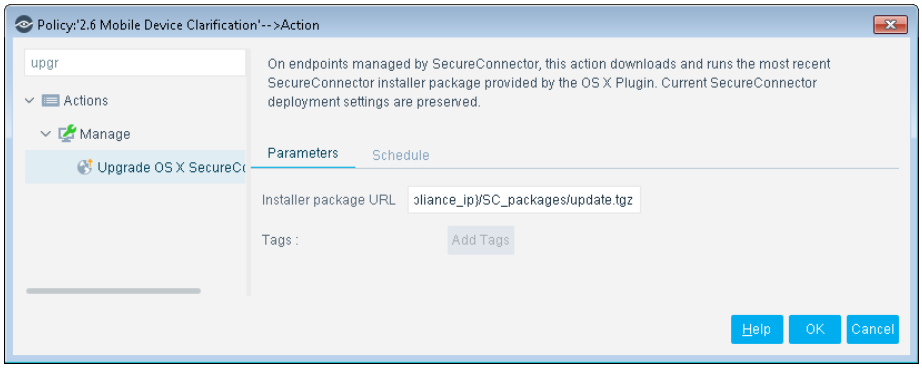
- Windows Manageable (Connector)
- Windows Manageable (Domain)
- Windows Manageable (Local)

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.

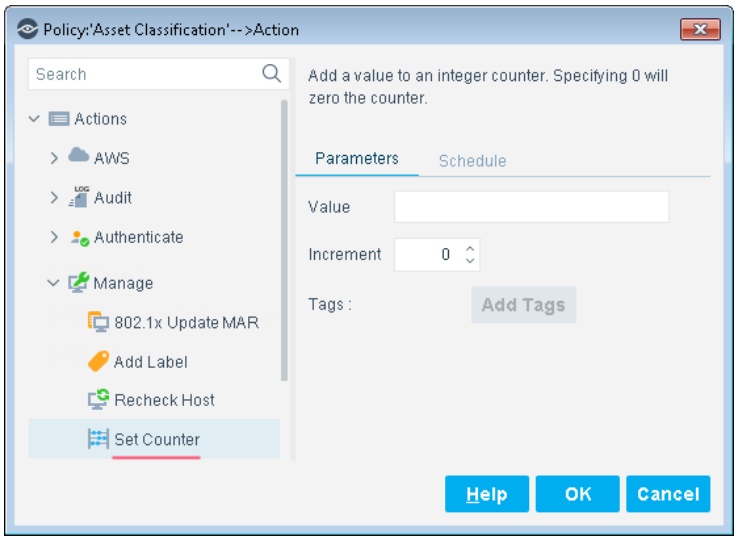
In the Installer package URL field, specify a valid network path to the update.tgz archive that is used to update endpoints. By default, this field points to the file that the OS X Plugin places on each CounterACT Appliance. If you copy this archive to a content distribution network or server, specify the full network path to this new location. For details, refer to the *OS X Plugin Configuration Guide*.



Upgrade OS X SecureConnector Action

Set Counter Action

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 Setting and Incrementing Counters for more information.

Notify Actions

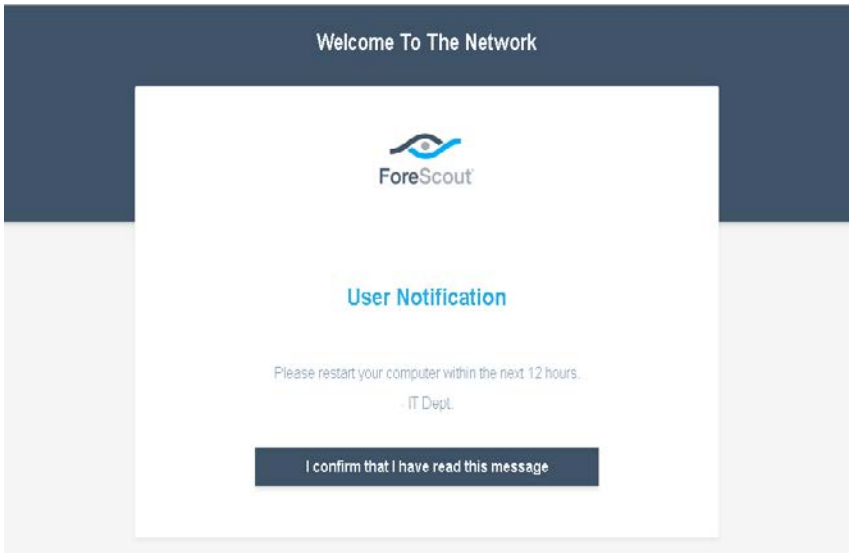
This section describes actions used for communicating with endpoint users:

- HTTP Notification
- HTTP Redirection to URL
- Send Balloon Notification
- Send Email
- Send Email to User

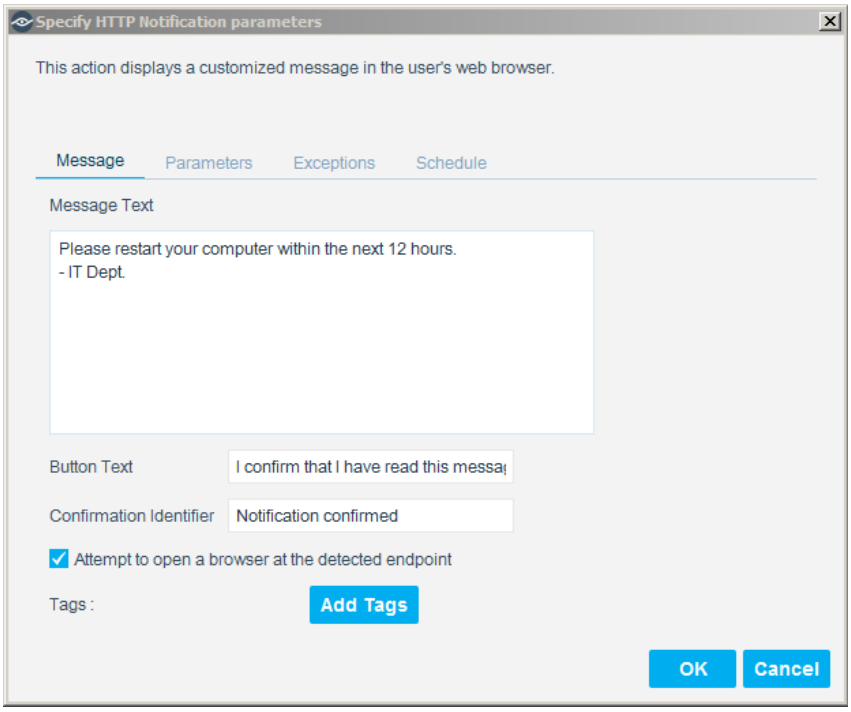
HTTP Notification

The user's web session is redirected when attempting to access the web. The user is presented with a message that you compose.

HTTP Notification is disabled whenever HTTP Redirection is disabled. For more information, see Disabling Web Portals.



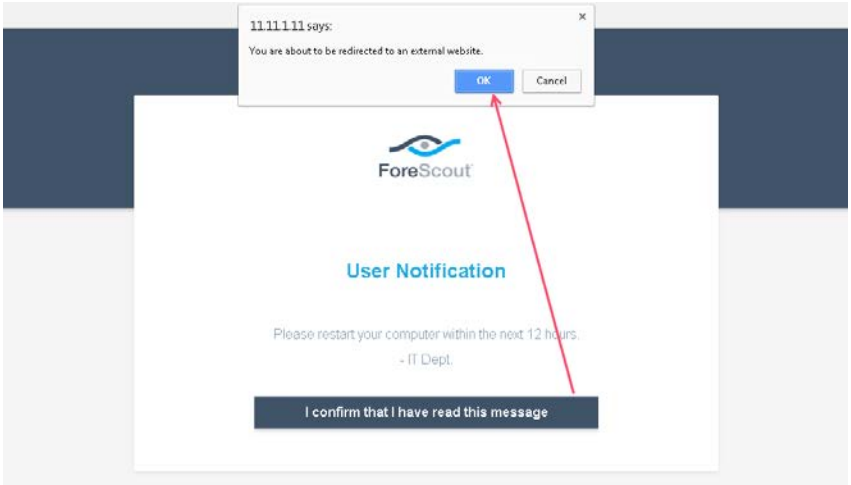
Notification Page



HTTP Notification Action

Web sessions are redirected until:

- The user confirms reading the message. See the Parameters Tab section for information about how to do this. After confirmation, a pop-up dialog box is displayed informing users that they are being redirected to an external website.



HTTP Notification – User Confirmation

- The endpoint is released via the Home view, Detections pane or Assets Portal.

Message Tab

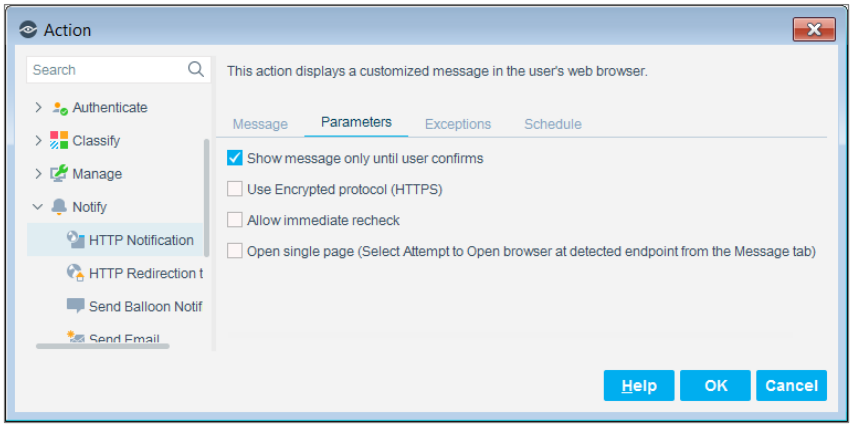
Type the message that you want the user to read.

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 then 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.) CounterACT uses a script when this option is selected. Refer to 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, see "Tuning" in the *HPS Inspection Engine Configuration Guide*.

Parameters Tab



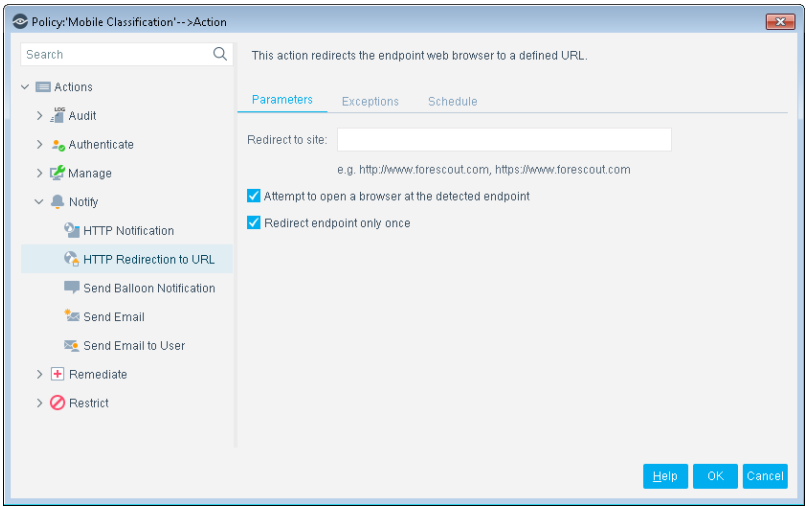
HTTP Notification Action

- 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 more information about this transmission method.
- 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 CounterACT 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 **Open single page** to only redirect the first web browser tab, allowing the user to continue browsing in other tabs. Verify that the **Attempt to open a browser at the detected endpoint** checkbox from the Message tab is selected.

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 customized message.

HTTP Redirection to URL is disabled whenever HTTP Redirection is disabled. For more information, see Disabling 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.) CounterACT uses a script when this option is selected. Refer to the *HPS Inspection Engine Configuration Guide* for details about how scripts work. Select **Options** from the **Tools** menu. Select **Modules**. Select this plugin and then select **Help**.

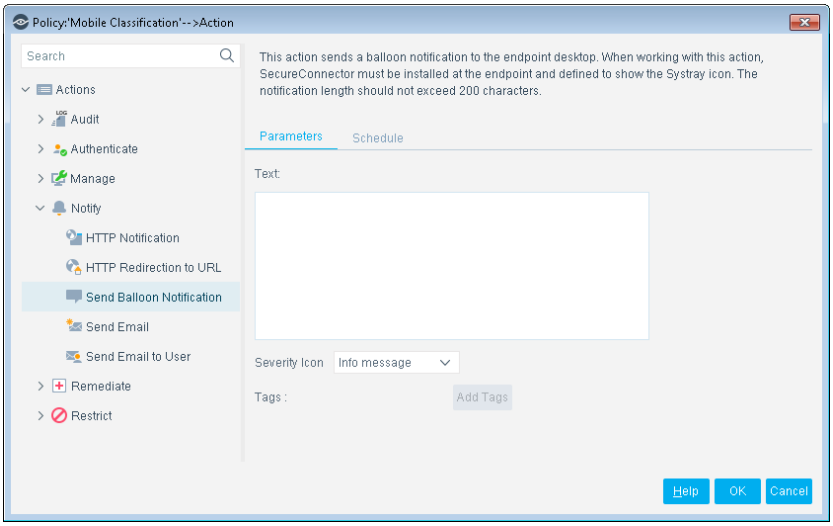
By default, the action is only applied one time during the match period. This means that the first time the end user enters a URL in the web browser, the endpoint is redirected to the URL configured in action. You can configure this action to continuously apply to endpoints that match the policy rule by clearing the **Redirect endpoint only once** checkbox. This means 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 is 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.

The character limit may vary slightly in certain languages.



Send Balloon Notification

Balloon messages are displayed in the endpoint system tray.

Balloon Message

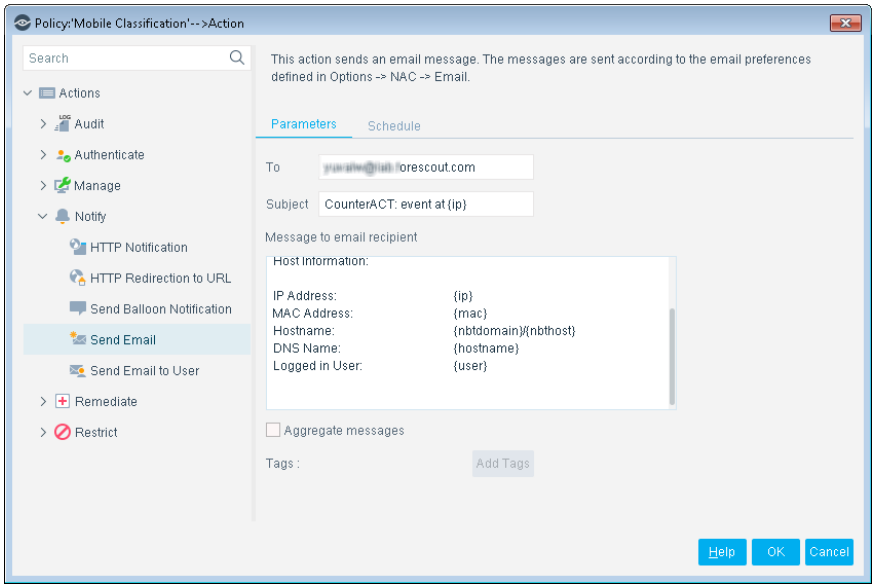
Send Email

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 Working with Property Tags for more information.

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

See Policy Preferences for more information.

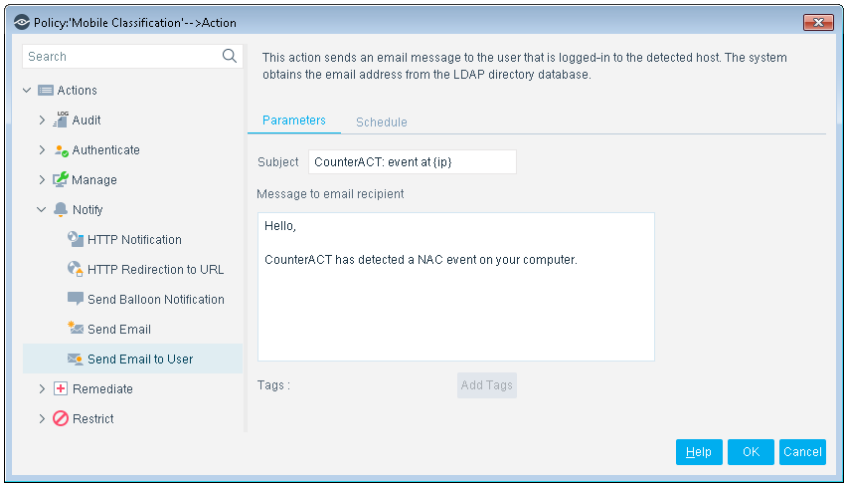


Send Email Action

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 Email to User

This action sends an email message to the User Directory, *User Mail Address* that is registered with the detected endpoint.



Send Email to User Action

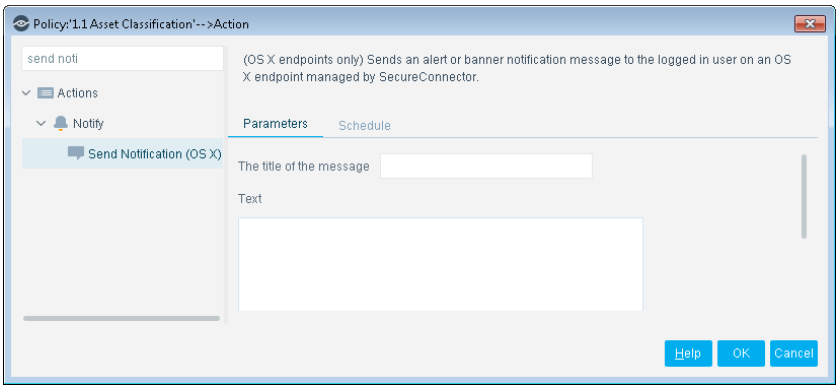
Basic information about the endpoint is displayed by default in the email message. Add additional text as required. When composing the message, you can insert any number of property tags. For example, if you enter {ip}, the IP address at which the event was detected is automatically inserted into the message. See Working with Property Tags for more information.

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 Working with Property Tags for more information.

Banner notifications appear briefly on screen. Alerts persist on screen until the user interacts with them.



Send Notification (OS X) Action

Remediate Actions

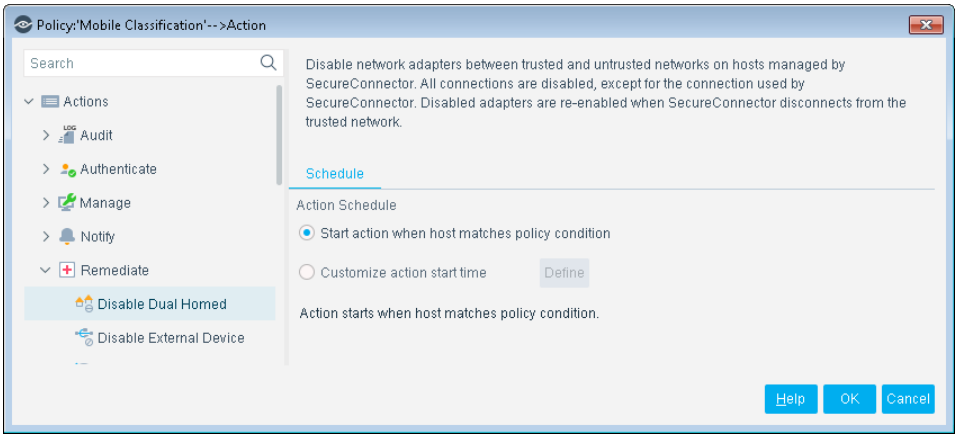
This section describes actions that help you remediate endpoint vulnerabilities, install security patches, kill processes and more:

- Disable Adapters on Dual Homed Devices
- Disable External Devices
- Expedite IP Discovery
- Kill Instant Messaging
- Kill Cloud Storage
- Kill Peer-to-Peer
- Kill Process on Linux and Kill Process on Macintosh
- Kill Process on Windows
- Run Script on CounterACT
- Run Script on Linux and Run Script on Macintosh
- Run Script on Windows
- Set Registry Key on Windows

- Start Antivirus
- Start Macintosh Updates
- Start Windows Updates
- Update Antivirus
- Windows Self Remediation

Disable Adapters on Dual Homed Devices

The 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.



Disable Dual Homed Adapters

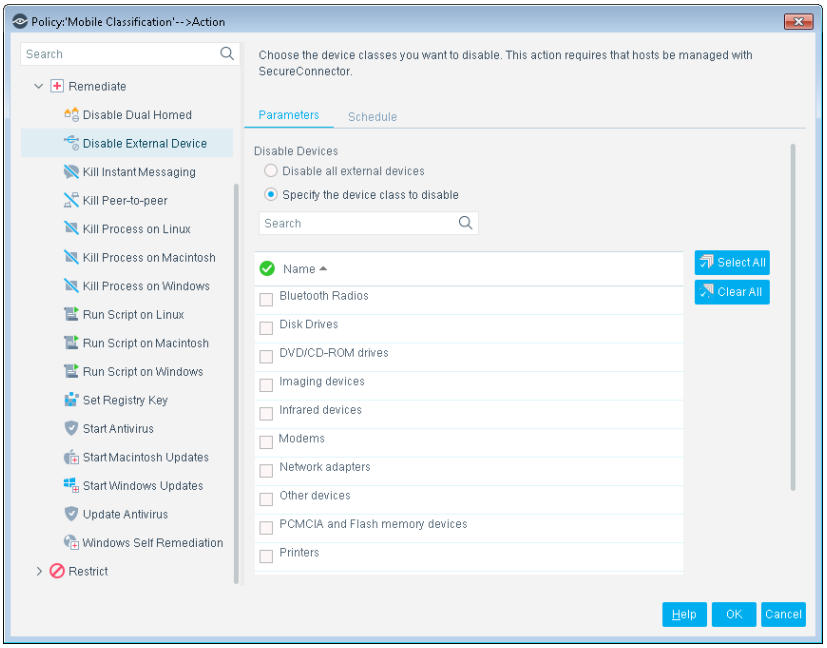
Requirements

- Verify that the endpoint is managed by SecureConnector.

Disable External Devices

This action disables external devices connected to Windows endpoints; for example, USB mass storage devices, modems, printers, cameras, NIC cards, PCMCIA, CD/DVD, gaming, smartphones, etc. The devices remain blocked until the action is cancelled, 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.

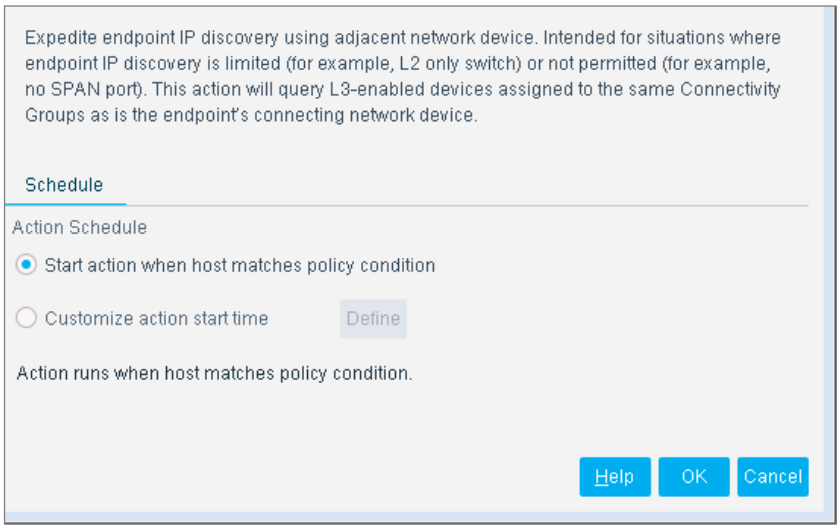
This action requires that endpoints be managed with SecureConnector. You can automatically install SecureConnector when deploying this action. Select **Options** from the **Tools** menu, select **HPS Inspection Engine** and then select the SecureConnector tab.



Disable External Device Action

Expedite IP Discovery

The *Expedite IP Discovery* action is a remediate action provided by the Switch Plugin. Use the *Expedite IP Discovery* 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.



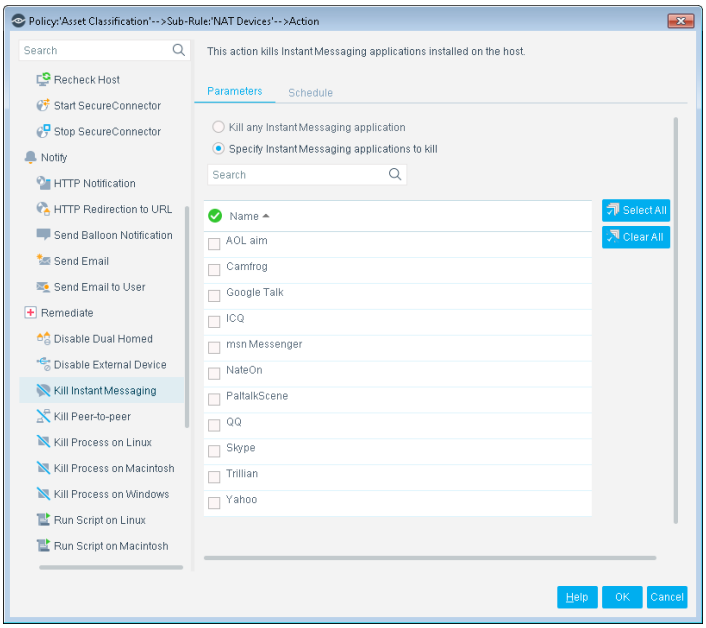
Expedite IP Discovery Action, Configuration Window

For details about this action, including the symptoms and root causes of delayed endpoint IP discovery, refer to the CounterACT Switch Plugin Configuration Guide. Select **Options** from the **Tools** menu. Select **Modules**. Select the Switch Plugin and then select **Help**.

Kill Instant Messaging

This 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 the *Windows Applications Configuration Guide* for more information about the module. Select **Options** from the **Tools** menu. Select **Modules**. Select **Windows Applications** and then select **Help**.



Kill Instant Messaging Action

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 when using this action:

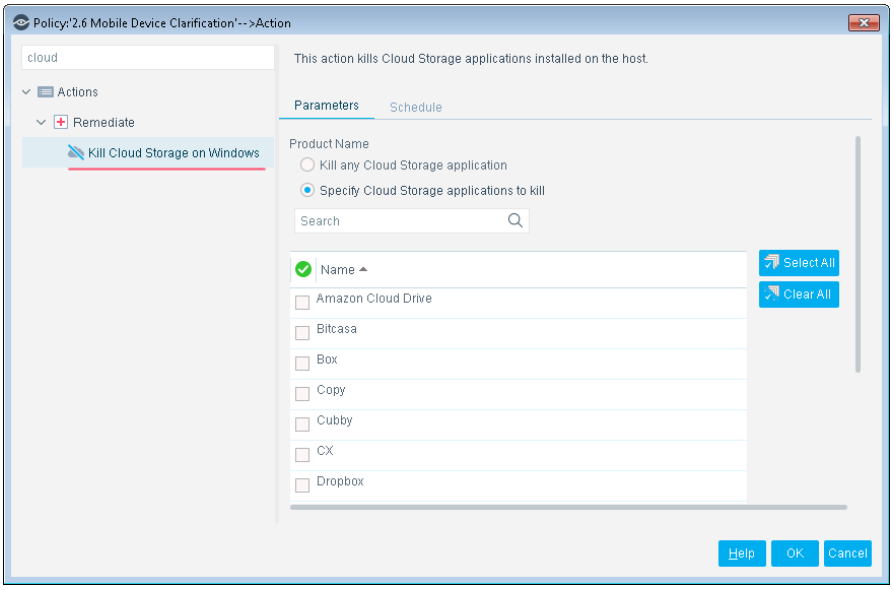
1. Select **Options** from the **Tools** menu and then select **HPS - Inspection Engine**.
2. Select the **SecureConnector** tab.
3. Select **SecureConnector**.
4. Select the **Automatically run SecureConnector on Windows endpoints...** checkbox.
5. Select **Apply** and then **Close**.

*CounterACT uses a script on the endpoint to apply this action if the endpoint is managed via domain credentials (**Windows Manageable (Domain)** is True). See the* HPS Inspection Engine Configuration Guide *for details about scripts. Select **Options** from the **Tools** menu. Select **Modules**. Select this plugin and then select **Help**.*

Kill Cloud Storage

This 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.



Kill Cloud Storage Action

To increase kill frequency, CounterACT 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.

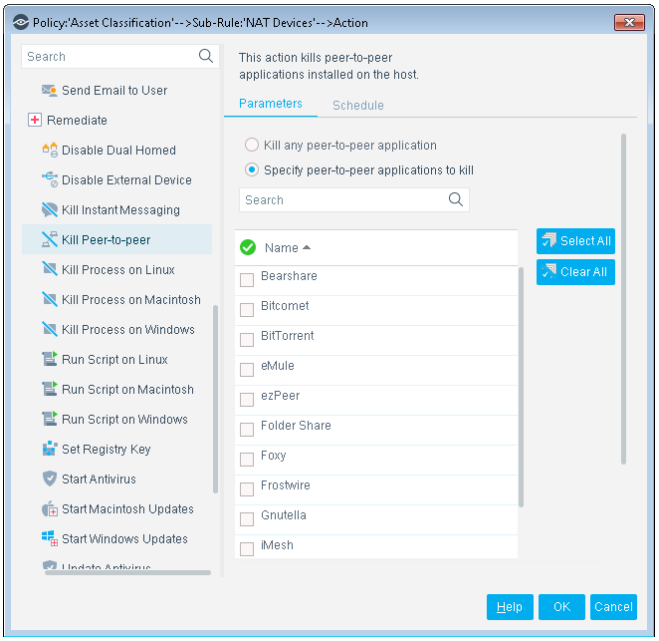
See the *HPS Inspection Engine Configuration Guide* for details about SecureConnector configuration. Select **Options** from the **Tools** menu. Select **Modules**. Select this plugin and then select **Help**.

*CounterACT uses a script on the endpoint to apply this action if the endpoint is managed via domain credentials (**Windows Manageable (Domain)** is True). See 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 **Options** from the **Tools** menu. Select **Modules**. Select **Windows Applications** and then select **Help**.

Kill Peer-to-Peer

This action halts specific peer-to-peer applications installed at Windows endpoints.



Kill Peer-to-Peer Action

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 when using this action:

1. Select **Options** from the **Tools** menu and then select **HPS - Inspection Engine**.
2. Select the SecureConnector tab.
3. Select the **Automatically run SecureConnector on Windows endpoints...**checkbox.
4. Select **Apply** and then **Close**.

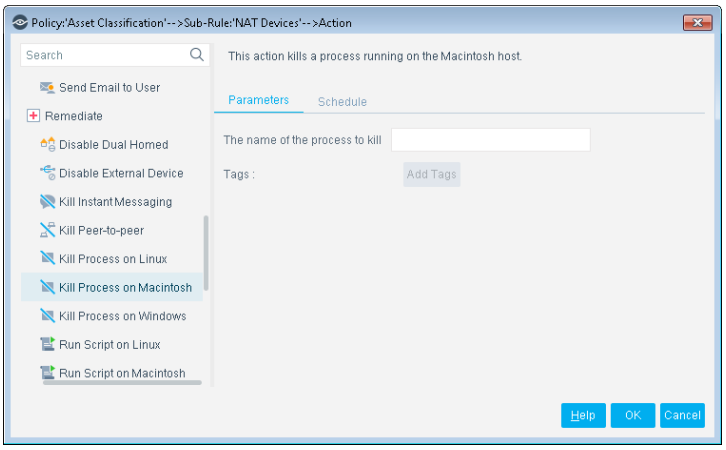
*CounterACT uses a script on the endpoint to apply this action if the endpoint is managed via domain credentials (**Windows Manageable (Domain)** is True). See the* HPS Inspection Engine Configuration Guide *for details about scripts. Select **Options** from the **Tools** menu. Select **Modules**. Select this plugin and then select **Help**.*

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 **Options** from the **Tools** menu. Select **Modules**. Select **Windows Applications** and then select **Help**.

Kill Process on Linux and Kill Process on Macintosh

These actions halt 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 using the **Add Tags** button. For example, if you enter the {user} tag, the user name of the endpoint is automatically inserted into the process name. See Working with Property Tags for more information. 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.

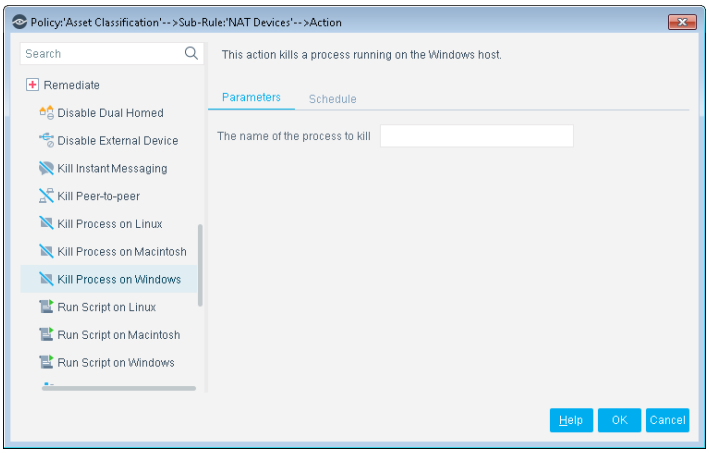


Kill Process Action

Kill Process on Windows

This action halts 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 using the **Add Tags** button. For example, if you enter the {user} tag, the user name of the endpoint is automatically inserted into the process name. See Working with Property Tags for more information.



Windows Kill Process

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.

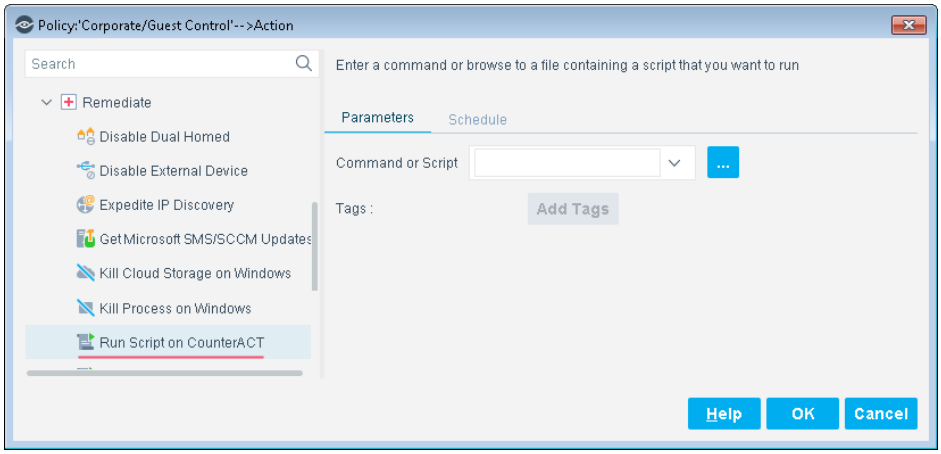
To install SecureConnector when using this action:

1. Select **Options** from the **Tools** menu and then select **HPS - Inspection Engine**.
2. Select the SecureConnector tab.
3. Select the **Automatically run SecureConnector on Windows endpoints...**checkbox.
4. Select **Apply** and then **Close**.

*CounterACT uses a script on the endpoint to apply this action if the endpoint is managed via domain credentials (**Windows Manageable (Domain)** is True). See the* HPS Inspection Engine Configuration Guide *for details about scripts. Select **Options** from the **Tools** menu. Select **Modules**. Select this plugin and then select **Help**.*

Run Script on CounterACT

This 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.



CounterACT evaluates the script or command for each endpoint that matches previous conditions of the policy.

If you are running a script in an action, the {IP} tag should 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.

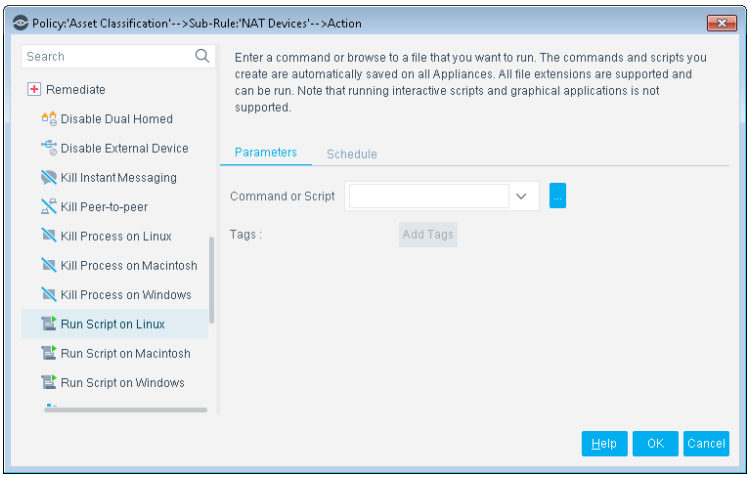
Run Script on Linux and Run Script on Macintosh

You can leverage scripts to:

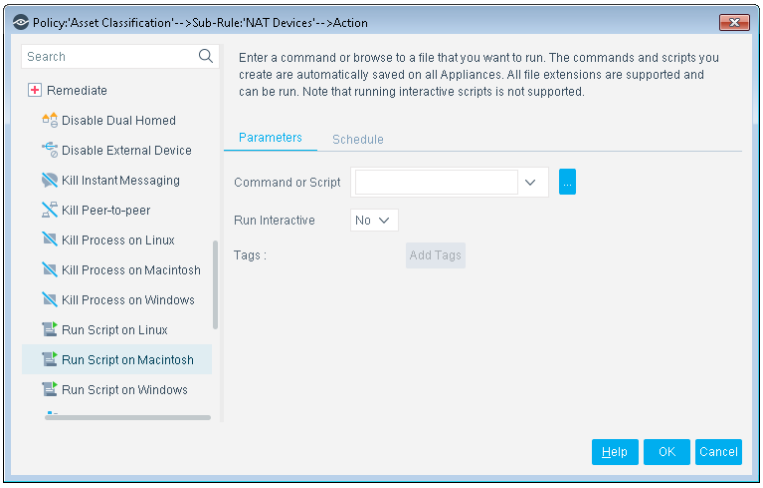
- Automatically run Macintosh and Linux updates.
- Automatically deploy vulnerability patches.
- Automatically delete files.
- Create customized scripts to perform any action that you want.

For example, to prevent music sharing, use these actions to run the following command on endpoints:

```
net share “my music”/delete
```



Run Script on Linux Action

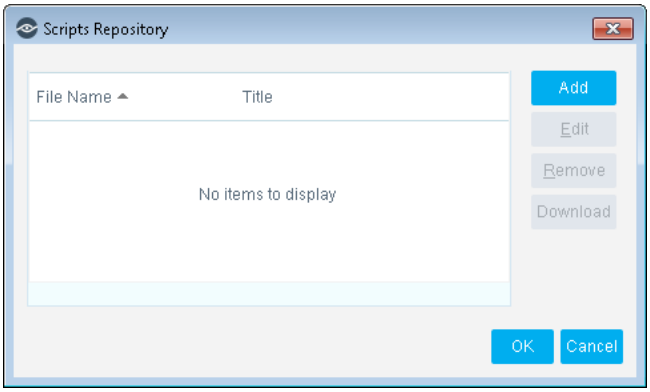


Macintosh Run Script Action

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.

To use these actions:

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 the Continue button to select from the repository of user-defined scripts and commands.



Scripts Repository Dialog Box

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 CounterACT does not use root credentials 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 CounterACT enter sudo mode. Refer to the *Linux Plugin Configuration Guide*.

3. Use the options of the Schedule tab to specify when the action is applied, to delay application of the action, or to specify repeat application of the action.

Run Script on Windows

This action is used to achieve automated, centrally managed remediation across the network. Leverage scripts, for example, to:

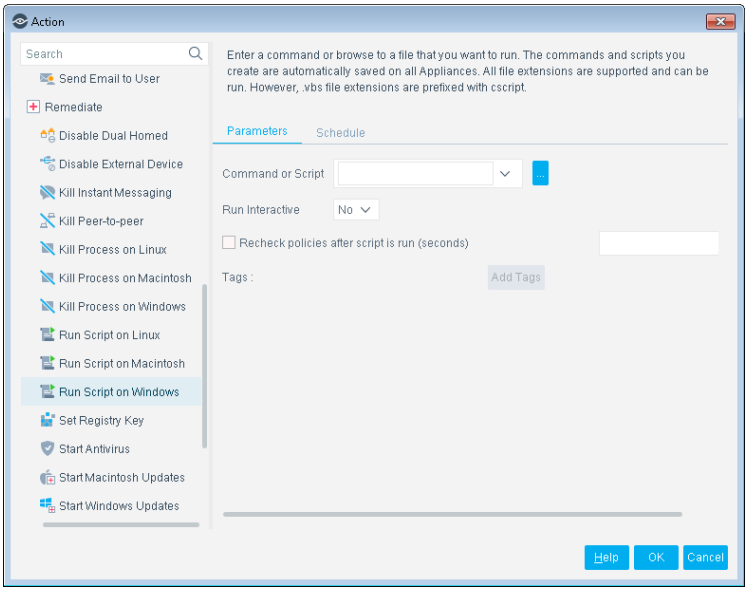
- Automatically run Windows updates.
- Automatically deploy vulnerability patches.
- Automatically delete files.

- Automatically deploy antivirus updates.
- Create customized scripts to perform any action that you want.

This action may only be used on managed Windows machines.

Select **Yes** in the **Run Interactive** drop-down list if the script launches a process or dialog box at the endpoint.

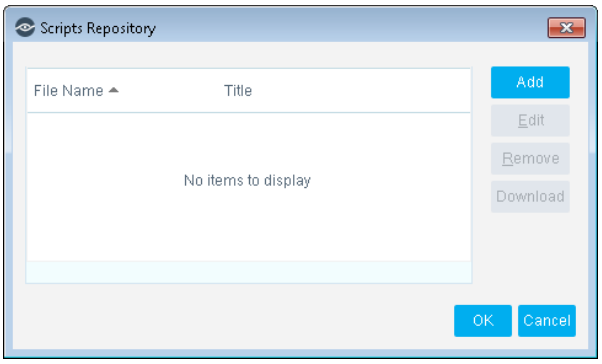
The Terminal Services service must be running if interactive scripts are used. If you use this action and it fails, the service may have been stopped.



Windows Run Script Action

Type a command or browse to a file that you want to run. If you use a file that exists on the endpoint, type 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 scripts that you created.



Scripts Repository Dialog Box

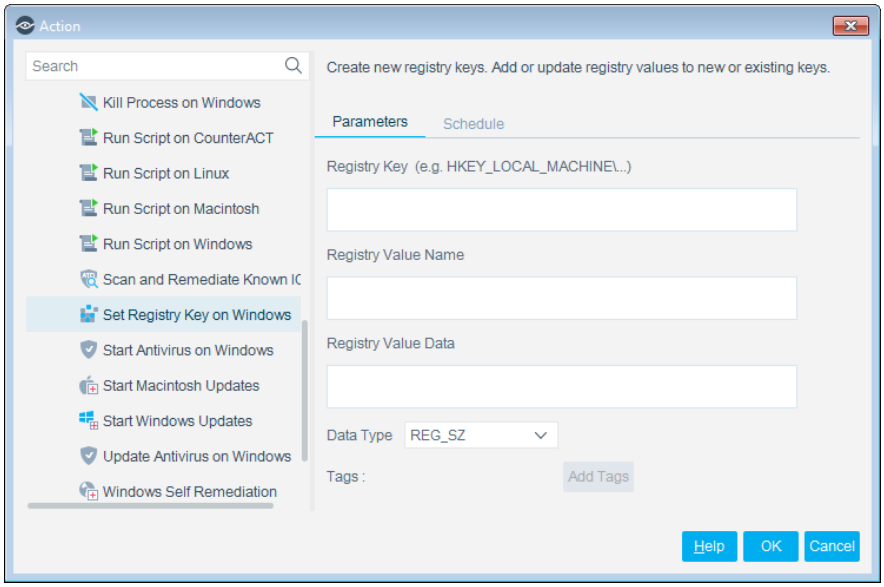
Quickly recheck endpoints after they are remediated by the script. Select **Recheck policies after script is run (seconds)** and indicate how many seconds to wait before carrying out the recheck.

*CounterACT uses a script on the endpoint to apply this action if the endpoint is managed via domain credentials (**Windows Manageable (Domain)** is True). See the* HPS Inspection Engine Configuration Guide *for details about scripts. Select **Options** from the **Tools** menu. Select **Modules**. 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

CounterACT cannot set the registry key under "HKEY_LOCAL_MACHINE" unless permissions on the relevant registry key are set to everyone/full control.

*CounterACT uses a script on the endpoint to apply this action if the endpoint is managed via domain credentials (**Windows Manageable (Domain)** is True). See the* HPS Inspection Engine Configuration Guide *for details about scripts. Select **Options** from the **Tools** menu. Select **Modules**. 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

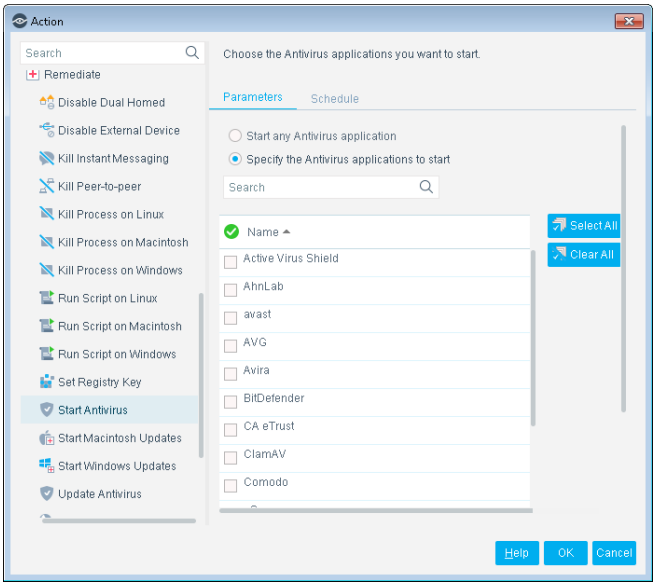
ddd

The strings **bbb** and **ccc** are separated by an end-of-line character.

*The string **__fsln__** begins and ends with two underscore characters.*

Start Antivirus

Launch antivirus applications that have been halted at Windows endpoints.



Start Antivirus Action

An extensive range of applications are supported. For example,

- Symantec
- McAfee

- Kaspersky
- AVG
- avast
- and more

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 **Options** from the **Tools** menu. Select **Modules**. Select **Windows Applications** and then select **Help**.

Suppress Splash Screens for Background Installation

As an option, you can configure CounterACT 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.

This option is available for users working with Symantec, McAfee and Trend Micro.

To suppress splash screens for the Update Antivirus action:

1. Log in to an Appliance CLI.
2. Submit the following command:

   `fstool set_property config.av_non_interactive_mode.value <vendor>`

   Where **`<vendor>`** may be Symantec, McAfee or Trend Micro.

Recommended Usage – Conditions

When using this action, you should configure the following condition properties:

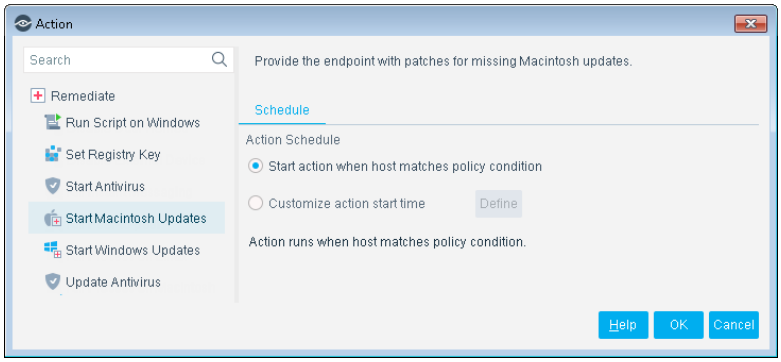
- Windows Security>Windows Antivirus Installed>Meets the following criteria
- Windows Security>Windows Antivirus Running>Does not meet the following criteria

Start Macintosh Updates

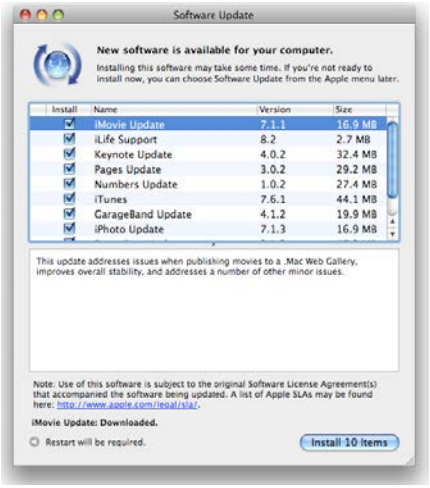
This action lets you provide the endpoint with patches for missing Macintosh updates. It displays a notification to end users indicating that specific security and other updates are missing on their machines. The notification includes a list of links that should be accessed in order to install the updates.

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.



Start Macintosh Updates Action



Macintosh Software Update

The Software Update page will continue 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.

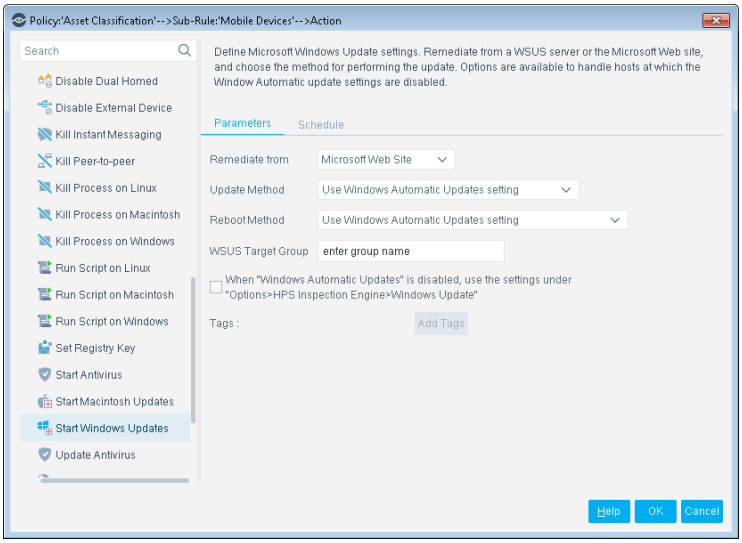
Start Windows Updates

This 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.



Start Windows Updates Action

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 **Options** from the **Tools** menu and then select **HPS Inspection Engine**.
2. Select the Windows Update tab.

3. Type the URL of the WSUS server and the reports server.

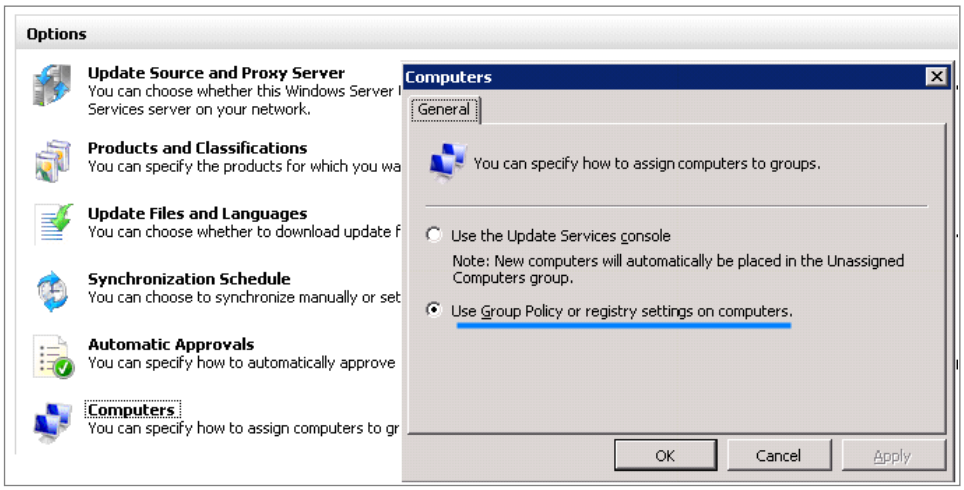
   You can test connection with the server by selecting **Test**.

4. Select **Apply** and **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**.



User Group Policy

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

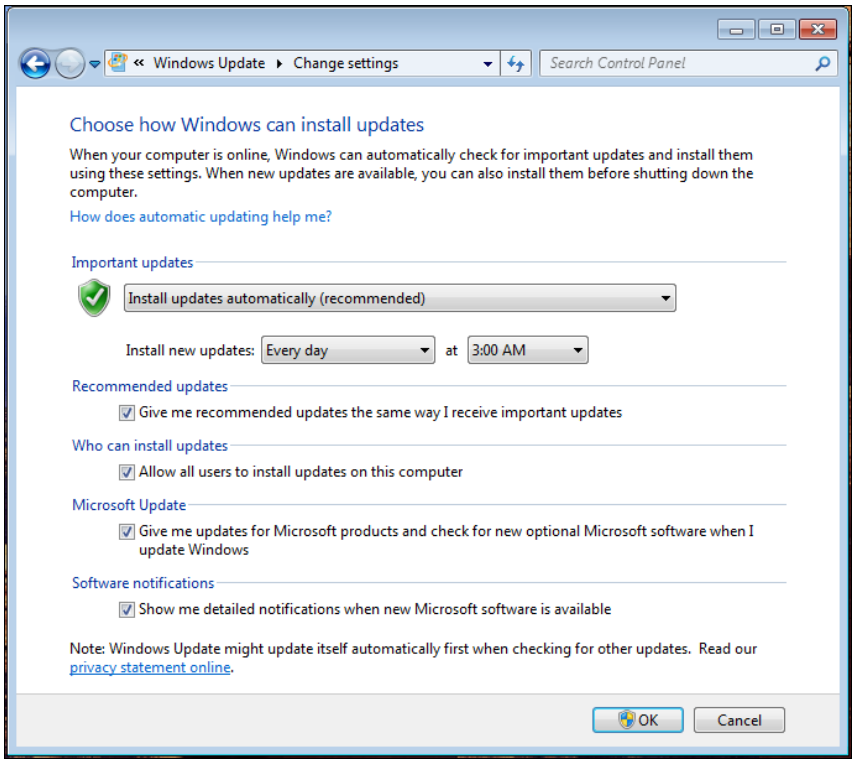
The endpoint user is notified that updates are available. The endpoint user can either update immediately or wait till later. Some patches may require machine reboot; in this case, CounterACT will reboot the machine according to endpoint settings.

The Windows Automatic update may have been defined to let the user decide which patches to install.

Use Windows "Automatic Updates" Settings

The Windows *Automatic Updates* settings are used to determine how the update is performed.

In a scenario where the Windows *Automatic Update* setting is defined to *Turn off Automatic Updates* and the action Update method is defined as *Use Windows "Automatic Updates" Settings*, the action will not be carried out. To force the update, see Handling Windows Automatic Updates That Are Turned Off.



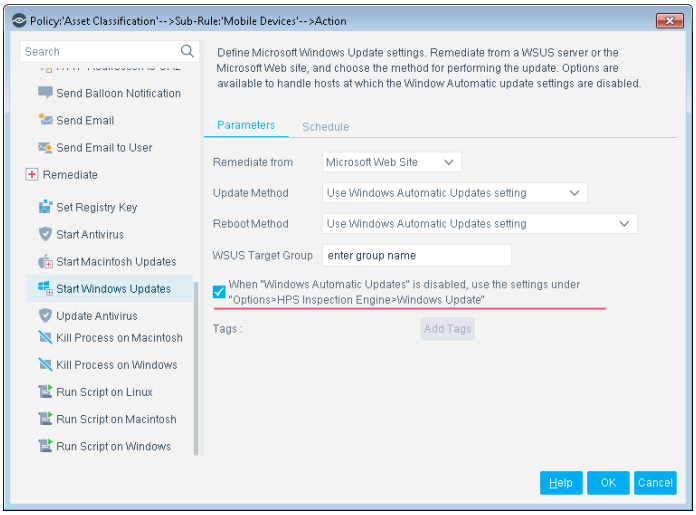
Windows Automatic Updates Dialog Box – Automatic Updates Turned off

Handling Windows Automatic Updates That Are Turned Off

In a scenario where the Windows endpoint *Automatic Update* setting is defined to *Turn off Automatic Updates* and the action is defined as *Use Windows "Automatic Updates" Settings*, the action will not be carried out. You can avoid this situation and force the update by carrying out the following configurations.

To handle Windows automatic updates that are turned off:

1. In the Windows Updates Dialog Box, select **When 'Windows Update' is disabled**. If the checkbox is cleared, and this scenario exists, the action will not be carried out.

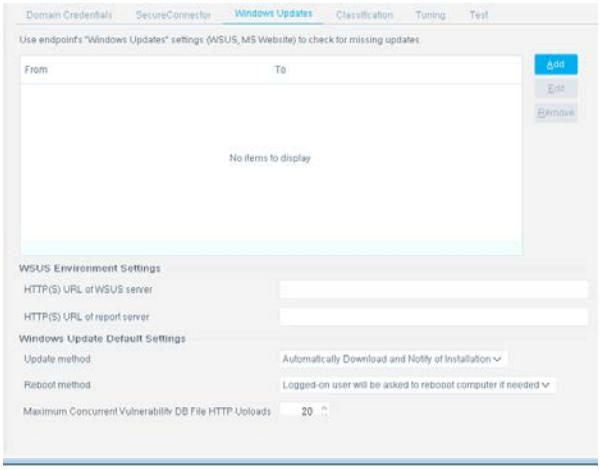


Start Windows Update

2. In the HPS Inspection Engine configuration pane:

   a. Select **Options** from the **Tools** menu and then select **HPS Inspection Engine**.

   b. Select the Windows Updates tab.



Windows Update 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

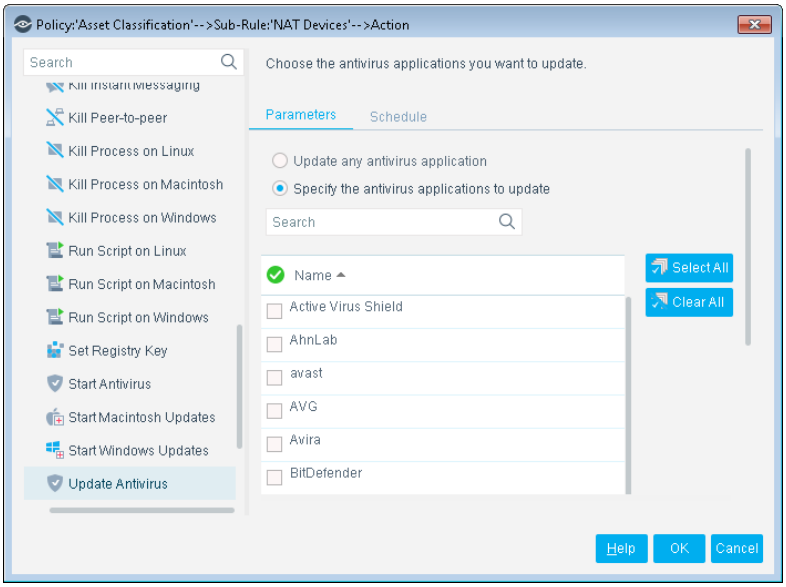
Minimize Bandwidth Usage During Microsoft Vulnerability Patch Download

The Windows Vulnerability DB provides Microsoft vulnerability updates to CounterACT Appliances. The plugin works by pushing Microsoft vulnerability update information to the HPS Inspection Engine installed on CounterACT Appliances. These updates are used when working with vulnerability policies and downloaded at the endpoint.

Users can reduce network bandwidth during this process by limiting the number of concurrent HTTP downloads to endpoints. The default is 20.

Update Antivirus

Update outdated antivirus applications at Windows endpoints.



Update Antivirus Action

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.

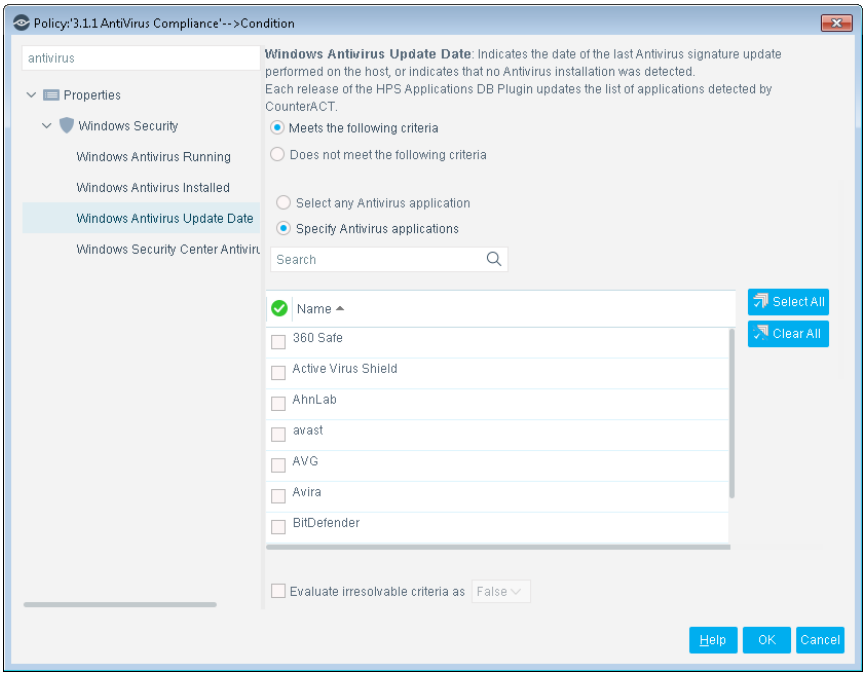
CounterACT uses a script on the endpoint when carrying out this action if the endpoint is managed via domain credentials **Manageable (Domain)**. *Refer to the* HPS Inspection Engine Configuration Guide *for details about how scripts work. Select* ***Options*** *from the* ***Tools*** *menu. Select* ***Modules****. 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 **Options** from the **Tools** menu. Select **Modules**. Select **Windows Applications** and then select **Help**.

Recommended Usage – Conditions

When using this action, you should configure the following condition properties:

- Windows Security>Windows Antivirus Installed>Meets the following criteria
- Windows Security>Windows Antivirus Running>Meets the following criteria
- Windows Security>Windows Antivirus Update Date>Meets the following criteria



Antivirus Update Date

Windows Self Remediation

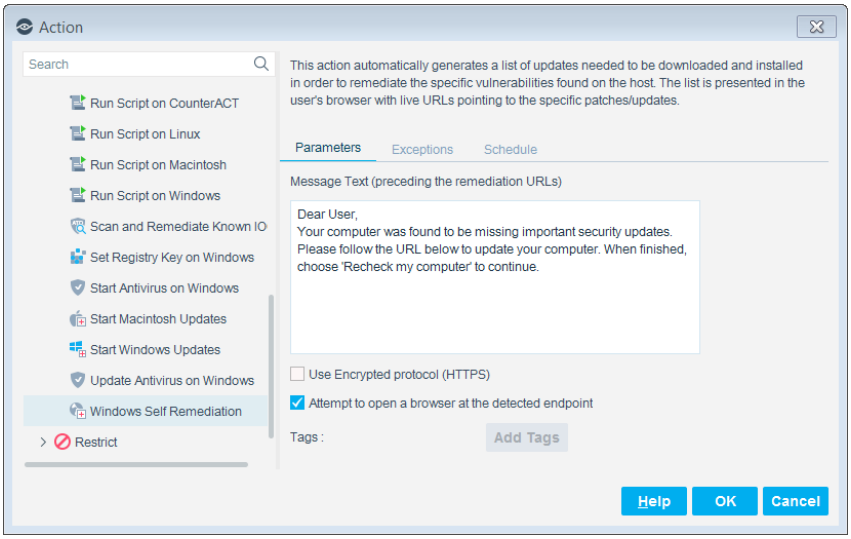
This action delivers web notification to network users indicating that specific vulnerabilities were detected on their machines. The notification includes a list of links that should be selected by the endpoint users in order to patch vulnerabilities. Users cannot access the web until their endpoint 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.

Automated remediation is also available. See Start Windows Updates.

Use the manual option if you want endpoint users to have more control over patching vulnerabilities on their machines.

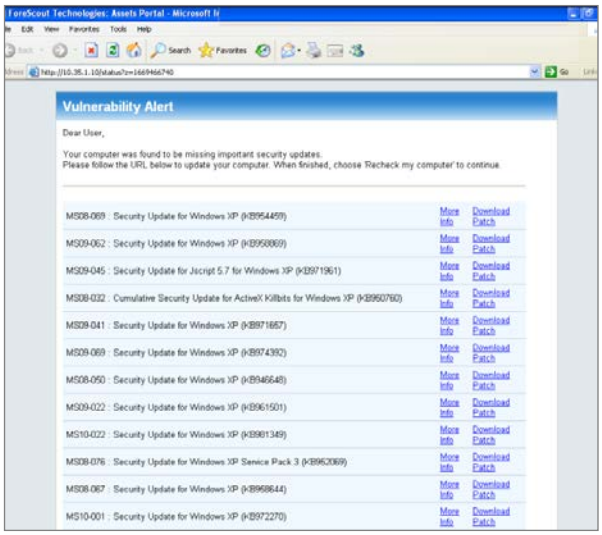
Windows Self Remediation is not accessible when HTTP Redirection is disabled. For more information, see Disabling Web Portals.



Windows Self-Remediation Action

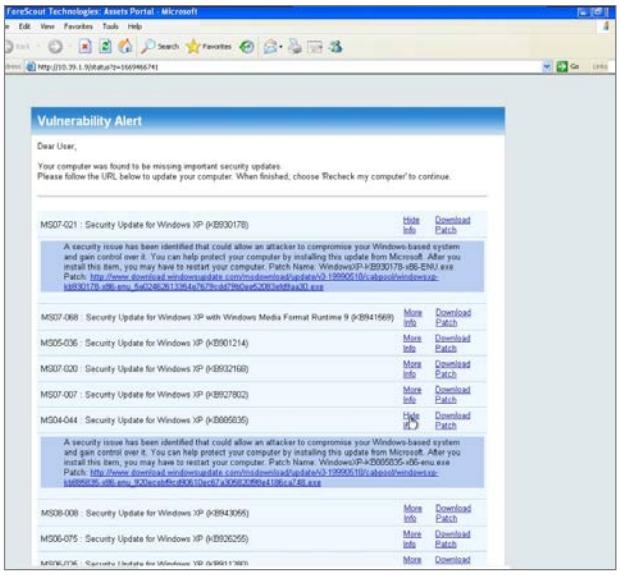
It is recommended to select the **Use Encrypted protocol (HTTPS)** checkbox to send the redirected page via HTTPS. To send it via the non-encrypted HTTP protocol, clear the **Use Encrypted protocol (HTTPS)** checkbox. See Transmitting Actions via HTTPS for more information about this transmission method.

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.) CounterACT uses a script when this option is selected and the endpoint is managed via domain credentials. Refer to the *HPS Inspection Engine Configuration Guide* for details about scripts. Select **Options** from the **Tools** menu. Select **Modules**. Select this plugin and then select **Help**.



Self-Remediation Page at the Endpoint

Network users can select the **More Info** link to review details about the vulnerability detected.



Self-Remediation Page at the Endpoint – More Info

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.

By default, CounterACT 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>]
```

   Example: **`fstool convert_patch_path replace http://server1/patches`**

Restrict Actions

This section describes actions that are used to restrict endpoint access to the network and Internet:

- Switch Restrict Actions
- Virtual Firewall

Switch Restrict Actions

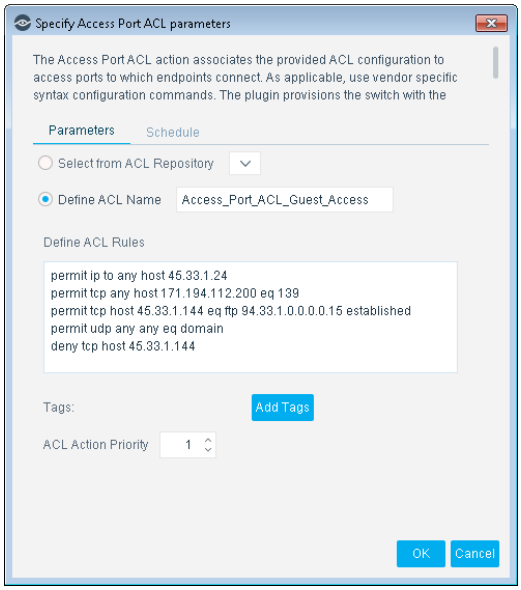
The Switch Plugin provides the following restrict actions:

- Access Port ACL
- Assign Security Group Tag
- Assign to VLAN
- Endpoint Address ACL
- Switch Block

For details about these actions, refer to the CounterACT Switch Plugin Configuration Guide. Select **Options** from the **Tools** menu. Select **Modules**. Select the Switch Plugin and then select **Help**.

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). The Switch Plugin only supports applying the *Access Port ACL* action on Cisco switches.

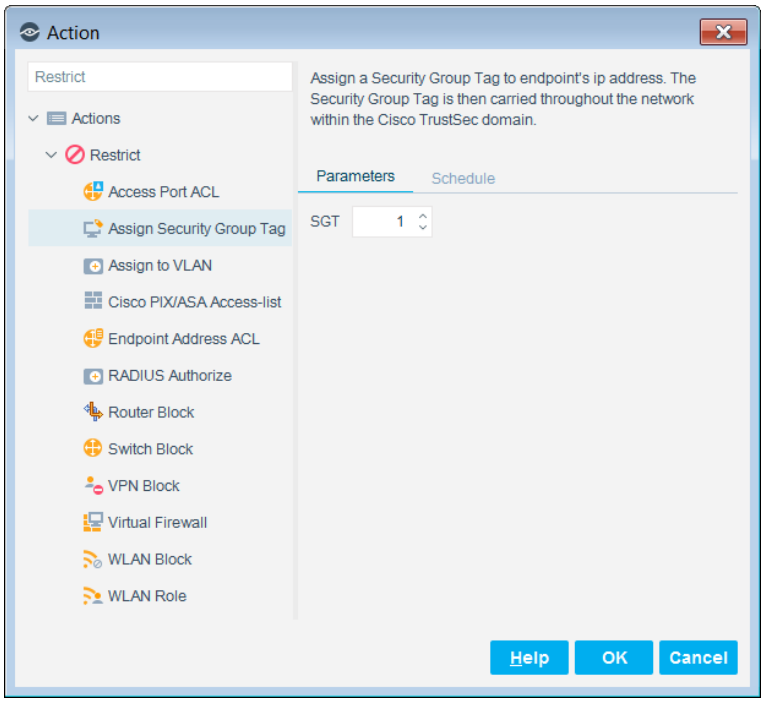


Access Port ACL Action, Configuration Window

In the ACL configuration, take advantage of the full set of switch capabilities. CounterACT 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 CounterACT-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.

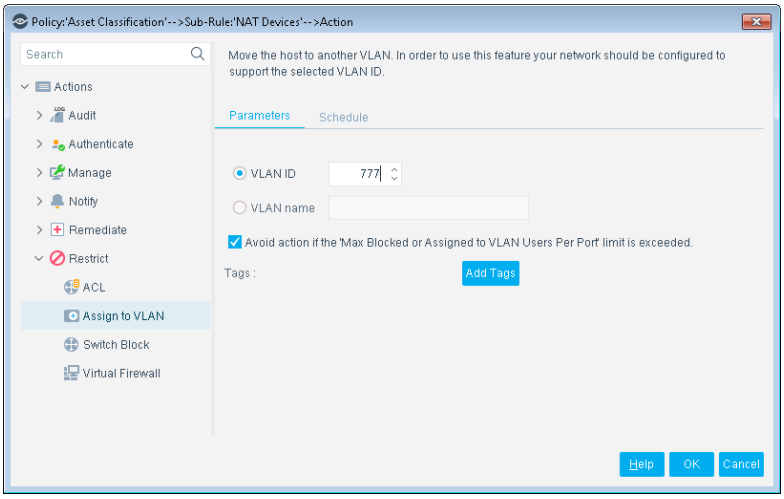


Assign Security Group Tag Action, Configuration Window

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 still prevents the propagation of unwanted traffic to other sections of the network.



Assign to VLAN Action, Configuration Window

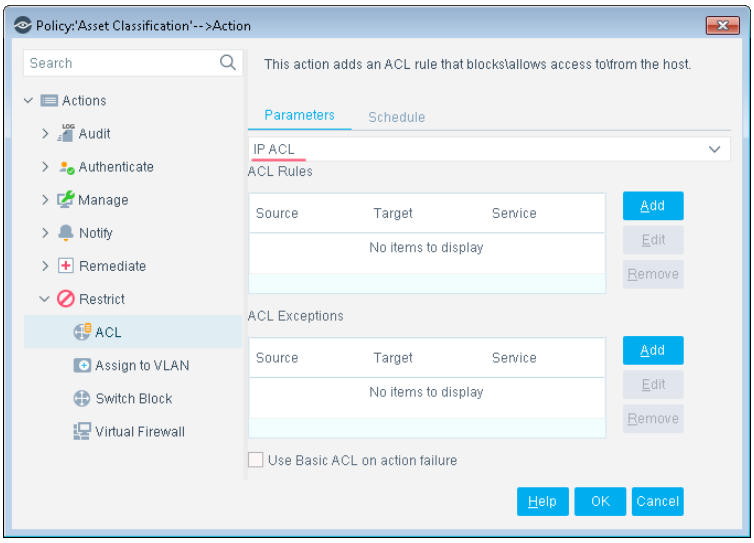
The *Assign to VLAN* action is not supported for the VoIP device if there is a VoIP device between the switch and the endpoint (a VoIP port with a connected VoIP phone and a connected PC behind the phone).

In this scenario, the *Assign to VLAN* action is supported for the endpoint, when specific CounterACT/Switch Plugin requirements are fulfilled.

Endpoint Address ACL

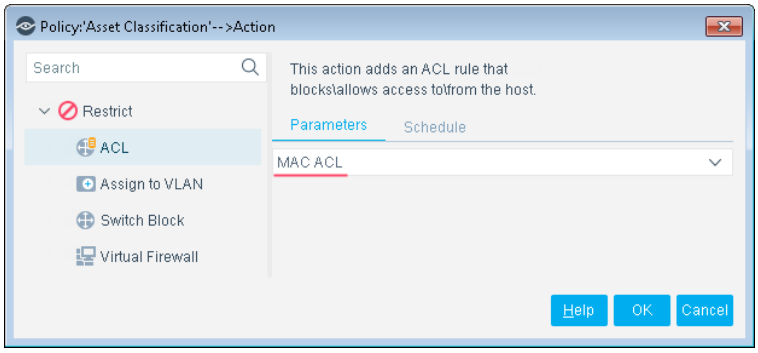
Use the *Endpoint Address ACL* action to define and apply any of the following, connected endpoint handling:

- ***IP ACL***: Instruct a switch to close (ACL rule) or to open (ACL exception) network zones, services or protocols to either ***traffic to*** or ***traffic from*** specific, endpoint IP addresses connected to the switch.



Endpoint Address ACL Action - IP ACL, Configuration Window

- ***MAC ACL***: Instruct a switch to block all traffic sent from the affected, endpoint MAC address.



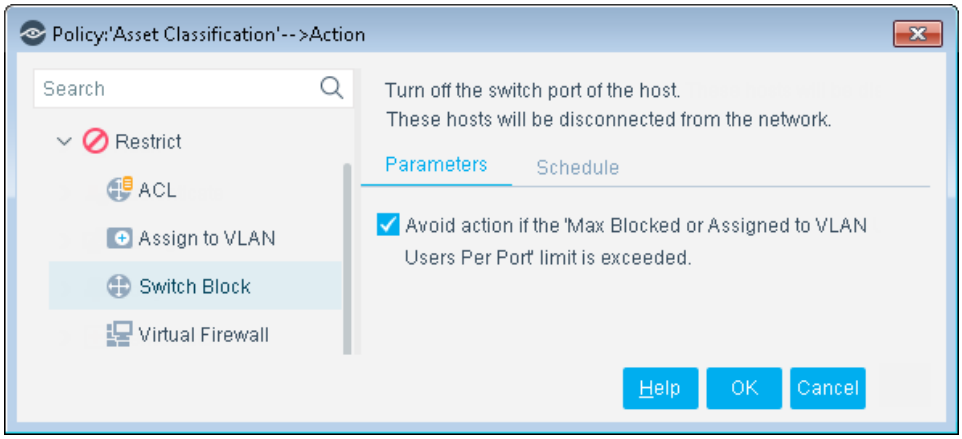
Endpoint Address ACL Action - MAC ACL, Configuration Window

The Switch Plugin only supports applying the *Endpoint Address ACL* action on the switches of the following switch vendors:

- Brocade/Foundry
- Cisco
- Enterasys Matrix N-Series

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.



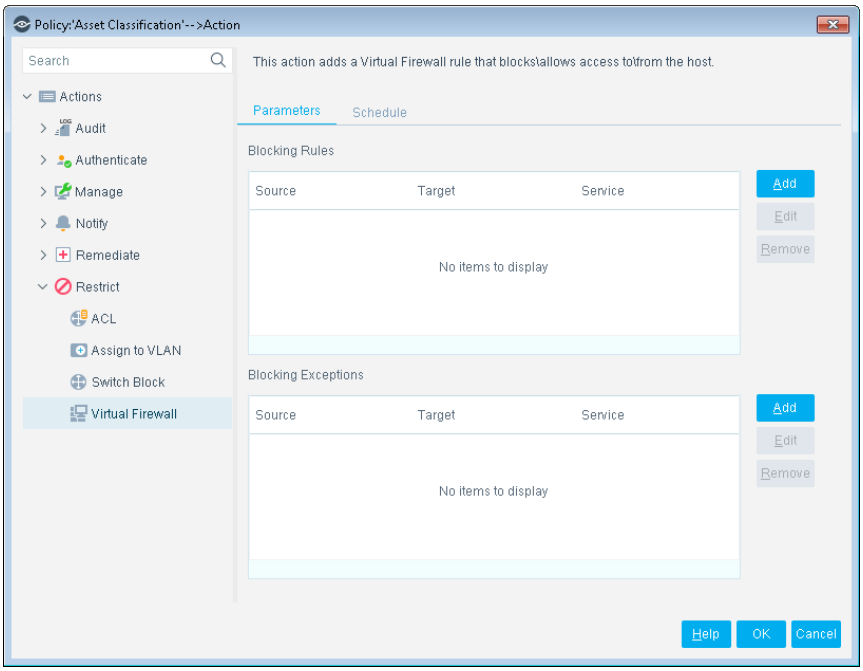
Switch Block Action, Configuration Window

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, using 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 you with 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 so that you can use the 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.



Virtual Firewall Action

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.

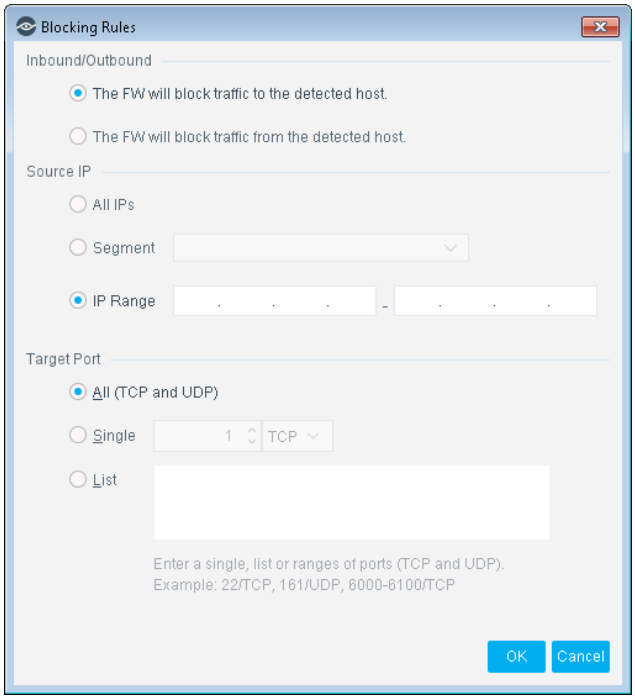
Rules created directly via the Virtual Firewall pane take precedence over policies created here.

Creating a Blocking Rule

This rule allows you to block traffic to or from the detected endpoint.

To block traffic to the detected endpoint:

1. In the **Blocking Rules** section, select **Add**.
2. Select **The FW will block traffic to the detected host**. This allows you to block inbound traffic to detected endpoints on specified services.



Blocking Rules Dialog Box

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 rules that you defined appear in the Blocking Rules list. Use **Edit** and **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 allows you to 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**.

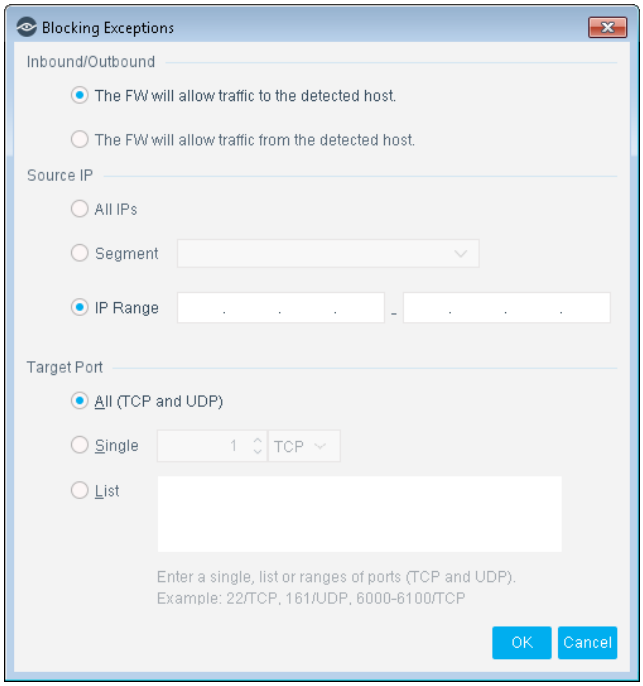
   The rules that you defined appear in the Blocking Rules list.
5. Use **Edit** and **Remove** as required.

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 exceptions to detected endpoints:

1. In the **Blocking Exceptions** section, select **Add**.



Blocking Exceptions Dialog Box

2. Select **The FW will allow traffic to the detected host**. This allows 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 **OK**. The rules that you defined appear in the Blocking Exceptions list. Use **Edit** and **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**. This allows 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 rules that you defined appear in the Blocking Exceptions list. Use **Edit** and **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.

Setup

To allow this action to block such endpoints, your system must be set up as follows:

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 using 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:

1. Run the following commands:

   ```
   fstool set_property engine.conf.params.blockOutgoingSessionInHijack 0
   fstool service restart
   ```

Action Tools

This section discusses the following tools:

- Creating Action Schedules
- Enabling and Disabling Actions
- Working with Property Tags
- Action Icon Display Tool

- Policy Action Log
- About HTTP Actions
- Transmitting Actions via HTTPS
- Captive Portal Detection Exceptions
- Action Thresholds

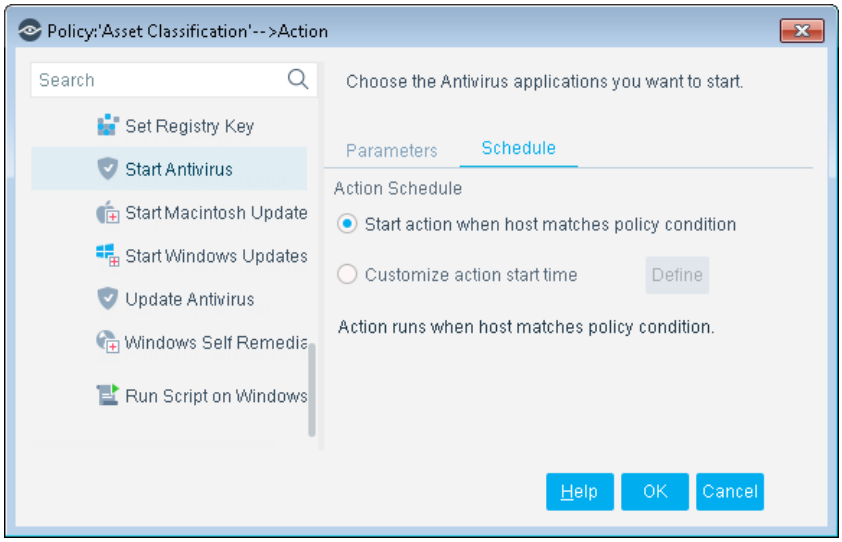
Creating Action Schedules

By default, actions are carried out when CounterACT detects that the endpoint matches the policy. Alternatively action schedules can be assigned to each action. This allows 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.

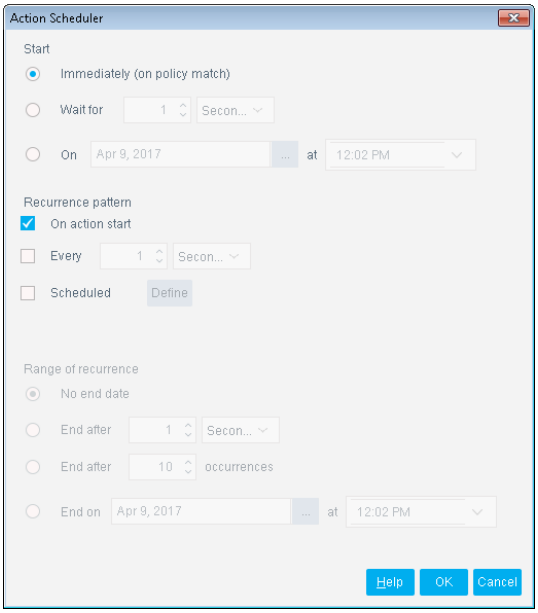
To create an action schedule:

1. Create or Edit a policy.
2. Navigate to the Actions dialog box and select an action.



Action

3. Select the Schedule tab and then select the Schedule tab.
4. Select **Customize action start time**. The Action Scheduler dialog box opens.



Action Scheduler

5. Create an Action schedule.

Enabling and Disabling Actions

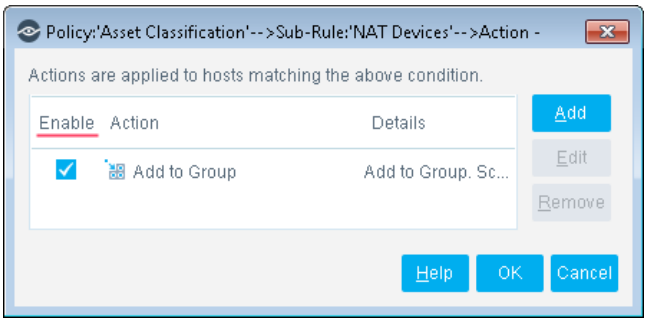
You can create actions for all your policies, and enable and disable them as required. You may need to disable actions; for example, to test your policies and get a sense of network compliance before communicating with network users or taking actions on network devices. Policies can be enabled or disabled from:

- The Home view, Detections pane.
- The Home view, Views pane. See Stop and Start Actions for Endpoints in Policies and Sub-Rules for details.

In addition, you can enable and disable the action from the policy.

To enable or disable an action:

1. Right-click a policy Main Rule or Sub-Rule from the Policy Manager.
2. Select **Quick Edit** and then select **Actions**.
3. Select or clear the **Enable** checkbox from the **Actions** section.



Enable or Disable Actions

Working with Property Tags

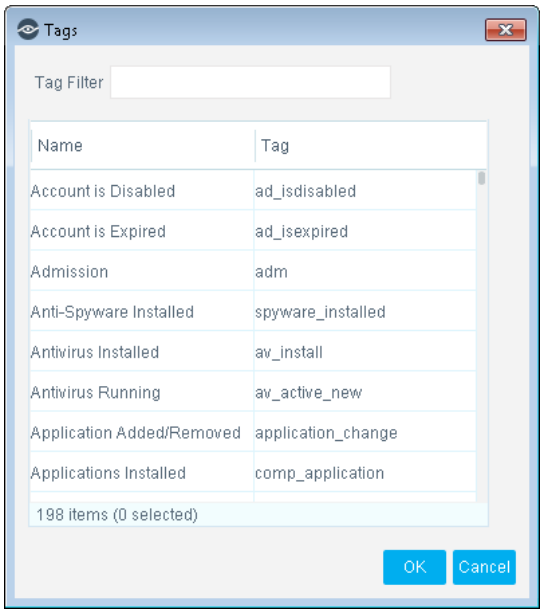
Property tags can be used to insert endpoint property values in condition or action definition fields. For example, important endpoint or User Directory information can be added to email messages, and endpoint identifiers can be added to comments and labels.

User Notification with Host Information Event Tags

If the information cannot be resolved, the message will display the tag code, rather than the resolved information.

To insert property tags:

1. At a Condition or Action dialog box, select a text field. The **Add Tags** button is enabled.
2. Select **Add Tags**. The Tags dialog box opens.



Tags Dialog Box

3. Select the tag that you want to insert and select **OK**.

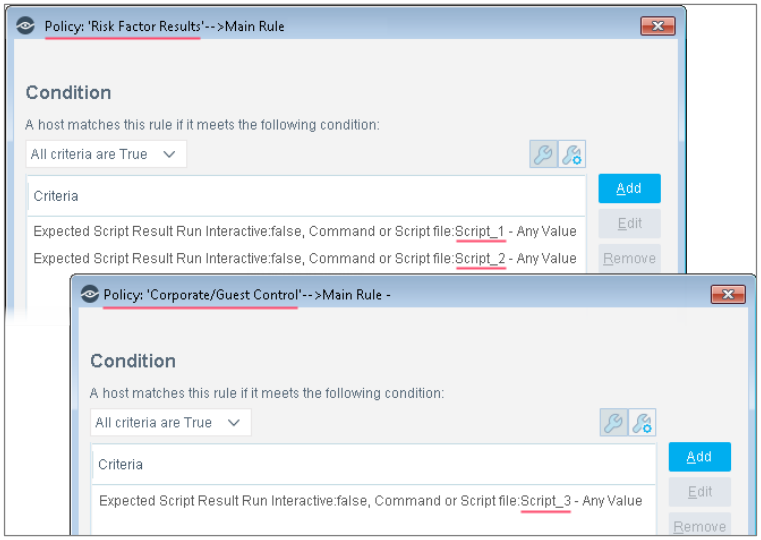
When the text field is evaluated, the tag is replaced by the actual property value of the endpoint.

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, CounterACT generates a property tag 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

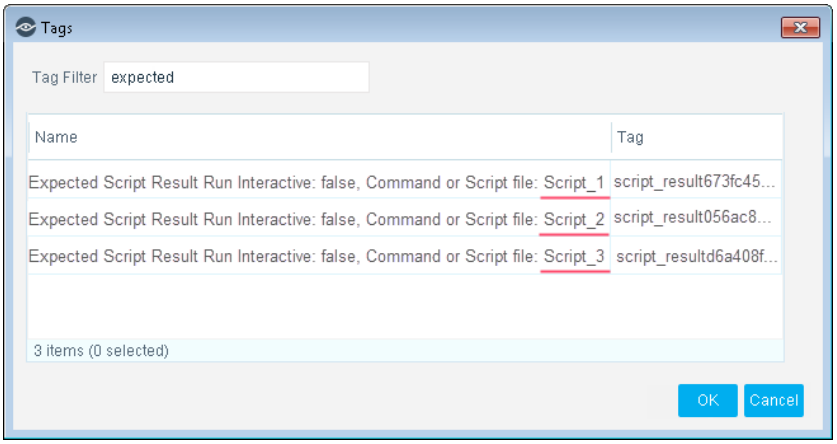
In the following example, two different policies use the Expected Script Result host property to evaluate three scripts on an endpoint.



Policies that use Script-based Host Properties

When CounterACT evaluates these conditions, it generates and maintains a *separate* value for each instance of the host property.

CounterACT 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.



Property tags for Script-based Host Properties

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 delivered.
- 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

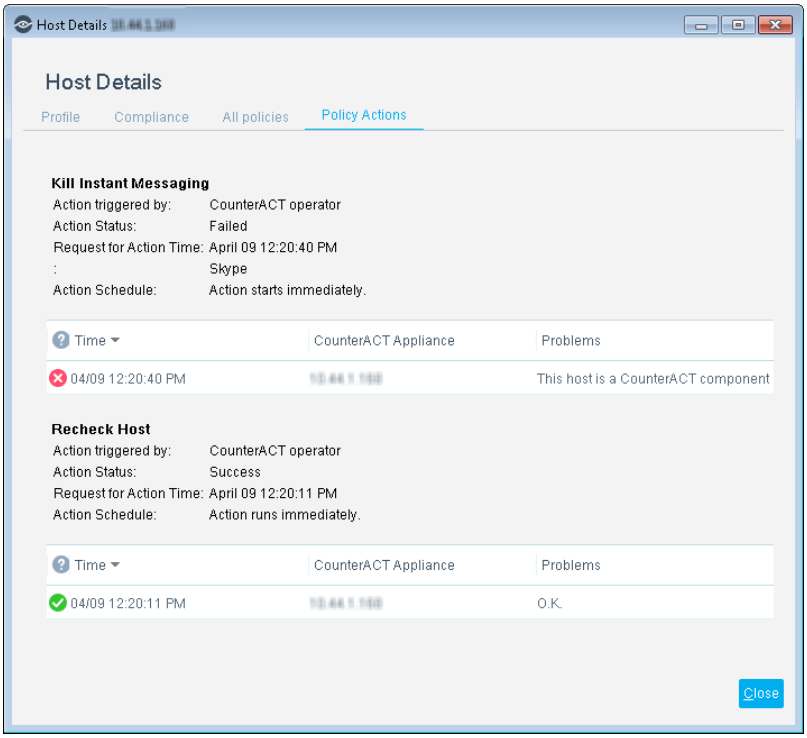
The Host Details dialog box provides specific information about actions carried out on detected endpoints. You can view this information from the Console as soon as the endpoint has been detected via the policy. The information displayed provides more details than presented in the Home view, Detections 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:

1. Double-click an endpoint from the Home view, Detections pane. The Host Details dialog box opens.
2. Select the Policy Actions tab.



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.

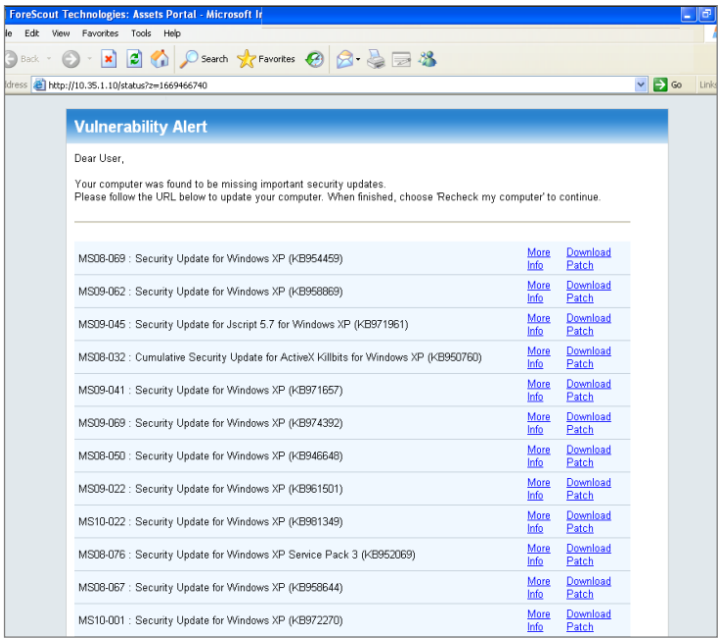
You can also export information in this table.

To export a table in the Policy Actions tab:

1. Right-click one of the tables shown in the tab and select **Export**. A Save As (Export) dialog box opens.
2. Browse to the location in which to save the file.
3. Configure an export option.
4. Select **OK**.

About HTTP Actions

The HTTP actions allow 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.



Sample Redirected Page

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 Appendix 4: HTTP Redirection for more information.
- If your organization uses a proxy for web connection, you must define the proxy ports to be used. See Policy Preferences for more information.
- You can redirect user Intranet sessions. See Defining HTTP Redirect Exceptions for more information.
- 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 more information.
- Messages that appear in the redirected pages can be changed to the language defined at your operating system. See Localizing CounterACT Redirected Web Pages and Messages for more information.
- 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 CounterACT 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 *CounterACT DNS Enforce Plugin Configuration Guide*. To open this guide, select **Options** from the **Tools** menu and then select **Modules**. 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.

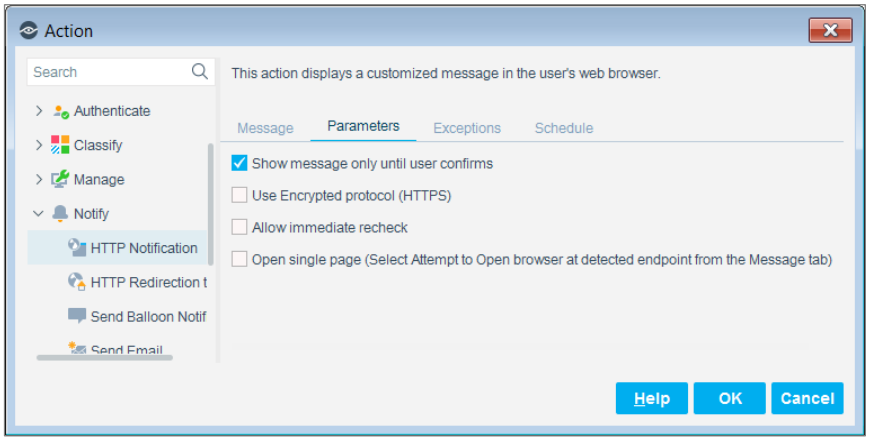
If you transmit via HTTPS, network users will see a security alert in their web browsers when they attempt to access the web. The alert indicates that the site's security certificate was not signed by a known Certificate Authority (CA). (A default self-signed certificate is installed during product installation.) You can generate a known CA Security Certificate to avoid this situation. See Appendix 3: Generating and Importing a Trusted Web Server Certificate and Appendix 4: HTTP Redirection for more information.

Two options are available for working with HTTPS:

- Use HTTPS per Action
- Use HTTPS for All Actions

Use HTTPS per Action

To send a redirected page via HTTPS, select **Use Encrypted protocol (HTTPS)** in the required HTTP action. To send it via the non-encrypted HTTP protocol, clear the checkbox.



Action Dialog Box, HTTP Notification – Use Encrypted Protocol

*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 CounterACT to work globally with HTTPS but defined *specific actions* to be HTTP, redirected traffic will *only be* transmitted via HTTPS.

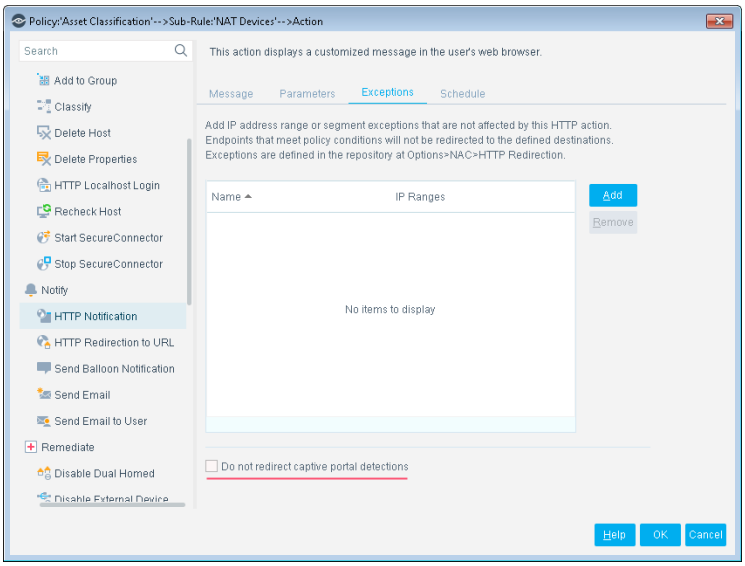
Captive Portal Detection Exceptions

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 option, *Do not redirect captive portal detections*.

This configuration is applied to individual HTTP actions, in the Exceptions tab of each HTTP action.



Captive Portal Detection Exceptions

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

There are scenarios in which policy enforcement requires blocking or restricting network devices and users.

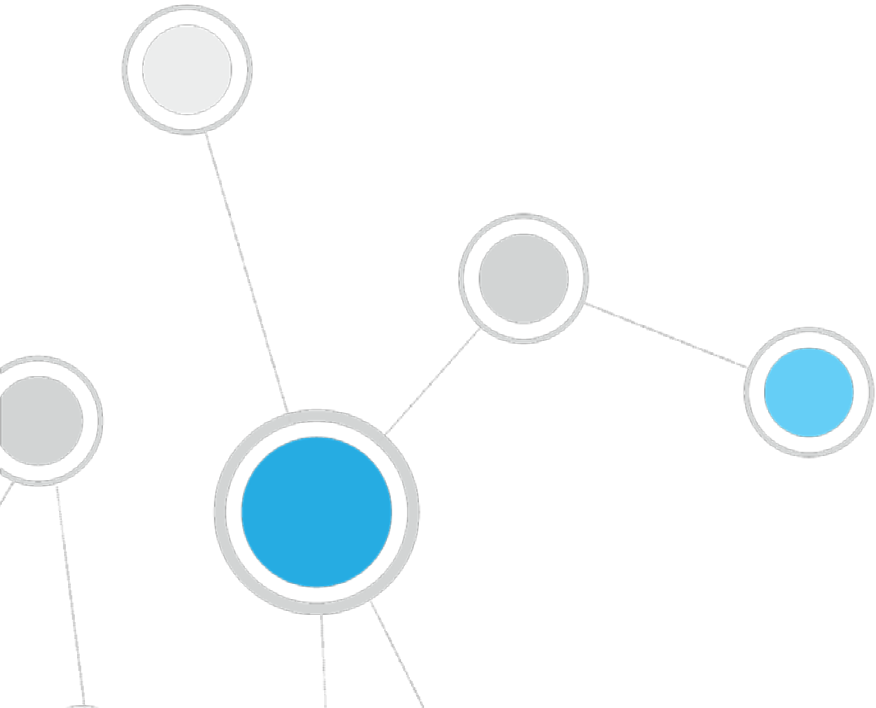
Action thresholds are designed to automatically implement safeguards when rolling out such sanctions across your network. Consider a situation in which you defined multiple policies that utilize a blocking action; for example, the *Virtual Firewall* or *Switch Block* action. In a situation where an extensive number of endpoints match these policies, you may block more endpoints than you 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.

Chapter 8: Base, Content and Extended Modules

- About Base, Content and Extended Modules
- Centralized Module Management
- Check for Updates
- Designing Customized Plugins



About Base, Content and Extended Modules

Base, Content and Extended Modules significantly expand the scope of CounterACT network inspection, data exchange, remediation and control.

Information gleaned from these modules is incorporated into CounterACT tools used for creating policy properties and actions, generating reports and inventory items, and more.

The Check-for-Updates feature automatically checks if your CounterACT devices are updated with the most recently released module versions. This saves you the trouble of checking for updates manually.

Three categories of modules are available:

- Base Modules
- Content Modules
- Extended Modules

Base Modules

Base Modules enhance CounterACT visibility, network connectivity, detection and control capabilities.

- Authentication Module
- Core Extensions Module
- Endpoint Module
- Hybrid Cloud Module
- Network Module

Authentication Module

Plugin Name
RADIUS
User Directory

Core Extensions Module

Plugin Name	Details
Advanced Tools	Provides host properties and actions in CounterACT 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

Plugin Name	Details
CEF Plugin	▪ Send policy compliance and other host information detected by CounterACT to SIEM systems using the CEF messaging format. ▪ SIEM servers can trigger remediation actions by sending alert messages to CounterACT. This functionality uses the alert messaging function common to most SIEM servers, and non-CEF-standard text messages.
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.
DHCP Classifier Plugin	Extract host information from DHCP messages. This information complements information sources used by CounterACT 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	Implement 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	▪ View traffic via the SPAN port and detects and parses DNS messages in the network that reference specific host names. ▪ Determine whether a given endpoint in the network is a DNS server. ▪ Check DNS lookups of specific domain names by endpoints in the network.
External Classifier Plugin	Access a set of MAC addresses maintained in an FTP server or an LDAP server to: ▪ Assign a configured text label to any host whose MAC address matches a MAC address in the retrieved set. ▪ Use 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.
IOC Scanner Plugin	Leverage threat detection and threat prevention mechanisms of third-party systems with the network visibility and enforcement capabilities of CounterACT.
IoT Posture Assessment Engine	Assesses the security risk associated with IoT devices based on their use of weak login credentials.
NBT Scanner Plugin	Obtains the user that is logged on to a given endpoint and the MAC address of that endpoint.
Reports	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.

Plugin Name	Details
Syslog Plugin	Send, receive and format messages to and from external Syslog servers.
Technical Support	Automatically analyze an extensive range of log files on your system and send them to the ForeScout support 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 CounterACT system.
NetFlow Plugin	Listen to NetFlow data streams and analyze them to detect endpoints or endpoint property values that the CounterACT Packet Engine might not learn.
Web GUI (Dashboard)	View dynamic at-a-glance web-based information about: ▪ Device compliance ▪ Device classification ▪ Device management status ▪ Network overview

Endpoint Module

Plugin Name	Details
HPS Inspection Engine	▪ Access Microsoft Windows endpoints. ▪ Perform comprehensive, deep inspection for the purpose of resolving an extensive range of endpoint information. ▪ Activate a variety of CounterACT *actions* to manage, remediate or control endpoints.
OS X Plugin	Manage endpoints running Mac/OS X operating systems. The plugin supports properties, actions and other management functionality for Linux endpoints.
Hardware Inventory Plugin	Extend 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	Manage endpoints running Linux operating systems. The plugin supports properties, actions and other management functionality for Linux endpoints.
Microsoft SMS SCCM Plugin	▪ Retrieve and display advertisement and report information related to SMS/SCCM hosts in CounterACT. ▪ Update SMS/SCCM clients with new advertisements, and updating the SMS/SCCM server with new host information.

Hybrid Cloud Module

Plugin Name	Details
AWS	▪ Gain visibility of endpoints in Amazon's public cloud ▪ Create and apply CounterACT policies ▪ Maintain security of cloud endpoints ▪ Enforce compliance on endpoints

Plugin Name	Details
VMware NSX	Allow 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	Allows you to monitor Cisco Meraki, cloud-managed networks. The integration enables real time discovery of endpoints connected to Meraki Switches (MS) and Wireless Access Points (MR).
Switch	▪ Track the location of endpoints connected to network switches and retrieve relevant switch information. ▪ Quickly detect new endpoints on the network. ▪ Assign switch ports to VLANs; you can set up dynamic, role-based VLAN assignment policies and quarantine VLANs. ▪ Use ACLs to open or close network zones, services or protocols for specific endpoints at a switch and handle scenarios that address broader access control.
Wireless	Provide NAC capabilities to wireless network controllers and access points for the purpose of controlling wireless endpoints connected to them.
VPN	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.

There are additional Base modules that are available to legacy customers who had them installed in CounterACT 7.0.0: the Router Blocking Module and Cisco PIX/ASA Firewall Integration Module.

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
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 & model. The Device Classification Engine uses this information to provide the best possible classification for the device.
Windows Vulnerability DB	Makes vulnerability updates available to CounterACT soon after they are released from Microsoft. These updates are used when working with vulnerability policies

Module Name	Details
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. Host properties are delivered that let you detect and manage endpoints based on this information.
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 Template	Security policy templates use existing ForeScout CounterACT 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.

Extended Modules

ForeScout Extended Modules expand CounterACT's 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.

Extended Modules require valid licenses. License requirements for Extended Modules differ depending on the licensing mode your CounterACT deployment is using. See Chapter 17: License Management for the relevant licensing requirements and to learn more about licensing modes.

The various Extended Modules relate to an extensive range of integration categories. For example:

- Advanced Threat Detection (ATD)
- Endpoint Protection Platform (EPP)
- Mobile Device Management (MDM)
- Open Integration
- Security Information and Event Management (SIEM)
- Vulnerability Management (VM)
- Privileged Access Management (PAM)
- IT Service Management (ITSM)
- Next Generation Firewall (NGFW)
- Client Management Tools (CMT)

Accessing Extended Modules

See Additional CounterACT Documentation for information on how to access Extended Module software downloads and related documentation.

Module Packaging

Modules can package individual modules or multiple modules.

- Extended Modules: Individual Modules
- Integration Modules: Multiple Modules

Integration Modules are not supported when operating in Centralized Licensing Mode.

Extended Modules: Individual Modules

An Extended Module packages an individual licensed module. For example, the XenMobile Module is packaged individually as part of the Citrix XenMobile Module.

An exception to this is the Open Integration Module, which is an Extended Module even though it packages more than one module.

Modules Released After Service Pack 2.3.0 (CounterACT Version 7.0.0)	Modules that were released for the first time (version 1.1.0) *after* Service Pack 2.3.0 are packaged individually as the sole component of an Extended Module even if you are working with a service pack version earlier than 2.3.0.
Modules Released Before Service Pack 2.3.0 (CounterACT Version 7.0.0)	Modules that were released for the first time *before* Service Pack 2.3.0 are packaged individually as the sole component of an Extended Module when all of the following are true: ▪ You did not install the same module packaged as part of an integration module. See Integration Modules: Multiple Modules. ▪ The Extended Module version was released after the Service Pack 2.3.0 release. ▪ Service Pack 2.3.0 or above is installed.

Extended Module demo licenses are valid for 90 days. See Demo Licenses.

Integration Modules: Multiple Modules

Prior to the release of Service Pack 2.3.0, groups of related licensed modules were packaged into Integration Modules. For example, the MDM Integration Module packaged MaaS360, XenMobile, and other MDM modules.

Integration Modules are not supported when operating in Centralized Licensing Mode.

If you already installed modules (with either a demo or permanent license) as components of Integration Modules, you can continue to use them, as well as the other modules packaged in the respective module, even if you are using Service Pack 2.3.0 or above. Upgrading these modules to versions released after the Service Pack 2.3.0 release does not change the way they are packaged.

Advanced Threat Detection (ATD)

Modules in this category integrate CounterACT with popular Advanced Persistent Threat (APT) detection products such as FireEye, Palo Alto Networks WildFire and Invincea. CounterACT ATD integrations identify advanced cyber-attacks that threaten network security, and remediate infected endpoints.

Endpoint Protection Platform (EPP)

Modules in this category integrate CounterACT with McAfee products such as McAfee ePO. These integrations leverages the visibility capability of CounterACT with the security features of Intel Security products for greater coverage and control to more devices on the network. Integration lets CounterACT:

- Report discovered endpoints to the ePO Detected System
- Detect endpoints and implement NAC actions based on ePO Events and attributes

Mobile Device Management (MDM)

Modules in this category integrate CounterACT with popular MDM service platforms such as AirWatch, MobileIron, XenMobile and others. CounterACT MDM integrations yield an easy-to-use platform that includes all of the essential functionality for end-to-end management of mobile devices. You can secure and manage apps, docs, and devices for global organizations, and support both corporate and individual owned devices.

Open Integration

This module contains the Data Exchange Plugin, which supports bidirectional query and update interactions with external SQL, Oracle, and LDAP servers.

In addition, it contains plugins and other components that support the CounterACT Web Service, which lets external entities communicate with CounterACT.

- Information can be retrieved from CounterACT using simple, yet powerful web service requests based on HTTP interaction.
- Information can be submitted to CounterACT using web service requests with an XML data body. The CounterACT Web Service parses the data to update CounterACT host properties.

Security Information and Event Management (SIEM)

Modules in this category let CounterACT send compliance and other host information to SIEM systems such as ArcSight, Splunk and QRadar, and correlate this information to perform risk assessment analysis.

Vulnerability Management (VM)

Modules in this category integrate CounterACT with vulnerability assessment platforms such as Nessus/Tenable VM and McAfee Vulnerability Manager to support auditing, asset profiling, sensitive data discovery, and more.

Privileged Access Management (PAM)

PAM Extended Modules provide real-time agentless visibility into undiscovered local privileged accounts and automated response to threats based on holistic visibility into user activity, device security posture, incident severity and overall threat exposure.

IT Service Management (ITSM)

ITSM Extended Modules share up-to-date device properties, classification, configuration and network context to help true-up assets in your CMDB, improve

asset compliance and maintain a trusted single-source-of-truth repository for better decision-making.

Next Generation Firewall (NGFW)

NGFW Extended Modules enable you to 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 endpoint context from CounterACT.

Client Management Tools (CMT)

CMT Extended Modules provide visibility and control across network-connected devices— including corporate devices—while they're off the enterprise network. They also verify device compliance with security and regulatory mandates and take remediation actions.

Centralized Module Management

Modules are centrally managed across the enterprise. This means if you install or update a Base, Content or 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
- Install and Uninstall
- Rollback (Can only be carried out on one module at a time)

You should carry out all tasks listed above from the Enterprise Manager, and not from individual Appliances.

If an Appliance on which a module is running is disconnected, it will not appear in the Modules pane. A warning message in the pane indicates that the Appliance is not connected.

Installing a Module

To install the module:

1. Navigate to one of the following ForeScout download portals, depending on the licensing mode your deployment is using:
   - Product Updates Portal - ***Per-Appliance Licensing Mode***
   - Customer Portal, Downloads Page - ***Centralized Licensing Mode***

   To find out which licensing mode your deployment is working with, see Identifying Your Licensing Mode in the Console.
2. Download the module `.fpi` file.
3. Save the file to the machine where the CounterACT Console is installed.

4. Log into the CounterACT Console and select **Options** from the **Tools** menu.
5. Select **Modules**. The Modules pane opens.
6. Select **Install**. The Open dialog box opens.
7. Browse to and select the saved module **`.fpi`** file.
8. Select **Install**. The Installation screen opens.
9. Select **I agree to the License Agreement** to confirm that you have read and agree to the terms of the License Agreement, and select **Install**. The installation will not proceed if you do not agree to the license agreement.

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

In modules that contain more than one component, the installation proceeds automatically one component at a time.

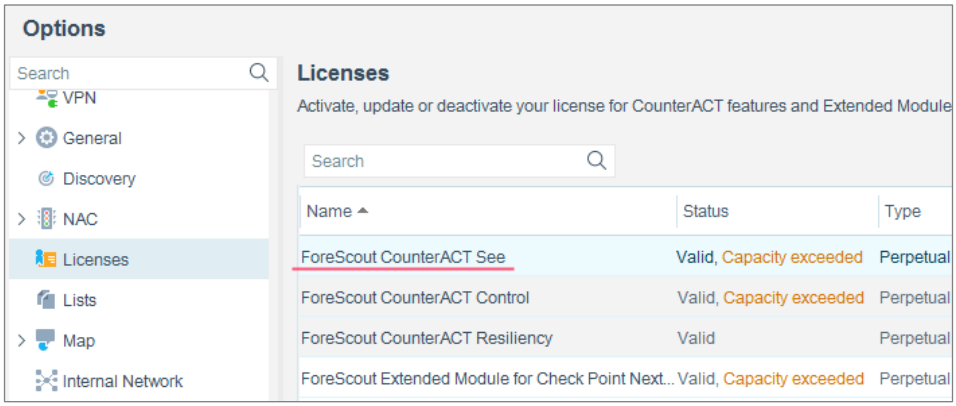
10. When the installation completes, select **Close** to close the window. The installed module is displayed in the Modules pane.

    Some components are not automatically started following installation.

Identifying Your Licensing Mode in the Console

If your Enterprise Manager has a *ForeScout CounterACT See* license listed in the Console, your deployment is operating in Centralized Licensing Mode. If not, your deployment is operating in Per-Appliance Licensing Mode.

Select **Options > Licenses** to see whether you have a *ForeScout CounterACT See* license listed in the table.



Contact your ForeScout representative if you have any questions about identifying your licensing mode.

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 CounterACT Device Management Overview for more information about managing CounterACT Devices.

Plugin and Module Security

Transfer of information between CounterACT and plugins or modules is secured. 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)
- Transferred encrypted over the wire (between CounterACT components)

Check for Updates

CounterACT automatically checks to see if updates are available for software that you installed on your CounterACT devices, or software that you have purchased but have not yet installed (under Centralized Licensing Mode). 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, Content, and Extended Modules, and notifications of CounterACT updates. Occasionally, plugins may also be available as hotfixes.

The default Check for Updates frequency is once an hour. See Configuring Check for Updates for information about updating the default.

How Do You Know if a New Software Version Is Available?

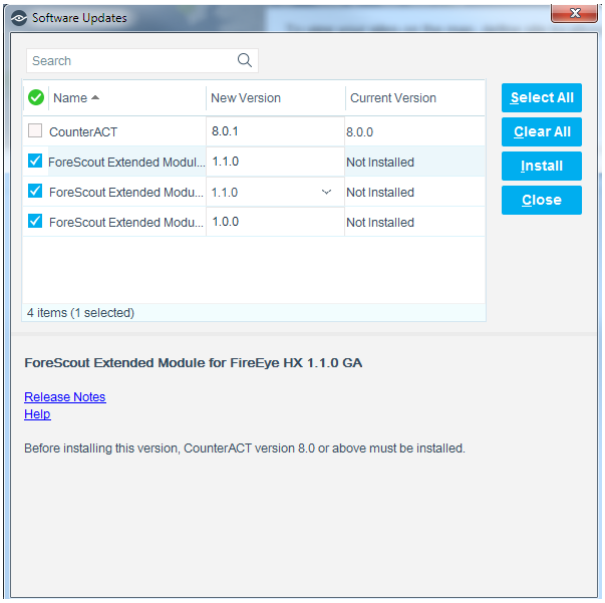
The **Check for Updates** icon appears on the status bar of the Console when an update is available for any installed or purchased (under Centralized Licensing Mode) software.

Check for Updates Icon

The installed CounterACT Console application automatically contacts the ForeScout support server periodically using HTTPS (secure 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.



About Unchecked Items

Certain items may appear but may not be checked. This happens if the item is a CounterACT release. CounterACT releases are upgraded from the CounterACT Devices menu. *Tools>Options>CounterACT Devices>Upgrade.*

2. Select the software items you want to install and select **Install**. The Install wizard opens.
3. Select **I agree to the License Agreement** and select **Install**. Installation will not proceed if you do not agree to the license terms.

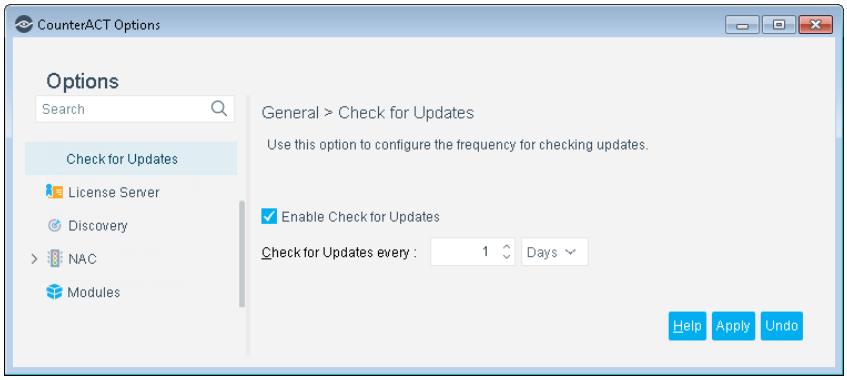
The progress bar indicates the progress of the installation. You can view the installation log file, which itemizes any installation failures.

Configuring Check for Updates

You can configure the frequency at which updates are checked, and enable or disable the Check-for-Updates option. The default frequency is once an hour.

To configure Check for Updates:

1. Select **Options** from the **Tools** menu and then select **General**>**Check for Updates**.



Check for Updates Pane

2. Configure and select **Apply**.

Roll Back to Previous Module Versions

Under certain circumstances, you may want to roll back a module to a previously installed version. This may happen, for example, if your system was not operating as expected after upgrade.

If you are working with modules on your Enterprise Manager, the modules on all Appliances are rolled back to the selected version. If the rollback occurred when the Appliance was not connected, the module is rolled back when the Enterprise Manager reconnects to the Appliance.

One or more versions may be available to which you can roll back. In some cases it may not be possible to roll back, in which case the **Rollback** button is disabled.

Rollback is supported for plugin hotfixes.

To roll back:

1. Select **Options** from the **Tools** menu and select **Modules**.
2. Select a module and then select **Rollback**. A dialog box is displayed listing all the versions to which you can roll back. Once the Rollback beings it cannot be interrupted or cancelled.
3. Select the version that you want and then select **Rollback**. A dialog box shows you the progress of the rollback.
4. Select **Close**.

Designing Customized Plugins

ForeScout partners and customers can write software plugins to enhance the capabilities of CounterACT. By preparing your own plugin you can:

- Obtain real-time information regarding endpoints
- Trigger third-party remediation and ticketing systems.
- Provide additional information to CounterACT regarding endpoints
- Create plugin-specific commands that control endpoints

To request the ForeScout CounterACT Plugin SDK, contact sdk@forescout.com

Chapter 9: Assets Portal

- About the Assets Portal
- Search Tools
- Expanding Information Discovered by the Assets Portal
- Assets Portal User Management
- Accessing the Assets Portal
- Performing an Assets Portal Search

About the Assets Portal

The Assets Portal is a web-based search and discovery tool that allows you to leverage extensive network information collected and correlated by CounterACT. This includes not only endpoint information, but also policy violations, login information, User Directory details, organizational mapping details, and endpoint device connections. The information will prove valuable across your organization, including:

- Security teams: Use an IP address to quickly locate and shut down switch ports and eliminate a security threat.
- 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.

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. Refer to Appendix 3: Generating and Importing a Trusted Web Server Certificate for more information. You can turn off this option and transmit via HTTP.

Supported Browsers

The Assets Portal runs in Internet Explorer, Chrome, and Firefox version 2 and above.

Search Tools

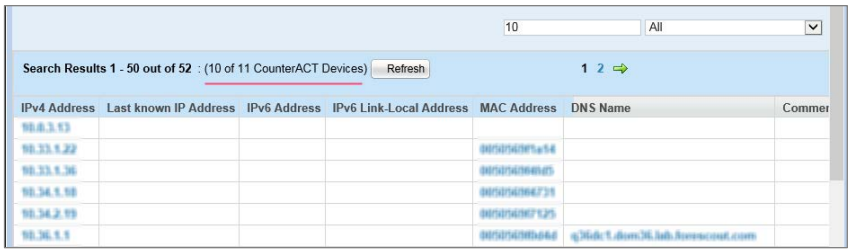
Powerful search tools give you immediate access to an extensive range of endpoint and user information.

- 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, 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.

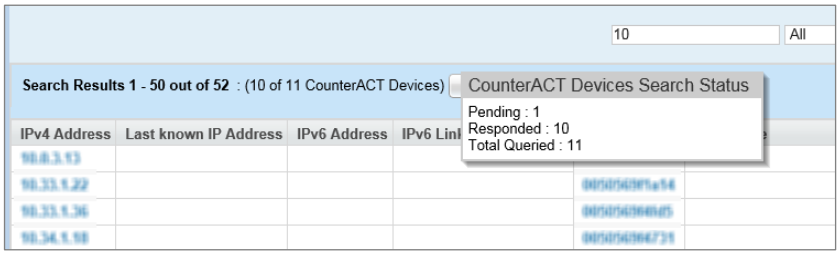
Search Status

The Assets Portal search result page indicates how many Appliances have been queried and how many responded to your Assets Portal search.



Assets Portal Search in Progress

Mouse-over this string to view a tooltip that details this information.



Search Status Tooltip

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.

Expanding Information Discovered by the Assets Portal

By default, CounterACT 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 CounterACT)
- Switch Plugin properties (this plugin is bundled with CounterACT)

You can update the default to include additional information; for example, properties that are only available via the policy (Nmap details). See Defining Endpoint Discovery Rules for more information. You can also broaden the scope and capacity of the portal when you install plugins/modules. For example, if you installed the VPN Plugin, related VPN properties are displayed in the portal. See Chapter 8: Base, Content and Extended Modules for more information.

Importing and Exporting Information

Assets Portal information can be imported and exported by using standard import and export tools from your web browser.

Assets Portal User Management

The Admin user has access to the portal and all portal features by default.

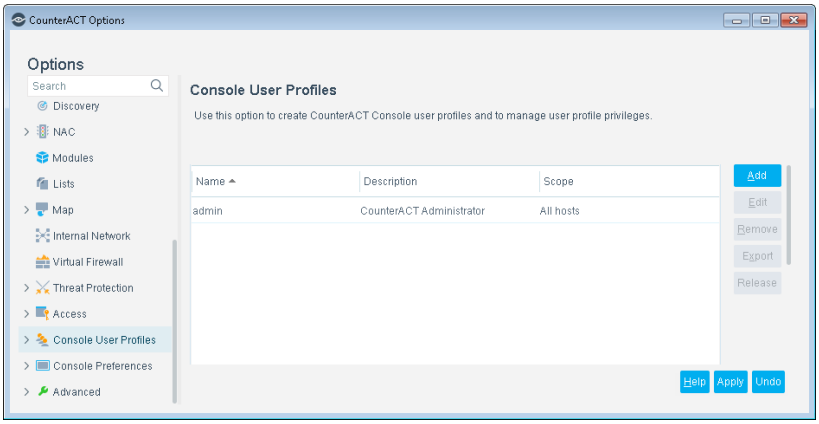
Additional portal users are defined in the User Definitions dialog box. Furthermore, you can assign permission levels to ensure that only certain portal users have access to certain types of information or activities. For example, you can grant all portal users the ability to view portal information, but only allow selected users to release blocked endpoints.

Defining Assets Portal Users and Permissions

By default all Console users have access to the Assets Portal web server, but cannot log in unless they are defined as Assets Portal users from the User Definition dialog box. The dialog box also allows you to define viewing and action permission levels for each Assets Portal user.

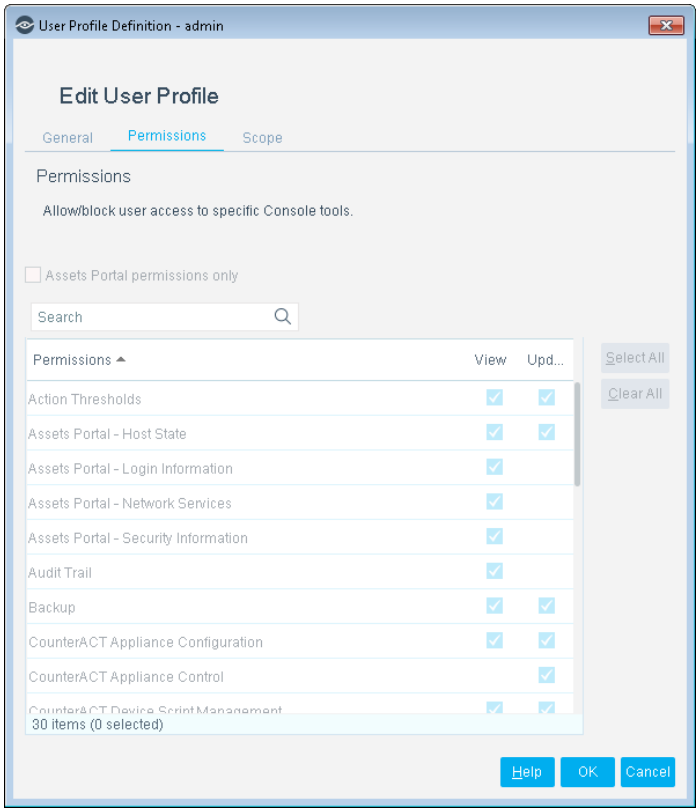
To define users:

1. Select **Options** from the **Tools** menu and select **Console User Profiles**.



Console Users Pane

2. Select **Add** or **Edit**. The User Definition dialog box opens.



User Definition Dialog Box

3. To create an Assets Portal user, select **Assets Portal User**. Assign Assets portal permissions from the **Permissions** section.
4. Update other user definitions as required and select **OK**.

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 **Options** from the **Tools** menu and then select **Access**>**Web**. 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. For more information about Network Policy settings, see What Is a Policy? It is not recommended to deny portal access.*

Accessing the Assets Portal

Two methods are available for accessing the Assets Portal.

- Log in from the Console. By default, Console login grants access to CounterACT web-based tools, such as the Assets Portal, without additional login prompts. You can however force a separate login to the Assets Portal. See Log in to Each CounterACT Web-Based Portal.

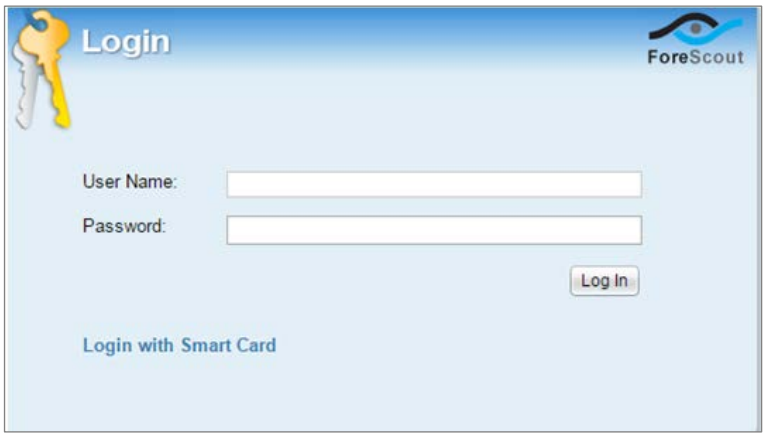
- Log in from your web browser. Log in from a browser always requires authentication.

To access the Assets portal:

1. Do one of the following:
   - In the Console toolbar, select **Tools>Assets Portal** from the menu.
   - Browse to the following URL: http://<Device_IP>/assets

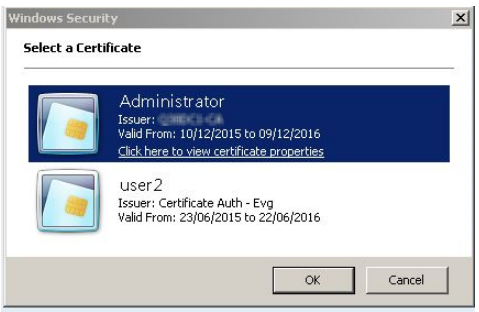
     Where <*Device_IP*> is the IP address of the Enterprise Manager or an Appliance. A login page opens.

   When you access the portal from the Console, you may not be prompted to log in. For more information see Log in to Each CounterACT Web-Based Portal.



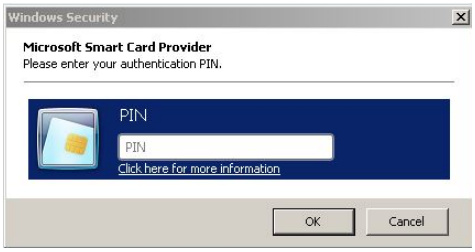
Portal Login Page

2. Enter the **User Name** and **Password** of a user that can access the portal. Typically the credentials you use to access the Console also grant access to the portal. For more information, see Creating Users and User Groups.
3. (Smart Card Authentication) If you are working with Smart Card authentication, you may be prompted for the login information described here.
   a. Select the **Login with Smart Card** link. The Select a Certificate dialog box opens.



Smart Card Login – Select Certificate

b. Select a certificate and then select **OK**. A PIN dialog box may open.



Smart Card Login – Enter PIN Code

c. Enter a PIN code and then select **OK**.

Add the Assets Portal to Your Web Browser

The Assets Portal link can be saved via your web browser search box.

To add the portal:

1. Select **Add to browser search box** from the Assets Portal home page.

Browser Support

The browser search is supported for Internet Explorer 7 and above, and Firefox version 2 and above.

Performing an Assets Portal Search

After logging in to the Assets Portal, you can begin using the search features to quickly and efficiently pinpoint network information that you need.

Wildcard searches are automatically performed. This means the search results will display all terms beginning with the characters that you entered. 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

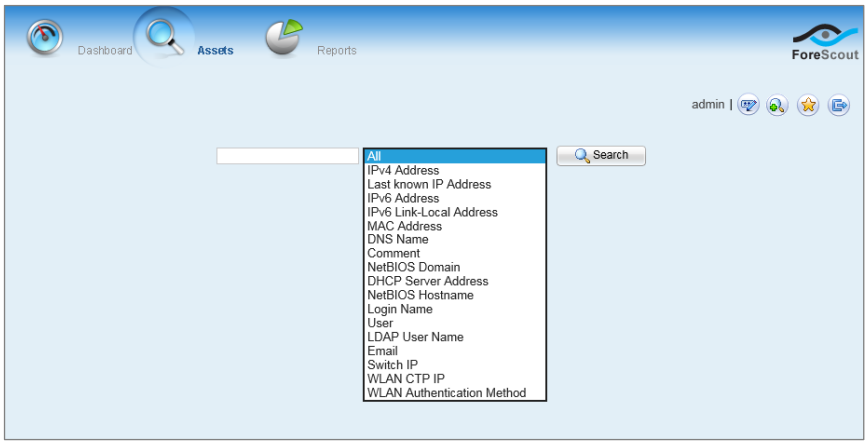
The following options are available for performing user-based searches:

- Login Name
- User (from User Directory)
- LDAP User Name
- Email (from User Directory)

Searches are only available for endpoints that were previously discovered. The User Directory search is only available for endpoints that were detected via a NAC policy or as a result of a Threats policy.

To perform the search:

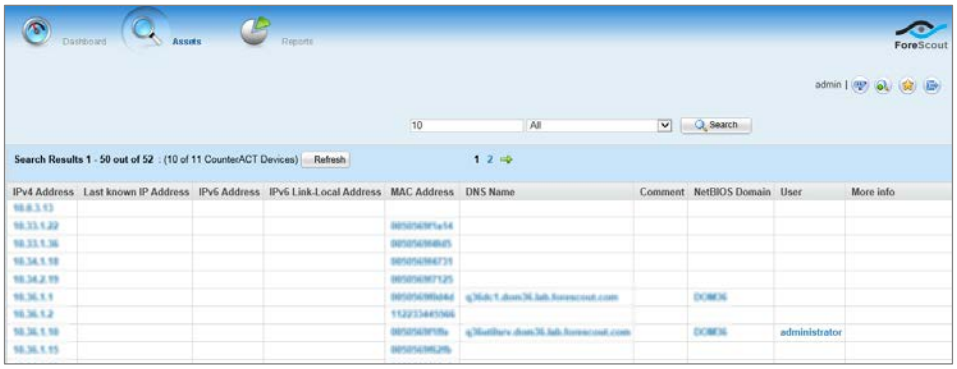
1. Log in to the Assets Portal.
2. From the home page, type in a value.
3. Alternatively, select a search type from the search drop-down list.



Specific Search

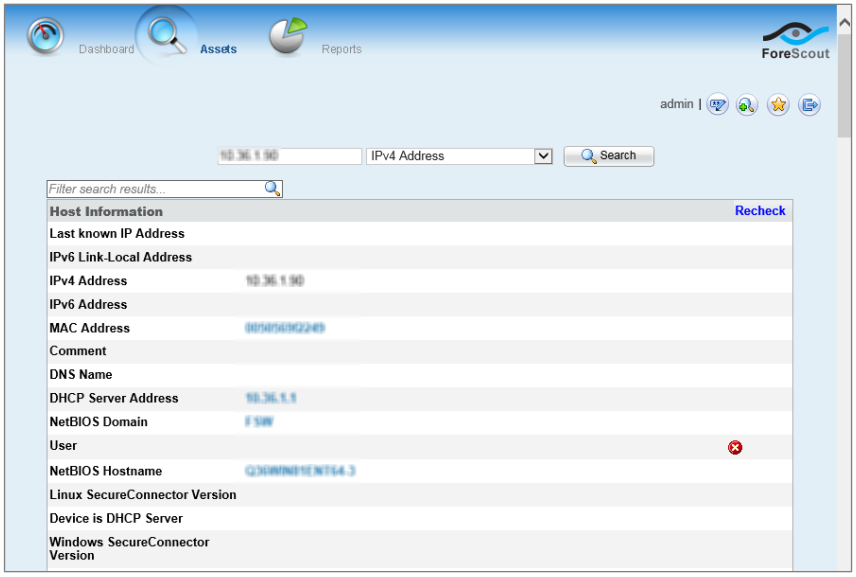
4. Select **Search**.
5. The **Search Results** page opens with items that match the search query.

   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.



Sample Search Results Page

6. Select the IP address or item of interest to you, or select any other linked item to continue the search. If the search produces only one result, the related ticket page opens.
7. The Host Ticket page opens with information about the selected item.



Host Ticket Page

Host-Based Ticket Results

Item	Description
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.
CounterACT NAC Policy Status	A list of the policies applied to the endpoint and the current endpoint status.
Threat Protection Activity Detected	Details regarding malicious endpoints activity currently detected.
Manual Actions	Manual actions applied on an endpoint (actions carried out from the Home view, Detections pane). You can select **Undo** or **Undo All Actions** to cancel manual actions applied on an endpoint; for example, releasing an endpoint if it is blocked. If you incorrectly reversed the action, you can return to the previous state by reassigning the action 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 that they were detected; for example, the last MAPI authentication or User Directory authentication. See also Clearing Event Detections.

Item	Description
Admission Events	The most current admission events detected and the time of detection. Any of 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 will initiate the activation. The default time period can be changed. See Policy Preferences for more information. ▪ 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 Event Detections.

User-Based Ticket Results

Item	Description
User Information	Displays the user login name entered to log in to the computer.
Machines Currently Logged On	Displays that 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.

Viewing Additional Information

An icon in a row of the Host Ticket page indicates that additional information is available in a tooltip. Place the cursor over the icon to see.

An icon in a row of the Host Ticket page indicates that additional troubleshooting information is available. Place the cursor over the icon to see details in a tooltip. Select the icon to open the matching troubleshooting page. See On-Screen Troubleshooting for more information.

Page Display

You can display information on one page, and use scroll features to view it.

Clearing Event 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:

1. Navigate to the event that you want to clear on the ticket page.

Clear Event Option

2. Select the **Clear** icon . A confirmation dialog box opens.
3. Select **Yes**.

Events can also be cleared from the Console. See Additional Controls in Viewing Mouse-Over Table Information.

Chapter 10: Generating Reports and Logs

- About Reports
- On-Screen Threat Protection Reporting
- Generating Scheduled Reports
- Reports Portal
- Working with System Event Logs
- Viewing Block Events
- Viewing a History of Monitored and Blocked Services

About Reports

Your Console is equipped with the following powerful report generation tools.

On-Screen Threat Protection Reports

These tools 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.

Two options are available for generating on-screen reports:

- Generate reports on-screen. See Generating On-Screen Threat Protection Reports for more information.
- Schedule automatically generated reports to be sent by email. See Generating Scheduled Reports for more information.

By default, an *Executive Summary* report is sent daily, at midnight, to the email addresses defined during initial wizard setup. This report provides you with important information regarding detections made at your network.

Report management tools let you save, print, and export the reports that you generate.

Reports

You can generate comprehensive real-time reports regarding policy detections and endpoint discovery information. See Reports for more information.

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.

On-Screen Threat Protection Reporting

This section details the Console reports. Two categories of reports are available:

- Executive Reports
- Operational Reports

In addition, various customization options are available for reports. See Customizing Reports for more information. Report results display activity that occurred within a time range that you specify and 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.

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 events is an event followed by a bite event that is detected at an open, real port on the service that the bite event was detected.

Executive Reports

The Executive Report provides you with a concise overview of important CounterACT 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. ▪ 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. ▪ Top ten 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. ▪ Event summary showing important CounterACT and endpoint events. Report customization options allow you to adjust the following for the top ten reports: ▪ Only display results greater than a set value. ▪ Update, for example, the top ten value to top five or top fifteen.

Operational Reports

Operational reports provide you with extensive information about probe, scan, bite and infection attempt events that occurred at targets, endpoints and services in your network. These reports allow in-depth drill-down of security information gathered by CounterACT.

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 ten infected endpoints are displayed. This value can be changed from the Report Options dialog box.
Infected Hosts Displays information about infected endpoints in your network.	
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 allow you to generate a table listing the details of all the events shown in the report, i.e. a list of all the events.
Infected hosts by Service	Displays the infected endpoints in your network, sorted by service. Report options allow you to generate a table listing the details of all the events shown in the report, i.e. a list of all the events.
Top Worm-Infected Hosts	Displays the IP addresses of infected endpoints that carried out the most infection attempts. By default, the top ten infected endpoints are displayed. This value can be changed from the Report Options dialog box. Report customization options also allow you to: ▪ Only display results greater than a set value. For example, only show results if infected endpoints initiated more than ten infection attempts. ▪ Generate a table detailing report events.
Probing Hosts	
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.
Email Worm Infection Attempts	
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 ten most active endpoints. You can change this default. Additional report customization options allow you to only display results greater than a set value – for example, only show the results if the endpoints generated more than five email events.

Report	Details
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.
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.
Targeted Hosts Displays information about infection attempts that occurred at the endpoints in your network.	
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 ten real endpoints that were most frequently targeted are displayed. This value can be changed from the Report Options dialog box. Additional report customization options allow you to only display results greater than a set value; for example, only shown the results if the real endpoint was targeted more than ten times.
Infection Attempt Summary for a Selected Host	Displays all infection attempts that were targeted at a specific endpoint. Report options allow you to generate a table listing the details of all the events shown in the report. For, the date and time the event occurred and the endpoint IP address that initiated the event.
Targeted Services Displays information about services targeted in your network.	
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 allow you to adjust the following for the top ten reports: ▪ Only display results greater than a set value (calculated according to infected endpoints). ▪ Update, for example, the top ten value to top five or top fifteen (calculated according to infected endpoints).

Report	Details
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. This allows you to 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 ten services that were most frequently targeted are displayed. This value can be changed from the Report Options dialog box. Additional options allow you to only display results greater than a set value; for example, only display a service if it was attacked more than ten times.
Scan Results Displays information about Scan policy 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 ten 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: ▪ Only display results greater than a set value. ▪ Generate a table detailing report events.
Activity Statistics	
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. By default, the top ten bite methods are displayed. You can update this value from the Report Options dialog box. Report customization options also allow you to: ▪ Only display results greater than a set value. For example, only display results for a method if the method was used more than ten times. ▪ Generate a table detailing report events.

Report	Details
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 ten scan methods are displayed. You can update this value from the Report Options dialog box. Report customization options also allow you to: ▪ Only display results greater than a set value. For example, only display results for a method if the method was used more than ten 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 ten mark types that were most frequently distributed are displayed. You can update this value from the Report Options dialog box. Report customization options also allow you to: ▪ Only display results greater than a set value. For example, only display results for a mark type if the mark was distributed more than ten times. ▪ Generate a table detailing report events.
Top Always Allowed Services	Shows *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 ten 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 allow you to: ▪ Only display results greater than a set value. For example, only show services that were accessed more than ten times. ▪ Generate a table detailing report events. See Chapter 11: Managing Your Virtual Firewall Policy for more information.
Appliances	
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.

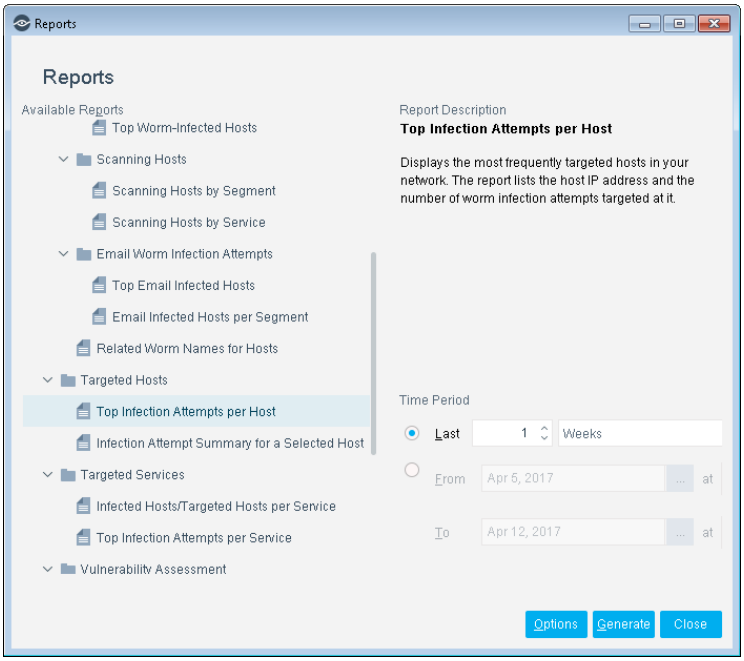
See Customizing Reports for information about customizing the report results display.

Generating On-Screen Threat Protection Reports

This section details how to generate reports on-screen and details the on-screen management tools, such as printing and exporting reports.

To generate a report on screen:

1. From the Console select **Reports** > **Threat Protection Reports** > **New**. The Reports dialog box opens.



Reports Dialog Box

2. Select a report.
3. In the **Time Period** section, specify a time period for results:
   - Relative time: Select **Last** and then specify the required number of hours, days, weeks or months by using the spin controls or by typing a value in the field. Select a time unit from the drop-down list.
   - A time range: Select **From** / **To** and then specify the beginning and end of the time range.
4. Select **Options** to customize the report. See Customizing Reports for more information.
5. Select **Generate** to create the report.

Customizing 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.

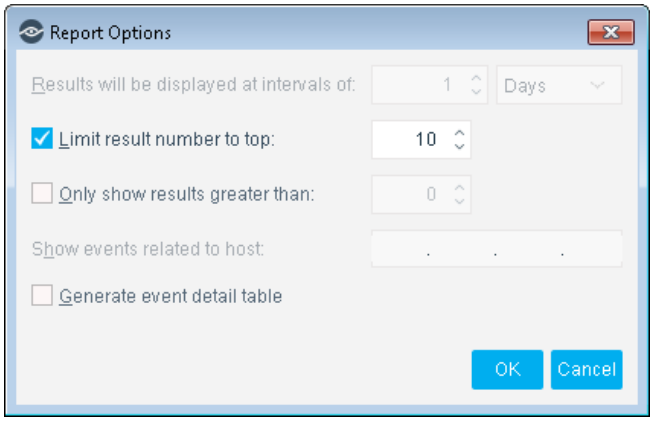
- Define the intervals at which results are displayed, i.e. hourly, daily, or weekly. The default is on a daily basis. See Define Result Display Intervals.
- Show only top-level results. The default is the top ten highest results. See Limit to Top Results Only.
- Show only results for a specific endpoint in the network. See Show Only Results for a Specific Endpoint.
- Show only results greater than a certain value. The default minimum value is one. See Show Only Results Greater Than a Set Value.

- Generate a table listing details of each event displayed in the report. See Generate a Detailed Event Table.
- Generate a report of activity at specific Appliances. See Generate a Report from Activity at Selected Appliances.

If you update the default, it is only applied to the current report. This means that after the report is generated, the default is restored.

To customize the report:

1. In the Reports dialog box, select a report and time period.
2. Select **Options**. The Report Options dialog box opens.



Report Options Dialog Box

Define Result Display Intervals

By default, report results are displayed on a daily basis. This means, for example, that if you choose to show the number of events that occurred over a two-month period, the results are displayed for each day over those two months.

You can customize the display by showing results on an hourly, per day, weekly or monthly basis. For example, you can show infection attempts that occurred over a two-month period, and display the results for each week, i.e., numbers of infection events that occurred each week.

To update the intervals:

1. In the Reports dialog box, select a report and time period.
2. Select **Options**. The Report Options dialog box opens.
3. In the **Results will be displayed at intervals of** field, enter a numerical value and click the drop-down arrow to select a time unit.
4. Select **OK**.
5. Select **Generate** from the Reports dialog box.

Limit to Top Results Only

Reports can be customized so events are displayed for the highest level of results only, i.e. only showing the top five or top ten results. For example, you can choose to display only the ten endpoints with the highest number of infection events or only

the five top targeted services. This option is useful when your system generates an extensive number of results, and you want to limit the report to display only significant information.

To display top results only:

1. In the Reports dialog box, select a report and time period.
2. Select **Options**. The Report Options dialog box opens.
3. In the **Limit result number to top** field, enter a value for top results.
4. Select **OK**.
5. Select **Generate** from the Reports dialog box.

Show Only Results Greater Than a Set Value

You can customize the report to only show results that are greater than a set value. This means that results are reported only if a specific threshold is passed. For example, you can generate a report of events at real endpoints, and set the “greater than” value to 20. This means that the report will only display the real endpoints at which more than 20 events occurred. This option is useful when your system generates an extensive number of results, and you want to limit the report to display only significant information.

To set a greater than value:

1. In the Reports dialog box, select a report and time period.
2. Select **Options**. The Report Options dialog box opens.
3. In the **Only show results greater than** field, enter a top value or use the spin controls to set the value.
4. Select **OK**.
5. Select **Generate** from the Reports dialog box.

Show Only Results for a Specific Endpoint

The Infection Attempt Summary for a selected Host report allows you to generate a report displaying infection attempt events that occurred at a specific endpoint in the network.

1. In the Reports dialog box, select a report and time period.
2. Select **Options**. The Report Options dialog box opens.
3. Insert the endpoint address in the **Show events related to host** field.
4. Select **OK**.
5. Select **Generate** from the Reports dialog box.

Generate a Detailed Event Table

Most reports are presented in chart form and summarize activity. These reports can be supplemented with more detailed information. For example, if the report chart shows the number of infection attempt events that occurred over a two-week period, you can generate a list that itemizes each of the events.

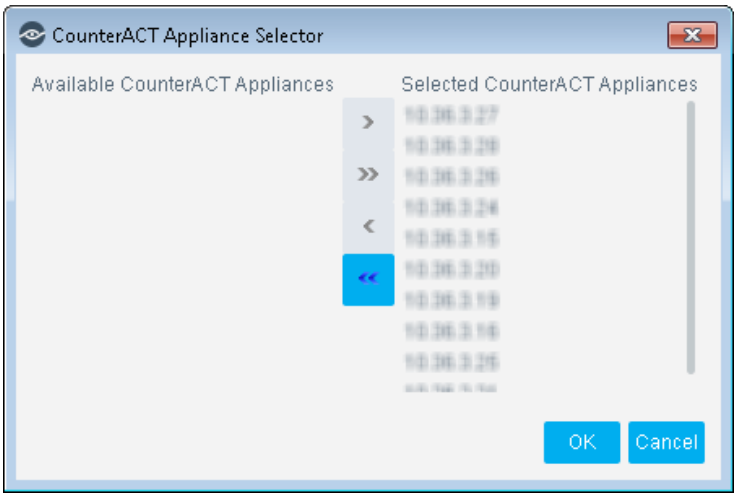
1. In the Reports dialog box, select a report and time period.
2. Select **Options**. The Report Options dialog box opens.
3. Select **Generate event detail table**.
4. Select **OK**. The information is viewed from the report toolbar. See Working with On-Screen Report Management Tools for more information.
5. Select **Generate** from the Reports dialog box.

Generate a Report from Activity at Selected Appliances

Your reports can include information collected from one or more Appliances.

To select an Appliance:

1. In the Report Options dialog box, select **Appliance**. The Appliance Selector dialog box opens.



Appliance Selector Dialog Box

2. Select an Appliance from the **Available Appliances** list.
3. Use the arrow buttons to assign the Appliances to the **Selected Appliances** list.
4. Select **OK**.
5. Select **OK** in the Report Options dialog box.
6. Select **Generate** in the Reports dialog box.

Viewing Multiple Reports

You can generate multiple reports and view them. In addition, you can display a list of the report windows that you have opened and select a report to view if that report is minimized.

To open a list of reports:

1. Select **Reports** from the **Window** menu and then select the report to open.

Viewing Report Definitions

You can display the report definitions for the reports that you generate on-screen, including the report name, the time period the report covers and report options. This is particularly useful when you have several reports open simultaneously.

To view report definitions:

1. Generate a report.
2. Select **Report Definitions** from the **View** menu. The report definitions for the report that you created are shown.

Working with On-Screen Report Management Tools

On-screen tools are available to manage and navigate around the reports that you generate. These tools can be accessed from both the menu and toolbar of the report. This section details toolbar options.

Reports Toolbar

Icon	Details
First/Last Page	Moves to first or last page of the report. (Only available when the report is displayed in print layout view).
Previous/Next Page	Moves to 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 update if required. See Modifying the Report Output Location for Manually Saved Reports. You can open saved reports from the **Reports** menu on the Console.
Print/Normal Layout View	View the report in either print layout view or normal layout view. The cover page and the header and footer can be seen in the print layout.
	View the report chart or the event detail table, if you generated one.

Exporting Reports and Report Event Details

You can export reports and report event detail tables to a:

- PDF file viewable in Adobe Acrobat

- CSV file viewable in Microsoft Excel
- HTML format viewable in your web browser

To export a report:

1. Select **Export** from the **File** menu. 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 and the **Export Event Table** menu option to export the table as a PDF file.

Generating Scheduled Reports

The report scheduler allows you to generate reports according to a defined schedule, and receive them by email. Generating a report schedule includes the following steps:

a. Select a report.
b. Define a delivery schedule.
c. Define a report file format.
d. Define email delivery addresses.
e. Design a report cover page, and header and footer text.

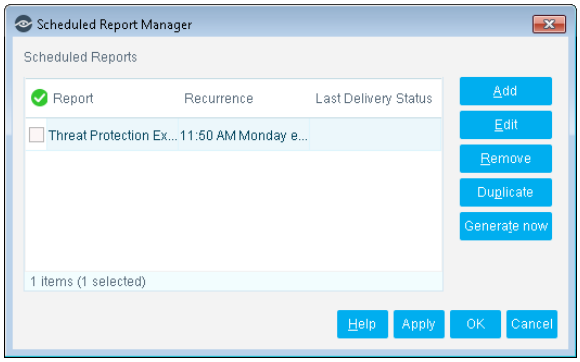
Tools are also available to edit, delete and duplicate report schedules, and automatically run scheduled reports.

In addition, all reports that you receive through the scheduler are automatically saved to a default location on the CounterACT device. You can access and open the reports from the Console. See Opening Saved Reports for more information.

Report schedules are created and managed from the Scheduled Report Manager dialog box. Not all users have access to the scheduled report features.

To open the Scheduled Report Manager dialog box:

1. Select **Threat Protection Reports** from the **Reports** menu on the Console and then select **Scheduler**. The Scheduled Report Manager wizard opens for creating a schedule.

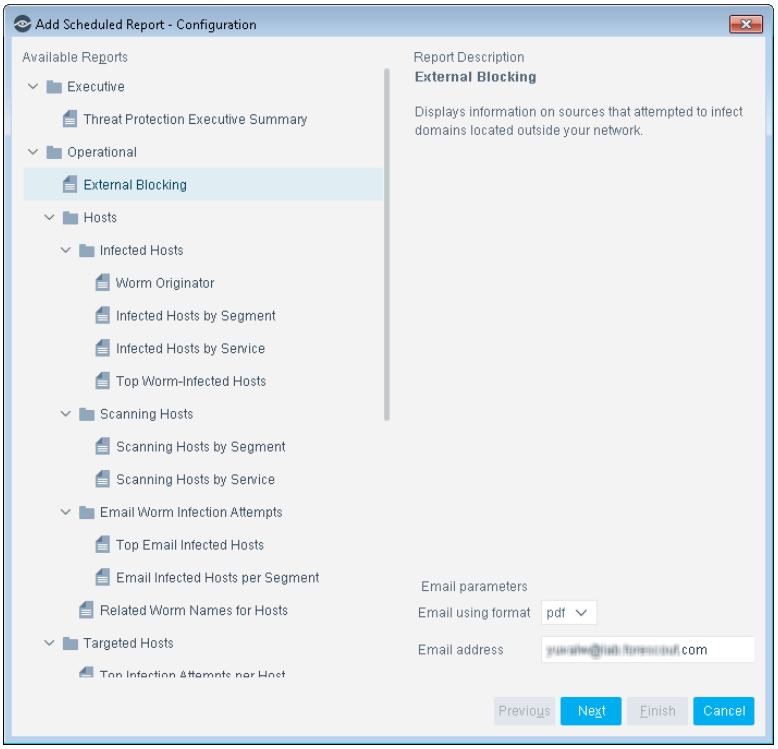


Scheduled Report Manager Dialog

☑	When the checkmark is displayed, the schedule is activated. If de-activated, the report will not be created.
Report	Displays the name of the report.
Recurrences	Displays the creation schedule.
Last Delivery Status	Displays the last time the report was delivered.

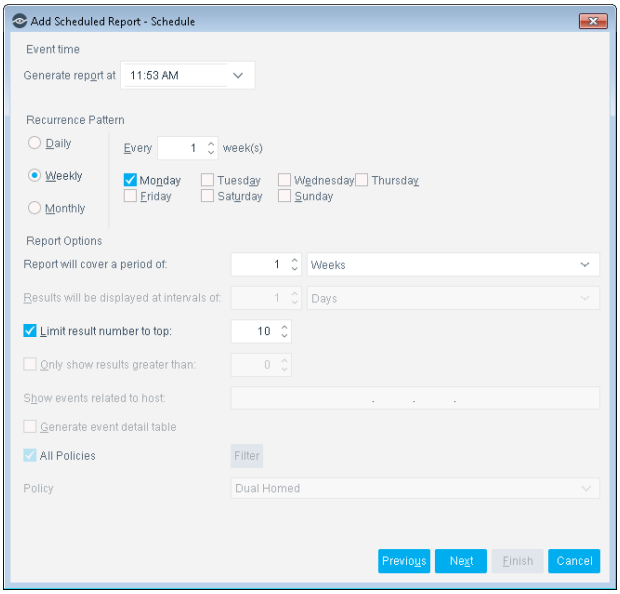
To create a report schedule:

1. Select the **Reports** menu and then select **Threat Protection Reports**>**Scheduler**. The Scheduled Report Manager dialog box opens.
2. Select **Add**. The Available Reports dialog box opens.



Configuration Dialog Box, Add Scheduled Reports

3. Select a report from the Available Reports tree.
4. Select the file format in which to deliver reports from the **Email using format** field. The default is PDF. If you select CSV format, you cannot use the report cover page and header/footer option. If you select HTML format, you can only use the cover page option.
5. In the **Email address** field, enter any number of email addresses in which to send the reports. Multiple addresses must be separated by commas.
6. Select **Next**. The Add Scheduled Report – Schedule dialog box opens.

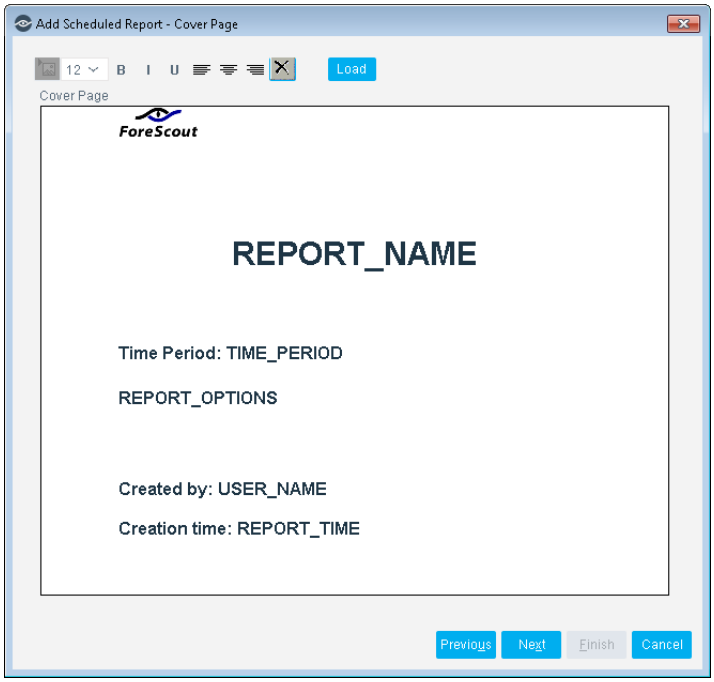


Add Scheduled Report Dialog Box, Schedule

7. In the **Generate report at** drop-down list, specify a time to generate and send the report.
8. Select an interval in which to generate the reports. The report can be generated daily, weekly or monthly.

Daily	Type a value in the **Generate every** field; for example, every eight days.
Weekly	Type a value in the **Generate every** field; for example, every two weeks. Select the required checkboxes to indicate which days of the week the report is generated.
Monthly	In the **Days** field, enter the days of the month to generate the report. Use a hyphen to indicate day ranges. Days and ranges must be comma-separated. Type a value in the **every** field. For example, you can receive reports on the 1st, 10th and 20th day of the month, every two months.

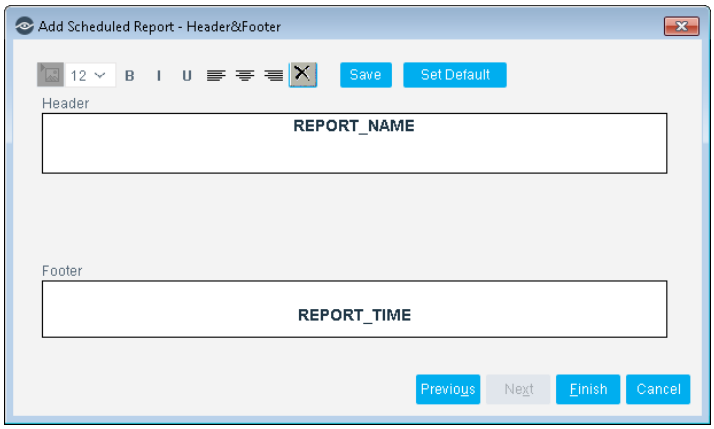
9. Customize the report by selecting a customization option from the Report Options pane. See Customizing Reports for more information.
10. Select **Next**. The Add Scheduled Report – Cover Page dialog box opens.



Add Scheduled Report Dialog Box, Cover Page

11. By default, the Report name, user name, creation date and report options that you selected will appear on the report cover. You can update or delete this text or add a JPG graphic file by using the standard editing tools located on the toolbar.

12. Select **Next**. The Add Scheduled Report – Header&Footer dialog box opens.



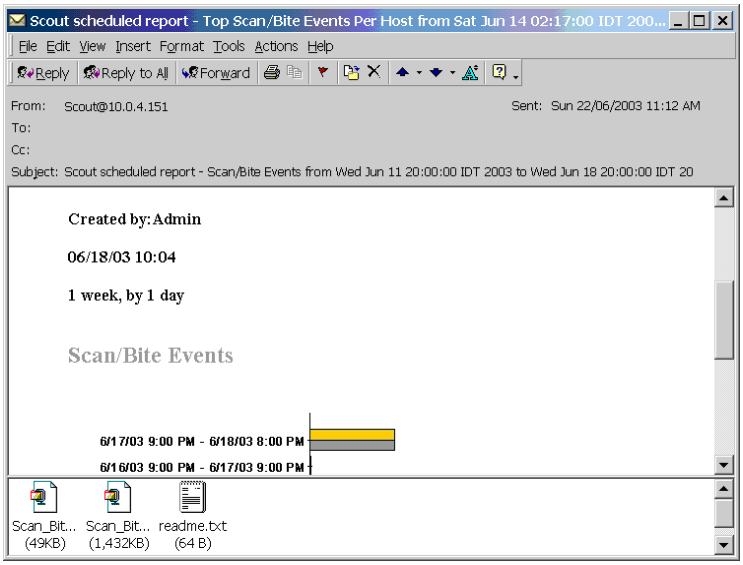
Header&Footer Dialog Box, Add Scheduled Reports

13. If required, delete, add or edit the text using the standard editing tools located on the toolbar. Page numbers automatically appear for reports generated as PDF files, and in the print layout view.

Tools are also available to save your cover page, header and footer text, and load them to other reports, or to create a default cover page, header and footer. See Managing the Cover Page, Header and Footer Text for more information.

14. Select **Finish**. The report that you scheduled is displayed in the Scheduled Report Manager dialog box.
15. Select **OK** in the Scheduled Report Manager dialog box.

    The report is sent to the email addresses that you defined, according to the delivery schedule and report format that you chose. If you generated an event detail table, the email will also include a zipped CSV file containing the detailed event information.



Sample Mail, HTML Report with Attached Event Detail File

Report Scheduler Management Tools

The following management tools are available from the Scheduled Report Manager dialog box:

- Removing a scheduled report
- Editing scheduled report
- Duplicating a scheduled report
- Running a scheduled report
- Managing the cover page, header and footer

To remove a scheduled report from the scheduler:

1. Select a report schedule from the Scheduled Report Manager dialog box.
2. Select **Remove**.
3. Select **OK**.

   The report is removed and will not be generated.

To edit a scheduled report:

1. Select a scheduled report from the Scheduled Report Manager dialog box.
2. Select **Edit**. The Edit Scheduled Report dialog box opens.

3. Use the tabs to edit the schedule.
4. Select **OK**.
5. Select **OK** from the Scheduled Report Manager dialog box to save your changes.

To duplicate a scheduled report:

1. Select a scheduled report from the Scheduled Report Manager dialog box.
2. Select **Duplicate**. The Add Scheduled Report dialog box opens.
3. Update as required.
4. Select **OK** on the Edit Scheduled Report dialog box.
5. Select **OK** on the Scheduled Report Manager dialog box to save your changes.

To run a scheduled report:

1. Select a scheduled report from the Scheduled Report Manager dialog box.
2. Select **Generate Now**. A confirmation is displayed.
3. Select **Yes** to send the report.

Managing the Cover Page, Header and Footer Text

Tools are also available to save your cover page, header and footer text, and load them to other reports, create a default cover page, header and footer, and work with automated text.

To save the cover page, header and footer:

1. Update the cover page, header and footer as required.
2. Select **Save** from the Add Scheduled Report – Header&Footer dialog box. A standard save dialog box opens.
3. Save the information to the required location.

To load a previously saved cover page, header and footer:

1. Select **Load** from the Add Scheduled Report – Cover Page dialog box. A standard Open dialog box opens.
2. Locate and open the required file.

To create a default cover page, header and footer:

1. Select **Set Default** from the Add Scheduled Report – Header&Footer dialog box. A confirmation message opens.
2. Select **Yes** to save the cover page, header and footer as the default.

Working with Automated Text Tags

Your cover page, header and footer are generated by default with automated text tags.

The text is viewable in the print preview layout (on-screen reports), in reports exported or mailed as a PDF file. The cover page text is available if you export or email the report as an HTML file.

The following text tags are available:

REPORT_NAME	The name of the report generated.
REPORT_TIME	The time the report is generated.
USER_NAME	The name of the user that generated that sent the report.
TIME_PERIOD	The time period that the report covers.
REPORT_OPTIONS	All parameters, except the time.

Any tag can be entered on the cover page, header or footer, according to the following format requirements:

- Use all caps (upper case), i.e. REPORT_TIME and not Report_Time.
- Use the same font for each tag.
- Use up to three lines of text for each of the header and footer.

To enter text tags:

1. Enter the tags according to the relevant format requirements.

   The tags are converted with the related information, and viewable in the print preview layout (on-screen reports) and in reports exported or delivered as a PDF file.

Opening Saved Reports

Two options are available for opening reports.

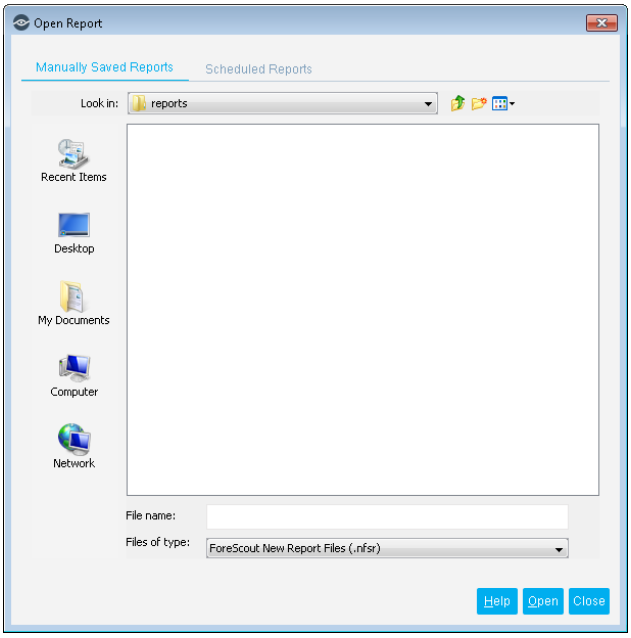
- Open a report that you saved manually.
- Open scheduled reports. Reports created by the report scheduler are automatically saved in the CounterACT device, and can be opened from the Console.

Opening a Report That You Saved Manually

The reports that you manually saved are stored by default at the location where you installed the Console. This location can be changed.

To open a report that you saved:

1. Select **Threat Protection Reports** from the **Reports** menu and then select **Open**. The Open Report dialog box opens.



Open Report Dialog Box, Manually Saved Reports

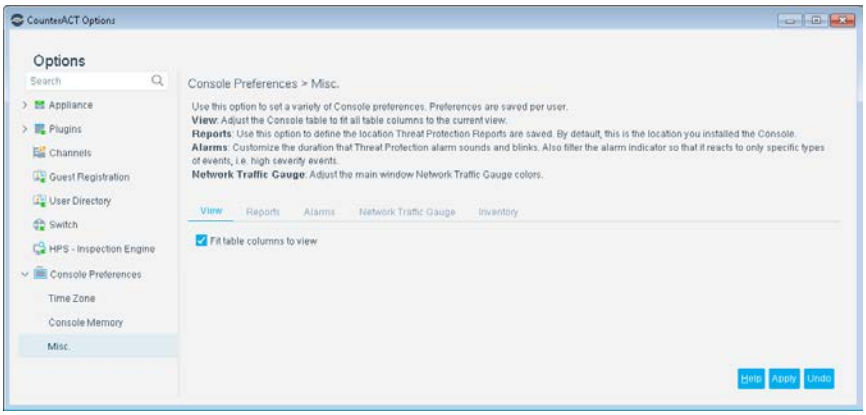
2. Select the Manually Saved Reports tab.
3. Locate the report that you saved and then select **Open**. The report opens.

Modifying the Report Output Location for Manually Saved Reports

The reports that you manually save are stored by default at the location where you installed the Console. This location can be changed.

To set the default location for report files:

1. Select **Options** from the **Tools** menu and then select **Console Preferences**>**Misc**.
2. In the Reports tab, type in the desired directory path or use the browse button to open a dialog box from which you can choose the path. Files are saved to the specified path.



Reports Path for Manually Saved Reports

3. Select **OK**.

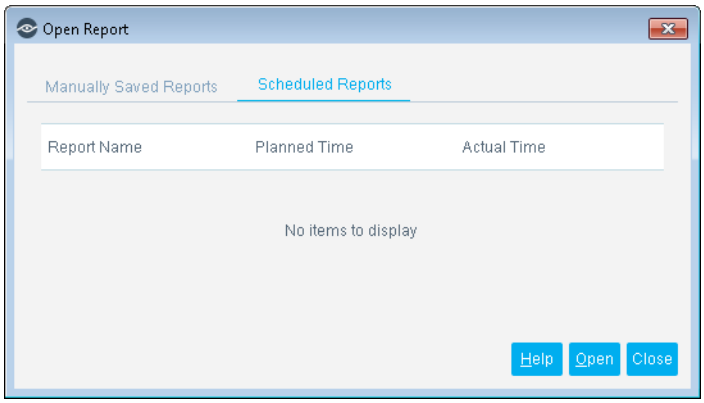
Opening a Scheduled Report

CounterACT automatically saves all reports that you received through the report scheduler. These reports can be opened in the Console, printed and exported.

Scheduled reports are automatically saved to the Appliance under the Reports directory. Reports are deleted when the directory size reaches 20 MB. The oldest reports are deleted first.

To open a scheduled report saved by CounterACT:

1. Select **Threat Protection Reports**>**Open** from the **Reports** menu. The Open Report dialog box opens.



Open Report Dialog Box, Scheduled Reports Tab

2. Select the Scheduled Reports tab.

   All reports that you created through the report scheduler are displayed. The dialog box displays the scheduled and actual time of delivery. Slight discrepancies may occur if you scheduled several reports for delivery at the same time or because of technical issues.

3. Select a report and then select **Open**. The report opens.

   Event detail tables generated for reports saved by CounterACT are not automatically available. This information must be saved separately and then opened.

To view a related event detail table:

1. Select **Open** on the Open Report dialog box.
2. Select **Save** from the **File** menu. A standard Save dialog box opens.
3. Save the event detail file as required in CSV format and select **Save**.

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 CounterACT Reports Plugin. Plugin updates may be available in between CounterACT version releases.

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 to provide information about:

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

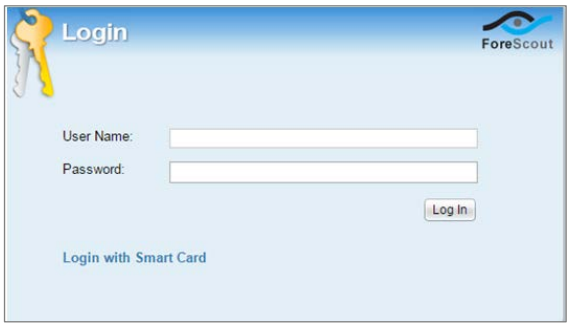
You can create reports and view them immediately, save reports, or generate schedules to ensure that network activity and detections are automatically and consistently reported.

In addition, you can use any language supported by your operating system to generate reports. Reports can be viewed and printed as PDF or CSV files.

To access the Reports portal:

1. Do one of the following:
   - In the Console toolbar, select the ellipsis icon and select **Reports**, or press **CTRL+ R**.
   - Browse to the following URL: http://<Device_IP>/report

     Where <*Device_IP*> is the IP address of the Enterprise Manager or an Appliance. A login page opens.



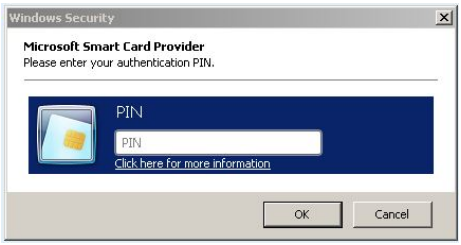
Portal Login Page

When you access the portal from the Console, you may not be prompted to log in. For more information see Log in to Each CounterACT Web-Based Portal.

2. Enter the **User Name** and **Password** of a user that can access the portal. Typically the credentials you use to access the Console also grant access to the portal. For more information, see Creating Users and User Groups.
3. (Smart Card Authentication) If you are working with Smart Card authentication, you may be prompted for the login information described here.
   a. Select the **Login with Smart Card** link. The Select a Certificate dialog box opens.

Smart Card Login – Select Certificate

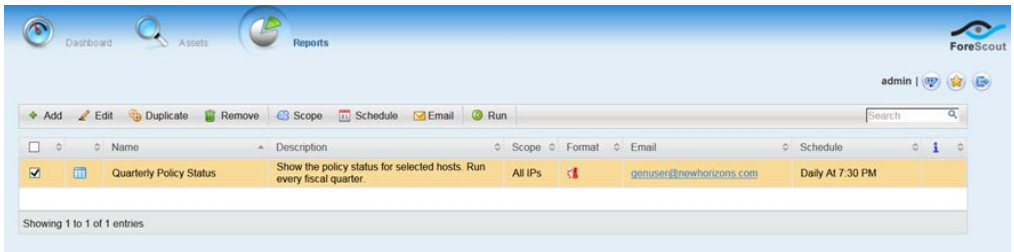
b. Select a certificate and then select **OK**. A PIN dialog box may open.



Smart Card Login – Enter PIN Code

c. Enter a PIN code and then select **OK**.

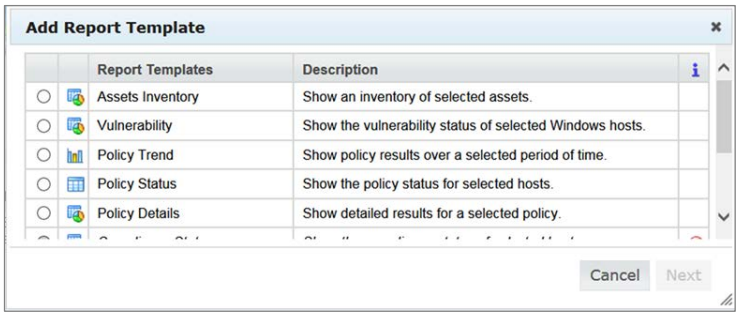
4. The portal opens.



Reports Home Page

To add a Report:

1. Select **Add** from the Reports portal home page. The Add Report Template window opens.



Add Report Template Window

2. Select a report template and define the report parameters.

Working with System Event Logs

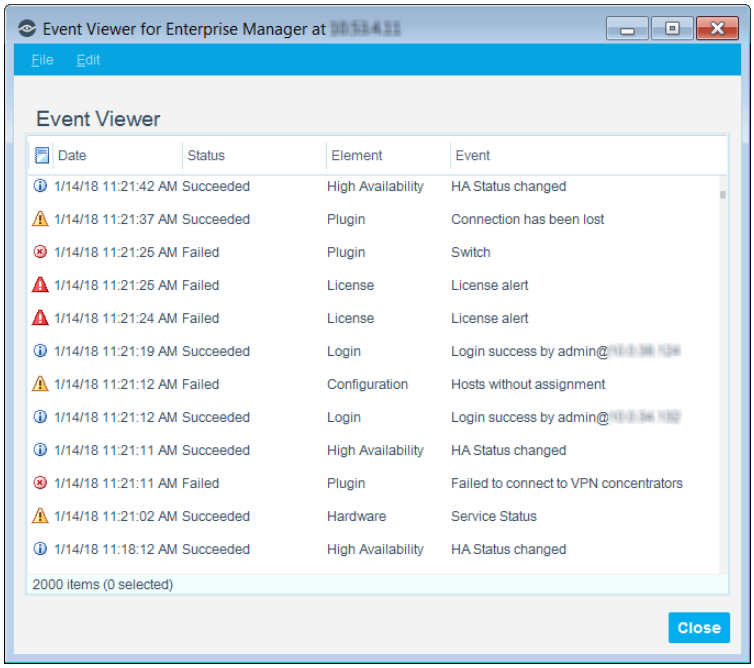
You can view logs about system activity; for example, successful and failed user login operations.

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, review the Syslog Plugin documentation. See Additional CounterACT Documentation for information about how to access the documentation.

To view events:

1. Select **Event Viewer** from the **Log** menu. The Event Viewer dialog box opens.



Event Viewer Dialog Box

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 that 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.

To clear all data from the table:

1. Select **Clear All** from the **File** menu.

   The data is cleared from the table. This information remains in the system. The toggle option displays as **Reload**.

Clear All *and* ***Reload*** *is a toggle option.*

To reload data in the table:

1. Select **Reload** from the **File** menu.

   The latest data loads from the database. The toggle option displays as **Clear All**.

To find an entry in the event viewer:

1. Select **Find** from the **Edit** menu or press **Ctrl-F**. The Find dialog box opens.
2. Use the Text to find field and options to make your search more efficient.

To save the log to an external file:

1. Select **Export** from the **File** menu. The Export Event dialog box opens.
2. Select a location and file format. You can save the file in TXT or XLS format.

To view details for an event in the log:

1. Double-click a selected line. The Event Viewer opens with details about the selected event.

Viewing Block Events

A Block Events log allows you at-a-glance display of the following block events. For example:

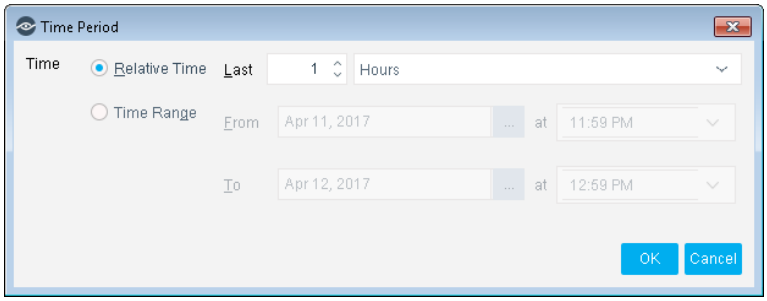
- Host blocks
- Port blocks
- External Port blocks
- External Host blocks
- Services closed as a result of service attacks
- Services closed as a result of the blocking rules that you defined via the Virtual Firewall

Use the log to troubleshoot problematic network block events. You can export the information displayed to a CSV file.

These events are sent automatically to the Syslog server. If you do not want to send them, configure the CounterACT Syslog Plugin not to transfer this information. Select ***Tools*** > ***Options*** > ***Modules > Core Extensions > Syslog > Configure > Events filtering***.

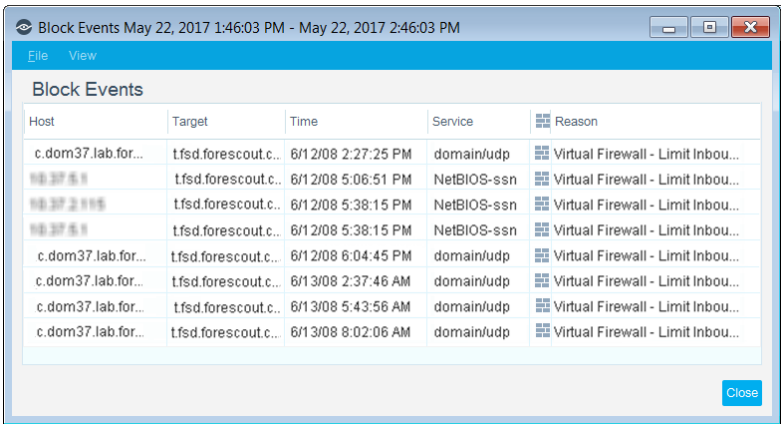
To view blocked events:

1. Select **Blocking Logs** from the **Log** menu. The Time Period dialog box opens.



Time Period Dialog Box

2. Select a time period by doing one of the following:
   - Select **Relative Time** and then specify the required number of hours, days, weeks or months by using the spin controls or by typing a value in the field. Select a time unit from the drop-down list.
   - Select **Time Range** and then specify the beginning and end of the time range.
3. Select **OK**. The Block Events dialog box opens.



Block Events Dialog Box

The following information is available:

Item	Description
Host	The endpoint that was blocked.

Item	Description
Target	The IP address to which the blocked endpoint attempted to connect.
Time	The time 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.

To export the list of block events:

1. Select **Export** from the **File** menu.

To find specific text in the list of events:

1. Select **Find** from the **View** menu.

Refreshing the List of Events

If you selected a relative time when generating the block events list, you can refresh the information to include events blocked from the start time that you indicated, up to and including the current time (while the dialog box is open).

To refresh the information:

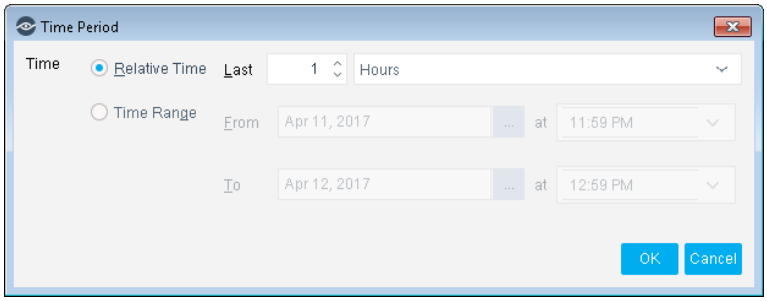
1. Select **Refresh** from the **File** menu.

Viewing 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. See Handling Service Attacks for more information about how to work with these policy definitions.

To view a history of monitored and blocked services:

1. Select **Service Attack History** from the **Log** menu. The Time Period dialog box opens.



Time Period Dialog Box

2. Select a time period by doing one of the following:
   - Select Relative Time and then specify the required number of hours, days, weeks or months by using the spin controls or by typing a value in the field. Select a time unit from the drop-down list.
   - Select Time Range and then specify the beginning and end of the time range.
3. If you have logged in to the Console via an Enterprise Manager, you can select specific Appliances for which to run a report.
4. Select **OK**. The Blocked Events dialog box opens.

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 mouse to view a tooltip that lists 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 that 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.

Chapter 11: Managing Your Virtual Firewall Policy

- Defining a Virtual Firewall Policy
- Defining Block Rules
- Viewing Block Events
- Defining Allow Rules

Defining a Virtual Firewall Policy

Virtual Firewall protection allows you to easily create network security zones, giving you more 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 unwanted protocols from being transmitted 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.

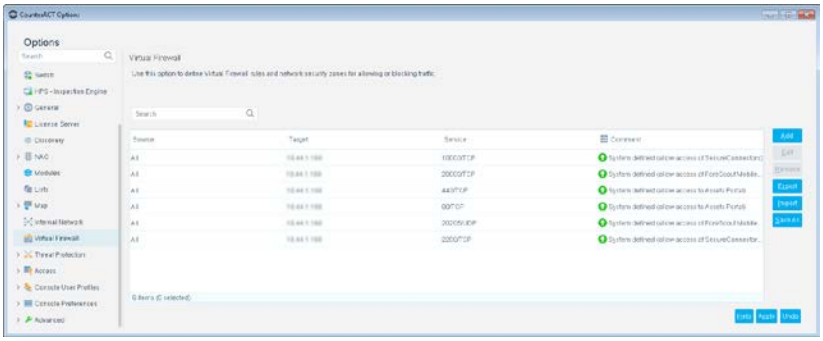
The Virtual Firewall gives you all the benefits of an inline firewall, without being located inline. This means there are no issues of latency. In addition, you can export a list of allow and blocking rules to a CSV file, and can also view a list of block events that were detected as a result of the blocking rules that you defined.

If you have created an exception rule via the Virtual Firewall and also create a policy rule that blocks detected endpoints, the Virtual Firewall exception rule takes precedence. This means that the endpoints will not be blocked.

Virtual Firewall rules are centrally managed. This means rules cannot be added, edited or removed from individual Consoles that are part of your enterprise.

To access the Virtual Firewall pane:

1. Select **Options** from the **Tools** menu and then select **Virtual Firewall**.



Virtual Firewall Pane

What You See on Your Screen

The Virtual Firewall pane displays rules that were generated from the following locations:

- Rules defined directly from the Virtual Firewall box, as detailed in this section.
- Endpoints that were detected as a result of a policy Virtual Firewall action.

- System-defined rules: These are rules that support basic CounterACT 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 here, but were created either 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 at which 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.

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

Defining Block Rules

Define Block rules by using the Virtual Firewall to prevent outbound traffic at source IP addresses from reaching target IP addresses.

TCP versus 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:

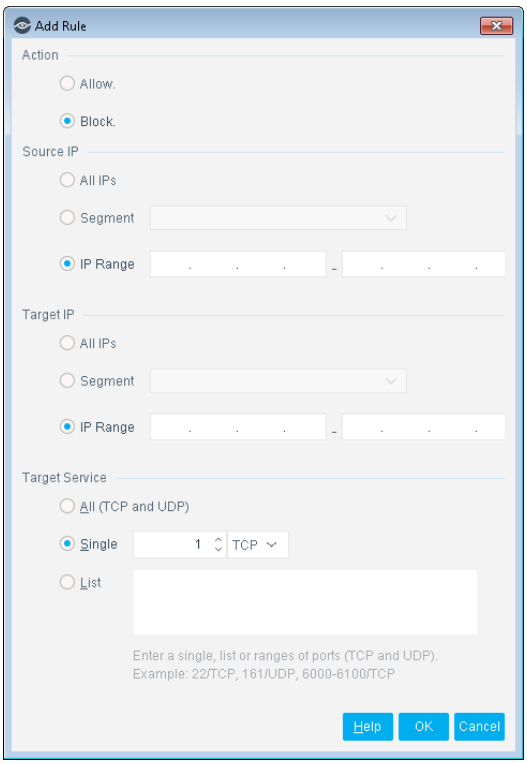
- With syslog, there is no opportunity to terminate the session. The sender transmits the data message to the syslog server but does not wait for a reply.
- With DNS, there is a single opportunity to terminate the session. After the sender transmits a query, they wait for a reply. If the Virtual Firewall 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.

To be sure that UDP sessions are terminated, it is recommended that you block them using the Switch Port Access List or integrate CounterACT with a third-party firewall such as Cisco ASA. See Chapter 8: Base, Content and Extended Modules for more information.

Working with Block Rules

To define Block rules:

1. Select **Options** from the **Tools** menu and then select **Virtual Firewall**.
2. Select **Add**. The Add Rule dialog box opens.



Add Rule Dialog Box

3. In the **Action** section, select **Block**.
4. In the **Source IP** section, define addresses that are prevented access to target IP addresses:
   - Select All to block traffic from all IP addresses.
   - Select Addresses to define a single IP address or an address range.
   - Select Network Segment to define a segment.
5. In the **Target IP** section, define the endpoints that are prevented access to the previously defined source IP addresses:
   - Select All for all IP addresses.
   - Select Addresses to define a single IP address or an address range.
   - Select Network Segment to define a segment.
6. In the **Target Service** section, define the services that are blocked on the targeted (detected) endpoints:
   - Select All for all services (at the previously defined target IP addresses) on the endpoint to remain blocked.
   - Select Single to define a service. Type a port and select a protocol from the drop-down list.
   - Select List to enter a comma-separated list of services.
7. Enter comments as required.
8. Select **OK**. The rule is displayed on the Virtual Firewall pane.

To remove a rule from the blocking rule list:

1. Select a Block rule from the Virtual Firewall pane.
2. Select **Remove**.
3. Select **Apply**.

To edit a rule from the blocking rule list:

1. Select a Block rule from the Virtual Firewall pane.
2. Select **Edit** and edit the rule required.
3. Select **Apply**.

Viewing Block Events

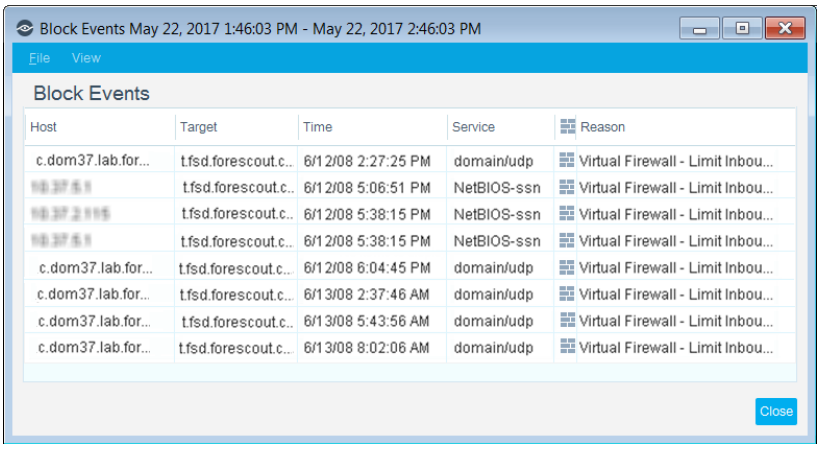
A list of sources and endpoints that have been blocked as the result of a blocking rule (Virtual Firewall pane) can be viewed from the Block Events dialog box. This may be useful for troubleshooting.

To view a list of events:

1. Select the **Blocking Log** from the **Log** menu. The Time Period dialog box opens.
2. Select a time period by doing one of the following:

– Select Relative Time and then specify the required number of hours, days, weeks or months by using the spin controls or by typing a value in the field. Select a time unit from the drop-down list.
– Select Time Range and then specify the beginning and end of the time range.

3. Select **OK**. The Block Events dialog box opens. The Reason column indicates which events were blocked due to a blocking rule defined in the Virtual Firewall.



Block Events Dialog Box

Defining Allow Rules

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:

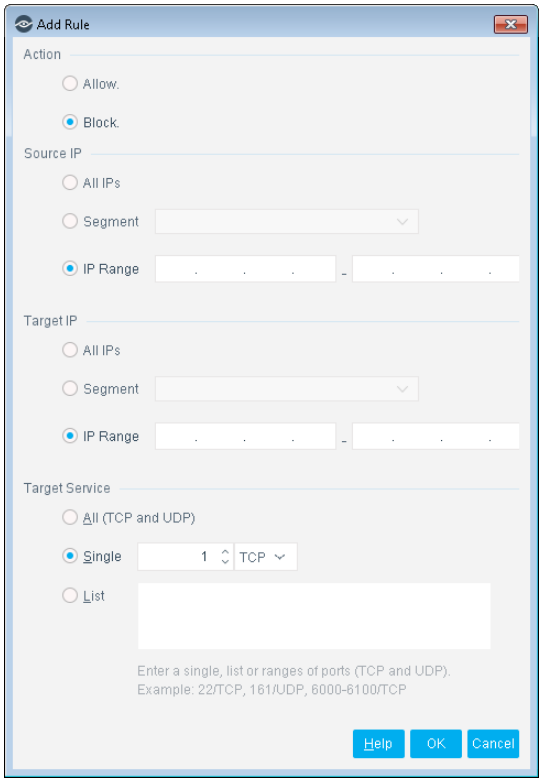
- The Threat Protection Policy is set to block
- The source is manually blocked or ignored
- The policy is set to block
- The policy for handling email worm infection attempts is set to block
- You have manually blocked an endpoint from the Home view, Detections pane
- You have assigned an identical blocking rule

Use this option to keep mission critical services available.

Allow rules are not applied to endpoints that are blocked by external systems, i.e. switches, router, VPNs or firewalls.

To define Allow rules:

1. Select **Options** from the **Tools** menu and then select **Virtual Firewall**. The Virtual Firewall pane opens.
2. Select **Add**. The Add Rule dialog box opens.



Add Rule Dialog Box

3. Select **Allow**.
4. In the **Source IP** section, select addresses that are always allowed to transmit traffic to specified target endpoints:
   - Select All for all addresses.
   - Select Addresses for a single address or a group of addresses.
   - Select Network Segment to define a segment.
5. In the **Target IP** section, define the endpoints that are always accessible to the previous defined Source IPs:
   - Select All for all addresses.
   - Select Addresses for a single address or a group of addresses.
   - Select Network Segment to define segments.
6. In the **Target Service** section, define the services that are accessible on the target (detected) endpoints:
   - Select All for all services (at the previously defined target IP address ranges) on the endpoint to remain open.
   - Select Single to define a service. Define a port and select a protocol from the drop-down list.
   - Select List to enter a comma-separated list of services.
7. Enter comments as required.
8. Select **OK**.

   The rule is displayed in the Virtual Firewall pane.

Removing and Editing Allow Rules

To remove a range:

1. Select a rule from the Virtual Firewall pane.
2. Select **Remove**.
3. Select **OK**.

To edit a range:

1. Select a rule from the Virtual Firewall pane.
2. Select **Edit**.
3. Edit the range as required.
4. Select **OK**.

Chapter 12: Threat Protection

- About Threat Protection
- About the Threat Protection Policy
- Viewing Threat Detections
- Viewing and Updating the Policy
- Customizing Basic Policy Settings
- Working with Manually Added Endpoints
- Defining the Active Response Range
- Viewing Endpoint Activity Details
- Managing Enterprise Lockdown Alerts
- Legitimate Traffic

About Threat Protection

This section details basic concepts and terminology regarding network threats. A network threat is a device from which a malicious event, for example, a NetBIOS attack, was detected via a Threat Protection policy.

- Detecting Threats – How It Works
- Basic Terminology

Detecting Threats – How It Works

This section details how infection attempts are carried out and how CounterACT protects your network.

CounterACT detects and handles email worm infections differently than network worm infections. See Email Worm Policy for more information.

Infection Attempt – Network Not Protected

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 existing or new attack methods. Malicious traffic quickly infects your network through various entry points, such as VPN users, trusted partner networks, or vulnerable laptops.

Infection Attempt – Network Protected

CounterACT prevents infection attempts by identifying and suppressing malware before it propagates within your network and to organizations outside your network. CounterACT 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, CounterACT 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 CounterACT identifies a request for a service in the network, it 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, CounterACT immediately recognizes it. Either CounterACT continues to monitor the traffic, or CounterACT 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*.

CounterACT also automatically detects heavily scanned services, and responds by either monitoring or blocking these services. When a service is monitored, CounterACT records all traffic going to the service. When a service is blocked, no communication with that service is permitted.

CounterACT also responds to:

- Service attacks
- Emails worms

Worm Slowdown Mechanism

A worm slowdown mechanism, part of the threat protection technology, provides two significant benefits:

Reduces network traffic congestion, thus improving network availability and stability	The worm slowdown mechanism enables CounterACT to notably reduce the amount of traffic generated by an infected machine while it attempts to propagate within your network. Specifically, the mechanism allows CounterACT to lock the infected machine in a static TCP dialog. As a result, traffic from the infected machine is kept at a standstill.
Provides added protection to hosts within a cell and the remaining network	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 CounterACT 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.

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 CLI.
2. Run the following command: **`fstool wormdelay disable`**

   The following message opens:

   ```
   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`**

Basic Terminology

This section details basic 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. This means that CounterACT 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.

CounterACT 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 CounterACT 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, CounterACT considers this activity a scan*. 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.)

  **The default probe count is five probes for port scans.*

- 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. This means, for example, that 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. See Customizing Scan Settings for details.

CounterACT updates the port scan category when subsequent probe activity takes place within the required 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 required time period, the category is changed to a TCP vertical scan.

Viewing Port Scan Categories

The Reason column in the Detections pane, and the Activity tab of the Host Details dialog box indicate which port scan categories were detected.

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, CounterACT allows the endpoint to communicate with the network and records the endpoint activity. In addition, CounterACT responds by sending marks to the endpoint – virtual resource information required to carry out the infection.

If the endpoint continues to scan your network while it is being monitored, 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.

This 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 that 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.

CounterACT 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, CounterACT 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 CounterACT responds to infected endpoints.

Manually Added Endpoints

Manually added endpoints are endpoints that you manually add to your system. This means that 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 that 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 block or monitor period for probing endpoints or infected endpoints 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 – the total block time would be 14 hours. If the endpoint does not perform another event within the block or monitor time, it is released – 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

CounterACT identifies and responds to email worms sent over email, specifically 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 to 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

CounterACT identifies services attacks when a service-probing criterion is met, i.e. when a service is heavily probed by multiple endpoints. CounterACT 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.

About the Threat Protection Policy

Threat Protection policies allow you to define how CounterACT should handle endpoints that scan and attempt to infect your network. Endpoints can be blocked entirely or prevented from accessing the service that they targeted. You can also choose to monitor endpoints. When monitored, the endpoints can communicate with the network, but CounterACT continues to record their activity and sends marks to them, as required.

Not all users have access to the policy features. See Access to Console Tools – Permissions for details.

About Advanced Policy Tools

Advanced policy definition tools let you customize settings for various types of scan and infection attempts. For example, you can customize the time interval in which to

monitor endpoints that use specific scan methods. HTTP scans may be handled differently than NetBIOS scans.

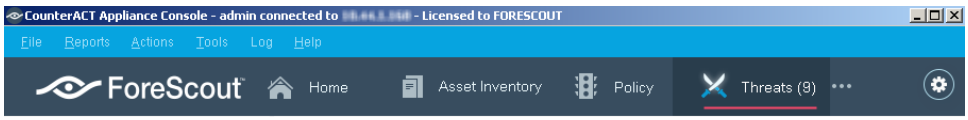
You can also choose to block endpoints that use specific types of infection methods. For example, a Login infection attempt may be handled differently than a Port infection attempt.

The 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.

Advanced email options allow you to customize the email delivery policy for email alerts regarding scans and infection attempts.

Viewing Threat Detections

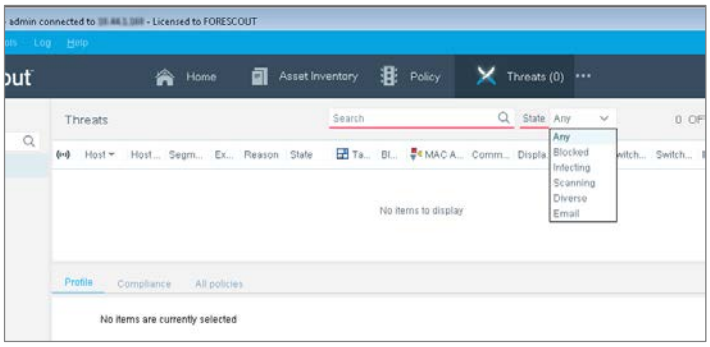
Endpoints detected by your threat detection policies are displayed in the Console, Threats view.



Threats Tab

The Console, 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:*** Use a drop-down list to display endpoints that were resolved with a specific state, i.e., Blocked, Scanning, etc.



Search Tools

High Activity Mode

During periods of high activity, CounterACT stops displaying new endpoints scanning your network. This gives higher priority to the display of offensive endpoints. The threshold for switching to the High Activity mode is when 5000 malicious endpoints are being handled simultaneously.

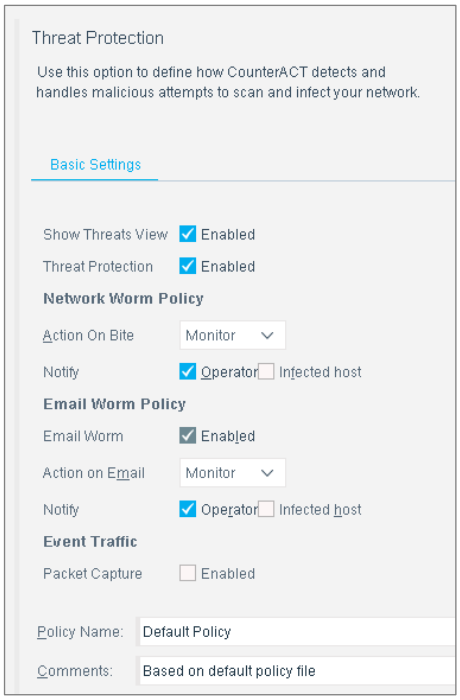
After this threshold has passed, new scanning endpoints are monitored but are not displayed. If, however, the scanning endpoint performs a bite event, it is displayed in the Console. During high activity periods, the status bar on the Console reads High Activity Mode.

Viewing and Updating the Policy

You can view or update the currently applied policy.

To view or update the current policy:

1. Select **Options** from the **Tools** menu and then select **Threat Protection**.



Threat Protection Pane – Basic Settings Tab

2. Update the policy definitions as required.

Threat Protection

Item	Description
Threat Protection	Select **Enabled** to activate the Threat Protection policy features in CounterACT. These features let you define how CounterACT handles hosts that attempt to attack or infect your network. Threat Protection may not be suited to all environments, such as those with asymmetric traffic. ***In such environments, if left enabled, these features will not work properly and endpoints may be mistakenly blocked***. In such a case you may want to disable Threat Protection. Disabling Threat Protection means that the Threats policy templates and all configurations defined in **Options>Threat**

Item	Description
	Protection, including all of the following child directories will not work: ▪ Legitimate Scan ▪ Legitimate Email Servers ▪ Manual Set State ▪ Advanced Although these configuration options will still be accessible and configurable from the Console, they are functionally disabled. Any changes made to these options in the Console will not take effect until Threat Protection is enabled. Threat Protection is already automatically disabled when your system is working in Partial Enforcement mode. If you are working in Full Enforcement mode, you can choose to selectively disable Threat Protection while continuing to enable all other CounterACT functionality. Refer to the section about Enforcement Mode in this document for more information.

Network Worm Policy

Item	Description
Action On Bite	Choose one of the following responses to a bite: ▪ Monitor: the endpoint is permitted to communicate with your network. CounterACT records the activity of the endpoint and sends marks to it. ▪ Port Block: The endpoint is prevented from establishing communication in the service it attempted to infect for a specified time period. You can escalate the Port Block policy to the Host Block policy. When escalated, the endpoint is prevented from communicating with the entire network, rather than the service it attempted to infect. By default, the Port Block policy is automatically escalated to the Host Block after the endpoint attempts to infect three separate services, that is, when the third service is bitten. You can change this default. ▪ Host Block: The endpoint is prevented from establishing communication with the network for a specified time period. The default block or monitor period for infected endpoints is 12 hours. If the endpoint performs another scan or uses any system mark during this time, the blocking or monitoring period is extended. This means, for example, that if the endpoint is blocked and after two hours uses a system mark again, the 12-hour block period is restarted, and the total block time is 14 hours. The block or monitor expiration time for each malicious endpoint can be seen in Detections pane in the Expires In column.
Notify	Select **Operator** to send email notification regarding bite detections. Addresses that receive email are defined during installation, but can be changed. See Chapter 15: Managing Appliances, Enterprise Managers and Consoles for information about updating addresses. See Managing Threat Protection Mail Alert Deliveries for information about additional email customization options.

Item	Description
	Select **Infected host** to send a Net Send message informing of infected endpoints running under the Windows platform. The message alerts the user that the machine is infected. See Customizing Email Worm Settings for information about changing the default and customizing the message sent.

Email Worm Policy

Item	Description
Email Worm	Select **Enabled** for CounterACT to detect and respond to email worm infections.
Action on Email	Choose to either block or monitor the endpoint when an email infection is detected.
Notify	Select **Operator** to send email notification regarding the email infection detection. Addresses that receive email are defined during installation, but can be changed. See Chapter 15: Managing Appliances, Enterprise Managers and Consoles for information about updating addresses. Select **Infected host** to send a Net Send message the infected endpoint running under Windows platforms. The message alerts network users that their machine may be infected. See Customizing Email Worm Settings for information about changing the default and customizing the message text.

Event Traffic

Item	Description
Packet Capture	Select **Enabled** for CounterACT to display the packets that were transferred between a malicious host and the network in the Traffic dialog box. Enabling Packet Capture may affect CounterACT device performance.

3. Type a new name in the **Policy Name** field (if required) to maintain the previous policy, and save the update under a new name.
4. Type comments in the **Comments** field.
5. Select **Apply**. A confirmation dialog box opens.
6. Select **OK** to apply the policy changes.

Blocking 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 Plugins. Refer to the relevant plugin configuration guide for more information.

By using a policy rule, you can also 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.

Customizing Basic Policy Settings

Advanced policy tools allow you to customize how CounterACT 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 various types of infection methods used. For example, 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.

Customizing 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 allow you to customize these values for specific scan types and scan methods.

Customizing Parameters for Each Scan Type

The system handles the following scan types:

- Finger
- HTTP
- Login
- NetBIOS (disabled by default)
- Port
- SNMP

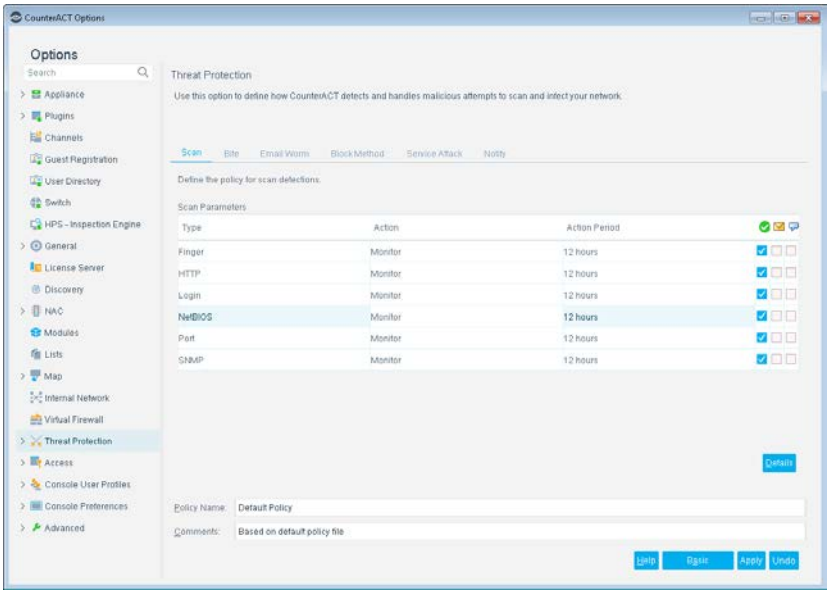
You can customize the following parameters for each scan type:

- Scan method
- Update the monitor or block response to probing endpoints
- Update the period that the probing endpoint is monitored or blocked
- Enable or disable the system's response to the scan event
- Enable or disable email notification per event type

To customize parameters for each scan type:

1. Select **Options** from the **Tools** menu and then select **Threat Protection**.

2. At the bottom of the Threat Protection pane, select **Customize** and then select the Scan tab.



Threat Protection Pane – Scan Tab

3. Double-click an **Action** field and select **Monitor** or **Host Block** scan type from the drop-down list.

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 CounterACT will block the spoofed address instead of the scanning endpoint address.

4. Double-click the value in the **Action Period** column to update the time period. Type a value or use the arrows to adjust the value. From the drop-down list, select a unit of time.
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 when it occurs.
6. Select the second checkbox [operator email] to send email notification for this type of scan event.
7. Select the third checkbox [infected endpoint notification] to deliver a Net Send message to the infected endpoint.
8. 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.
9. Select **Apply** to save your changes.
10. 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 Customizing Scan Recognition Criteria.

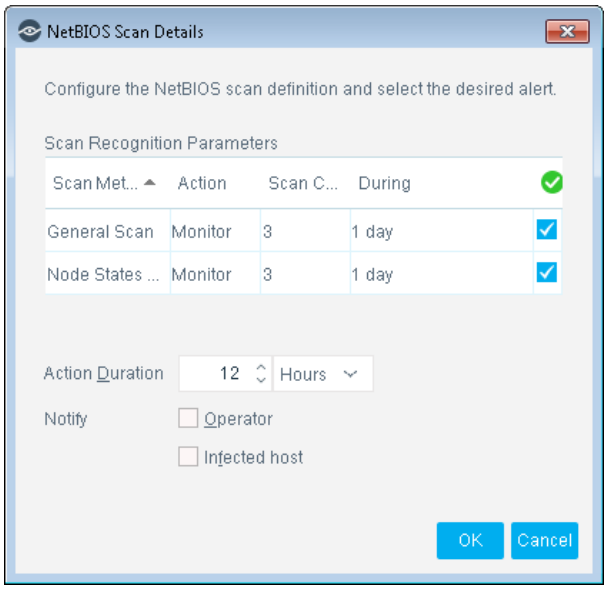
Customizing Scan Recognition Criteria

You can customize the scan recognition criteria for specific types of scan events. This means that for each scan type, you can define the number of probe events that must occur within a specified period in order 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 allow you to define different scan criteria for each scan method. For example, you can define that endpoints using the Login password method must 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 **Options** from the **Tools** menu 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.



Details Dialog Box, Finger Scan

4. Double-click the **Action** field to define how CounterACT 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 in order 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.

Scan Types and Related Methods

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

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. Type in a parameter or use the spin controls to adjust the parameter. Use the drop-down list to assign a unit of time.
9. Select the **Notify Operator** checkbox to send email notification to designated operators when the event occurs.
10. Select **Notify Infected host** to deliver a Net Send message to the infected endpoint.
11. Select **OK** to save changes and close the dialog box.

Customizing Bite Settings

Your system is installed with predefined bite values. These parameters determine how CounterACT responds to infected endpoints, i.e. block or monitor.

The advanced policy options let you customize bite parameters. This means that you can define that various types of bite events are handled differently. 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.

Options are also available to 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).

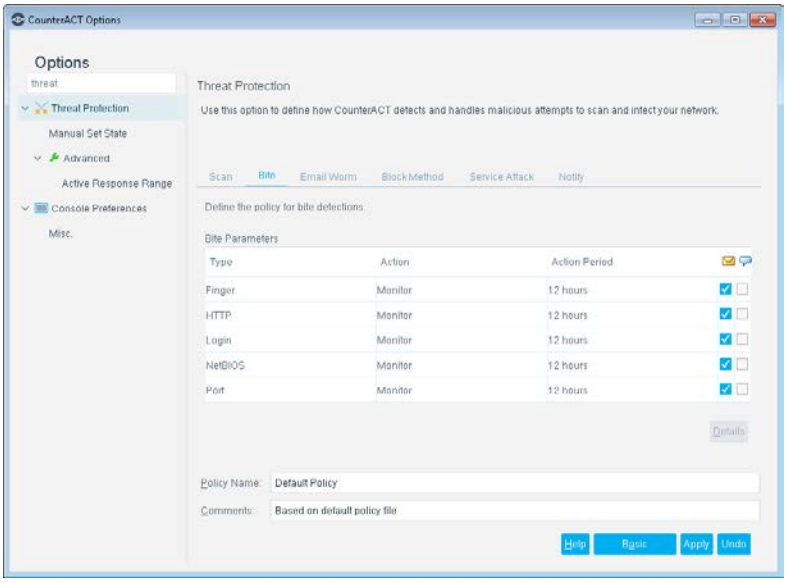
Customizing Block or Monitor Response to Each Bite Type

You can customize the following parameters for each bite type handled by CounterACT:

- The block or monitor response
- The period that the endpoint is blocked or monitored
- Enable or disable email notification for specific types of bite events

To customize bite parameters:

1. Select **Options** from the **Tools** menu and then select **Threat Protection**.
2. Select **Customize** and then select the Bite tab.



Threat Protection Pane – Bite Tab

3. Double-click the **Action** field for the required bite and select **Monitor**, **Port Block** or **Host Block** from the drop-down list. See Viewing and Updating the Policy for details.

If you update the action for a bite type to Port Block while the endpoint is currently being blocked from the network, the Port Block is postponed until the Host Block period is expired, and the endpoint performs another bite.

4. Double-click the value in the **Action Period** column to update the period in which the system blocks or monitors this bite type. Type a value or use the arrows to adjust the value. From the drop-down list, select a unit of time.
5. Select the first checkbox [operator email] to send email notification for this type of event.
6. Select the second checkbox [infected endpoint notification] to deliver a Net Send message to the infected endpoint.
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 block or monitor response for each bite type, based on the kind of bite mark used. For more information, see Customizing Bite Type Values.

Customizing Bite Type Values

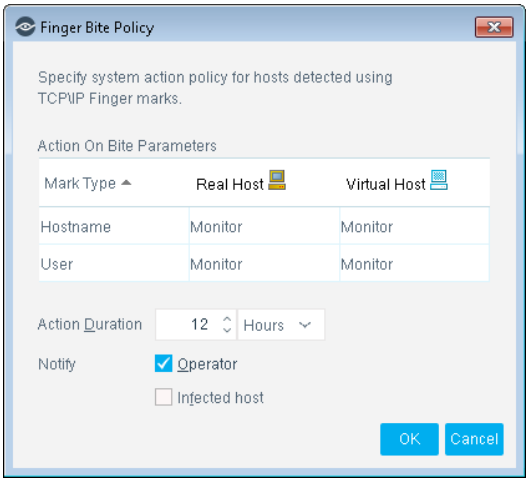
The system supports various marks for each bite type. For example, the NetBIOS bite method is an event in which a Hostname mark or Share mark was used. You can customize the block or monitor response for each type of mark, and customize the block or monitor response according to the endpoint that the infected endpoint

attempted to connect to (virtual or real). For example, you can define that you will block NetBIOS bites if they occur at real endpoints only.

*If the action is both blocked and monitored, the **Bite Type** field appears grayed out in the Bite tab.*

To customize bite type values:

1. Select **Options** from the **Tools** menu 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.



NetBIOS Bite Policy Dialog Box

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 list. See Viewing and Updating the Policy for these option details.
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. Type in a parameter or use the spin controls to adjust the parameter. Use the drop-down list to assign a unit of time.
6. Select the **Notify Operator** checkbox to send email notification to designated operators when the event occurs.
7. Select **Notify Infected host** to deliver a Net Send message to the infected endpoint.
8. Select **OK** to save changes and close the dialog box.

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 i.e. 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.

Customizing Email Worm Settings

CounterACT 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 certain number of emails within a specified time period. The default is ten 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:** **1.** Log in to the Enterprise Manager CLI. **2.** Submit 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 is mails with 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 ten 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 ten mails to ten servers within one minute.

See Customizing Email Anomaly Recognition Values for more information.

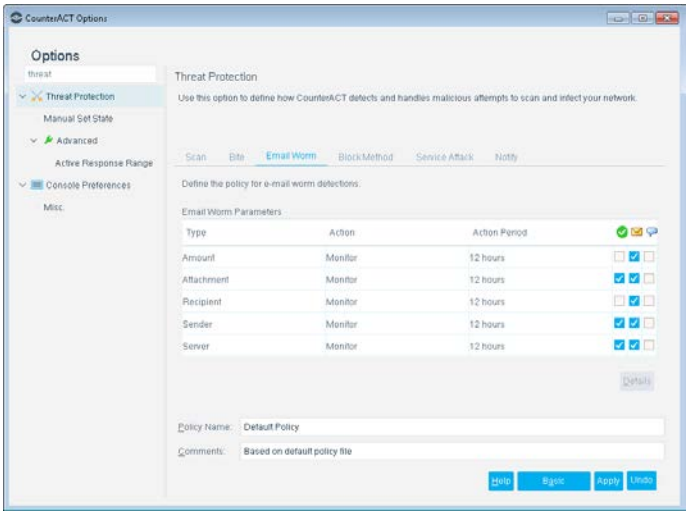
How Do I Know When an Email Worm Is Detected?

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 Chapter 10: Generating Reports and Logs for more information.

To customize email worm settings:

1. Select **Options** from the **Tools** menu and then select **Threat Protection**.
2. At the bottom of the Threat Protection pane, select **Customize** and then select the Email Worm tab.



Threat Protection Pane – 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 list.
4. Double-click the value in the **Action Period** column to update the time period. Type a value or use the arrows to adjust the value. From the drop-down list, select a unit of time.
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 when it occurs.
6. Select the second checkbox [operator email] to send email notification for this type of event.
7. Select the third checkbox [infected endpoint notification] to deliver a Net Send message to the infected endpoint.
8. 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.
9. Select **Apply** to save your changes.
10. Select **Basic** to return to the basic policy settings.

Alternatively, you can select **Details** to customize email anomaly recognition values. For more information, see Customizing Email Anomaly Recognition Values.

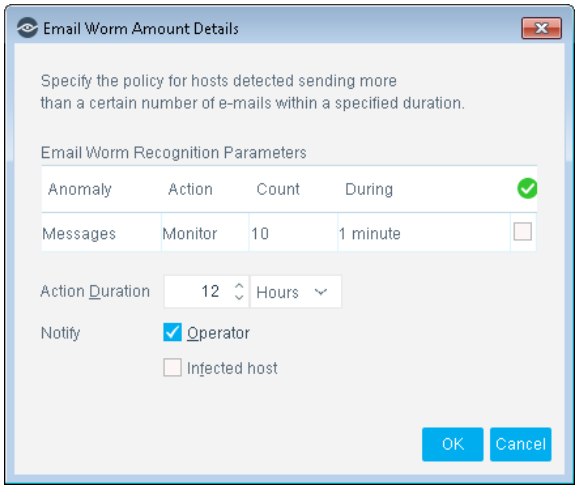
Customizing Email Anomaly Recognition Values

CounterACT 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 **Options** from the **Tools** menu 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**. The relevant Email Worm Details dialog box opens.



Email Worm Amount Details Dialog Box

4. Double-click the **Action** field for the anomaly and select **Monitor**, **Port Block** or **Host Block** from the drop-down list. See Viewing and Updating the Policy for an explanation of these options.
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** field to adjust the time interval in which the system blocks or monitors this anomaly type. Type in a parameter or use the spin controls to adjust the parameter. Use the drop-down list to assign a unit of time.
9. Select the **Notify Operator** checkbox to send email notification to designated operators when the event occurs.
10. Select **Notify Infected host** to deliver a Net Send message to the infected endpoint.
11. Select **OK** to save changes and close the dialog box.

Configuring the Block Method

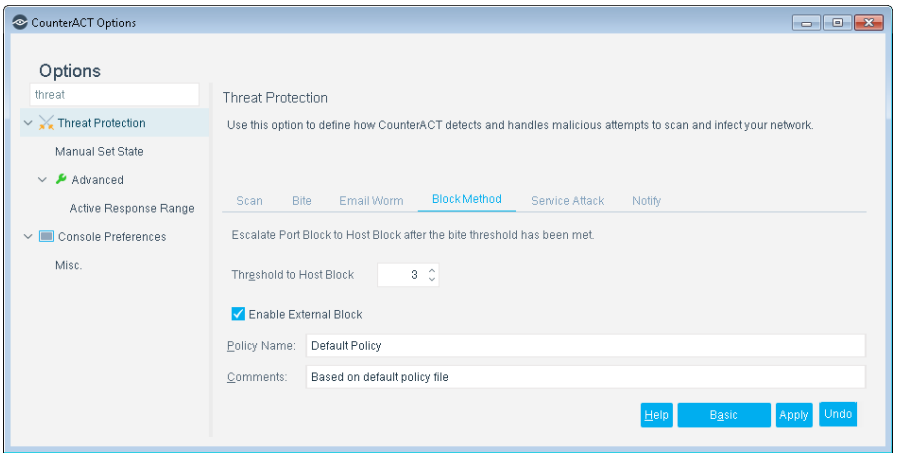
The following options are available to help you fine tune the CounterACT blocking mechanism:

- 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 **Options** from the **Tools** menu and then select **Threat Protection**.
2. At the bottom of the Threat Protection pane, select **Customize** and then select the Block Method tab.



Threat Protection Pane – 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 adjust this default.
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.

Handling Service Attacks

CounterACT identifies services attacks 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, however, can be adjusted to identify the attack after either fewer or more service-probing events occur.

About Monitoring and Blocking Service Attacks

CounterACT 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 – not just the traffic of the probing endpoint. After the time period has expired, CounterACT 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 – 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 when each service attack occurs.

Advanced Service Attack Features

Advanced service attack features allow you to adjust:

- Sensitivity threshold for identifying a service attack
- System response to the service attack at specific ports

For example, you can choose to monitor all TCP services but ignore FTP ports, or you can choose to block UDP services but only monitor SNMP ports. See Customizing Service Attack Criteria for more information.

Recommended Usage

Blocking services should be carried out carefully because when the service is blocked, no communication to the service is allowed for any endpoint, even if the endpoint is not malicious.

As a result, it is recommended to only monitor services.

UDP Blocking Prerequisites

To block endpoints at UDP services, you must configure your system to block with CounterACT and a firewall. Not all firewall products support service blocks. If your firewall does not support service blocks, you will 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.

Service Attack Indicator

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:

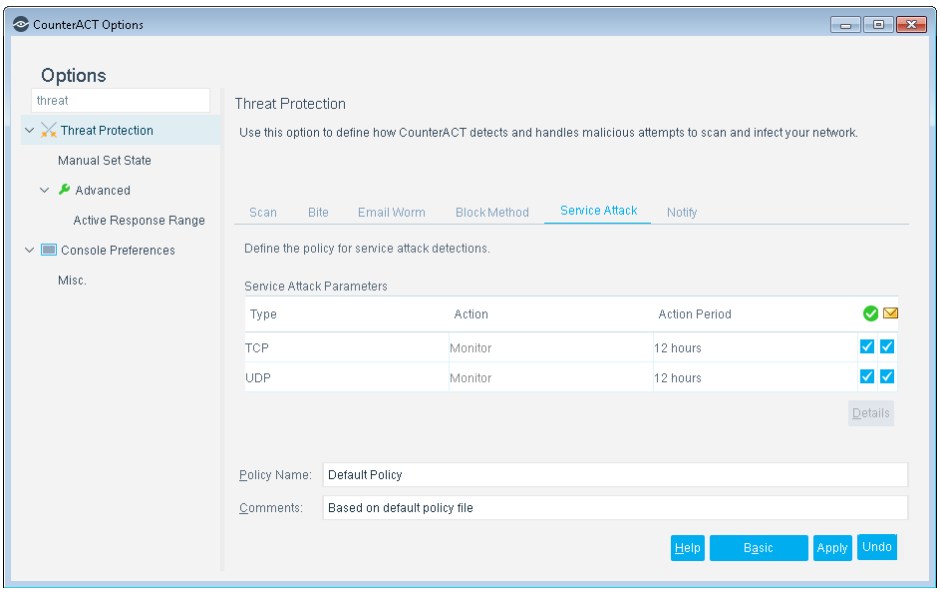
- Viewing the currently monitored and blocked services.
- Viewing a history of monitored and blocked services. See Viewing a History of Monitored and Blocked Services.
- Displaying a report with the number of UDP/TCP scans that occurred during a specific time period.
- Sending service attack traps to your management station. See Chapter 8: Base, Content and Extended Modules.

Setting the Service Attack Policy

This section describes how to set a service attack policy.

To set the service attack policy:

1. Select **Options** from the **Tools** menu and then select **Threat Protection**.
2. At the bottom of the Threat Protection pane, select **Customize** and then select the Service Attack tab.



Service Attack Tab

3. Double-click the **Action** field for TCP or UDP. From the drop-down list, select **Monitor** to record all traffic going to the selected service, or 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 Customizing Service Attack Criteria for details.
4. Double-click the value in the **Action Period** column to update the time period that the system blocks or monitors this type of service. Type a value or use the arrows to adjust the value. From the drop-down list, select a unit of time.

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 when it occurs. 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.

Alternatively, you can select **Details** to customize service attack parameters. For more information, see Customizing Service Attack Criteria.

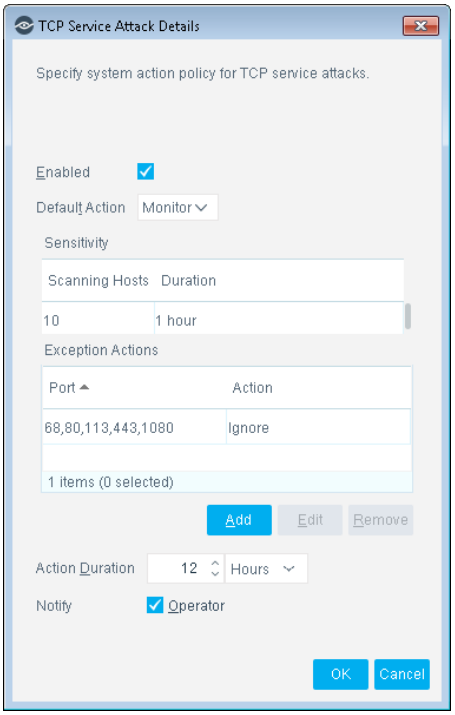
Customizing Service Attack Criteria

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 **Options** from the **Tools** menu 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.



Service Attack Details Dialog Box

4. Select **Enabled** to enable system response to the event. Clear the checkbox for the system to ignore the event when it occurs. If the checkbox is cleared, service attacks will not be monitored or blocked (recommended).
5. From the **Default Action** drop-down list, 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.

   CounterACT 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 the Scanning Hosts field to adjust the number of endpoints to be detected at a service. Type in a parameter or use the spin controls to adjust the parameter.
   – Double-click 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 list. To add actions for specific ports, see Customizing the Service Attack Response at Specific Ports.
8. Update the **Action Duration** field 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. Type in a parameter or use the spin controls to adjust the parameter. Use the drop-down list to assign a unit of time.
9. Select the **Notify Operator** checkbox to send email notification to designated operators when the event occurs.
10. Select **OK** to save changes and close the dialog box.

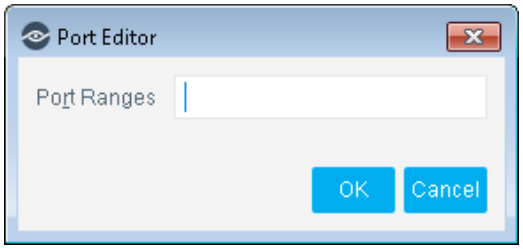
Customizing the Service Attack Response at Specific Ports

The **Exception Actions** section allows you to customize the system response to service attacks at specific ports.

For example, if you chose 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:

1. In the **Exception Actions** section of the relevant Service Attack Details dialog box, select **Add**. The Port Editor dialog box opens.



Port Editor Dialog Box

2. Type the port numbers required. Use a hyphen to indicate port ranges. Ports and ranges must be comma-separated.
3. Select **OK**. The Service Details dialog box is updated with the port numbers that you added.
4. Click the action field for the related port and choose an action response from the drop-down list that opens. The following options are available:

Monitor	Records all endpoint activity with the selected port.
Block	Prevents all endpoints from establishing communication with the port.
Ignore	Does not block or monitor traffic.

5. Select **OK**.

To edit the service attack exceptions:

1. Select the port that you want to edit from the **Exception Actions** section.
2. Select **Edit**. The Port Editor dialog box opens.
3. Edit the ports as required and select **OK**.

To remove service attack exceptions:

1. Select a port entry to remove from the **Exception Actions** section.
2. Select **Remove** and then select **OK**.

Removing 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.

CounterACT 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 from the Detections pane.
2. Right-click and select **Remove** and then **Apply**.

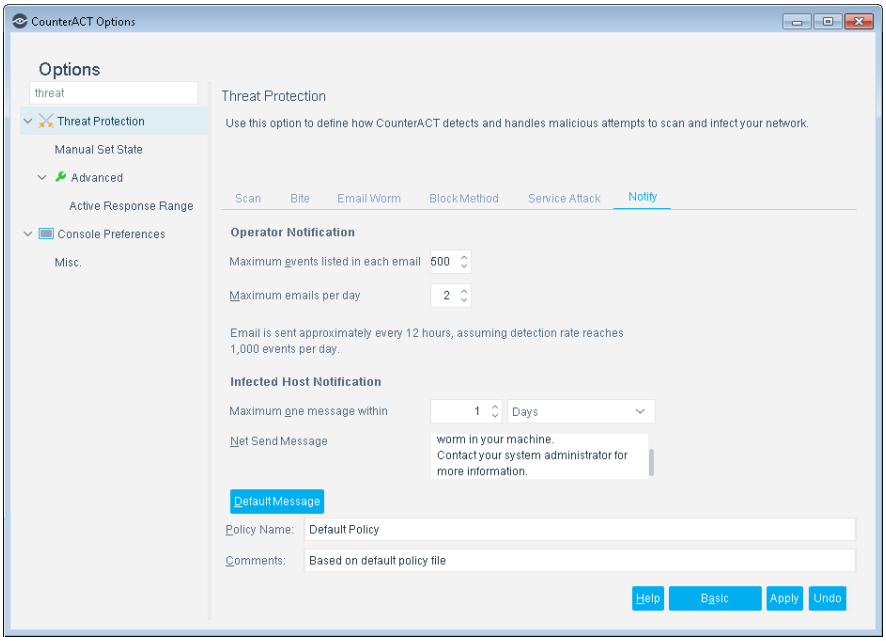
Managing Threat Protection Mail Alert Deliveries

CounterACT delivers two types of infection alerts:

- Infection alerts sent to the operator: CounterACT sends an email notification to specified email addresses regarding bite detections in the network.
- Infection alerts sent to the infected endpoint: CounterACT sends a Net Send message to the infected endpoint.

To access email deliveries:

1. Select **Options** from the **Tools** menu and then select **Threat Protection**.
2. At the bottom of the Threat Protection pane, select **Customize** and then select the Notify tab.



Threat Protection Pane, Notify Tab

Operator Notification

CounterACT 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.

Default Settings

By default up to 100 mails are sent within 24 hours. This means, for example, that 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 occurred 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 that 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.

Information about these events is viewable 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. Type a value in the **Maximum events listed in each email** field or use the spin controls to adjust the value.
2. Type a value in the **Maximum emails per day** field or use the spin controls to adjust the value. According to the values that you set here, the system calculates how often you receive mail, provided an event occurs.
3. To receive an email alert each time an event occurs, enter the value **1** in the **Maximum emails per day** field.
4. Configure Infected Host Notification settings. See Infected Host Notification Section.

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.

Infected Host Notification Section

CounterACT sends a Net Send message to an infected endpoint running under the Windows platform. By default, only one message is sent per day, but you can update this value. The message indicates that the endpoint is infected and the users should contact their system administrator. The message can be modified.

To manage infected endpoint Net Send deliveries:

1. In the **Maximum one message within** field, define the maximum number of messages to be sent to infected endpoints with a specified time period.
2. Update the **Net Send Message** as required.
3. Select **Apply** to save your changes.

Additional Email Options

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 that you receive regarding endpoint and service events include a summary of events. This information is displayed in a format that can be easily used for parsing by external applications. See Parsing Event Information Displayed in Email Alerts for more information.

Working with Manually Added Endpoints

Manual endpoints are endpoints that you manually enter into your system. This means that you can enter 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 state that you enter. 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 that you set 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 that were 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.

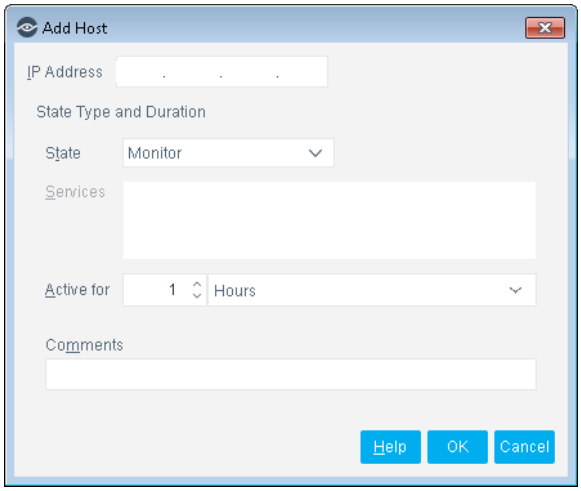
You cannot manually update an endpoint to the Port Block state.

Manually Adding an Endpoint

You can manually enter an endpoint into your system. Use this feature if you already know the IP address of an endpoint, and know that you want to either ignore, monitor or block endpoint activities for a specified period of time. After the period that you indicate expires, the endpoint is handled according to the current system policy.

To add an endpoint to the system:

1. Select **Options** from the **Tools** menu and then select **Threat Protection** > **Manual Set State**.
2. Select **Add**. The Add Host dialog box opens.



Add Host Dialog Box

3. Type the endpoint **IP Address**.
4. From the **State** drop-down list select the appropriate 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. See Advanced Policy Options for more information.

5. In the **Active for** area, use the spin controls and drop-down list to select the length of time that 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 or **Cancel** to close the dialog box without applying the changes.

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 the length of time that the system maintains that state. These tasks are performed from the Current Added Hosts dialog box. The list is updated each time that you open the dialog box.

To view manually added endpoints:

1. Select **Options** from the **Tools** menu 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	Indicates the ports at which the endpoint is blocked.
From / Until	The length of time that the endpoint is in the state.
Issued By	Name of the user that manually added the endpoint.
Comments	Related comments.
CounterACT Appliance	The Appliance that received the command.

3. Select **OK**.

To modify the manually added endpoint definitions:

1. Select an endpoint.
2. Select **Edit**. The Set State for <IP_address> dialog box opens.
3. Update the manual endpoint parameters.
4. Select **OK**.

To remove a manually added endpoint:

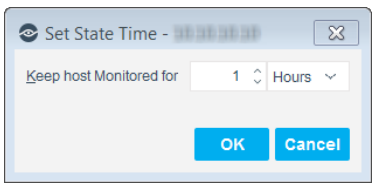
1. Select an endpoint.
2. Select **Remove**. A confirmation dialog box opens.
3. Select **Yes**. The endpoint is removed from the list of manually added endpoints. The system now responds to the endpoint activity according to the current policy definitions.

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 from the Detections pane.
3. Select **Threat Protection** and then **Set State Time**. The Set State Time for <IP_address> dialog box opens.

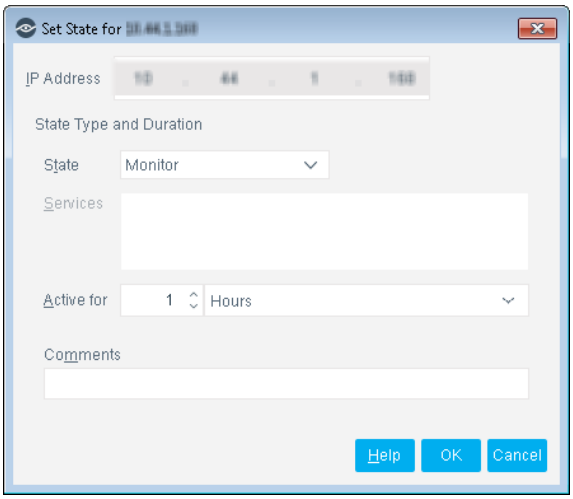


4. Type a value or use the spin controls to adjust the value. Use the drop-down list to assign a unit of time.
5. Select **OK**.

Changing the Host State

You can change the endpoint state. The endpoint expiration time remains the same.

1. Select an endpoint from the Detections pane.
2. Right-click and select **Set Threat Protection State**. The Set State for <IP_address> dialog box opens.



Set State Dialog Box

3. Update the endpoint parameters.
4. Select **OK**.

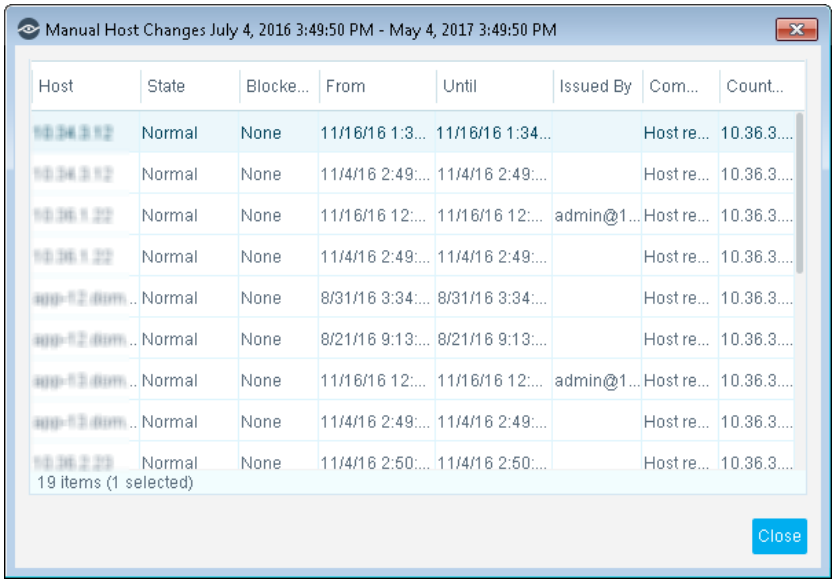
Viewing a History of Manually Added Endpoints and Manual Changes

You can view a list of manually added endpoints and endpoints whose states or times were manually changed.

To view the history manual list:

1. Select **Options** from the **Tools** menu and then select **Threat Protection** > **Manual Set State**.
2. Select **History**. The Time Period dialog box opens.
3. Select 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.



Manual Host Changes Dialog Box

Defining the Active Response Range

By default, the entire Internal Network is protected by CounterACT Active Response technology. Use this procedure to change this range. For example, you may want to limit Active Response protection to core operational segments of your network.

Segments you place in the Active Response range must be included in the Internal Network.

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 CounterACT that support your Active Response range configuration. See Working with CounterACT Segments.
2. Select **Options** from the **Tools** menu 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 Configuring Features for an Appliance or Group of Appliances.
5. Do one of the following:
   – Select **Segments**.
     In the Segment selection dialog, select or clear checkboxes to include or remove segments.
     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.

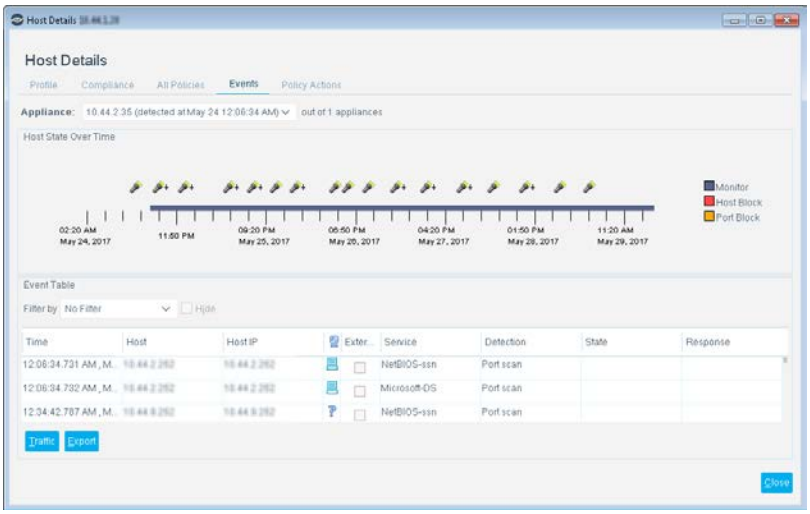
Changes made to the Active Response range must be supported by your network architecture. Specifically, addresses included the Active Response range defined for an Appliance must be visible to the Appliance.

Viewing Endpoint Activity Details

You can view comprehensive details regarding activities carried out by endpoints.

To view endpoint details:

1. In the Threats view, double-click a malicious endpoint from the Detections pane. The Host Details dialog box opens. The endpoint's address is displayed in the title bar. The Events tab displays the date and time of the first event.



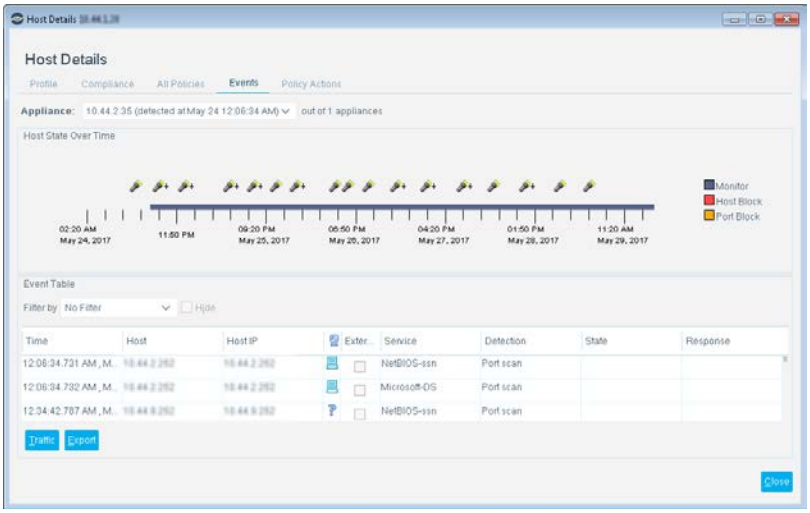
Host Details Dialog Box

General information as well as detailed event information about the event can be viewed. For example, you can review specifics about packets that were transferred during the session.

In addition, you can view information about the endpoint in the Assets Portal by selecting **Show full host details**. See Chapter 9: Assets Portal for more information about the portal.

Events Tab

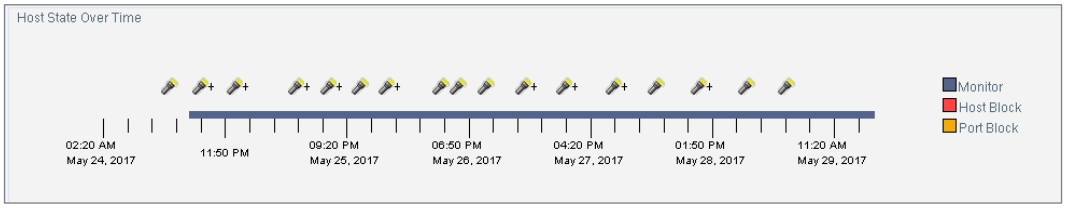
The Events tab displays a graphic time-line summary of the source state for the period that the source is active. In addition, the tab includes an Event table, which provides extensive, real-time information about the source events and responses to those events.



Source Details Dialog Box, Events Tab

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 states 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 mouse to view tooltip information about the scan or bite events detected.



Source Time-Line

Event Table

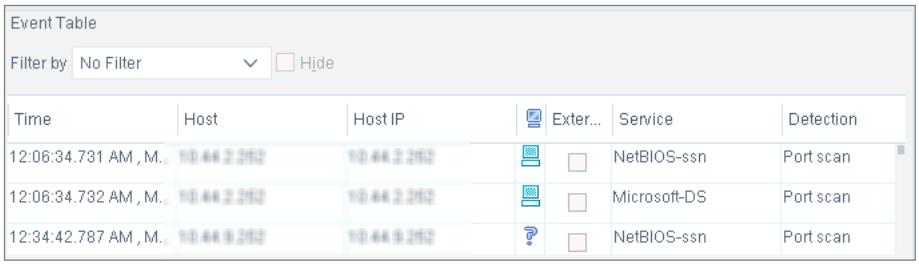
The Event Table provides extensive, real-time information about source events and CounterACT activity that occurs while the source is active. An event is defined as any attempt to access an endpoint on the network.

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 CounterACT 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 CounterACT activity.

Additional tasks can be carried out from the Event Table, including:

- Filtering the Information Displayed in the Event Table
- Adding Legitimate Traffic Rules from the Event Table
- Viewing a Summary of Event Details
- Viewing Event Traffic

Default columns appear with basic information about sources and related source activity. Additional information can be displayed by adding other columns.



Events Tab, Event Table

Source Activity

The following table details source activity for the selected event.

Item	Description
Time	The time and date the event occurred.
	Indicates that the source address is verified. Indicates that the source address is unverified (may be 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.

CounterACT Activity

The following table details activity for the selected event.

Item	Description
Detection	Indicates the event detected, i.e. NetBIOS scan or infection attempt.
Response	Indicates the response to the detection. Options include: ▪ **Block**: CounterACT does not allow packets from the source to go through to the specified destination (host + service). ▪ **Stall**: CounterACT simulates a virtual service for an infected source. This occurs when the policy is not set to block infected sources. ▪ **Mark**: CounterACT distributes a mark to the source.
Resulting State	Displays the new source state after detection and response.

Item	Description
Returned Data	Displays the data sent to the source from CounterACT. For example, if CounterACT 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 that you open the Console.

The following filter options are available:

Detections	Events that caused CounterACT to either change the current source state or extend the source state.
Detections and Marks	Events that caused CounterACT 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 that were targeted at the same host as an endpoint that you select in the table.
Same Service	Events that were targeted in the same service as a service that you select in the table.

To filter the table:

1. Select a filter type from the **Filter by** drop-down list located in the Event table.
2. Select the **Hide** checkbox to hide the event types that you selected, or clear the checkbox to display those events only.

Adding 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:

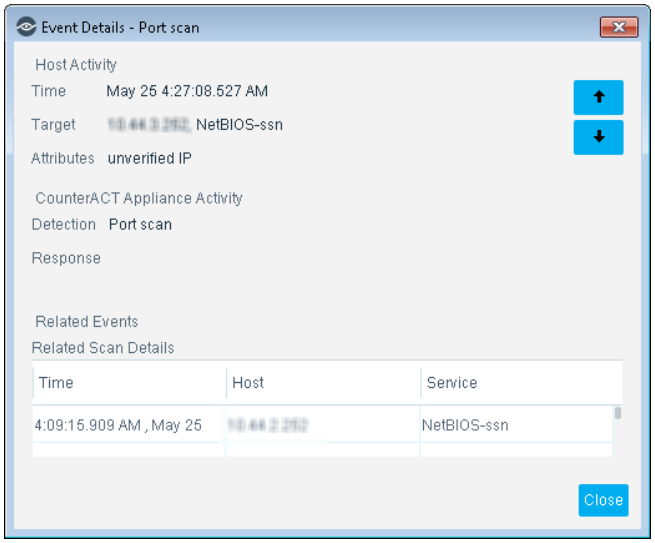
1. Right-click an event in the Event table and select **Legitimize Traffic**. The Add Custom Rule dialog box opens.
2. The currently selected source is displayed in the **Source** section. The targeted host and service selected in the Events table are also included in the Legitimate Traffic rule.
3. Edit the rule if required.
4. Select **OK**.

Viewing 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 selected a scan event, the probes that were included in the scan are listed.

To view a summary:

1. Double-click an entry in the Event Table or right-click an entry and select **Details**. The Event Details dialog box opens for the selected event.



Event Details Dialog Box

The following information is available:

Item	Description
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.

Scrolling to Addition Event Summaries

The Event Details Dialog box can be automatically updated to display information about other sources in the Event table.

To display information about additional events:

1. Click a scroll arrow from the **Host Activity** section.

Viewing Event Traffic

You can display information about the packets that were transferred between the host and the network.

To view event traffic for the selected source:

1. Select an event from the Event table.
2. Select **Traffic**. The traffic dialog box opens.

An option for hiding and showing table columns is available from this tab.

Session List Section

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

This section provides information about each packet.

	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.

Viewing and Saving Packet Data from the Packet Data Section

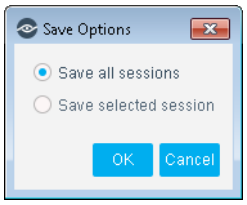
This section allows you to display and save the packet data of source sessions.

To display packet data:

1. Select an entry from the Packet List. This section displays the raw packet data.

To save packet data:

1. Select the session that you want from the Traffic tab. To save all sessions, do not select any sessions.
2. Select **Save**. The Save Options dialog box opens.



Save Options Dialog Box

3. Select an option and then select **OK**. A Save As dialog box opens enabling you to save the information in a selected directory.

If the source that you selected is still active, a message opens indicating that the source is still active and that you are not saving all the source sessions.

Managing 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.

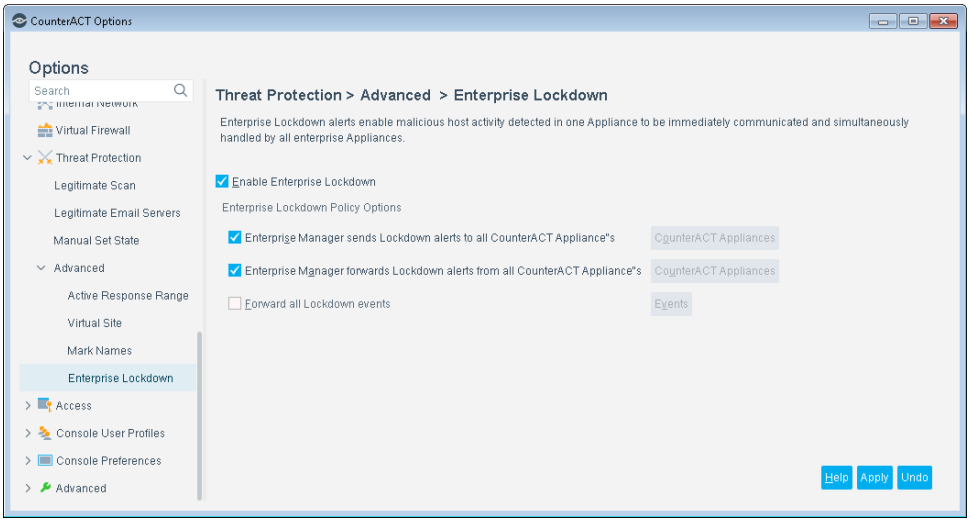
This means that if one Appliance in your enterprise has detected a bite event, a lockdown alert is sent to the other Appliances, alerting them of the source that performed the event. If the other Appliances detect that a source is communicating with the network that they are protecting, the source is 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 choose to 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 **Options** from the **Tools** menu and then select **Threat Protection** > **Advanced** > **Enterprise Lockdown**.



Enterprise Lockdown Dialog Box

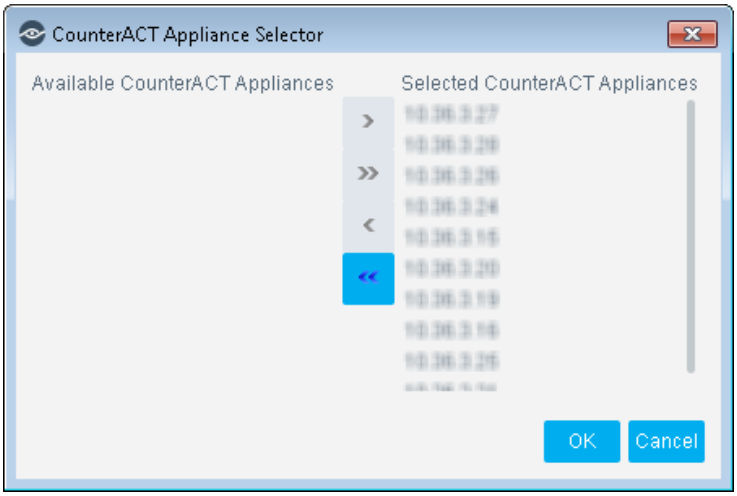
2. Select **Enable Enterprise Lockdown** to activate the lockdown policy.
3. Define a lockdown policy.

Enterprise Manager sends Lockdown alerts to all CounterACT 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 CounterACT 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 Lockdown events	▪ When selected, all bite event types are included in lockdown. ▪ Clear the checkbox to select specific types of bite events that are included in the lockdown alert.

4. Select **Apply**.

To send events to specific Appliances:

1. Clear one of the first two Enterprise Policy Lockdown options.
2. Select **CounterACT Appliances**. The CounterACT Appliance Selector dialog box opens.

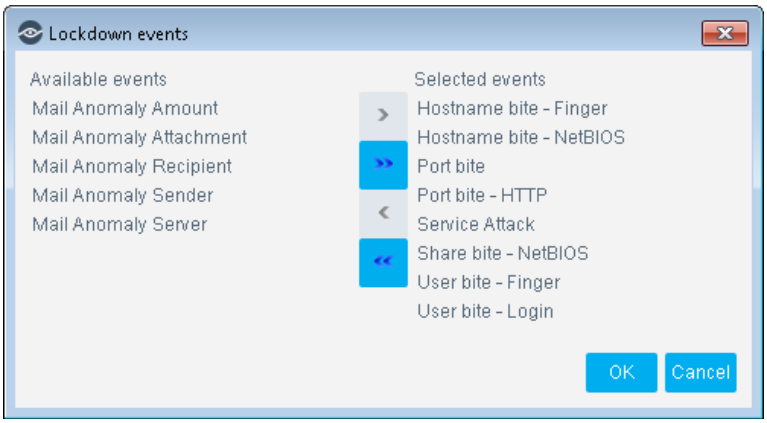


Appliance Selector Dialog Box

3. Select Appliances from **Available CounterACT Appliances** and use the arrow buttons to assign them to **Selected CounterACT Appliances**.

To customize the Forward All Lockdown Events policy:

1. Clear **Forward all Lockdown events**.
2. Select **Events**. The Lockdown events dialog box opens.



Lockdown Events Dialog Box

3. Select events from **Available events** and use the arrow buttons to assign them to **Selected events**.
4. Select **OK**.

Legitimate Traffic

This section describes the options available when working with legitimate traffic options.

The following options are available:

- Handling Legitimate Activity of Malicious Sources

- Defining Legitimate Traffic
- Automatically Defining Legitimate Scanning Activity – Wizard
- Manually Defining Legitimate Scanning Applications
- Manually Defining Removed Servers
- Creating Customized Legitimate Traffic
- Editing and Removing Legitimate Traffic

Handling Legitimate Activity of 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 will not be counted in the probe count by CounterACT when attempting to probe defined services or host.

Refer to Basic Terminology in Chapter 12: Threat Protection for more information about probing sources.

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 CounterACT 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.

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 Customizing Scan Recognition Criteria for information 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:

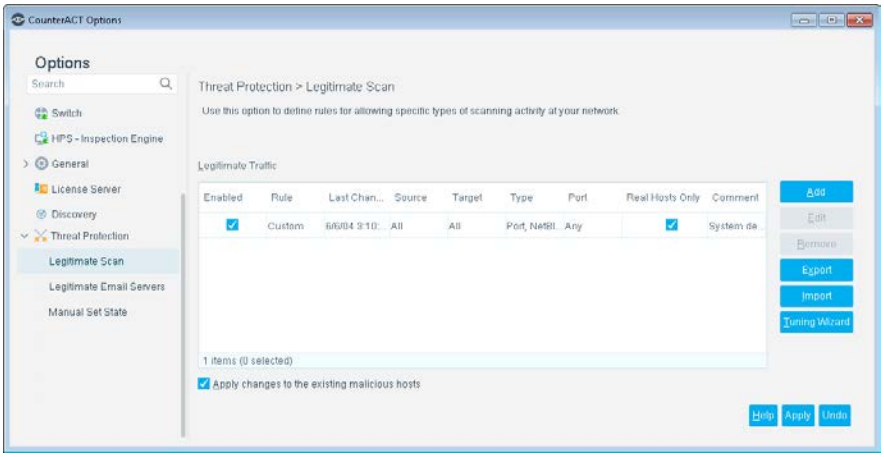
- The manual ignore feature is limited to a certain time, while the Legitimate Traffic rule is enabled until you disable it.
- The manual ignore feature does not allow you to customize specific endpoints or ports in which to ignore the source.
- The manual ignore feature allows you to ignore the source 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.

Defining Legitimate Traffic

Legitimate Traffic is defined and managed from the Legitimate Traffic dialog box. Use the dialog box to add, edit and remove rules, as well as to filter information in the dialog box about the rules that you already defined. A feature is also available to import and export Legitimate Traffic rules.

To open the Legitimate Scan Rules dialog box:

1. Select **Options** from the **Tools** menu and then select **Threat Protection** > **Legitimate Scan**.



Legitimate Traffic List

The following information is available:

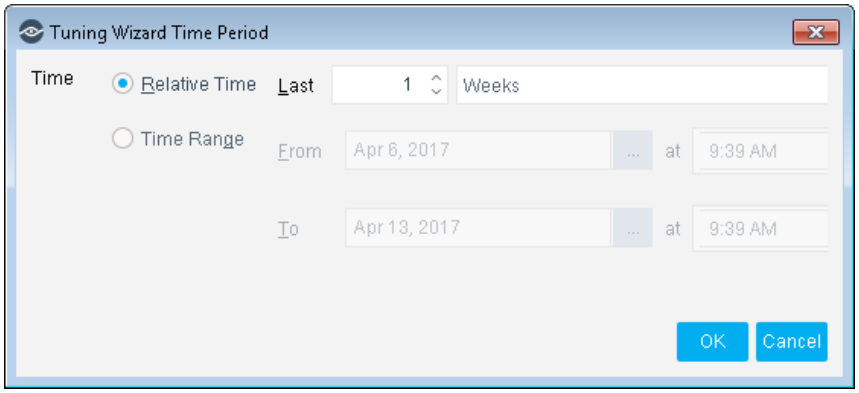
Enabled	Indicates that the rule is enabled.
Rule	Several types of rules can be created. For example, custom design rules, known scanning application rules or removed server rules. This column details the rule type created.
Last Change	The date the rule was most recently modified.
Source	The source addresses 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 chapter.

Automatically Defining 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 are still probed by network users. Use the wizard to define these applications or servers as sources of legitimate traffic. The Legitimate Traffics wizard automatically identifies most of the rules required, however fine-tuning may be required and can be done by adding custom rules.

To define Legitimate Traffic rules:

1. From the Legitimate Scan pane, select **Tuning Wizard**. The Tuning Wizard Time Period dialog box opens.



Tuning Wizard Time Period Dialog Box

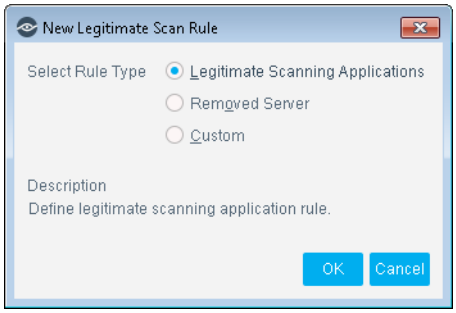
2. Select a time period by doing one of the following:
   - Select **Relative Time** and then specify the required number of hours, days, weeks or months by using the spin controls or by typing a value in the field. Select a time unit from the drop-down list.
   - Select **Time Range** and then specify the beginning and end of the time range.
3. Select **OK**. If results were 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 that should be allowed to scan your network.
6. Select **Next**. The Removed Servers dialog box opens listing removed servers that are still being probed by network sources, but cannot be reached. This may be, for example, because the server is uninstalled or because the server is no longer in use. CounterACT may unnecessarily block sources detected at these locations. Activity should be allowed at such servers. The ten 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 servers that should be open for scanning activity.
8. Select **Next**. The Finish dialog box opens. The applications or servers that you 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 from the wizard.
10. Select **Apply** to accept the rules.

Manually Defining Legitimate Scanning Applications

You can manually define specific legitimate scanning applications from which CounterACT ignores scanning activity.

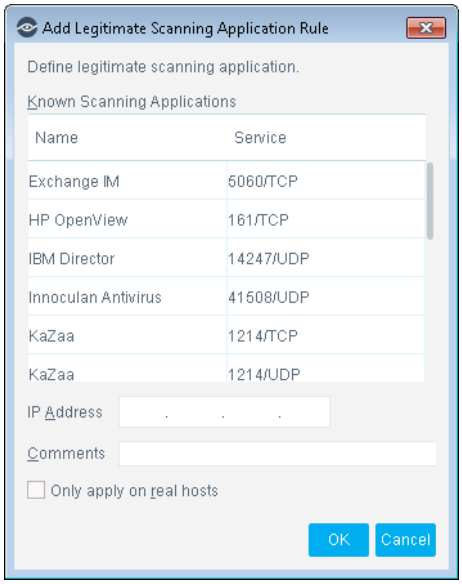
To manually define Legitimate Scan Rules:

1. Select **Options** from the **Tools** menu and then select **Threat Protection** > **Legitimate Scan**.
2. From the Legitimate Scan pane, select **Add**. The New Legitimate Scan Rule dialog box opens.



New Legitimate Traffic Dialog Box

3. Select **Legitimate Scanning Applications** and then select **OK**. The Add Legitimate Scanning Application Rule dialog box opens.



Add Legitimate Scanning Application Rule Dialog Box

The dialog displays the currently downloaded list of known legitimate scanning applications.

4. Select an application from the list.
5. In the **IP Address** field, enter the address at which the application is installed.
6. Use the **Comments** field as required.
7. Select **Only apply on real hosts** for all probes on real endpoints to be permitted by the application. This means a probe is considered legitimate only if the destination address was learned as a Real Host.

8. Select **OK**.

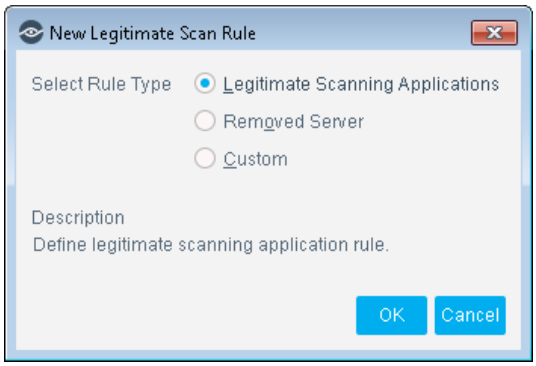
   If the application is installed at several locations, repeat the process for additional IP addresses.

Manually Defining Removed Servers

Removed servers are servers that network users have attempted to connect to, but cannot be reached. This may be, for example, because the server is uninstalled or because the server is no longer in use. CounterACT may unnecessarily block sources detected at these locations. Activity should be allowed at such servers.

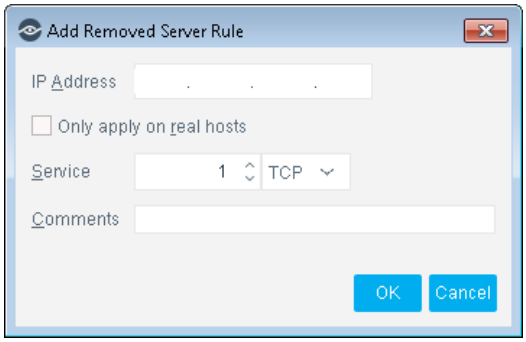
To manually define removed servers:

1. From the Legitimate Traffic List, select **Add**. The New Legitimate Scan Rule dialog box opens.



New Legitimate Scan Rule Dialog Box

2. Select **Removed Server** and then select **OK**. The Add Removed Server Rule dialog box opens.



Add Removed Server Rule Dialog Box

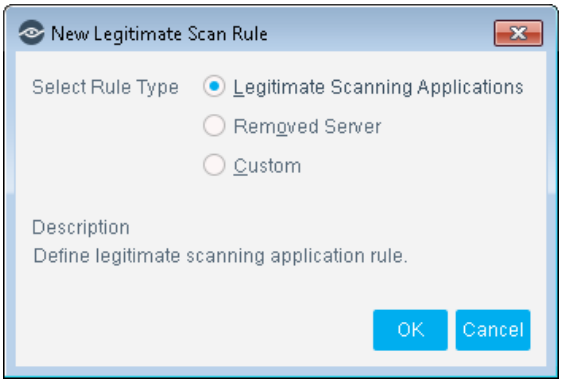
3. Type the IP address of the server in the **IP Address** field.
4. Select **Only apply on real hosts** to apply the rule to real endpoints only (and not virtual endpoints).
5. Define a service in the Service field.
6. Use the Comments field as required.
7. Select **OK**.

Creating Customized Legitimate Traffic

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.

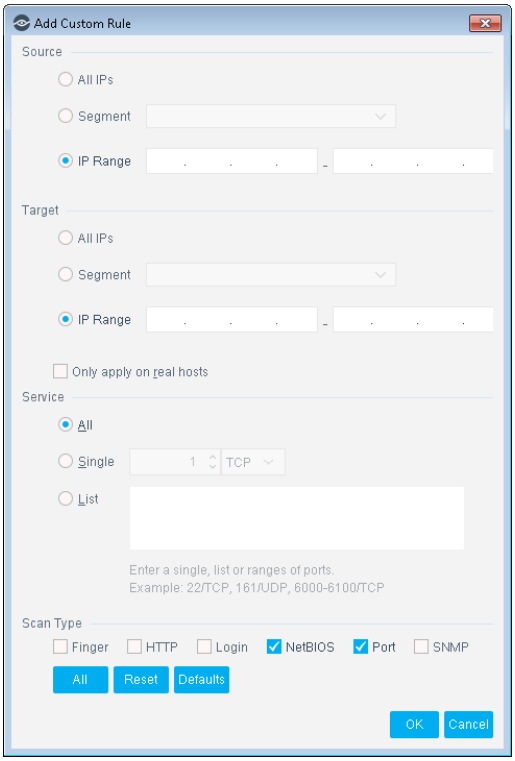
To create customized Legitimate Traffic rules:

1. From the Legitimate Traffic List, select **Add**. The New Legitimate Scan Rule dialog box opens.



New Legitimate Scan Rule Dialog Box

2. Select **Custom** and then select **OK**. The Add Custom Rule dialog box opens.



Add Custom Rule Dialog Box

Source and Target Sections

Define the direction traffic should be legitimatized – from which source to which target endpoints.

Services and Probe Type

Use the **Service** section to define the services at which traffic should be ignored.

1. In the Service section:
   - Select All to ignore traffic at all services.
   - Select Single to define a single service.
   - Select List to define a list of services. Enter services according to the format shown. For example, 22/TCP, 161/UDP.

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.

2. Use Probe Type to select which probe types are considered legitimate. For example, you can create a Legitimate Traffic rule in which only HTTP probes at port 80/TCP are legitimate.

Configurable probe types include: Finger, HTTP, Login, NetBIOS, Port and SNMP.

The default is NetBIOS and Port probe types on all ports.

3. Select **OK**.

Defining 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. CounterACT should allow this type of activity.

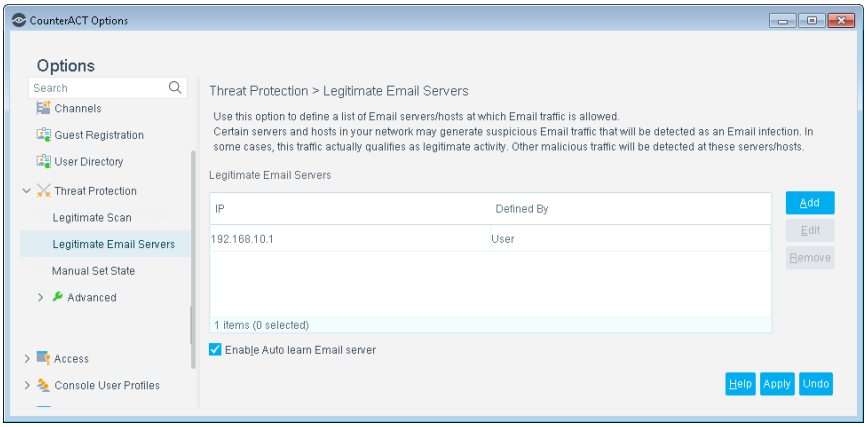
To do this, you can define a list of email servers and endpoints for which to allow email traffic. Other malicious traffic is detected at these servers and endpoints.

By default CounterACT 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 performing other Threat Protection activity, it is handled according to the block or monitor policy.

To define endpoints:

1. Select **Options** from the **Tools** menu and then select **Threat Protection** > **Legitimate Email Servers**.



Legitimate Email Servers Pane

2. Select **Add** and enter the IP address of the relevant endpoint in the Add dialog box.
3. 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 CounterACT or entered by a user.
4. Use **Remove** and **Edit** as required.
5. Verify that **Enable Auto learn Email server** is selected for CounterACT 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).

If there is no traffic at the server for a month, CounterACT will unlearn it.

6. Select **Apply**.

Creating 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:

1. Double-click an endpoint from the Detections pane.
2. Select the Events tab, and 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 other connected Appliances.

Editing and Removing Legitimate Traffic

Legitimate Traffic that is displayed in the Legitimate Traffic Manager can be removed and edited.

To remove a rule:

1. From the Legitimate Traffic List, select a rule and then select **Remove**.
2. Select **Apply**. The rule is removed from your system. Sources that were granted access are now handled according to the current policy.

To edit a rule:

1. From the Legitimate Traffic List, select a rule and then select **Edit**.
2. Edit the range as required.
3. Select **OK** and then select **Apply**.

Chapter 13: Threat Protection, Advanced Tools

- Defining Mark Naming Conventions
- Defining Virtual Site Endpoint Operating System Parameters
- Parsing Event Information Displayed in Email Alerts

Defining Mark Naming Conventions

CounterACT 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:

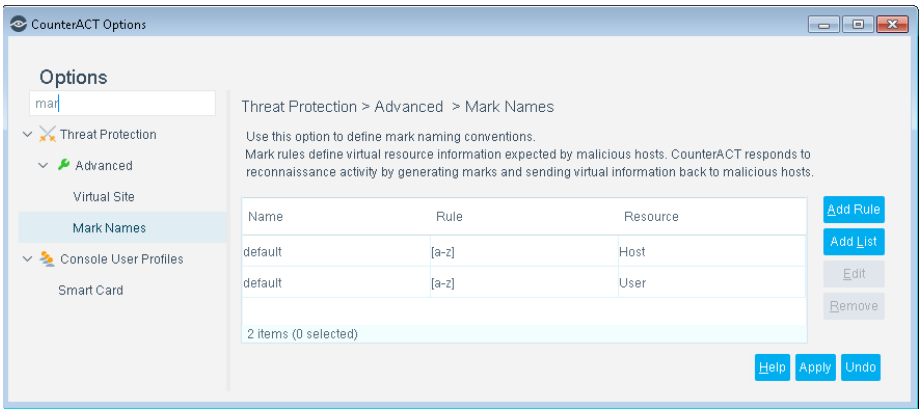
Create mark rules	Create mark rules that reflect the naming conventions used for host and user names in your network.
Create lists of names	Create lists of names similar to the host and user names used in your network.

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 – Permissions for information about granting and preventing access.

To open the Mark Names pane:

1. Select **Options** from the **Tools** menu and then select **Threat Protection** > **Advanced** > **Mark Names**.



Mark Names Pane

Defining Mark Rules

Endpoint and user names are often organized into logical segments, i.e., host names may always 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

In the previous examples:

- SC = the company name (Sample Company)
- WIN/LINX = the platform (Windows or Linux)
- 123/223 = a numeric sequence

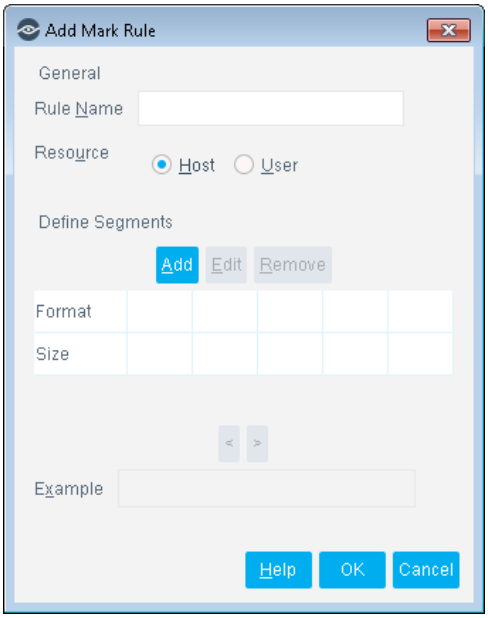
You can define the naming convention rules for the host and user resource names to use as marks for your system. The mark rules can contain several segments that reflect the naming conventions used in your networking/organizational environment.

Default Settings

CounterACT 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 that all host or user names are created according to a specific convention. This ensures that marks will appear consistently and realistically to probing endpoints.

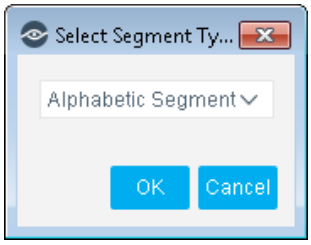
To define mark rules:

1. In the Mark Names pane, select **Add Rule**. The Add Mark Rule dialog box opens.



Add Mark Rule Dialog Box

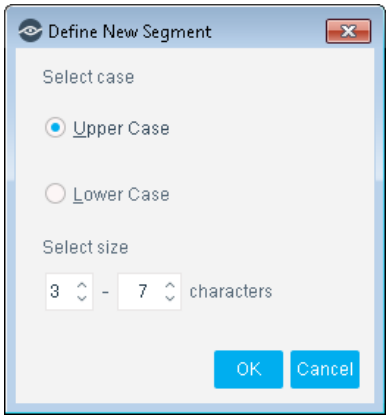
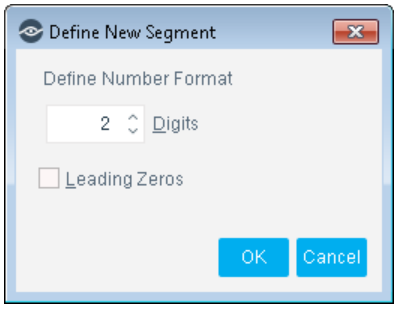
2. Type a rule name in the **Name** field.
3. Select **Host** or **User** to be applied to this resource type.
4. Select **Add** to create the rule segments. The **Select Segment Type** dialog box opens, allowing you to select a rule segment type.

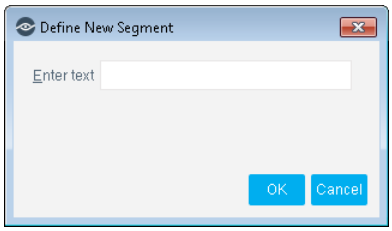


Select Segment Type Dialog Box

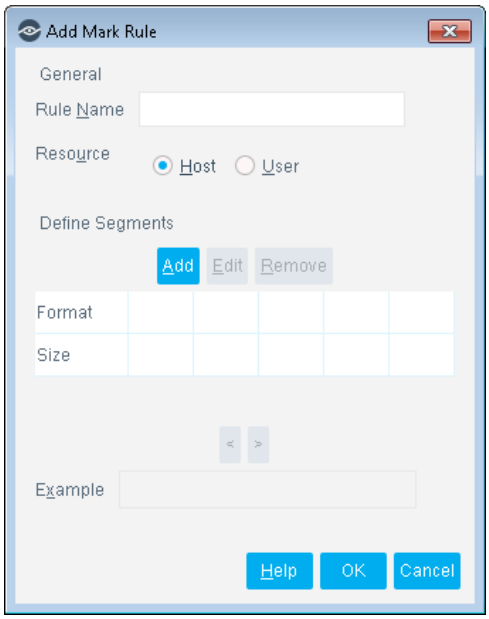
5. Select a segment type from the drop-down list and select **OK**.

   Three types of rule segments can be created:

Alphabetic Segment Define the rules for random text strings segments that appear in the resource name.  	**To define a string:** ▪ In the **Select case** section, select **Upper Case** or **Lower Case**. ▪ In the **Select size** section, use the spin controls to define 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, use the spin controls to define 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, etc. ▪ Select **Leading Zeros** to include leading zeros in the number. For example, 08, 003, 099, 023 ▪ Select **OK**.

Constant Segment Define a fixed string segments that will appear in the resource name.  	**To define a fixed 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.



Add Mark Rule Dialog Box

6. Use the arrow buttons to adjust the location of the segments, if necessary.

7. Select **OK**. The rule that you created is displayed in the Mark Names pane.

Editing and Removing Mark Segments

To edit a segment that you created:

1. From the Add Mark Rule dialog box, select the segment of the rule to edit from the Format and Size fields.
2. Select **Edit**. The Edit Segment dialog box opens.
3. Edit the segment as required and select **OK**.

   The segment is updated in the Add Mark Rule dialog box.

To remove a segment:

1. Select the segment of the rule to remove from the Format and Size fields.
2. Select **Remove** and then select **OK**.

Editing and Removing Mark Naming Rules

You can edit and remove mark-naming rules that you created for your system.

To edit the rules:

1. Select a rule to apply from the Mark Names pane.
2. Select **Edit** to open the corresponding Rule Editing dialog box.
3. Edit as required and select **OK**.

To remove a rule:

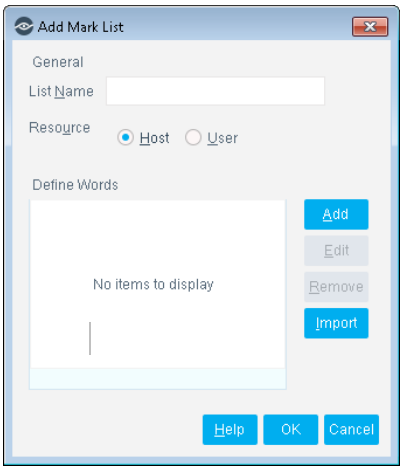
1. Select a rule to apply from the Mark Names pane.
2. Select **Remove** and then select **OK**.

Defining Lists

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. The Add Mark List dialog box opens.



Add Mark List Dialog Box

2. Type 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** section, 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 that you created is displayed as an entry in the Mark Names pane and you can apply the list to your system.

Applying Mark Naming Rules

After you have defined your naming rules, you can apply them to your system. You must apply all the rules that appear in the Mark Names pane. If you do not want to apply a rule, remove it.

To apply naming rules to your system:

1. Add rules as previously detailed.
2. Select **Apply**.
3. Edit the list or remove an item, as required.

Defining Virtual Site Endpoint Operating System Parameters

When responding to network scans, CounterACT 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:

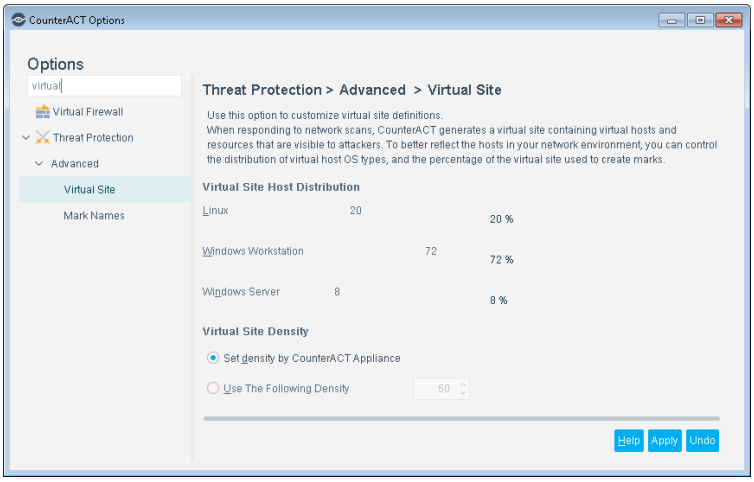
- The distribution of virtual host OS types that are presented on your virtual site. For example, Linux, Windows Workstations or Windows Servers.
- The density of virtual endpoints in your network. Density refers to the percentage of the virtual site, built with unused network resources (free IP addresses, closed ports etc.), to be used to create marks.

If you work with this tool incorrectly, CounterACT may not protect your network properly.

Only users with the required permission have access to this tool.

To define the virtual host OS distribution:

1. Select **Options** from the **Tools** menu then select **Threat Protection** > **Advanced** > **Virtual Site**.



Virtual Site Pane

2. Use the sliders to allocate a ratio. Distribution changes are built gradually. This means the changes will not be implemented immediately.
3. Set the virtual site density, either:
   - Select Set density by CounterACT Appliance, for a value optimally calculated by CounterACT.
   - To 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**.

Parsing 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 used for parsing by external applications. This information is located at the bottom of the email in the **Event Details for Parsing** section. 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
```

Details

192.0.2.1	Endpoint address.
Port bite	Event type.
port block	CounterACT 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.

Chapter 14: Managing Users

- About CounterACT Users
- Creating Users and User Groups
- Removing Users
- Password Protection
- Login Preferences
- Session Handling Preferences
- Manual User Password Change
- Using Smart Card Authentication
- Monitoring User Activity

About CounterACT Users

CounterACT user management features let you:

- Create user management accounts for single users or user groups
- Assign permissions to allow, limit or prevent user access to specific Console tools
- Limit view of endpoints per user
- Block and release users
- Generate reports detailing user activity
- Create user password policies and login consent pages
- Implement advanced security login methods
- And more

Default Admin User

CounterACT is installed with an “Admin” user who has access to all Console tools and features. This means that you do not need to create any other users in order to operate the system.

User Groups

In addition to creating an Admin and individual users, you can define single CounterACT users or define user groups. Working with user groups allows you to streamline and simplify user creation. Specifically, you can define CounterACT user groups based on existing Active Directory and RADIUS user groups. Users associated with groups receive identical CounterACT permissions and scope assignments.

For example, 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 segments.

Users can log in to CounterACT using Active Directory or RADIUS server credentials and are authenticated via the selected authentication server defined when the group was created.

Two methods are available for grouping CounterACT users.

- Associate CounterACT user groups with a specific RADIUS attribute and value.
- Associate CounterACT user groups with a specific User Directory group membership.

User Type – Group

Monitoring User Activity

You can view audit trail logs regarding user activity. These logs list, for example, users who updated policies, stopped or started CounterACT, or updated user passwords. The logs give additional information about the user activity, such as the date of the activity and the IP address from which it was carried out.

Creating Users and User Groups

CounterACT users or user groups can be assigned the following:

- Authentication requirements: Define which authentication method is required when logging in.
- Feature permissions: Prevent or allow access to Console features.
- Scope permissions: Define which network devices can be viewed and controlled.

Working with Permission and Scope Options

Work with *Permission* and *Scope* options to achieve powerful user control. For example:

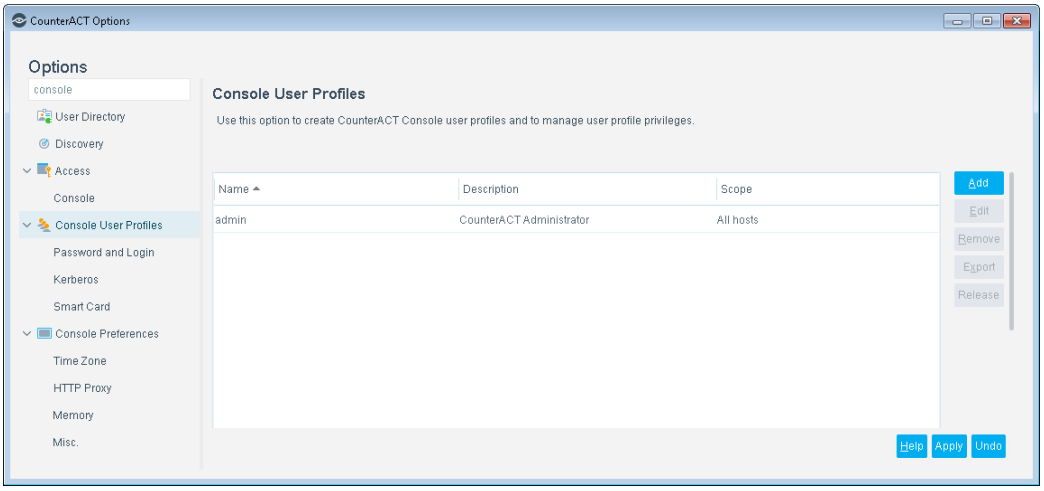
- Allow access to the entire network range but never allow access to certain high security features, such as the Appliance configuration or Action Threshold features.
- Allow access to a specific network range, such as a particular building, and grant permission to all CounterACT tools.

In addition, you can create users or user groups that have access to the Console or the Assets Portal, or users that can access both.

Users who are not assigned any permissions will not be granted login access to the Console or any of the CounterACT web-based portals.

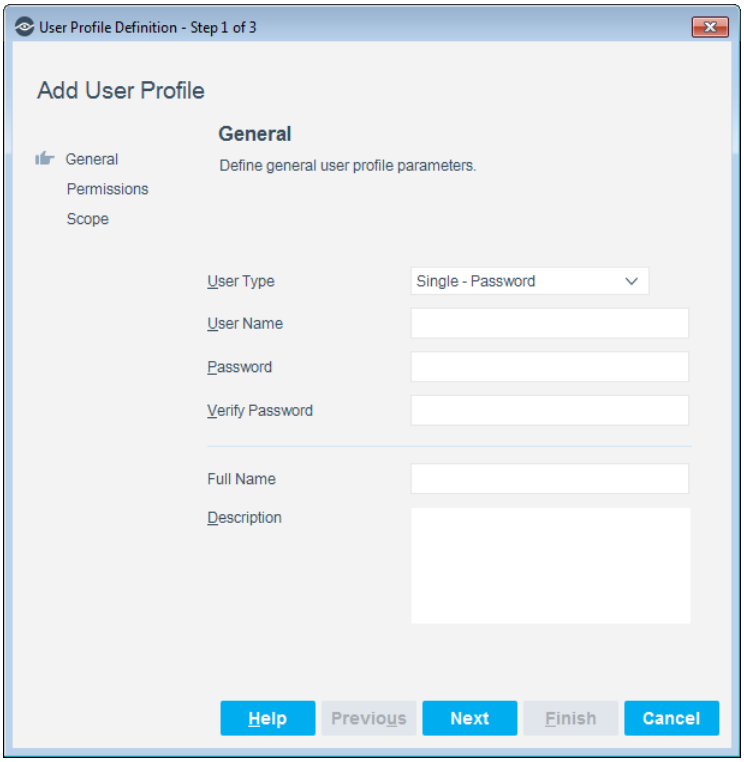
To create a new user or user group:

1. Select **Options** from the **Tools** menu and then select **Console User Profiles**.



Console User Profiles Pane

2. Select **Add**. The Add User Profile wizard opens.



General Pane

3. Select a user type from the User Type field to indicate if the user will be a single user or a group user, as well as the authentication method to be used. Authentication parameters vary depending on the user type selected.

Single User Options

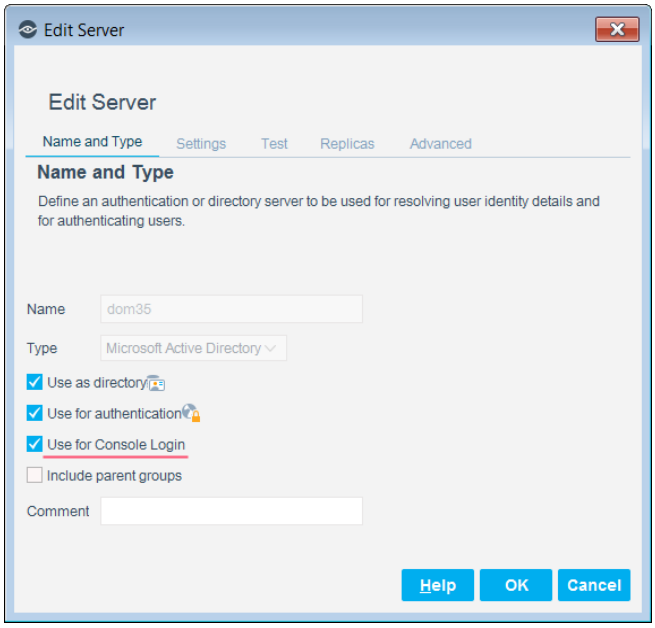
– Password: the user is authenticated via CounterACT server. Enter a user name and password.

  Enter a user name in the **User Name** field. This is the name used to log in to the Console. The user name cannot contain any of the following characters: **/:*?'<>|"**.

  Enter a password in the **Password** field. This is the password used to log in to the Console. You are informed if the password does not comply with the password rules (see Password Protection). The password can only contain ASCII characters. There is no character limitation. You must use at least one digit.

  Re-enter the password in the **Verify Password** field.

– External User Directory: The user is authenticated via a User Directory server defined in the User Directory Plugin. This may be, for example, an LDAP, RADIUS or TACACS server. Verify that the User Name defined here matches the user name listed in your User Directory server.
  In the User Directory Plugin, verify that the **Use for Console Login** option was selected for this server.



User Directory Server > Name and Type tab

– Smart Card: Enter a user name. When working with this kind of authentication, you must configure CounterACT to work with Certificate Authority (CA) files and Certificate Revocation Lists (CRLs), and configure the frequency (in seconds) to poll the CRLs. See Using Smart Card Authentication.

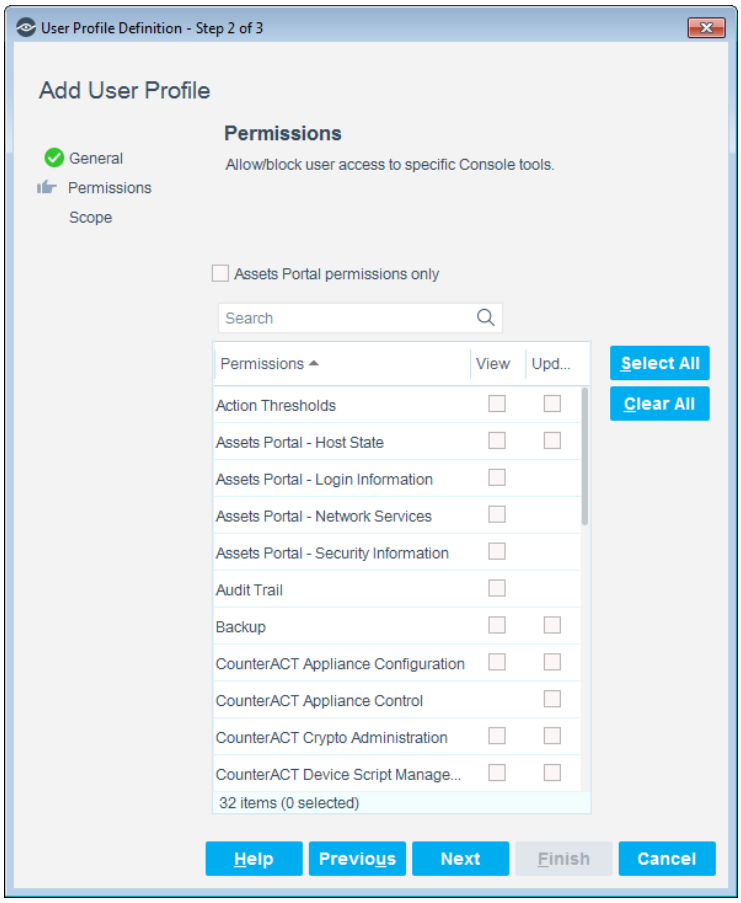
User Group Options

These options associate CounterACT user groups with a specific external directory group membership. Users associated with this group will receive permissions and scope assignments listed here. The directories defined here were defined in the User Directory Plugin. Verify that the **General** > **Use for Console Login** option is selected for this server in the plugin.

External User Directory – Associate CounterACT user groups with a specific Active Directory group. Select a server name from the drop-down list and enter a group name in the **Active Directory Group Name** field. When entering the group name, use the format resolved when working with the CounterACT *User Directory* > *Member Of* property. Names are case sensitive.

External Radius – Associate CounterACT user groups with a specific RADIUS attribute and value. Enter the attribute and value parameters to which you want to associate this group. Values are cases sensitive. Valid Attributes are numbers between 0 and 255.

4. After defining user types, enter a description of the user or group in the **Description** field.
5. Select **Next**. The Permissions pane opens.



Permissions Pane

6. If you only want the user to work with the Assets Portal, select **Assets Portal permissions only**. The Assets Portal is a web-based search and discovery tool that allows you to leverage extensive network information collected and correlated by CounterACT and its plugins. It is recommended to create Assets Portals users for IT, Security and Helpdesk teams. See Chapter 9: Assets Portal for more information.
7. Select the appropriate permission settings for the user that you are creating:
   - (View) only allow users to view information
   - (Update) allow users to view and update information
   - (No selection) prevents users from viewing the feature

   If you are updating permission for other users, those users must exit and then log in to the Console again for the permissions to take effect.

   Users who are not assigned any permissions will not be granted login access to the Console or any of the CounterACT web-based portals.

Access to Console Tools – Permissions

Permission	Details
Action Thresholds	
Action Thresholds	Implement Action Thresholds when working with blocking and restrictive actions. See Working with Action Thresholds for details.
Assets Portal Permissions See Chapter 9: Assets Portal 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.
Console Permissions	
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. See Appliance Management.
CounterACT Appliance Control	Start, restart or stop CounterACT 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 CounterACT marks more realistic. See Defining Mark Rules.

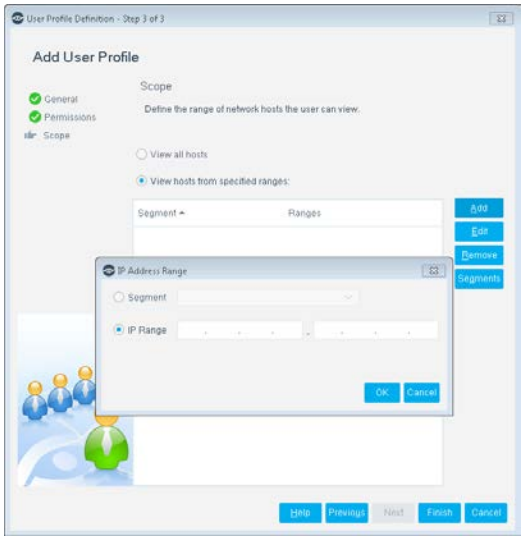
Permission	Details
CounterACT Crypto Administration	Import, edit and remove trusted and system certificates in CounterACT and configure certificate-related settings such as certificate expiration monitoring and checking for new CRLs and ongoing TLS sessions.
Enforcement Mode	Control the CounterACT Enforcement mode. The Full Enforcement mode allows complete functionality. The Partial Enforcement mode lets you monitor network traffic with limited ability to respond to it. The Partial enforcement mode is recommended for evaluation purposes only. See Working with the Enforcement Mode.
Enterprise Manager Control	Start, restart or stop CounterACT Enterprise Managers. See Standalone Appliance Management.
Event Log	View the Event Log that displays system events. See Working with System Event Logs.
Group Management	Add, edit, remove or update CounterACT Groups. The Group Management permission cannot be changed (to read-only or view only) if the Policy Management permission is selected. See Working with CounterACT Groups.
Host State Override	Update the state of endpoints and the length of time that the state is maintained. See Changing the Host State and Changing the Host State Maintenance Time.
Legitimate Traffic	Define the addresses of legitimate traffic at your network. See Defining Legitimate Traffic.
License Management	Install and manage CounterACT device licenses and Extended Module licenses. See Chapter 17: License Management.
Malicious Traffic	View malicious traffic. See Chapter 12: Threat Protection.
Multiple CounterACT Appliance Management	Manage a number of Appliances within the network. See Chapter 15: 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 or delete import and export policies. Create, edit or delete import and export segments, Groups and Lists. See: ▪ The Policy Manager ▪ Working with CounterACT Segments ▪ Working with CounterACT Groups ▪ Defining and Managing Lists
Plugin Control	Start, stop, test and get help on plugins and modules. See About Base, Content and Extended Modules.
Plugin Management	Install and uninstall plugins and modules. See About Base, Content and Extended Modules.

Permission	Details
Policy Reports	View NAC reports. See Policy Reports.
Reports	Work with the Reports Portal. See Reports.
Scheduled Reports	Generate schedules for reports. See Generating Scheduled Reports.
Software Upgrade	Upgrade CounterACT Appliance software. See Upgrading Appliance Software, Upgrading the Enterprise Manager Software.
Threat Protection Policy	View and manage Threat Protection Policy settings. See Viewing and Updating the Policy.
User Management	View and edit user management features. See Chapter 14: 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 Chapter 11: Managing Your Virtual Firewall Policy.

8. Select **Next**. The Scope pane opens.

Access to Network Endpoints – Scope

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 that they are assigned Scope access.



Scope Pane

Limited Scope access means that users can only see or control the following feature in the ranges or segments defined:

- Policy Management
- Segment Management

- Group Management
- Organizational Units
- All tools listed in the CounterACT Options window, with the exception of the Console Preferences folders
- Check for Updates
- Lists

For example, if you grant Scope access to the Finance segment in your organization to user Alice, then user Alice will only be able to work with the Console tools listed above for this segment.

If permissions are closed to a particular segment, buttons to these features are grayed out or users are provided with a message indicating that they cannot access the feature because they do not have the required user *Scope*.

To allow users access to a specific range but limit their access to a specific feature, you can grant *Scope permissions* and then limit feature *Permissions*. For example, allow users to view permission to the entire network range but restrict their access the Appliance configuration features.

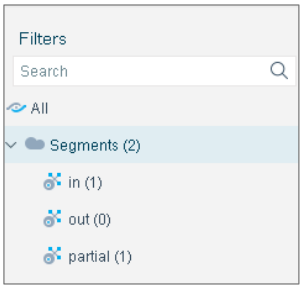
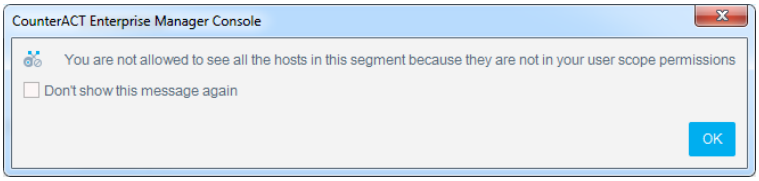
To define Scope access:

1. Select **View all hosts** to grant full access.
2. Select **View hosts from specific ranges**.
   - Select **Add**. The IP Address Range dialog box opens.
   - Enter the range or segment to which this user will have access.
   - Alternatively, select multiple segments by selecting **OK** and then selecting **Segments**.
   - Select **OK**.
3. Select **Finish**. The user definition is displayed in the Console User Profiles pane.

How Do Users Know That They Have Limited Scope Access?

The Console displays the following indicators to users with limited scope access:

Title bar	The title bar indicates that the user has a limited view. CounterACT Enterprise Manager Console - connected to [redacted] - Licensed to FORESCOUT - Limited user scope range

Filters pane	 ▪ No viewing access ▪ Partial viewing access When a user with limited viewing permissions attempts to view a blocked network segment or IP address range, the appropriate message is displayed. 

Modifying User Details

You can modify the permissions, password, and other details created for system users. The user permissions for Admin user cannot be modified.

Users can also manually change their password in the Console. See Manual User Password Change for details.

To modify user details:

1. From the Console User Profiles pane, select a user.
2. Select **Edit** or double-click a user entry. The Edit User Profile dialog box opens.
3. Edit the information as required.
4. Select **OK** to accept changes.
5. Select **Apply** to apply the changes to the configuration.

Removing Users

You cannot remove the default CounterACT Admin user.

To remove other users:

1. From the Console Users Profile pane, select a user.
2. Select **Remove** and then **OK** on the pop-up message.
3. Select **Apply** to apply the changes to the configuration.

Password Protection

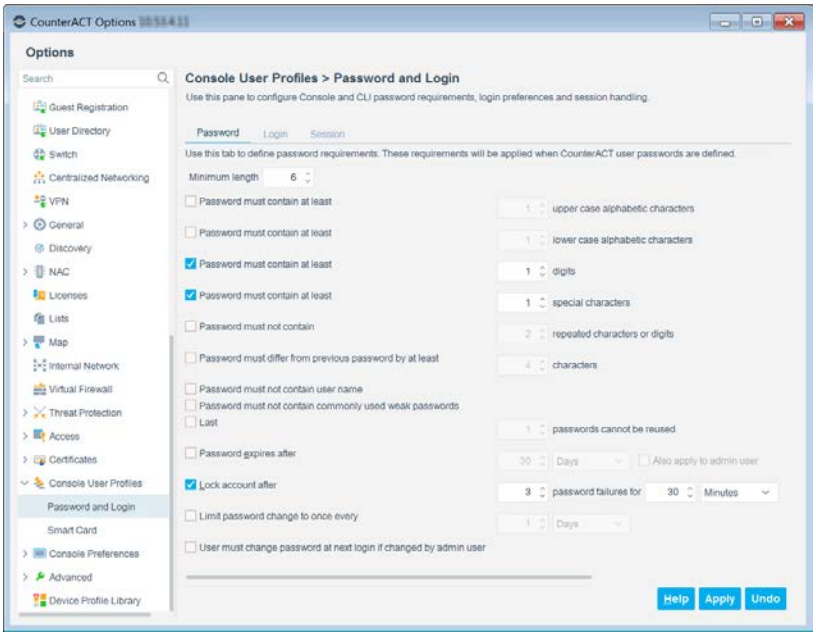
The password protection features let you:

- Define CounterACT password requirements, such as the minimum length of CounterACT passwords.
- Define a password expiration period.
- Lock out users after password failures for a defined lockout period.

Unless specified otherwise below, these settings apply both to Console users and users logging in to CounterACT devices through the command-line interface (CLI).

To define password policy:

1. Select **Options** from the **Tools** menu and then select **Console Users** > **Password and Login**.



Password and Login Pane

2. Select the **Password** tab.
3. Define:
   - Minimum password length.
   - Minimum number of upper and lower case letters
   - Minimum number of alphabetic and non-alphabetic characters.
   - Minimum number of digits.
   - Minimum number of special characters required in password.
   - Number of forbidden repeated characters or digits.

   This option only applies to Console users, and not users logging in to CounterACT devices through the command-line interface (CLI).

- Minimum number of characters that the password must differ from the previous password.
- If password can contain user name.
- If password can contain commonly used weak passwords.

  Selecting this option also enforces the following additional requirements:

  Minimum password length of 6 characters. *Note that the actual minimum length requirement may be higher than this depending on the value selected in the Minimum length option.*

  Password must contain at least 5 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)
- Number of most current passwords that cannot be reused.
- A password expiration period. A Change Password dialog box opens during login when this period expires.

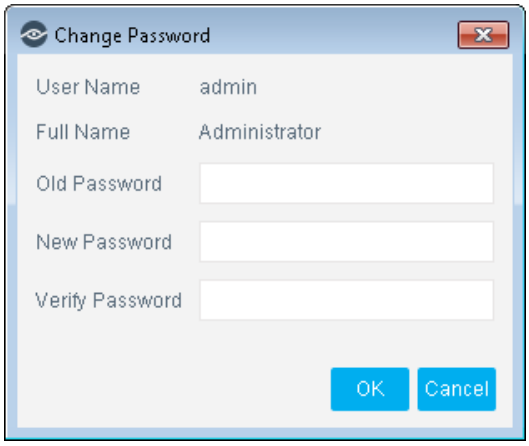
  You can choose to also apply this expiration period to admin users.
- Number of password failures within a defined time that cause the account to be locked.

This option only applies to Console users, and not users logging in to CounterACT devices through the command-line interface (CLI).

- Amount of time allowed between password changes.

  This only applies when the password was last changed by the same user. If, for example, an 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.
- If user must change password at next login after changed by admin user.

This option only applies to Console users, and not users logging in to CounterACT devices through the command-line interface (CLI).



Change Password Dialog Box

4. Define a password failure threshold and lockout period to enforce when the threshold is passed. For example, if a user entered the wrong password three times, that user is locked out of CounterACT for two days. Note that:
   - Admin users cannot be locked out.
   - Users who enter the wrong user name are not locked out.

Unlock Account

5. Select **Apply**.

Audit Logs

The audit log shows information about:

- Blocked and released users: Blocked and released users can be viewed in the Events Viewer Log.
- Policy changes: CounterACT users who created and edited password policies can be viewed in the Audit Trails Log.

Login Preferences

Define login preferences that determine whether to display consent messages to users during the login process and how users log in to CounterACT web portals.

These settings apply both to Console users and users logging in to CounterACT devices through the command-line interface (CLI).

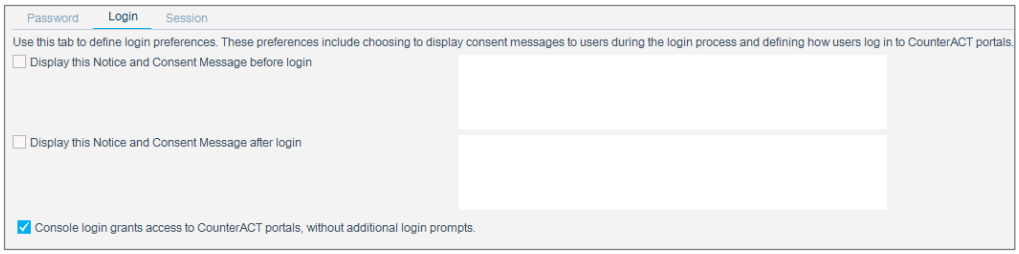
Login Notice and Consent Message Before Login

You can create a consent message displayed to users before login to the Console and web-based portals. Users must confirm the message to continue. This message can serve to describe restrictions of use, legal restrictions or other relevant information.

To define a consent message:

1. Select **Options** from the **Tools** menu and then expand the **Console User Profiles** folder.
2. Select **Password and Login**. The Password and Login pane opens.
3. Select the **Login** tab.

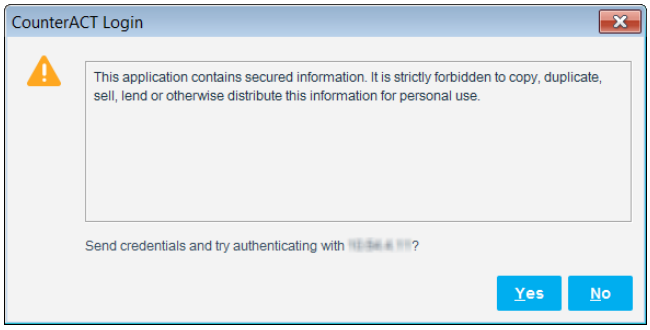
4. Select **Display this Notice and Consent Message before login** and type a message.



Login Consent Section

5. Select **Apply**.

   Users will see a consent message in the login screen before they can log in to the Console.



Sample Notice and Consent Message – Before Login

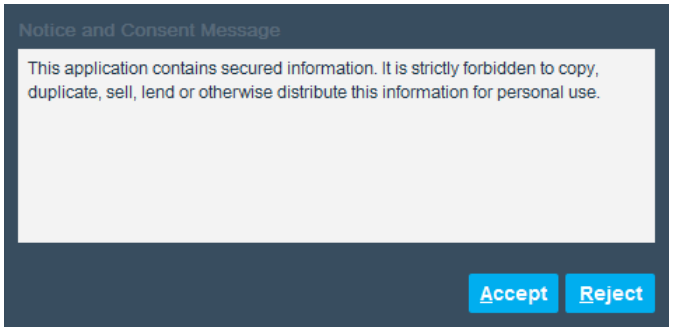
Login Notice and Consent Message After Login

You can create a consent message displayed to users immediately after login to the Console and web-based portals. Users must confirm the message to continue. This message can serve to describe restrictions of use, legal restrictions or other relevant information.

To define a consent message:

1. Select **Options** from the **Tools** menu and then expand the **Console User Profiles** folder.
2. Select **Password and Login**. The Password and Login pane opens.
3. Select the **Login** tab.
4. Select **Display this Notice and Consent Message after login** and type a message.
5. Select **Apply**.

   Users will see a consent message when they log in and must accept it to continue.



Sample Notice and Consent Message – After Login

Log in to Each CounterACT Web-Based Portal

Two methods are available for accessing CounterACT Web-based portals, such as the Assets Portal and Dashboard.

- Log in from your web browser. Log in from a browser always requires authentication. Smart Card authentication is also available.
- Select the **Ellipsis icon** ••• from the **Toolbar**, and Select **Dashboard** from the dropdown menu.

CounterACT can be configured to require users to reenter credentials when accessing CounterACT web-based portals from the Console, even after they logged in to the Console. By default, Console login grants access to CounterACT web-based tools, without additional login prompts.

To require users to reenter credentials to each portal:

1. Log in to the Console and select the **Options** icon from the Console toolbar.
2. Select the **Console User Profiles** folder, and then select the **Password and Login** pane.
3. Select the **Login** tab.
4. Disable the **Console login grants access to CounterACT portals, without additional login prompts** option.

Session Handling Preferences

Define session handling preferences to control how CounterACT handles idle, dropped and concurrent user sessions. You may need to configure some of these options to support one-time passwords and other authentication behaviors.

These settings apply both to Console users and users logging in to CounterACT devices through the command-line interface (CLI).

Support for One-Time Password Authentication

This section describes configuration options to support Console user authentication in environments that use one-time password (OTP) authentication.

To work with one-time passwords:

1. Select **Options** from the **Tools** menu and then expand the **Console User Profiles** folder.
2. Select **Password and Login**. The Password and Login pane opens.
3. Select the **Session** tab.
4. Disable the **Always query external authentication server to restore sessions** option.
5. (Optional) Select the **Sustain Console session for:** option, and specify a time period. For the time period you specify, CounterACT restores idle or dropped Console sessions without requiring a new login. Restored sessions can only be used from the endpoint that originally logged in.

Disconnecting Inactive Console Users

You can choose to disconnect Console users whose computer sessions have been inactive for a defined amount of time, reducing the potential for unauthorized user access. If this option is selected, and the computer has been inactive for the defined amount of time, the Console user will receive a dialog box notification indicating that the session has timed out and that the Console will close.

The Console closes either when the user acknowledges the notification or two minutes after the timeout period ends. This option is disabled by default.

To disconnect inactive users:

1. Select **Options** from the **Tools** menu and then expand the **Console User Profiles** folder.
2. Select **Password and Login**. The Password and Login pane opens.
3. Select the **Session** tab.
4. Select the **User Inactivity Timeout** option and define the period of time to wait before disconnecting inactive sessions.

Allowing One Login Session per Console User

Allow Console user accounts to be logged in from only one workstation at a time. Limiting access in this way can prevent unauthorized, and potentially harmful users from accessing the Console. When CounterACT detects a login attempt made by a user who is already logged in, choose to either:

- ***Log out the existing user session and allow the new login attempt***. If you choose to log out the existing user session, the existing user's Console session will end and the Console will close.
- ***Deny the new login attempt***. If you choose to deny the new login attempt, the existing user will be able to continue using the Console.

If you are using this feature, consider adding a backup Admin user with the required permissions so that you can preserve Console access in the rare circumstance that the Admin user is mistakenly logged out or denied access.

To allow only one login session per user:

1. Select **Options** from the **Tools** menu and then expand the **Console User Profiles** folder.
2. Select **Password and Login**. The Password and Login pane opens.
3. Select the **Session** tab.
4. Select the **Allow only one login session per user** option and select one of the following:
   - Log out existing session
   - Deny new login attempts

Manual User Password Change

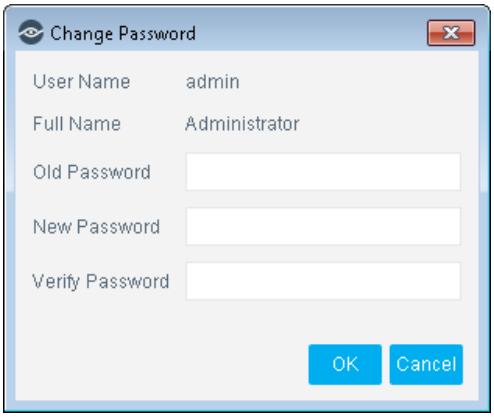
In addition to administrator-controlled password changes (see Creating Users and User Groups), CounterACT users can manually change their user password from the Console and from the CounterACT web-based portals (the Dashboard, the Assets Portal and the Reports Portal). The user password configured is global and applies to all CounterACT logins; for example, the Console and Reports Portal logins.

This option is disabled for users logging in to the Console 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 Administrator user. Administrator users can define users and how these users connect to CounterACT by selecting **Options** > **Console Users Profiles** in the Console.

Change password activity is written to the Audit Trail. To access the Audit Trail, in the Console **Log** menu, select **Audit Trails**. See Monitoring User Activity for details about the Audit Trail log.

To change your CounterACT User Password from the Console:

1. Select **Change Password** from the **Tools** menu. The Change Password dialog box opens.



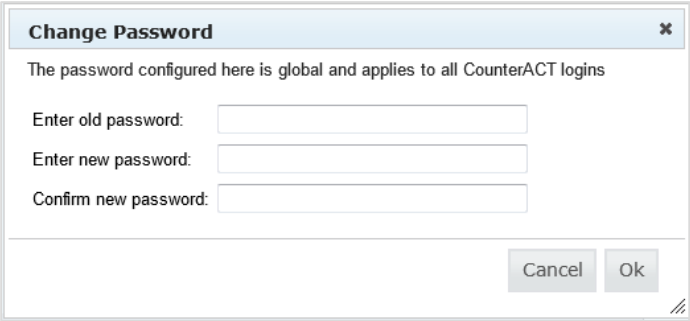
Change Password

2. In the Change Password dialog box, enter the old and new passwords and select **OK**.

To change your CounterACT User Password from the web-based portal:

1. In the **Admin** section of the web-based portal, select the **Change Password** icon .

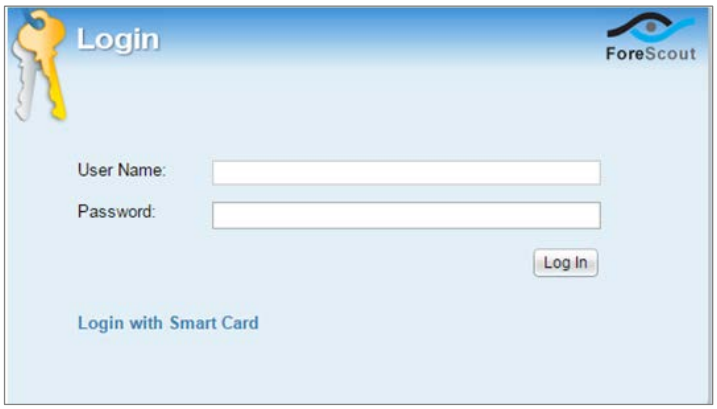
2. In the Change Password dialog, enter the old and new passwords and select **OK**.



Using Smart Card Authentication

Users can log in to CounterACT and CounterACT portals using Smart Card authentication.

Console Smart Card Login



Smart Card Portal Login

About CounterACT Smart Card Portal Login

Smart Card authentication is supported on the following CounterACT portals:

- Assets Portal. See Chapter 9: Assets Portal for details.
- Reports Portal. See Reports Portal for details.

Users may be required to enter a PIN code when logging in to CounterACT portals with a Smart Card.

If login credentials are incorrect or there is a problem with the Smart Card certificate, an error message will appear. Messages will vary depending on the browser being used.

Smart Card Login Error

Setting Up Smart Card Authentication

Smart Card authentication requires:

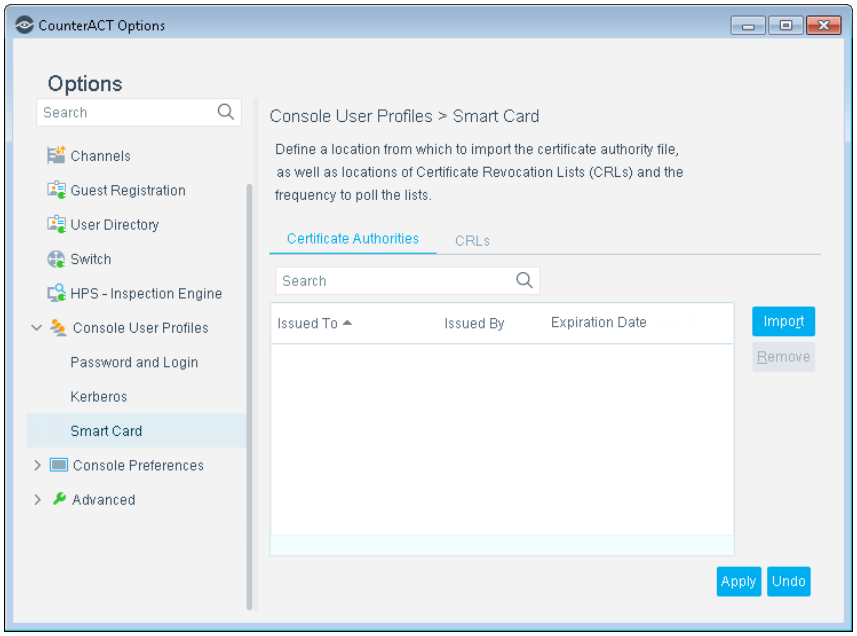
- Smart Card Configuration
- Smart Card User Setup

Smart Card Configuration

When working with this kind of authentication, you must configure CounterACT to work with Certificate Authority (CA) files and Certificate Revocation Lists (CRLs), and configure the frequency (in seconds) to poll the CRLs.

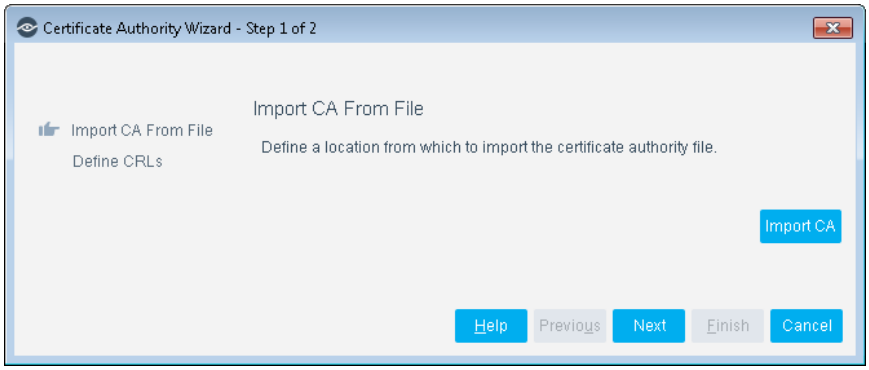
To configure Smart Card authentication:

1. Select **Options** from the **Tools** menu and then select **Console User Profiles** > **Smart Card**.



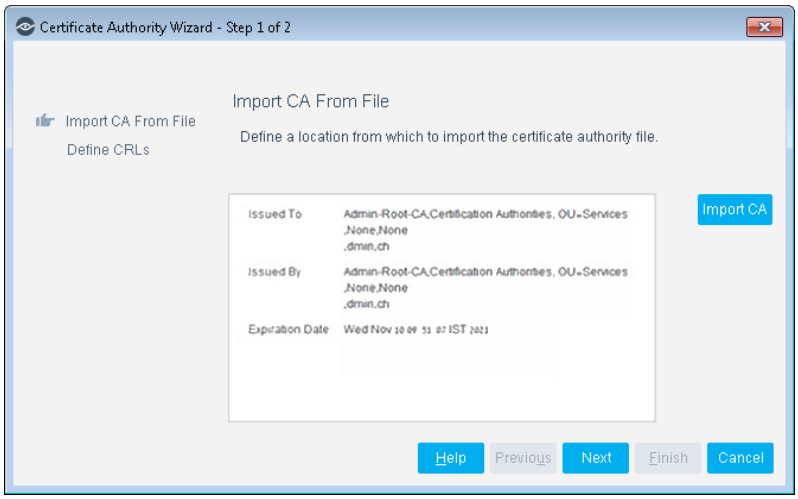
Smart Card Pane

2. Select **Import**. The Certificate Authority Wizard opens.



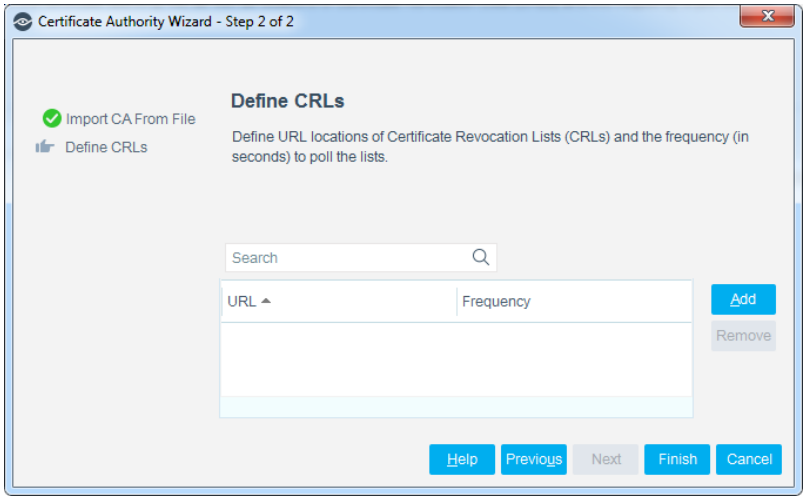
CA Import Pane

3. Select **Import CA**. An import dialog box opens.
4. Locate the required file and import. CA file information appears.



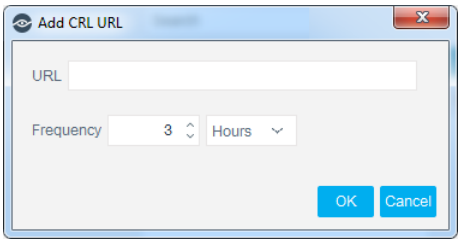
CA File Imported

5. Select **Next**. The Define CRLs pane opens.



Define CRLs Pane

6. Select **Add**. The CRL definition dialog box opens.

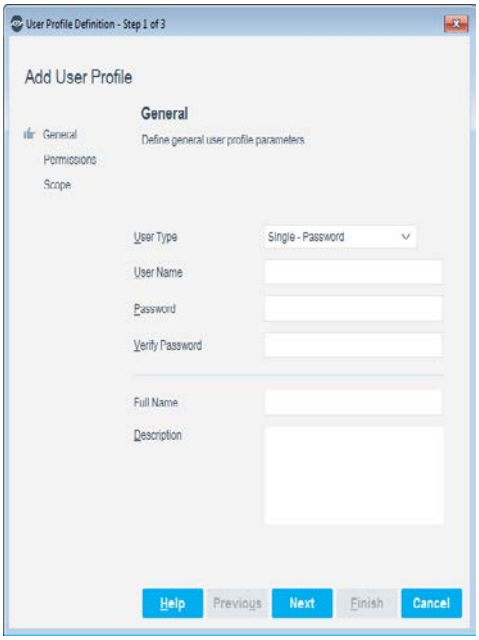


CRLs Definition Dialog Box

7. Define locations of Certificate Revocation Lists (CRLs) and the frequency (in seconds) to poll the lists.
8. Select **Finish**. User sessions are authenticated as follows:
   - CounterACT 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. CounterACT logs this event in the Event Viewer.
   - CounterACT imports Certificate Revocation Lists (CRLs) at the specified frequency, and updates its certificate store. After each update, CounterACT rechecks all user sessions authenticated by certificates.

Smart Card User Setup

In order to work with Smart Card authentication you must verify that the Smart Card Common Name (CN) and CounterACT user name are identical, including case sensitive spelling. CounterACT user names are defined in the Console User Profile pane. See Creating Users and User Groups for details about creating CounterACT users.



User Profile Definition Dialog Box

Monitoring User Activity

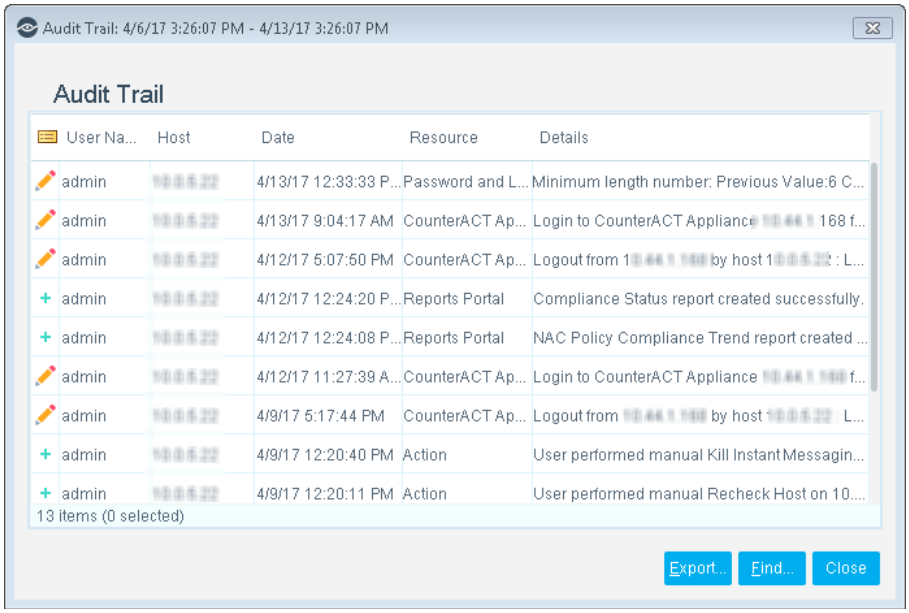
You can view user audit trail reports that contain information about user activities during a specified time period. These reports list operations (add, delete, edit) performed by users related to, for example, some of the following Console configurations:

- Policies
- Stopping or starting CounterACT
- User passwords
- Plugins and Modules

The logs give additional information about the user activity, such as the date of the activity and the IP address from which it was carried out. These reports can be exported.

To view audit trail reports:

1. In the Console **Log** menu, select **Audit Trails**. The Time Period dialog box opens.
2. Select a time period by doing one of the following:
   - To specify a relative time, select Relative Time. In the Last field, select the required number of hours, days, weeks or months by using the spin controls or by typing a value in the field. Select an option from the drop-down list.
   - To specify a time range, select Time Range. Select the beginning of the time range with the drop-down arrow in the From field. Select the end of the time range with the drop-down arrow in the To field. Use the calendar to set the range.
3. Select **OK**. The Audit Trail dialog box opens.



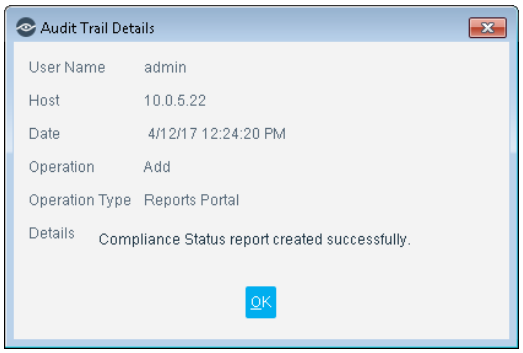
Audit Trail Dialog Box

The following information is available:

(Operation)	Add Edit Delete
Severity	Emergency Alert Critical Error Warning Notice Information Debug
Date	The date and time that 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.

To view details of an audit trail entry:

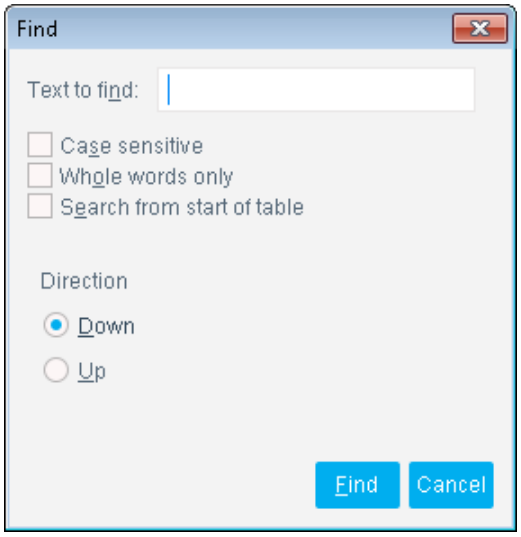
1. Double-click the selected line. The Audit Trail Details dialog box opens with event details.



Audit Trail Details Dialog Box

To find an entry in the audit trail list:

1. Select **Find**. The Find dialog box opens.



Find Dialog Box

2. Type the text and select the relevant options.
3. Select **Find** to locate the required text or **Cancel** to close the dialog box.

   CounterACT searches the currently active table for the specific text.

To save the log to an external file:

1. Select **Export** from the Audit Trail dialog box. A standard export dialog box opens.
2. Select a location to export the file and select **Save**. You can save the file in TXT or XLS format.

Chapter 15: Managing Appliances, Enterprise Managers and Consoles

- About Management
- Console Management
- Standalone Appliance Management
- Enterprise Manager Management
- Appliance Management
- Configuring Features for an Appliance or Group of Appliances
- Limiting User Access to Appliances
- Controlling Command-line Access to CounterACT Devices

About Management

This chapter describes features available for managing CounterACT devices (Appliances and Enterprise Managers) and Consoles.

Not all users have access to these tools. For more information see Access to Console Tools – Permissions.

CounterACT Device Management Overview

When an Appliance registers with an Enterprise Manager, most of the Appliance settings are automatically replaced with Enterprise Manager settings, as detailed in the following tables. Any subsequent changes to these settings on the Enterprise Manager are automatically applied to all registered Appliances.

Automatically Applied Settings

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

Automatically Applied Settings That Can Be Fine-Tuned

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

Appliance-Specific Settings

The following settings are unique per Appliance and are not affected by Enterprise Manager settings.

- Channel configuration
- License management (Per-Appliance Licensing Mode only)
- Appliance upgrade

Console Management

This section describes the following Console management options:

- Defining Console Access
- Multiple Console Logins
- Defining Web Access
- Disabling Web Portals
- Configuring HTTP Strict Transport Security
- Configuring the Time Zone
- Customizing Alarm Indicators
- Configuring Console Memory Settings
- Configuring Console View Settings

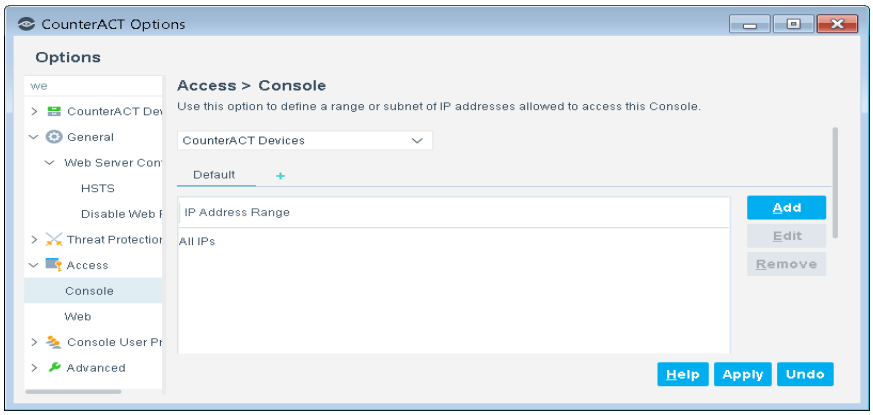
Defining Console Access

By default all IP addresses have access to the Console. Use this procedure to modify the IP addresses that can access the Console.

To manage Console access:

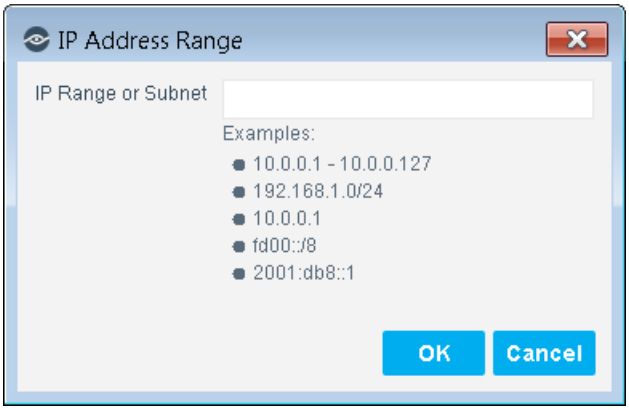
1. Select **Options** from the **Tools** menu and then select **Access** > **Console**.

   The Ranges table lists all IP addresses that are permitted to communicate with this Console.



Access>Console pane

2. (Optional) Create a configuration for a group of Appliances, or select a configuration to modify. See Configuring Features for an Appliance or Group of Appliances.
3. Select **Add**. The IP Address Range dialog box opens.



IP Address Range

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. It is not recommended for multiple users to log in to the same instance of the Console.

To support multiple Console users from a single endpoint, install a separate, uniquely named instance of the Console for each user.

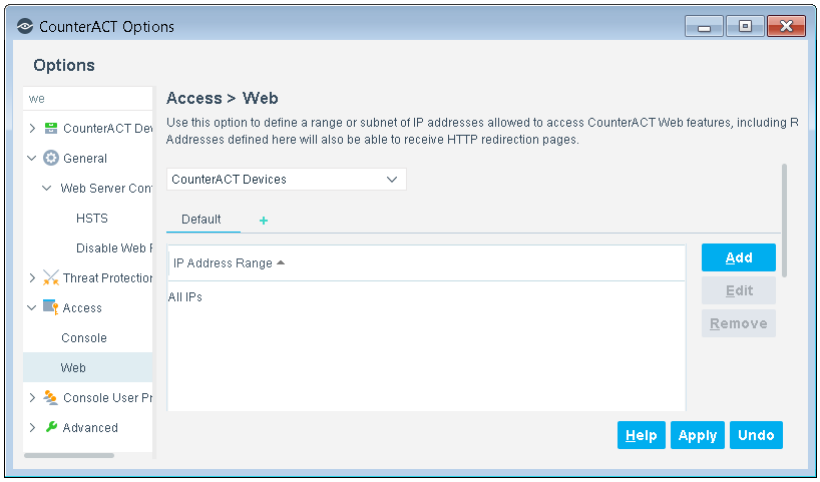
Defining Web Access

Use this option to define a range of IP addresses allowed to access the web. These IP addresses also can access the Reports and Assets Portal, and receive HTTP redirect notifications pages.

Grant web access only to IP addresses that are included the Internal Network.

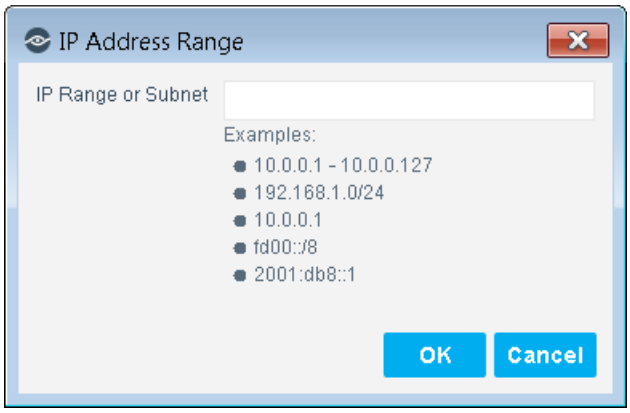
To define web access IP ranges:

1. Select **Options** from the **Tools** menu and then select **Access** > **Web**. The IP Address Ranges table lists all IP addresses that are permitted to communicate across the web.



Access>Web pane

2. (Optional) Create a configuration for a group of Appliances, or select a configuration to modify. See Configuring Features for an Appliance or Group of Appliances.
3. Select **Add**. The IP Address Range dialog box opens.



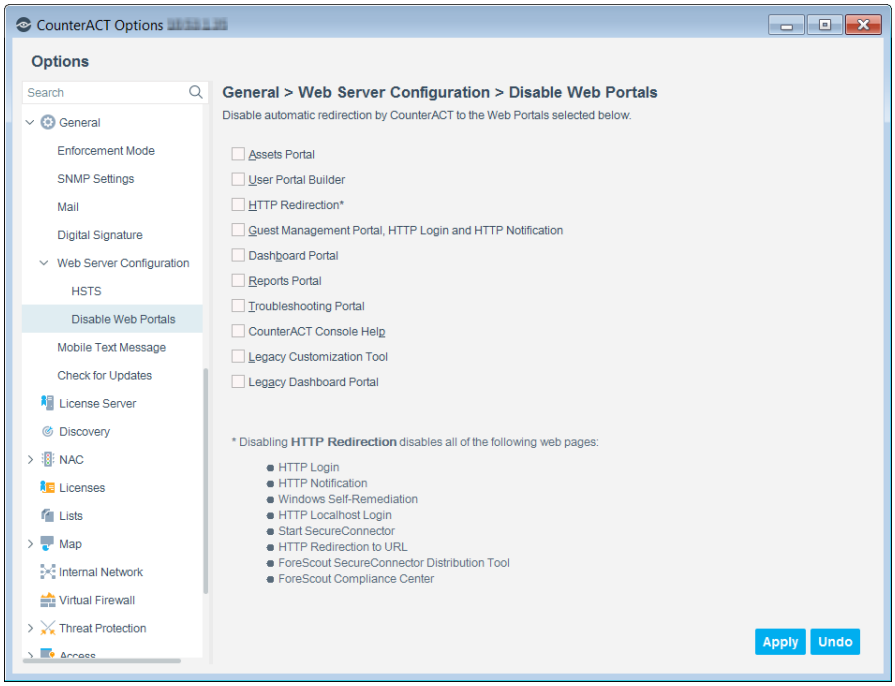
IP Address Range

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**.

Disabling Web Portals

Under some security scenarios, you may want 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 CounterACT to web portals and web pages.



General > Web Server Configuration > Disable Web Portals pane

To disable a web portal or page:

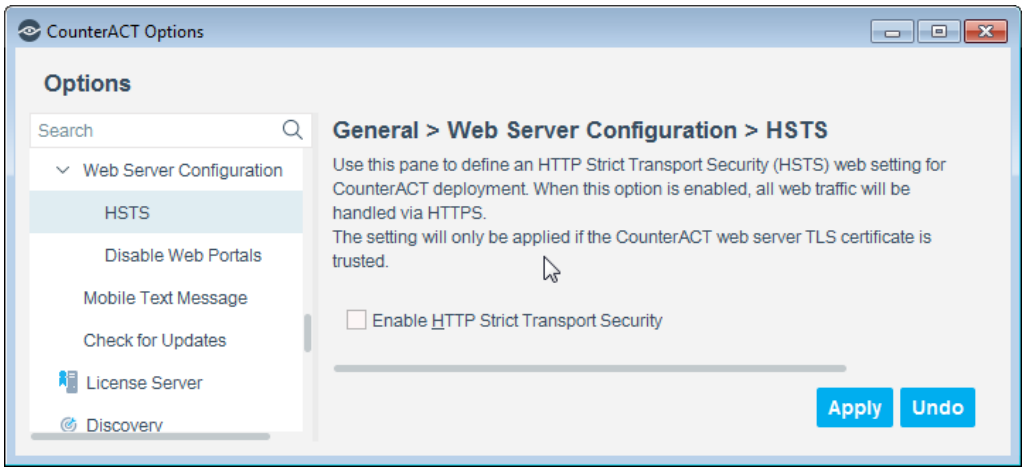
1. Select **Options > General > Web Server Configuration > Disable Web Portals**
2. Select one or more of the following options:
   - Assets Portal
   - User Portal Builder
   - HTTP Redirection*
   - Guest Management Portal, HTTP Login and HTTP Notification
   - Dashboard Portal
   - Reports Portal
   - Troubleshooting Portal
   - CounterACT Console Help
   - Legacy Customization Tool
   - Legacy Dashboard Portal

* Disabling *HTTP Redirection* also disables the following actions and web pages:

- HTTP Login
- HTTP Notification
- Windows Self-Remediation
- HTTP Localhost Login
- Start SecureConnector
- HTTP Redirection to URL
- ForeScout SecureConnector Distribution Tool
- ForeScout Compliance Center

Configuring HTTP Strict Transport Security

Use this pane to define an HTTP Strict Transport Security (HSTS) web setting for the CounterACT deployment. When enabled, all web traffic will be handled via HTTPS. The setting will only be applied if the CounterACT web server TLS certificate is trusted.



General > Web Server Configuration > HSTS pane

To enable HTTP Strict Transport Security (HSTS):

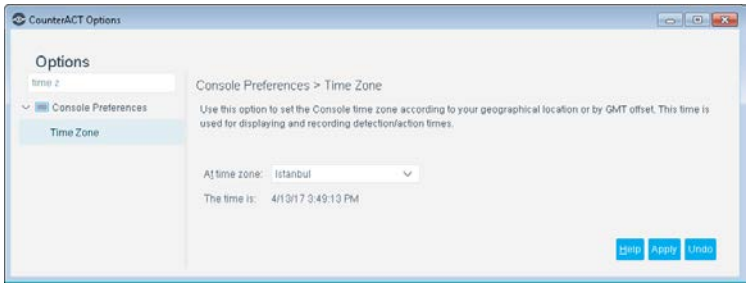
1. Select **Options** from the **Tools** menu and then select **General > Web Server Configuration > HSTS**
2. Select **Enable HTTP Strict Transport Security**.

Configuring the Time Zone

Set the time-zone according to your geographical location or by GMT offset. This time is used for displaying and recording detection and action times in the Console.

To select a time zone:

1. Select **Options** from the **Tools** menu and then select **Console Preferences** > **Time Zone**.



Time Zone Pane

2. Select a zone from the **At time zone** drop-down list.
3. Select **Apply**. All the times displayed in the Console change to reflect the time in the location that you selected.

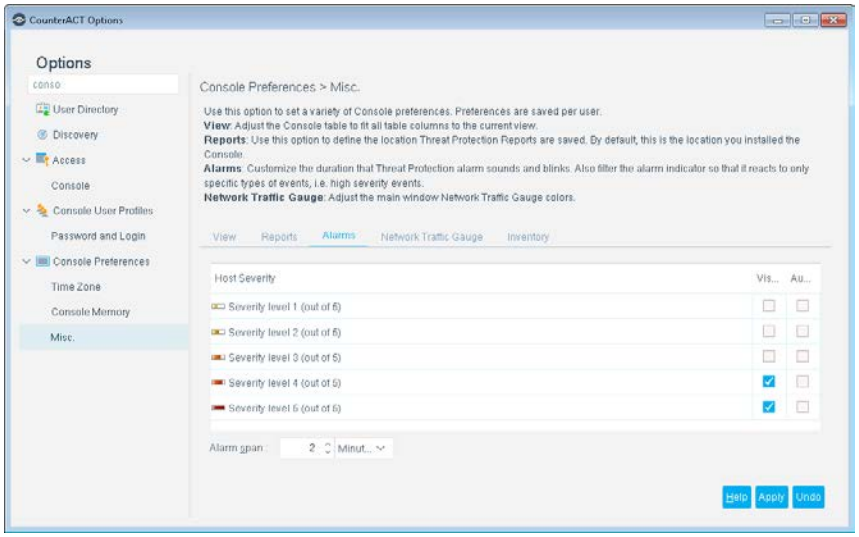
Customizing Alarm Indicators

An alarm flashes in the Console status bar when a specific type of malicious event occurs.

You can customize the length of time that the alarm flashes, and filter the alarm indicator so that it reacts to only specific types of events, i.e. high severity events. Severity levels are determined by the system.

To customize the alarm indicator:

1. Select **Options** from the **Tools** menu and then select **Console Preferences** > **Misc**.
2. Select the Alarms tab.



Alarms

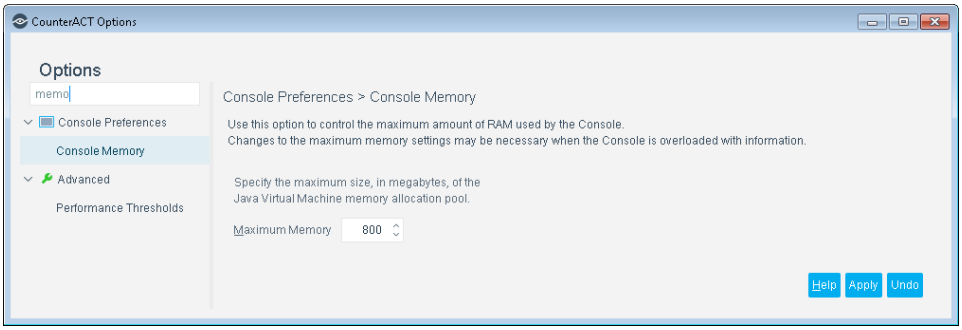
3. Select the **Visual** checkbox for the alarm light to flash for a specific severity level.
4. Select the **Audio** checkbox to activate a sound signal when the event occurs.
5. Adjust the alarm span duration as required.
6. Select **Apply**.

Configuring Console Memory Settings

Default maximum memory settings for the Console can be changed. This may be necessary when event traffic information is loaded from the Host Details dialog box. 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.

To configure memory settings:

1. Select **Options** from the **Tools** menu and then select **Console Preferences** > **Memory**.



Memory Pane

2. Define the maximum required memory limitations.
3. Select **Apply**.

Configuring Console View Settings

Use this procedure to configure some aspects of Console views.

To configure Console view settings:

1. Select **Options** from the **Tools** menu and then select **Console Preferences > Misc**.
2. Select the **View** tab.
3. Enable or disable the following settings:

Fit table columns to view	CounterACT resizes columns 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.

4. Select **Apply**.

Standalone Appliance Management

In an environment where there is only one Appliance, CounterACT functions as a standalone component. This means the Enterprise Manager is not managing the Appliance. See Appliance Management for more information about Appliance management.

Enterprise Manager Management

The Enterprise Manager is a dedicated second tier management and aggregation device that communicates with multiple CounterACT 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.

The following Enterprise Manager tasks can be performed:

- Upgrading the Enterprise Manager Software
- Viewing Enterprise Manager System Health Information
- Stopping and Starting the Enterprise Manager

Upgrading the Enterprise Manager Software

You can upgrade your version of the software from the Console. The procedure here works for High Availability devices as well.

For High Availability devices, back up the pair before you upgrade. See Backing Up System and Component Settings. The pair must be up and running when you upgrade. To upgrade a single active High Availability node when the Secondary node has failed or has not been set up:
Make sure the Secondary node is not accessible, and create the file *.ignorestandby* under */etc/* on the node to be upgraded.

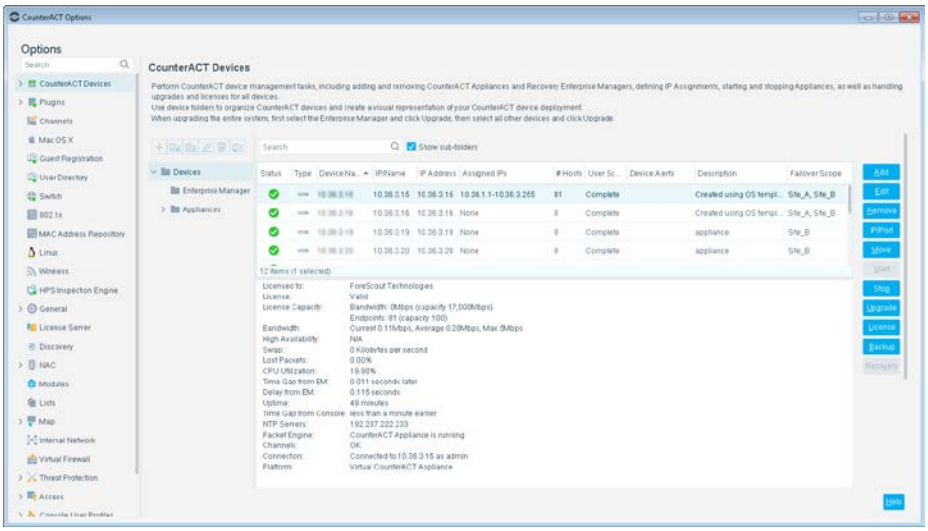
Refer to the *CounterACT Release Notes* for important upgrade information.

Not all users have access to the tools detailed in this section.

To upgrade Enterprise Manager software:

1. Download or obtain the upgrade file and save it to a location on your computer.
2. Select **Options** from the **Tools** menu and if necessary, select **CounterACT Devices**.

   The installed CounterACT devices and their current versions are displayed.



CounterACT Devices

3. Select an Enterprise Manager and select **Upgrade**. Do not select Enterprise Managers together with Appliances, because you cannot upgrade both Appliances and Enterprise Managers at the same time. The Upgrade Enterprise Manager dialog box opens.

4. Locate the upgrade file that you saved on your computer and select **OK**. After a check of the digital signature of the upgrade file is performed, the CounterACT Upgrade screen opens.
5. Select the **I accept the Terms and Conditions** checkbox. It is recommended to read the Release Notes.

   When upgrading an Appliance connected to an Enterprise Manager that was upgraded to the current CounterACT version, the pre-upgrade check is not performed, and the Upgrade button is immediately available in the CounterACT Upgrade screen.

6. Select **Verify**. A pre-upgrade check is performed to verify that the environmental and software requirements have been met. When the verification finishes, the Pre-Upgrade Verification summary screen opens.
7. Select **Upgrade** when you are sure you want to proceed with the upgrade. Once you confirm, the upgrade process proceeds to completion and cannot be interrupted or cancelled.

   High Availability Devices – Upgrade for High Availability devices can take a long time (up to a number of hours). 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:

	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 and **do not** continue with more upgrades.

Upgrading the Console During an Enterprise Manager Upgrade

During an Enterprise Manager upgrade, any Console applications 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 do a Console update select **Yes**. If you select **No**, the application automatically closes.
2. The update process consists of two stages.
   a. The software is downloaded while a dialog box shows the download progress.
   b. The software is upgraded.

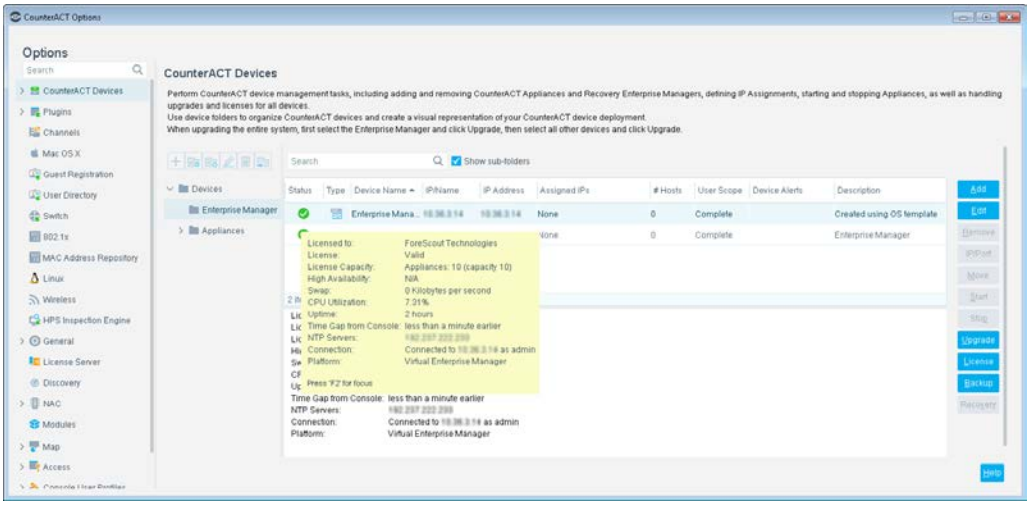
3. The Software Installation progress window opens showing the installation progress.
4. When the upgrade completes, select **Launch Console** at the bottom of the window to return to the CounterACT Login dialog box.

Viewing Enterprise Manager System Health Information

You can view at-a-glance system health information about your Enterprise Managers. This feature can be also used for troubleshooting.

To view Enterprise Manager health information:

1. Select **Options** from the **Tools** menu and then, if necessary, select **CounterACT Devices**. The CounterACT Devices pane opens displaying all the installed Enterprise Managers.
2. Place the cursor over the **Status** icon for the Enterprise Manager health information that you want to view. The Enterprise Manager details are displayed as a pop-up.



Enterprise Manager System Health

Items in red may require your attention.

The fields displayed may differ depending on your CounterACT deployment setup. For example, which licensing mode you are using, or whether you are using a virtual machine or not.

License	License status information.
License Request	License request details.
High Availability	Indicates whether a High Availability system is running.

Swap	Indicates whether the swap exceeded 100 kilobytes per second consecutively in the last one 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.
CPU Utilization	Indicates the percentage of actual CPU Utilization. If the value is high, contact your ForeScout representative.
Uptime	Indicates the amount of time the Enterprise Manager has been running.
Time Gap from Console	Indicates the time delay between the Console and the Enterprise Manager.
Connection	Indicates whether the Enterprise Manager Console is connected to the Enterprise Manager.

Stopping and Starting 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. For more information about using the utility see the *fstool Command Reference Guide*.

To control communication:

1. Log in to the Enterprise Manager.
2. Open a CLI run application.
3. Run the following command:

   `fstool service start|stop|restart|status|shutdown`

Appliance Management

The following Appliance Manager tasks can be performed:

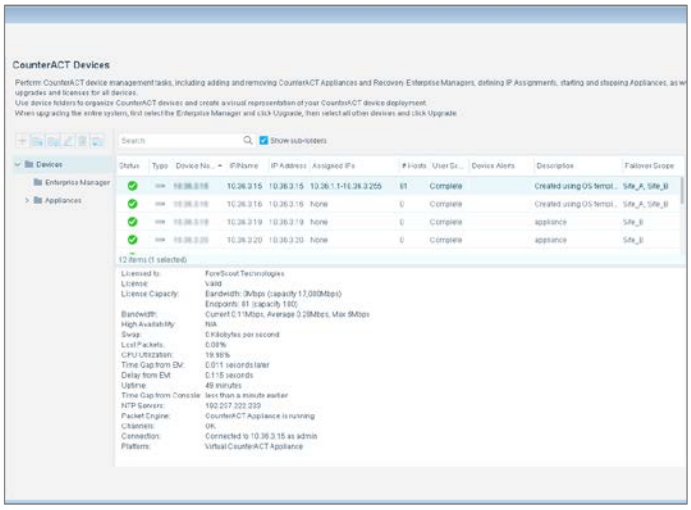
- Viewing Appliance Health Information
- Registering Appliances with the Enterprise Manager
- Upgrading Appliance Software
- Upgrading the Console
- Starting and Stopping Appliances
- Working with Appliance Folders
- Managing Groups of Appliances
- Appliance Endpoint Performance Capacity
- Working with Appliance Channel Assignments
- Viewing Information about CounterACT Devices
- Viewing Appliance Traffic Statistics

Viewing Appliance Health Information

You can view at-a-glance system health information about your Appliance. This feature can be also used for troubleshooting.

To view health information:

1. Select **Options** from the **Tools** menu.
2. Select an Appliance from the CounterACT Devices pane.
3. The Appliance health details are displayed in the Status section.



Health Information

Items in red may require your attention.

The fields displayed may differ depending on your CounterACT deployment setup. For example, which licensing mode you are using, or whether you are using a virtual machine or not.

License	The number of days remaining until the demo license expires.
Capacity	Bandwidth and endpoint assignment capacity violations. See Appliance Endpoint Performance Capacity for details.
Bandwidth	Statistical information on bandwidth usage.
High Availability	Indicates whether a High Availability System is running.
Swap	Indicates whether the swap exceeded 100 kbps consecutively in the last one 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 Appliance with a new Appliance that has more physical memory.

Lost Packets	Indicates whether the Appliance 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.
CPU Utilization	Indicates the percentage of actual CPU Utilization. If the value is high, contact your ForeScout representative.
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.
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.
Uptime	The amount of time the Appliance has been running.
Time Gap from Console	Indicates the time delay between the Console and the Appliance.
NTP	Indicates the NTP server connection status and server IP address.
Packet Engine	Indicates the status of the CounterACT packet engine: this is the engine that runs the Appliance. If this is down, many of your CounterACT features will not work.
Channels	Indicates if Channel connections are working properly.
Connection	Information about the connection between the Appliance and the Enterprise Manager. An error may include, for example, a version mismatch.
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.

4. Select **Close**.

Registering Appliances with the Enterprise Manager

Your system is installed to begin working with minimal user intervention. However, the tools provided for managing the Appliances through the Enterprise Manager are only available when you register your Appliances with the Enterprise Manager.

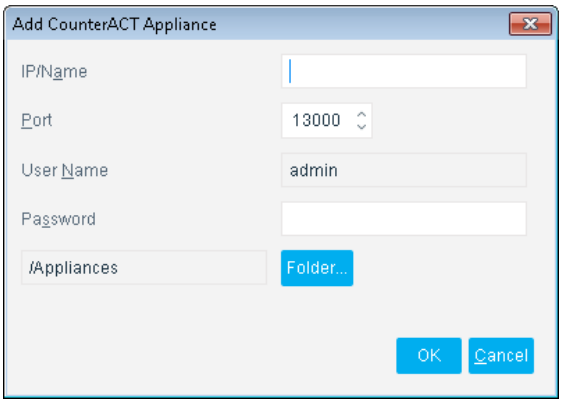
Appliances may have been added via the Initial Setup wizard. If necessary, you can add additional Appliances after the wizard is finished.

You cannot add an Appliance running CounterACT version 7 or below to an Enterprise Manager running CounterACT version 8 or above.

You must have a valid CounterACT license installed for your deployment. See Chapter 17: License Management for specific license requirements.

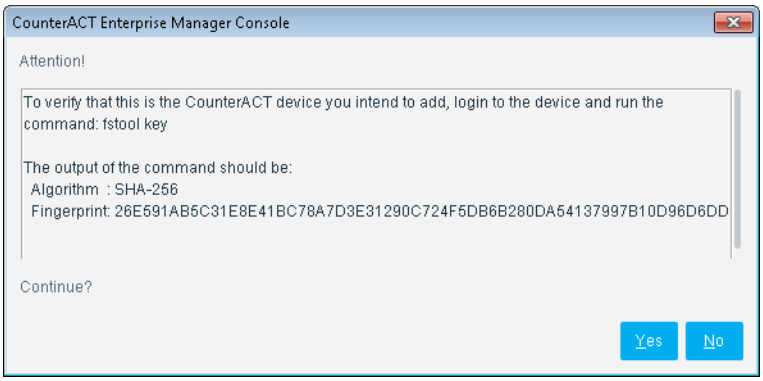
To add a new Appliance:

1. Select **Options** from the **Tools** menu.
2. Select **CounterACT Devices**.
3. Select **Add**. The Add CounterACT Appliance dialog box opens.



Add CounterACT Appliance

4. Type the Appliance IP address.
5. The default port number is displayed, which it is recommended not to change. This port is used to enable a network connection.
6. Type the admin password that should be used to connect to this Appliance.
7. Select the folder in which you want to add the Appliance. For more information about how to work with folders, see Managing Groups of Appliances.
8. 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 before continuing.



Public Key Dialog Box

9. To verify the Appliance key, log in to the Appliance CLI and run the following command:

   `fstool key`

   A message opens with the key ID.

10. An Initial Setup wizard opens. Set up the Appliance as required. See Set Up an Appliance with Enterprise Manager Settings for more information.

Appliance Operating in Per-Appliance Licensing Mode

If you are adding an Appliance operating in Per-Appliance Licensing Mode to an Enterprise Manager operating in Centralized Licensing Mode, you must switch the licensing mode of the Appliance to Centralized Licensing mode to match the Enterprise Manager. Perform the following before adding the Appliance:

1. Verify that the Appliance is operating as a Standalone Appliance and is not connected to any other Enterprise Manager.
2. Log in to the Appliance via the Console.
3. If the Appliance is running CounterACT version 7, upgrade the Appliance to CounterACT version 8. See Upgrading Appliance Software.
4. *Contact ForeScout Support or your ForeScout representative for more information on how to switch licensing modes. See* Switch Licensing Mode from Per-Appliance to Centralized*.*

Upgrading Appliance Software

You can upgrade your version of the software from the Console. The procedure here applies to High Availability devices as well.

For High Availability devices, back up the pair before you upgrade. See Backing Up System and Component Settings. The pair must be up when you upgrade. To upgrade a single active High Availability node when the Secondary node has failed or has not been set up:
Make sure the Secondary node is not accessible, and create the file *.ignorestandby* under */etc/* on the node to be upgraded.

Refer to the CounterACT Release Notes for this version for important upgrade information.

Not all users have access to the tools detailed in this section. See Access to Console Tools – Permissions for information about granting and preventing access.

To upgrade Appliance software:

1. Before upgrading Appliances, you should upgrade your Enterprise Manager. See Upgrading the Enterprise Manager Software.
2. Download or obtain the upgrade file and save it to a location on your computer.
3. Select **Options** from the **Tools** menu.

   CounterACT devices are shown with their current version.

4. Select Appliances and then select **Upgrade**. Do not select Enterprise Managers as well because you cannot upgrade both Appliances and Enterprise Managers at the same time. The file selection dialog box opens.
5. Locate the upgrade file that you saved on your computer and select **OK**. After a check of the digital signature of the upgrade file is performed, the CounterACT Upgrade screen opens.
6. Select the **I accept the Terms and Conditions** checkbox. It is recommended to read the Release Notes.
7. Select **Verify**. A pre-upgrade check is performed to verify that the environmental and software requirements have been met. When the verification finishes, the Pre-Upgrade Verification summary screen opens.

   *When upgrading an Appliance connected to an Enterprise Manager that was upgraded to the current CounterACT version, the pre-upgrade check is not performed, and the **Upgrade** button is immediately available in the CounterACT Upgrade screen.*

8. Select **Upgrade** when you are sure you want to proceed with the upgrade. Once you confirm, the upgrade process proceeds to completion and cannot be interrupted or cancelled.

   High Availability Devices – Upgrade for High Availability devices can take a long time (up to a number of hours). 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:

	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.

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.

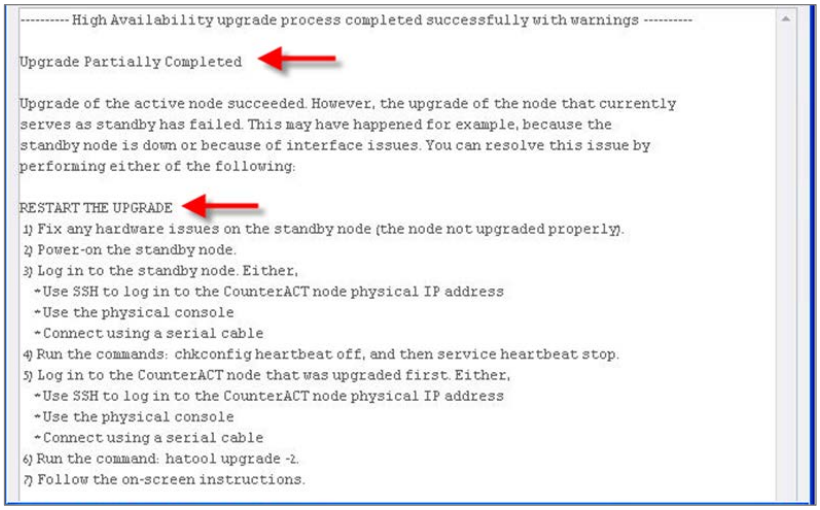
High Availability Upgrade Options

High Availability upgrades are performed on both nodes in the pair. Use the upgrade dialog box to indicate if you want to complete the upgrade if one of the nodes of the pair cannot be properly upgraded.

If you clear the **Continue the upgrade if one node of the cluster cannot be upgraded** checkbox, the upgrade will only continue if both nodes are running and functional. If you select the checkbox, the upgrade will continue even if the standby node is not working or powered-off.

Troubleshooting the Upgrade

Troubleshooting logs and web pages are available to help you handle upgrade complications. The web pages are accessed from the CounterACT Options window, CounterACT Devices, Status section. The logs are displayed during the upgrade process in the Upgrade Progress dialog box.



Troubleshooting High Availability Upgrade – Log

Upgrading the Console

During Appliance upgrade, any Consoles applications 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 Upgrading the Console During an Enterprise Manager Upgrade.

Starting and Stopping Appliances

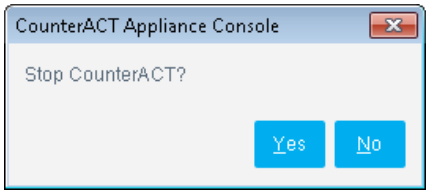
When an Appliance stops, Threat Protection, NAC, Discovery detections and other functionality are stopped. In addition, plugin and module functionality is stopped. This means that blocked endpoints are released and plugin/module actions previously taken on endpoints are undone.

When you start the Appliance again, plugin/module activity and endpoint detection resume. In addition, all endpoints that were released as a result of the Stop operation are returned to their previous state.

See Access to Console Tools – Permissions for more information about granting and preventing access to this feature.

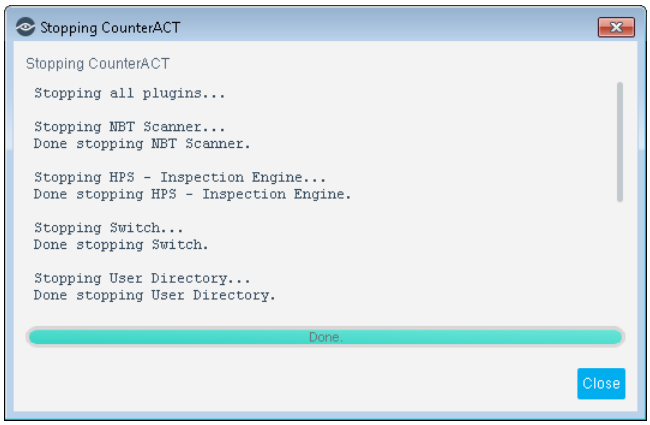
To start or stop an Appliance:

1. Select **Options** from the **Tools** menu.
2. From the CounterACT Devices pane right-click an Appliance and then select **Start** or **Stop**.



Stop Appliance Confirmation

3. Select **Yes**. The Stopping Appliance dialog box opens.



Stop Appliance

4. Select **Close**. The Appliance is displayed as stopped.

To start or stop the Appliance if you are logged on to a single Appliance:

1. Select **Options** from the **Tools** menu.
2. Select the Appliance from the Appliances pane and then select **Start** or **Stop**.

Working with Appliance Folders

Use Appliance folders to group CounterACT 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:

- Help CounterACT efficiently support large or geographically disperse networks
- Implement automatic IP allocation between Appliances
- Create failover clusters (licensed feature: refer to the *ForeScout CounterACT Resiliency Solutions Guide*.)

You use CounterACT segments based on the Internal Network to assign IP addresses to folders or Appliances. Define these segments in using Segment Manager before you work with folder tools. For example, if your network expands, you typically:

- Install new Appliances
- Use Segment Manager to define segments with your network's new IP addresses. See Working with CounterACT Segments.

- Add these segments to the Internal Network. See Working with the Internal Network.
- Use the procedure described in this section to define folders that contain the new Appliances, and to assign the new segments to Appliances.

If you change the definition of Internal Network segments, this can change which IP addresses are assigned to folders or Appliances.

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, CounterACT automatically assigns IPs in these segments to available Appliances in the folder. Endpoint sessions are distributed proportionally based on each Appliance's licensed capacity.
- Static Allocation: Assign segments to a specific Appliance. Only this Appliance handles endpoints in these segments. If this Appliance is part of a folder, it does not participate in automatic IP allocation.

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 which has no Appliances to handle it.

User Permissions for This Feature

The following Console user permissions are required to work with the features described in this section. For more information about Console user permissions, see Access to Console Tools – Permissions.

The following general permissions are required:

- CounterACT Configuration
- CounterACT Policy Management

To work with folder tree actions, the following addition permissions are required:

- Multiple CounterACT Appliance Management (update)
- CounterACT Appliance Control

Write permission is required to save changes.

To work with Appliance folders:

1. In the Console main menu, select **Options**.

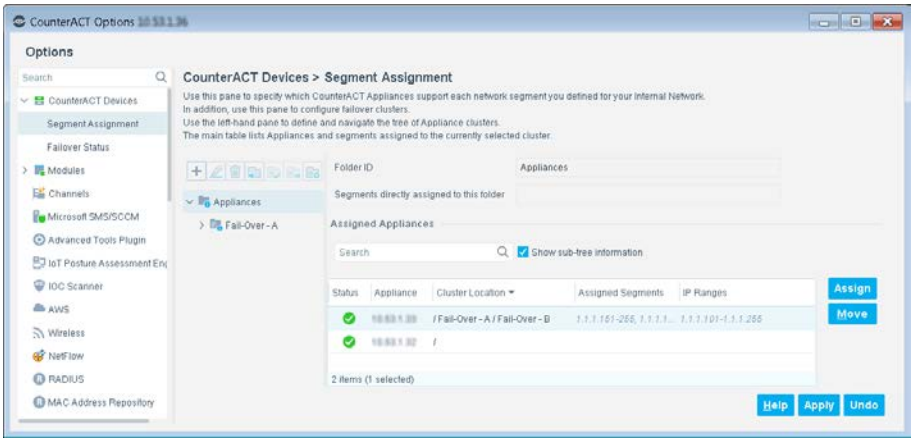
   The Options window opens.

2. In the Options tree, select **CounterACT Devices > IP Assignment and Failover**.

   The IP Assignment and Failover pane opens.

   – The tree of Appliance folders is shown in the left-hand pane.
   – The main table lists information for the folder that is currently selected.

If you defined Appliance folders when working with earlier releases, the folders appear in the tree.



IP Assignment and Failover pane

For each Appliance, the table lists the following information:

- The **Status** of the Appliance, as reported in the CounterACT Devices pane.
- The **Appliance** name or other identifier.
- The full path to the **Folder Location** that includes the Appliance.
- **Assigned Segments** 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.
- The **IP Addresses** corresponding to the assigned segments. If some segments are statically assigned to Appliances in the folder, this column indicates the remaining unassigned IP addresses.

3. To modify the folder tree, select a node in the tree and apply 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 of the right-hand pane.

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 of the right-hand pane. To support these segments, CounterACT allocates endpoints to free Appliances of the folder (which do not have statically assigned segments).

Reassign segments to this folder from Appliances in child folders. All segments that were statically assigned to Appliances in sub-folders of the selected folder are assigned to the selected folder. Note that:

- 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 of licensing and failover cluster configuration, refer to the *ForeScout CounterACT Resiliency Solutions Guide*.

4. To move Appliances to a folder:
   a. Find the Appliance(s) you want to move:

      Select a folder in the tree. The table lists all Appliances in that folder.

      Use the Assigned Appliances search field to refine the table: enter an Appliance or folder ID, or enter an IP address to locate the Appliance/folder that handles that network segment.

      *By default the **Show child folder information** checkbox is enabled, and the table also lists Appliances in children of the selected folder.*

      *To view all Appliances in your network that are not yet in a folder, clear the **Show child folder information** checkbox and select the All Appliances node of the folder tree.*

   b. Select the Appliances you want to move. Then select **Move**.

      In the dialog box, specify a folder and select **OK**.

      The selected Appliances are members of the folder.
5. To assign network segments to an Appliance:
   a. Find the Appliance you want to modify:

      Select a folder in the tree. The table lists all Appliances in that folder.

      Use the Assigned Appliances search field to refine the table: enter a string that identifies the Appliance or folder you seek.

      *By default the **Show child folder information** checkbox is enabled, and the table also lists Appliances in children of the selected folder.*

   b. Select the Appliance you want to modify. Then select **Assign**.

      The Assign IP Ranges dialog opens.
   c. Specify the segments you want to assign to the Appliance, and select **OK**. The segments are statically assigned to the selected Appliance. This means that:

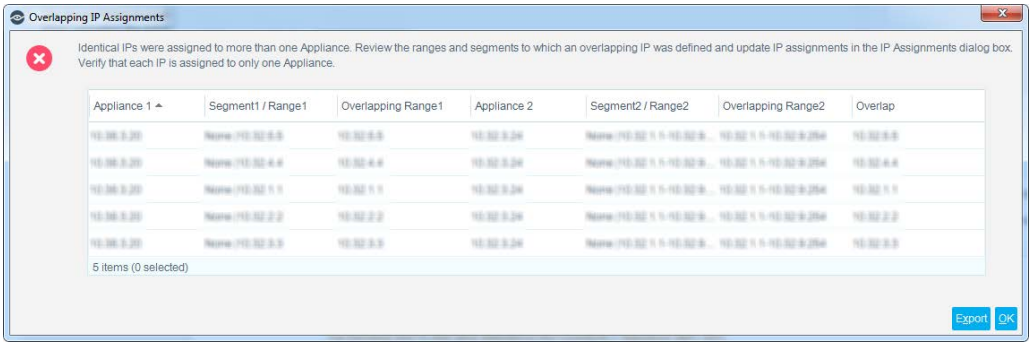
      Only this Appliance handles endpoints in these segments.

      This Appliance only handles these segments: it does not support segments assigned to its folder.
6. Select **Apply** to save configuration changes.

Overlapping IP Assignments

CounterACT verifies that each network IP address is only assigned to one Appliance. This ensures, for example, accurate endpoint monitoring and policy execution.

If you mistakenly define an IP address to more than one Appliance, CounterACT 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 are overlapping. 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.

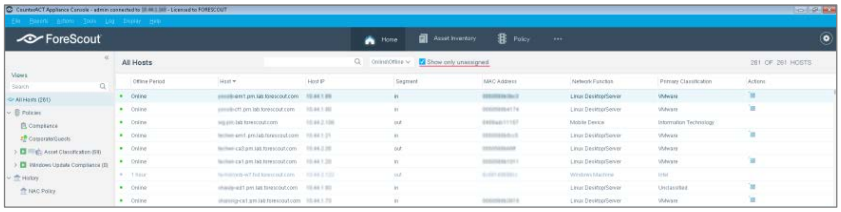


IP Assignment Overlap

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 that exist between any two specific Appliance segments 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 CounterACT detects an endpoint with an IP adddress 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**.



View Unassigned IPs

Modify the Appliance Folders tree to assign the segment that contains the endpoint to an Appliance or folder. CounterACT can then connect to the endpoint. When there are no longera any unassigned endpoints, an entry in the Event Log indicates that all detected endpoints are assigned to an Appliance.

Conflicting Configurations

When you configure CounterACT modules and other components, you can define groups of Appliances that have the same configuration settings, as described in Configuring 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 popup 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.

Managing Groups of Appliances

CounterACT Appliance folders let you simplify and unify CounterACT device management and configuration tasks. These folders are especially useful for medium and large scale CounterACT deployments. This section discusses the following topics:

- Updating Appliance Connection Details
- Configuring Sets of Appliances Simultaneously
- Viewing and Managing Plugin and Module Assignments per Folder

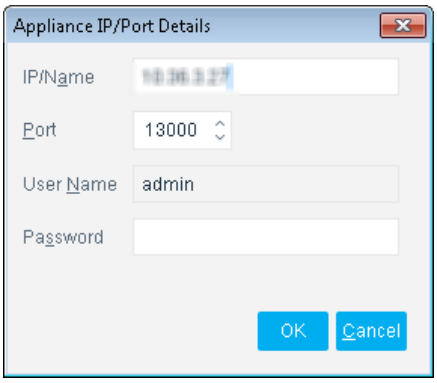
Updating Appliance Connection Details

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 will 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 will indicate that the Appliance is connected.

To update Appliance connection details:

1. Select **Options** from the **Tools** menu.
2. Select an Appliance from the CounterACT Devices pane and then select **IP/Port...**. The Appliance IP/Port Details dialog box opens.



Appliance IP/Port Details

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 a port number of 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>Console User Profiles**. See Modifying User Details for information about changing the password. 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 will be updated to indicate that the Appliance is connected.

Configuring Sets of Appliances Simultaneously

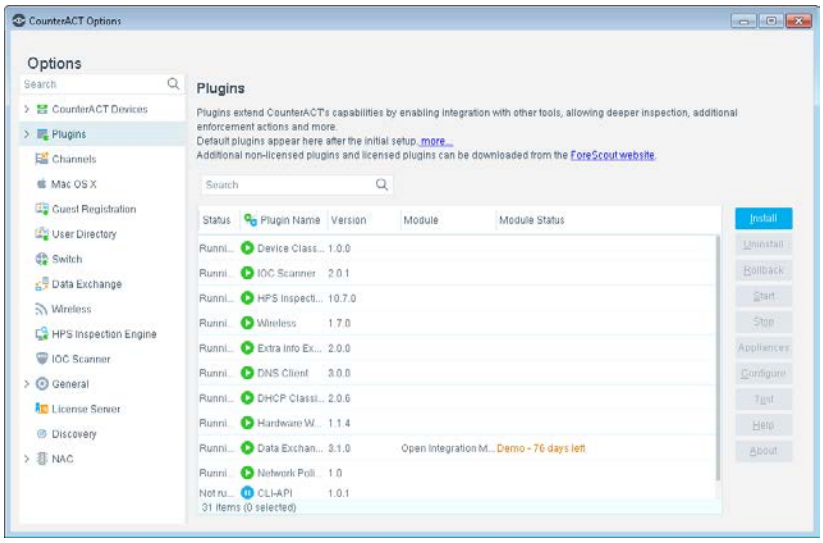
You can configure groups of Appliances with identical configuration for specific features. This ensures more streamlined configurations across the network. For details, see Configuring Features for an Appliance or Group of Appliances.

Viewing and Managing Plugin and Module Assignments per Folder

You can quickly view all CounterACT devices that have installed a specific plugin or module. Management tasks, for example, Start, Stop, Rollback and Configure, can also be performed from this dialog box.

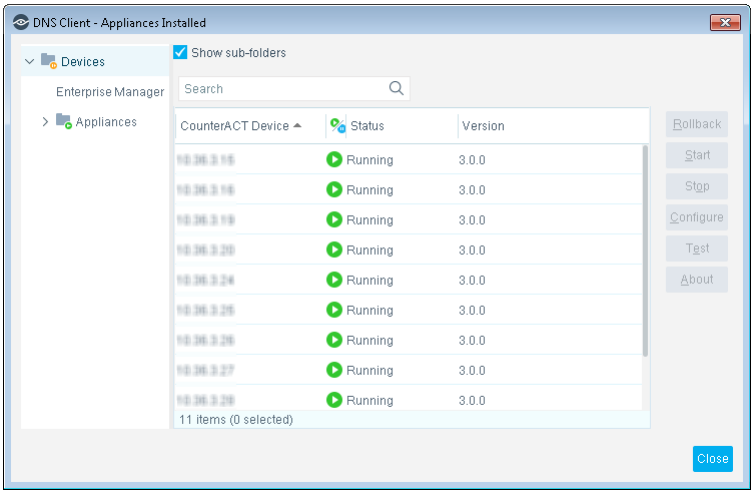
To work with assignments on a folder basis:

1. Select **Options** from the **Tools** menu and then select **Modules**.



Options>Modules

2. Double-click the Content Module of interest, or expand a module and double-click the plugin of interest.



Manage Assignments

3. From the left pane navigate to and select the Appliance, folder or Enterprise Manager to display the list of devices on which the plugin or module is installed.
4. Select **Close** to close the dialog box.

Appliance Endpoint Performance Capacity

Each Appliance has a set number of endpoints allotted to the Appliance. 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 CounterACT 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, CounterACT licenses also have a *license endpoint capacity* which defines how many endpoints your Appliance (Per-Appliance Licensing Mode) or deployment (Centralized Licensing Mode) is allowed to handle. See About License Management for more details.

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 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 then select the Channels tab.

If they were not defined via the wizard, you should define them here. See Adding Channels for more information.

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.

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.

About 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.

Adding Channels

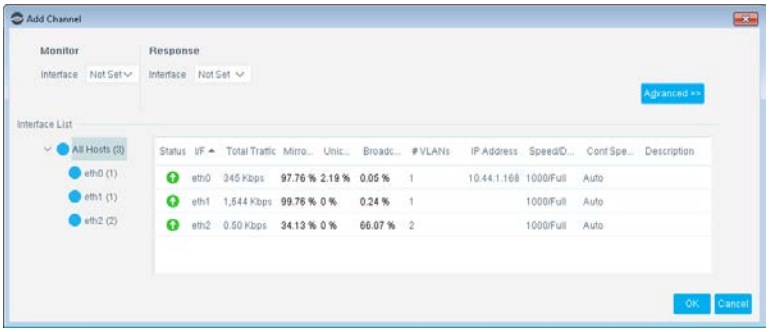
It is recommended that you create channels to match Appliance interface connections to monitor and respond to traffic on network interfaces.

To add channels:

1. Select **Options** from the **Tools** menu and then select **Channels**.
2. Use the **Select Appliance** drop-down list to select the Appliance to which you want to add channels. If you already defined channels from the Initial Setup wizard, the pane displays channels and related traffic detected on the Appliance.

Channels Pane

3. Select the **Channel** drop-down list and then select **Add**. The Add Channel dialog box opens.



Add Channel Dialog Box, Basic Setup

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 being seen on interfaces to which you connected in the Data Center, for example, if traffic is actually mirrored. If you change monitoring 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 read just 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)	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 allows you to 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	VLAN number.
IP Address	Interface IP address.
Speed Duplex	Current speed and whether the interface is automatic or full or half duplex.
Conf Speed/Duplex	Configured speed and whether the interface is automatic or full or half duplex.
Description	Interface description.

Troubleshooting alerts appear at the bottom of the dialog box if traffic detection is exceptionally low or high.

4. Select the **Monitor** drop-down list and assign the interface connected in the Data Center to a mirroring port.
5. Select the **Response** drop-down list and assign the interface connected in the Data Center.
6. Select **OK**. The Channels pane displays the channel setup that you defined. Alternatively, select **Advanced** to modify VLAN tagging definitions. See Customizing VLAN Tagging Definitions.

Channels Manager

The dialog box contains the following information:

Enabled (checkbox)	Activates the channel configuration. Monitoring and response activity will not function until you select **Apply** from the Channels pane.
Monitor Interface Information	
Monitor VLAN	Displays 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)	Displays total VLAN traffic detected on the monitored interface.
Mirrored Traffic	Displays 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	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 (Bps)	Displays 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	Response interface 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, CounterACT will not be able to respond to ARP requests. In this case, manually define the address. Addresses are defined per VLAN, if required. See Manually Adding a VLAN for more information.

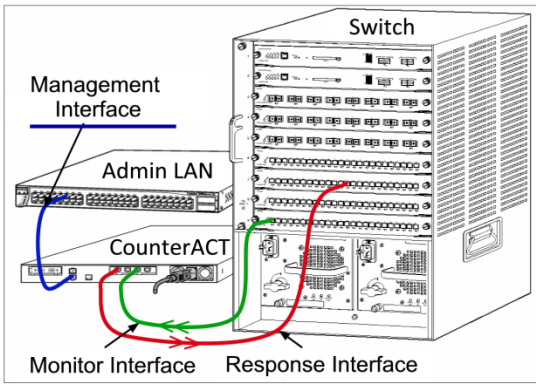
7. Select **Use DHCP by Default** if a DHCP address is used by CounterACT for monitored traffic. Clear **Use DHCP by Default** to manually configure the IP address.
8. Select the **Enabled** checkbox for each VLAN that you want to activate.
9. Select **Apply**. A Symmetric and Response test is performed. If the test fails, you can review related troubleshooting information at the bottom of the dialog box.

Customizing 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.

Appliance Management Interface VLAN Tagging Requirements

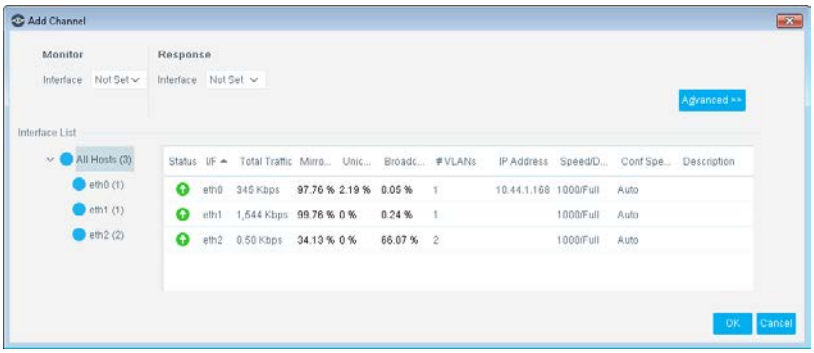
The Appliance Management interface should be untagged.



Management Interface

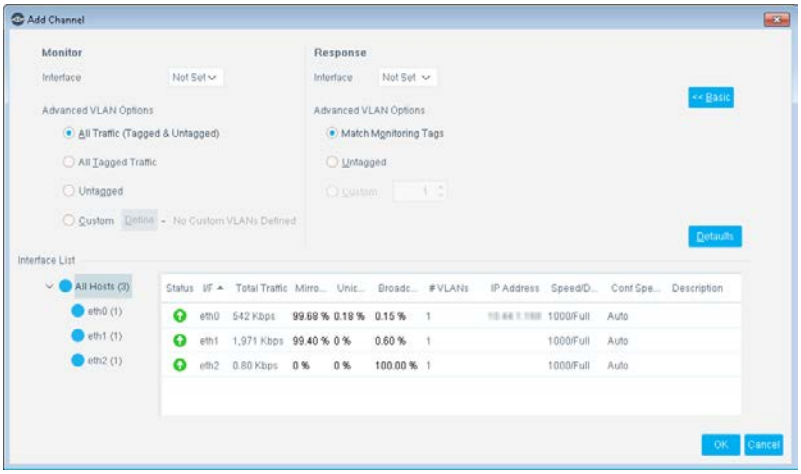
To customize:

1. Select **Options** from the **Tools** menu and then select **Channels**.
2. Select the **Channel** drop-down list and then select **Add**. The basic Add Channel dialog box opens.



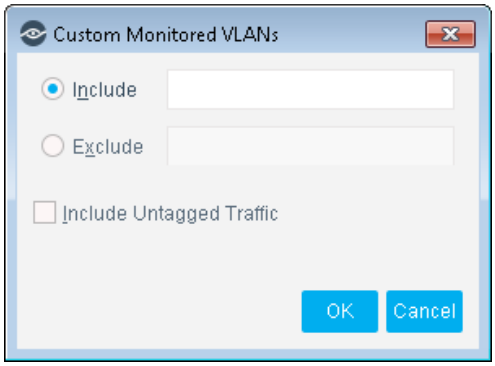
Basic Add Channel Dialog Box

3. Using the **Monitor** and **Response** drop-down lists, define the channel monitor and response settings and then select **Advanced**. The advanced Add Channel dialog box opens.



Advanced Add Channels Dialog Box

4. In the Monitor – Advanced VLAN Options section:
   - 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.



Custom Monitored VLANs

5. In the Response – Advanced VLAN Options section:
   - Select Match Monitoring Tags to send response packets with VLAN IDs identical to the IDs of the monitoring packet that triggered the response. Use 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 which 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 CounterACT to detect scans aimed at the IP addresses included in the monitored subnet. This limitation does not apply when traffic between two routers is being monitored.
6. Select **OK**. The Add Channel dialog box closes.
7. Select **Apply** to activate the configuration.

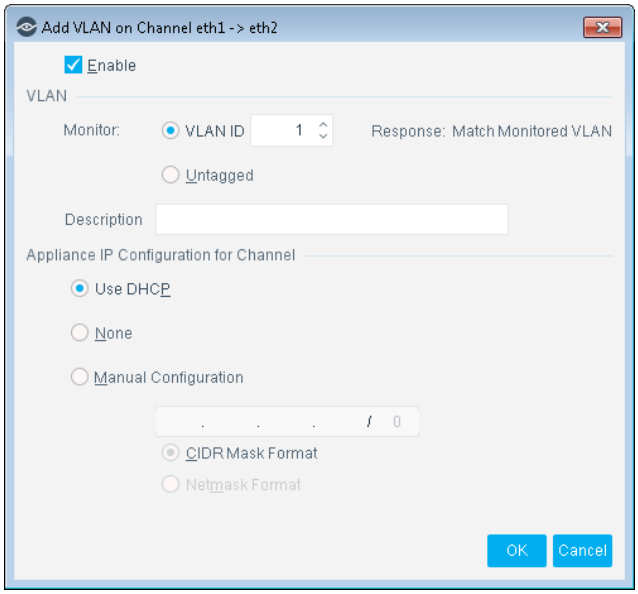
Manually Adding a VLAN

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 **Options** from the **Tools** menu and then select **Channels**.
2. Use the **Select Appliance** drop-down list to select the Appliance to which you want to add a VLAN. The Appliance channel list is displayed in the Channels pane.
3. From the **VLAN** drop-down list select **Add**. The Add VLAN on Channel dialog box opens.



Add VLAN on Channel Dialog Box

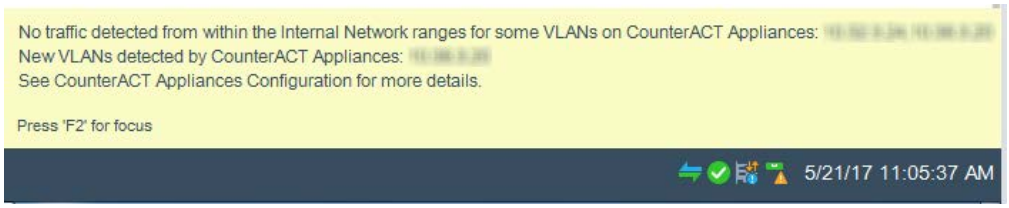
4. Configure the VLAN settings and select **OK**.

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.



Indicator and Tooltip

802.1ad and 802.1QinQ VLAN Tag Termination Traffic

You can configure CounterACT to identify 802.1ad and 802.1QinQ VLAN Tag Termination traffic. Identifying this traffic expands VLAN discovery, provides increased visibility and enables CounterACT 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:

1. 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`
2. Run the following command:

   `fstool service restart`

To disable identifying 802.1ad and 802.1QinQ VLAN Tag Termination traffic:

1. Run the following commands:

   `fstool set_property engine.conf.params.VlanQStacking 0`

   `fstool service restart`

Viewing Information about CounterACT Devices

To view and edit information about a CounterACT device:

1. Select **Options** from the **Tools** menu.
2. Select the CounterACT device in the CounterACT Devices pane for which you require information. The Status section opens beneath the listing of all devices.
3. Double-click the CounterACT device to open the Host Details dialog box. Alternately, you can select **Edit** in the CounterACT Devices pane.

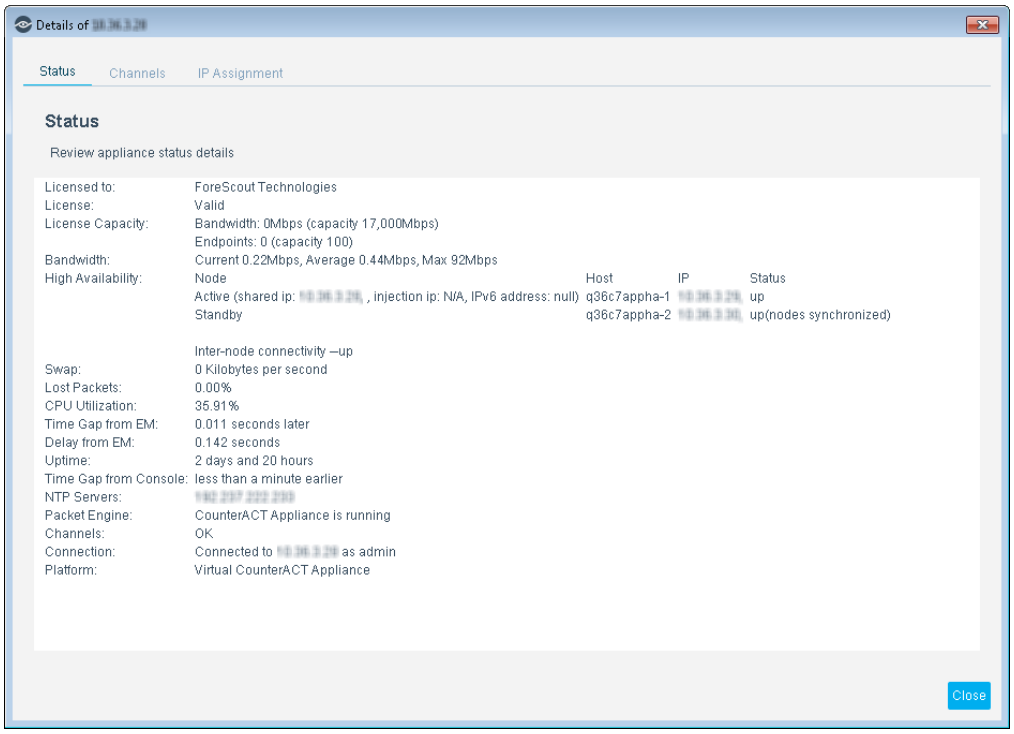
This section describes the tabs of the Host Details dialog box.

Status Tab

You can view at-a-glance system health information about Appliances using this tab.

Information about Appliance health is displayed in a tooltip that opens when you hover over a specific Appliance in the Status column of the CounterACT Appliances pane. Icons summarize the Appliance status in the Status column. Appliance health information is also displayed in the Status tab when you double-click an Appliance or when you select **Edit** in the CounterACT Devices pane.

If the status of any item in the Status section is acceptable and does not require special attention, it is shown in black. Alerts are shown in orange, and error messages in red.



System Health Information

Information displayed is useful for troubleshooting. Entries in red may require your special attention.

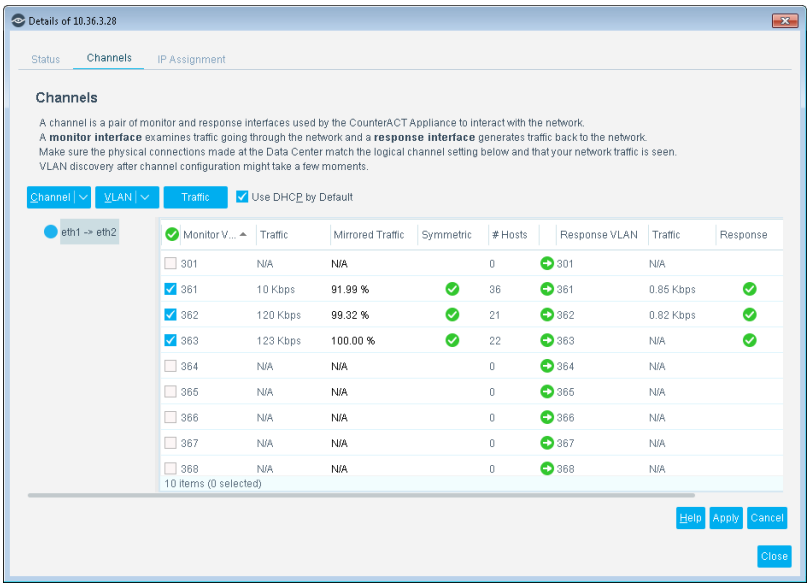
The following information is displayed about the Appliance status.

Item	Description
License	The validity of a license, and the time remaining to expiration, if applicable.
Capacity	The bandwidth and number of endpoints per Appliance.
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. Refer to the *ForeScout CounterACT Resiliency Solutions User Guide* for more information about High Availability. See Additional CounterACT Documentation for information on how to access this guide.

Item	Description
Swap	Indicates whether the swap exceeded 100 kilobytes per second consecutively in the last one 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 Appliance with a new Appliance that has more physical memory.
Lost Packets	Indicates whether the Appliance engine experienced on an average more than a 10% packet loss in the last one minute. Packet loss is displayed in 10% accuracy blocks, i.e., 0% is 0-10, 10% is 10-20, and so on. **OK** 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 this issue, upgrade the Appliance or configure the channels to monitor less traffic.
CPU Utilization	Indicates the percentage of actual CPU Utilization. If the value is high, contact your ForeScout representative.

Channels Tab

Entries in the Channels tab indicate the logical setup and traffic between the monitor and response interfaces that the CounterACT Appliance uses to interact with the network.



Appliance Channel Details

Alerts on specific channels where traffic problems have been detected are shown at the bottom of the Channels pane.

To modify the listings and monitor traffic:

1. Select **Channel** to add, edit or remove channel listings.
2. Select **VLAN** to add a single VLAN listing, or to perform actions on all VLANs listed including remove, enable and disable.

3. Use **Traffic** to view traffic being monitored by a specific interface.

For details about how to work with channels, see Working with Appliance Channel Assignments.

Fingerprint Tab

The Appliance fingerprint allows you to 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 CounterACT device to verify.

Appliance Fingerprint

To verify the fingerprint:

1. Log in to the CounterACT device CLI.
2. Run the following command:

   `fstool key`

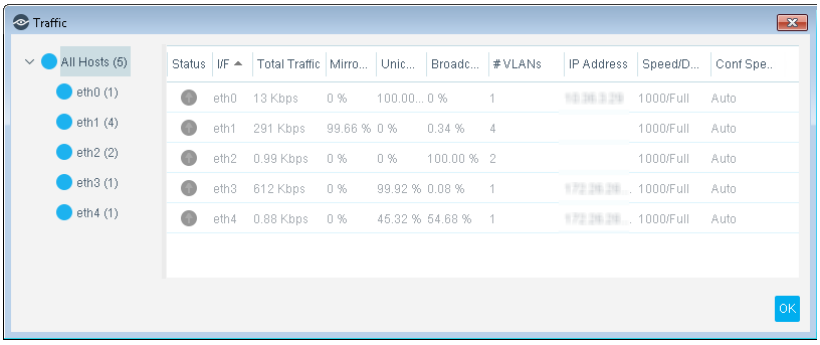
3. Verify that the output of the command matches the value displayed in the Fingerprint tab.

Viewing Appliance Traffic Statistics

View dynamic network traffic information about the Appliances in your enterprise.

To view traffic:

1. Select **Options** from the **Tools** menu.
2. Right-click an Appliance from the Devices pane and select **Traffic**. The Traffic dialog box opens.

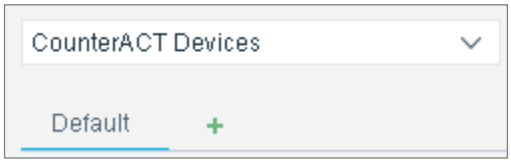


For more information about Appliance traffic see Adding Channels.

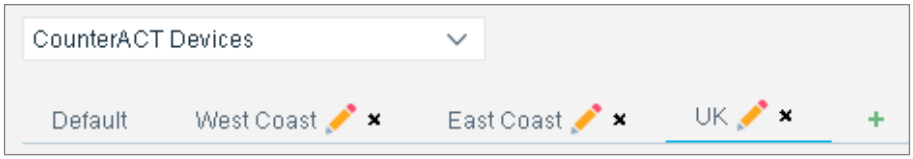
Configuring Features for an Appliance or Group of Appliances

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.

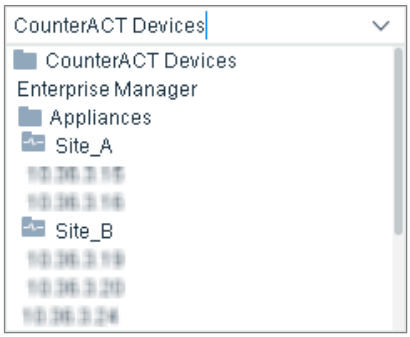


In the following example, additional tabs have been added, with separate configurations for regional groups of Appliances.



Use the following controls to create and manage configurations:

- Select the Plus-sign tab to create a new 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.



Apply Uniform Configuration Settings to All Appliances

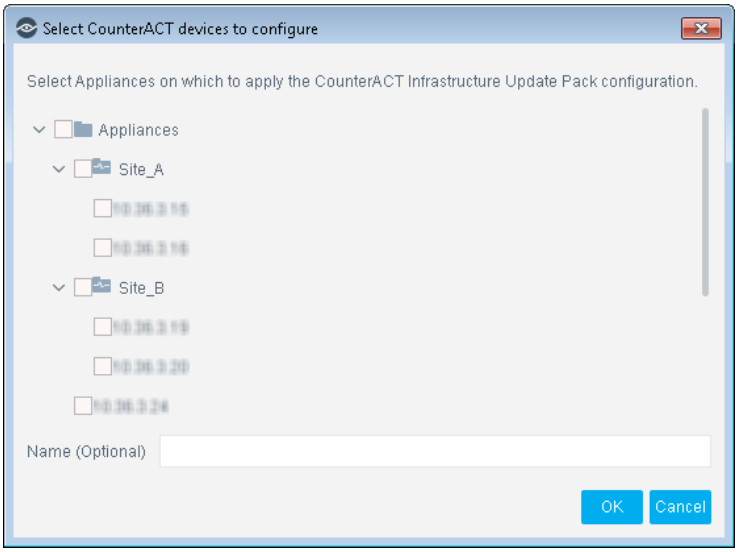
The settings of the Default tab apply to all CounterACT devices that are not included in other configurations. If you do not create other configurations, these settings apply to all CounterACT devices. Settings for the Enterprise Manager are defined only in the Default tab. As a result, the Enterprise Manager is not available when you define a new tab for configuration settings.

Define a Configuration for a Single Device or Group of Devices

Use this procedure to define configuration settings that apply to a specified CounterACT device or group of devices.

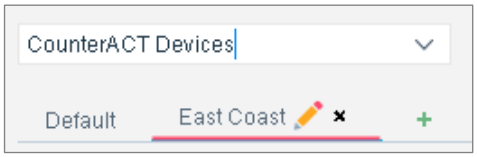
To create a separate configuration for a device or group of devices:

1. Select the Plus-sign tab. The Select CounterACT devices to configure dialog box opens.



Select devices to configure

2. Select the CounterACT devices to which these configuration settings will apply.
3. (Optional) Specify a text label for this configuration instance in the **Name (Optional)** field.
4. Select **OK**. A new tab appears in the pane.



Configuration settings you define while this tab is selected apply *only* to the CounterACT devices you selected in step 2.

Editing and Updating a Configuration

Use the **Edit** and **Delete** icons to update a configuration.

To modify the scope of configuration settings:

1. Select the Edit icon on a tab. The Edit devices to configure dialog box opens.
2. Edit the devices to which these configuration settings apply:
   - Select devices to add to the configuration.
   - Clear selected devices to remove them from the configuration.
3. (Optional) Modify the text label of the configuration.
4. Select **OK** to save changes to the configuration.

To delete a configuration:

1. Select the Delete icon ***x*** on a tab.
2. Select **Yes** to confirm deletion.

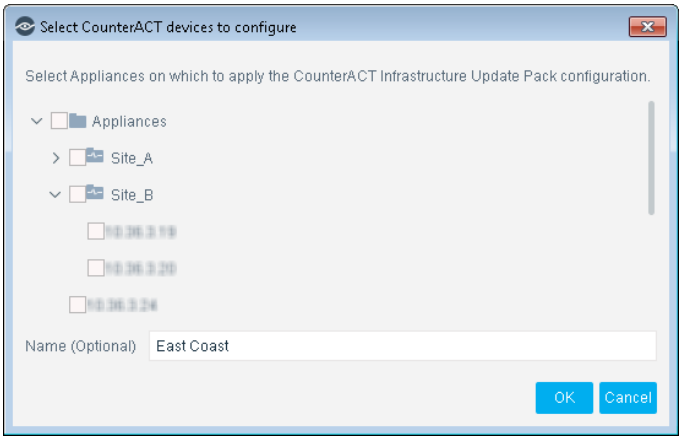
   The configuration tab is removed from the pane.

Settings of the Default tab apply to all devices that were in the scope of the deleted configuration.

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.



Select Appliances

Scope definitions are made by CounterACT administrators for the purpose of granting and limiting user access to specific endpoints or segments in the network. *Scope* definitions are configured in the Console Users pane. To access the pane, select **Options** from the **Tools** menu and then select **Console User Profile**.

Viewing Limitations

Certain Appliances that you want to view may contain endpoint IP address assignments that are not in your *Scope*. When this happens, you may not be able to view the Appliance configuration and change it.

Appliances that contain endpoint IP address assignments partially out of your *Scope* will appear with a red circle and line through it.

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 list.

Scope definitions are made by CounterACT administrators for the purpose of granting and limiting user access to specific endpoints or segments in the network. *Scope* definitions are configured in the Console Users pane. To access the pane, select **Options** from the **Tools** menu and then select **Console User Profiles**.

Controlling Command-line Access to CounterACT Devices

CounterACT 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.

The user accounts defined at the CLI level are not related to Console users.

The following tools support more secure management of CLI level access.

- Configure Session Security Features for Command-Line Interaction
- Configure Password Protection for the Boot Loader

Configure Session Security Features for Command-Line Interaction

Define audit log file properties and other security features that apply when users log in to CounterACT devices through the command-line interface. By default, logs report general operations related to, for example, some of the following activities:

- User login
- Stopping or starting CounterACT

You can configure CounterACT devices to monitor additional audit events that can be used to help discover violations of security policies used on your system (**`os.enable.audit.rules`** property). These additional audit events relate to, for example, some of the following activities:

- Service requests

- File modification
- Time modification
- Permission changes

To configure security features for command-line interaction:

1. Log in to the CounterACT device CLI and run the **`fstool set_property`** command followed by the relevant property from the table below:

Property	Description
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.value	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.value	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*, CounterACT 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 after the device is rebooted. This property will only be enforced if **`os.enable.audit.rules`** is set to *True*.

2. After setting one or more of the properties above, run the following command:

   `fstool os_security config`

Configure Password Protection for the Boot Loader

CounterACT 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.

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:

1. Log in to the CounterACT device CLI.
2. Submit the following command:

   `fstool grub –setpassword`
3. The following prompt appears:

   `Enter grub password:`
4. Enter the password. The following prompt appears:

   `Re-type grub password:`
5. Re-enter the password. The following prompt appears:

   `Successfully updated grub password.`

The system prompts for this password when users try to edit boot loader settings.

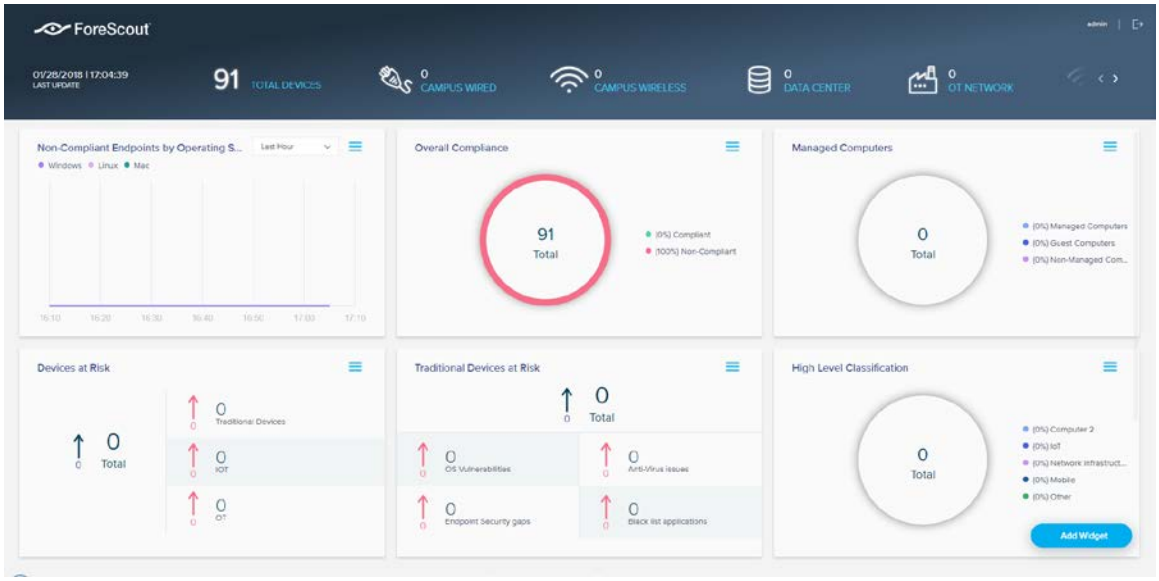
Chapter 16: The Dashboard

- About the Dashboard
- Accessing the Dashboard
- What You See in the Dashboard
- Before You Begin
- Working with Dashboard Widgets
- Dashboard Feature Updates

About the Dashboard

The Dashboard is a web-based information center that delivers dynamic at-a-glance information about:

- Device compliance
- Device classification
- Device management status
- Network overview



The dashboard is designed for corporate executives who want a quick overview of important network activities, and for security administrators that would like to easily monitor their security state. This information is collected from CounterACT policies and is periodically updated as endpoints are monitored and controlled by CounterACT.

Accessing the Dashboard

Two methods are available for accessing the Dashboard.

- Login from the Console.
- Login from a web browser (requires authentication).

To access the Dashboard from the Console:

1. Select the **Ellipsis icon** ••• from the **Toolbar**, and select **Dashboard** from the dropdown menu. The Dashboard opens in a new browser window.

To access the Dashboard from a web browser:

1. Browse to the following URL: *http://<Device_IP>/board*. Where *<Device_IP>* is the IP address of the Enterprise Manager or an Appliance. A login page opens.

2. Enter the User Name and Password of a user that can access the dashboard. Typically the credentials you use to access the Console also grant access to the dashboard. For more information, see Log in to Each CounterACT Web-Based Portal.

What You See in the Dashboard

The default Dashboard installation provides the following of information:

- Network Overview
- Compliance Trends
- Classification Status
- Computer Manageability

Network Overview

The Discovery Bar of the Dashboard displays a summary of the total numbers of endpoints and devices in each of the monitored categories:

- Total Devices
- Campus Wired
- Campus Wireless
- Data Center
- OT Network

Compliance Trends

The Compliance widgets provide a picture of the compliance status and trends on your network.

- Non-Compliant Endpoints by Operating System - dynamic, changes over time
- Overall Non-Compliant Endpoints - dynamic, changes over time
- Overall Compliance - static display of total numbers

Classification Status

There are two widgets available that provide the classification status of devices on your network.

- High Level Classification
- IoT Classification

Computer Manageability

The Computer Manageability widget provides information about managed computers, guest computers, and non-managed computers that are connected to your network.

Dashboard Layout

This section provides an overview of the Dashboard layout.

Dashboard

Discovery Bar

The Discovery bar contains the following information

Item	Description
Last Updated	Displays the last time the data was polled and updated. The timestamp is presented in USA time format (mm/dd/yyyy | hh:MM:ss). The default update interval is 5 minutes.
Total Devices	The total number of detected devices.
Campus Wired	The number of wired devices detected on the network.
Campus Wireless	The number of wireless devices detected on the network.
Data Center	The number of devices detected in your data center.
OT Network	The number of detected Operational Technology devices.

To change the update interval of the Dashboard, use the CLI command fstool set_property to change the interval (in seconds) in the dashboard.portal.polling.time.seconds property.

To change the Last Updated time format, use the CLI command fstool set_property to change the dashboard.portal.date.format property.

Dashboard Widgets

Each widget in the dashboard displays a donut chart, a trend chart, or a counter chart with statistics that are collected from CounterACT policies. The policies provide the number of hosts that are compliant, their classification function, and changes over time in the number of hosts that are compliant.

Dashboard widgets provide information about:

Item	Description
High Level Classification	General classification of devices according to the following categories - Computer, IoT, Network Infrastructure, Mobile, Other
Non-Compliant Endpoints by Operating System	Non-compliant devices on the network, according to the operating system they are running - Windows, Linux, Mac
Overall Non-Compliant Endpoints	A general view of non-compliant devices in the network
Overall Compliance	Compliant or non-compliant devices in the network
IoT Classification	Classification of device types according to the following categories - Printers, VoIP, Wearables, Healthcare, Surveillance, Building Automation, Other
Computer Manageability	Managed Computers, Guest Computers, or Non Managed Computers on the network

Before You Begin

The following tasks should be performed before working with the dashboard.

- Enable JavaScript in browsers that are running the dashboard.
- Run the Dashboard Policy Template

How the Dashboard is Populated

To begin populating reports in the Dashboard, verify that you are running a set of basic policy templates that retrieve the compliance statistics, classification results and managed device properties from your network. The default set of Dashboard policies is installed with CounterACT, but needs to be activated by Run the Dashboard Policy Template.

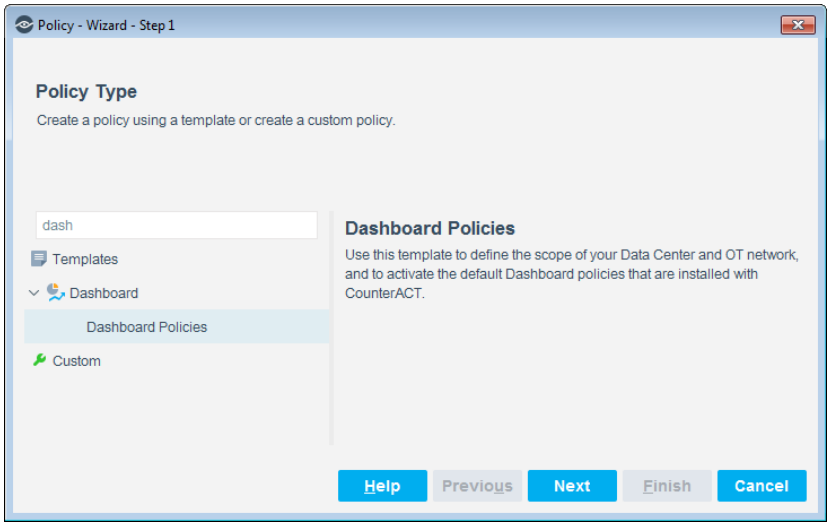
If you are monitoring Data Center or Operational Technology statistics in your network, you need to define the IP range scope for your *Data Center* and *OT Network* in the Dashboard policy template.

Run the Dashboard Policy Template

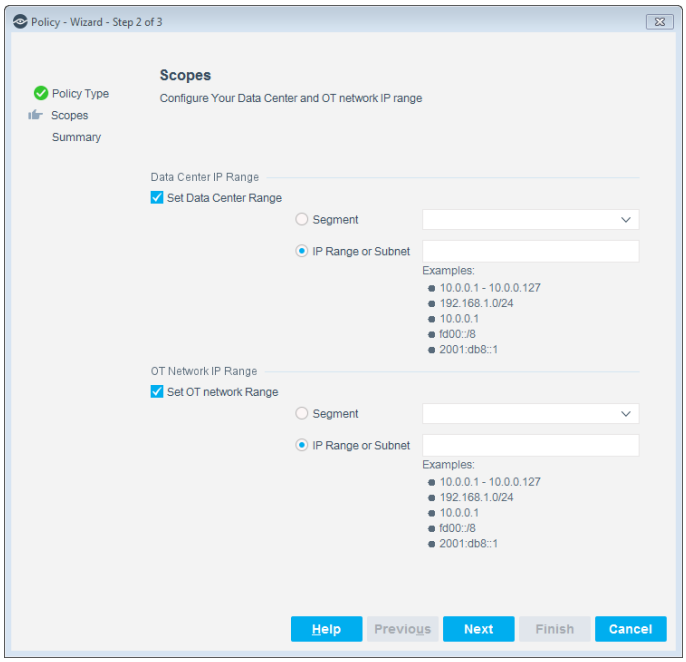
Use the Dashboard policy template to activate the default Dashboard policies, and to configure the IP scope for your Data Center and OT Network.

To run the template:

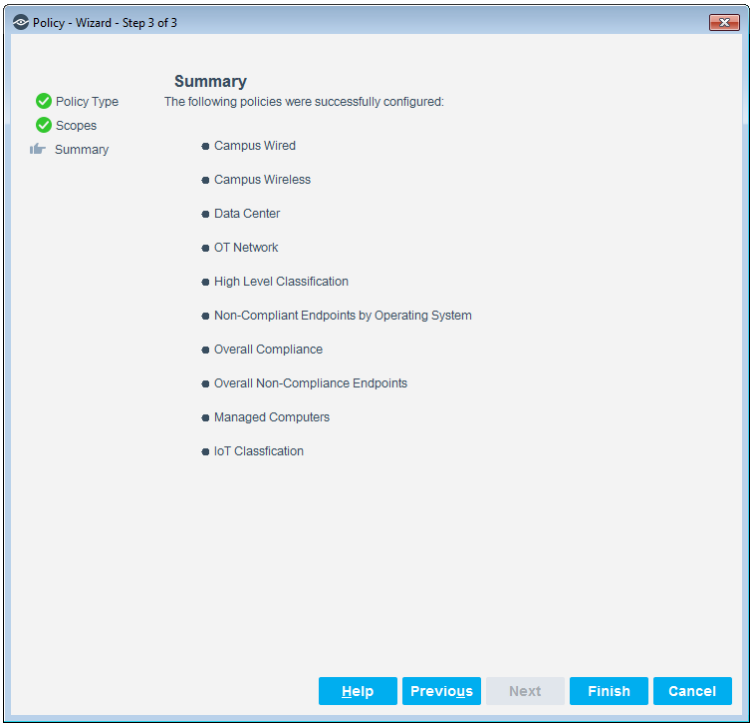
1. Log in to the CounterACT Console and select the **Policy** tab.
2. Create a new folder to hold the default Dashboard policies.
3. Select **Add** from the Policy Manager. The Policy Wizard opens.
4. Expand the **Dashboard** folder, and select **Dashboard policies**. The **Dashboard policies** pane opens.



5. Select **Next.** The **Scopes** pane opens.



6. Use the Set Data Center Range and Set OT network Range options to define which endpoints are inspected. The following options are available for defining the scope:
   - **Segment**: Select a previously defined segment of the network.
   - **IP Range or Subnet**: Define a range of IP addresses or a Subnet.
7. Select **Next**. The **Summary** pane opens, displaying a summary of the policies that have been activated.



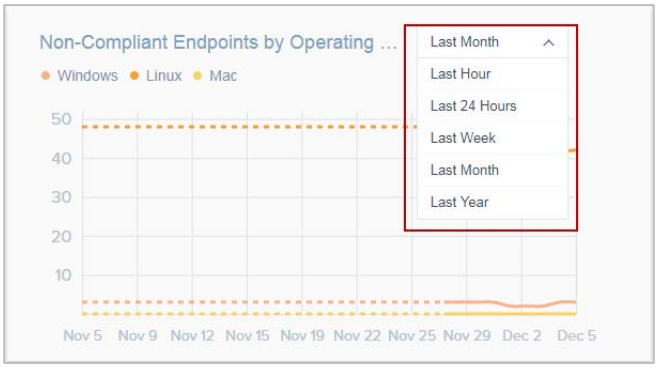
8. Select **Finish** to save the policy settings.

Working with Dashboard Widgets

This section describes how to create and work with Dashboard widgets.

- Selecting the Reporting Interval
- Expanding a Widget
- Adding a Widget

Selecting the Reporting Interval



To select a reporting interval

1. Select the drop down menu and select a reporting interval.

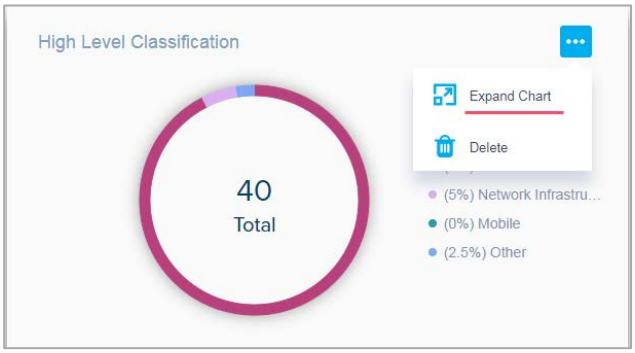
2. The chart refreshes the display to include data from the selected interval.

Expanding a Widget

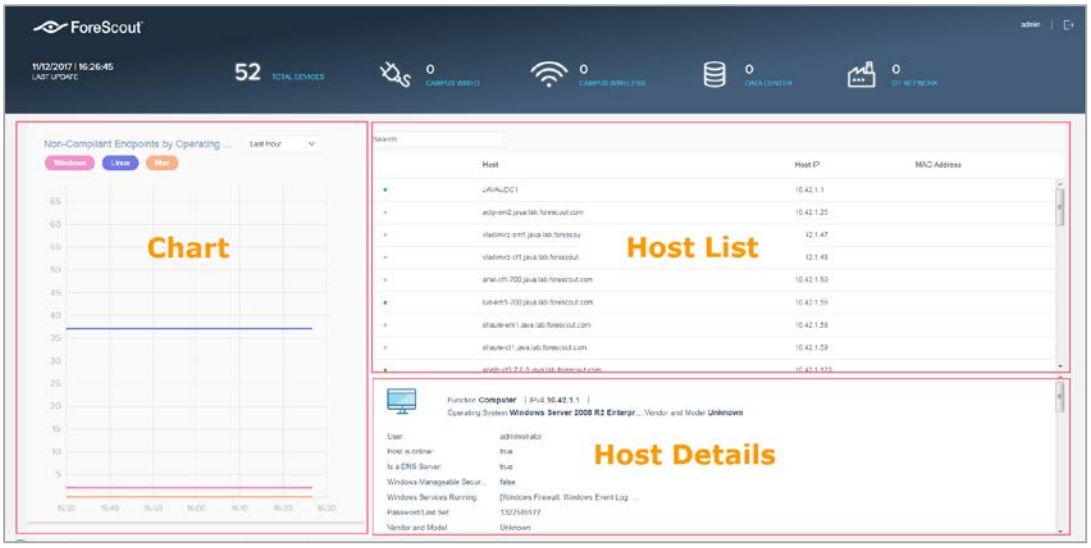
When you expand a widget to full screen size, the expanded view provides additional information in the **Host List** pane and **Host Details** pane.

To expand a widget and display it in full screen mode:

1. Click anywhere in the chart, or select the **Ellipsis icon** ••• in the widget, and select **Expand Chart** from the dropdown menu.



2. The widget is displayed in full screen mode, with two additional information panes displayed, the **Host List** and the **Host Details**.



3. Expanded widgets display the following information:

- **Chart** - an enlarged view of the chart, with buttons corresponding to each sub-rule displayed at the top of the chart. Selecting the sub-rule buttons determines what data is displayed in the expanded chart.

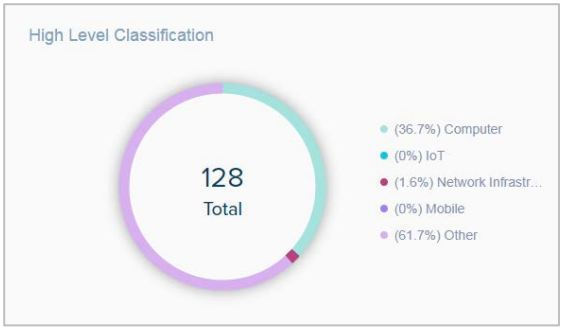
- **Host List** - Displays a list of the individual endpoints detected by CounterACT that are represented in the chart. The properties displayed are host name, IP Address, network segment, MAC Address, and network function. The Search box at the top of the pane allows you to search the Host List for specific entries.
- **Host Details** - Displays the detailed properties for a host selected in the Host List.

4. To return to the regular view, select the *collapse chart* icon in the upper left corner of the expanded widget.

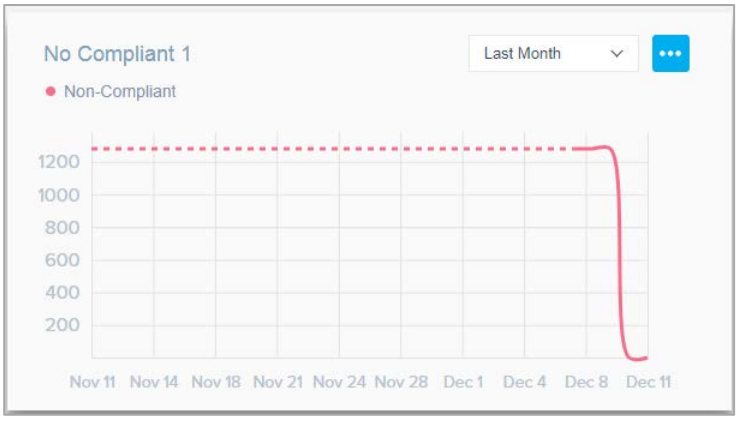
Adding a Widget

The Widget Builder wizard allows you to add new widgets that are customized according to the specific information you want to see in the Dashboard. The wizard allows you to select any policy that you defined in CounterACT. Each widget provides a chart presented in one of three Widget Types:

- Donut - a circular chart that displays the total number and the relative percentages of each property matched in the sub rule, according to the policies selected in this widget.

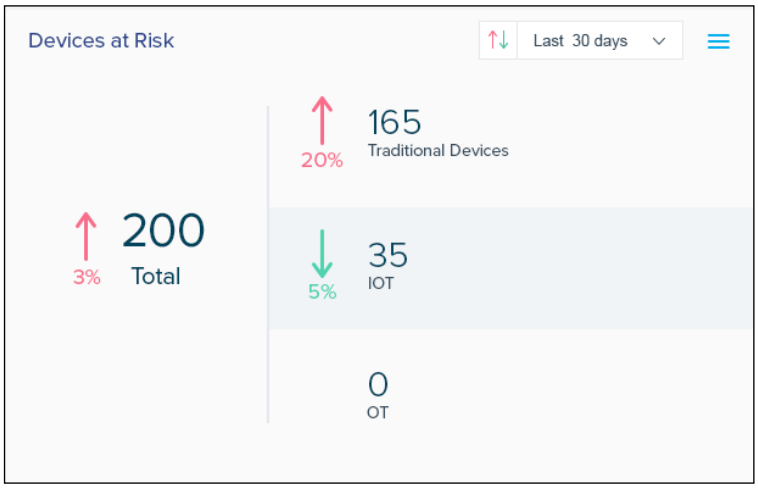


- Trend - a graph that displays the number of devices that match the sub rules over time according to the policies selected in this widget.



When you hover with the mouse pointer over the trend chart, a tooltip displays the number value of that point in the chart.

- Counter - a widget that displays the number of devices that match the policy sub rules, according to the policy selected for this widget. Up to four counters can be included in each Counter widget.

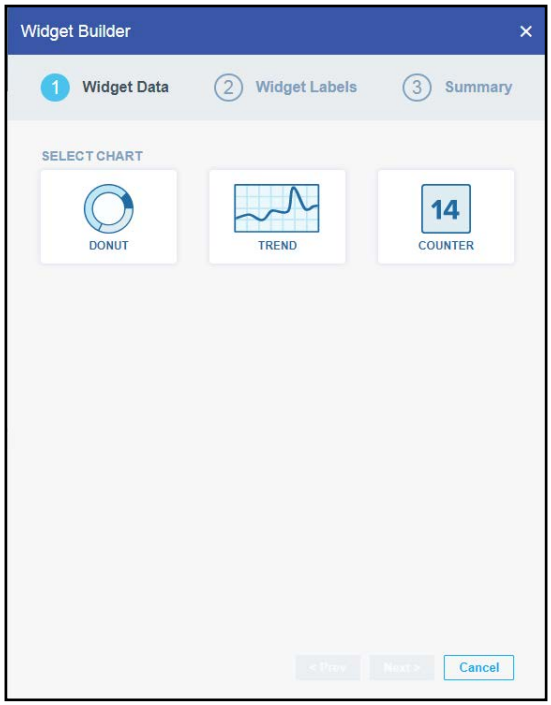


To create report widgets that accurately reflect the data you want to see in the Dashboard, you should understand how CounterACT policies and other basic features work.

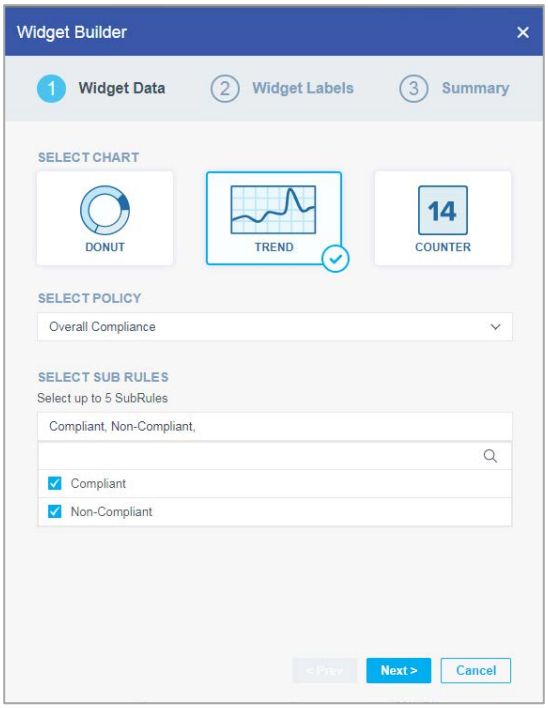
To add a new widget:

1. At the lower right corner of the screen, select **Add Widget**

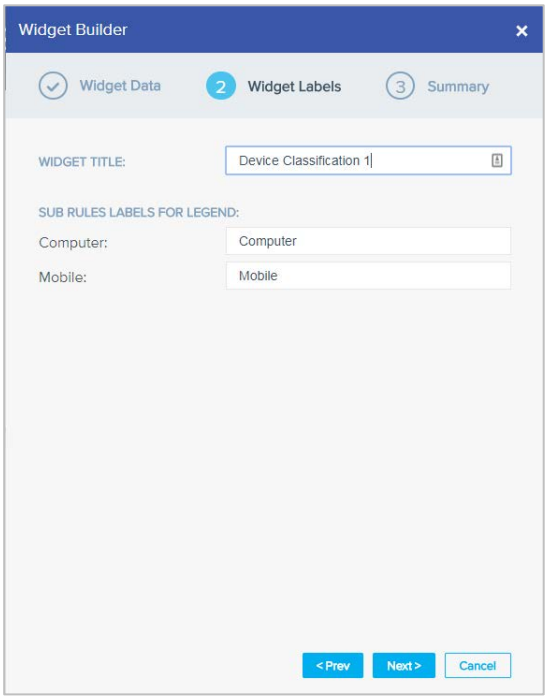
. The **Widget Builder** wizard opens.



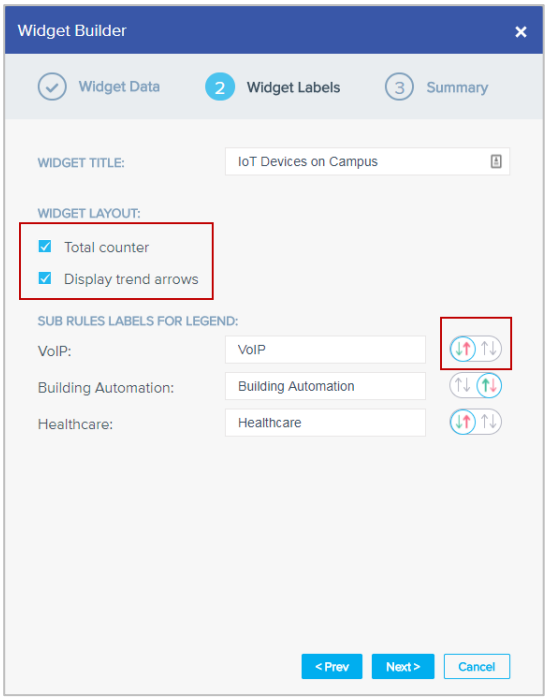
2. Select the chart type you want to use: *donut*, *trend*, or *counter*.
3. Select a Policy and Sub Rules to populate the chart, and select **Next**.



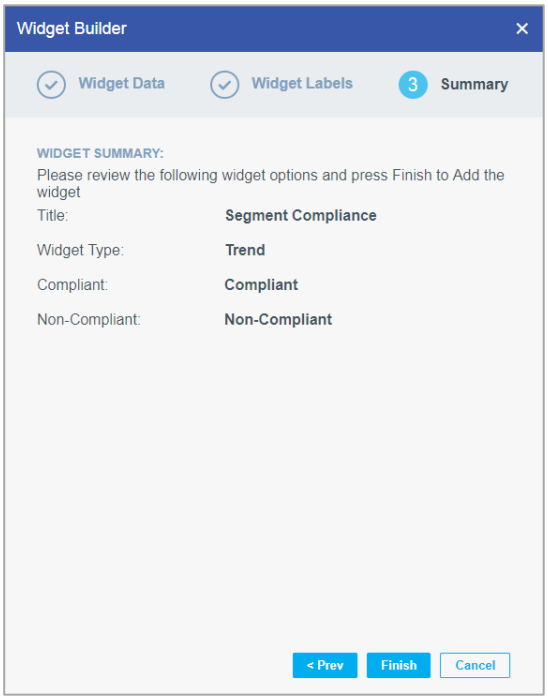
4. Enter a title for the new widget, and select **Next**.



5. If you are adding a Counter widget, select the Widget Layout options and the trend arrow directions for each sub-rule, and select **Next**.



6. A summary of the selected widget options is displayed. Select **Finish** to complete the new widget creation. The new widget is placed in the next available spot in the Dashboard screen.



When you add a number of widgets to the Dashboard screen, each new widget is placed in the next available spot at the bottom of the screen. A scroll bar appears on the right side to allow you to scroll up or down and view the additional widgets.

Dashboard Feature Updates

The Dashboard is delivered through the Web GUI plugin, a component of the CounterACT Core Extensions Module. Periodic updates to the Dashboard are delivered whenever the Module is updated.

Chapter 17: License Management

- About License Management
- Centralized Licensing Mode
- Per-Appliance Licensing Mode
- Switch Licensing Mode from Per-Appliance to Centralized
- Receiving License Alerts

About License Management

CounterACT version 8.0 supports two different licensing modes:

- Centralized Licensing Mode
- Per-Appliance Licensing Mode

This guide includes documentation for working with Per-Appliance Licensing Mode. Refer to the ForeScout Centralized Licensing How-to Guide *for information on how to work with Centralized Licensing Mode.*

Each CounterACT deployment operates in one of the two modes. You may have multiple deployments that use different licensing modes. License requirements differ according to the licensing mode activated on your deployment.

The following table describes each mode and lists the components/features that need to be licensed.

Licensing Mode	Description	What needs to be licensed?
Centralized Licensing Mode (Refer to the *ForeScout Centralized Licensing How-to Guide* for more information)	▪ Licenses are activated centrally on the Enterprise Manager or Standalone Appliance. ▪ License endpoint capacity is calculated per-*deployment*; you can distribute this capacity across Appliances as you see fit. ▪ Extended Modules are acquired separately and with an associated endpoint count. Extended Modules: Individual Modules are supported. Integration Modules: Multiple Modules are not supported.	▪ Each licensed feature and Extended Module per deployment. Licensed features enable specific capabilities in CounterACT (*See*, *Control*, *Resiliency*, *Extended Modules*).

Licensing Mode	Description	What needs to be licensed?
Per-Appliance Licensing Mode	▪ Licenses are activated separately on the Enterprise Manager and on each Appliance in the deployment. ▪ License endpoint capacity is calculated per-*Appliance*; each Appliance license includes a specific number of endpoints that the Appliance can handle. ▪ Extended Modules are acquired separately and with an associated endpoint count. Extended Modules: Individual Modules and Integration Modules: Multiple Modules are supported.	▪ Each Appliance and Enterprise Manager in your deployment. See Per-Appliance CounterACT Device License. ▪ Each Extended Module. See Per-Appliance Extended Module License.

Default Licensing Modes in CounterACT

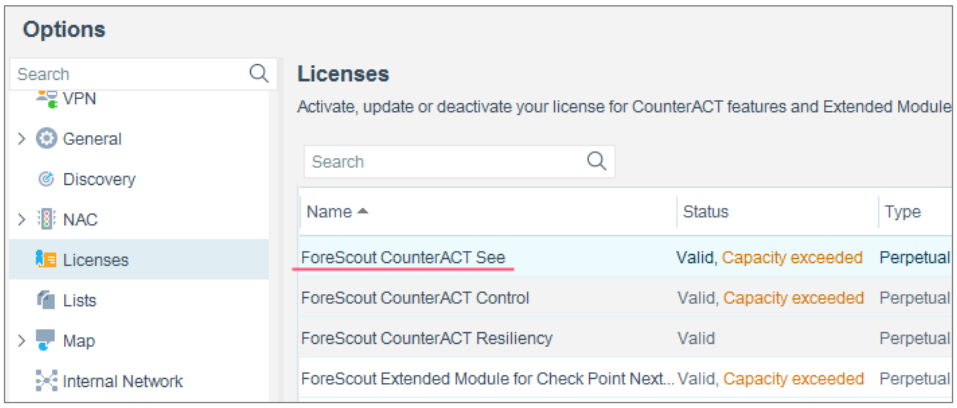
The following table describes the default licensing modes in use based on the version of CounterACT that you are using.

CounterACT Version	Licensing Mode	Notes
All releases prior to version 8.0	Per-Appliance Licensing Mode	If you upgrade to CounterACT version 8.0, you can choose to switch to Centralized Licensing Mode. *Contact ForeScout Support or your ForeScout representative for more information on how to switch licensing modes. See* Switch Licensing Mode from Per-Appliance to Centralized*.*
CounterACT version 8.0 (*Upgrade from previous version*)	Per-Appliance Licensing Mode	All license information is retained after upgrade. You can switch to Centralized Licensing Mode. *Contact ForeScout Support or your ForeScout representative for more information on how to switch licensing modes. See* Switch Licensing Mode from Per-Appliance to Centralized*.*
CounterACT version 8.0 (*New installation*)	Licensing mode is determined during purchase.	You are asked to identify the predetermined licensing mode during initial installation and configuration of your CounterACT device. Refer to the *CounterACT Installation Guide* for information about CounterACT device installation and configuration.

Identifying Your Licensing Mode in the Console

If your Enterprise Manager has a *ForeScout CounterACT See* license listed in the Console, your deployment is operating in Centralized Licensing Mode. If not, your deployment is operating in Per-Appliance Licensing Mode.

Select **Options > Licenses** to see whether you have a *ForeScout CounterACT See* license listed in the table.



Contact your ForeScout representative if you have any questions about identifying your licensing mode.

Centralized Licensing Mode

Refer to the *ForeScout Centralized Licensing How-to Guide* for information on how to work with Centralized Licensing Mode. See Additional CounterACT Documentation for information on how to access this guide.

Per-Appliance Licensing Mode

If you are operating in Per-Appliance Licensing Mode, you must install a license for each Appliance and Enterprise Manager in your deployment as well as for each Extended Module.

- Per-Appliance CounterACT Device License
- Per-Appliance Extended Module License

Per-Appliance CounterACT Device License

The request and installation procedures, identical for all CounterACT devices, are described in this section. The following subjects are covered:

- Your Demo License
- Virtual Licenses
- Generating a License Request
- Viewing and Managing Your Requests

- Receiving Your License via the Web
- Receiving Your License via Email
- Saving Your Request to a File
- Viewing License Alerts

Your Demo License

During system installation, a demo license is automatically installed. Each demo license is valid for 30 days. During this period, you should receive a permanent license from ForeScout and place it in an accessible folder on your disk or network. Install the license from this location before the 30-day demo license expires or request to extend your demo license. If you did not receive your license, you can generate a request. See Generating a License Request for details about requesting an extension or a permanent license.

You are alerted that your demo license is about to expire as follows:

- Through periodic email reminders.
- Through an **Alert** icon (⚠) in the Status and License columns in the CounterACT Devices pane (accessible by selecting **Options** from the **Tools** menu), including the number of days remaining before license expiration.
- When you move your cursor over the Appliance entry in the CounterACT Devices pane.
- Through 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.

License Status Bar Alert

Virtual Licenses

This section provides information about virtual licenses and about connecting to the ForeScout License Server. Refer to the *CounterACT Installation Guide* for information about installing CounterACT virtual systems. See Additional CounterACT Documentation for information on how to access this guide.

Virtual Demo License (Virtual Machines)

After the Appliance installation, you should have installed a demo license provided by your ForeScout representative by email. The license can be installed during the initial Console setup using the Initial Setup wizard and is valid for 30 days from the time it was generated by the ForeScout representative. See License (CounterACT Virtual Systems Only, Per-Appliance Licensing Mode).

You must request and install a permanent license from the Console before the demo license expires. You can also request an extension to the demo license from this location.

If you skipped the virtual demo license installation at the Initial Setup wizard, you can generate a request from the Console. See Generating a License Request for details.

Virtual Permanent License

Before your demo license expires, you must install a permanent license. This license has an installation begin and end date. You must install the permanent license within these dates, which will be sent to you when the license is issued.

Virtual License Authorization

The demo and permanent license are authorized daily by the ForeScout License Server.

Communication with ForeScout's License Server is performed by one CounterACT device, which has access to all other CounterACT devices. This is required so that one device can perform the authentication for all the devices. The first device that has connectivity is used for the communication. If there are no communication problems, the first on the list will usually be used for performing the communication with ForeScout License server for all devices in the network. You should expect daily traffic from that device equivalent to the number of VM devices installed.

Licenses that cannot be authorized for a month will be revoked. When this happens, significant CounterACT functionality will stop. You will be contacted via email regarding the expiration date and violations. In addition, license alerts, violations, status and troubleshooting information can be accessed from the Appliance, Details pane.

If policies are stopped as a result of a license being revoked (for example, due to expiry or license violations) and an authorized license is subsequently installed, the policies are not automatically restarted. You must restart policies from the Console. See Policy Manager Tools and Stopping the Policy from the Appliance.

Connecting to the ForeScout License Server

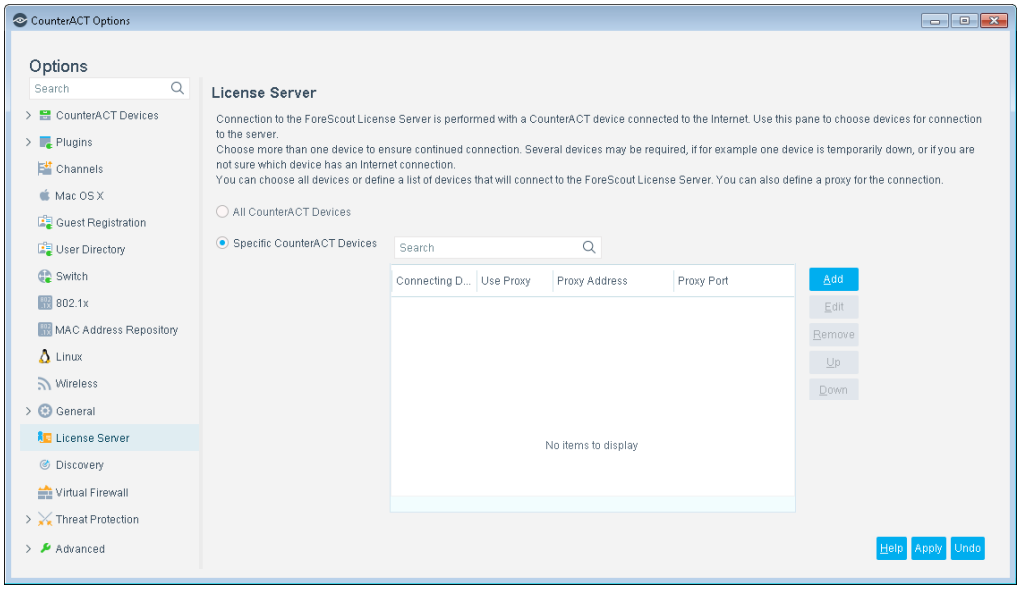
Connection to the ForeScout License Server (at https://license.forescout.com) is performed via a CounterACT device connected to the Internet. By default, CounterACT assumes that all devices are connected.

At least one CounterACT device must have an Internet connection, but you may select more than one to ensure a continued connection. Several devices may be required, for example, if one device is temporarily down or if you are not sure which device has an Internet connection. You can define a proxy for these connections.

Licenses that cannot be authenticated for one month are revoked. You will receive a warning email once a day indicating that there is a communication error with the server.

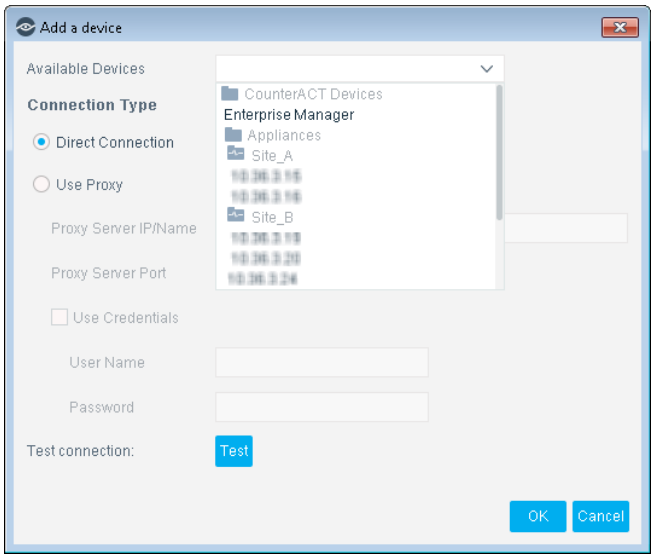
To specify a device to connect to the license server:

1. Select **Options** from the **Tools** menu and then select **License Server**.



License Server Pane

2. Select **Specific CounterACT Devices**.
3. Select **Add**. The Add a device dialog box opens.



License Server Proxy

4. Select a device from the **Available Devices** drop-down list.
5. (Organizations working without an Internet connections can use a proxy to ensure communication with the ForeScout License server.) Select **Use Proxy** and define the proxy.
6. To test the connection to the selected CounterACT device, select **Test**.

7. Select **OK**.
8. Repeat steps 3 to 7 as required.

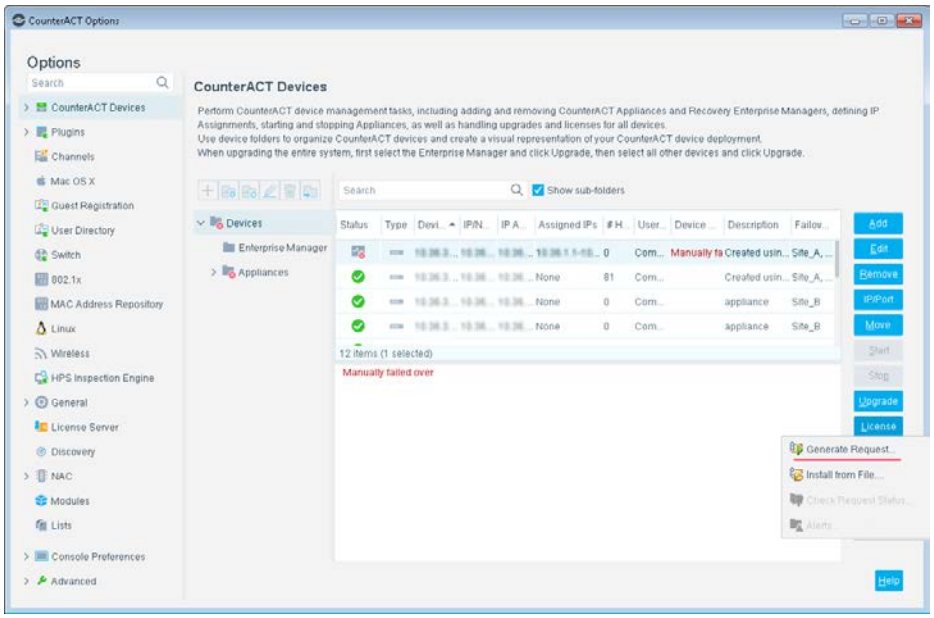
Generating a License Request

This section describes how to generate a request for:

- Extending your demo license
- A new license

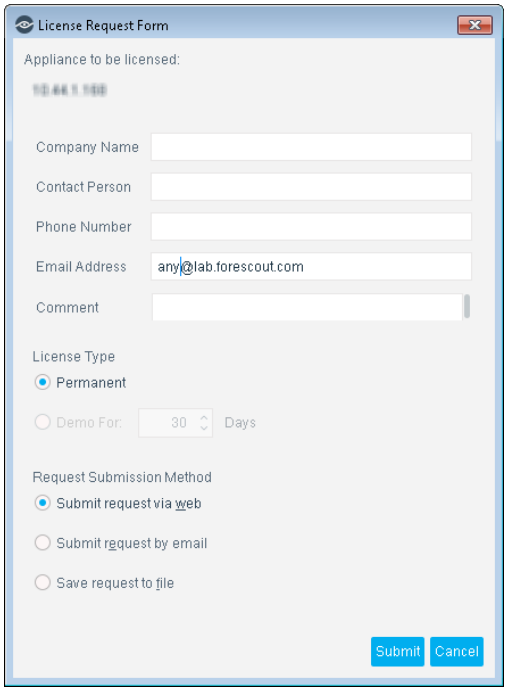
To generate a license request for Appliances:

1. Select **Options** from the **Tools** menu and then, if necessary, select **CounterACT Devices**.
2. Select the Appliances for which you need a license.
3. Select **License** and then **Generate Request** from the drop-down list.



Generate Request for License from CounterACT Devices Pane

4. A **License Request Form** opens, showing the IP addresses of the Appliances you selected.



License Request Form

5. Complete the contact information.
6. To extend the license, select **Extend Demo Licenses By** and specify an extension period. If you clear the checkbox, a permanent license request is sent.
7. In the License Submit Method section, select to submit the request in one of three ways:
   - Through the web: It is advisable to use this automated method because it is the fastest of the three methods. See Receiving Your License via the Web for more information.

     If your organization uses a proxy to perform HTTP access from the Console, proxy settings are taken from those configured in the Windows machine that hosts the Console.
   - By email: The license is sent to the email address that you enter in the License request form. See Receiving Your License via Email for more information.
   - By saving the request to a file: Use this option if you currently do not have Internet access and cannot send the request via the web or by email options. Send the request from, for example, a USB drive. See Saving Your Request to a File for more information. To save a request to file select **Save request to file**.
8. Select **Submit**. There may be one more step before the request is submitted:
   - If you are requesting a license for a virtual Appliance, provide the Appliance model type in the dialog box that opens and select OK.
   - If you chose to save a request to a file, provide the path in the dialog box that opens and select Apply.

Viewing and Managing Your Requests

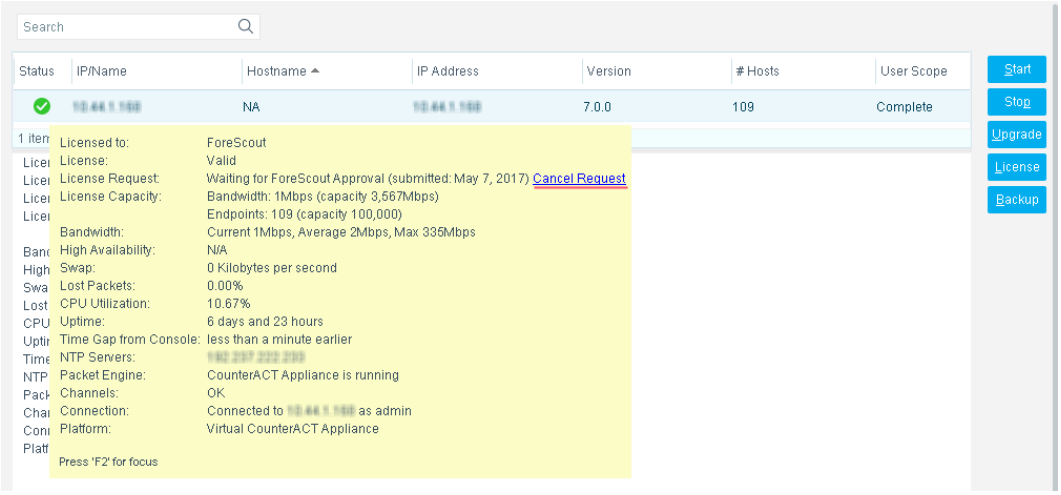
After you request a permanent license or license extension, the request status is automatically displayed at the Console. You can view the status and cancel requests that are no longer relevant. To make changes to the request, you must cancel the specific entry by deleting it. Then re-enter a modified request.

These tasks can be performed from two locations:

- The CounterACT Devices pane
- The License Request Manager

To work from the CounterACT Devices pane:

1. The request status is automatically listed in the Status section of the CounterACT Devices pane when you move your cursor over the Status column.

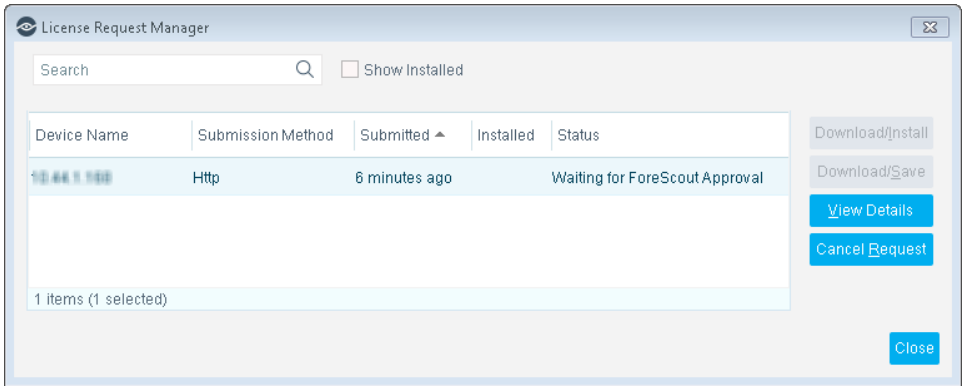


CounterACT Device Details

2. To cancel your request, select **Cancel Request**.

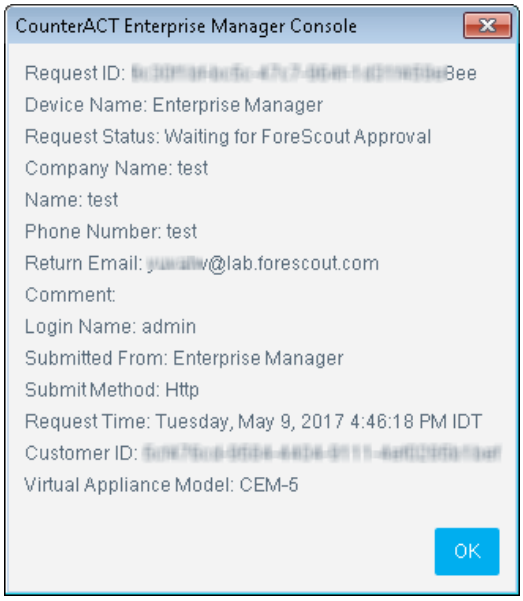
To work from the License Request Manager:

1. Select **Options** from the **Tools** menu.
2. Select the drop-down arrow on the **License** button in the CounterACT Devices pane.
3. Select **Check Request Status**. The License Request Manager opens and displays basic request information.

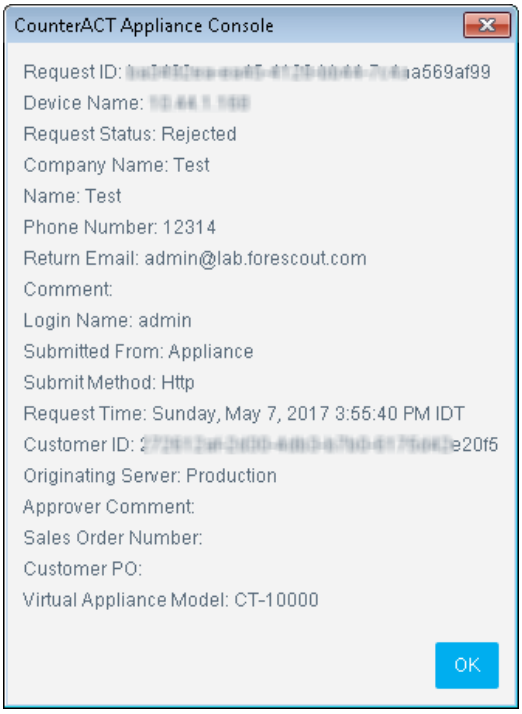


License Request Manager

4. To delete unnecessary requests, select the request to delete and then select **Cancel Request**.
5. To view details about the status of your license request, contact information, submission request and time, and other license-related matters, select **View Details**. Depending on whether you have requested a license for Appliances or an Enterprise Manager, the details shown vary. Details for Appliances include endpoint and bandwidth information, which is automatically determined by your Appliance model.



Enterprise Manager License Request, Details



Appliance License Request, Details

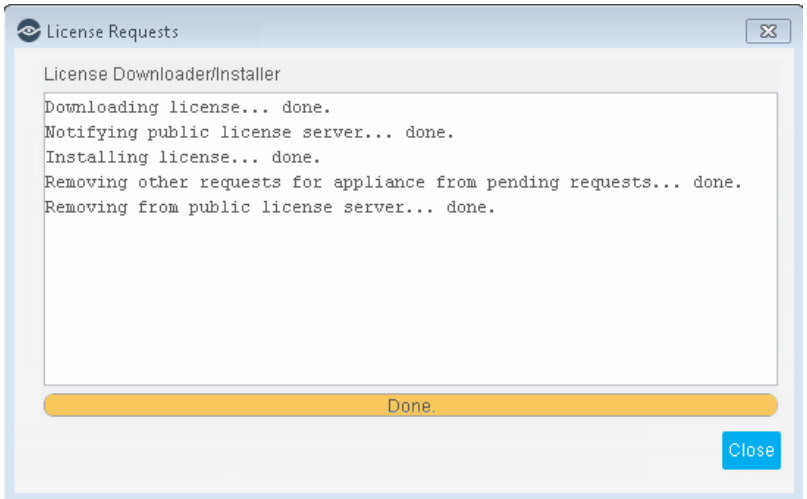
Receiving Your License via the Web

If you requested to receive your license via the web in the **License Request Form**, you can either download and install it automatically or only download it, save it, and then install it at a later date. When your license is ready to be downloaded, you are notified via an email sent to the address that you provided in the **License Request Form**, and by CounterACT in the following ways:

- An icon ( ) on the Console status bar.
- **Ready** is displayed in the Status column in the CounterACT Devices pane.
- **Signed and Ready to Install** is displayed in the Status column when you select **Check Request Status** in the CounterACT Devices pane.

To download and install a license automatically:

1. Select **Options** from the **Tools** menu.
2. Select the Appliances for which you need a license.
3. Select **Check Request Status** from the **License** button drop-down list.
4. Select **Download / Install**. The License Installation process dialog box opens describing the installation process. On completion the dialog indicates this status by displaying **Done**.



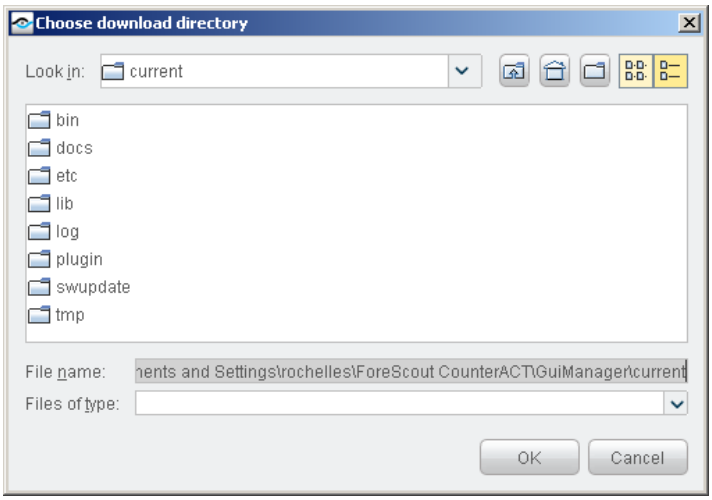
License Installation Completion

The license request is removed from the **License Request Manager**.

5. After a license is downloaded and installed, it is added to a list of installed licenses. To view this list, select **Show Installed**.

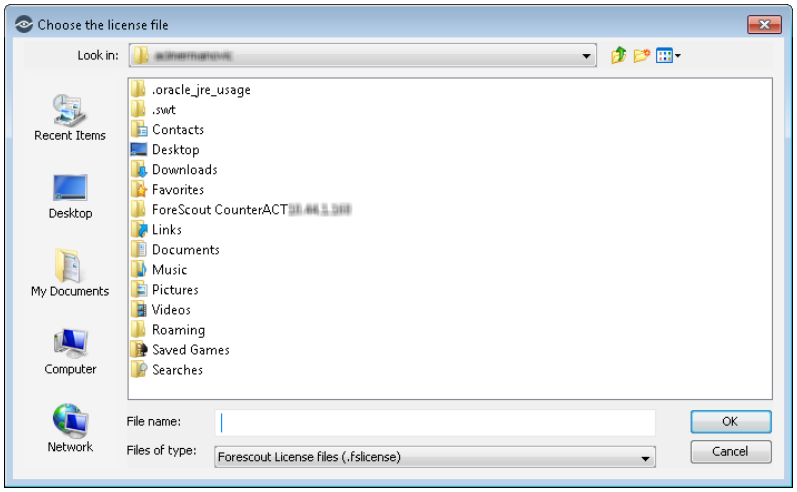
To download and save a license and install it later:

1. Select **Options** from the **Tools** menu.
2. Select the Appliances for which you need a license.
3. Select **Check Request Status** from the **License** button drop-down list.
4. Select **Download/Save** from the **License Request Manager**. The Choose download directory dialog box opens.



Download a License to a File

5. When you are ready to install the license, continue.
6. Select **Options** from the **Tools** menu.
7. Select **License** and then **Install from File** from the drop-down list.



Installing a License from a File

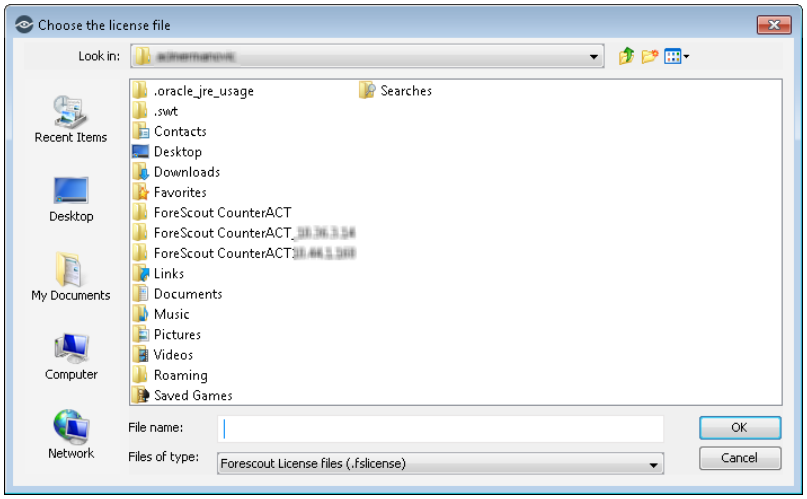
8. Select the saved license file and then select **OK**.

Receiving Your License via Email

If, in the **License Request Form**, you requested to receive your license via email, your license is sent to the email that you provided in this form.

To save and install the license:

1. Save the licenses that you received by email to a file.
2. Select **Options** from the **Tools** menu.
3. Select the Appliances for which you need a license.
4. Select **License** and then **Install from File** from the drop-down list. The Choose a License dialog box opens.



Choose a License Dialog Box

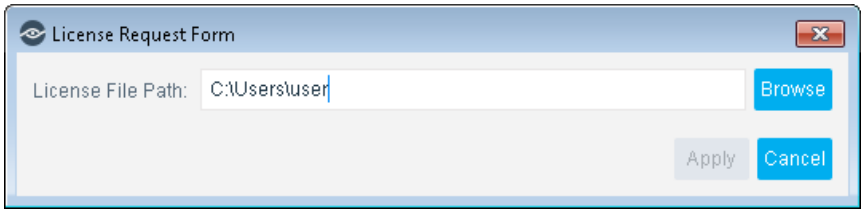
5. Navigate to your license and select **OK**.

Saving Your Request to a File

You may choose to save your request to a file in the **License Request Form** if you have no Internet connection or cannot send or receive an email. If you select this option, you must transfer the saved request file to ForeScout another way.

To save your request to a file and submit it at a later date:

1. Select **Options** from the **Tools** menu.
2. Select the Appliances for which you need a license.
3. Select **License** and then **Generate Request** from the drop-down list. The **License Request Form** opens.
4. Select the option **Save request to a file** and select **Save**. The License Request dialog box opens.



License Request File Path

5. Type in the license file path or select the folder where want to save your request file, and select **Apply**.
6. Submit the saved request to a ForeScout representative. For example, transfer the request file to a USB drive and send it from another computer.


```
  <?xml version="1.0" encoding="UTF-8" standalone="no" ?>
- <UserData Comment="" Company_Name="BigShot" Login_Name="Administrator" Name="ann" Phone_Number="09
    7756138" Return_Email="anny@forescout.com">
    <Device Appliance_IP="10.31.1.209" Appliance_Mac_Address="00:0C:29:9A:29:20" Appliance_Model=""
      Appliance_Serial_Number="VMware-56 4d 4f 00 89 bb 95 a1-af 83 a6 fc 00 9a 29 20" Bandwidth="-1"
      CPU_Family="16" CPU_MHz="2908.805" CPU_Model="6" CPU_Name="AMD Athlon(tm) II X2 245 Processor"
      CPU_Stepping="2" CPU_Vendor_ID="AuthenticAMD" Days_Left="-1" Endpoints_Grace_Percent="10"
      Endpoints_Limit="-1" Endpoints_Limit_Time_Sec="600" Ethernet_Interfaces_Drivers="e1000 e1000 e1000 e1000"
      Ethernet_Interfaces_Names="eth0 eth1 eth2 eth3" Ethernet_Interfaces_Number="4" License_Features=""
      Processors_Number="1" Product="CounterACT" Registration_Date="1153227581161" Software_Version="6.3.4.0-
      113" Total_RAM="773516 kB" Type="scout" />
    <Request License_Format="Permanent_V1" Request_Id="5923baec-3d75-4884-a04b-c8119128e735"
      Request_Time="1277382864568" Submit_Method="Save" Submitted_From="Enterprise_Manager" />
  </UserData>
```

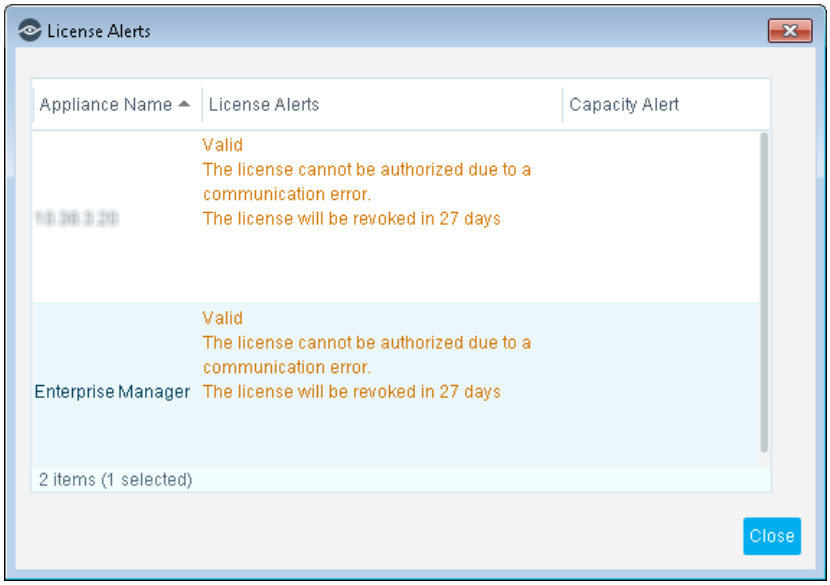

Saved Request for a License

Viewing License Alerts

You can view license alerts in the Console.

To view License alerts:

1. Log in to the Enterprise Manager via the Console.
2. Select **Options** from the **Tools** menu and then, if necessary, select **CounterACT Devices**.
3. Select **License** and then **Alerts** from the drop-down list. The License Alerts dialog box opens.



License Alerts

Appliance Name	The CounterACT device name.
License Alerts	All licenses that are near their expiration dates are listed in red.
Capacity Alert	Indicates violation in bandwidth utilization and endpoint capacity for the Appliance at which the license is installed. These alerts are displayed for informational purposes only, and no action is taken by ForeScout if a violation occurs. Your Appliance, however, may not work as efficiently when capacity violations occur. See Appliance Endpoint Performance Capacity for details.

Per-Appliance Extended Module License

Extended Module licenses provide access to Extended Modules.

Each Extended Module license has an associated capacity, indicating the number of endpoints the license can handle.

How Module Licenses Work

In order for a module to be functional, a valid module license is required. You can only install one license per module.

Demo Licenses

You will receive a demo license after installing a module. This license is valid for 90 days.

> *The demo license period for integration modules that package groups of related licensed modules is 30 days. The expiration period is calculated from the first installation of any of the packaged modules. The expiration date applies to all packaged modules, regardless of how many of the modules are installed. This means if you only installed one of the two packaged modules, the expiration date applies to both modules. See Integration Modules: Multiple .*

Request a demo license extension or permanent license before this period expires.

Permanent Licenses

Each module is licensed for a specified number of devices. A module needs to be licensed for the total number of devices that are managed by CounterACT or, if the module license is being applied to an Enterprise Manager, the module needs to be licensed for the total number of devices that are managed by the Enterprise Manager.

> *EMM/MDM modules are licensed for a specified number of mobile devices. An EMM/MDM module needs to be licensed for the total number of mobile devices that are managed by an EMM/MDM system and which appear in the CounterACT inventory.*

Each module license is designed to be installed on an individual Appliance or Enterprise Manager. If a network has multiple Enterprise Managers, or multiple Standalone Appliances, then module licenses should be purchased separately for each CounterACT device. The size of each module license should cover the number of devices managed by each CounterACT device.

If you add Recovery and High Availability devices to your CounterACT system after purchasing Module licenses, you will need to request licenses to work with the updated system.

Module licenses should be installed on the Enterprise Manager. Once installed, they are automatically applied to all managed Appliances. If your environment does not have an Enterprise Manager, module licenses should be installed on the Standalone Appliance.

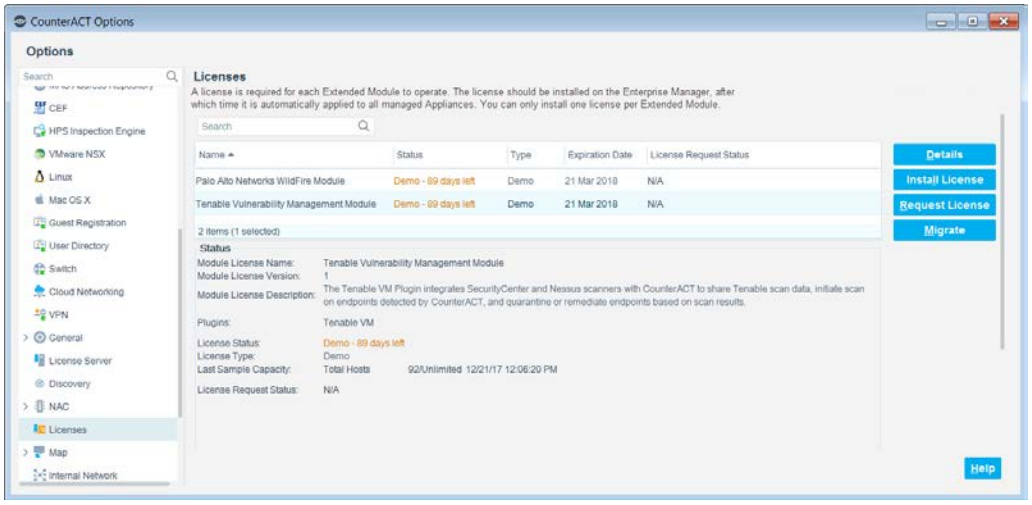
> *Not all users have access to the module features. See Access to Console Tools – Permissions for details.*

Requesting a Demo Extension or Permanent License

Request a demo license extension or permanent license before the demo period expires.

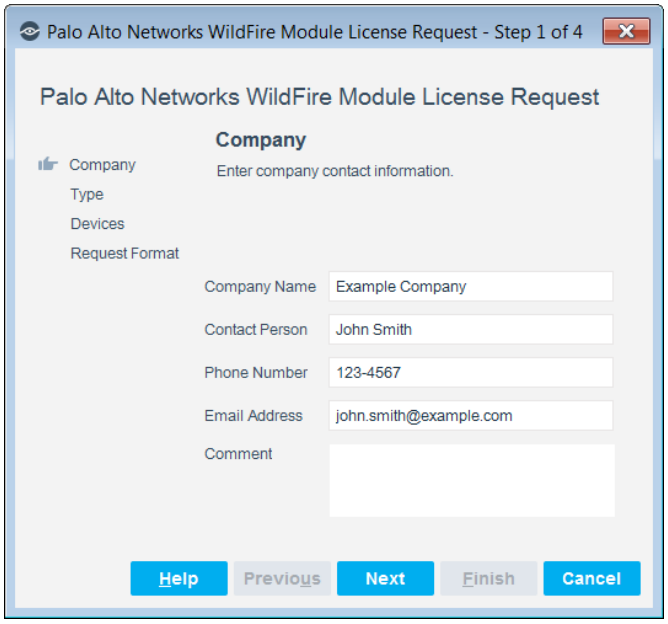
To request a demo extension or permanent license:

1. Select **Options** from the **Tools** menu and then select **Licenses**. The Licenses pane opens.



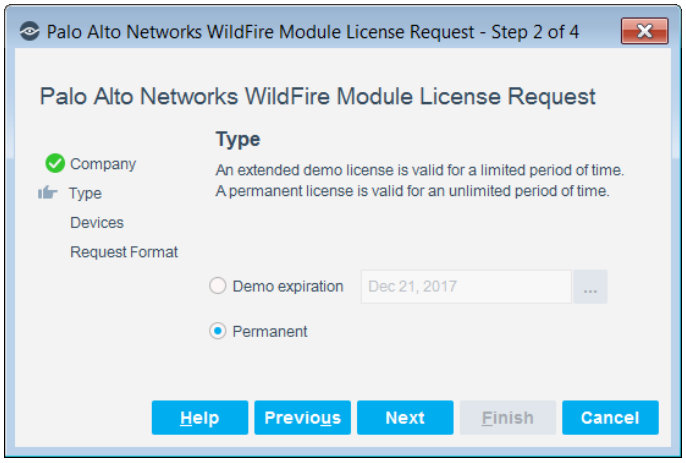
Licenses Pane

2. Select **Request License** and then select **Generate Request.** The License Request wizard, Company pane opens.



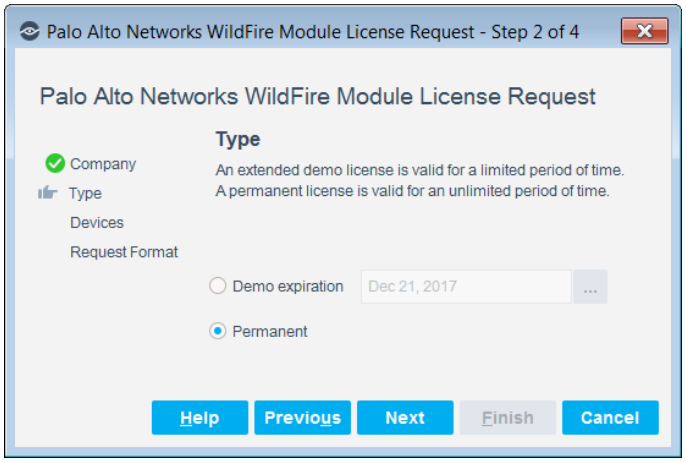
Company Information Pane

3. The pane may include company information taken from previous CounterACT license installations or requests. Update the information if required or enter new information if none was displayed. License alerts and license files will be sent to the address listed here. You can enter more than one email address. Separate addresses with spaces, commas or semicolons.
4. Select **Next.** The Type pane opens.



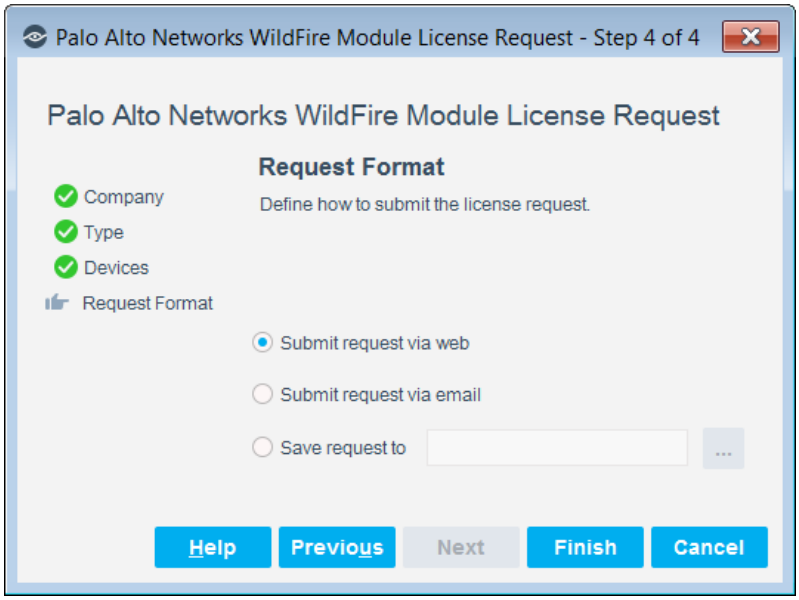
License Type Pane

5. Request either a permanent license, which does not have a time limitation, or to extend your demo license for a specific time period.
6. Select **Next**. The Devices pane opens.



License Devices Pane

7. Indicate the number of endpoints you want the license to handle. Options may vary depending on the module you are working with.
8. Select **Next**. The Request Format pane opens.



Request Pane

9. Select to submit the request in one of three ways:
   - ***Through the web***: Your request is sent to the ForeScout license server. After your request is accepted, the license is sent to the email address you entered in the request wizard. You can also download the license from the Modules pane. If your organization uses a proxy to perform HTTP access from the Console, proxy settings are taken from those configured in the Windows machine that hosts the Console.
   - ***By email***: Your request is sent to the ForeScout module license team. After your request is accepted, the license is sent to the email address you entered in the request wizard.
   - ***By saving the request to a file:*** Use this option if you currently do not have Internet access and cannot send the request via the web or by email options. Submit the saved request to a ForeScout representative, for example, transfer the request file to a USB drive and send it from another computer.
10. Select **Finish**.

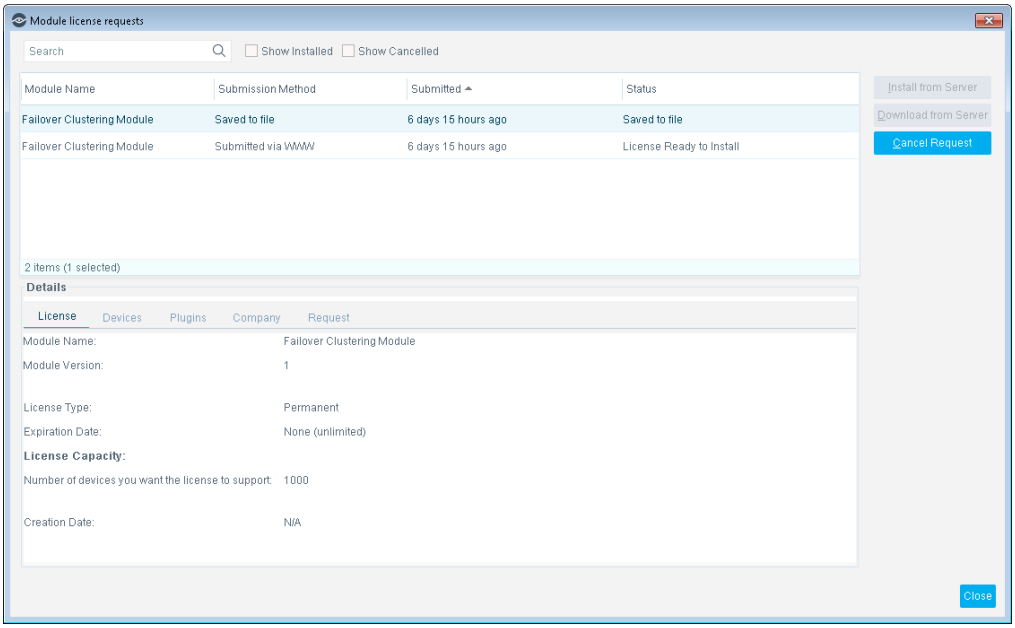
See Installing Licenses for installation information.

Viewing and Cancelling Module License Requests

After sending your license request, the request details and status are automatically displayed in the Modules pane. You can view the status and cancel requests that are no longer relevant. To make changes to the request, you must cancel the specific entry by deleting it and then re-enter a modified request.

To view and cancel requests:

1. Select **Options** from the **Tools** menu and then select **Licenses**.
2. Select **Request License** and then select **Request Details**. The Module License Request pane opens.



License Request Manager

3. To cancel a request, select a module and then select **Cancel Request**.

Installing Licenses

Once your license is approved it will be sent to the email addresses listed in the License Request wizard. If you sent your request via the web, the license will also be immediately accessible from Modules pane. You will be notified as follows:

- An icon will appear on the Console status bar.
- *Ready* is displayed in the Status column in the Modules pane.
- *Signed and Ready to Install* is displayed in the Status column when you select Check Request Status in the Modules pane.

To install a license you received by email:

1. Save the license.
2. Select **Options** from the **Tools** menu and then select **Licenses**.
3. Select **Install License** and then select **Install from File**.
4. Navigate to the location you saved the file and select **OK**.

To download and install a license:

1. Select **Options** from the **Tools** menu and then select **Licenses**.
2. Select the module for which you need a license.
3. Select one of the following from the **Install License** button drop-down list:
   - **Install from Server**: If the request was submitted via HTTP, to download and install the license from the server.
   - **Download from Server**: If the request was submitted via HTTP, to download the license file from the server and install it from a file later.

– **Install from File**: If you have a license file to install.

Or:

a. Select **Request Details** from the **Request License** button drop-down list.

b. The Module license requests dialog box opens. Select a license request that appears as ready to install, corresponding to the license you want to install.

c. Select either **Download from Server**, **Install from Server** or **Install from File.** The options function identically.

4. A pop-up dialog appears indicating that the license is being downloaded.

After a license is downloaded and installed, it is added to a list of installed licenses.

5. To view this list, select **Request Details** from the **Request License** button drop-down list:

a. The Module license requests dialog box opens. Select **Show Installed**.

b. Highlight the license request you want to examine.

c. The license request details appear in the **Details** pane.

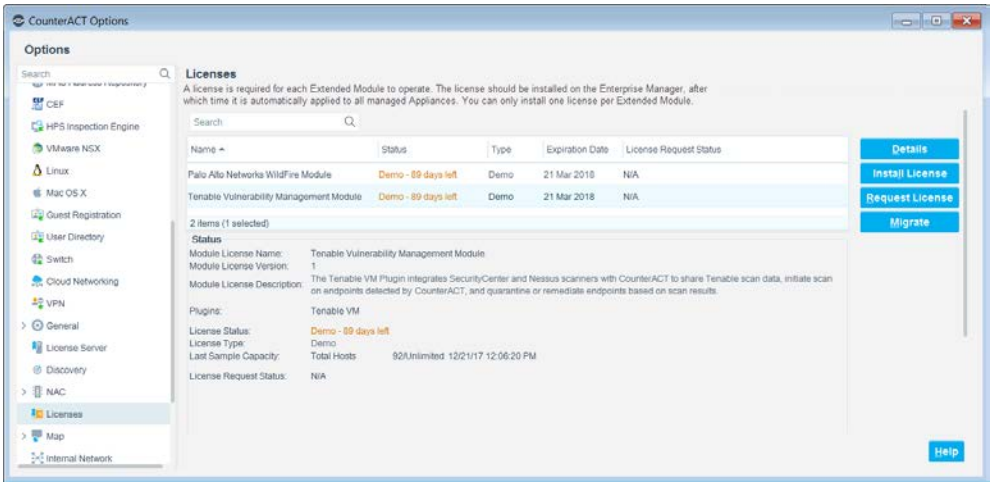
Viewing Module Information

License information appears in the Modules pane after the plugin is installed.

This information includes for example:

- License Request Status
- License Capacity Status
- Extensive information about endpoints being managed via the module plugins.

This information is automatically updated when the license request status and license status changes.



Modules Pane

In addition the module name and status appear in the Modules pane.

Previously Installed Plugins

You will be alerted to licensing requirements for plugins already installed if you install a plugin update after the CounterACT module is released.

Tracking Extended Module License Activity

Information about Extended Module license activity is automatically shown in the CounterACT Audit Trails log and Events Viewer.

Audit Trails Log

The Audit Trails log indicates when a module license was installed.

To access the Audit Trails log:

1. In the Console **Log** menu, select **Audit Trails**.
2. Enter a time period and select **OK**. The Audit Trails log opens.

Event Viewer

The Event Viewer indicates:

- When a module license was installed
- Periodic license alerts
- When a module license expires
- When a module license is invalid
- When the number of devices handled by the license is exceeded

To access the Event Viewer:

1. Select **Event Viewer** from the **Log** menu. The Event Viewer opens.

Viewing Endpoint Information

You can view extensive information about the endpoints that were detected by the modules. Quickly find information that is important to you by using the search filter and plugin drop-down filter.

1. Select **Options** from the **Tools** menu and then select **Licenses**.
2. Select a module.
3. Select **Details**.

Switch Licensing Mode from Per-Appliance to Centralized

If you are running CounterACT version 8.0 operating in Per-Appliance Licensing Mode, you can switch to Centralized Licensing Mode.

Contact ForeScout Support or your ForeScout representative for more information on how to switch licensing modes.

Before switching modes, verify that you have:

- Valid credentials to access the ForeScout Customer Portal. Contact your ForeScout representative for more information.
- A valid license entitlement.

Refer to the ForeScout Centralized Licensing How-to Guide *for information on how to work with Centralized Licensing Mode. See Additional CounterACT Documentation for information on how to access this guide.*

If you are using ForeScout Extended Modules, be aware that Integration Modules that package together *groups of related licensed modules* are not supported when operating in Centralized Licensing Mode. Only Extended Modules that package *individual licensed modules* are supported. An exception to this is the Open Integration Module, which is an Extended Module even though it packages more than one plugin.

Before switching modes, uninstall any Integration Modules and reinstall them as Extended Modules. See Extended Modules and Module Packaging for more information.

Receiving License Alerts

CounterACT License Alerts provide information about the status of licenses that you have already installed, for example, if the license is about to expire or if you have added endpoints and exceed your license capacity.

You will receive alerts if there are issues regarding your licenses. Alerts are displayed through:

- Periodic email reminders

  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.

Chapter 18: Additional Options

- Working with the Internal Network
- Managing Email Notification Addresses
- Signing Emails with an S/MIME Certificate
- Defining Endpoint Discovery Rules
- Working with the Enforcement Mode
- Backing Up System and Component Settings
- Recovering an Enterprise Manager
- Language Support
- Pre-Registration and Guest Registration Management
- The ForeScout Research and Intelligent Analytics Program

Working with the Internal Network

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

The Internal Network defines the extent of CounterACT's management activity - for example, when a CounterACT 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 CounterACT's Internal Network definition, are not managed by CounterACT.

Internal Network Pane

During installation, the Internal Network is defined when you run the Initial Setup Wizard. See Internal Network.

Administrators with appropriate permissions can use the Segment Manager tool to edit the segment definitions that define the Internal Network. See Working with CounterACT Segments and Chapter 14: Managing Users, Access to Console Tools – Permissions. For example, if your network expands, you typically:

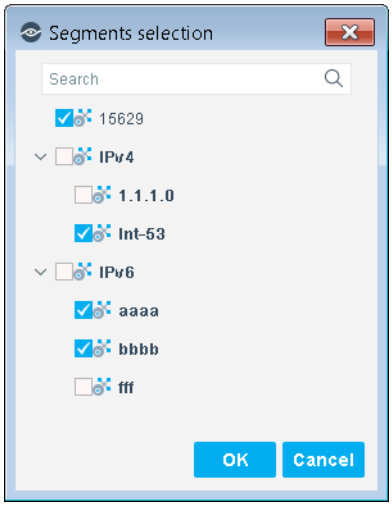
- Use Segment Manager to define segments with your network's new IP addresses.
- Use the procedure described in this section to add these segments to the Internal Network.

Several CounterACT 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.

In addition to defining the IP addresses in the Internal Network, you can specify how CounterACT handles endpoints without IP addresses. For more information, see Working with Hosts without IPv4 Addresses.

To define the Internal Network:

1. Select **Options** from the **Tools** menu and then select **Internal Network**. The Internal Network Pane opens.
2. To add or remove IP addresses to the Internal Network, select **Segments**. The Segments selection dialog box opens.



Segments selection Dialog Box

3. Select and clear checkboxes to specify the segments that make up the Internal Network, and select **OK**. Only segments that you selected are included in the Internal Network. The table reflects your choices.
4. To remove a segment from the Internal Network, select it in the table and then select **Remove**.
5. Select **Apply** to apply the changes to the Internal Network configuration.

Working with Hosts without IPv4 Addresses

Optional settings let CounterACT detect and manage endpoints based on their MAC or IPv6 address when an IPv4 address is not available to CounterACT. This option is useful for example:

- When a rogue device without an IP is discovered by the network switch.
- When an IP address is discovered after the MAC address.
- 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 will still be displayed in the Console with Layer 2 information.

When you enable these options, it is very important that the Internal Network definition includes all network segments that CounterACT 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
- Recheck Host
- 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

To enable management of endpoints without an IPv4 address:

1. Select **Options** from the **Tools** menu and then select **Internal Network**. The Internal Network pane opens.
2. Enable the **Handle new hosts with MAC address and no IPv4 address** option at the bottom of the Internal Network pane.

Working with Hosts Whose IPv4 Address Is Used by Another Host

CounterACT 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. Use this option for example, if you are working with guest hosts that may frequently log in and out of the network. Selecting this option will retain previous authentication events on these hosts, and (depending on the relevant policy) will not require them to authenticate when they reconnect.

To retain disconnected host information:

1. Select **Options** from the **Tools** menu and then select **Internal Network**. The Internal Network pane opens.
2. Select **Retain disconnected host information for hosts whose IP address is used by another host**.

   *Use the **Last Known IPv4 address** property to create conditions based on the previous IPv4 address.*

Managing Email Notification Addresses

The email addresses defined during initial setup are used to:

- Send notices when specific endpoint events, email worm events and service attacks occur. Not applicable to policy detections.
- Send notices expiration warning notice regarding your licenses.
- System operation alerts.

You can update the addresses to which CounterACT sends email alerts. Options are available to add, modify or delete addresses.

Options are available to configure the mail options differently for different Appliances in your enterprise and to view different configurations per Appliance. See Configuring Features for an Appliance or Group of Appliances.

An option is also available to define the maximum number of emails delivered to these addresses daily, and to define how many events are listed in each email. See Operator Notification for information about Threat Protection mail, and Policy Preferences.

To update the addresses:

1. Select **Options** from the **Tools** menu and then select **General** > **Mail**.

Email Options

2. Update the address in the **Operator email** field. If you are using more than one address, enter a space in between each address.
3. Enter mail relay, DNS domain, and DNS server values.
4. Select **Apply** to apply the changes to the configuration.
5. Select **Test Email** to send a test email to this address.

Signing Emails with an S/MIME Certificate

You can sign emails sent by CounterACT using a digital certificate, as specified by the Secure/Multipurpose Internet Mail Extensions (S/MIME) standard.

This does **not** *include mails sent by the ForeScout License Server (only relevant when operating in Per-Appliance Licensing Mode). For example, mails sent regarding:*
- CounterACT Extended Module license request and approval status.
- CounterACT device license request and approval status.

- Generating CSRs and Importing Signed Certificates
- Working with Digitally Signed Emails

Generating CSRs and Importing 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 into CounterACT.

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 Appendix 8: Configuring the Certificate Interface.

When you generate a CSR:

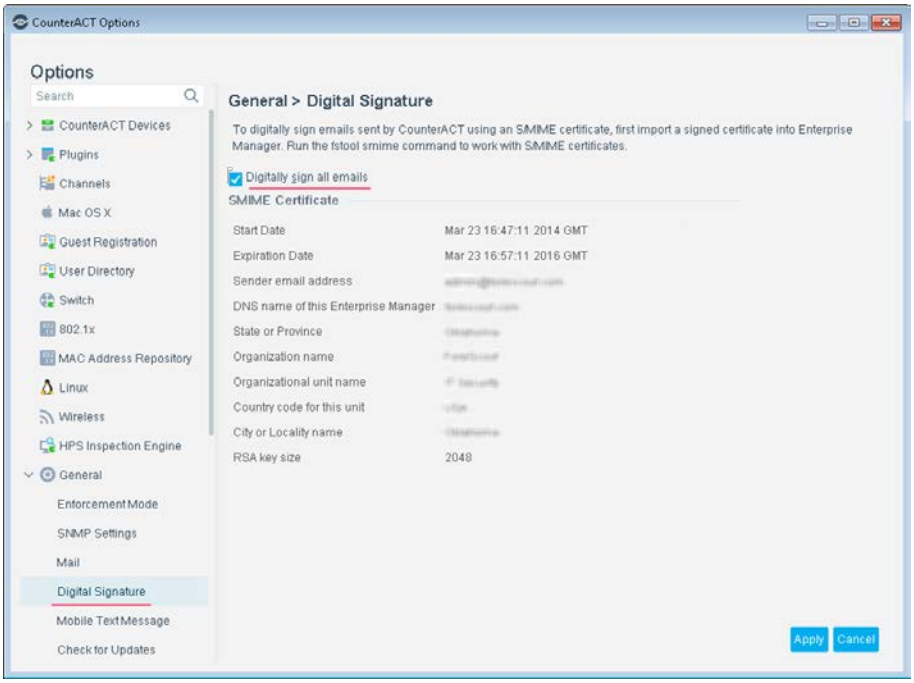
- In the Used for and Key Usage fields of the CSR wizard, specify that the certificate will be used for email signing.
- In the Email Address field, specify the email address of the Enterprise Manager that applies the digital signature to emails. When you install the signed certificate on the Enterprise 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 CounterACT Enterprise Manager.

Working with Digitally Signed Emails

When digital signatures are enabled, all emails sent by CounterACT are signed using the S/MIME certificate. The body of the email is sent as clear text in digitally signed emails. It is not encrypted.

To work with digitally signed emails:

1. In the Console, select **Options**.
2. In the Options tree, select **General > Digital Signature**.



Digital Signature

3. Verify the S/MIME certificate: the tab shows data fields for the current signed certificate.
4. The **Digitally sign all emails** option controls this feature. Do one of the following:
   - To enable digitally signed emails, select this option.
   - To send emails without a digital signature, clear this option.
5. Select **Apply**.
6. To apply the settings of Step 4 to guest registration emails, restart the User Directory Plugin.

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 that normally are sent directly by the Appliance are routed through the Enterprise Manager.

Defining Endpoint Discovery Rules

By default, CounterACT 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 CounterACT)
- Switch Plugin properties (this plugin is bundled with CounterACT)

Additional properties may also be discovered by default, depending on the plugins that you have installed. For example, if you installed the VPN 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

Expanding 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 Chapter 8: Base, Content and Extended Modules and Chapter 5: Policy Management for more information.

Limiting the Information Discovered by Default

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 CounterACT, such as admission events, MAC addresses, NetBIOS domain and host names or open ports.
- Properties listed in policies.
- Properties displayed in Detections pane columns.

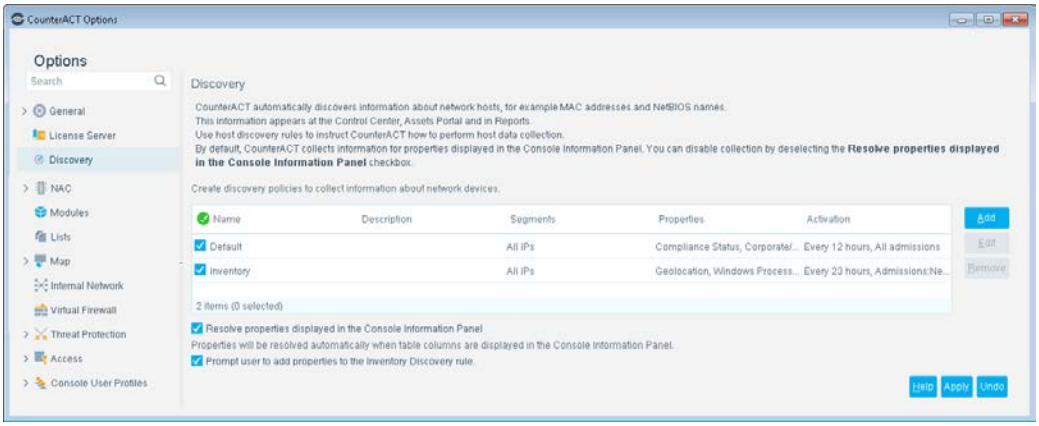
Limiting discovery does not impact the policy discovery mechanisms. This means that if you choose not *to discover certain properties via the Network Host Discovery Policy, they can still be discovered via the policy.*

To define discovery rules:

1. Select **Options** from the **Tools** menu and then select **Discovery**.

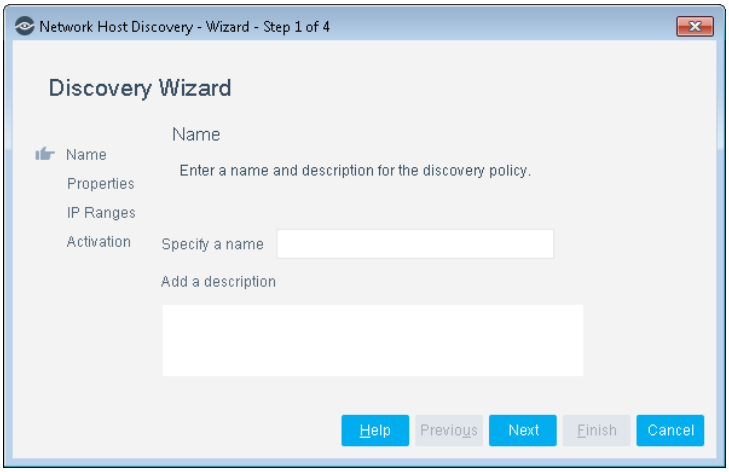
By default, CounterACT collects information for properties displayed in the Console table columns. You can disable this collection by clearing ***Resolve properties displayed in the Console Detections pane****.*

By default, CounterACT presents users working in the Asset Inventory with a prompt to add properties to the Inventory Discovery rule. You can disable this prompt by clearing ***Prompt user to add properties to the Inventory Discovery rule****.*



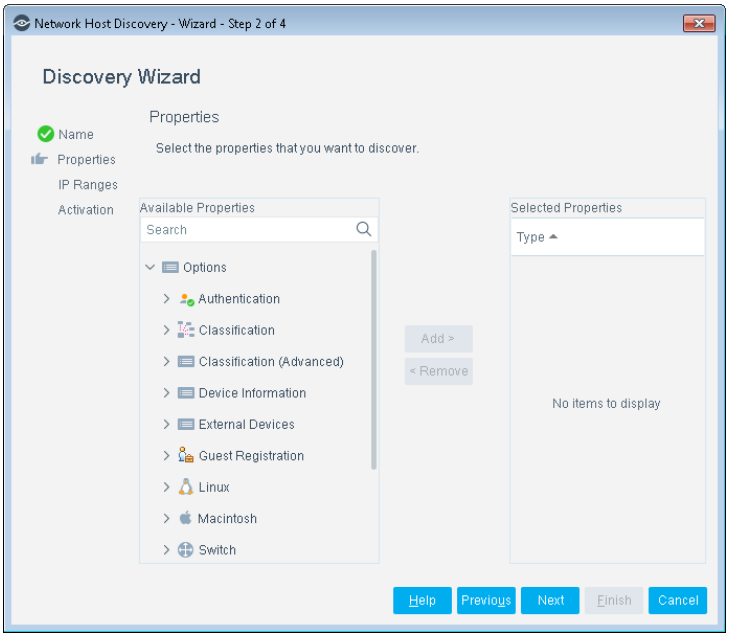
Discovery Pane

2. Select **Add**. Type a rule name and description.



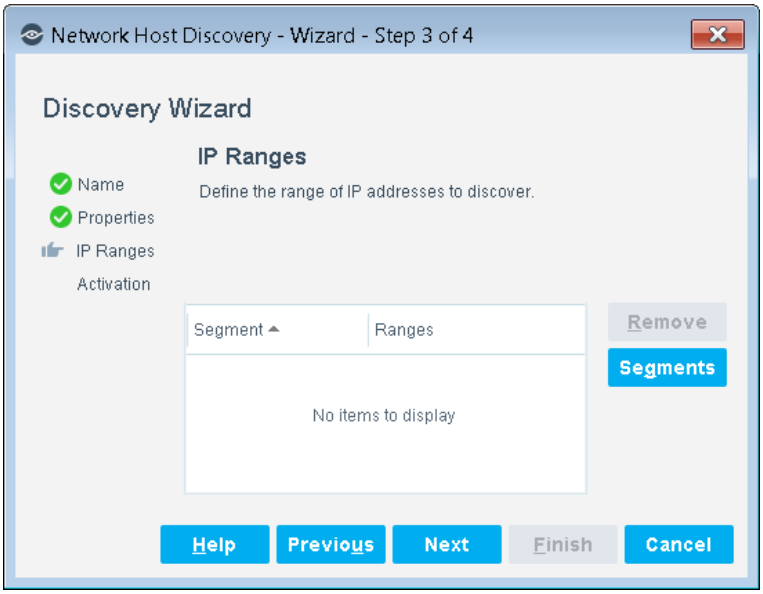
Discovery Wizard, Name

3. Select **Next**. The Properties tab opens. Select the properties that should be discovered.



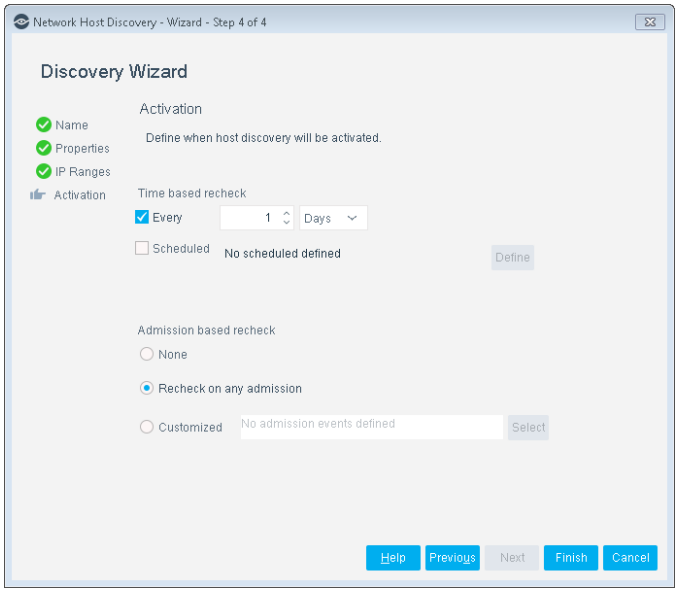
Discovery Wizard, Properties

4. Select **Next**. The IP Ranges tab opens.



Discovery Wizard, IP Ranges

5. Define the IP addresses to which to apply the rule.
   - Select **Segments** to add segments of the CounterACT Internal Network to the scope of the rule.
   - To remove a segment, select it in the table and select **Remove**.
6. Select **Next**. The Activation tab opens.



Discovery Wizard, Trigger

Use the activation option 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**: Use 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 exits between the detection of Network Admission triggers 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 will start when more details could be learned about the endpoint (after all services have loaded). You can update the delay default time.

8. Select **Finish**.

Working with the Enforcement Mode

Set up your system to work with either full enforcement or partial enforcement.

The Full Enforcement mode allows complete functionality.

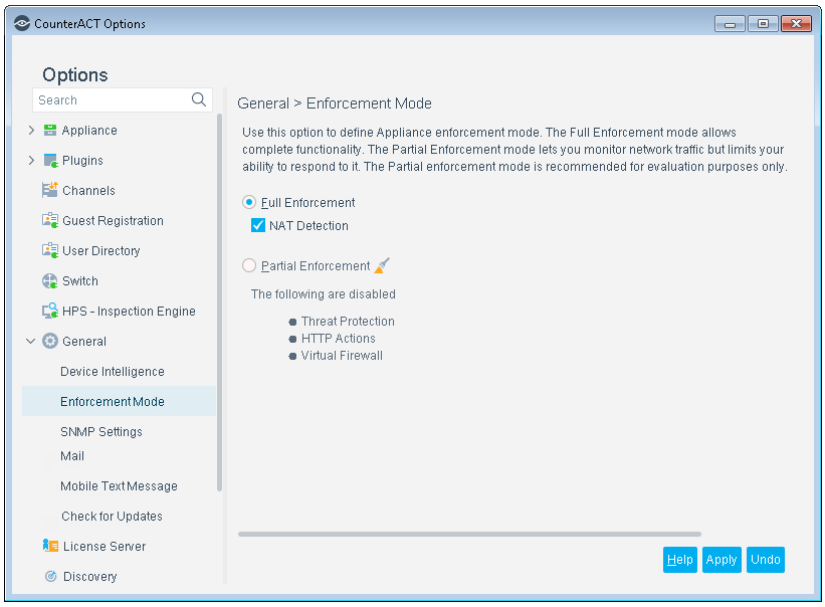
The Partial Enforcement mode lets you monitor network traffic but limits your ability to respond to it. Specifically, the Threat Protection, HTTP Actions and Virtual Firewall options will be disabled. This mode is recommended for evaluation purposes only.

The **Partial Enforcement Mode** icon is displayed on the status bar if your system is set to this mode.

The icon on the status bar may show that CounterACT is running in **Forced Partial Enforcement** mode. This means that there may be connectivity problems between CounterACT and the network.

To set the Enforcement mode:

1. Select **Options** from the **Tools** menu and then select **General** > **Enforcement Mode**.



Enforcement Mode

2. To work with full enforcement, select **Full Enforcement**. If your network is configured with NAT devices and you want to detect them, select **NAT Detection** to detect NAT devices.
3. To work with partial enforcement, select **Partial Enforcement**.
4. Select **OK** in the Configuration successfully saved dialog box.

Backing Up System and Component Settings

Backup and restore procedures allow you to save CounterACT device system or component settings and scheduled or saved reports. You can later restore them to

the CounterACT device. This feature should be used in cases of CounterACT device hard drive failures or when data is lost for any other reason.

You can perform the following backup-related activities:

- Scheduling Automatic Backups of CounterACT Settings to External Servers
- Performing a One-Time System Backup
- Backing Up and Restoring the rSite for Your Appliances

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.

In addition, there is a tool that allows you to back up the rSite (real site) and restore it for a single version. This includes the machines and open services currently learned. See Backing Up and Restoring the rSite for more information.

You must restore the same version of CounterACT that you backed up.

A remote recovery feature is also available. This features 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.

Scheduling Automatic Backups of CounterACT Settings to External Servers

You can schedule automatic backups of CounterACT 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 have logged in to the 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 before performing either a system or a component backup.

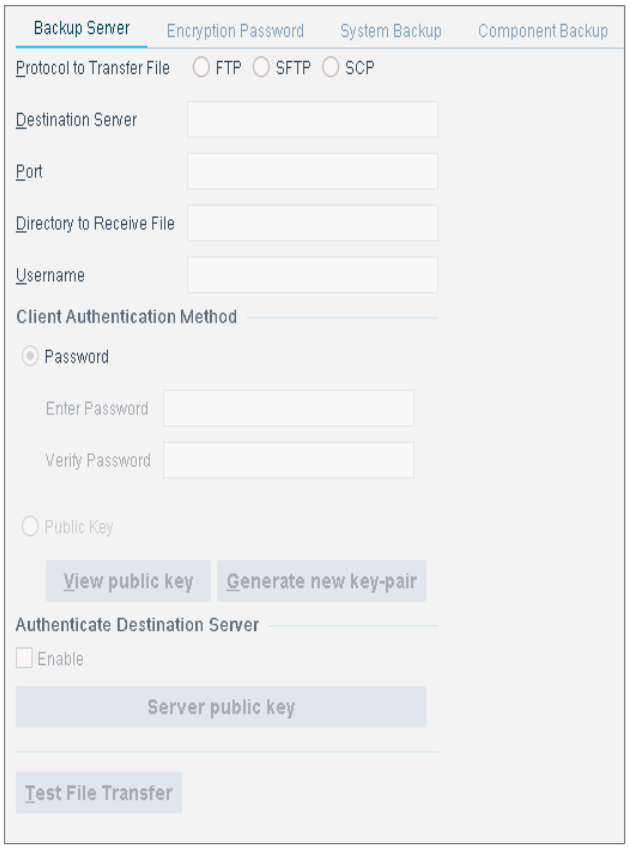
- Configuring a Backup Server
- Configuring an Encryption Password
- Performing a System Backup
- Performing a Component Backup

Configuring a Backup Server

You must configure a backup server. The backup server is used for both Performing a System Backup and Performing a Component Backup.

To configure a backup server for either system or component backup:

1. Select **Options** from the **Tools** menu and then select **Advanced** > **Backup**.



Backup Pane

2. Select a protocol 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 connection between the CounterACT 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 CounterACT installation. The private key is protected by a passphrase. You can also generate a new key-pair by selecting Generate new key-pair.

   *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 CounterACT devices. You can view the status of the creation and transfer of each backup file in the Event Viewer. Only Console 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** to apply the changes.

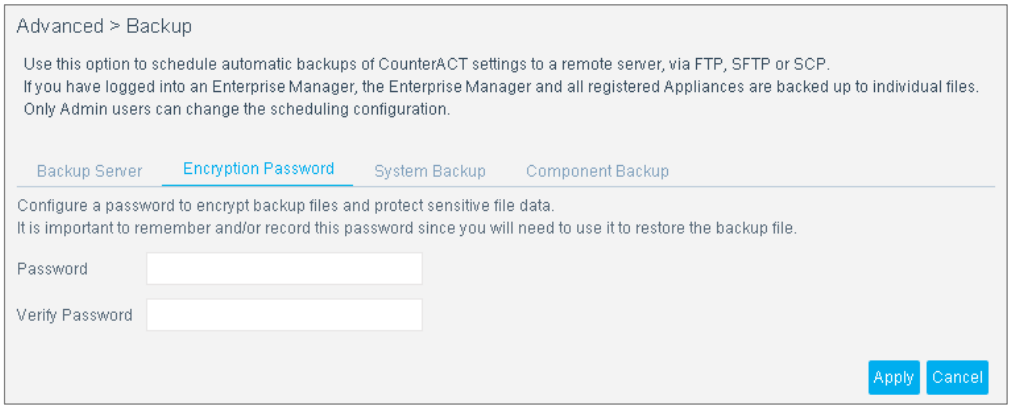
Configuring an Encryption Password

Both system and component backup files, backed up either manually or via a schedule, will be 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 to proceed with backup configuration.

The defined password is also used to encrypt files manually backed up via the **Options > CounterACT Devices** pane. When backing up files using this method, you will be requested to define a password if you have not previously done so.

To encrypt a backup file:

1. Select **Options > Advanced > Backup** and select the **Encrypted Password** tab.



Encryption Password

2. Type a password. The password must be at least six characters long, and must contain at least one digit and one letter.

   Remember and/or record this password as you will need to use it to restore the backup file.

Performing a System Backup

You can perform scheduled backups of the CounterACT system to FTP, SFTP and SCP sites. Using scheduled backups provides extra safety and protection against hard drive failures and data loss. The maximum number of Appliances that can be concurrently backed up is 1-100. The restore procedure requires that you reinstall CounterACT.

The system backup feature saves all CounterACT device and Console settings. This data includes the following:

- Configuration
- License

  If your deployment is using Centralized Licensing Mode, the license file is not saved during system backup. If you still have the license file, and are restoring the backup file on the same machine that the backup was taken from, you can update the existing license file and re-upload the file after the restore. Otherwise, you will need to deactivate the license file, reinstall the CounterACT ISO file, and then activate a new license file. Refer to the ForeScout Centralized Licensing How-to Guide *for information on how to work with Centralized Licensing Mode. Refer to the* CounterACT Installation Guide *for more information on installing the CounterACT ISO file. If you need additional assistance, contact your ForeScout representative.*

- Operating System configuration
- Plugins/Modules

These categories include, for instance:

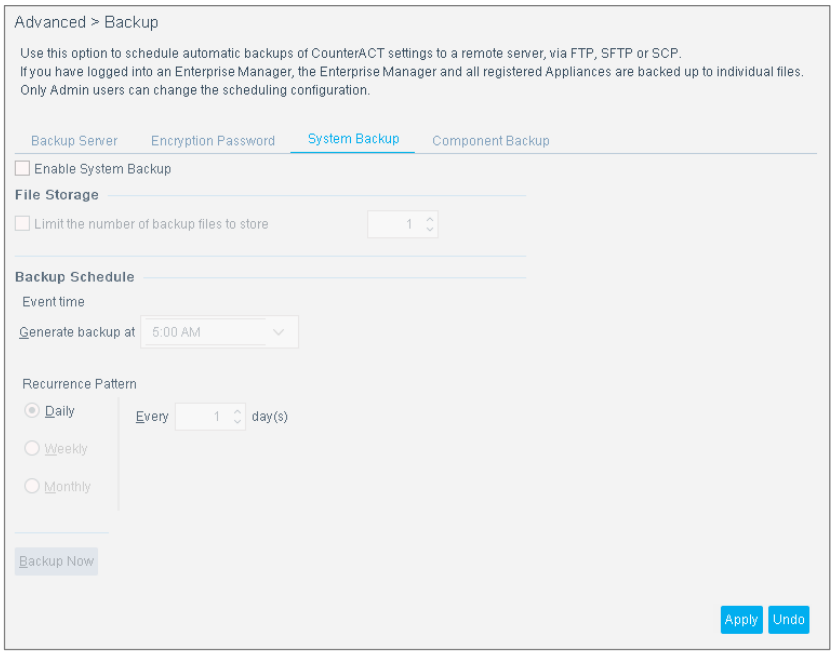
- CounterACT IP address
- License information
- Channel
- Email
- Internal network parameters
- Basic and advanced NAC Policy definitions
- Legitimate traffic definitions
- Report schedules

To perform a system backup:

1. Select **Options** from the Tools menu and then select **Advanced > Backup**.

   To perform a scheduled system backup, you must first configure a backup server and an encryption password. See Configuring a Backup Server and Configuring an Encryption Password.

2. Select the System Backup tab and then select **Enable System Backup**.
3. To disable scheduled backups, clear the **Enable System Backup** checkbox.



System Backup

4. If you want to limit the number of backup files to store, select **Limit the number of backup files to store** and select a number.

   The number of backup files that will be stored is equal to the number you configure plus an additional backup file. This ensures that the requested number of backup files is stored in case of a transfer failure.

   If you apply this option and run the backup, and then decrease the configured number of backup files to store, you will need to manually delete any superfluous backup files.

5. Configure the **Maximum number of concurrent backups**. The maximum number of Appliances that can be concurrently backed up is 100.

6. Select the event time and recurrence pattern in the Backup Schedule section.

7. Select **Apply**.

8. (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

Performing a Component Backup

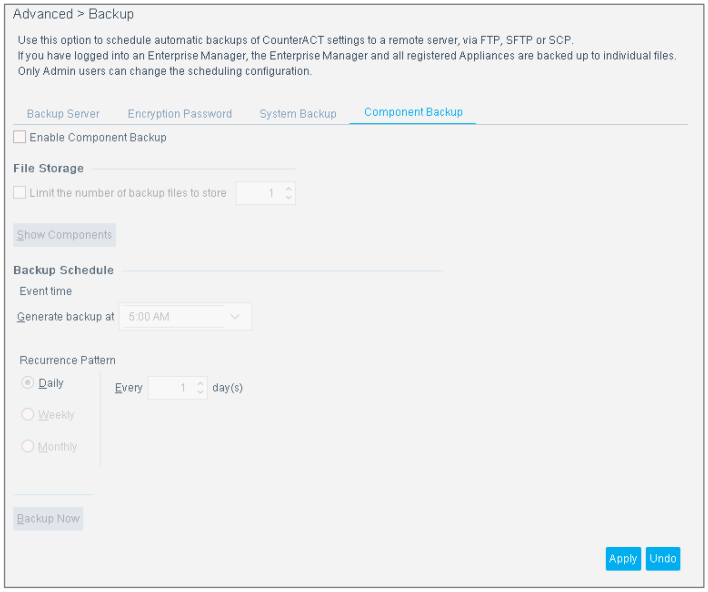
You can perform scheduled backups of CounterACT components to FTP, SFTP and SCP sites. Using scheduled backups provides extra safety and protection against hard drive failures and data loss. The Component Backup feature does not require that you reinstall CounterACT.

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. See Export and Import Policies for details. 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.

To perform a component backup:

1. Select **Options** from the **Tools** menu and then select **Advanced > Backup**.
2. To perform a scheduled system backup, you must first configure a backup server and an encryption password. See Configuring a Backup Server and Configuring an Encryption Password.
3. Select the Component Backup tab and then select **Enable Component Backup**.
4. To disable scheduled backups, clear the **Enable Component Backup** checkbox.



Component Backup

5. If you want to limit the number of backup files to store, select **Limit the number of backup files to store** and select a number.

   The number of backup files that will be stored is equal to the number you configure plus an additional backup file. This ensures that the requested number of backup files is stored in case of a transfer failure.

   If you apply this option and run the backup, and then decrease the configured number of backup files to store, you will need to manually delete any superfluous backup files.

6. Select the event time and recurrence pattern in the Backup Schedule section.
7. Select **Apply**.
8. (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:

   Component_backup.EnterpriseManager_<*EM_IP_Address*>_<*backup_index*>.zip

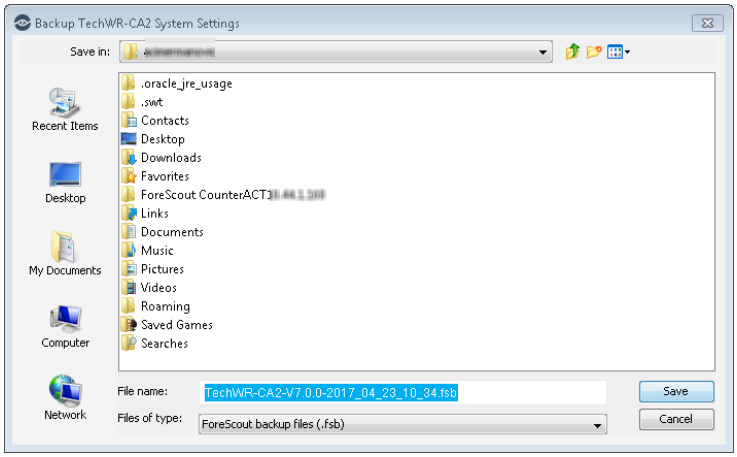
Performing a One-Time System Backup

This section describes how to perform a one-time backup of CounterACT 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 Configuring an Encryption Password for details.

To back up your system settings:

1. Select **Options** from the **Tools** menu.
2. Select a component from the CounterACT Devices pane.
3. Select **Backup**. By default the device name, CounterACT version number, date, and time appear as the name of the backup file.

   *The backup file name can only contain alphanumeric characters. Special characters are not allowed (e.g. $ % *).*



Backing Up and Restoring the rSite 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 feature is recommended, not mandatory. You can use it, for example, to replace an Appliance.

This tool may only be used for a single version. This means that 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 CounterACT device that contains the rSite that you want to back up.
2. Submit the following command:

   `fstool set_property fs.backup.def config license os plugin site`

   There is no need to restart the Appliance.
3. Perform backup and restore of the CounterACT device.
4. To restore original backup behavior, submit the following command:

   `fstool set_property fs.backup.def config license os plugin`

   Rsite information is no longer included in backups.

Recovering an Enterprise Manager

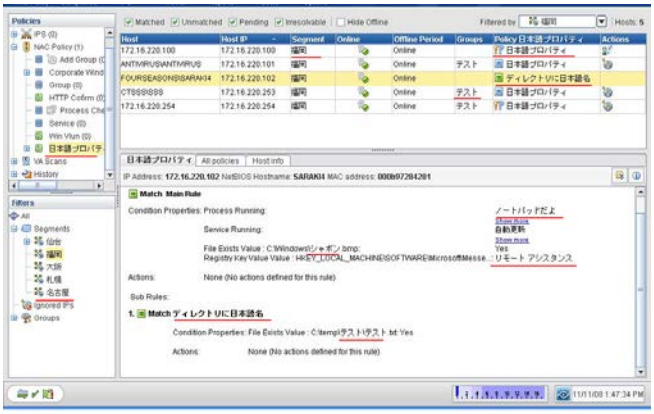
A CounterACT remote recovery tool provides a comprehensive recovery system for an Enterprise Manager that is no longer functioning, for example, if it failed as a result of an earthquake or fire. This feature provides complete and continued management of Appliances from a remote Recovery Enterprise Manager after the crisis.

Refer to the *ForeScout CounterACT Resiliency Solutions User Guide* for more information about this feature and other CounterACT resiliency solutions. See Additional CounterACT Documentation for information on how to access this guide.

Language Support

CounterACT offers the following tools for displaying and working with local languages:

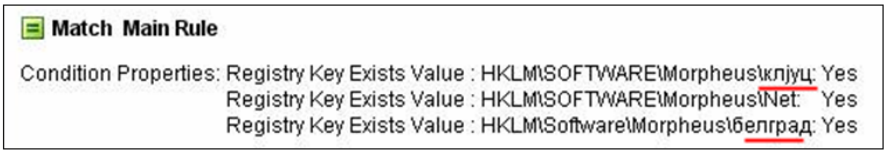
- Displaying Endpoint Information in a Local Language
- Localizing CounterACT Redirected Web Pages and Messages
- Displaying Local Languages in Reports, Actions and Other Features
- Localizing Guest Management Portal



Japanese Language Support

Displaying Endpoint Information in a Local Language

An extensive range of endpoint information is automatically displayed in the active code page language set at the endpoint, such as user and host names, registry key information, file paths, processes and more. This information is displayed in the required languages in the Console Detections pane, Details pane, Assets Portal and in reports.



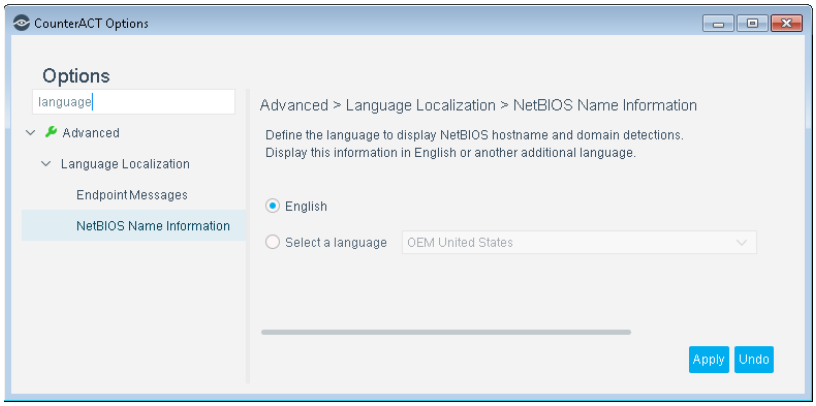
Registry Key in Local Languages

Displaying NetBIOS Names and NetBIOS Domains

You must perform the following configuration to display Microsoft Windows NetBIOS Names and NetBIOS Domains in a foreign language. CounterACT will resolve in the language that you select and in English, if both languages are detected.

To display:

1. Select **Options** from the **Tools** menu and then select **Advanced** > **Language Localization** > **NetBIOS Name Information**.



2. Select a language or language set.
3. Select **Apply**.

If Windows host names or Windows domain names appear as "######" (boxes) in the Console, select a language to match the local language.

Localizing CounterACT Redirected Web Pages and Messages

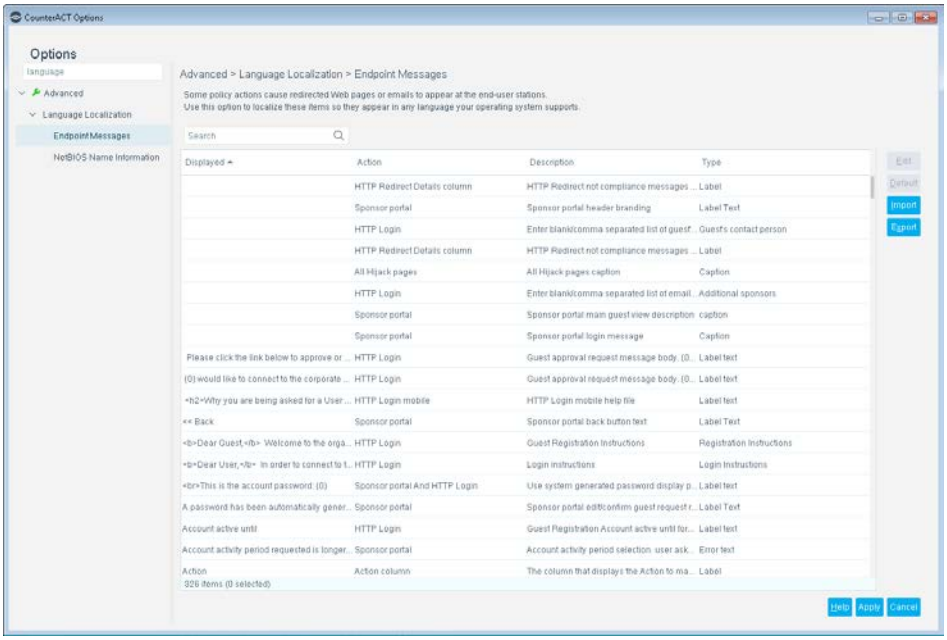
Some policy actions send web page messages and emails to endpoints. You can edit these messages or localize them so that they appear in any language your operating system supports. Actions that can be localized include, for example:

- HTTP Notification
- Windows Self Remediation
- HTTP Login
- Start SecureConnector
- Default Email Messages

To localize text:

1. Select **Options** from the **Tools** menu and then select **Advanced** > **Language Localization** > **Endpoint Messages**.

   The table lists text strings that CounterACT displays in various interactions between CounterACT and a detected endpoint.



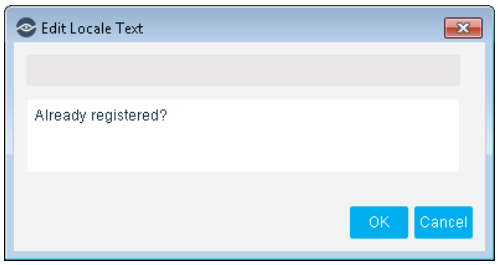
Localization>Endpoint Messages Pane

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. Do either one of the following actions:
   - Select a table entry and then select **Edit**.
   - Double-click a table entry.

   The **Edit Locale Text** dialog box opens and displays the text of the selected entry.



Edit Locale Text

4. In the **Edit Locale Text** dialog box, modify the text as needed.
5. Select **OK**.

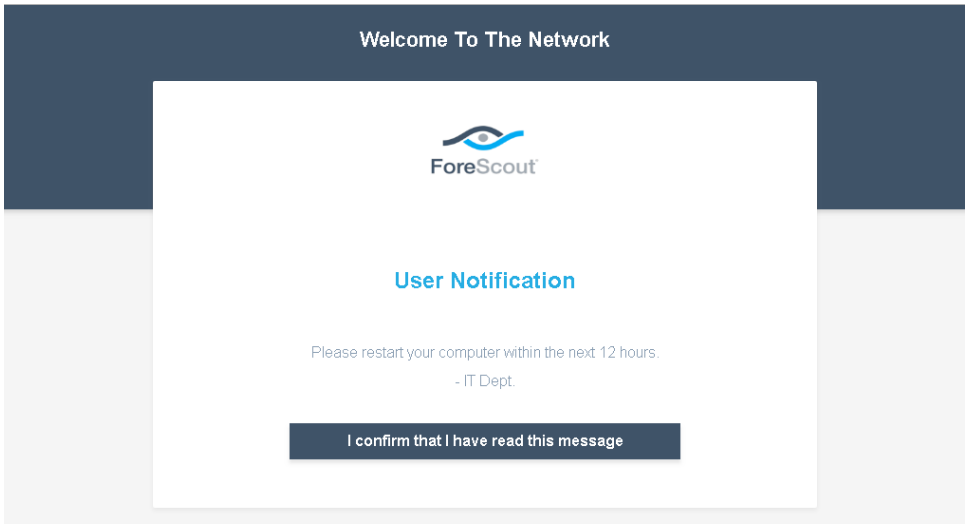
   *Select a table entry and then select **Default** to return to the default text.*

6. Select **Apply**. Your changes are saved in the CounterACT configuration.

Sample Web Pages

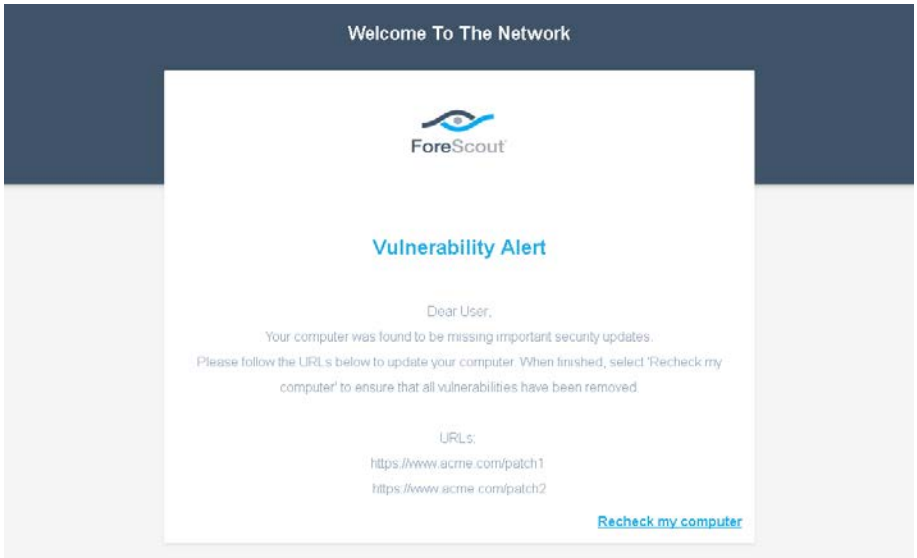
This section displays sample message pages that can be localized.

HTTP Notification



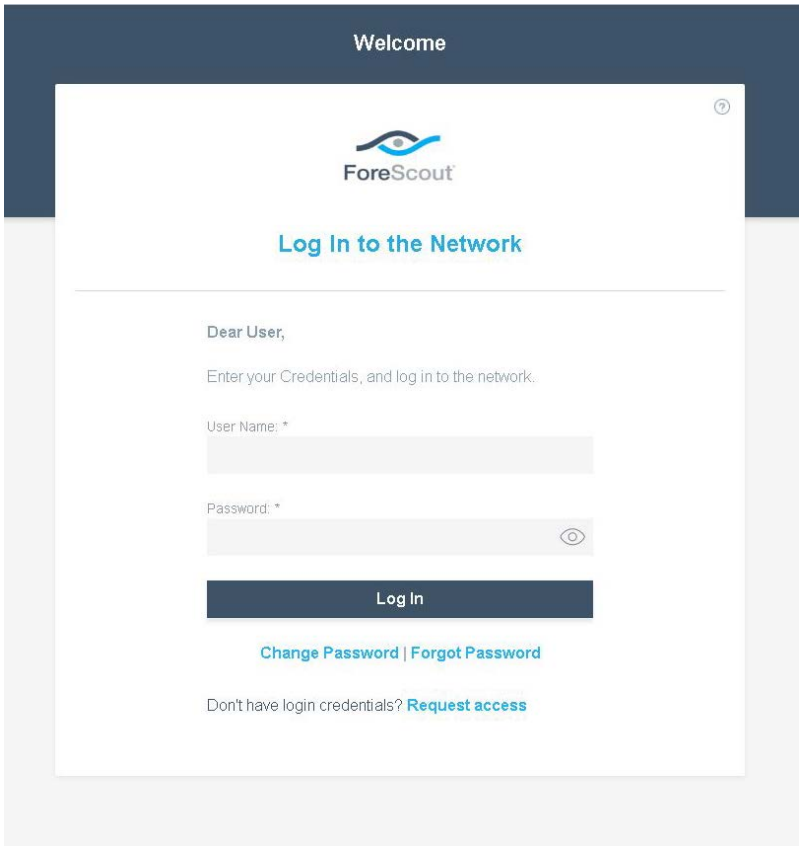
HTTP Notification Page

Windows Self Remediation



Localization, Missing Updates

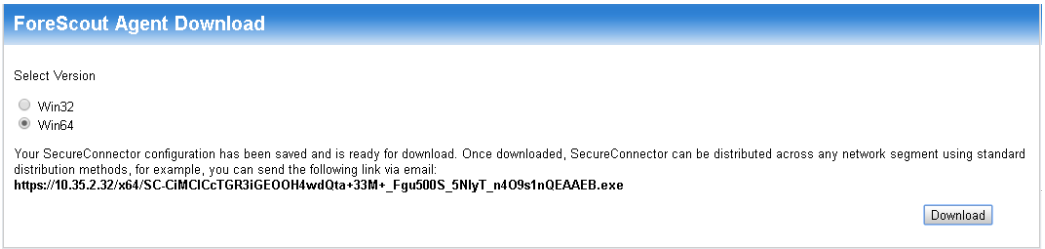
HTTP Login



Login Page

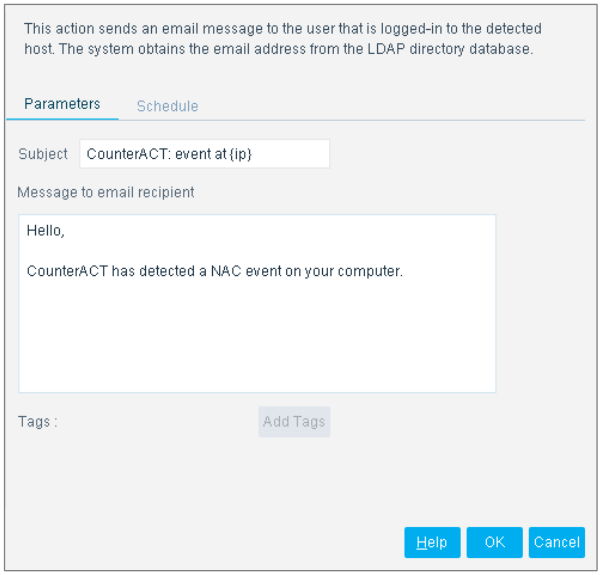
Start SecureConnector

SecureConnector

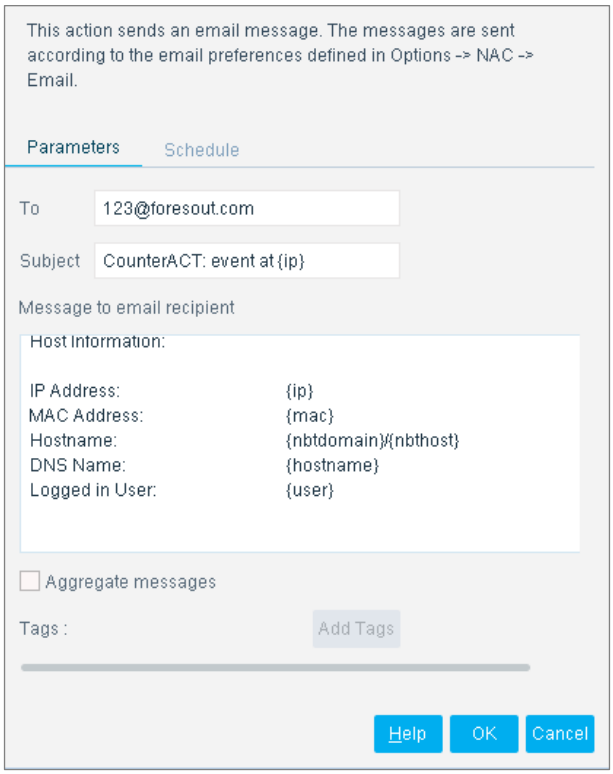


SecureConnector Link

Default Email Messages



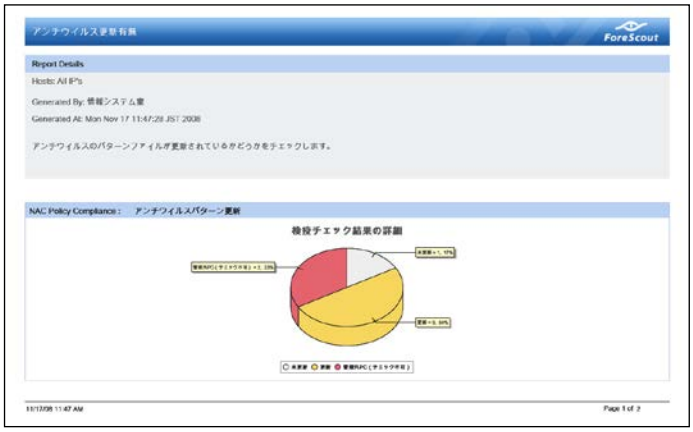
Send Email to User Action



Send Email Action

Displaying Local Languages in Reports, Actions and Other Features

CounterACT supports foreign text entered in reports, action, conditions and other features. No configuration is required to detect or display foreign language text.



Report Localization

Localizing Guest Management Portal Texts

You can customize the texts displayed in the Guest Management Portal. To customize texts, select **Options** > **Advanced** > **Language Localization** > **Endpoint Messages**. The Endpoint Messages pane opens. Search for **Guest Management Portal**.

For details about customizing texts that CounterACT processing generates in a user's endpoint, see Localizing CounterACT Redirected Web Pages and Messages.

Pre-Registration and Guest Registration Management

Many organizations want 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 Registration 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 either manually applied to a detected endpoint or applied during a CounterACT Corporate/Guest Control policy evaluation of detected endpoints.

Guest Management Portal

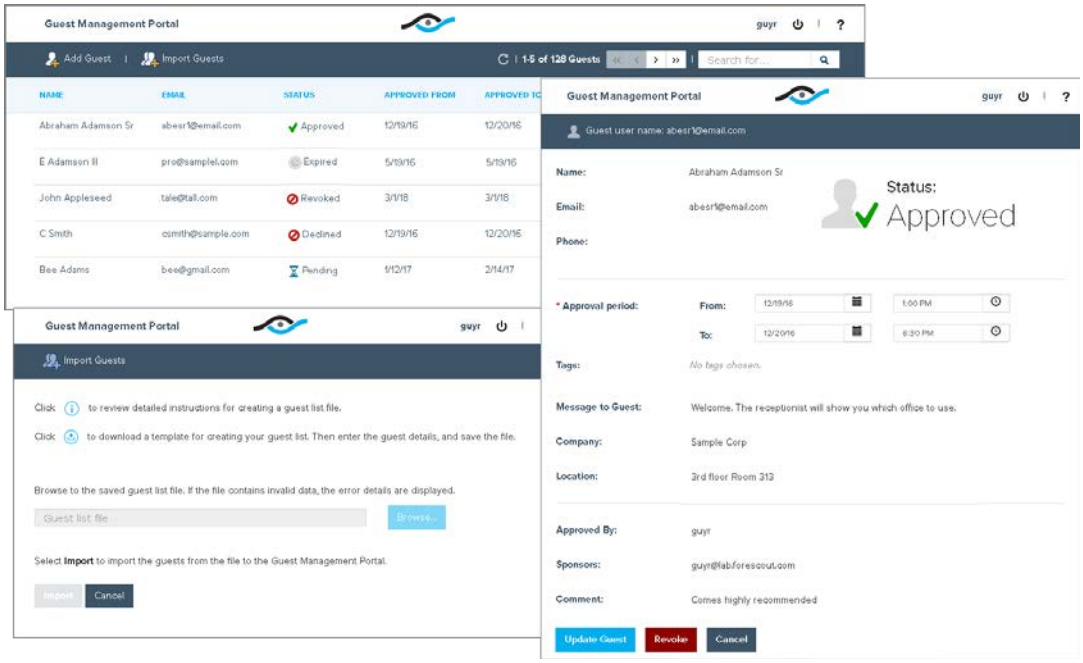
The Guest Management Portal is a Web-based portal that enables corporate personnel to view and manage network guests who have requested access to the organization's network. When access is approved, guests can browse the network and possibly use other network resources.

Individuals who manage network guests from this portal are referred to as *sponsors*.

Sponsors can use the Guest Management Portal for various tasks, including:

- Viewing all their sponsored guests.
- Importing lists of guests to be granted network access, and adding a single guest. These guests are automatically approved for network access.
- Approving and declining guests who registered for network access using the Guest Registration form.
- Revoking network access to guests who were approved.
- Assigning and updating network access approval periods.
- Assigning tags to guests. Tags can be used in CounterACT policies.

Sponsors' corporate email addresses must be included in the Sponsors table, or they will not be able to access the Guest Management Portal. See Sponsors.



The Guest Management Portal in your organization may look different from the examples shown in this document.

For detailed information about working with the Guest Management Portal, refer to both of the following documents.

- Guest Management for CounterACT Operators How-to Guide
- Guest Management Portal for Sponsors How-to Guide

See Additional CounterACT Documentation for information on how to access these guides.

You can localize the strings in the Guest Management Portal. See Localizing Guest Management Portal.

You can customize the appearance of the Guest Management Portal with the look-and-feel and branding requirements of your organization. For details, see Appendix 7: Customizing User Interfaces.

Guest Registration Pane

Use the Guest Registration pane to:

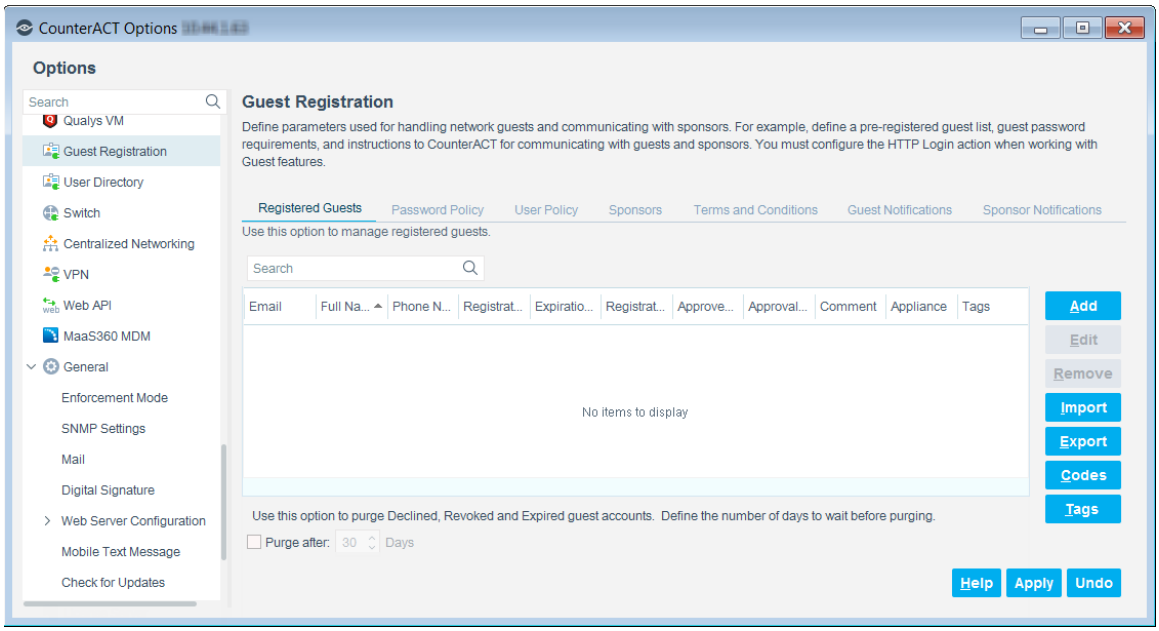
- Add approved guests, edit and remove them. Generate registration codes and administer guest tags. See Registered Guests.

  Individuals defined as Sponsors *can add and import pre-approved guests directly to the Guest Management Portal. Refer to the* Guest Management Portal for Sponsors How-to Guide*. See Additional CounterACT Documentation for information on how to access the guide.*

- Define a password policy that will be enforced when passwords are system-generated or self-selected by guests for login to the corporate network. See Password Policy.
- Define how certain guest fields are validated. See User Policy.
- Define the corporate sponsors who can use the Guest Management Portal for managing guests. See Sponsors.
- Define the terms and conditions for registered guests and for sponsors using the Guest Management Portal. See Terms and Conditions.
- Define the manner in which CounterACT notifies guests about the state of their guest registration requests. See Guest Notifications.
- Define the manner in which CounterACT notifies corporate sponsors about the state of guest registration requests that are assigned to be administered by the sponsor. See Sponsor Notifications.

When you are finished configuring the Guest Registration pane, select **Apply** to save your changes in the CounterACT configuration.

The CounterACT user who works with Guest Registration functionality must have the **Plugin Management** update permission. See Access to Console Tools – Permissions for more information.



Guest Registration Pane

To open the Guest Registration pane:

1. Select **Options** from the **Tools** menu and then select **Guest Registration**. The Guest Registration pane opens.

For more information about working with the Guest Registration pane, refer to the *Guest Management for CounterACT Operators How-to Guide*. See Additional CounterACT Documentation for information on how to access this guide.

Registered Guests

Guests can be managed from both the Guest Registration pane option in the Console and from the Guest Management Portal.

- Operators use the Registered Guests tab in the Guest Registration option of the Console to view and manage all guests.
- Sponsors use the Guest Management Portal to view and manage only guests assigned to them.
- Admin Sponsors use the Guest Management Portal to view and manage all guests that have registered for network access, and to override the decisions of other sponsors.

Task	Sponsors	Operators
View guests.	✔	✔
Add pre-approved guests, including the following information: ▪ Full name ▪ Email (Required) ▪ Phone number ▪ Comment	✔	✔
Add the following guest information: ▪ Date range of network access approval (Required) ▪ Tags ▪ Message to be sent to the guest ▪ Company name ▪ Location ▪ Comment	✔	
Add the following guest information: ▪ Password for network access.		✔
Create Tags.		✔
Approve network access for guests who submitted a Guest Registration form.	✔	
Decline network access for guests who submitted a Guest Registration form.	✔	
Revoke guests who have network access.	✔	
Remove guests from the Console and the Guest Management Portal lists.		✔
Automatically purge guests a certain number of days after their accounts expired, were declined, or were revoked. Purging removes them from the Console and the Guest Management Portal lists.		✔

In the Guest Registration, Registered Guests tab, you can perform the following guest management activities:

- Adding Guests Using the Console
- Removing Guests

- Purging Inactive Guests
- Editing Guests
- Retrieving Registration Codes
- Managing Guest Tags

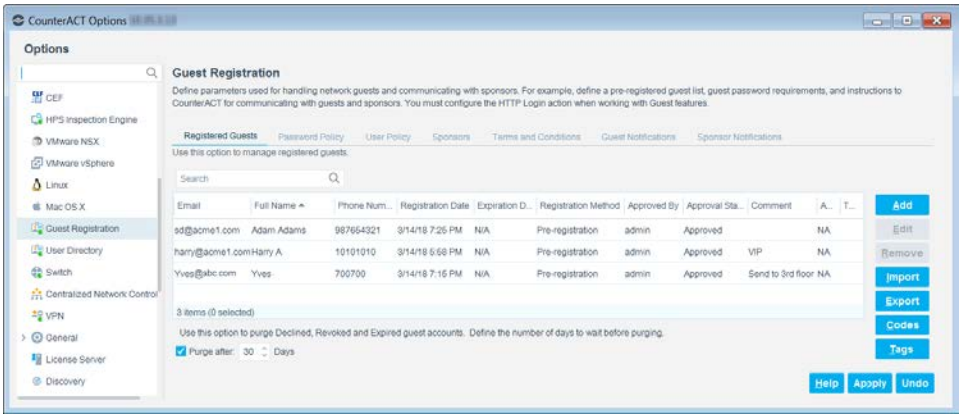
Adding Guests Using the Console

If you know ahead of time that your organization is expecting guests and you have their identity information, you can pre-approve the guests and later verify that they are authenticated.

Individuals defined as Sponsors *can add and import pre-approved guests directly to the Guest Management Portal. It is recommended to add guests using the Guest Management Portal. Refer to the* Guest Management Portal for Sponsors How-to Guide*. See Additional CounterACT Documentation for information on how to access the guide.*

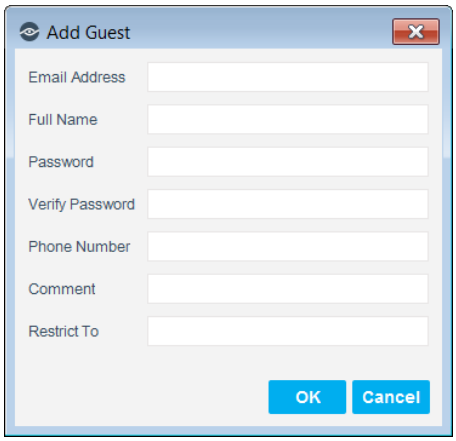
To view and add guests at the Console:

1. Select the Registered Guests tab of the Guest Registration pane. The list of guests is displayed.



Registered Guests

2. To add a guest, select **Add**. The **Add Guest** dialog box opens.



3. Complete the guest information, and provide a password for guest login.

   *The **Restrict To** field is not used in this version.*

4. Select **OK**.
5. After all guests have been added, select **Apply**. The added guests are automatically approved for network access.
6. It is the responsibility of your organization to forward the login credentials to guests added at the Console. CounterACT does not do this for you.

The Registered Guests tab also supports:

- Importing guest entries into the tab from a CSV file. To initiate this action, select Import.
- Exporting guest entries from the tab into a CSV file. To initiate this action, select Export.

Removing Guests

Guests that you remove are automatically and immediately signed out of the network, and their accounts are purged from both CounterACT and the Guest Management Portal. Users who are removed while still browsing are notified by a web message of this management action.

In the Guest Management Portal, sponsors can revoke their approved guests and decline guest requests. Refer to the Guest Management Portal for Sponsors How-to Guide*. See Additional CounterACT Documentation for information on how to access the guide.*

To remove a guest:

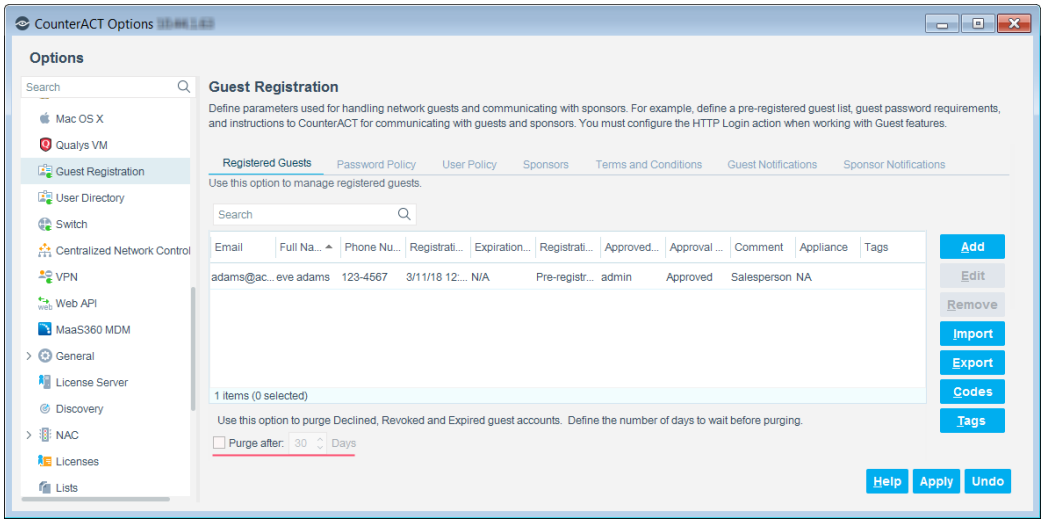
1. In the Registered Guests tab of the Guest Registration pane, select a guest entry.
2. Select **Remove** and then select **Apply**.

Purging Inactive Guests

Guests become inactive when their status is changed to Declined, Revoked or Expired. Guests can be automatically purged a certain number of days after they become inactive. Inactive guest accounts are purged from both the CounterACT Console and the Guest Management Portal.

To purge inactive guests:

1. Select **Options** from the Tools menu. The Options window opens.
2. Select **Guest Registration**.
3. At the bottom of the Registered Guests tab, select **Purge after**.



4. Enter the number of days to wait before a guest is purged after its status is set to *Declined*, *Revoked* or *Expired*.
5. Select **Apply**.

Editing Guests

You can edit guest registration values. If you update the password, you must notify the guest.

To edit a guest:

1. In the Registered Guests tab of the Guest Registration pane, select a guest entry.
2. Select **Edit**. The **Edit Guest** dialog box opens.
3. Update the guest information.
4. Select **OK** and then select **Apply**.

In the Guest Management Portal, sponsors can edit the approval period requested by guests. Refer to the Guest Management Portal for Sponsors How-to Guide*. See Additional CounterACT Documentation for information on how to access the guide.*

Retrieving Registration Codes

Registration codes are used when working with the *HTTP Login* action that requires guests to register before the Guest Registration request is processed. If the guest does not provide the correct code, the request is not processed. Use this feature to ensure that only guests with whom you've shared the registration code can apply for network access.

Enable the registration code option from the Registration Page tab in the *HTTP Login* action.

To retrieve registration codes to send to guests:

1. Select **Options** from the **Tools** menu and then select **Guest Registration**.

2. In the Registered Guests tab of the Guest Registration pane, select **Codes**. The Registration Codes dialog box opens and displays the daily registration codes.

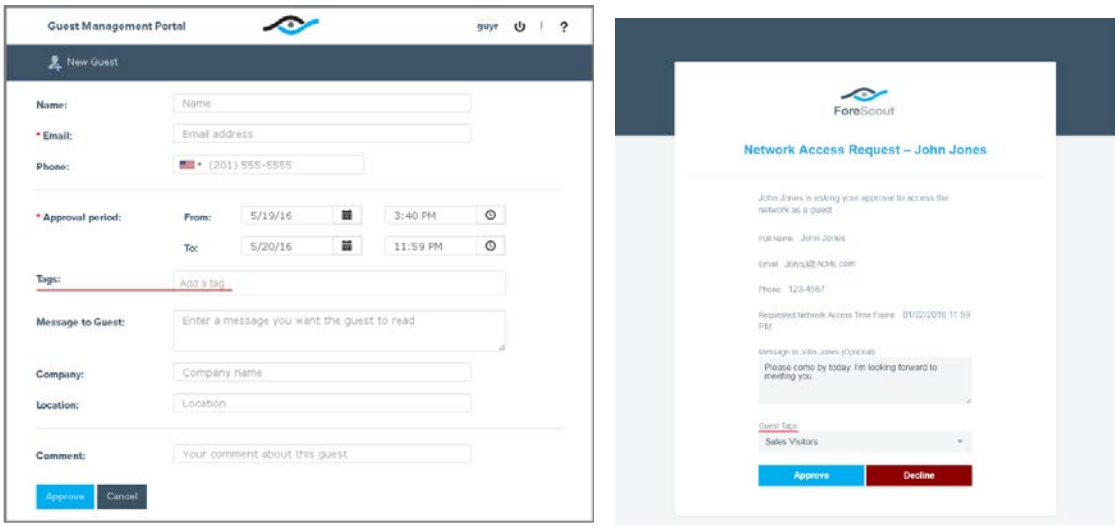
Registration Codes

3. A unique code is shown for each day. Identify the registration code for the day you expect your guest to require network access.
4. It is the responsibility of your organization to forward the code to the network guests. CounterACT does not do this for you.

Managing Guest Tags

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.

Use *guest tags* to categorize network guests into specific groups as they are being approved/declined network access by a sponsor. For example, *Limited Access* guests, *Full Access* guests, *Building A* guests and *Sales Visitors* guests.



Guest Tags Selected by Sponsors

These tools are available when **Guests must be approved by the sponsor...** is selected in the **Guests** tab of the *HTTP Login* action.

The CounterACT administrator creates guest tags, and a sponsor, using the Network Access Request page to approve/decline guests, can assign tags to guests.

To work with tags, perform the following:

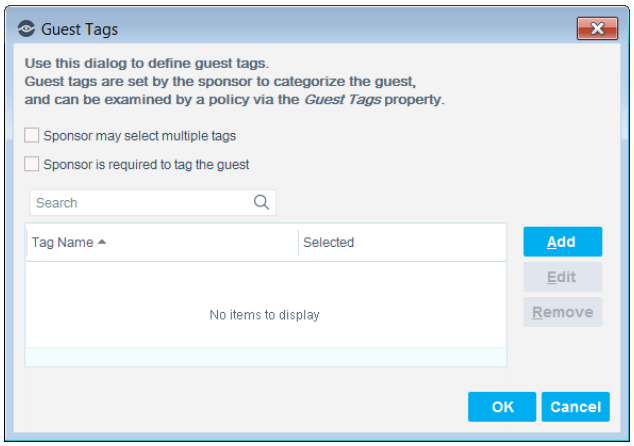
- Create Tags
- Assign Tags
- Create Policies with Your Tags

Create Tags

Create tags that sponsors can assign to guests.

To create tags:

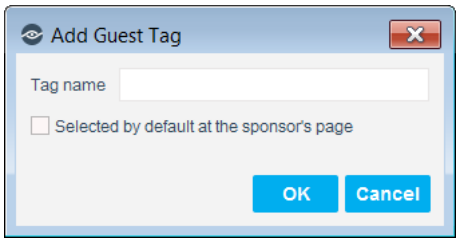
1. Select **Options** from the **Tools** menu and then select **Guest Registration**.
2. In the Registered Guests tab, select **Tags**. The Guest Tags dialog box opens.



Guest Tags dialog box

3. In the Guest Tags dialog box, you can select guest tag options:
   - **Sponsor may select multiple tags**: Selecting this option enables the sponsor to assign the guest multiple tags.
   - **Sponsor is required to tag the guest**: Selecting this option makes it mandatory for the sponsor to assign the guest one or more tags.

   If you do not select any option, sponsors can optionally assign each guest a single tag.
4. Select **Add**. The Add Guest Tag dialog box opens.

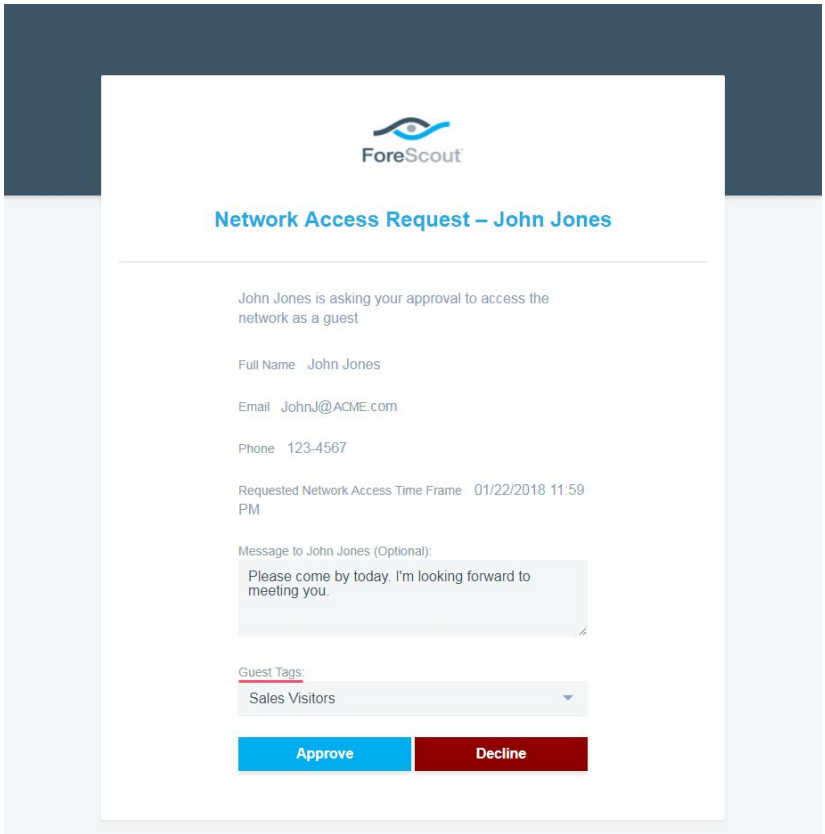


Add Guest Tag

5. Enter the tag name.
6. If you select **Selected by default at the sponsor's page**, the tag is displayed when the Add Guest page is opened in the Guest Management Portal. The sponsor can manually remove it.
7. Select **OK**.
8. After all tags have been added, select **OK** to save the created guest tags in the CounterACT configuration.

Assign Tags

Sponsors can assign tags to guests when approving/declining guest network access using a Network Access Request page, and when adding guests in the Guest Management Portal. Guest tag assignment is not available to sponsors when approving pending guests in the Guest Management Portal.

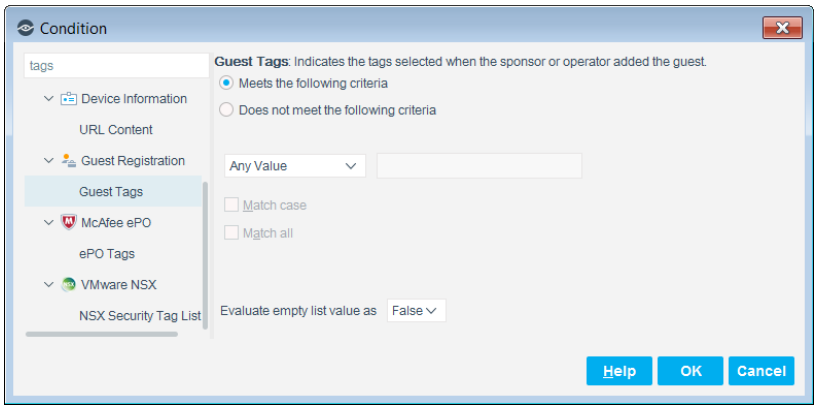


Network Access Request Page with Tags

Create Policies with Your Tags

Guest Tags property values come from the tags that you create. See Create Tags. For example, if you created a *Limited Access* guest tag, this tag appears as a property value to select.

Control guests based on their guest tags. Do this by incorporating the evaluation of the **Guest Tags** property in your policies. For example, create a policy that detects guests with an *Authentication, Signed In Status* property value of *Signed In as a Guest* and a *Guest Tag* property value of *Building A* and then assigns them to a specific VLAN or allows them minimum network access.



Guest Tags Property

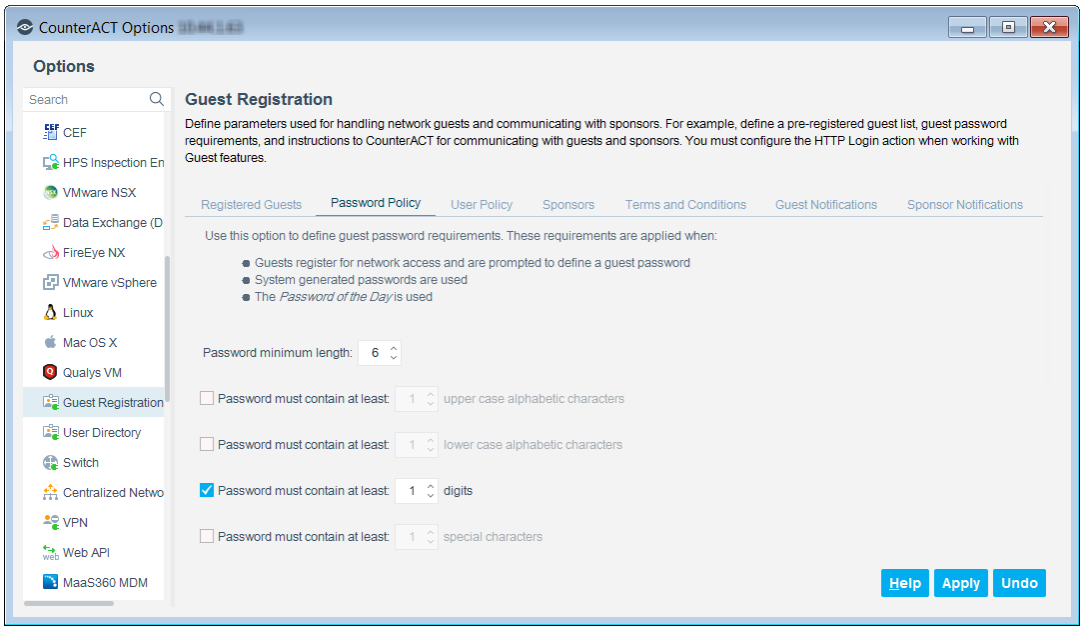
To incorporate guest tags:

1. Edit or create a policy.
2. Define the condition so it includes the *Guest Registration* > *Guest Tags* property. The list of available property values contains all the tags created in the Guest Registration pane.

Password Policy

Use the **Password Policy** tab to define requirements enforced on passwords that are used by approved guests to log in to the network. These requirements are applied to both system-generated passwords for guest login and passwords that registering guests define by themselves for login.

When defining the *HTTP Login* action, in the **Guests** tab, select the option **Provide a system-generated password to self-registering guests** to have CounterACT generate passwords for guest login.

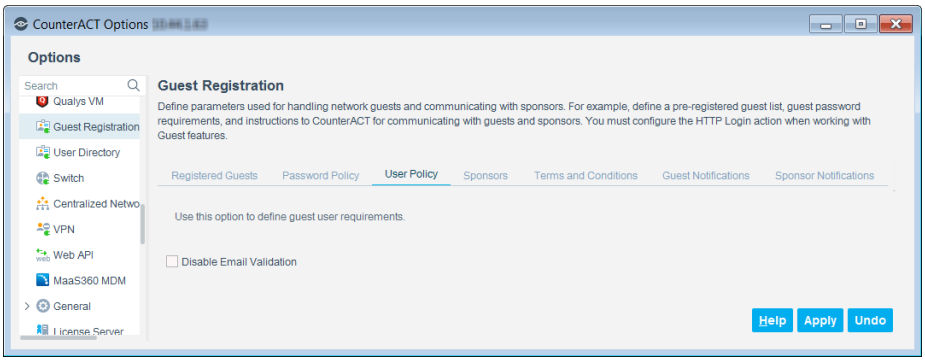


Password Policy Tab

1. Define any of the following password requirements:
   - Minimum password length - the default, minimum length is 6 characters
   - Minimum number of uppercase characters to include
   - Minimum number of lowercase characters to include
   - Minimum number of digits to include
   - Minimum number of special characters to include
2. Select **Apply** to save your changes in the CounterACT configuration.

User Policy

In the Guest Registration window, use the **User Policy** tab to define how certain guest fields are validated.



User Policy Tab

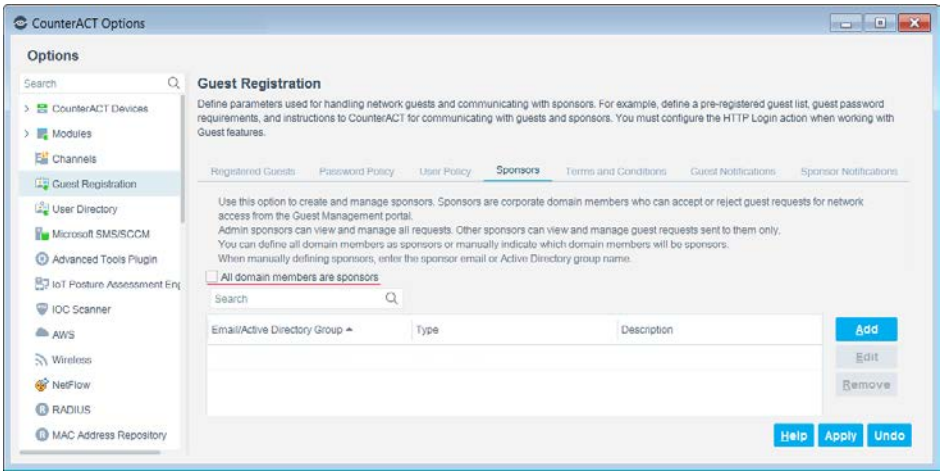
The *Email* field is always mandatory for guests, and guests are identified by its contents.

- Clear the **Disable Email Validation** checkbox to ensure that this field contains a valid email address.
- In environments where guests are identified by information other than their email address, select the **Disable email validation** checkbox so that no validation is done on the field. Any value will be accepted in the *Email* field.

Sponsors

In the Guest Registration window, use the **Sponsors** tab to define the corporate sponsors who are authorized to log in to the Guest Management Portal and use the portal to manage guests. Corporate employees whose contact emails are provided by guests in the Guest Registration form must be included in the Sponsors table. The tab provides **Add**, **Edit** and **Remove** sponsor capabilities.

All sponsor email addresses must be configured in Active Directory.

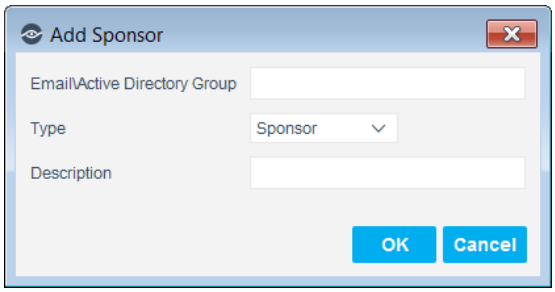


Sponsors Tab

In the tab, you can select the **All domain members are sponsors** option to make sponsors of all user directory domain members.

Add sponsors in any of the following ways:

- Individually, by defining an email address
- As a group, by defining an Active Directory group
- Globally, by selecting all Active Directory members



Add Sponsor

Define the following sponsor information:

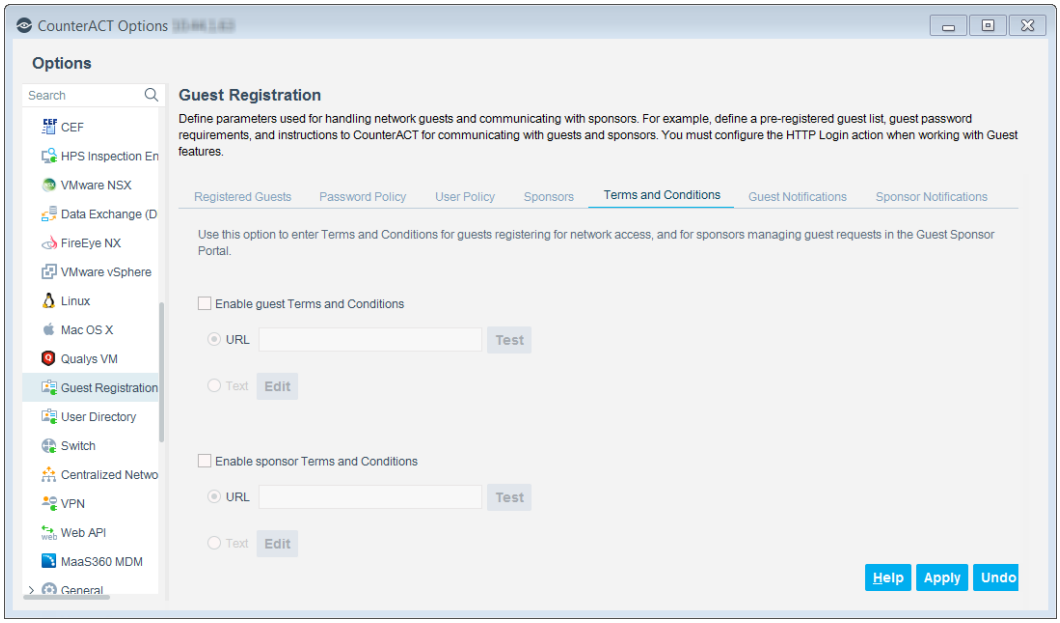
- Email or Active Directory Group (*required*): specify either a sponsor's Active Directory email address or specify an Active Directory group. Specifying an Active Directory group makes sponsors of all Active Directory group members.
- Type (*required*): One of the following sponsor types must be assigned to each sponsor entry:
  - **Sponsor** - A *Sponsor* can access the portal to view and manage guests assigned to them only.
  - **Admin Sponsor** - An *Admin Sponsor* can access the portal to view and manage all guests that have registered for network access, and can override the decisions of other sponsors.
- Description (*optional*)

Select **Apply** to save your changes in the CounterACT configuration.

Terms and Conditions

Use the **Terms and Conditions** tab to enable the presentation of terms and conditions to any of the following recipients:

- Only registering guests
- Only sponsors (working in the Guest Management Portal to manage guests)
- Both of the above



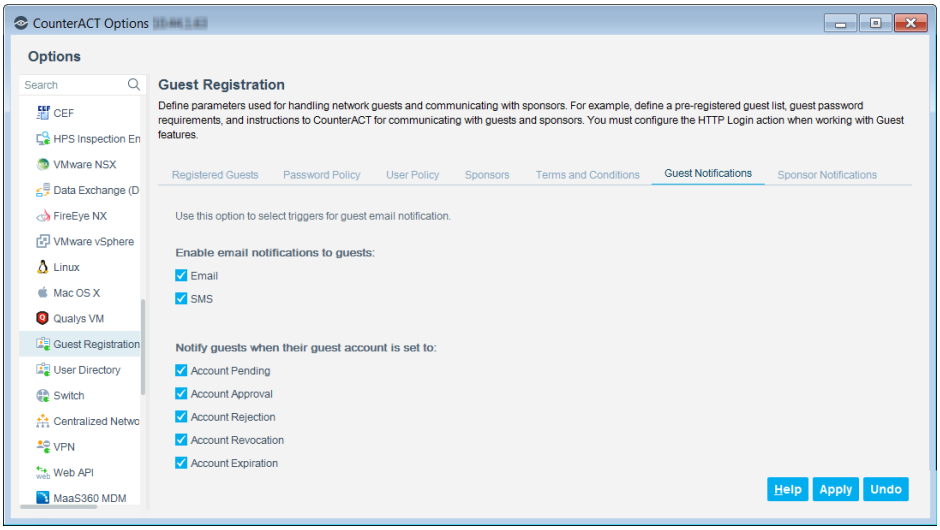
Terms & Conditions Tab

1. Specify the terms and conditions to be presented to recipients using one of the following methods:
   - Select the **URL** option. In the associated field, provide the absolute URI of a Web page for presentation to the designated recipients. Select **Test** to ensure that the address is correct.
   - Select the **Text** option and select **Edit**. A <recipient> Terms & Conditions window opens. In the window, enter or update the terms and conditions to be presented to the designated recipients. Select **OK**.
2. Select **Apply** to save your changes.

Guest Notifications

Use the **Guest Notifications** tab to instruct CounterACT about guest notification method and triggers.

- Use either or both of the following media to send notifications to guests:
  - Email
  - SMS (text messaging)
- Optionally notify guests about the state of their network access when:
  - Their guest registration request is pending.
  - Their guest registration request is approved.
  - Their guest registration request is rejected.
  - Their previously approved network access is revoked. This state can only occur when the managing sponsor of the guest is working with the Guest Management Portal.
  - Their network access period has expired.



Guest Notifications Tab

Customize Guest Notifications

In the Console, customize notifications that CounterACT sends to guests. To customize notifications, select **Options** > **Advanced** > **Language Localization** > **Endpoint Messages**. The Endpoint Messages pane opens.

For details about customizing texts that CounterACT processing generates in a user's endpoint, see Localizing CounterACT Redirected Web Pages and Messages.

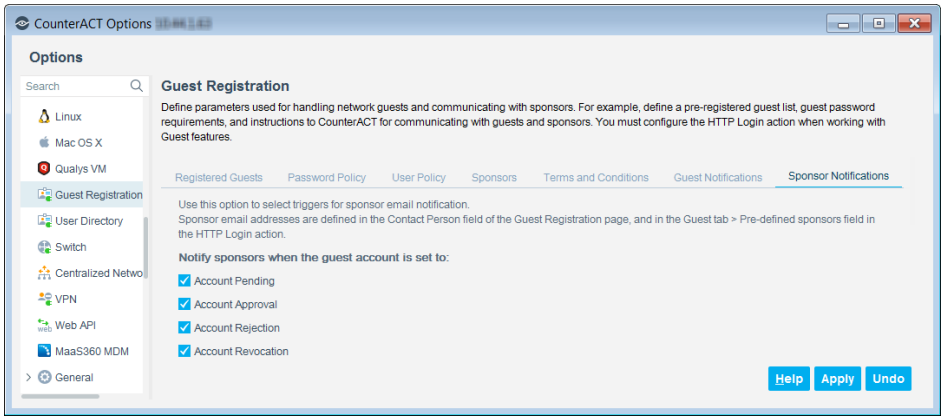
Sponsor Notifications

Corporate personnel are considered a sponsor of a guest when either one of the following conditions is true:

- The registering guest specified the person's email address in the Contact Person Email field of the Guest Registration form.
- The person's email address is provided in the **Pre-defined sponsors for all guests** field in the **Guests** tab of the *HTTP Login* action.

Use the **Sponsor Notifications** tab to instruct CounterACT to notify sponsors about any or all of the following guest network access events:

- A guest registration request is pending for a guest for whom they are a sponsor.
- A guest registration request is approved for a guest for whom they are a sponsor.
- A guest registration request is rejected for a guest for whom they are a sponsor.
- A guest registration request is revoked for a guest for whom they are a sponsor. This event can only occur when a managing sponsor of the guest is working with the Guest Management Portal.



Sponsor Notifications Tab

Select **Apply** to save your changes in the CounterACT configuration.

Customize Sponsor Notifications

In the Console, customize notifications that CounterACT sends to sponsors. To customize notifications, select **Options** > **Advanced** > **Language Localization** > **Endpoint Messages**. The Endpoint Messages pane opens.

For details about customizing texts that CounterACT processing generates in a user's endpoint, see Localizing CounterACT Redirected Web Pages and Messages.

The ForeScout Research and Intelligent Analytics Program

ForeScout continually attempts to provide better classification and posture assessment services to customers. Customers who voluntarily opt in to the ForeScout Research and Intelligent Analytics Program allow anonymous information from their environment, such as policy-based or manual endpoint classification, to be shared with ForeScout researchers for improving the product. It also allows you to share with ForeScout additional information regarding your classification changes that will aid ForeScout in capturing your requirements in future content updates. By contributing to the ForeScout Research and Intelligent Analytics Program, you benefit from a better out-of-the-box classification service.

Refer to the *ForeScout Research and Intelligent Analytics Program Data Security Document* for an up-to-date list of the shared properties and how they are anonymized. See Additional CounterACT Documentation for information on how to access this document.

Using analytics, ForeScout researchers can use the anonymous data shared by you and other customers to:

- Develop classification profiles for new devices
- Better classify existing devices
- Reduce the number of false positive classifications
- Develop new techniques for assessing endpoint posture

The ForeScout Research and Intelligent Analytics Program is a voluntary program. Customers are under no obligation to share their data to help ForeScout improve classification. In the long term, the program benefits customers in the form of more detailed classification profiles.

By default, after you accept the ForeScout Research and Intelligent Analytics Program participation terms, your CounterACT devices share selected endpoint properties with ForeScout.

Before any data is uploaded, all personally identifiable information (PII) is removed, and potentially sensitive data is sanitized. For example:

- Usernames, as well as other information garnered from the corporate user directory about the logged in users, are removed.
- The IP and MAC addresses of endpoints are converted to simulated addresses using a one-way function which ensures that the data shared with ForeScout can never reveal the actual addresses of endpoints in your network.

Anonymized properties from managed CounterACT Appliances are transmitted to the Enterprise Manager which uploads the information to the ForeScout Research and Intelligent Analytics Program. Each Appliance uploads (via the Enterprise Manager) no more than once per day. For example, if you have one Enterprise Manager and five Appliances, six distinct uploads will run at random times each day.

The Enterprise Manager connects to a server named ds.forescout.com *using HTTPS (port 443/TCP). Ensure that your firewall is configured to allow this, or configure the proxy server settings.*

Sharing Additional Endpoint Properties

You can additionally opt to share properties created by the CounterACT Flow Analyzer which detects flow information regarding the endpoints in your environment. The Flow Analyzer collects a statistical sampling of data about network traffic, such as average packet size, average packet rate per second, inbound and outbound bandwidth usage, and DNS resolutions. Sharing these additional properties would be an important contribution to the ForeScout Research and Intelligent Analytics Program.

The purpose of the Flow Analyzer is to provide additional properties to the ForeScout Research and Intelligent Analytics Program. Properties resolved by the Flow Analyzer are not available to an administrator in the Policy Manager.

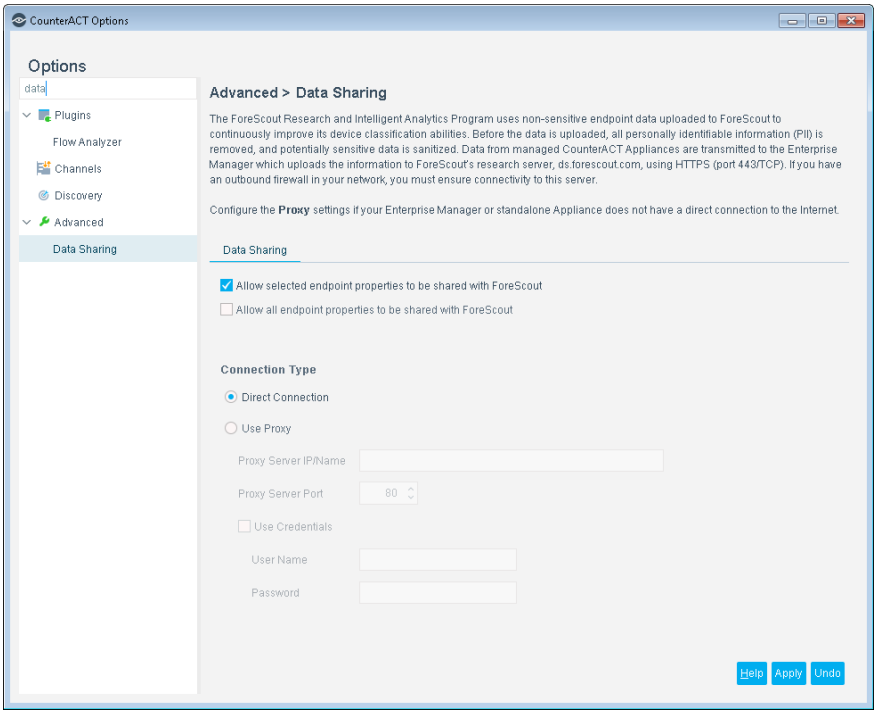
You can additionally opt to allow CounterACT to share other properties. Refer to the *ForeScout Research and Intelligent Analytics Program Data Security Document* for an up-to-date list of these additional shared properties. See Additional CounterACT Documentation for information on how to access this document.

Opting In or Out of Data Sharing

If you have not yet accepted or rejected the ForeScout Research and Intelligent Analytics Program participation terms, you will be prompted to accept the participation terms each time you log in to CounterACT.

To opt in or out of data sharing:

1. In the Console main menu, select **Tools>Options**. In the Options tree, select **Advanced>Data Sharing**.



Data Sharing Dialog Box

2. To opt in to the program, select **Allow selected endpoint properties to be shared with ForeScout**. The Participation Terms open.

Participation Terms

3. In the Participation Terms window, select **I accept these Terms**, and select **OK**. In the Data Sharing window, **Allow selected endpoint properties to be shared with ForeScout** is selected.
4. To opt out of the program, clear **Allow selected endpoint properties to be shared with ForeScout**.
5. Configure the *Proxy* settings if your Enterprise Manager does not have a direct connection to the Internet.
6. Select **Apply**.

Appendix 1: Handling Network Connectivity Failures

This appendix details how to handle network connectivity failures between the Appliance and your enterprise network.

During installation, a connectivity test is performed to verify that packets are properly injected into the network and that CounterACT sees symmetric traffic on the monitoring interfaces. That is, for every session, both incoming and outgoing directions are visible. In addition to being run automatically during installation, the test will also be run after configuration changes are made to the network (for example, NAC or Active Response range, Ethernet NIC, VLAN).

There are several reasons the test results may not be successful:

1. 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.

   Symptom: A message to this effect is shown.

   What to do: Make sure CounterACT is connected to the mirroring port and sees live data.

2. The mirroring port is misconfigured in such a way that only one side (incoming or outgoing) is mirrored.

   Symptom: This will result in all the sessions being asymmetric.

   What to do: Configure the switch to mirror both incoming and outgoing traffic.

3. There is an asymmetric routing of packets going in to and out of the containment cell.

   Symptom: Some asymmetric sessions are detected.

   What to do: 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).

4. The wrong port is mirrored.

   Symptom: Not much traffic is seen, as in (1) or some asymmetric sessions are detected, as in (3).

   What to do: Mirror the right port.

5. The packet loss rate is high.

   Symptoms: Some asymmetric sessions are detected.

   What to do: 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).

6. Some of the traffic in one direction is encapsulated (tunneled).

   Symptom: Some asymmetric sessions are shown.

   What to do: Either mirror traffic after it is de-encapsulated or mirror when both directions are encapsulated (and is ignored).

7. Some traffic is tagged with VLAN IDs, which are not defined in the system.

   Symptoms: Number of "Wrong VLAN ID" packets detected is shown.

   What to do: Define proper VLAN IDs (Channel configuration) or instruct the switch to remove the VLAN ID while mirroring (if only one VLAN is mirrored).

Appendix 2: Remote Access to Endpoints

- When Is Remote Access to Endpoints Needed?
- Domain Account Requirements
- Troubleshooting Domain Credentials
- Troubleshooting Deep Inspection

When Is Remote Access to Endpoints Needed?

CounterACT needs remote access to the endpoint's registry service to properly access service pack installations, antivirus installations, and perform other important tasks. This appendix details how to obtain remote access.

Domain Account Requirements

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 options available depend on the Windows version running on the endpoints. Options include:

- Using a Domain-Wide Policy. This option is recommended for Windows 2000-style domains.
- Using an Administrator Group. This option may be used with Windows NT-style domains.
- Using the Security Configuration wizard. This option may be used with Windows Server 2003 Service Pack 1.
- Set ACL Remotely Using the SetACL Tool. This option may be used with Windows NT-style domains.

Using a Domain-Wide Policy

This option is only available to Windows 2000-style domains that support ACL-level control through domain-wide registry policies. This is the recommended option for Windows 2000 style domains.

To configure the account:

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). Note that the time it takes for this configuration to be propagated to endpoints may vary, depending on network configuration and traffic.

Set registry processing options as follows:

1. Open the Group Policy MMC.
2. Select the Default Domain Policy, and go the Group Policy section.
3. Select Default Domain Policy and then Computer Configuration, Administrative Templates, then System, Group Policy.
4. 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.

Using an Administrator Group

You can create a new user account in the Global administrator group. This option may be used with Windows NT-style domains.

To set up configuring the account:

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.

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**.

Refer to the following Microsoft link for more information about this tool:

http://www.microsoft.com/downloads/details.aspx?FamilyID=903fd496-9eb9-4a45-aa00-3f2f20fd6171&displaylang=en

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 CounterACT can perform remote inspection on these machines. This means that 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 CounterACT can retrieve Windows related information.

It is recommended to allow access from all CounterACT devices to each endpoint. This ensures that no matter where the endpoint is located, it is managed by the system. This means, 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 CounterACT devices.

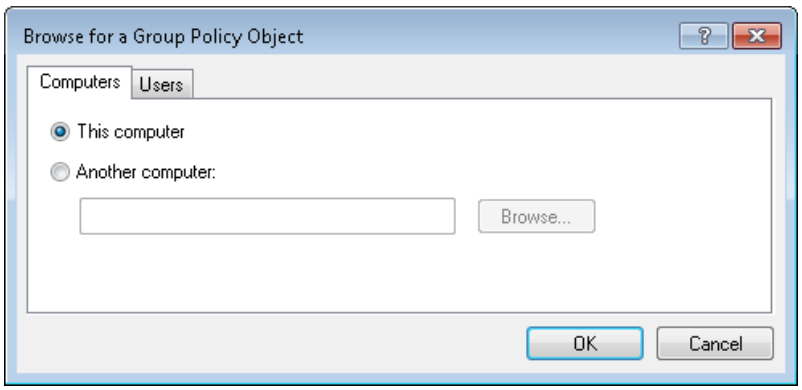
Updating Group Policy Objects with New Windows Firewall Settings

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).

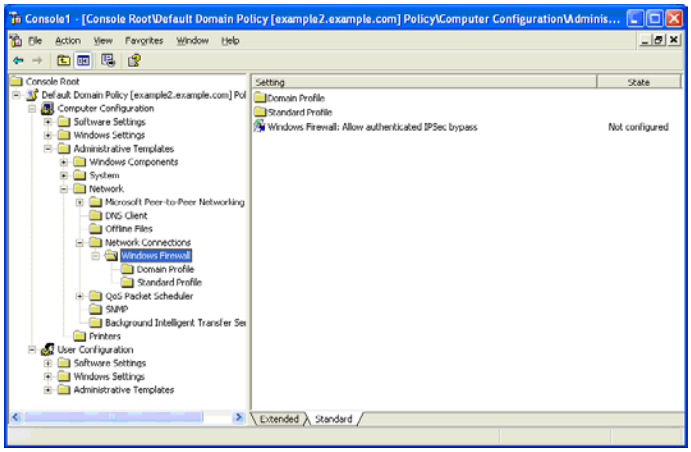
To update these objects:

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**, type **mmc**, and then select **OK**.
4. On the **File** menu, select **Add/Remove Snap-in**.
5. On 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 want to update with the new Windows Firewall settings.



Group Policy Object Box

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, open **Computer Configuration**>**Administrative Templates**>**Network**>**Network Connections**>**Windows Firewall**.



Windows Firewall Tree

14. Select **Domain Profile** and then **Windows Firewall**: Define port exceptions.
15. Select **Enabled**.
16. Select **Show**.
17. Select **Add**.
18. Define the desired 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**.

A restart may be needed on the client machines in order for this definition to take effect.

Troubleshooting Domain Credentials

This section describes Domain Credential troubleshooting procedures:

A. Test the Domain Credentials

B. Test the Credentials on the Endpoint Using a Localhost Query

C. Test the Credentials in the Endpoint Using Remote Query

A. Test the Domain Credentials

Perform the following steps to test the domain credentials.

1. Log in to an endpoint using the CounterACT user name and password. If this fails, check the CounterACT 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.

B. 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 CounterACT 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:

```
Local name
Remote name   \\127.0.0.1\C$
Resource type   Disk
Status   OK
# Opens   0
# Connections   1
The command completed successfully.
```

   If this test fails:

   – 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.

C. 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 CounterACT user

If this fails, check the following:

a. Domain Configuration

b. TCP/IP Configuration

c. Port Setup

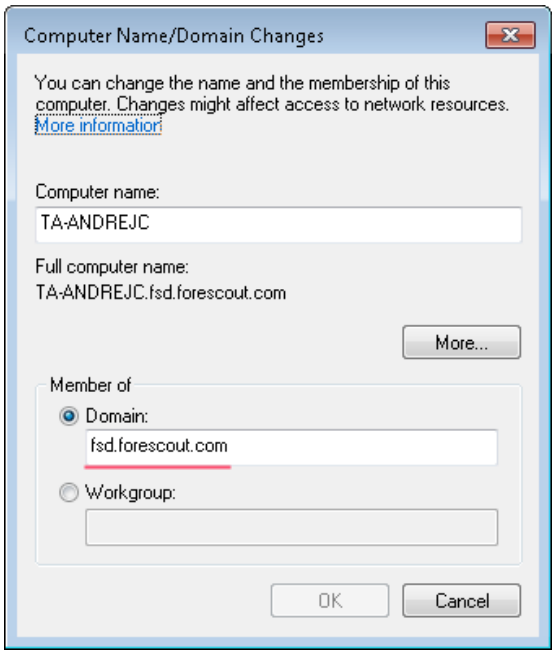
d. NetBIOS over TCP/IP Setup

e. Services

f. Shares

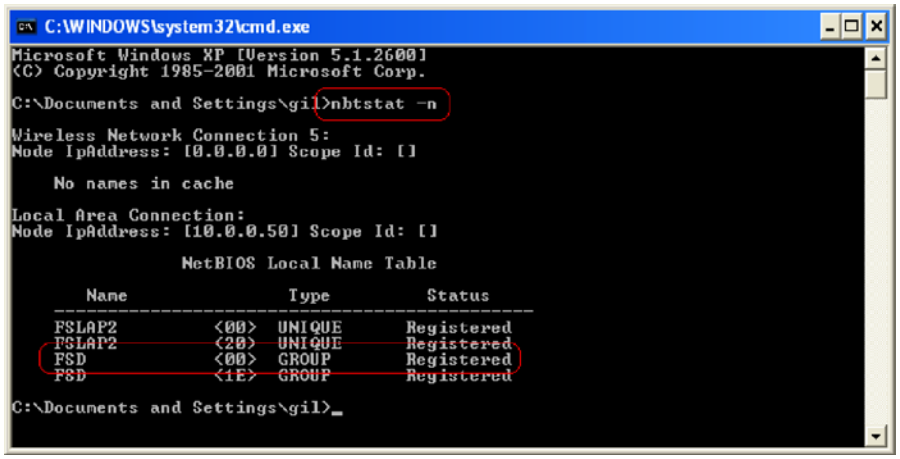
a. Domain Configuration Test

1. Open the System dialog.
2. Select **Start**, select **Run**, type **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.



Computer Name Change Dialog Box

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.



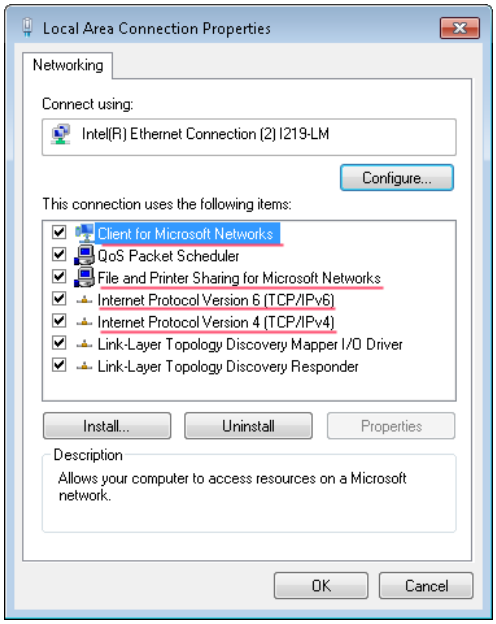
NetBIOS Domain Name

b. TCP / IP Configuration Test

Open the properties dialog box of the relevant network connection.

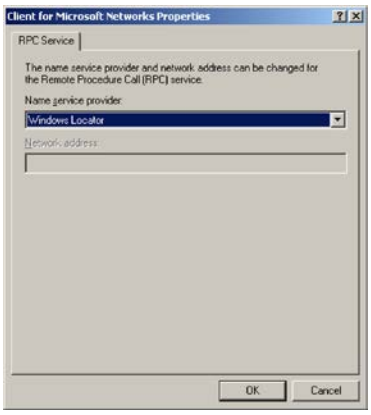
To open the dialog box:

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).



Local Area Connections Dialog Boxes

3. The “Client for Microsoft Networks” should be configured as follows:



RPC Service Dialog Box

c. Port Setup Test

CounterACT should have access to either one of the following ports: 139/TCP, 445/TCP.

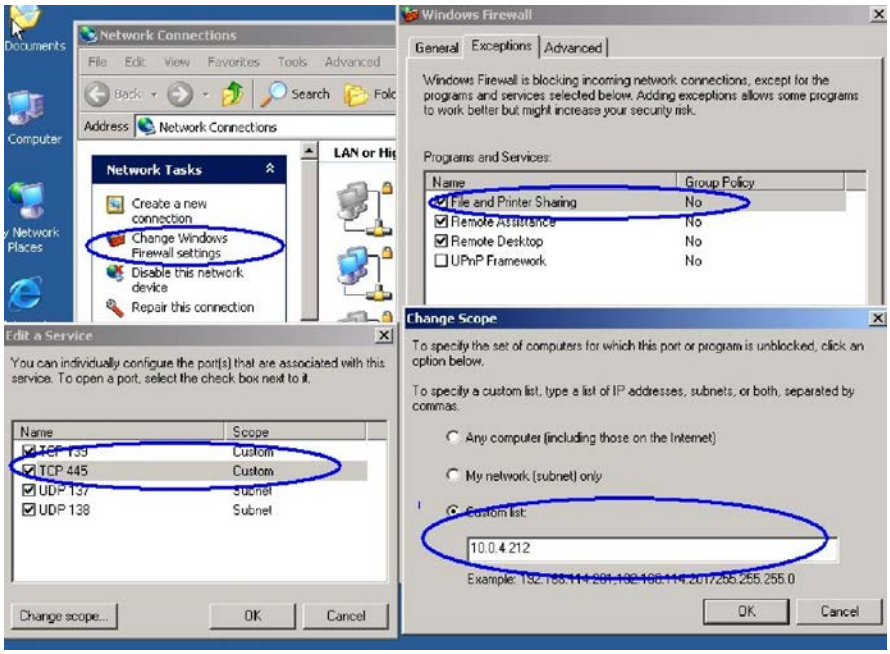
Group policy test

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** and **Printer sharing**. Ports TCP 139 and TCP 445 should be set.
2. Select **Change Scope** and in the Custom List add the CounterACT device IP address.



Local Firewall Configuration

Disabling the firewall

For testing purposes the firewall can be disabled.

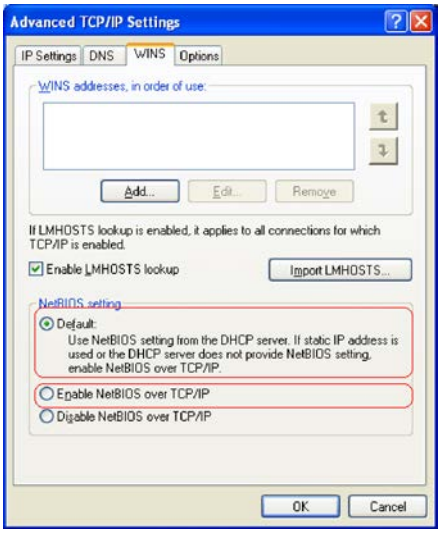
To disable the firewall:

1. In the Advanced tab, select **Setting** from the **Windows Firewall** group.
2. Disable the firewall by turning it off.

Windows Firewall Dialog Box

d. NetBIOS over TCP/IP Setup Test

NetBIOS over TCP/IP should be enabled either directly or from the DHCP server. One of the options in red below should be enabled:



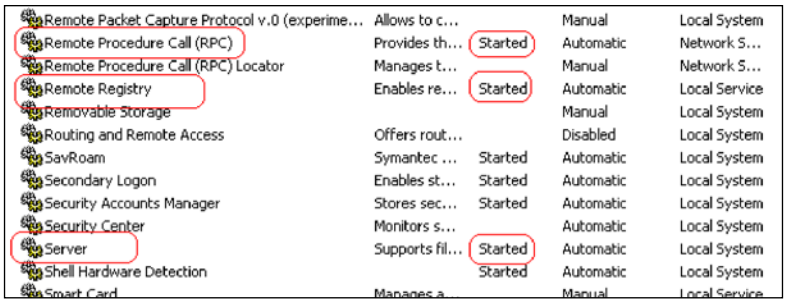
NetBIOS over TCP/IP option

e. 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



Remote Packet Capture Protocol v.0 (experime...	Allows to c...		Manual	Local System
Remote Procedure Call (RPC)	Provides th...	Started	Automatic	Network S...
Remote Procedure Call (RPC) Locator	Manages t...		Manual	Network S...
Remote Registry	Enables re...	Started	Automatic	Local Service
Removable Storage			Manual	Local System
Routing and Remote Access	Offers rout...		Disabled	Local System
SavRoam	Symantec ...	Started	Automatic	Local System
Secondary Logon	Enables st...	Started	Automatic	Local System
Security Accounts Manager	Stores sec...	Started	Automatic	Local System
Security Center	Monitors s...		Automatic	Local System
Server	Supports fil...	Started	Automatic	Local System
Shell Hardware Detection		Started	Automatic	Local System
Smart Card	Manages a...		Manual	Local Service

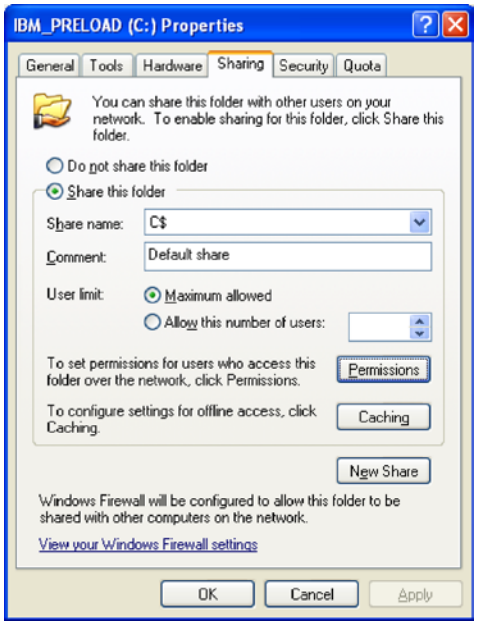
2. If any of them is not running then start it (right-click>**Start**).

f. 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

Verify the following if you cannot perform deep inspection on network Windows endpoints:

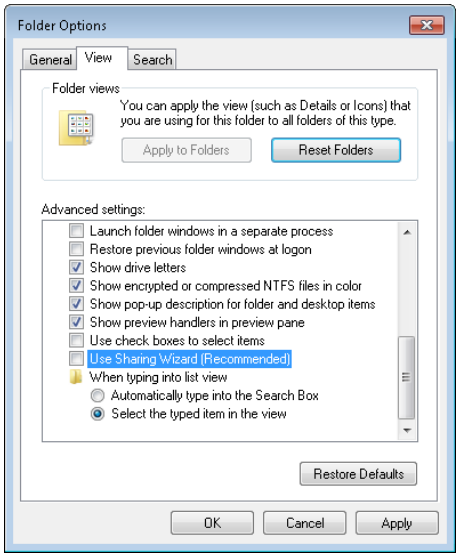
- Windows 2000
- Windows XP
- Windows Server 2000
- Windows Vista
- Windows 7

- Windows Server 2003
- Windows Server 2008

  32-bit and 64-bit machines are supported.
- 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 CounterACT 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 CounterACT 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).

To clear Use Simple File Sharing:

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**.



Use Sharing Wizard Dialog Box

Appendix 3: Generating and Importing a Trusted Web Server Certificate

This appendix describes how to generate and import a trusted certificate and remove the browser security warning that opens when trying to access the CounterACT Web Portals; for example, the Assets Portal or the Reports Portal.

This appendix describes how to generate and import a trusted certificate and remove the browser security warning that opens when trying to access the CounterACT Web Portals; for example, 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.

The procedure described below should be carried out on the Enterprise Manager and each system Appliance, as required.

During the installation of the Appliance or Enterprise Manager, a default self-signed certificate is created for this purpose. However the certificate was not signed by a CA such as VeriSign or Thawte. This causes the web browser not to trust the self-signed certificate. As a result, a security alert warning appears each time you connect to a CounterACT portal.

Initial Warning Message

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 and import a trusted certificate, as follows:

1. Generate a Certificate Signing Request (CSR), with your company details.
2. Submit the CSR to a Certificate Authority and request a signed TLS certificate.
3. Import the signed certificates you receive.

For detailed information about defining and provisioning certificates, see Appendix 8: Configuring the Certificate Interface.

Appendix 4: HTTP Redirection

- About HTTP Redirection
- HTTP Redirection Procedure
- Security Considerations
- Sample fstool netconfig Session

About HTTP Redirection

The browser notification, login and remediation actions require that the Appliance see traffic going to the web. In order for these actions to work properly, you may need to set the IP address used by the HTTP redirection features. This appendix details this procedure.

The HTTP feature works by redirecting an HTTP request made by a user to the Appliance for further processing. 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 separated there is a need to change the default behavior, otherwise 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.

HTTP Redirection Procedure

To redirect:

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. See the following sample session.
3. Test connectivity to and from CounterACT by pinging various addresses in the network. Invoke the **`fstool fw`** command to temporarily allow outgoing ICMP traffic prior to these tests.
4. Configure CounterACT 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 CounterACT 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 Appendix 3: Generating and Importing a Trusted Web Server Certificate).
   - The system will redirect 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 true
fstool service restart
```

The default setting for this property is false (i.e. redirection using DNS names is not performed).

Security Considerations

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 watched for 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 watched for periodically and reset if found in the wrong state.

Sample fstool netconfig Session

*The **fstool netconfig** command supports IPv6 address format.*

```
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
```

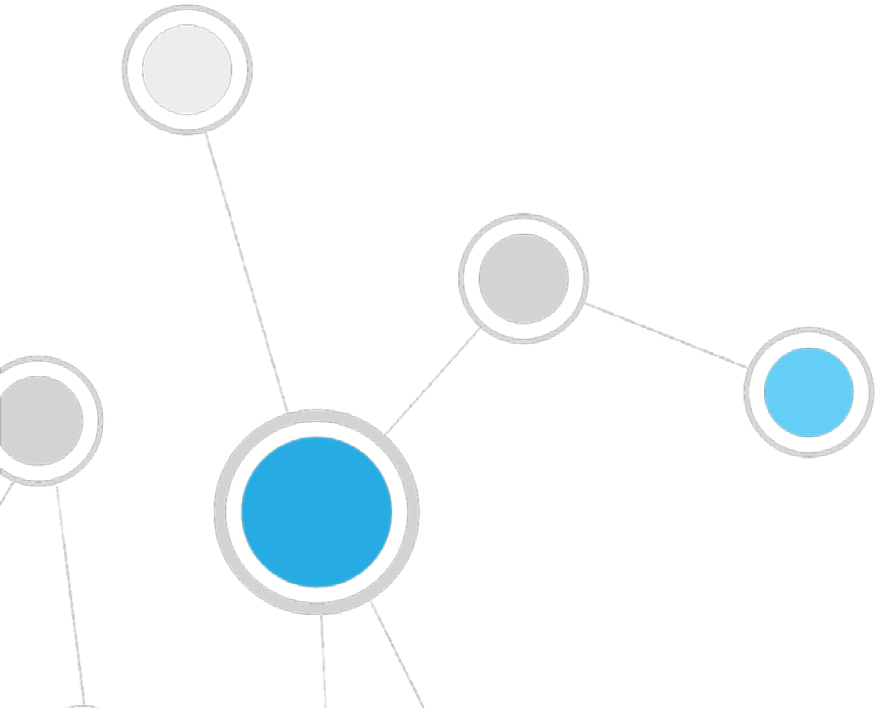
```
CounterACT Machine Network Configuration Options:

1) Configure network interfaces
2) Configure default gateway
3) Restart network service
4) Quit

Choice (1-4) : 4
```

Appendix 5: SNMP Support and Integration

- SNMP Integration
- Performance Thresholds for SNMP Notifications



SNMP Integration

CounterACT hosts an SNMP service that 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)
  - Encryption (AES or DES)
  - View of the MIB tree via industry standards

SNMP functionality is supported in IPv4, IPv6 and dual-stack CounterACT device configurations.

CounterACT uses the Net-SNMP suite to support most SNMP functionality. More information about Net-SNMP is available at http://www.net-snmp.org/.

This section describes how to configure the SNMP service on CounterACT devices, including definition of external MIB users and trap targets, and enabling/disabling of CounterACT-specific traps. Users who configure the SNMP service on CounterACT devices should be familiar with SNMP and with the View Based Access Control Model (VACM).

About SNMP Service Settings

Configuration tools for the SNMP Service are based on the configuration model of the View Based Access Control Module (VACM). This module 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.

Typically, you configure the service in the SNMP Settings pane of the CounterACT Console. This pane provides a subset of the most useful settings supported by the VACM model. For details about using the options of the SNMP Settings pane, see Configure SNMP Service Settings.

Configure SNMP Service Settings

Configuration tools for the SNMP Service are based on the configuration model of the View Based Access Control Module (VACM). This module 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.

You configure these settings in the SNMP Settings pane of the CounterACT Console.

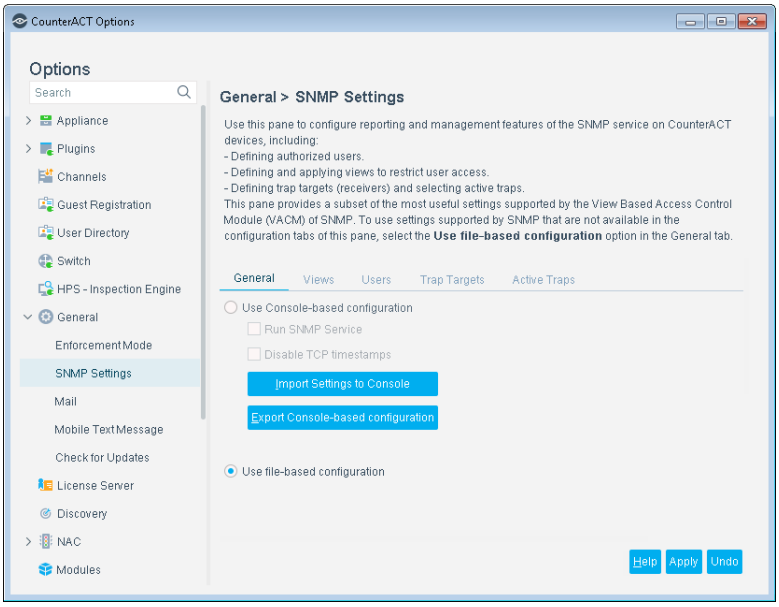
Related Tasks and Options

- Apply settings to the SNMP service. You can choose whether the service uses the Console-based settings of the SNMP Settings pane, or whether file-based configuration is used. See About SNMP Service Settings.
- Import an SNMP configuration file. The SNMP Settings pane reflects imported settings. You can use imported settings as the basis for further modifications. See Import SNMP Service Settings.
- Export current settings to a file. See Export SNMP Service Settings.

During initial configuration, it is recommended to follow the order of the tabs in the SNMP Settings pane. For example, it is recommended to define Views before you define Users.

To configure SNMP Service settings:

1. In the Console main menu, select **Tools>Options**. In the Options tree, select **General>SNMP Settings**. The SNMP Settings pane opens.



SNMP Settings Pane

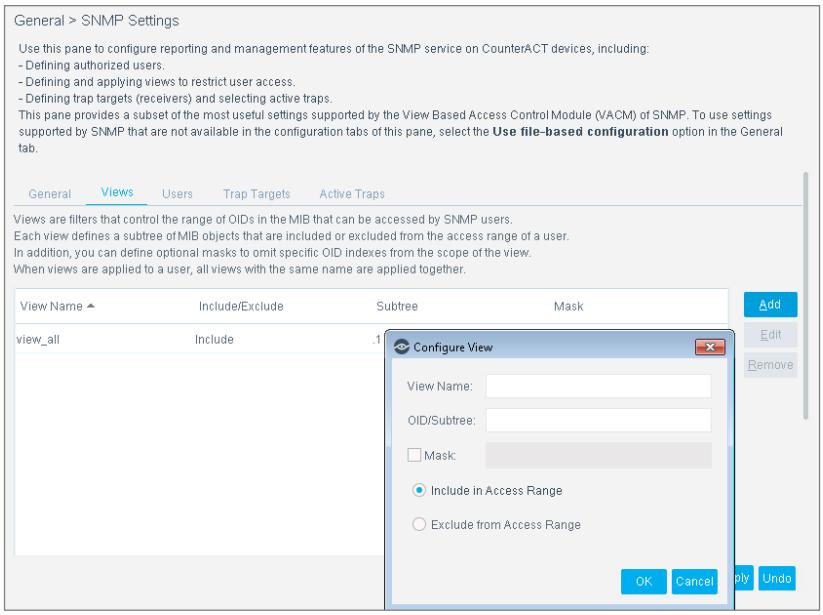
2. (Optional) To define or modify a configuration for a subset of CounterACT devices, see Configuring Features for an Appliance or Group of Appliances.
3. From this pane you can perform the following tasks:
   - Configure SNMP Views
   - Configure SNMP Users
   - Configure Trap Targets
   - Test Trap Targets
   - Enable and Disable CounterACT Traps
   - Import SNMP Service Settings
   - Export SNMP Service Settings
   - Start and Stop the SNMP Service from the Console
   - Disabling TCP Timestamps

Configure SNMP Views

Use this procedure to define inbound Views that restrict user access to the CounterACT MIB.

To configure Views:

1. In the SNMP Settings pane of the Options tree, select the Views tab. The table lists existing views.



SNMP Settings – Views Tab

2. Do one of the following:
   - Select **Add** to create a new view.
   - Select an existing view in the table, and select **Edit** to modify it.

   The Configure View dialog box appears.
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 subtree in the CounterACT device MIB, for example: .3.4.5.2.78 Apply the view to an SNMP user to define user access to this subtree.
Mask	(Optional) Select this option to mask specific OIDs in the subtree. 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 subtree is *permitted* to users when this view is applied to them. ▪ Exclude from access range – the subtree is *prohibited* to users when this view is applied to them.

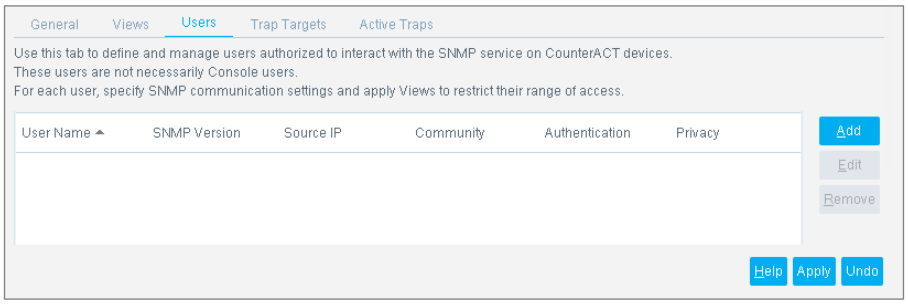
4. To remove a view, select it in the table and select **Remove**.

Configure SNMP Users

Use this procedure to define inbound users that can access the CounterACT MIB. These users are not necessarily Console users.

To configure SNMP users:

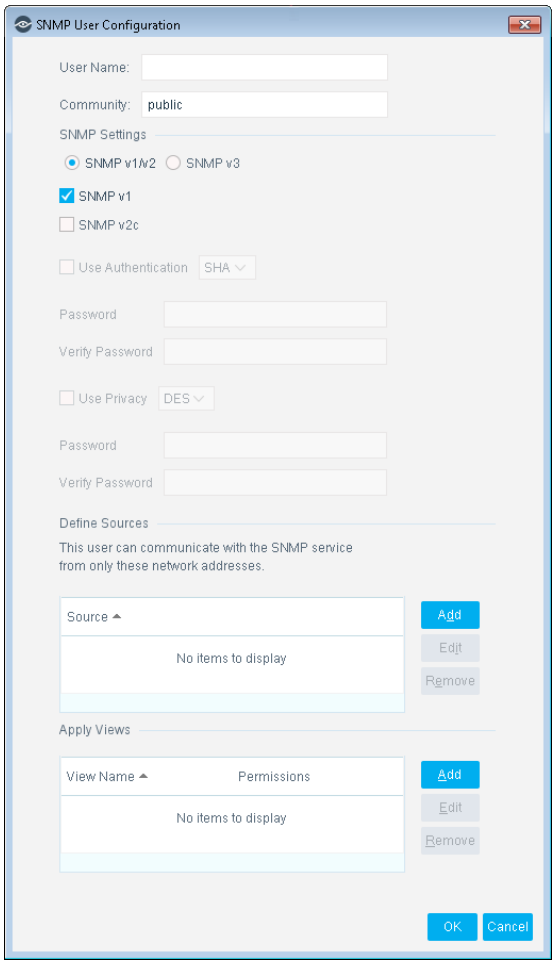
1. In the SNMP Settings pane of the Options tree, select the Users tab. The table lists users that can interact with the SNMP service on CounterACT devices.



SNMP Settings – Users Tab

2. Do one of the following:
   - Select **Add** to create a new user.
   - Select an existing user in the table, and select **Edit** to modify it.

   The User Configuration dialog box appears.



SNMP User Configuration

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 CounterACT.
5. In the SNMP Settings area, select the version of the SNMP protocol that is used to communicate with this user.

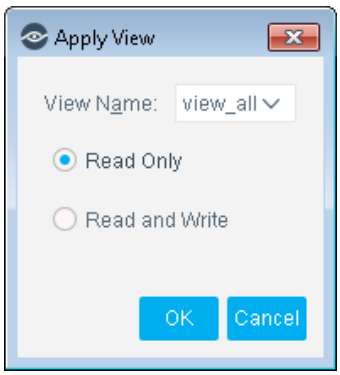
   (Optional) When SNMP V3 is selected, **Authentication** and **Privacy** encryption options are available. Specify encryption protocols and passwords.
6. In the Define Sources area, define the network addresses from which this user can access the SNMP service. Do one of the following:
   - Select **Add** 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 select **Edit** to modify it.

   The Apply View dialog box appears.



SNMP Apply View

Define how a view is applied using the following fields and options.

View Name	The drop-down 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 – user can only read the MIB objects in this view. ▪ Read/Write –user can read and write to the MIB objects in this view.

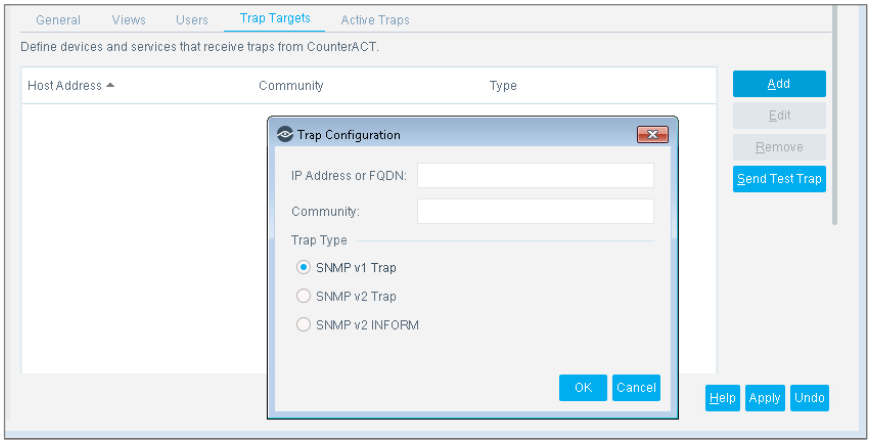
To remove a view from a user, select it in the table and select **Remove**. The view still appears in the Views tab, but no longer applies to this user.

Configure Trap Targets

Use this procedure to define targets that receive outbound traps from the CounterACT SNMP service.

To configure trap targets:

1. In the SNMP Settings pane of the Options tree, select the Trap Targets tab.



SNMP Settings – Trap Targets Tab

2. Do one of the following:
   - Select **Add** to create a new target.
   - Select an existing target in the table, and select **Edit** to modify it.

   The Trap Configuration dialog box appears.

   Define a target using the following fields and options. Select **OK** to save changes. To test trap reporting to this target, see Test Trap Targets.

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. SNMP v3 TRAP messages are not available when you use Console-based configuration. Use file-based configuration to send SNMP v3 TRAP messages.

3. To remove a target, select it in the table and select **Remove**.
4. To test communication with trap targets, see Test Trap Targets.

Test Trap Targets

Use this procedure to verify that configured targets receive traps from CounterACT.

To test trap targets:

1. In the SNMP Settings pane of the Options tree, select the Trap Targets tab.
2. Select **Send Test Trap**. Select **OK** to confirm.

A test trap is sent to all the targets configured in the Trap Targets table.

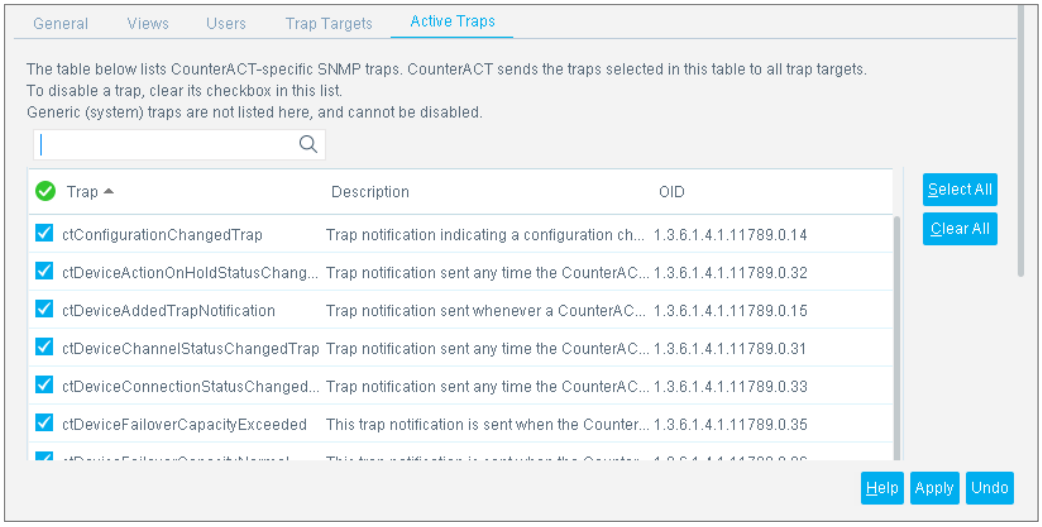
Enable and Disable CounterACT Traps

Use this procedure to configure which CounterACT-specific outbound traps are sent by CounterACT devices to external trap targets.

Standard SNMP traps are always sent, and cannot be disabled.

To configure active traps:

1. In the SNMP Settings pane of the Options tree, select the Active Traps tab.



SNMP Settings – Active Traps Tab

The table lists all the CounterACT-specific traps supported by the SNMP service on CounterACT devices. By default, all traps are enabled.

2. (Optional) Use the search field to show traps that match a substring of any trap identifier fields, or a MIB subtree.
3. Do one of the following:
   - Clear the checkbox beside a trap to disable the trap. The trap is not sent by CounterACT devices.
   - Select the checkbox beside a trap to enable the trap. The trap is sent when CounterACT 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.

Import SNMP Service Settings

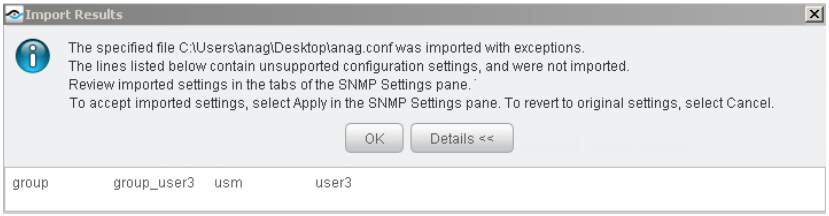
Use this procedure to import SNMP service settings from an SNMP **.conf** file. Imported settings overwrite the current settings of the SNMP Settings pane of the Console. After import, the Console-based configuration of the SNMP Settings pane reflects the settings of the imported file. You can use this imported configuration as the basis for further customization.

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 results popup 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**. Review imported settings in the tabs of the SNMP Settings pane. 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.

Start and Stop the SNMP Service from the Console

When the Console-based configuration of the SNMP Settings pane is applied to the service, use the **Run SNMP service** option to start and stop the SNMP service on configured devices.

To stop or start the SNMP service from the Console:

1. In the General tab of the SNMP Settings pane, do one of the following:
   - Select the Run SNMP Service checkbox to start the SNMP service on configured devices.
   - Clear the Run SNMP Service checkbox to stop the SNMP service on configured devices.

When the service is enabled, the firewall on the CounterACT device automatically opens.

Disabling TCP Timestamps

You can choose to disable TCP timestamps to prevent potential attackers from discovering information on system uptime. Disabling these timestamps also prevents system administrators from accessing this information. This option is available when you are using Console-based SNMP configuration. TCP timestamps are enabled by default.

To disable TCP timestamps:

1. In the Console, select **Options > General > SNMP Settings**.
2. In the General tab, verify that the *Use Console-based configuration* option is selected.
3. Select **Disable TCP timestamps**.

Performance Thresholds for SNMP Notifications

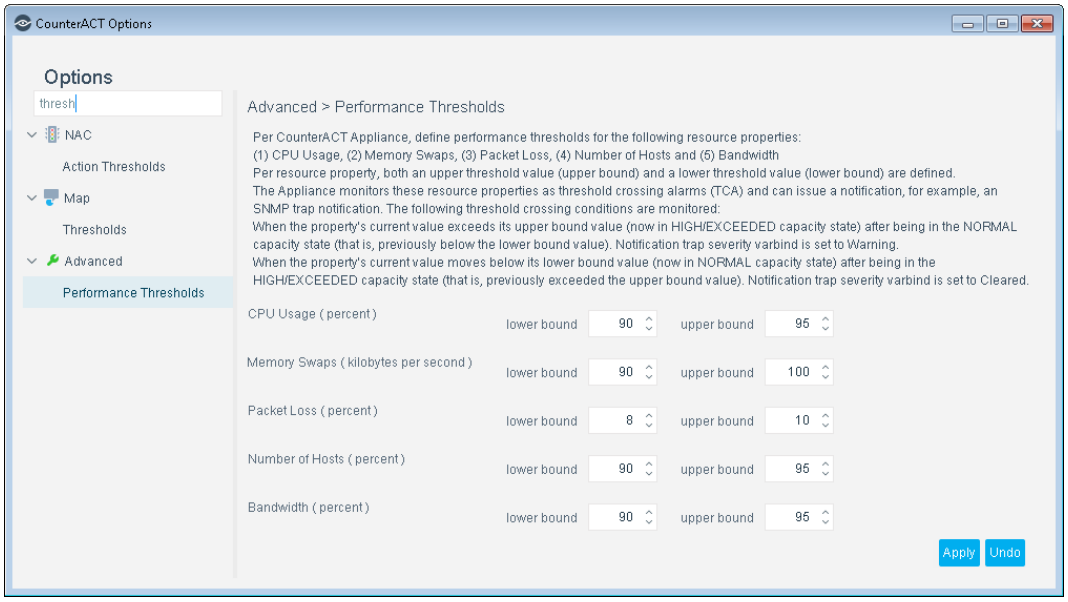
To work with the SNMP MIB for CounterACT Appliances, you must define performance thresholds for the following Appliance resources, which are monitored and reported by MIB attributes:

- CPU Usage (percent)
- Memory Swaps (kilobytes per second)
- Packet Loss (percent)
- Number of Hosts (percent)
- Bandwidth (percent)

For each resource, both an upper threshold value (upper bound) and a lower threshold value (lower bound) are defined. These boundaries are used to generate Threshold Crossing Alarm (TCA) trap notifications, as follows:

- When a MIB attribute has a value below the Lower Bound, the monitored resource is considered to have Normal functional status.
- When the value of a MIB attribute increases from Normal (below the Lower Bound) until it exceeds the Upper Bound value, the monitored resource is considered to be in High/Exceeded status, and an alarm trap notification is sent with severity set to Warning (6).
- When the value of a MIB attribute decreases from High/Exceeded (above the Upper Bound) to below its Lower Bound, the monitored resource is considered to have returned to Normal status, and a trap notification with severity set to Cleared (1) is sent to clear the previous alarm trap.

Define the thresholds for SNMP MIB attributes in the Console **Tools > Options > Advanced > Performance Thresholds** pane.



Performance Thresholds for CounterACT Appliance SNMP MIB

Appendix 6: SNMP MIB for CounterACT Appliances

- About the SNMP MIB for CounterACT Appliances
- MIB Table Objects for CounterACT Appliances
- SNMP Trap Notifications for CounterACT Appliances

About the SNMP MIB for CounterACT Appliances

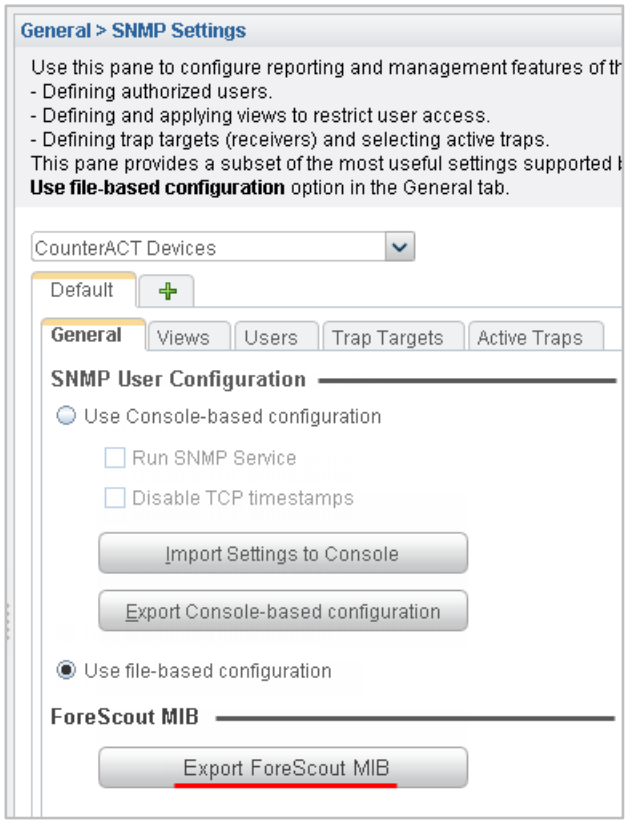
A MIB Table for CounterACT Appliances provides objects that report detailed information about status, configuration and performance information.

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 CounterACT Appliance return a table containing a single row providing the MIB attributes of the queried Appliance.

To obtain the CounterACT SNMP MIB file:

1. In the CounterACT Console, select **Options**.
2. In the Options tree, select **General>SNMP** Settings.
3. In the ForeScout MIB area of the General tab, select **Export ForeScout MIB**.



Load this file in your external management system.

The ArcSight Module also provides SNMP MIB and Trap Notification information about the interaction between CounterACT devices and their peer ArcSight servers. Refer to the ArcSight Module documentation. See Additional CounterACT Documentation for information on how to access documentation.

In order for an external network management system to query a CounterACT Appliance SNMP MIB and receive SNMP trap notifications, you must enable SNMP on the CounterACT Appliance. By default, the CounterACT SNMP agent is disabled. See Appendix 5: SNMP Support and Integration for details.

MIB Table Objects for CounterACT Appliances

The CounterACT 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 CounterACT 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 CounterACT 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 CounterACT 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 (see CounterACT documentation for more details). This value accounts for internal traffic between CounterACT 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 support or 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 CounterACT device is up, responsive and is in sync with the active CounterACT device.

statusDegraded (2) Indicates that the standby CounterACT device is unreachable, down, or currently out of sync with the active CounterACT device.

inMaintenanceMode(3) Indicates that the active or the standby CounterACT device is currently 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 CounterACT 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 (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 administrator 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 (Options>NAC>Action Thresholds).

blockStatusUnknown (3) Indicates that the queue status cannot be verified (for example, if the CounterACT 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 CounterACT 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 CounterACT 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 CounterACT Appliances

The SNMP trap notifications described in this section are issued when the value of a configuration, status, or performance attribute of the CounterACT 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.

The ArcSight Module also provides SNMP MIB and Trap Notification information about the interaction between CounterACT devices and their peer ArcSight servers. Refer to the ArcSight Plugin documentation.

In order for an external network management system to query a CounterACT Appliance SNMP MIB and receive SNMP trap notifications, you must enable SNMP on the CounterACT Appliance. By default, the CounterACT SNMP agent is disabled. See SNMP Integration for details.

CounterACT 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 CounterACT 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 a CounterACT Appliance was added to CounterACT Enterprise Manager (EM).

ctDeviceRemovedTrapNotification

OID:.1.3.6.1.4.1.11789.0.16

Indicates that a CounterACT Appliance was removed from CounterACT 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 only sent after a **`ctDeviceTrapHighCPUUtilization`** alarm trap was 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 only sent after a **ctDeviceTrapHighPacketLoss** alarm trap was 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 only sent after a **ctDeviceTrapHighMemorySwapping** alarm trap was 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 only sent after a **`ctDeviceHighBandwidthUtilizationTrap`** alarm trap was 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)
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)
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 CounterACT 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 CounterACT trap notifications:

ctDeviceId

OID:.1.3.6.1.4.1.11789.4.3.1.1

An internally-defined unique identifier for the CounterACT 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. The following are the possible severity levels:

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 that 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.

Appendix 7: Customizing User Interfaces

- The CounterACT User Portal Builder
- The Legacy Customization Tool
- Customize Text and Labels

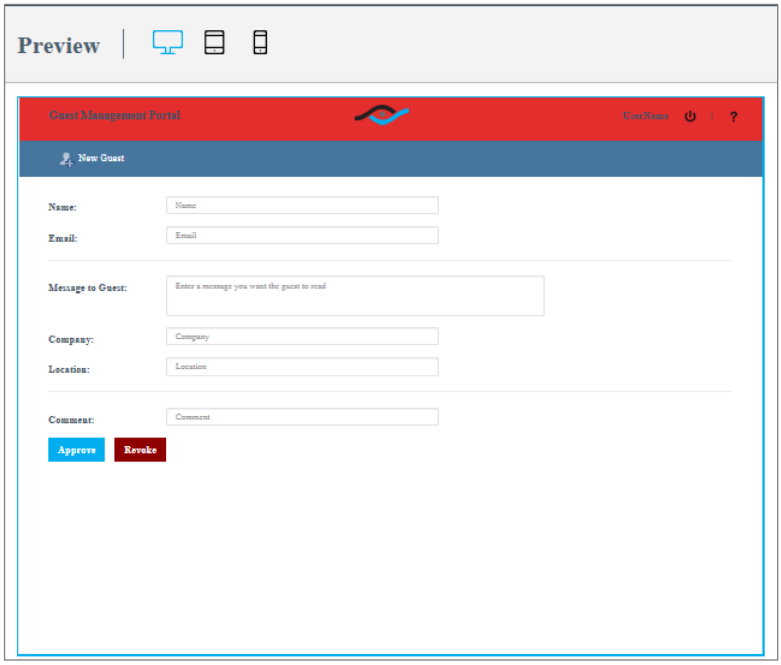
The CounterACT User Portal Builder

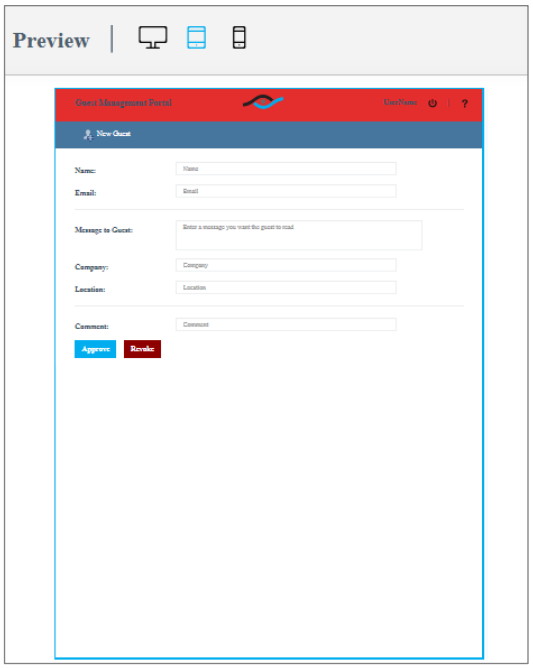
Use the CounterACT User Portal Builder to customize the following CounterACT user interfaces:

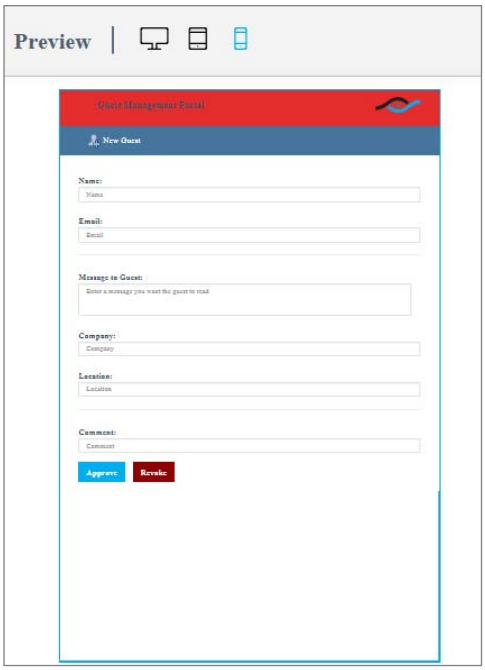
- HTTP Notification
- HTTP Login
- Guest Management Portal

The legacy Customization Tool is still used for customizing the interfaces for HTTP Localhost Login, Start SecureConnector, Start Macintosh Updates, Start Windows Updates, Windows Self Remediation and Compliance Center. See The Legacy Customization Tool.

When using the User Portal Builder, each skin is responsive to laptop/PC mode, tablet mode, and also mobile device mode. There is no unique customization for mobile devices.



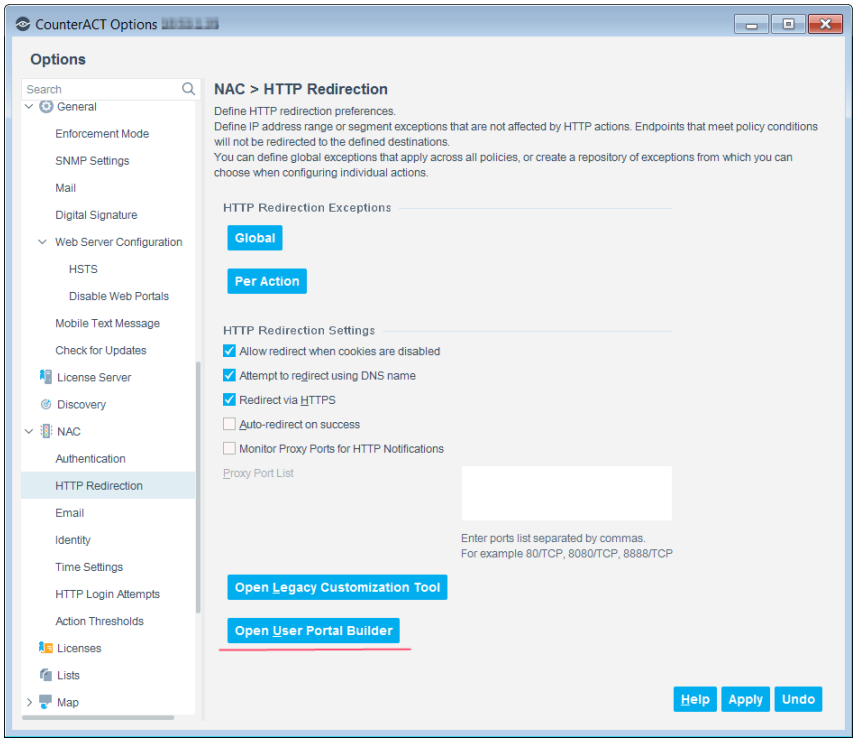




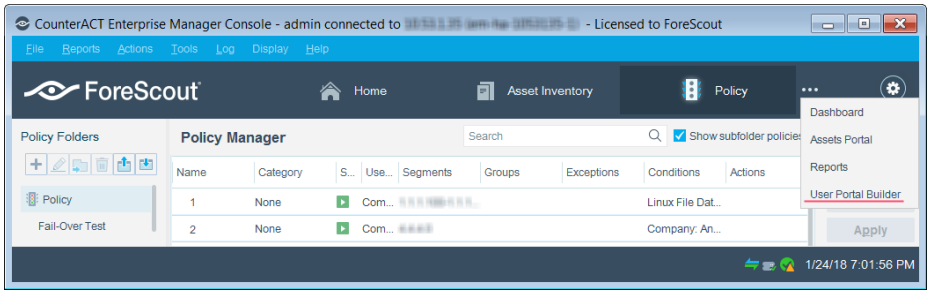
Opening the User Portal Builder

To open the User Portal Builder, do one of the following:

- Select **Options** from the **Tools** menu, navigate to **NAC > HTTP Redirection**, and select **Open** User Portal Builder.



- In the Console, select the Ellipsis icon ••• from the **Toolbar** menu, and select **User Portal Builder**.



Using the User Portal Builder to Customize Skins

The User Portal Builder includes an out-of-the-box default skin for each of the CounterACT user interfaces.

Each CounterACT user interface has its own type of skin. You can customize a skin in different ways:

- Basic Customization
- Advanced Customization

Basic Customization

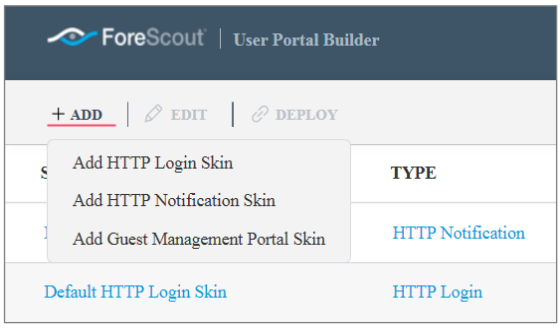
The User Portal Builder provides a simple way to edit and preview:

- the color settings of the most commonly customized fonts
- the color settings of the most commonly customized background areas and buttons
- the logo

New skins can be added, and skins that were added can be edited.

To add a new skin:

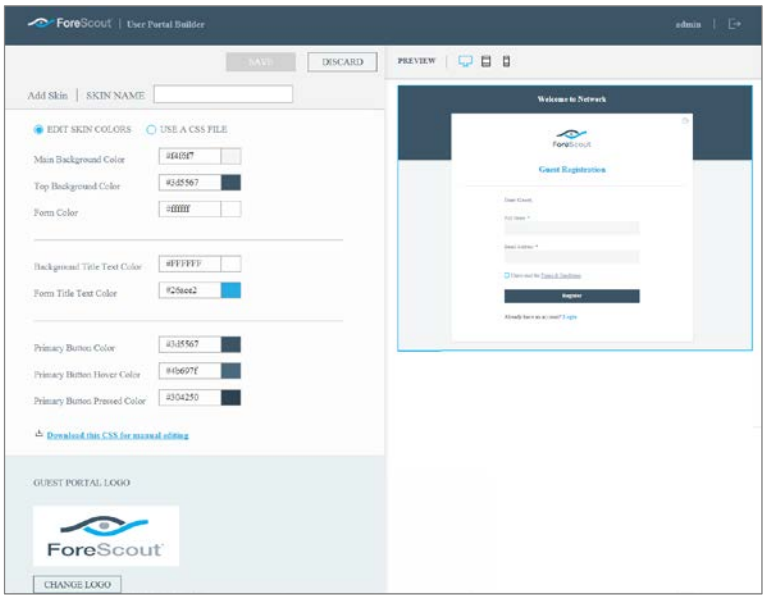
1. In the User Portal Builder, select **Add**.



2. Select the user interface:
   - **Add HTTP Login Skin** to customize the HTTP Login window.
   - **Add HTTP Notification Skin** to customize the HTTP Notification window.

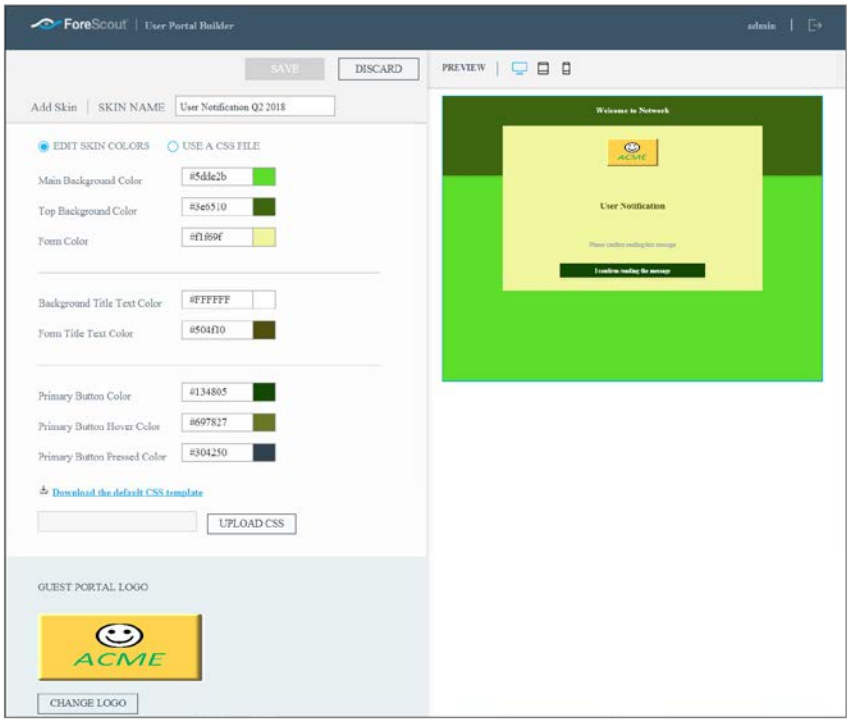
– **Add Guest Management Skin** to customize the Guest Management Portal.

3. A copy of the default skin opens for you to edit.



4. Edit the skin colors and logo as needed, and assign a name to the new skin.

🗎 *Uploaded logo files must be in PNG format and cannot be larger than 1 MB.*



5. Name the skin, and select **Save** to save it to the User Portal Builder.

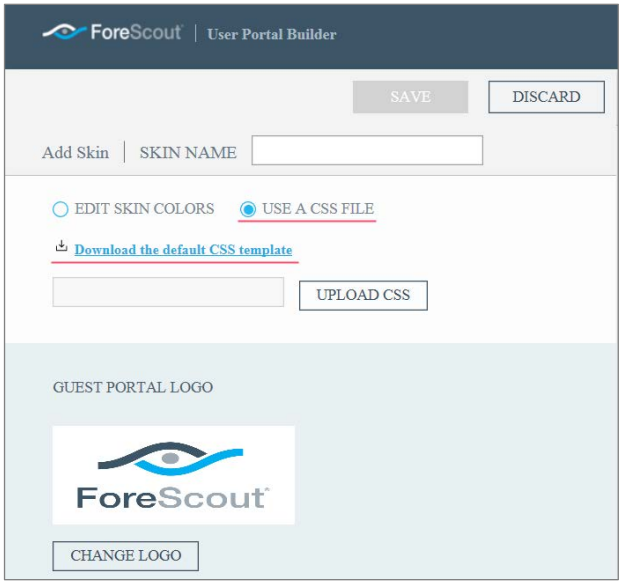
Advanced Customization

You may want to configure user interface features that are not included in the User Portal Builder basic customization. For example:

- Fonts and font sizes
- Field shapes and positions
- Background images

To edit customized features:

1. In the Add Skin page, select **Use a CSS file**.

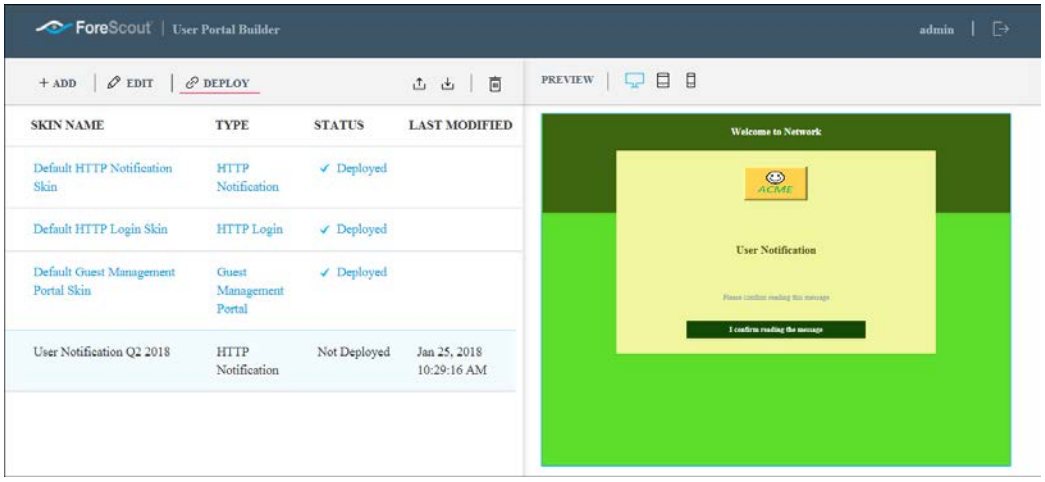


2. Select **Download the default CSS template** to download the CSS file of a pre-defined skin template. (Optional)
3. Edit the downloaded skin or a skin that has been previously added.
4. When you are done editing the CSS file, select the **Upload CSS** button to upload it to the User Portal Builder.

*The User Portal Builder cannot be used to localize user interface text. To localize the text, select **Options** from the Console **Tools** menu, and navigate to **Advanced > Language Localization > Endpoint Messages**. For more information, see Localizing CounterACT Redirected Web Pages and Messages.*

Deploying a Skin for a User Interface

Exactly one skin is deployed throughout your network for each type of user interface. In the User Portal Builder, select the skin to be deployed in place of the one currently deployed, and then select **Deploy**.



The Legacy Customization Tool

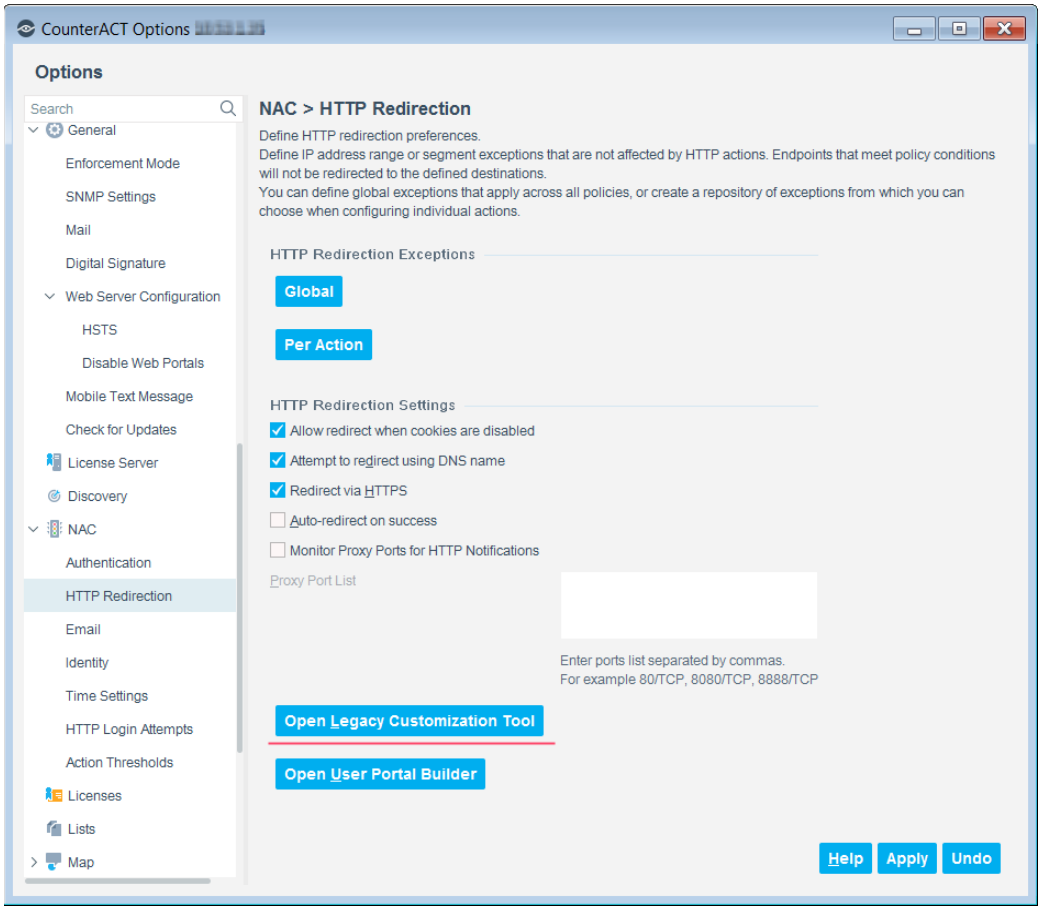
Use the legacy Customization Tool to customize the following CounterACT user interfaces for laptops and PCs:

- HTTP Localhost Login
- Start SecureConnector
- Start Macintosh Updates
- Start Windows Updates
- Windows Self Remediation
- Compliance Center

Opening the Legacy Customization Tool

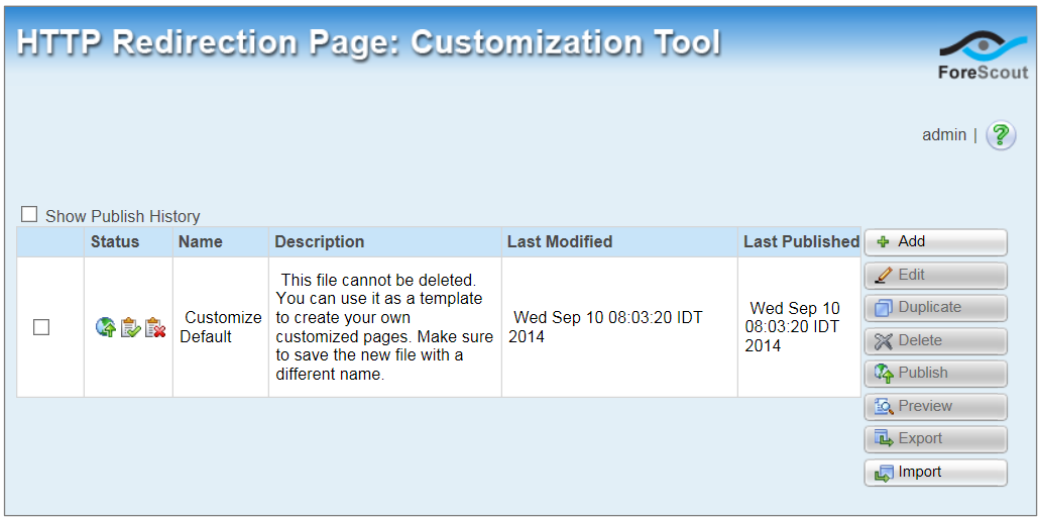
To open the Customization Tool:

1. Select **Options** from the **Tools** menu, navigate to **NAC > HTTP Redirection**, and select **Open Legacy Customization Tool**.



HTTP Redirection Pane

2. The HTTP Redirection Page: Customization Tool page opens in your web browser. The page contains a table listing all saved customized pages. When first using the tool, a default template is displayed. This default template is automatically selected to be used to create a new customized template.



HTTP Redirection Page

To use a customized page, it must be published. In the HTTP Redirection Page: Customization Tool page, the template published status is displayed in the Status column. The icons and descriptions are as follows:

– Template used when FCC compliance is enabled

– Template used when FCC compliance is disabled

– Template used for all general pages

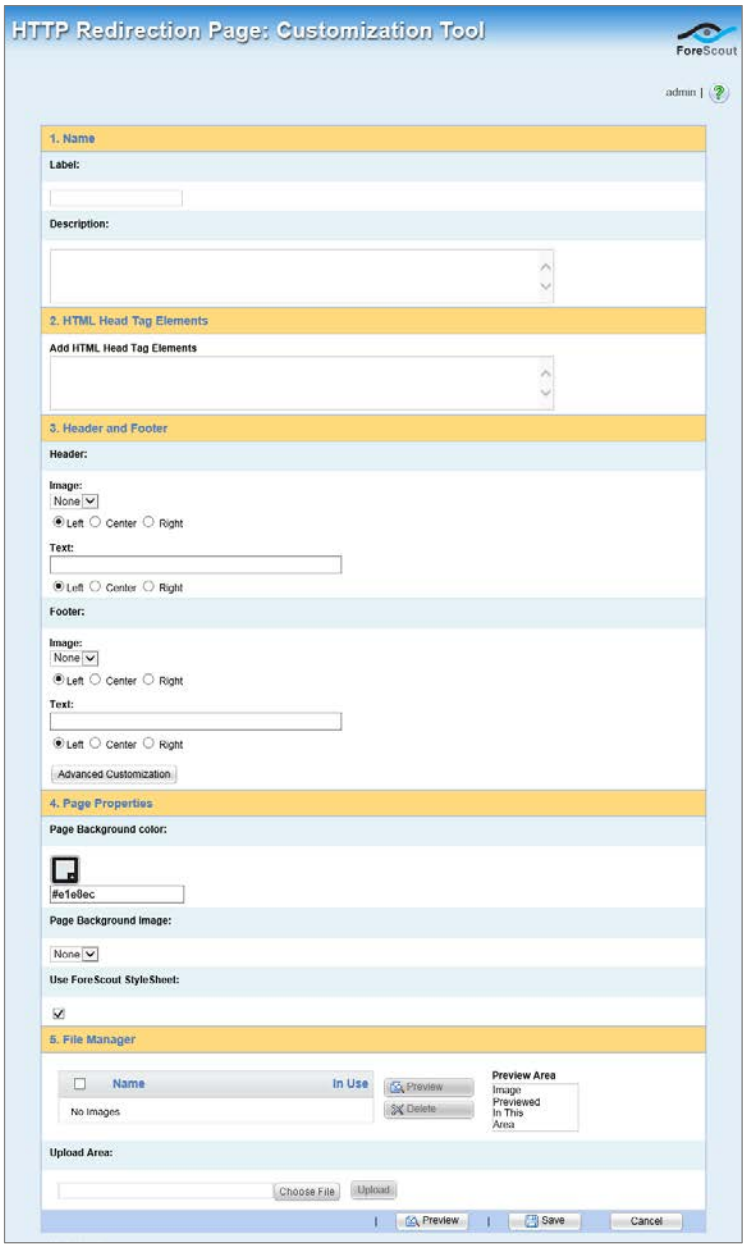
– Indicates that the template is not being used

– Indicates that the template has been published in the past

The HTTP Redirection Page: Customization Tool page contains the buttons described in the following table.

Button	Description
Add	Used to create new templates.
Edit	Used to open saved customized pages for modification.
Duplicate	Used to create a duplicate customized page from an existing saved customized page.
Delete	Used to delete a saved customized page.
Publish	Used to integrate saved customized pages.
Preview	Used to preview a saved customized page.
Export	Used to export saved customized pages to external systems such as backup servers in Web Developer mode.
Import	Used to import saved customized pages from external systems such as backup servers in Web Developer mode.

3. Select **Add** to create a new template or select an existing template and select **Edit**. The Customization Tool opens.



HTTP Customization Tool

For customization, CounterACT provides you with the basic option for entering the customization elements, as well as an advanced HTML editing option.

To work with the advanced features, prior HTML knowledge is required.

4. In the **Name** section type the template name in the **Label** field and a template description in the **Description** field.
5. Complete the rest of the fields in accordance with your preferences; see Basic Customization Using the Tool and Advanced Customization Using the Tool.

6. Select **Save**. If the template name already exists an overwrite confirmation dialog box opens. In the confirmation dialog box select **OK**. The template is saved and the page preview opens.
7. Select **Return to Customize menu**. The HTTP Redirection Page: Customization Tool page opens.

Using the Customization Tool to Customize Skins

Each CounterACT user interface has its own type of skin. You can customize a skin in different ways:

- Basic Customization Using the Tool
- Advanced Customization Using the Tool

Basic Customization Using the Tool

There are three configuration areas available for customization:

- **Page Body**: Used to configure the page Header and Footer.
- **Page Properties**: Used to configure the page background.
- **File Manager**: Used to manage images, CSS files and JS files used in the Header, the Footer and the background.

HTML Head Tag Elements

The **HTML Head Tag Elements** area is used to add HTML Head Tag elements. See Advanced Customization Using the Tool.

Header and Footer

In the Header and Footer area there are two sub-areas, one for the Header and one for the Footer.

The Header and Footer customization options are the same.

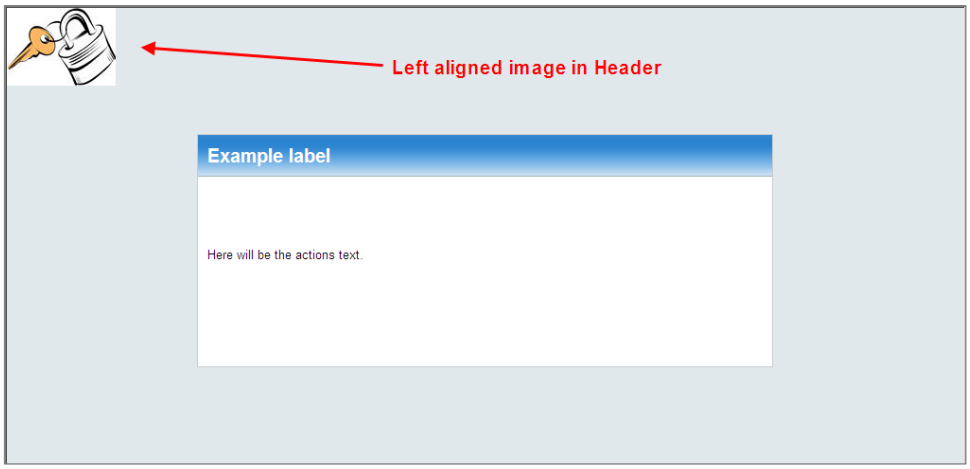
Images

The **Image** drop-down list provides a list of all uploaded images, see File Manager. To include an image in the Header or Footer, select the image from the drop-down list.

Where the selected image is placed in the Header or Footer, the image alignment is customized by selecting one of the following options under the **Image** field:

- Left
- Center
- Right

The following figure illustrates a left aligned image.



Customized Left Aligned Image

Text

In the **Text** field type the text to be displayed in the Header.

Where the entered text is placed in the Header or Footer, the text alignment is customized by selecting one of the following options under the **Text** field:

- Left
- Center
- Right

The following figure illustrates center aligned text.

Customized Center Aligned Text

For advanced customization select **Advanced Header Customization** or **Advanced Footer Customization**, see Advanced Customization Using the Tool.

Page Properties

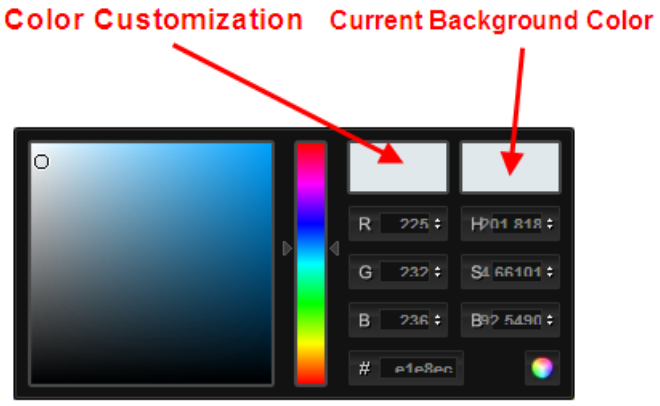
In the Page properties area there are the following sub-customization areas:

- Page Background Color: Used to customize the page background color.
- Page Background Image: Used to add an image in the page background.
- Use ForeScout StyleSheet: Used to remove the pre-configured ForeScout page configuration.

Page Background Color

The current background color is displayed in the icon.

To customize the background color, select the icon. The Background Color Customization panel opens.



Background Color Customization Panel

The current background color is displayed at the top right. To its left, the proposed color being selected is displayed.

In the center color strip all the available colors are displayed. Where the arrow is located, the expanded color option is displayed in the left area. The color can be selected from the left area or a color code can be entered on the panel's right side.

Select your preferred color and then apply the color by selecting the icon. The color is displayed in the modified icon.

Page Background Image

The **Page Background Image** drop-down list provides a list of all uploaded images. See File Manager for details about how to add an image to this list. To include an image in the background, select the image from the drop-down list.

Use ForeScout StyleSheet

The default ForeScout style sheet is the standard HTTP message page. This is set up to enable three customization areas, Header, Footer and background.

To enable more HTML customization options clear **Use ForeScout StyleSheet**. After clearing the checkbox, the current page configurations are removed, effectively providing a page without styling.

File Manager

The File Manager area is used for managing images used in the HTTP page customization. The images can be used in the Header, Footer and the background. Only images, CSS files and JS files uploaded to the File Manager can be utilized in the page customization.

To upload an image:

1. Select Choose File. The standard Windows Explorer window opens.
2. Navigate to the folder containing the image to upload.
3. Select the image and select **Open**. The path is displayed in the field next to the browse button.
4. Select **Upload**. The uploaded image is displayed in the File Manager uploaded file list. The uploaded image is also added to the **Image** drop-down list in the **Header and Footer** and **Page Properties** sections.

To preview an uploaded image:

1. Select the checkbox next to the image to view.
2. Select Preview. The image is displayed in the **Preview Area**.

If an image is used in the Header, Footer or background, a ✔ is displayed in the File Manager uploaded file list.

To remove an image from the list:

1. Select the checkbox next to the image to remove.
2. Select Delete. The image is removed from the list.

If the image is being used in the Header, Footer or background, an error message dialog box opens.

Advanced Customization Using the Tool

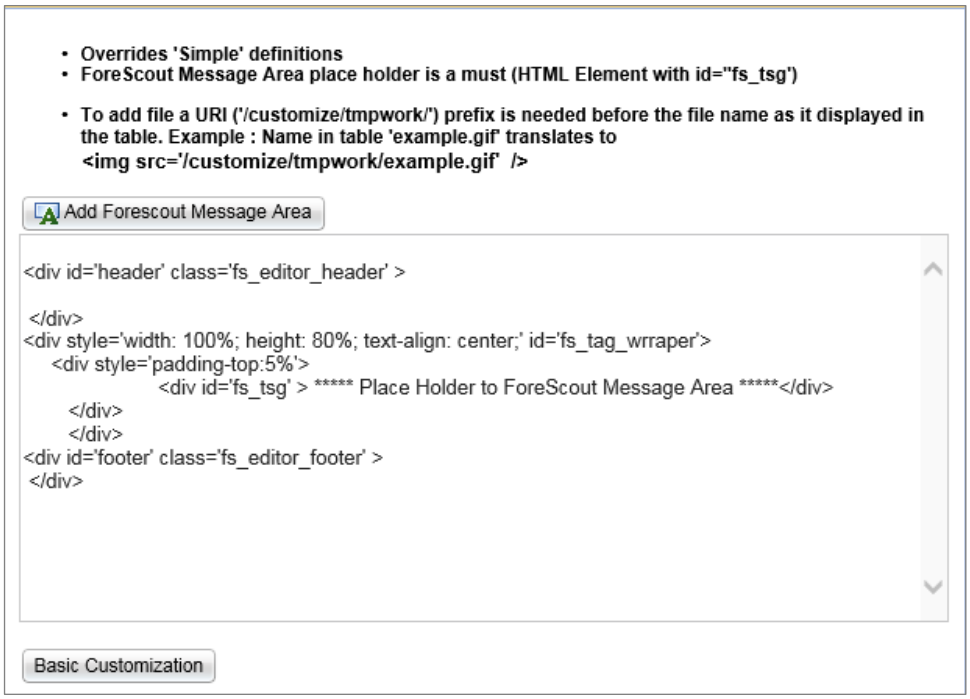
Advanced customization requires good HTML knowledge. CounterACT provides the following advanced customization options:

- Additional Head Tags Elements
- Advanced Header and Footer customization

In the **HTML Head Tag Elements** section, additional HTML Head Tag elements can be added to enhance the HTML customization options. These can include elements such as scripts, instructions to the browser where to find style sheets, provide meta-information, etc.

The following tags can be added to this section: <title>, <base>, <link>, <meta>, <script> and <style>.

For advanced Header or Footer customization, in the **Header and Footer** section select **Advanced Customization**. The simple customization **Image** and **Text** field area is replaced by the advanced customization text box displaying the basic customization HTML equivalent.



Advanced Customization

It is important that the Place holder for the ForeScout Message area is not deleted from the code.

The advanced HTML customization automatically overrides the basic customization.

Saving and Integrating a Customized Page

To use a customized page, it must be published. In the HTTP Redirection Page: Customization Tool page the template published status is displayed in the Status column. The icons are as follows:

: Used when the endpoint is FCC compliant

: Used when FCC detects that the endpoint is not compliant

: Used for all general pages

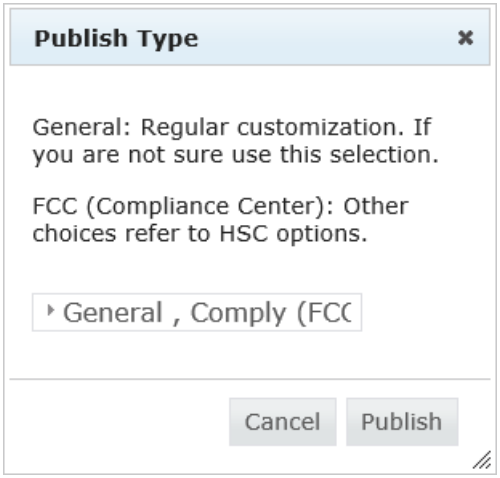
To create a duplicate customized page from an existing page:

1. Create the customized page as required see Basic Customization Using the Tool and Advanced Customization Using the Tool.
2. Select **Duplicate**. The Save As dialog box opens.
3. Type a new page name and description, and select **Save**. The customized page is saved and is displayed in the **Customize HTTP Page** the next time it is opened.

To publish a page:

1. Save the customized page.

2. Select **Publish**. The Publish Type Page opens.



Publish Customized Page

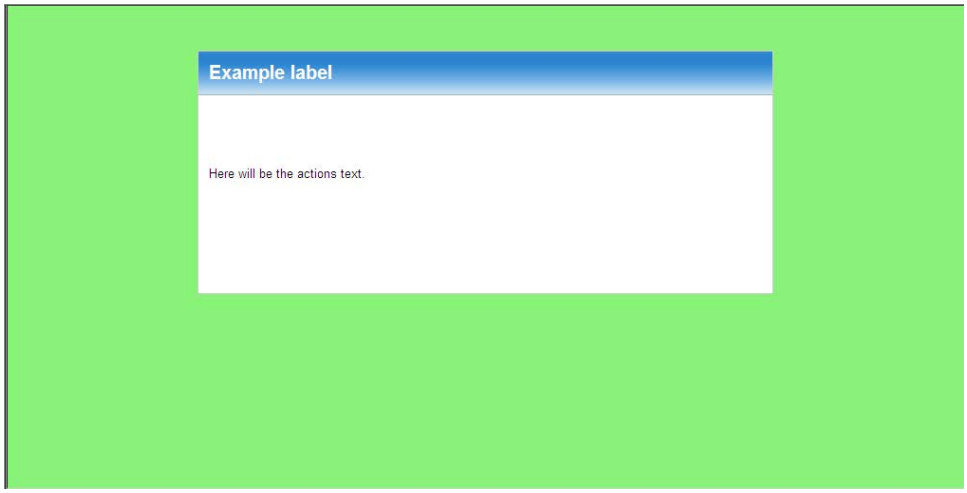
3. From the drop-down list there are three publishing options:
   - General: This option is for all pages.
   - Comply (FCC mode): This option is for all FCC compliant pages.
   - Not Comply (FCC mode): This option is for all noncompliant FCC pages.
4. Select **Publish**. The customized page is integrated.

Customized ForeScout Compliance Center (FCC) Pages

The ForeScout Compliance Center (FCC) lets you display your compliance status at endpoints for the purpose of:

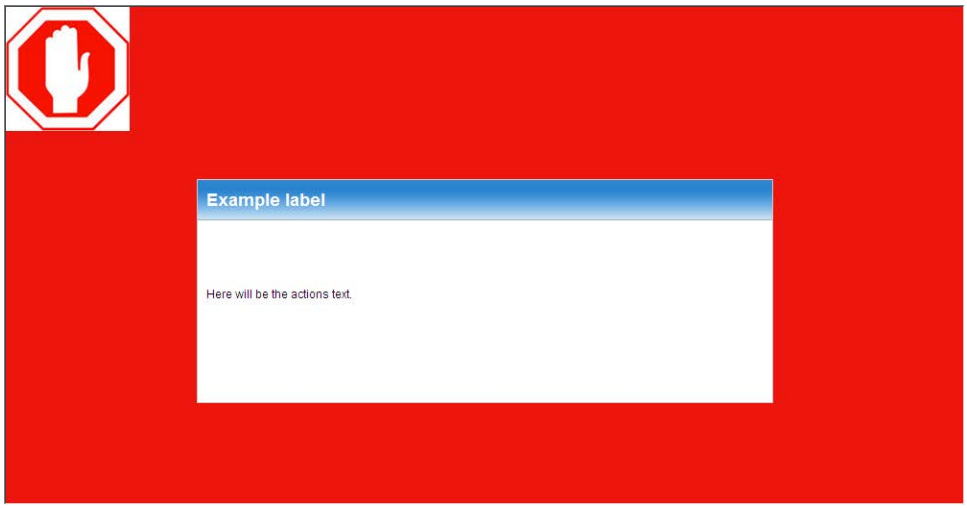
- Letting endpoint users log in
- Bringing endpoints users to network compliance

When the FCC mode is activated, the two FCC customized pages are engaged. If the endpoint is compliant the Comply (FCC Mode) customized page is used. The following FCC compliant page example has a green background. See Working with the ForeScout Compliance Center for details.



FCC Compliant Customization Example

If the endpoint is not compliant the Not Comply (FCC Mode) customized page is used. The following FCC noncompliant page example has a red background and a stop sign.



FCC Noncompliant Customization Example

When FCC mode is disabled in CounterACT, the General customized page is used.

*To use this feature, you must have both **Assets Portal User** and **Policy Management** permissions. See Access to Console Tools – Permissions for details about acquiring permissions.*

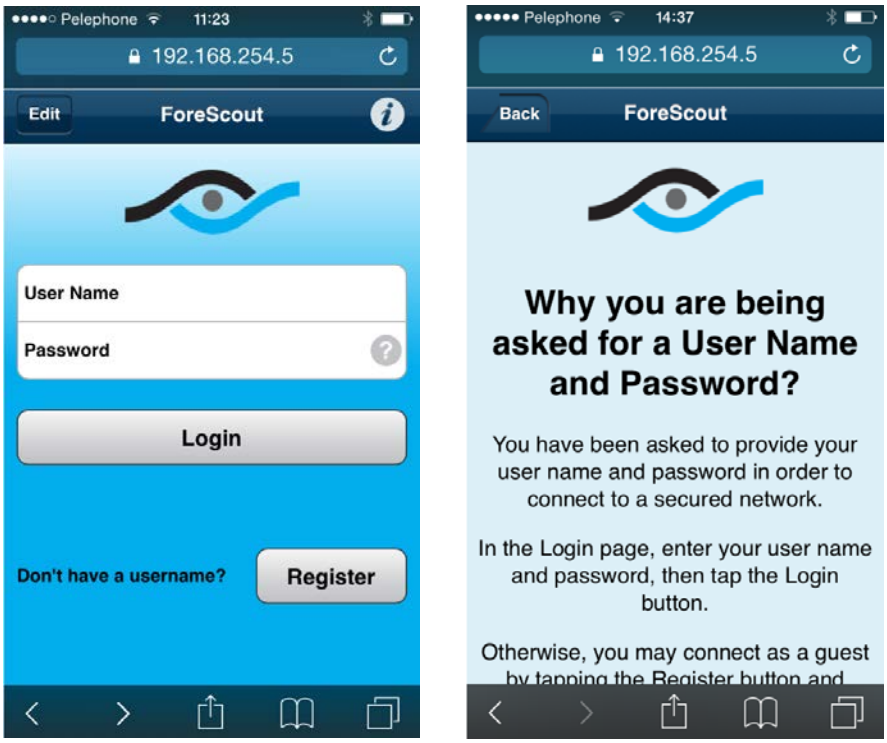
The customized page can be integrated in one of three ways:

- **General**: The customization is applied to all CounterACT redirected pages.
- **Comply (FCC Mode)**: The customization is applied only to CounterACT endpoints that are compliant with the ForeScout Compliance Center requirements.

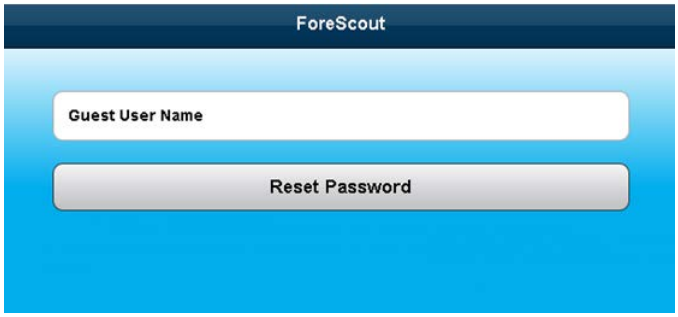
- **Not Comply (FCC Mode)**: The customization is applied to all CounterACT endpoints not compliant with the ForeScout Compliance Center configuration.

Customize Text and Labels

Several CounterACT HTTP actions include texts and labels displayed on mobile endpoints. You can edit these items or can localize them so that they appear in any language that your operating system supports.



Sample Mobile Endpoint Texts and Labels - 1



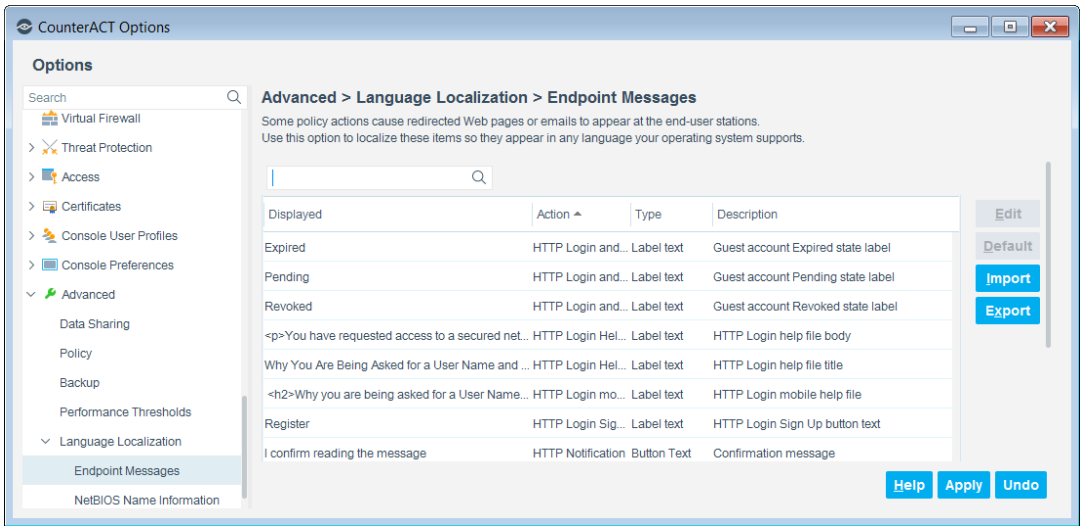
Sample Mobile Endpoint Texts and Labels – 2

Text and label edits you make are applied to laptop/PC and mobile endpoints, with the exceptions of three items that are applied to mobile endpoints only. These three items are described below.

You can apply HTML formatting code to texts; for example, bold and underlines. A new line <Enter> in action text areas is automatically translated to a <br> tag.

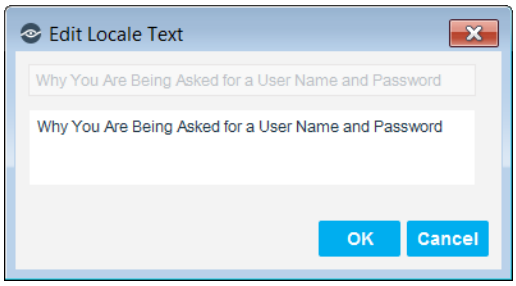
To localize/customize HTTP Mobile Redirect Texts:

1. Select **Options** from the **Tools** menu and then select **Advanced** > **Language Localization** > **Endpoint Messages**.
2. Type the word *mobile* in the search field.



Localize Mobile Endpoint Messages

3. Select an entry and select **Edit**. The Edit Locale Text dialog box opens.

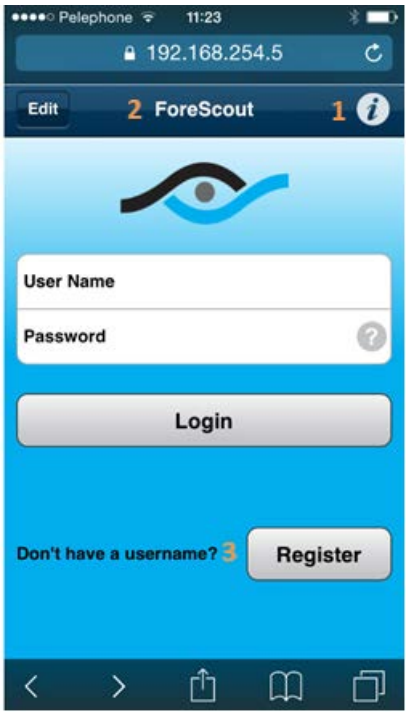


Localize Mobile Endpoint Messages – Edit Locale Text

4. Type in the new text.
5. Select **OK**. You can select **Default** to return to the default text.

See figure below	Displayed	Description
1	Why you are being asked for a User Name and Password? You have been asked to provide your user name and password in order to connect to a secured network. In the Login page, enter your user name and password, then tap the Login button. Otherwise, you may connect as a guest by tapping the Register button and completing the form.	HTTP Login: Mobile help text

2	ForeScout	Redirection page title bar
3	Don't have a username?	HTTP Login: Mobile help text



Appendix 8: Configuring the Certificate Interface

- About the Certificate Interface
- Configure Certificate-Related Settings
- Configure the Trusted Certificates Table
- Configure the System Certificates Table

About the Certificate Interface

The CounterACT certificate interface is the easy-to-use method for handling both trusted and system certificates. This interface replaces previously used *fstools* features.

Each certificate is associated with a specific scope, allowing the same or different certificates to be used for different CounterACT subsystems running on different devices. A scope is one or more specific CounterACT services or applications running on one or more CounterACT devices.

To access the Certificate Interface:

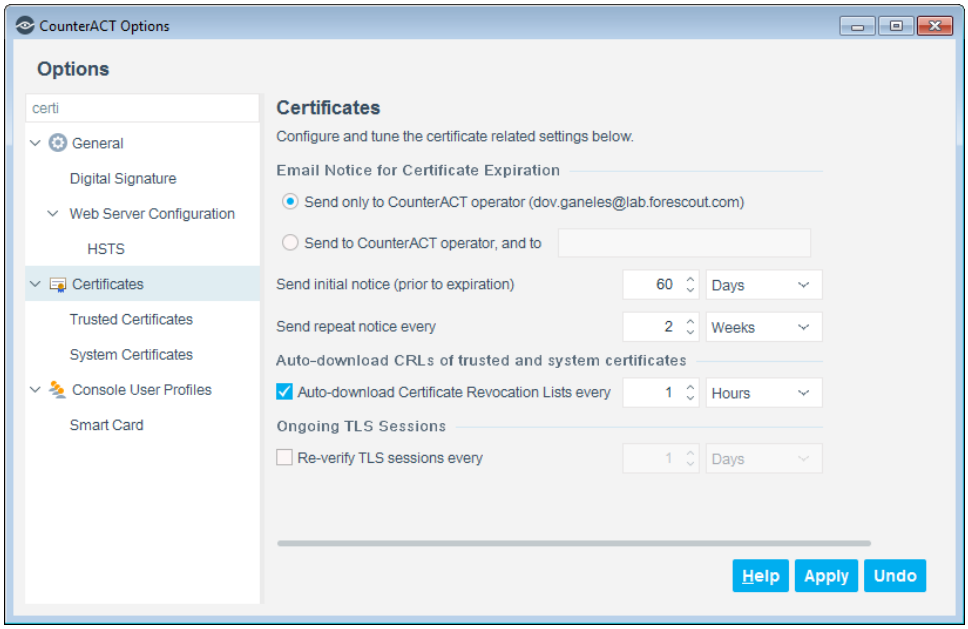
- In the CounterACT Console, select **Options > Certificates**. The Certificates pane opens. This pane provides general certificate-related configuration settings. See Configure Certificate-Related Settings.
- In the Options tree, select **Certificates > Trusted Certificates**. Use this pane to add certificate authority (CA) certificates to the Trusted Certificates table, and to configure the scopes for which they are trusted. See Configure the Trusted Certificates Table.
- In the Options tree, select **Certificates > System Certificate**s. Use this pane to create certificates and add them to the System Certificates table, and to configure the scopes for which they are used. See Configure the System Certificates Table.

Certificates used in earlier versions of CounterACT are automatically migrated, along with their scopes, to the System Certificates and Trusted Certificates tables.

Configure Certificate-Related Settings

Configure and tune the following certificate-related settings:

- Configure Certificate Expiration Monitoring
- Auto-download CRLs
- Verify Ongoing TLS Sessions



Configure Certificate Expiration Monitoring

Define email addresses for CounterACT to send notifications regarding certificate expiration. By default, notifications are only sent to the CounterACT Operator. You can also send notifications to an additional email address.

To configure certificate expiration monitoring:

1. Log in to the CounterACT Console using an account that has *CounterACT Crypto Administration* permissions.
2. Select Options, and navigate to **Certificates**. The Certificates pane opens.
3. In the **Email Notice for Certificate Expiration** section, configure to send email notices as follows:
   - **Send only to CounterACT Operator** (The Operator email address is configured in the Console in Options > General > Mail).
   - Send to CounterACT Operator and **to** one additional email address.
4. Configure the time interval to **Send initial notice (prior to expiration)**. By default, the value is 60 days.
5. Configure the time interval to **Send repeat notices every** X time interval. By default, the value is 2 weeks.
6. Select **Apply** when you have finished changing the configuration.

Auto-download CRLs

Configure whether, and how often to auto-download certificate revocation lists (CRLs) of trusted and system certificates. If a new CRL is found, there may be new revocation information available in the system. This option is enabled by default, with the time period set to check for new CRLs every hour.

To auto-download CRLs:

1. Log in to the CounterACT Console using an account that has *CounterACT Crypto Administration* permissions.
2. Select Options, and navigate to **Certificates**. The Certificates pane opens.
3. In the **Auto-download CRLs of trusted and system certificates** section, select **Auto-download Certificate Revocation Lists every, and** set a time interval to check for new CRLs.
4. Select **Apply** when you have finished changing the configuration.

Verify Ongoing TLS Sessions

Configure whether, and how often to verify certificates for ongoing TLS sessions. Sessions can sometimes be kept alive for performance reasons to serve multiple requests (e.g. User Directory Plugin connection to Active Directory server for properties). By default, this option is cleared.

To verify ongoing TLS sessions:

1. Log in to the CounterACT Console using an account that has *CounterACT Crypto Administration* permissions.
2. Select Options, and navigate to **Certificates**. The Certificates pane opens.
3. In the Ongoing TLS Sessions section, select **Re-verify TLS sessions every, and set** a time interval to verify ongoing TLS sessions. By default, the time period is 1 day.
4. Select **Apply** when you have finished changing the configuration.

Configure the Trusted Certificates Table

To ensure secure communication, CounterACT verifies certificates presented by external services and applications. Peer certificates can be verified only if the issuer chain they present ends with a certificate authority (CA) that is trusted for the specific scope.

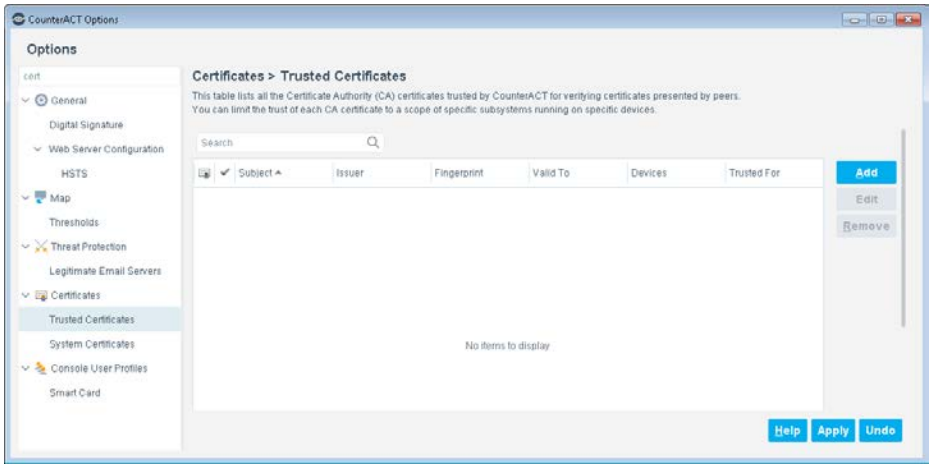
Ensure that each subsystem is scoped to the correct certificate on every device on which it runs.

Import and Configure Trusted Certificates

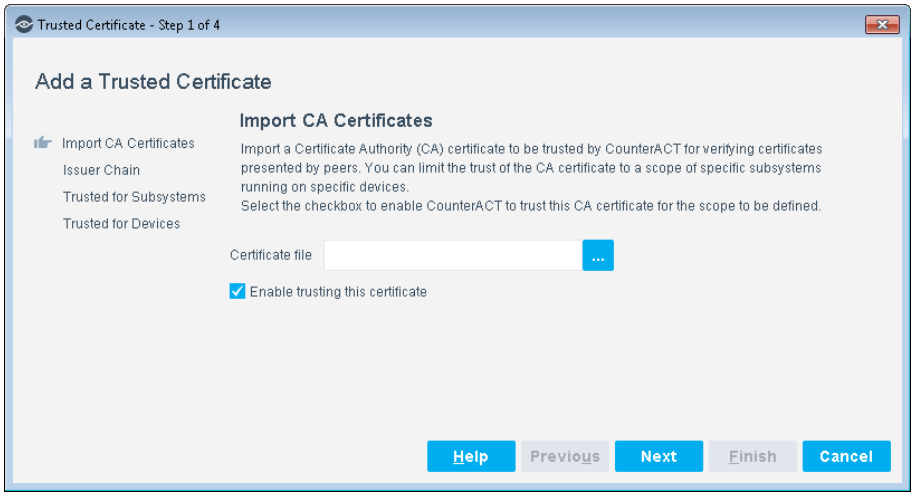
Import the CA certificates to be trusted by CounterACT into the Trusted Certificates table, and define the issuer chain and scope for which each certificate is trusted.

To import a trusted certificate and configure its scope:

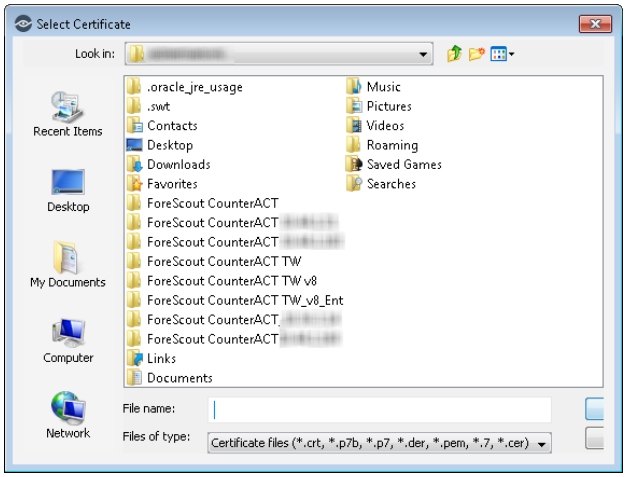
1. Log in to the CounterACT Console using an account that has *CounterACT Crypto Administration* permissions.
2. Select Options, and navigate to **Certificates > Trusted Certificates**. The Trusted Certificates pane opens.



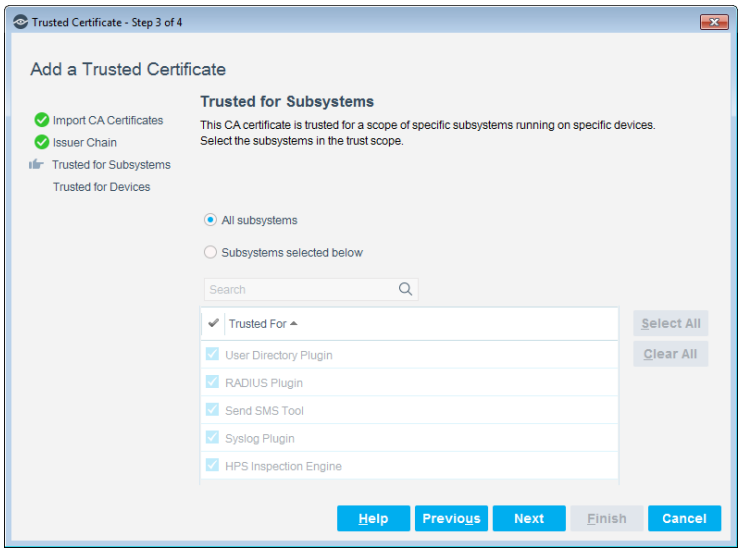
3. Select **Add** to import a CA certificate file for verifying system certificates presented by external services and applications. The Add a Trusted Certificate wizard opens.



4. Select the browse button.



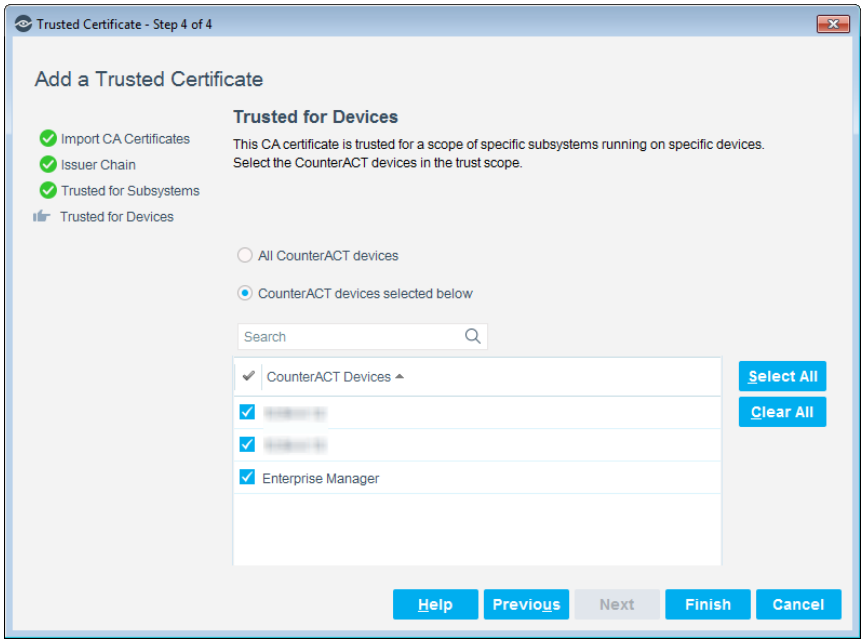
5. Browse to and select the CA certificate file to be imported, and select **Apply**. The file is imported.
6. Use the checkbox to enable or disable the imported certificate for the defined scope. Certificates are trusted only if they are enabled for the scope.
7. Select **Next**. The Certificate Details pane opens, displaying the details of the imported certificate.
8. Select **Next**. The Trusted for Subsystems pane opens.



9. To set the scope of subsystems that trust peers presenting certificates signed by this CA, do one of the following:
   - To indicate that all CounterACT subsystems trust peers presenting a certificate signed by this CA, select **All subsystems**.
   - To indicate that only specific CounterACT subsystems trust peers presenting a certificate signed by this CA, select **Subsystems selected below**. In the table, select the relevant subsystems.

   The CA certificate scope includes also the CounterACT device on which the subsystem runs. See step 11.

10. Select **Next**. The Trusted for Devices pane opens.



11. To set the scope of CounterACT devices on which the CA certificate is trusted, do one of the following:

- To trust the CA certificate on all CounterACT devices, select **All CounterACT devices**.
- To trust the CA certificate on only specific CounterACT devices, select **CounterACT devices selected below**. In the table, select the relevant devices.

The CA certificate scope includes also the subsystem that presents the signed certificate. See step 9.

12. Select **Finish**.

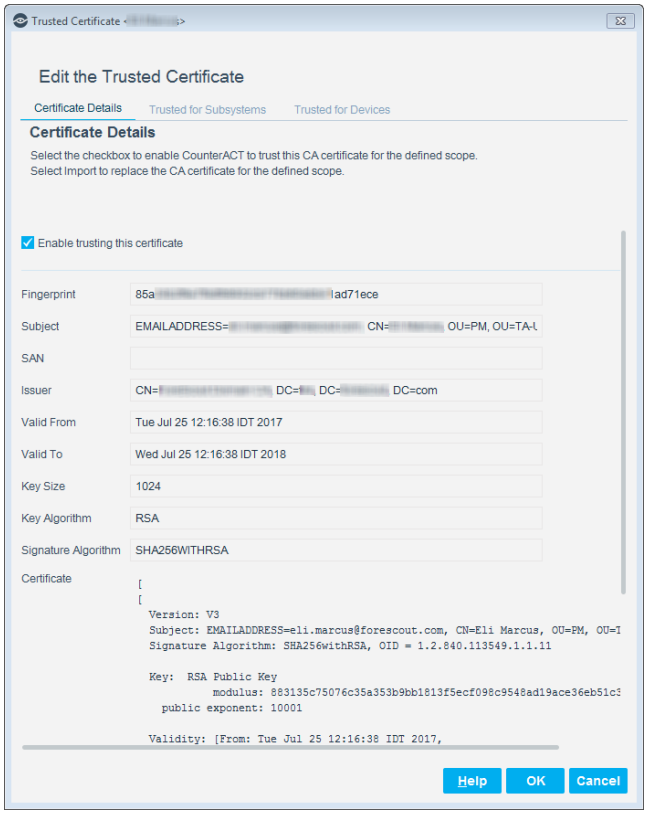
13. Select **Apply** when you have finished changing the configuration. A dialog box opens displaying all the changes to be applied. If the changes are correct, select **OK**.

Edit Trusted Certificate Entries

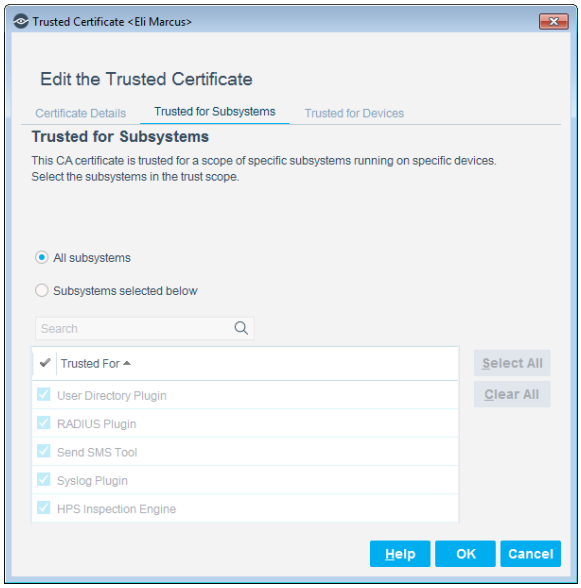
Edit the certificate scope, or replace the CA certificate for the defined scope.

To edit a CA certificate entry:

1. Log in to the CounterACT Console using an account that has *CounterACT Crypto Administration* permissions.
2. Select Options, and navigate to **Certificates > Trusted Certificates**. The Trusted Certificates pane opens.
3. Select the table entry to be edited, and select **Edit**. In the Edit the Trusted Certificate dialog box, the Certificate Details tab opens, displaying the details of the CA certificate.



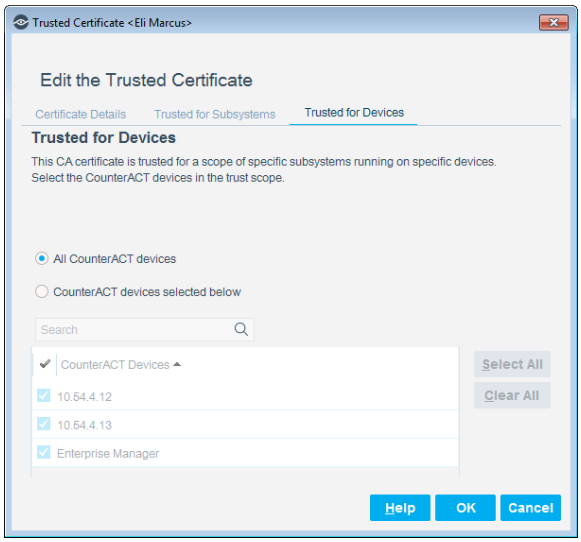
4. To import a different CA certificate for the scope defined in this table entry, select the **Import** button, browse to and select the CA certificate file to be imported, and select **Apply**. The file is imported.
5. Use the checkbox to enable or disable the certificate for the defined scope. A CA certificate is trusted only when enabled for the scope.
6. To change the subsystem scope, select the Trusted for Subsystems tab.



7. To set the scope of CounterACT subsystems that trust this CA certificate, do one of the following:
   - To trust this certificate for all CounterACT subsystems verifying external certificates, select **All subsystems**.
   - To trust this certificate for specific CounterACT subsystems verifying external certificates, select **Subsystems selected below**. In the table, select the relevant subsystems.

   The CA certificate scope includes also CounterACT device on which the subsystem runs. See step 9.

8. To change the CounterACT device scope, select the Trusted for Devices tab.



9. To set the scope of CounterACT devices on which CounterACT subsystems can run when presenting the system certificate signed by this certificate, do one of the following:
   - To allow subsystems running on all CounterACT devices, select **All CounterACT devices**.
   - To allow subsystems running on only specific CounterACT devices, select **CounterACT devices selected below**. In the table, select the relevant devices.

   The CA certificate scope includes also the subsystem that presents the signed certificate. See step 7.

10. Select **OK**.

11. Select **Apply** when you have finished changing the configuration. A dialog box opens displaying all the changes to be applied. If the changes are correct, select **OK**.

Remove Trusted Certificate Entries

You can remove a certificate table entry.

To remove a certificate entry:

1. Log in to the CounterACT Console using an account that has *CounterACT Crypto Administration* permissions.
2. Select Options, and navigate to **Certificates > Trusted Certificates**. The Trusted Certificates pane opens.
3. Select the table entry to be removed, and select **Remove**.
4. Select **Apply** when you have finished changing the configuration. A dialog box opens displaying all the changes to be applied. If the changes are correct, select **OK**.

Configure the System Certificates Table

To ensure secure communication, CounterACT presents system certificates to external services and applications for them to authenticate CounterACT. The scope defined in the certificate table determines which certificate CounterACT presents for each specific subsystem, such as Web Portal and User Directory Plugin, running on each specific device.

Ensure that each subsystem is scoped to the correct certificate on every device on which it runs.

Use the System Certificates pane to add or import certificates, their private keys, and their issuer chains, and to configure the subsystems and devices using these certificates.

System certificates used in earlier versions of CounterACT are automatically migrated, along with their scopes, to the System Certificates table as system certificates. The description of each of these migrated certificates begins with Migrated from*, followed by the CounterACT subsystem that uses it.*

Certificate Precedence between Appliance and Enterprise Manager

When adding an Appliance to an Enterprise Manager, the certificates of one may take precedence over the other, according to the following scenarios:

- A first Appliance is added to an Enterprise Manager - you can choose to copy the full Appliance configuration, including certificates to the Enterprise Manager, or to define them from scratch.
- An Appliance is added to an Enterprise Manager that has no certificates for the Appliance - the Appliance certificates are pushed to the Enterprise Manager, and scoped for the Appliance.
- An Appliance is added to an Enterprise Manager that has certificates whose scope covers the Appliance - the Enterprise Manager certificates take precedence, and the Appliance certificates are removed. The Enterprise Manager certificate should be scoped for all-devices to qualify.

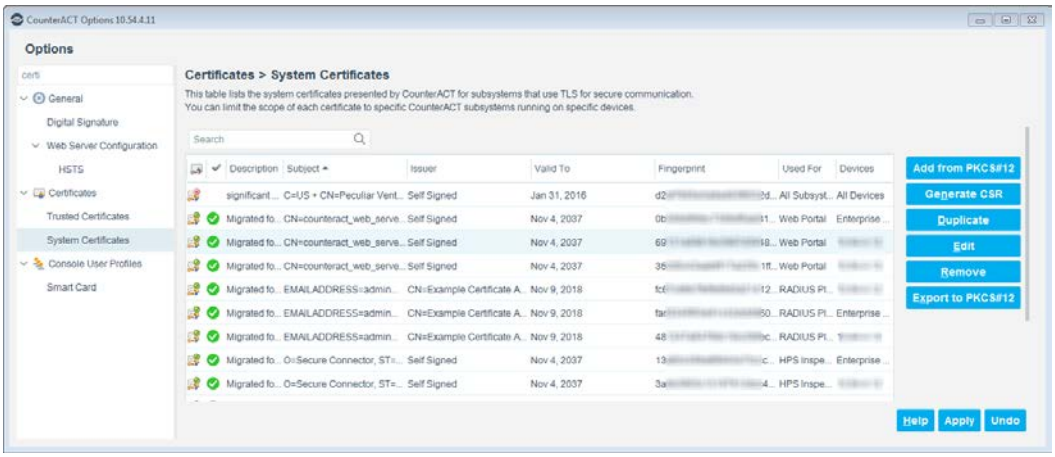
- To retain the original Appliance certificates, export them to a PKCS#12 file before adding the Appliance to the Enterprise Manager, and import the saved certificates once the Appliance has been successfully added.

Import and Configure System Certificates

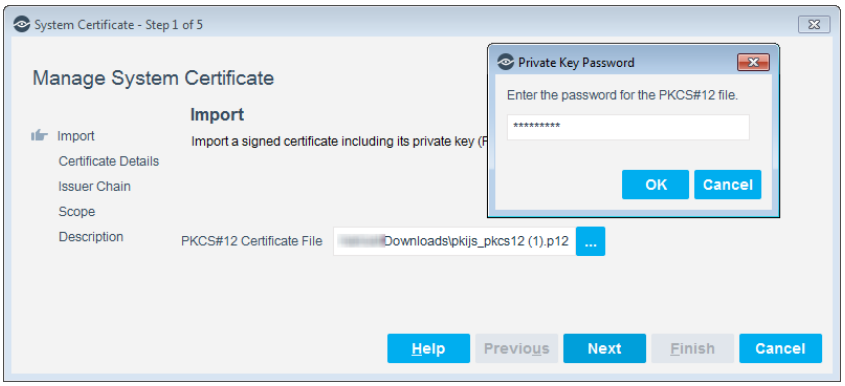
Import system certificates into the System Certificates table, and define the issuer chain and scope for which each certificate is presented by CounterACT to an external service or application.

To import and configure a PKCS#12 certificate:

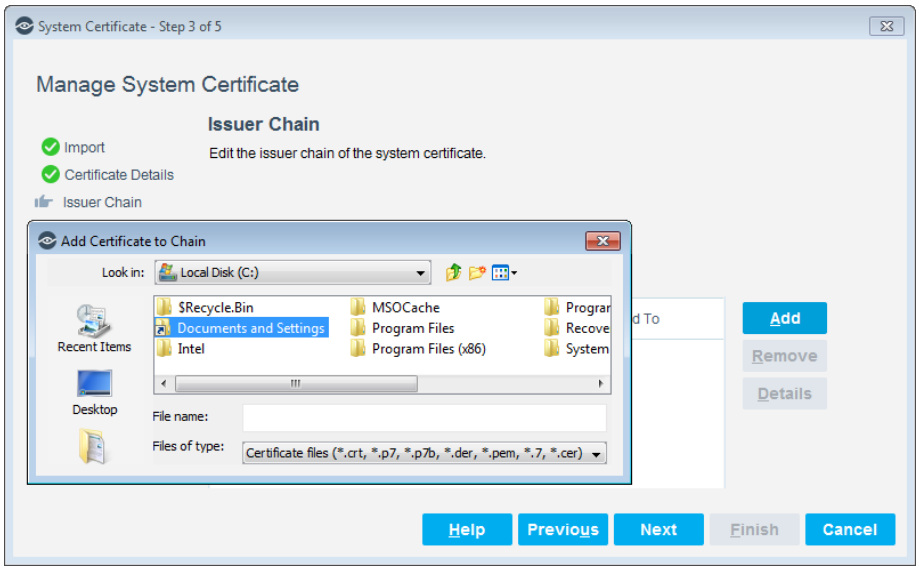
1. Log in to the CounterACT Console using an account that has *CounterACT Crypto Administration* permissions.
2. Select Options, and navigate to **Certificates > System Certificates**. The System Certificates pane opens.



3. Select **Add from PKCS#12** to import a certificate. The Manage System Certificate wizard opens to the Import pane.
4. Select the browse button, select the PKCS#12 file to be imported, and select **Apply**.
5. Select **Next**, enter the private key password for the signed certificate file, and select **OK**. The file is imported.



6. Select **Next**. The Certificate Details pane opens, displaying the details of the imported certificate.
7. Select **Next**. The Issuer Chain pane opens.
8. 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.

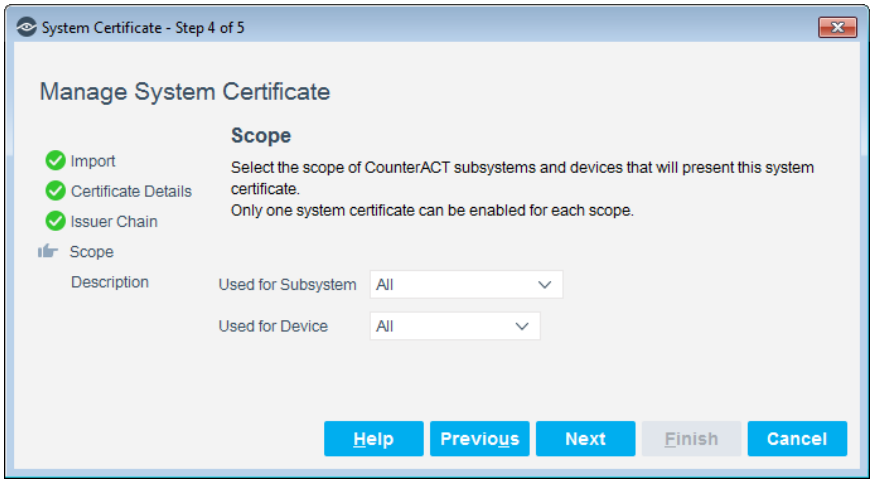


9. Select **Next**, the Scope pane opens.
10. To set the scope of CounterACT subsystems that present the system certificate to external services and applications, do one of the following in the **Used for Subsystem** field:
    - To present the system certificate for all CounterACT subsystems, select **All**.
    - To select a specific CounterACT subsystem for which the certificate is presented, select the relevant subsystem.

*You can select either **All** or one specific subsystem. To use the same certificate for some, but not all, CounterACT subsystems, duplicate the certificate and edit the new certificate's scope. See Duplicate System Certificate Entries.*

11. To set the scope of CounterACT devices on which CounterACT subsystems can present the system certificate, do one of the following in the **Used for Device** field:
    - To allow subsystems running on all CounterACT devices to present the certificate, select **All**.
    - To allow subsystems running on only a specific CounterACT device to present the certificate, select the relevant device.

*You can select either **All** or one specific device. To use the same certificate for some, but not all, CounterACT devices, duplicate the certificate and edit the new certificate's scope. See Duplicate System Certificate Entries.*



12. Select **Next**. The Description pane opens.
13. Enter a user-friendly description to identify this certificate and its scope in the System Certificates table.
14. Use the checkbox to enable or disable the imported certificate for the defined scope. Certificates are presented only when enabled for the scope.
15. Select **Finish**. The certificate is displayed in the System Certificates pane.
16. Select **Apply** when you have finished changing the configuration. A summary the changes to be applied is displayed. If the changes are correct, select **Yes**.

Generate a New System Certificate

If a new certificate is required for communicating with external services or applications, use the System Certificates > Generate CSR option to do the following:

1. Define the scope of the new system certificate.
2. Generate a certificate signing request (CSR).
3. Copy the CSR text and send it to an external certificate authority (CA).
4. After the CA creates and sends the signed system certificate to CounterACT, import it to the certificate table entry.
5. Define or review the issuer chain of the certificate.
6. Define a user-friendly description to easily identify the certificate in the System Certificates table.

Self-Signed Certificates

If you need a temporary certificate until a permanent one is issued, or if a "dummy" certificate will suffice for demo/lab environments where the security, even of secure connections, is not as critical, you can create a new system certificate that is self-signed. To work with this type of certificate, it is recommended to do one of the following:

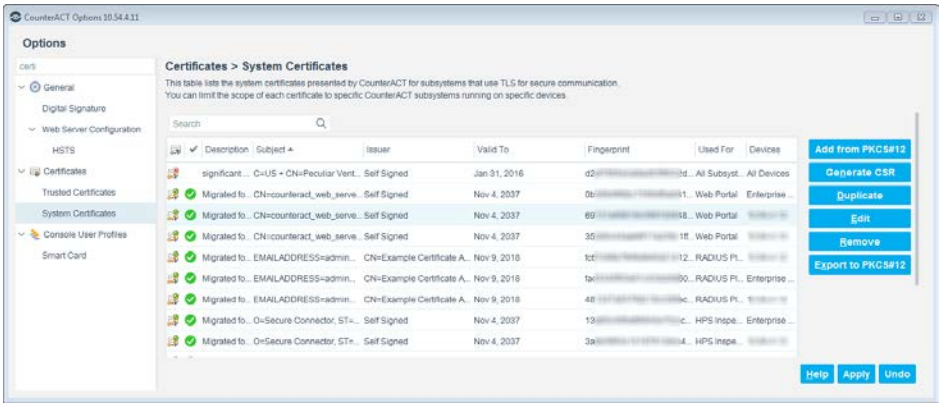
- Add the self-signed system certificate as trusted to the services that need to verify it.

- Disable certificate validation at the verifying end.

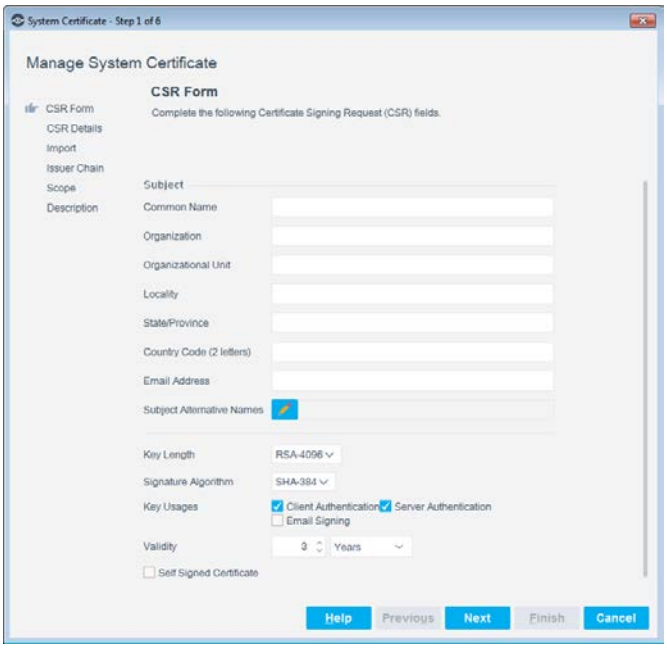
Generate a CSR for a New System Certificate

To generate a CSR for a signed system certificate and configure its scope:

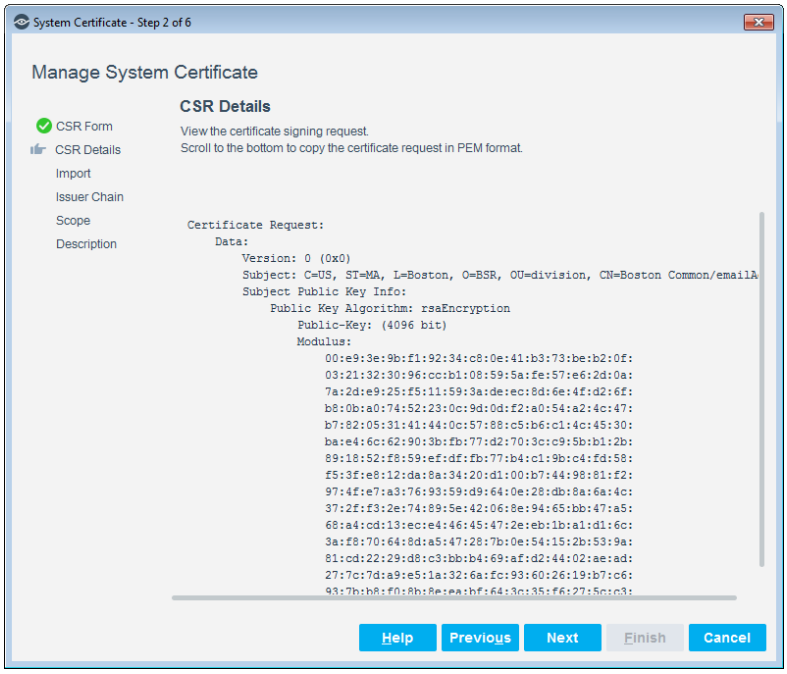
1. Log in to the CounterACT Console using an account that has *CounterACT Crypto Administration* permissions.
2. Select Options, and navigate to **Certificates > System Certificates**. The System Certificates pane opens.



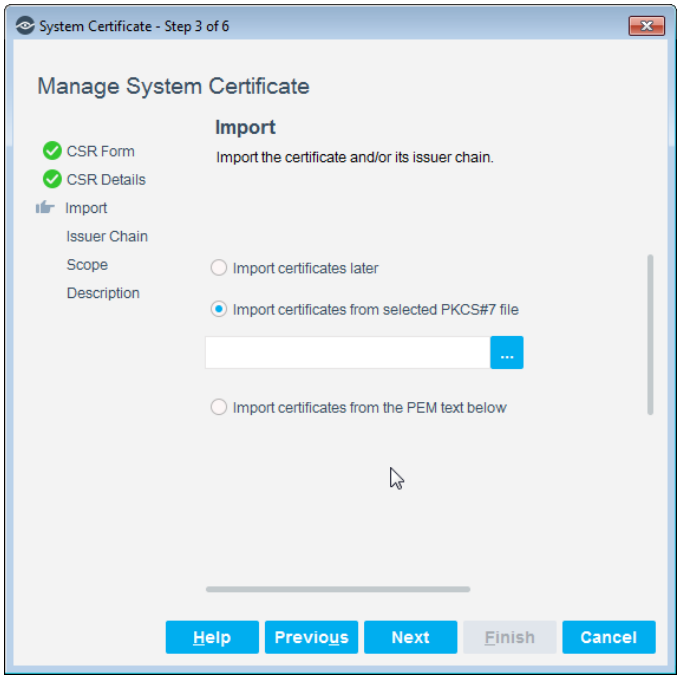
3. Select **Generate CSR** to create a signed certificate to be verified by external services and applications. The Manage System Certificate wizard opens to the CSR Form pane. For your convenience, most of the fields are automatically populated with the values used during the last CSR.
   You can set the certificate validity from 30 days to 10 years. The default validity is three years.



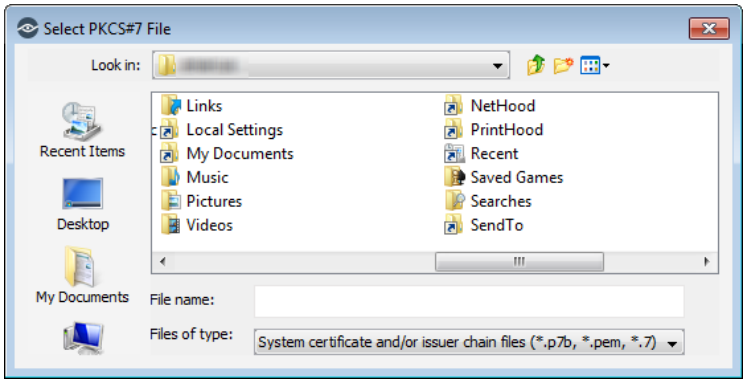
4. Complete the fields and select **Next**. When the CSR generation completes, the details of the generated CSR are displayed.



5. Select **Next**, the Import pane opens.

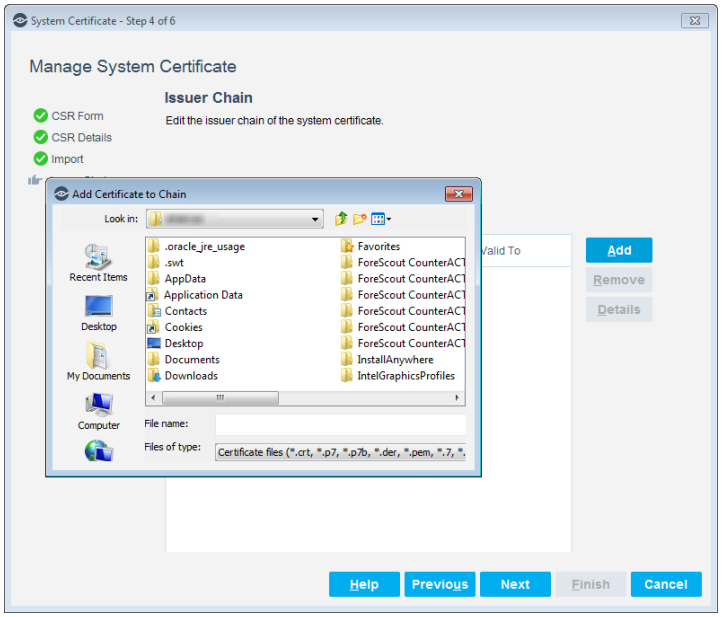


6. Do one of the following:
   - If you have not yet received the signed certificate from the external CA, select **Import certificates later**. When the certificate becomes available, you can download it to the local file system and then use the Edit feature to import it to this certificate table entry. 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 be imported (the following file extensions are supported: .p7b, .pem, .7).



   - 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.

7. Select **Next**. The Issuer Chain pane opens.
8. 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.



9. Select **Next**, the Scope pane opens.

10. To set the scope of CounterACT 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 CounterACT subsystems, select **All**.

   – To select a specific CounterACT subsystem for which the certificate is presented, select the relevant subsystem.

*You can select either **All** or one specific subsystem. To use the same certificate for some, but not all, CounterACT subsystems, duplicate the certificate and edit the new certificate's scope. See Duplicate System Certificate Entries.*

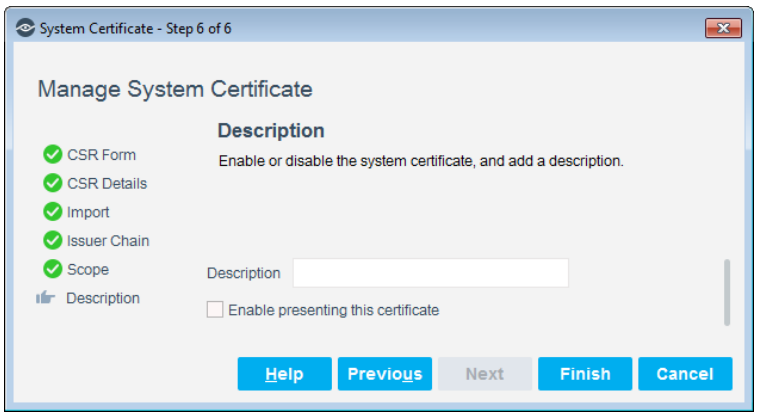
11. To set the scope of CounterACT devices on which CounterACT subsystems can present the system certificate, do one of the following in the **Used for Device** field:

   – To allow subsystems running on all CounterACT devices to present the certificate, select **All**.

   – To allow subsystems running on only a specific CounterACT device to present the certificate, select the relevant device.

*You can select either **All** or one specific device. To use the same certificate for some, but not all, CounterACT devices, duplicate the certificate and edit the new certificate's scope. See Duplicate System Certificate Entries.*

12. Select **Next**. The Description pane opens.



13. Enter a user-friendly description to identify this certificate and its scope in the System Certificates table.

14. Use the checkbox to enable or disable the imported certificate for the defined scope. Certificates are presented only when enabled for the scope.

15. Select **Finish**. The certificate is displayed in the System Certificates pane.

16. Select **Apply** when you have finished changing the configuration. A summary of the changes to be applied is displayed. If the changes are correct, select **Yes**.

Duplicate System Certificate Entries

You can create a duplicate of a certificate entry and then modify it. This is useful when you want to use the same certificate for a different scope.

To duplicate a certificate entry:

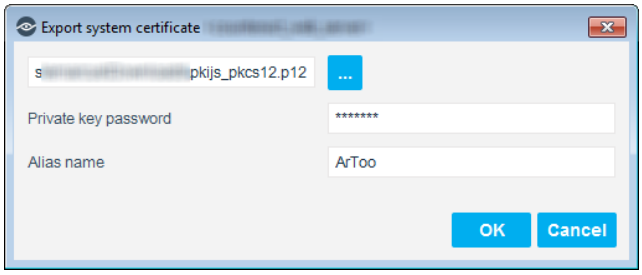
1. Log in to the CounterACT Console using an account that has *CounterACT Crypto Administration* permissions.
2. Select Options, and navigate to **Certificates > System Certificates**. The System Certificates pane opens.
3. Select the table entry to be duplicated, and select **Duplicate**. In the System Certificate dialog box, the Certificate Details tab opens, displaying the details copied from the existing system certificate.
4. 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.

To export a certificate entry:

1. Log in to the CounterACT Console using an account that has *CounterACT Crypto Administration* permissions.
2. Select Options, and navigate to **Certificates > System Certificates**. The System Certificates pane opens.
3. Select the table entry to be exported, and select **Export to PKCS#12**. The Export system certificate dialog box opens.



4. Select a certificate file to export to, and provide a private key password and an alias name for the file. Select **OK** to finalize.

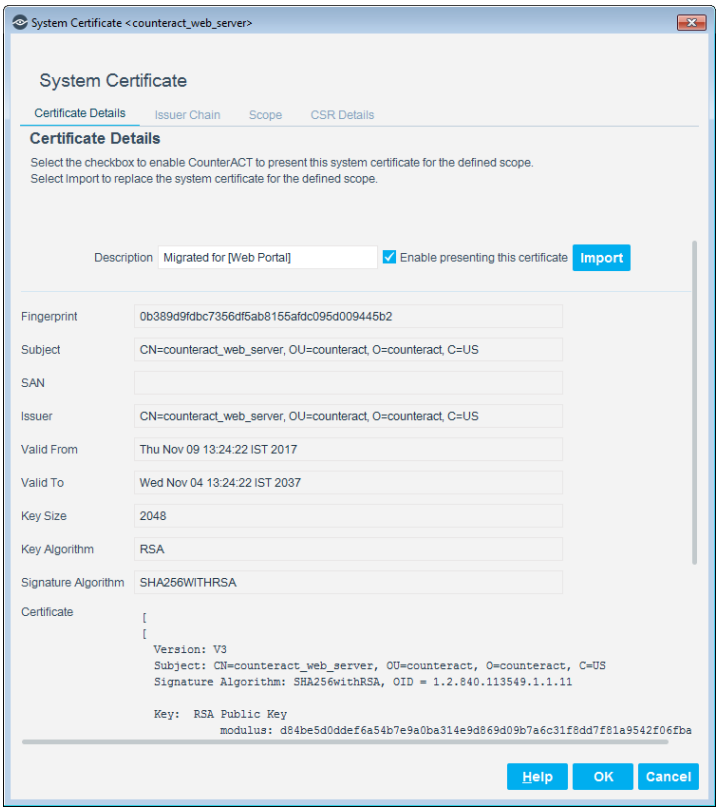
Edit System Certificate Entries

Edit the certificate scope, or replace the certificate for the defined scope.

To edit a certificate entry:

1. Log in to the CounterACT Console using an account that has *CounterACT Crypto Administration* permissions.

2. Select Options, and navigate to **Certificates > System Certificates**. The System Certificates pane opens.
3. Select the table entry to be edited, and 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. Use 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 CounterACT 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 CounterACT subsystems, select **All**.
   - To select a specific CounterACT subsystem for which the certificate is presented, select the relevant subsystem.

*You can select either **All** or one specific subsystem. To use the same certificate for some, but not all, CounterACT subsystems, duplicate the certificate and edit the new certificate's scope. See Duplicate System Certificate Entries.*

10. To set the scope of CounterACT devices on which CounterACT subsystems can present the system certificate, do one of the following in the **Used for Device** field:

- To allow subsystems running on all CounterACT devices to present the certificate, select **All**.
- To allow subsystems running on only a specific CounterACT device to present the certificate, select the relevant device.

*You can select either **All** or exactly one specific device. To use the same certificate for some, but not all, CounterACT 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** when you have finished changing the configuration. A summary the changes to be applied is displayed. If the changes are correct, select **Yes**.

Remove System Certificate Entries

You can remove a certificate table entry.

To remove a certificate entry:

1. Log in to the CounterACT Console using an account that has *CounterACT Crypto Administration* permissions.
2. Select Options, and navigate to **Certificates > System Certificates**. The System Certificates pane opens.
3. Select the table entry to be removed, and select **Remove**.
4. Select **Apply** when you have finished changing the configuration. A summary the changes to be applied is displayed. If the changes are correct, select **Yes**.

Legal Notice

© 2018 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.

2018-11-28 17:22

CA 8.0.1 M