



NetWitness® Endpoint User Guide
for Version 4.4



Copyright © 1994-2019 Dell Inc. or its subsidiaries. All Rights Reserved.

Contact Information

RSA Link at <https://community.rsa.com> contains a knowledgebase that answers common questions and provides solutions to known problems, product documentation, community discussions, and case management.

Trademarks

For a list of RSA trademarks, go to www.emc.com/legal/emc-corporation-trademarks.htm#rsa.

License Agreement

This software and the associated documentation are proprietary and confidential to Dell, are furnished under license, and may be used and copied only in accordance with the terms of such license and with the inclusion of the copyright notice below. This software and the documentation, and any copies thereof, may not be provided or otherwise made available to any other person.

No title to or ownership of the software or documentation or any intellectual property rights thereto is hereby transferred. Any unauthorized use or reproduction of this software and the documentation may be subject to civil and/or criminal liability.

This software is subject to change without notice and should not be construed as a commitment by Dell.

Third-Party Licenses

This product may include software developed by parties other than RSA. The text of the license agreements applicable to third-party software in this product may be viewed on the product documentation page on RSA Link. By using this product, a user of this product agrees to be fully bound by terms of the license agreements.

Note on Encryption Technologies

This product may contain encryption technology. Many countries prohibit or restrict the use, import, or export of encryption technologies, and current use, import, and export regulations should be followed when using, importing or exporting this product.

Distribution

Dell believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

August 2019

Contents

RSA NetWitness Endpoint 4.4 User Guide	11
About this Guide	11
Terminology and Acronyms	12
Technical Support	14
RSA NetWitness Endpoint System Overview	15
Components	16
System Analysis of Endpoints	17
System Analysis on Windows Machines	17
System Analysis on Mac Machines	19
System Analysis on Linux Machines	19
NetWitness Endpoint Architecture	20
Single-Server Architecture	20
Multi-Server Architecture	22
Getting Started	24
NetWitness Endpoint User Interface	24
Top Menu	25
Main Menu	28
Main Window	28
Tabs	31
Access the NetWitness Endpoint UI	31
NetWitness Endpoint Environment	33
Main Menu	33
Dashboard Window	35
Machines Window	36
Machine View	41
Modules List	44
Summary, Downloaded, and Scan Data Panes	46
More Info List	52
More Info Panes	54

Modules Window	54
IP List Window	57
Certificates Window	59
InstantIOCs Window	61
Downloads Window	63
Events Window	66
Server Configuration Window	68
Blocking Window	71
Tracking Systems	71
No Monitoring	72
Network Monitoring	72
Full Monitoring and Tracking	74
Full Monitoring, Except Network	75
Scan Your Network Environment	76
Scan Categories	76
Categories (Windows Machines)	77
Categories (Mac OS-X Machines)	79
Categories (Linux Machines)	80
Throttle Agent CPU	80
Download New Modules Automatically	82
Configure Scans for a Machine Group	83
Set Automatic Scan Request	86
Request an Agent Scan Manually	87
Differences Between Quick Scan and Full Scan	88
Perform a Scan in Standalone Mode	89
NetWitness Endpoint ConsoleServer Logs During a Scan	92
Known Compatibility Issues with Other Antivirus Programs	93
InstantIOCs	94
Levels of IIOCs, IIOC Scores, and Risk Score	96
IIOC Levels	96
Module IIOC Scores	97
Machine IIOC Scores	98
Risk Score	98
Differences between IIOC Score and Risk Score	100
Types of IIOCs	101

Event IIOCs	101
Machine IIOCs	102
Module IIOCs	102
Network IIOCs	103
Persistent and Non-Persistent IIOCs	104
Persistent IIOCs	104
Non Persistent IIOCs	104
Active IIOCs	104
Edit or Create IIOCs	105
Edit IIOCs	105
Change the Level of an IIOC	106
Create Your Own IIOCs	106
Whitelist Machine IIOCs	106
Investigate Results	108
Investigation Best Practices	108
Investigation Process Flows	109
Recommended Column Configurations	110
Review Modules	111
Floating Code	113
Hide Certain Files	114
Whitelisting and Gold Images	115
Use Filters to Find Malware	117
Faceted Filtering	118
Table Filter Editor	121
Use IIOCs to Find Malware	122
Analyze Files	126
VirusTotal	127
File Path	128
Filename	128
Machine Count	129
File Size	129
Packed	129
Signature	129
Days Since Compilation (or Compile Time)	129
Section Names	130
Hidden	130

Created Times	130
File Content	130
Analyze Scan Data for a Machine	133
Processes	134
DLLs and Drivers	135
Autoruns	135
Services	135
Tasks	135
Hosts	136
Files	136
Image Hooks	136
Kernel Hooks	136
Window Hooks	136
Suspicious Threads	137
Registry Discrepancies	137
Network History	137
Event Tracking	137
Trojan Functionality and API Calls	137
Access the Module Analyzer	139
Edit Module Status	143
Forward to Malware Analysis	144
Configure Forward to Malware Analysis	145
Perform Forward to Malware Analysis	145
Baselining	147
Checksums	147
Import Checksums	148
Bad Certificates	149
Bad Domains	150
Bad IPs	151
Bad File Hashes	152
Remediate Results	154
Use the Blocking System	154
Enable/Disable the Blocking System	155
Identify and Block Modules	158
View Blocked Modules	160
Restore Blocked Modules	163

Unblock a Blocked Module	163
View Global Blocking	163
Performance Considerations	164
Troubleshoot Blocking	164
Use Machine Containment	166
Supported Machines for Containment	167
Turn Containment On or Off	169
Configure Containment Warning Message	170
Edit Containment Exclusion List	170
Community Sources for Module Analysis	173
File Reputation Service	173
RSA Live Connect	174
Search Modules with Online Services	176
Add a New Search Engine	177
Analyze Modules with OPSWAT Metascan or YARA	178
Manage Modules	181
Automatic Status Assignment	182
Change Certificate Status	182
Configure Automatic Status Assignment	183
Update Certificates	184
Assign Hooks to Modules	185
MFT Viewer	185
View the Machine List for a Module	186
Download Modules	186
Automatically Download New Modules	187
Manually Download Modules	187
Retrieve Downloaded Modules	188
Export Blacklist-Whitelist Files	188
Import Blacklist-Whitelist Files	189
Manage Agents	190
Agent Status Icons	190
Modify Machine Status	191
Modify Machine Comments	192
Machine Groups	193
Perform a Full Memory Dump	195

Reboot a Machine	196
Kernel Adaptation System	197
Identify Unsupported Kernels	198
Kernel Update Process	198
Update an Agent	198
Update an Agent Using the NetWitness Endpoint UI	199
Update an Agent Using Agent Installer	200
Change Agent Server	200
Uninstall Agents and Remove Agents from the Database	201
Manage Alerts	203
Types of Alerts	204
Alert Fields	204
Alert Destination	210
Alertable Flags	211
Configure Alerts	212
Configure Syslog Alerts	212
Configure Incident Management Alerts	216
Configure Email (SMTP) Alerts	216
Test Connectivity	218
Modify or Delete an External Component	218
Temporarily Disable Alerting	219
Manage Users	220
Role-Based Access Control	220
Pre-Configured Roles	220
Role Permissions	221
Manage Users and Roles	225
Access User and Role Information	225
Perform User Management Tasks	226
Perform Role Management Tasks	228
Monitoring and External Components	230
Configure External Components	230
RSA NetWitness Suite Integration	231
Integrate NetWitness Endpoint with NetWitness Suite	232
Configure the .CSV Feed in NetWitness Endpoint	233

Export the NetWitness Endpoint CA Certificate from the NetWitness Endpoint ConsoleServer	235
NetWitness Suite Endpoint Meta Integration	238
Meta Integrator Installation	238
Enable the Meta Integrator	239
Meta Configuration File	243
Agent Meta Collection	244
View Agent Meta in NetWitness Suite	244
Integrating the Endpoint 4.4.0.2 or Later Console Server with an Endpoint Hybrid or Endpoint Log Hybrid	246
RSA Live	252
Configure RSA Live in NetWitness Endpoint	253
Connect RSA Live through Proxy	255
Select Available Feeds from RSA Live	256
Deploy RSA Live Feeds Offline	256
RSA NetWitness v9.7	256
SMTP	258
OPSWAT Scan Engine	258
YARA Scan Engine	259
References	261
REST API Server	261
REST Resources Architecture	263
Start/Stop the API Server	263
Data Format and HTTP Verbs	264
Authentication and Authorization	265
Authentication Type	265
Create Custom Usernames Using /register API	267
API Server Admin User	267
API Self-Discovery Using HATEOAS	268
Pagination	270
Debugging and Logging	270
Managing the API Server DB Connecting User	271
Tuning the API Server	272

NetWitness Endpoint ConsoleServerSync Tool	273
Phase 1	274
Phase 2	276
Phase 3	276
Alternate Command Line Procedure	277
Updating Connection Parameters	278
Live Feedback	279
Live Feedback Acceptance	279
Viewing Activity	281
JSON File Structure	281
NetWitness Endpoint UI URL Commands	286
List of Host and Service Ports	292
NetWitness Endpoint and Third-Party Antivirus Products	295
For Machines Running the NetWitness Endpoint Agent	295
For Machines Running the NetWitness Endpoint UI	296
For Machines Running the NetWitness Endpoint Console Server	297
Troubleshooting	297
1. Machines don't refresh in the NetWitness Endpoint UI; whitelisting isn't applied to modules; other functions don't seem to work	298
2. The InstallShield says that a port is not available or invalid	298
3. In the Packager, only half of the Connection Test is succeeding	299
4. Cannot Commission a new Secondary Server: Login failed	299
5. After installing a new Agent, it doesn't appear in the UI	300
6. After Installing Metascan, the Server Still Says "Antivirus Engine Disabled"	300
7. The Signature Column Says "Need Signature Revoke Update"	300
8. The ECAT_ProcessMergeScanBatches (ECAT\$PRIMARY)] process refuses to start after staging scan files	301
9. Troubleshooting IM Integration	301

RSA NETWITNESS ENDPOINT 4.4

USER GUIDE

This guide is intended for all NetWitness Endpoint administrators and analysts. It provides detailed information about NetWitness Endpoint product features and related technologies. It is assumed the user has a good understanding of low-level PC security and related terminology.

For information about installing and configuring NetWitness Endpoint, as well as the Roaming Agents Relay, see **RSA NetWitness Endpoint 4.4 Installation Guide** available on [RSA Link](#).

About this Guide

The *RSA NetWitness Endpoint User Guide* describes:

- NetWitness Endpoint and its components, as detailed in the following sections:
 - [RSA NetWitness Endpoint System Overview](#)
 - [Getting Started](#)
- How to scan and investigate your environment using NetWitness Endpoint and InstantIOCs, as detailed in the following sections:
 - [Scan Your Network Environment](#)
 - [InstantIOCs](#)
 - [Investigate Results](#)
 - [Community Sources for Module Analysis](#)
- How to remediate investigation findings, as detailed in [Remediate Results](#).
- How to manage modules (files) and agents (endpoints) in the NetWitness Endpoint environment, as detailed in the following sections:
 - [Manage Modules](#)
 - [Manage Agents](#)
- How to take advantage of and configure the alerting options in NetWitness Endpoint, as detailed in [Manage Alerts](#).

- How to set up NetWitness Endpoint users and user roles, as detailed in [Manage Users](#)
- How to use and configure RSA External Components to supplement the monitoring and investigative capabilities of NetWitness Endpoint, as detailed in [Monitoring and External Components](#).
- The REST API's of NetWitness Endpoint and how to use the NetWitness Endpoint API Server, as detailed in [REST API Server](#).
- Additional tools and reference information for NetWitness Endpoint, as detailed in the following topics:
 - [NetWitness Endpoint ConsoleServerSync Tool](#)
 - [Live Feedback](#)
 - [NetWitness Endpoint UI URL Commands](#)
 - [List of Host and Service Ports](#)
 - [NetWitness Endpoint and Third-Party Antivirus Products](#)
 - [Troubleshooting](#)

Audience

This guide is intended for all NetWitness Endpoint administrators. It is assumed the user has a good understanding of low-level PC security and related terminology.

Terminology and Acronyms

The following table defines some of the terms and acronyms found in this guide:

Term/Acronym	Definitions
Agent	The NetWitness Endpoint software that resides on the machine.
Baselining	Choosing a standard setup computer (or gold image) as a base to whitelist all trusted modules and have preloaded data on NetWitness Endpoint, which helps to remove noise for security analysts during investigation.
CEF	Common Event Format.
DB	Database.

Term/Acronym	Definitions
File Reputation Service	An optional service that checks files against a database of known, valid software as well as known malware.
Get Command Loop	The act of an NetWitness Endpoint agent periodically checking if it has a command.
IIOC or InstantIOC	Instant Indicator of Compromise.
Machine	The computer (Windows and Mac desktops, laptops or servers; physical and virtual) targeted by the analysis; machines can be laptops, workstations, servers, tablets, routers, or any system, physical or virtual, where a supported OS is installed.
MFT	Master File Table.
Modules	The files and code fragments found for all assessed clients.
OPSWAT Metascan	An optional third-party application supported by NetWitness Endpoint, which, when enabled, will scan all files downloaded by NetWitness Endpoint against a configured choice of anti-virus (AV) engines.
OS	Operating System.
PCS	Primary ConsoleServer or Primary Server.
Process Memory Dump	A file containing a direct copy of the content of all the memory used by a process.
Risk Score	A data-driven score that ranges from 0 to 100. This score is the output of a machine-learning algorithm and represents the probability of the module being malicious.
Roaming Agents Relay (RAR)	RAR provides visibility of endpoints that are disconnected from a corporate network and can be deployed as a cloud service.
Server Discovery	The act of an NetWitness Endpoint agent discovering its ConsoleServer.

Term/Acronym	Definitions
SCS	Secondary ConsoleServer or Secondary Server.
UI	The user interface terminal through which the NetWitness Endpoint Admin manages/checks NetWitness Endpoint agents and ConsoleServers.
YARA	YARA is an open source static analysis tool.

Technical Support

Support Option	Online Address
RSA Link	https://community.rsa.com
Contact RSA Support	https://community.rsa.com/docs/DOC-1294
Community	https://community.rsa.com/community/products/netwitness
Support Plans and Options	https://Community.rsa.com/docs/DOC-40401
Email	support@rsa.com

RSA NETWITNESS ENDPOINT

SYSTEM OVERVIEW

The RSA NetWitness Endpoint product is an endpoint threat detection solution that exposes malware and other threats, highlights suspicious activity for investigation, and instantly determines the scope of a compromise to help security teams stop advanced threats faster. NetWitness Endpoint's unique signature-less approach identifies known, as well as previously unknown threats that other solutions miss.

NetWitness Endpoint enables you to discover and analyze malware, including rootkits, viruses, advanced threats, and other unwanted software on your endpoints. NetWitness Endpoint helps security teams to detect, analyze, and respond to malware and other threats on endpoints.

NetWitness Endpoint provides the following:

- Behavior Tracking and Alerting
- Deep System Analysis
- Suspect and Legitimate File Management

NetWitness Endpoint monitors endpoint activity through behavior tracking and runs scans of the endpoints for deep system analysis. Once data has been collected, NetWitness Endpoint can alert on suspicious activity. To help analysts quickly triage and focus their investigation, NetWitness Endpoint provides capabilities to manage suspect and legitimate files.

NetWitness Endpoint tracks operations performed on endpoints and looks for behavior typically exhibited by malware. Security teams can receive alerts for an early warning of potentially malicious activity.

NetWitness Endpoint provides the following tools to quickly whitelist files that may have suspicious behaviors but are in fact legitimate (such as security products), and also blacklist known threats:

- Check for known file hashes with the File Reputation Service, NIST, and custom hash databases
- Complete digital signature validation of all executable files
- Binary analysis for strings, packing, and loaded DLLs
- Complete environment correlation that shows on which machine and the number of systems where the file is found

- Optional OPSWAT Metascan can scan all files against four or more AV engines to find known malware
- Optional YARA analysis tool to help classify known threats
- Optional File Reputation service checks against a database of known, valid software, as well as known malware

Components

NetWitness Endpoint consists of the following components.

Component	Description
Machine	The computer (Windows and Mac desktops, laptops or servers; physical and virtual) targeted by the analysis.
Agent	The NetWitness Endpoint software that resides on the machine.
Primary Server	The primary server software module used to operate and communicate with the agent and Secondary Servers. It is also used to control the agent via the management console.
Secondary Servers	Any number of optional server software modules that will share the job of the primary server.
Management Console (NetWitness Endpoint UI)	The graphical user interface used to interact with the agent, server, and database.
Database Server	NetWitness Endpoint databases are run on a SQL server database, Microsoft SQL Server 2012 and 2014 are the supported versions.
Packager	Executable used to configure and generate the agent installer that will be deployed to the client machines. The agent installer will then install and activate an agent when executed.

Component	Description
Installer	Executable installer to install a Primary or Secondary NetWitness Endpoint ConsoleServer when executed.
File Reputation Service	The File Reputation Service provides access to a large whitelist database, updated in real-time, so the latest file validation information is always available.
OPSWAT Metascan	An optional third-party application supported by NetWitness Endpoint, which, when enabled, scans all files downloaded by NetWitness Endpoint against antivirus engines.
Roaming Agents Relay (RAR)	RAR provides visibility of endpoints that are disconnected from a corporate network and can be deployed as a cloud service.

System Analysis of Endpoints

NetWitness Endpoint performs a complete assessment of a machine (Windows, Mac OS-X, or Linux) at selected time intervals, or upon request.

System Analysis on Windows Machines

During the scanning of a Windows machine, NetWitness Endpoint:

- Retrieves lists of drivers, processes, DLLs, network connections, files (executables), services, autoruns, Windows hooks, Service Tables hooks, Registry Discrepancies, Inline hooks, IAT/EAT Hooks, IDT hooks, SYSENTER hooks, Kernel Object hooks, Host file entries, scheduled tasks, and suspicious threads, as well as all hidden modules
- Gathers security information such as network share, patch level, Windows tasks and much more
- Analyzes Windows internal structures for alteration and consistency
- Searches for kernel and user mode hooks in SSDT, IDT, IAT/EAT, and IRP_MJ
- Reports the hashes (SHA-256, SHA-1, MD5) and file size of all executable files found on the system

- Integrates with YARA and OPSWAT Metascan AV engine
- Reports on known, legitimate software as well as malware using the File Reputation service

More specifically, the NetWitness Endpoint agent performs the following checks during a scan:

Hooking

- SSDT (System Service Dispatch Table) hooks
- Alternate SSDT hook (KTHREAD.ServiceTable)
- IDT (Interrupt Descriptor Table) Hooks
- System drivers IO hooks
- System entry (SYSENTER and int2E) hooks
- Local and global Windows hooks (SetWindowsHookEx)
- User mode hooks (IAT, EAT, Inline) for processes and DLLs
- Model Specific Registers hooks
- Kernel Object hooks
- Metasploit detection

Integrity

- Windows Kernel integrity validation
- User mode process code section validation
- Code sign signature verification

Behavior

- Number of connections per process
- Auto start program identification (Autoruns)
- Windows Services analysis

Hidden Items

- Hidden process
- Hidden threads
- Hidden files

- Executables in ADS (Alternate Data Streams)
- Hidden registry keys

System Analysis on Mac Machines

During the scanning of a Mac machine, NetWitness Endpoint:

- Retrieves lists of kernel extensions, running processes, loaded dylibs, frameworks, network connections, files (executables), daemons/agents, and host file entries
- Gathers machine security settings such as gatekeeper, file vault, and safari
- Searches for various autorun strategies such as cron jobs, launched scheduled jobs, startup items, and more
- Reports the hashes (SHA-256, SHA-1, MD5) and file size of all executable files found on the system
- Integrates with YARA and OPSWAT Metascan AV engine
- Reports on known, legitimate software as well as malware using the File Reputation service

More specifically, the NetWitness Endpoint agent for Mac performs the following checks during a scan:

Integrity

- Code sign signature verification for modules

Behavior

- Number of connections per process
- Auto start program identification (Autoruns)
- Running daemons, agents analysis for anomaly

System Analysis on Linux Machines

During the scanning of a Linux machine, NetWitness Endpoint:

- Retrieves lists of drivers, processes, files (executables), services, autoruns, and Host file entries
- Searches for various autorun strategies such as cron jobs
- Reports the hashes (SHA-256, SHA-1, MD5) and file size of all executable files found on the system

- Integrates with YARA and OPSWATMetascan AV engine
- Reports on known, legitimate software as well as malware using the File Reputation service

More specifically, the NetWitness Endpoint agent for Linux performs the following checks during a scan:

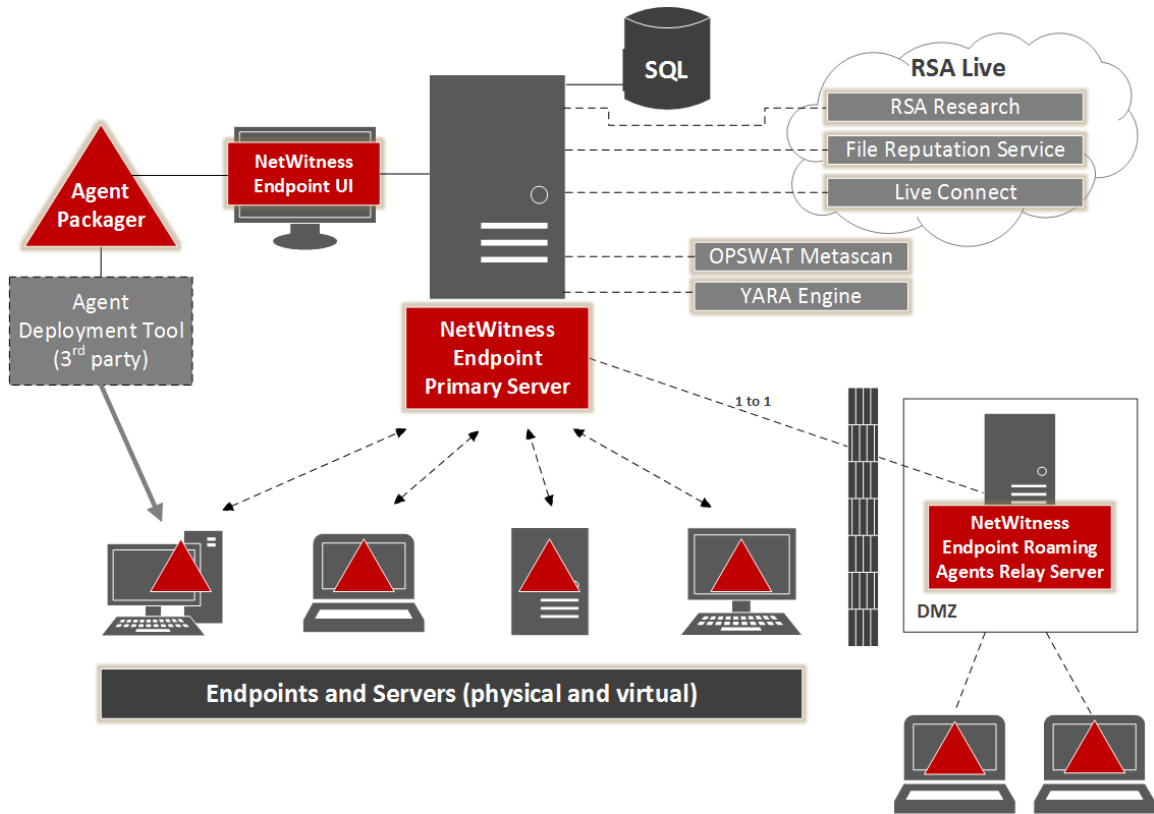
- Number of connections per process
- Auto start program identification (Autoruns)
- Root bash history of users
- Mounted paths
- Services (both init.d and system)
- Logged in users

NetWitness Endpoint Architecture

This topic provides an overview of NetWitness Endpoint architecture and the differences between single-server and multi-server architecture.

Single-Server Architecture

The following figure shows the overall NetWitness Endpoint deployment architecture, with a single server. The Administrator accesses the system through two main programs with a graphical interface: the NetWitness Endpoint User Interface (UI) and the Agent Packager.



The NetWitness Endpoint Console is a graphical front-end to the NetWitness Endpoint servers, which can run on the same or a different machine as the NetWitness Endpoint Server. The data is stored in a Microsoft SQL Server database, which may be hosted on the same or a different machine. The NetWitness Endpoint Server also optionally communicates with the third-party OPSWAT Metascan system and YARA engine, if installed, as well as a variety of information sources available through RSA Live.

The NetWitness Endpoint Server communicates with the NetWitness Endpoint agents that are deployed on client machines (laptops, desktops, servers; physical and virtual machines). The NetWitness Endpoint agents monitor and scan the machines and send the information to the NetWitness Endpoint Server, which stores the data in the SQL Server database.

The administrator uses the separate NetWitness Endpoint Agent Packager program to create the agent installer program that can then be deployed to the client machines, where the agent program is installed and configured with the Primary Server URL. The agent then runs unobtrusively on the client machines.

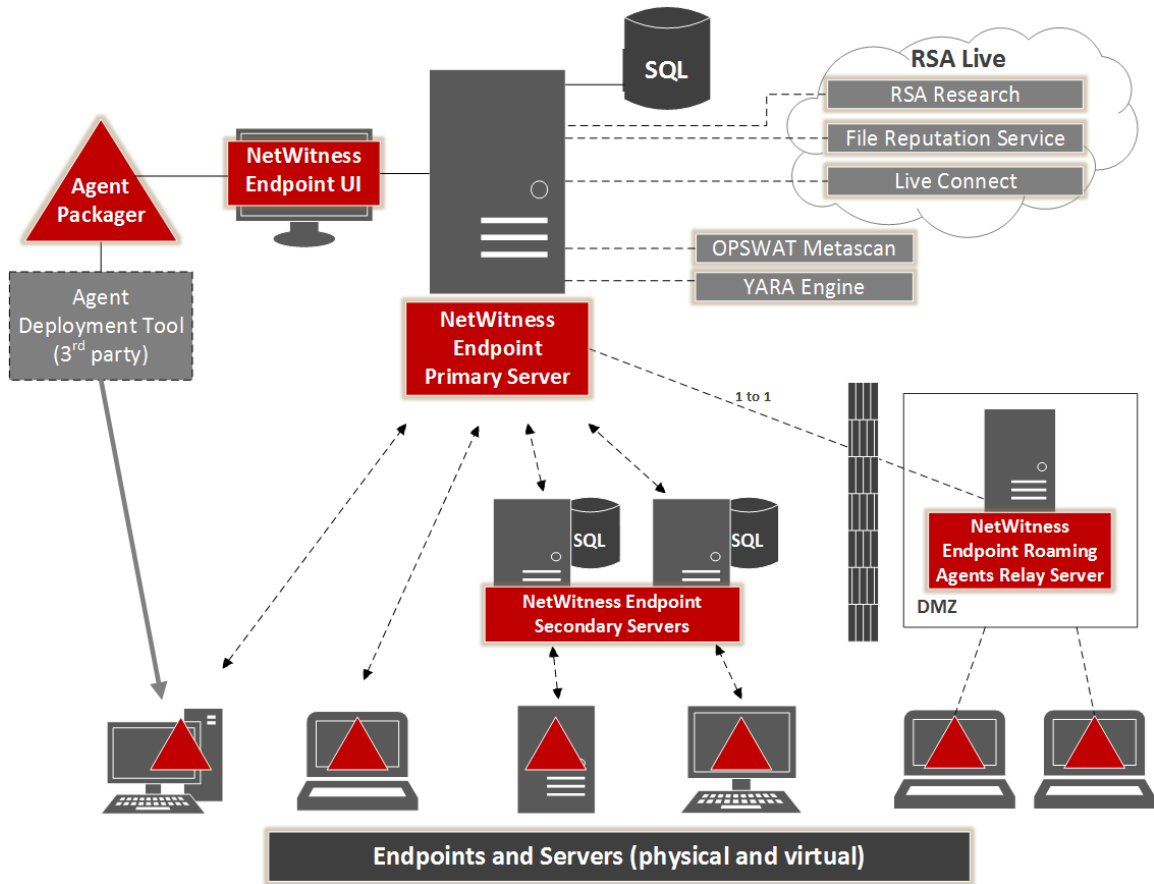
There is also the option of installing the NetWitness Endpoint Roaming Agents Relay Server. If the endpoints are taken outside the corporate network, the agent can no longer communicate with the NetWitness Endpoint Primary Server, and the endpoint behavior will not be evaluated. Modifying the firewall settings to accommodate NetWitness Endpoint will increase the attack surface and is not an acceptable workaround. The Roaming Agents Relay is designed to address this problem. A RAR Server can be set up in the public environment that is accessible to both an endpoint outside the network and the NetWitness Endpoint Server within the enterprise network. The endpoint outside the enterprise network sends the data to the RAR Server and the NetWitness Endpoint Server pulls data from the RAR Server. Thus the communication between the endpoint and the NetWitness Endpoint Server happens through the secure infrastructure provided by the RAR Server. For more information about the RAR Server, see the *Roaming Agents Relay Overview* topic in the **RSA NetWitness Endpoint 4.4 Installation Guide** available on [RSA Link](#).

Multi-Server Architecture

The workload of the NetWitness Endpoint Server can be distributed amongst any number of servers. There will always be one main server that has primary responsibility, which is called the Primary Server. The other servers are called Secondary Servers. A maximum of three Secondary servers may be installed for each Primary Server.

The following figure gives a high-level picture of the NetWitness Endpoint deployment architecture for multiple servers, coordinated by a single Primary Server.

The job of allocating the workload amongst the servers is done automatically. In normal usage, the existence of Secondary servers is relatively invisible. The Primary Server's database periodically syncs with all of the Secondary servers' databases, and presents the latest picture to the NetWitness Endpoint UI.



GETTING STARTED

This topic provides information to help you get started using NetWitness Endpoint once the setup is completed.

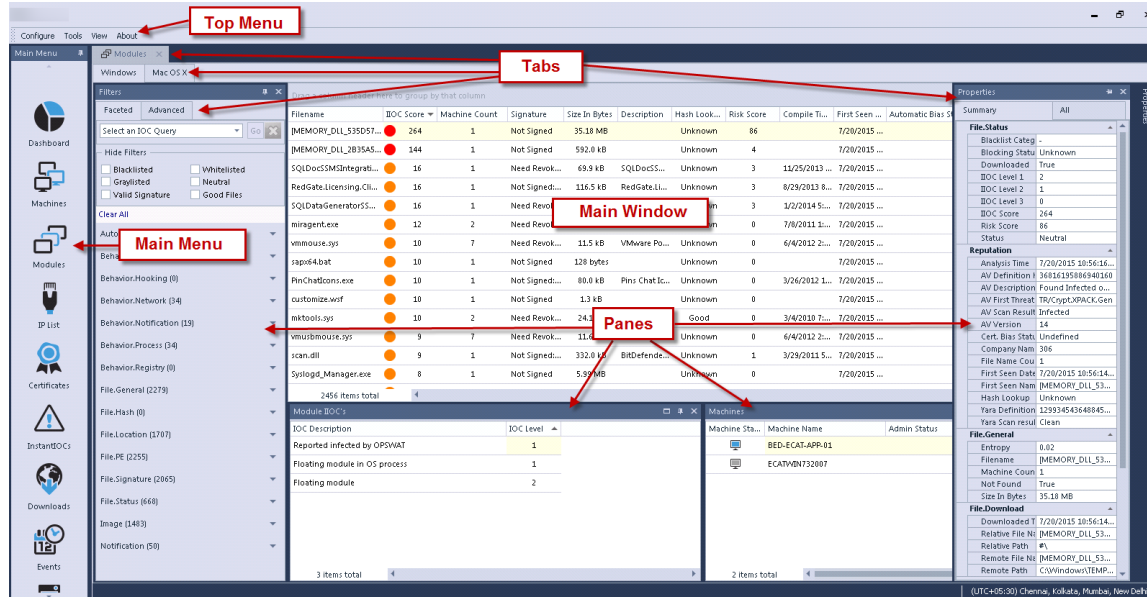
Topics Covered:

- [NetWitness Endpoint User Interface](#)
- [NetWitness Endpoint Environment](#)
- [Tracking Systems](#)

NetWitness Endpoint User Interface

The NetWitness Endpoint UI displays information related to your network assessment. There are a variety of methods available to customize and view a wide assortment of information about your environment.

The following figure shows the NetWitness Endpoint UI with the **Modules** window open in the main window.



The interface consists of:

- **Top Menu:** The Top Menu consists of basic functions and commands that can be accessed at any time.

- **Main Menu:** When you click on any Main Menu option, the respective window opens in the Main Window as a tab. You can toggle between Main Menu option tabs or close any option.
 - Click the **Pin** button to enable or disable the auto-hide function.
- **Main Window:** The Main Window displays information based on the option currently selected in the Main Menu and tabs for other options that were previously accessed from the Main Menu.
- **Panes:** Panes display additional information related to the content in the Main Window.
- **Tabs:** Tabs display hidden panes/windows.

Note: Every part of the UI can be dragged and docked according to your preferences. To restore the original layout, click **Tabs > Restore Layout**.

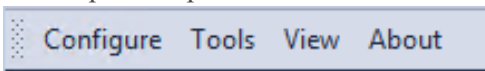
Modify the style of the UI: You may modify the style of the UI by selecting one of the preset styles by clicking **Configure > Skins** in the Top Menu.

The following topics provide more detailed information on the main parts the NetWitness Endpoint UI:

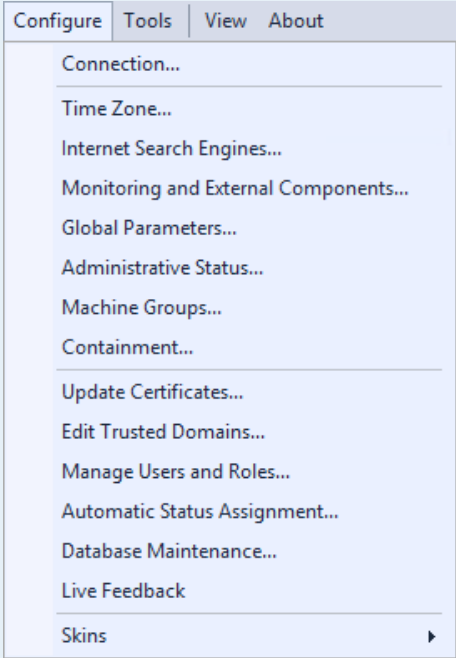
- [Top Menu](#)
- [Main Menu](#)
- [Main Window](#)
- [Tabs](#)

Top Menu

The Top Menu provides access to all available sub-menu items, as shown below.



Menu	Description
------	-------------

Menu	Description
	<p>Allows you to configure:</p> <ul style="list-style-type: none"> • NetWitness Endpoint Connection and time zone • Internet Search Engines • Monitoring and External components (Syslog, SMTP, IM Broker, Security Analytics, NetWitness, Live), select and refresh RSA Live feed options (see Monitoring and External Components) • Global parameters, administrative status, and machine groups (see Machine Groups) • The Containment Exclusion List (see Edit Containment Exclusion List) • Certificates and trusted domains • User Management (only users with administrative rights) (see Manage Users) • Automatic Status Assignment of modules based on the certificate status (see Automatic Status Assignment) • Database Maintenance provides database clean up settings • Live Feedback (see Live Feedback) • Modify skins (style of interface)

Menu	Description
 <p>The screenshot shows a menu with the following items: Refresh (F5), Module Analyzer, MFT Viewer, Standalone Scan, Import/Export, Agent Maintenance, and Force Blocking State Update.</p>	<p>Allows you to:</p> <ul style="list-style-type: none"> • Refresh (view latest machine data) • Analyze downloaded or local executable files (see Access the Module Analyzer) • View MFT (Master File Table) (see MFT Viewer) • Perform a standalone scan and export scan configuration (see Perform a Scan in Standalone Mode) • Import or export Whitelist/Blacklist XML files or STIX data (see Export Blacklist-Whitelist Files and Import Blacklist-Whitelist Files) • Enter or upload Checksums (see Checksums) • Update all agents using Agent Maintenance (see Update an Agent) • Force Blocking State Update (see Identify and Block Modules and Unblock a Blocked Module)
 <p>The screenshot shows a menu with the following items: Show Compact View, Disable Machine Status Auto-Refresh, and Restore Layout.</p>	<p>Allows you to:</p> <ul style="list-style-type: none"> • Show compact view • Disable/Enable Machine Status Auto-Refresh • Restore the default layout
 <p>The screenshot shows the About menu item.</p>	<p>Displays the NetWitness Endpoint version and copyright information. It also displays the permissions assigned to the currently logged in user according to the users assigned role.</p>

Main Menu

The Main Menu organizes information. You can click on an option in the Main Menu and the respective information is displayed in the main window. If you have more than one window open, then each previously opened window is available as a tab until you close the tab.

The following options are available in the Main Menu:

- Dashboard
- Machines
- Modules
- IP List
- Certificates
- InstantIOCs
- Downloads
- Events
- Server Configuration
- Blocking

For detailed information for each option in the Main Menu, refer to [NetWitness Endpoint Environment](#).

Main Window

When one of the Main Menu options is accessed, it opens in the Main Window. The Main Window is generally made up of different tables and panes.

Note: You can move most of the panes and tables outside the Main Window. This provides different views with fewer clicks, especially if you have multiple windows/pages.

Tables

Tables can be customized and organized in different ways. Column sorting, order, and visibility are stored between NetWitness Endpoint sessions.

Note: If the width of the column header is small, you can hover over a column title to view the column title.

Column Option	Directions
---------------	------------

Column Option	Directions
Group by one or more columns	<ul style="list-style-type: none"> • Drag the column header to the horizontal border above the column headers. • Drag additional columns to the border to create a sorting hierarchy. • Hover your mouse to the right of the column header name to adjust ascending/descending order.
Move columns	Click the column header and drag it to a desired position.
Resize columns	<p>Click the column separator in the title bar and drag it to the desired size.</p> <div style="border: 1px solid green; padding: 5px;"> <p>Note: If you double-click the column separator, the column will automatically default to the widest column size.</p> </div>
Customize the columns or the information available in a column	<ul style="list-style-type: none"> • Hover over the column header, and click the chevron on the right to sort the column in ascending or descending order. • Right-click the title of the column to access a drop-down menu that offers a variety of options including sorting, grouping, hiding, and filter editing options. This is also how you access Column Chooser, where you can select additional column headers that are not defaults. • Hover over the column header to access a pin on the right. Click the pin and select the desired option from the drop-down menu.

Panes

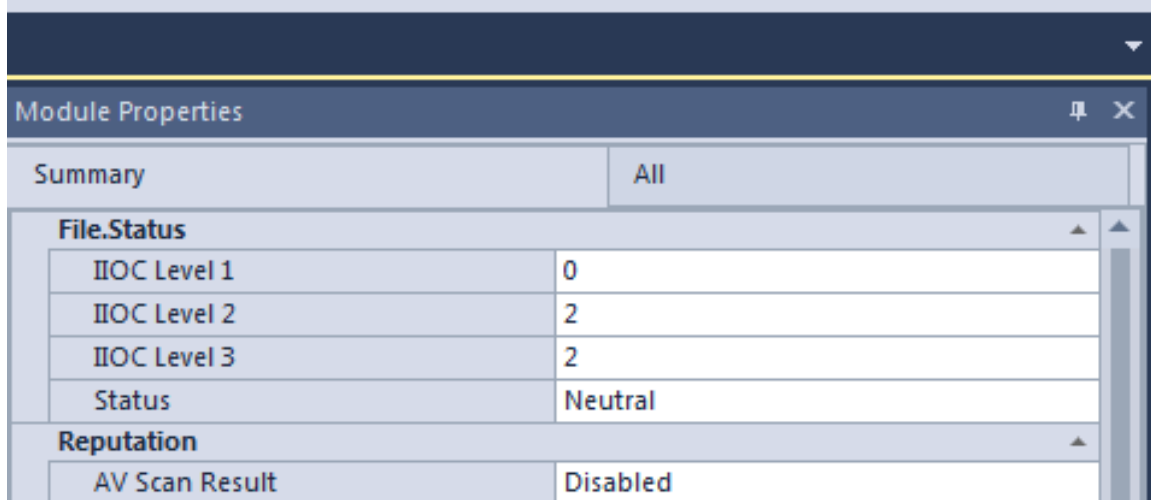
Panes display additional information related to a Main Menu option selected in the Main Window. They can be customized and moved anywhere in the Main Window, or even outside of the Main Window. Also, they have an auto-hide option that hides the pane when the option is not selected.

Pane Option	Directions
Enable or disable the auto-hide function	 Click the Pin button.

Pane Option	Directions
Close a pane	Click the X .
Relocate a pane	Click the pane header and drag it to the new location.
Resize a pane	Click and drag a corner or edge of a pane to resize it.
Re-open a closed pane or reset the layout	Click Tabs > Restore Layout

Following are the two types of common panes:

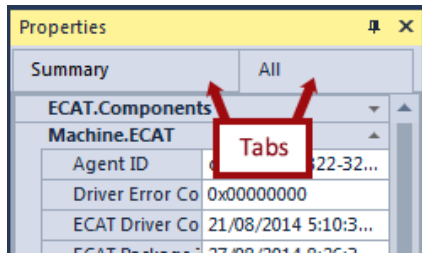
- **Property Pane:** Property panes are common on the user interface. They are made up of two tabs namely:
 - **Summary:** Displays properties that are of interest.
 - **All:** Displays all properties for the selected item.



- **Filtering Pane:** Provides a variety of filtering options. It consists of two tabs namely:
 - **Faceted:** Provides a variety of preset, and instant filtering options.
 - **Advanced:** Is for advanced users who wish to have additional control over the filter options.

Tabs

Tabs are available in panes and windows and each tab provides different information and options. Click the tab to make it active.



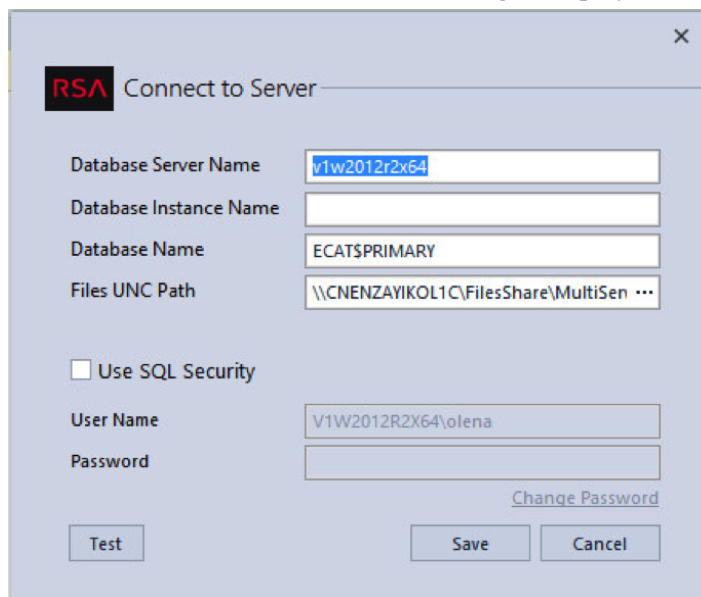
Access the NetWitness Endpoint UI

This topic provides information about opening the NetWitness Endpoint User Interface (UI) and related tasks.

Open the NetWitness Endpoint UI

To connect to the console and open the NetWitness Endpoint UI:

1. Select **Start > All Programs > NetWitness Endpoint > NetWitness Endpoint UI** to run the NetWitness Endpoint UI.
2. If you have previously connected to the NetWitness Endpoint database with this installation, the NetWitness Endpoint UI will automatically reconnect every time you open NetWitness Endpoint UI. Only if this is the first time the NetWitness Endpoint UI was opened for this installation, the **Connect to Server** dialog is displayed.



Note: NetWitness Endpoint supports multiple UI instances on the same machine connecting to a single or multiple servers, with both Windows and SQL credentials. When launching the UI, if no other UI instance is running, the new instance automatically connects to the previously connected server with Windows credentials. However, if another instance of the UI is already running, the Connect to Server dialog will display. However, on the same machine, only one UI instance can be established for each single set of credentials. If a user attempts to connect with credentials currently in use on the same machine, the following Connection error message will display: "There is already a UI instance opened with the same connection values."

3. To complete the Connect to Server dialog, refer to the table below:

Dialog Field	Description
Database Server Name	Name of the machine running the SQL Server.
Database Instance Name	Name of the SQL Server instance (if it was named, otherwise leave this blank).
Database Name	Name of the database used by NetWitness Endpoint. This was entered during installation, and the database automatically generated on the SQL Server. If you need to look up the name, select Start > All Programs > Microsoft SQL Server 2012 > SQL Server Management Studio , and look under Databases .
Files UNC Path	The path name for the folder where agents will upload files. (It must be a shared network folder for a multi-server environment.)
Use SQL Security	Check this if you want to use SQL Security instead of Windows authentication, and enter your user name and password. If you need to reset your password, click the Change Password link. On the Change SQL Password dialog, enter your current password, enter a new password, and click Change .

Note: OPSWAT does not support UNC file path. Hence, it is recommended to use a non-UNC file path for OPSWAT scan. If you choose to use UNC file path for OPSWAT scan, you must mount the share on the file system as a symbolic link. For more information, see <https://my.opswat.com/hc/en-us/articles/202371520-How-do-I-scan-mapped-drives-with-Metascan->.

Reconfigure the NetWitness Endpoint UI

If you are not opening the NetWitness Endpoint UI for the first time, you get connected to the database automatically. But, you can still reconfigure the connection settings manually, at any time.

To Reconfigure the NetWitness Endpoint UI:

1. Select **Configure > Connection** from the **Top Menu**.
2. Update the **Configuration** dialog and click **Save**.

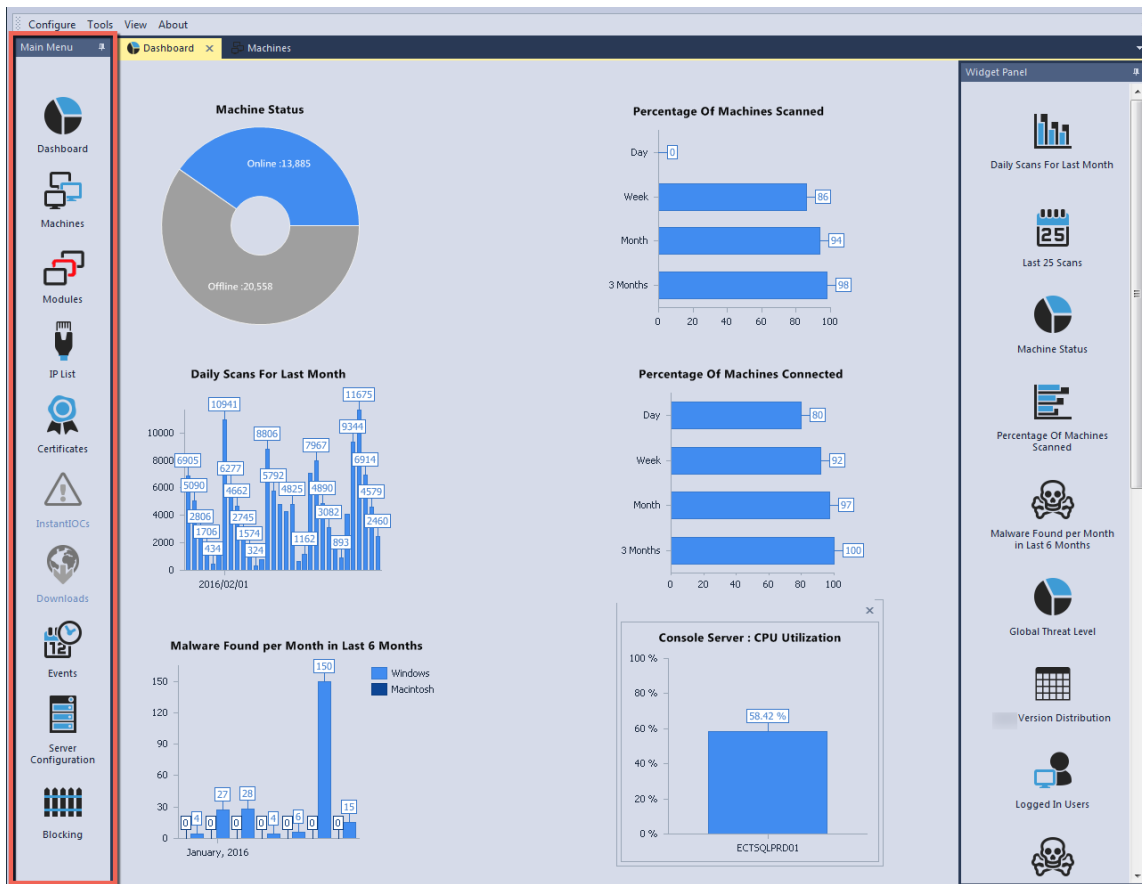
To exit the NetWitness Endpoint UI:

Click the close box in the upper right-hand corner of the NetWitness Endpoint UI window.

NetWitness Endpoint Environment

Main Menu

This topic provides detailed information about the Main Menu options available in the NetWitness Endpoint UI. When opening the NetWitness Endpoint UI, the NetWitness Endpoint Main Menu displays down the left side, and the Dashboard displays in the Main Window, as shown in the following figure.



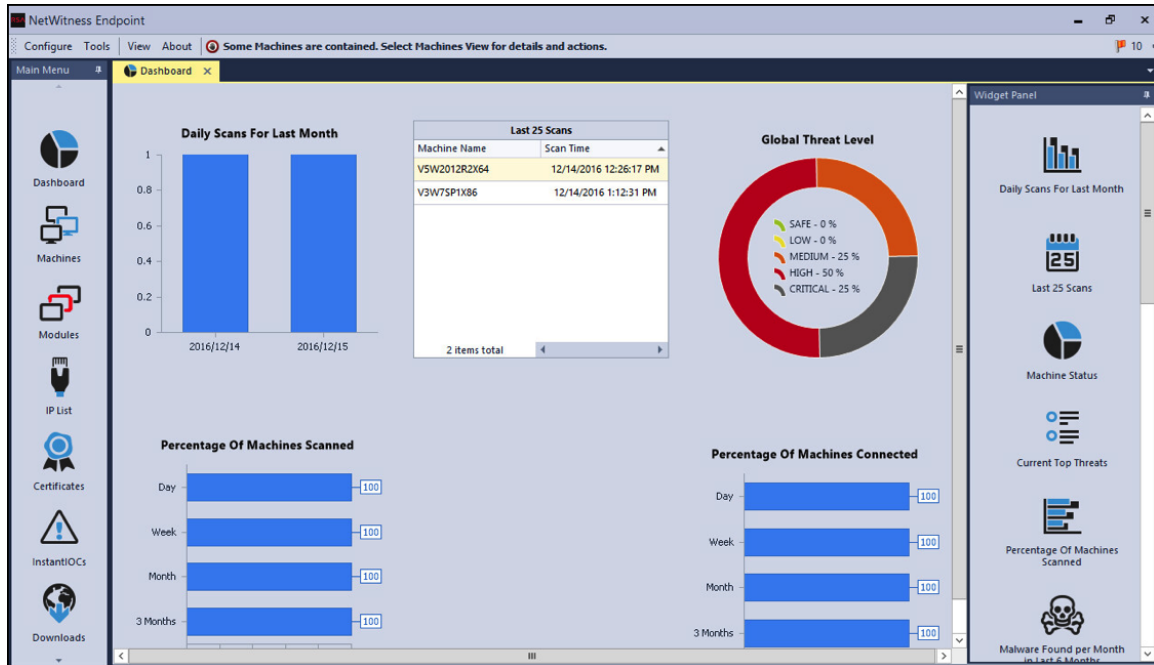
Selecting an option from the Main Menu changes the display accordingly in the NetWitness Endpoint main window. The options are:

- [Dashboard Window](#)
- [Machines Window](#), from which you can then access the [Machine View](#) for a selected machine
- [Modules Window](#)
- [IP List Window](#)
- [Certificates Window](#)
- [InstantIOCs Window](#)
- [Downloads Window](#)
- [Events Window](#)
- [Server Configuration Window](#)
- [Blocking Window](#)

Dashboard Window

The Dashboard window is a customizable workspace that lets you track NetWitness Endpoint agent activities and data at a glance.

To open the Dashboard, click **Dashboard** in the **Main Menu**. The Dashboard window is displayed as shown in the following figure.



Using the **Widget Pane**, you can design your Dashboard to give you the information that you want to access quickly. You can drag and drop the widgets to the desired location or close widgets by clicking the **X** in the top right corner of the widget.

Widgets include:

- Daily Scans For Last Month
- Last 25 Scans
- Machine Status
- Current Top Threats
- Percentage Of Machines Scanned
- Malware Found per Month in Last 6 Months
- Global Threat Level
- NetWitness Endpoint Version Distribution
- Logged In Users

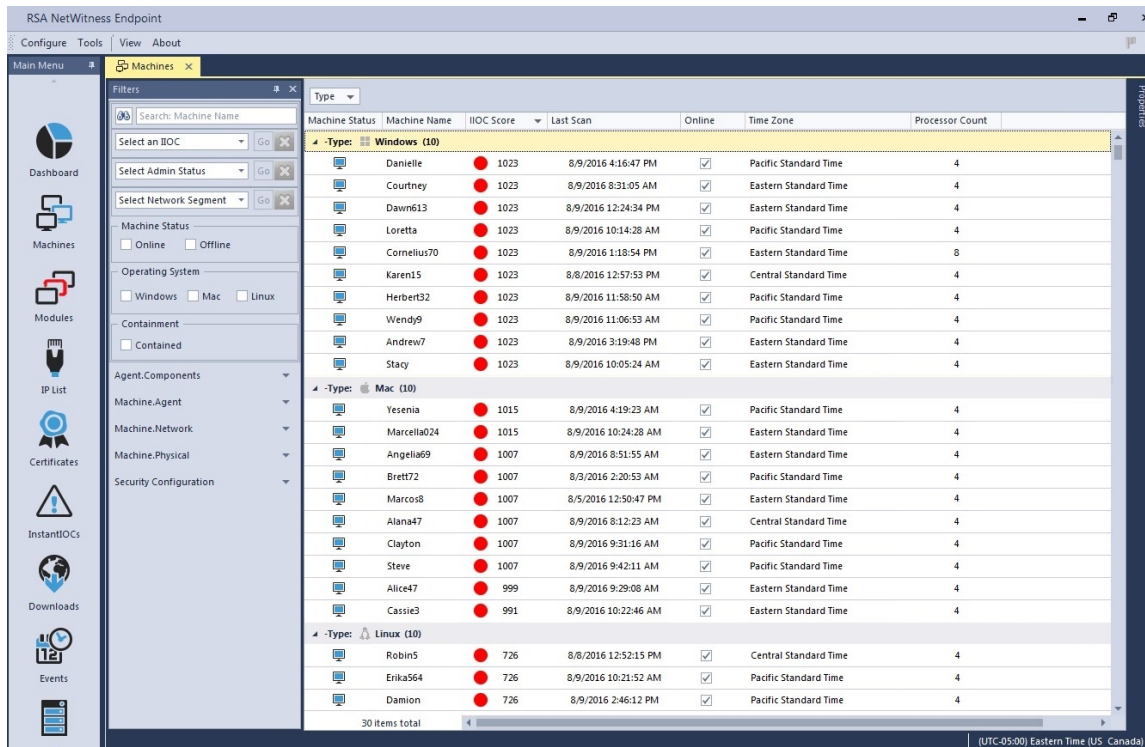
- Last 25 Malware Found
- Top 5 Malware Hunters In the Last 6 Months
- Percentage Of Machines Connected
- ConsoleServer: CPU Utilization
- ConsoleServer Memory Utilization
- ConsoleServer: Free Disk Space
- ConsoleServer: Agent Counts
- NetWitness Endpoint icon
- High Risk Score Modules

Machines Window

The **Machines** window contains the list of all computers with an NetWitness Endpoint agent.

Note: Click **Tools > Refresh** or press F5 to refresh the Machines list when you need the latest data.

To open Machines, click **Machines** in the **Main Menu**. The **Machines** window is displayed as shown in the following figure.



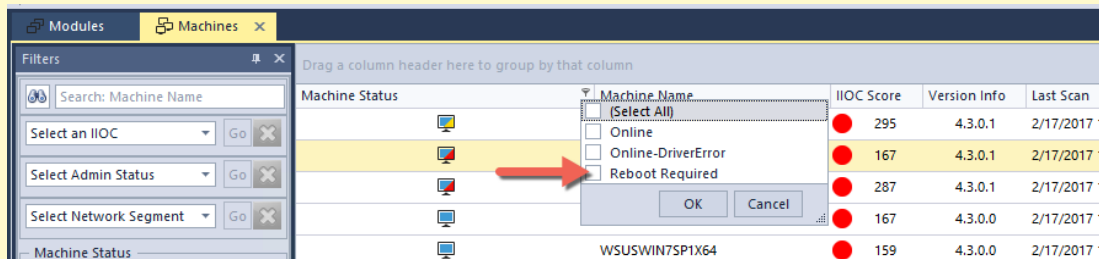
The **Machines** window is made up of the Machines table and a number of panes that allow you to filter and view more information about the machines.

Caution: When the Machines table first loads, if any NetWitness Endpoint agents are currently in the driver error 0x20010007 state, the following message will be displayed:



You must reboot the affected machines to ensure agents are collecting complete data, as follows:

1. In the Machines table, select to filter the Machine Status column by **Reboot Required**, as shown below:



2. Select all machines that match that status (these machines will all have this machine status icon:).

3. Right-click and select **Advanced > Reboot...**

For more information on rebooting machines, see [Reboot a Machine](#).

Machines Table

Note: For more information about configuring and customizing tables, see the topic [Tables in Main Window](#).

There are a number of actions available by right-clicking an entry:

- **Open:** Opens a machine in a new tab with a more detailed view. For more details see [Machine View](#).
- **Request Scan:** Starts a scan on the machine.
- **Cancel Scan:** Cancels an ongoing scan.
- **Modify Status:** Modifies the status of the machine.

- **Modify Comment:** Modifies the user's comment associated with the machine in the NetWitness Endpoint UI.
- **Containment:** Provides options to start or stop the machine containment feature for the selected machine. For more information, see [Use Machine Containment](#), and [Turn Containment On or Off](#).
- **Blocking System:** Provides options to enable or disable the blocking status. For more information, see [Use the Blocking System](#).
- **Configuration Group > Add Machine to Group:** Provides options for adding the machine to a configuration group.

Note: Configuration groups are useful for scan scheduling, alerting, and other processes.

- **Configuration Group > Remove from Group:** Provides options for removing the machine from a configuration group.
- **Forensics > Request File(s):** Uploads files from the machine to the NetWitness Endpoint server. Enter the full path on the machine from where files have to be uploaded.
- **Forensics > Request MFT:** Requests the Master File Table (MFT).

Note: Request MFT is not currently supported for Mac machines.

- **Forensics > Request Memory Dump.** Requests a full memory dump. For more information, see [Perform a Full Memory Dump](#).

Note: Request Memory Dump is not currently supported for Mac machines.

- **Agent Maintenance > Update Agent:** Updates the agent to the latest version.
- **Agent Maintenance > Uninstall Agent:** Uninstalls the agent but does not remove it from the database.
- **Agent Maintenance > Change Server:** Provides an option to change the console server in case of multi-server environment.
- **Advanced > Reboot:** Reboots the client machine at the scheduled time.
- **Advanced > Remove Selection from the Database:** Removes the selection from the database but does not uninstall the agent.

Note: Agent Maintenance options are not available if the machine is currently under containment.

The Machines table includes the following default column headings.

Note: There are a variety of columns you can choose to display using the Column Chooser function. For more information about configuring and customizing tables, see the topic *Tables* in [Main Window](#).

Column	Description
Machine Status	Status of the machine. For more information, see Agent Status Icons . By default, NetWitness Endpoint queries the database for updates to machine status every 30 seconds. To disable this function, in the Top Menu click View and select Disable Machine Status Auto-Refresh . The function can be enabled again using the same process (when disabled, the menu option changes to Enable Machine Status Auto-Refresh).
IIOC Score	The Machine IIOC Score indicates the likelihood that the behavior described in the IIOC was found. Higher scores also denote a greater probability of malicious intent. Also provides a color (green, yellow, orange, red or black) that represents the severity of the threat found in the machine. For more information, see Levels of IIOCs, IIOC Scores, and Risk Score
Operating System	Specifies whether the agent is using Windows, Mac, or Linux OS.
Containment Status	Specifies whether or not the machine is currently under containment. For more information, see Use Machine Containment .
Containment Supported	Indicates whether machine containment is supported for the machine. For more information, see Supported Machines for Containment .
Admin Status	The status of the machine. It could be Infected, None, Skipped, Test, Verified, or Under Investigation. It could also be a custom status.
Comment	Any comment entered for the machine.
NetWitness Endpoint Version	Indicates the version of NetWitness Endpoint running on the agent.


Column	Description
Last Scan	Indicates the last time the machine submitted data to the server.
User Name	The username that was logged in on the agent when the scan started or when the agent was installed.
Online	The box is checked if the machine is online.

Machine Panes


Note: For more information about configuring and customizing panes, see the topic *Panes in Main Window*.

The Machines window has two panes to filter the machines or access more data:

- **Properties** allows you to view properties of a selected machine and offers two tabs (Summary/All).

Properties Pane	Description
 <p>The screenshot shows the Properties Pane with the Summary tab selected. The properties are organized into three sections: Machine.Agent, Machine.Network, and Machine.OperatingSystem. The Machine.Agent section includes details like Agent ID, Blocking Active, and various timestamps. Machine.Network shows DNS, Gateway, and IP addresses. Machine.OperatingSystem provides information on boot time, country, domain role, and OS details.</p>	<p>The Summary tab displays the most important properties. The All tab displays all the properties for the machine.</p> <p>The properties are divided according to category and provide pertinent details about:</p> <ul style="list-style-type: none"> • The NetWitness Endpoint agent currently installed on the machine • Network information • The machine operating system

- **Filters** allows you to filter the machines in the list according to a variety of parameters.

Filters Pane	Option	Description
	Search: Machine Name	Filters the list according to the criteria entered.
	Select an IIOC	Use the drop-down menu to select an IIOC to filter the list.
	Select Admin Status	Use the drop-down menu to select an admin status to filter the list.
	Select Network Segment	Use the drop-down menu to select a network segment to filter the list.
	Machine Status	Filters the list according to whether a machine is offline or online.
	Operating System	Filters the list according to the selected operating system.
	Containment	Filters the list to show machines currently under containment.
	Additional Options	Click the down arrow next to a category to view subcategories for additional options to select to refine the list of machines.

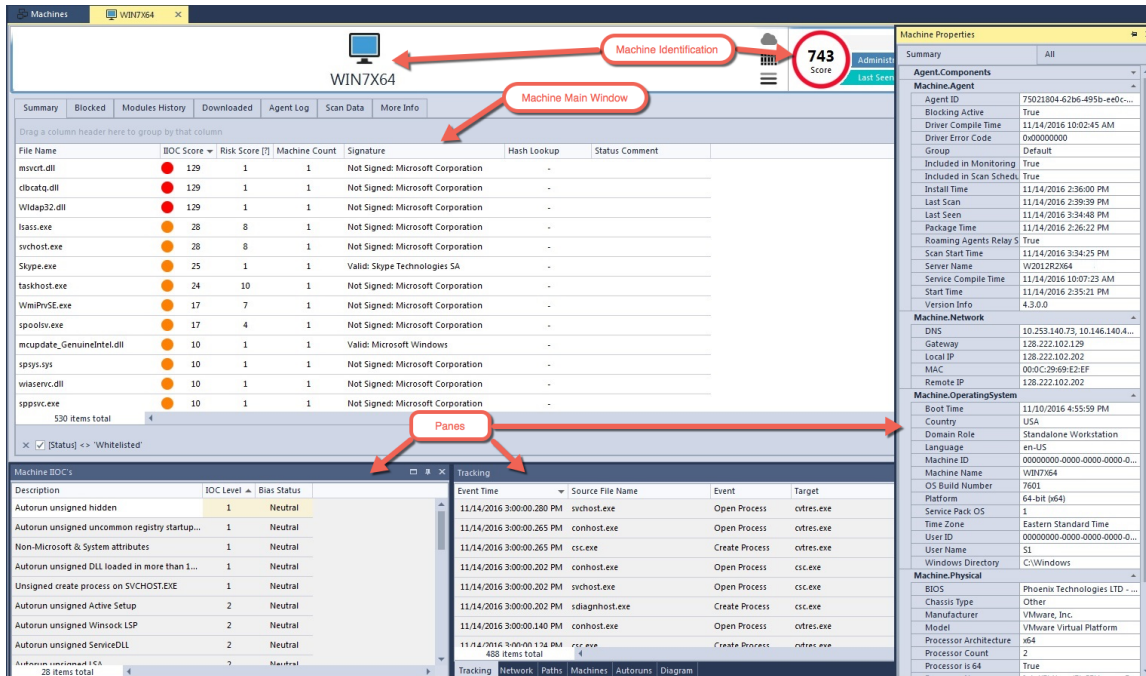
Machine View

The Machine View provides a variety of information for a selected machine within the NetWitness Endpoint environment. There is basic identification and history information, as well as detailed scan results information to aid in investigation. After a scan is complete, you can open the machine to display its list of modules and related information.

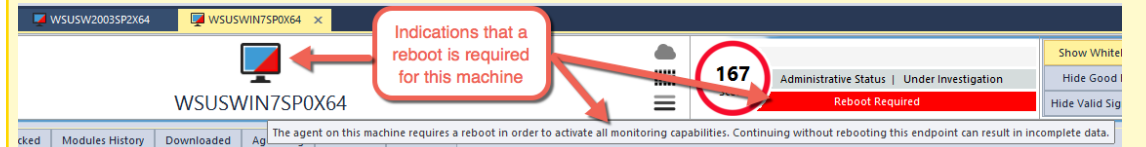
To open a machine, locate the machine in the Machines Table and do one of the following:

- Double-click the machine.
- Right-click the machine and select **Open**.


The following figure shows the Machine window for a selected machine.



Caution: If the current machine is in the driver error 0x20010007 state, its machine identification (at the top of the window) will appear as follows:



To ensure all monitoring capabilities are active, you must reboot this machine as follows:

1. Click the menu  icon. A list of available actions is displayed.
2. Select **Advanced > Reboot...**

For more details on rebooting a machine, see [Reboot a Machine](#).

The **Machine** window consists of the following sections:

- **Machine Identification:** provides key information about the machine.
- **Machine Main Window:** provides information according to the active tab. There are seven tabs for a Windows machine (Summary, Blocked, Module History, Downloaded, Agent Log, Scan Data, and More Info), five tabs for a Linux machine (Summary, Downloaded, Agent Log, Scan Data, and More Info), and four tabs for a Mac machine (Summary, Downloaded, Agent Log, and Scan Data).
- **Panes:** provide sorting and filtering options and additional information.

Machine Identification

The **Machine Identification** section is at the top of the Machine window. It contains basic information about the machine, including computer name, administrative status, score, when it was last seen, and any comment made in the record. At the right of the Machine Identification section are quick filters.



If the machine is currently under containment, the containment indicator will also display in this section, as shown below.



Moving the cursor over the containment indicator displays a tooltip that describes the status as one of the following: Containment Pending, Containment Enforced, or Releasing Containment. Clicking the indicator will release the machine from containment. For more information, see [Use Machine Containment](#).

Machine Main Window

The **Machine Main Window** organizes the machine's modules and related information in the following tabs:

- **Summary:** provides a summary by listing the most important modules scanned.
- **Blocked:** displays a list of modules that are blocked/quarantined. Supported for Windows agents only.
- **Module History:** displays a table containing the list of modules and module paths that are marked as deleted for a specific system. Supported for Windows agents only.
- **Downloaded:** provides a list of modules downloaded from the agent.
- **Agent Log:** displays all NetWitness Endpoint events related to the agent, such as requests for scans or file downloads.
- **Scan Data:** provides more complete information on scanned data, divided into categories and category groups.
- **More Info:** provides additional information such as identities of administrators and users connected to the machine, shared resources and so on.

Each tab organizes information in tables, including a main list of items and numerous panes that display information about whatever item is selected in the main list. Typically, a **Properties** pane will display the values of various properties of whatever is selected in the main list.

For example, one might navigate to the **Summary** tab to see a list of important modules. The default columns will include certain default properties of the file, such as filename, threat level, score, and so on. If a particular module is selected, the **Properties** pane will then display its properties. The default columns in the Modules list can be customized to include any of the available properties.

Note: For more information about configuring and customizing tables and panes, see the topics *Tables* and *Panes* in [Main Window](#).

Summary, Downloaded, and Scan Data Tabs

These three tabs contain information about modules and other scanned data found on the machine. The **Machine Main Window** contains the Modules List. The panes provide further information about the machine or a module, depending on whether the machine or a module is selected.

For Scan Data, there is also a Category List to the left of the Modules List, which organizes all the scanned data into categories, further organized into a small number of category groups. The Modules List in this case may also contain, for some categories, other kinds of scanned data, such as processes, network connections, and so on. For a description of all the category groups and categories for Windows, Mac OS-X, and Linux machines, see [Scan Categories](#).

Modules List

Note: There are a variety of columns you can choose to display using the Column Chooser function. For more information about configuring and customizing tables, see the topic *Tables* in [Main Window](#).

The default column headers for the list of modules may include.

Column	Description
IIOC Score	The Machine IIOC Score provides a level of confidence that the behavior described in the IIOC was found. Higher scores also denote a greater probability of malicious intent. Also provides a color (green, yellow, orange, red or black) that represents the severity of the threat found in the machine. For more information, see Levels of IIOCs, IIOC Scores, and Risk Score .
Module Count	The number of machines to which the IP connected.

Column	Description
Signature	Indicates the presence or absence, validity and source of the signature of this module. <div style="border: 1px solid green; padding: 5px; background-color: #e0f0e0;"> <p>Note: In NetWitness Endpoint, all signature information is obtained by a low-level system designed to avoid any malware signature verification bypassing techniques.</p> </div>
Hash Lookup	The classification of the module, based on its hash, from one or more databases.
Status Comment	Any comment entered for the machine.
Risk Score	A data-driven score that ranges from 0 to 100. This score is the output of a machine-learning algorithm and represents the probability of the module being malicious. For more information, see Levels of IIOCs, IIOC Scores, and Risk Score .
Compile Time	Tells when the module was compiled.
MD5	The file's hash thumbprint calculated by the MD5 algorithm.
Launch Arguments	The Command line arguments passed to the module when it is launched.

Right-clicking a module may provide various options, such as:

- **Edit Blacklist-Whitelist Status:** Edit the Blacklist or Whitelist status of the selected module.
- **List Computers with Module:** List the computers on which the module is found.
- **Download to Server:** Download the selected module to the server.
- **Analyze Module:** Opens an Analyze Module window that contains various information about the module.
- **Malware Analysis:** Allows you to forward the file to Malware Analytics for further analysis and investigation. For more information about Forward to Malware Analytics, see [Forward to Malware Analysis](#).
- **Search with Google > Filename:** Performs a search of the module filename using Google.

- **Search with Google > MD5:** Performs a search of the module MD5 using Google.
- **Search with Google > SHA1:** Performs a search of the module SHA1 using Google.
- **Search with Google > SHA256:** Performs a search of the module SHA256 using Google.
- **Search with VirusTotalSearch > MD5:** Performs a search of the module MD5 using VirusTotalSearch.
- **Search with VirusTotalSearch > SHA1:** Performs a search of the module SHA1 using VirusTotalSearch.
- **Search with VirusTotalSearch > SHA256:** Performs a search of the module SHA256 using VirusTotalSearch.
- **Open in a Separate View:** Opens the module in a new tab.
- **Dump Full Process Memory:** Available for Windows machines when right-clicking on a process; stores the process memory dump on the agent machine temporarily before being transferred automatically to the server. The memory snapshots are stored on the NetWitness Endpoint Server under the `Server\Files\Machines\<Client-Name>\<Client-Name_Date-Taken>.raw` subdirectory. Note that the process memory dump may take a fair amount of disk space and also may fail if the agent system goes offline/asleep during the request or if the agent kernel driver fails to load.
- **View Certificate:** Opens the Certificates window.
- **Download to Server:** Download the selected module to the server.
- **Scan with YARA.**
- **Scan with OPSWAT.**
- **Scan with OPSWAT and YARA.**

Summary, Downloaded, and Scan Data Panes

When the machine is selected, these panes provide data related to the machine. When a module is selected, the panes provide additional information about the selected module.

Note: For more information about configuring and customizing panes, see the topic *Panes* in [Main Window](#).

There are a number of pane options, even though some panes are initially seen as tabs. There are two kinds of panes:

- **Machine Panes.** These panes are active when the machine is selected.

Pane	Description
Machine InstantIOCs	Provides information about InstantIOCs triggered by the machine.
Network	Provides information about the machine network activity.
Autoruns	Lists all modules automatically started at boot time, login time, or execution time. Any of these techniques could be used to auto-start malware.
Tracking	Displays the results of the NetWitness Endpoint Behavior Tracking system. For more information, see the topic <i>Full Monitoring and Tracking</i> in Tracking Systems .
Machine Properties	Provides information about the properties of the machine. <div style="border: 1px solid green; padding: 5px; margin-top: 10px;"> <p>Note: For Linux machines, if the dmidecoder package is not present (as a result of installing the Minimal version of the OS), a few machine properties (Machine.Physical > Manufacturer, Model, and Serial) may display as "Unknown."</p> </div>

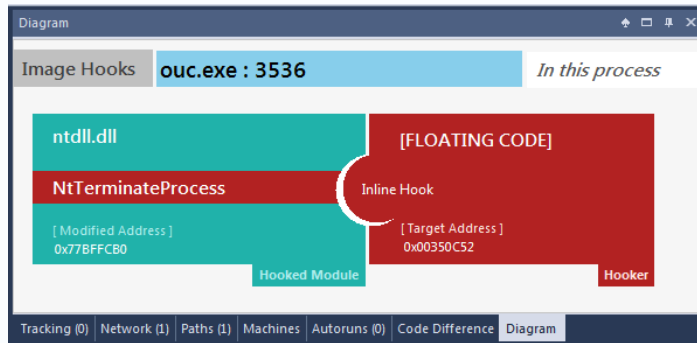
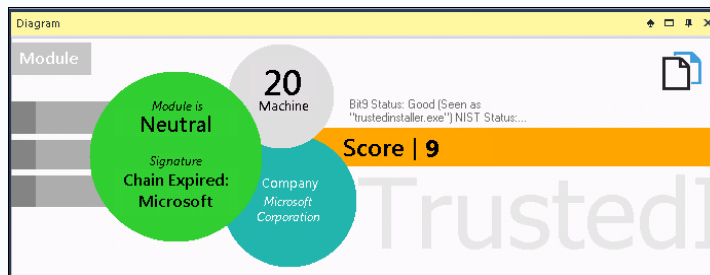
- **Module Panes.** These panes are active when a module is selected.

Pane	Description
Module InstantIOCs	Provides information about InstantIOCs triggered by the module.
Machines	Lists the machines on which a module is found.
Paths	Lists the path or paths for the module.
Autoruns	Lists all modules automatically started at boot time, login time, or execution time. Any of these techniques could be used to auto-start malware.
Tracking	Displays the results of the NetWitness Endpoint Behavior Tracking system. For more information, see the topic <i>Full Monitoring and Tracking</i> in Tracking Systems .

Pane	Description
Code Difference	<p>The Code Difference pane (found in the Machine View, in the More Info tab) highlights the difference between the original code and hooked code. For more information, see the figure below.</p>

Diagram

Displays the graphical representation of the Machines/Modules/Hooks as shown below:



Pane	Description
Module Properties	Provides information about the properties of the selected module.

Blocked Tab

The **Blocked** tab displays the list of modules that are blocked or quarantined and is supported for Windows agents only. The **Blocked** tab consists of the following two tabs:

- **Quarantined:** displays the list of modules that are quarantined for a particular machine.
- **History:** displays the history of the blocked files as well as quarantined files for a particular machine.

The blocked list includes the following default column headings:

Note: There are a variety of columns you can choose to display using the Column Chooser function. For more information about configuring and customizing tables, see the topic *Tables* in [Main Window](#).

Column	Description
--------	-------------

Quarantined

Date Blocked	The date when the module was blocked.
IIOC Score	The IIOC score provides an estimate of the severity of the behavior found in the machine. The higher the number, the more likely the computer is compromised. Also provides a color (green, yellow, orange, red or black) that represents the severity of the threat found in the machine. For more information, see Levels of IIOCs, IIOC Scores, and Risk Score .
Machine Count	The number of machines on which the blocked module was found.

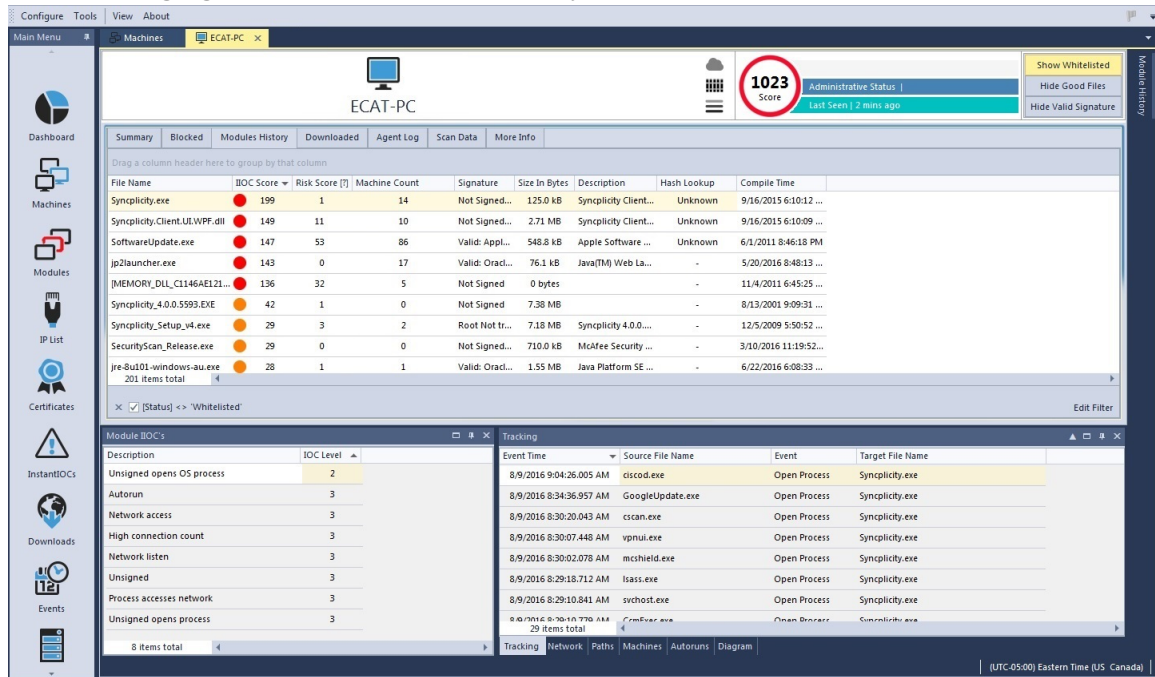
Column	Description
Signature	Indicates the presence or absence, validity, and source of the signature of this module. <div style="border: 1px solid green; padding: 5px; background-color: #e0f0e0;"> <p>Note: In NetWitness Endpoint, all signature information is obtained by a low-level system designed to avoid any malware signature verification bypassing techniques.</p> </div>
Hash Loop	The classification of the module, based on its hash, from one or more databases.
Status Comment	Any comment entered for the machine.
History	
Event Time	The time the event was initiated.
Event	The name of the blocking event (blocked, quarantined).
Event Type	The type of event.
Target Path	The path of the target file.
Target Filename	The name of the target file.
Status	The status of the module before using the remediation action.

For more information about Blocking System and using the Blocked tab, see [Blocking System](#).

Modules History Tab

The **Modules History** tab displays a table containing the list of modules and module paths that are marked as deleted for a specific system. These are the modules that are currently not active or not in use. The Modules History tab is supported only for Windows agents.

The following figure shows the Modules History tab:



The Modules History tab includes the following default column headings:

Note: There are a variety of columns you can choose to display using the Column Chooser function. For more information about configuring and customizing tables, see the topic *Tables* in [Main Window](#).

Column	Description
IIOC Score	The IIOC score provides an estimate of the severity of the behavior found in the machine. The higher the number, the more likely the computer is compromised.
Machine Count	The number of machines to which the IP connected.
Signature	Indicates the presence or absence, validity, and source of the signature of this module.
Size In Bytes	The size of the module in bytes.
Description	Describes the type of module.

Column	Description
Hash Lookup	The classification of the module, based on its hash, from one or more databases.
Compile Time	Tells when the module was compiled.

Agent Log Tab

The **Agent Log** tab displays all events related to the agent, such as requests for scans, file downloads, blocking status, kernel updates, and so on.

More Info Tab

The **More Info** tab, available only for Windows and Linux agents, provides further information about various aspects of the machine, organized into categories, including:

Windows Machine Categories	Linux Machine Categories
Current Users	Current Users
Network Shares	Mounted Paths
Security Products	Bash History
Windows Patches	Network Interfaces

A number of panes allow you to view more details.

Note: For more information about configuring and customizing panes, see the topic *Panels* in [Main Window](#).

More Info List

When a category is selected on the left, additional information is displayed in columns in the More Info list to the right of the Category list. The categories and corresponding columns vary depending on the machine OS, as defined in the following tables.

Note: There are a variety of columns you can choose to display using the Column Chooser function. For more information about configuring and customizing tables, see the topic *Tables* in [Main Window](#).

The More Info list column headings for Windows machines may include:

Category	Column	Description
Current Users	Groups	Groups this user belongs to.
	Is Administrator	Checkbox is checked if the user is an administrator.
Network Shares	Net Name	Network name of the shared resource.
	Path	Pathname of shared directory.

The More Info list column headings for Linux machines may include:

Category	Column	Description
Current Users	User Name	User name of currently logged in user
	Host	Host from which the connection was made
	Home	Home directory of user
Mounted Paths	Mounted Path	Directory mounted on
	File System	Type of file system
	Remote Path	Device or server for file system
Bash History	User	User who ran command
	Command	The actual command run
Network Interfaces	Local IP	IP address of the interface
	Mac Address	Mac address for interface
	Interface Name	Name of the interface
	Mask	Netmask of the interface
	Gateway	Gateway for the interface

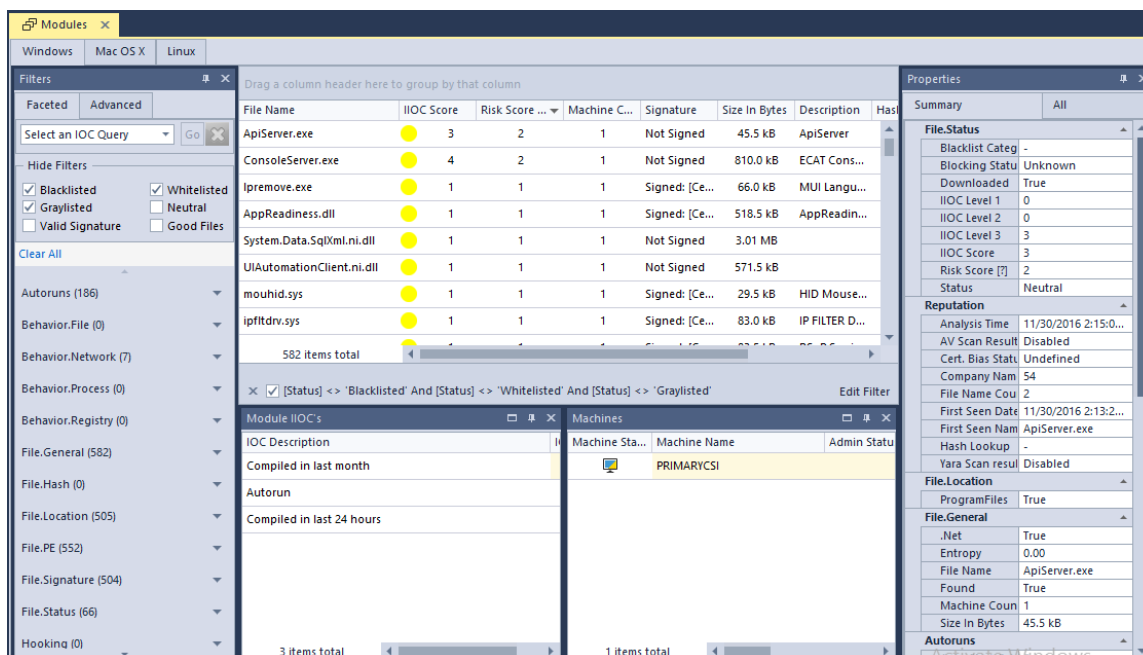
More Info Panes

In addition to the Category and More Info list panes, other panes (at the bottom of the More Info Tab window) may display a variety of information about the selected machine, such as Machine IIOCs.

Modules Window

The **Modules** window displays a table containing all modules and the relevant information for all assessed agents. Modules could be present on different machines, but they will appear only once in the list. Modules are listed under three main tabs: **Windows**, **Mac OS X**, and **Linux**, sorted by Risk Score.

To view Modules, click **Modules** in the **Main Menu**. The **Modules** window is displayed as shown in the following figure.



The **Modules** window is made up of a Modules table and three panes.

Modules Table

Note: For more information about configuring and customizing tables, see the topic [Tables in Main Window](#).

There are a number of actions available by right-clicking an entry:

- **Edit Blacklist-Whitelist Status:** Edit the Blacklist or Whitelist status of the selected module.
- **List Computers with Module:** List the computers on which the module is found.

- **Download to Server:** Download the selected module to the server.
- **Save Local Copy:** Save a local copy of the module.
- **Scan with YARA:** Scans the module with YARA.
- **Analyze Module:** Opens an **Analyze Module** window that contains various information about the module.
- **Malware Analysis:** Allows you to forward the file to Malware Analysis for further investigation. For more information, see [Forward to Malware Analysis](#).
- **Search with Google > Filename:** Performs a search of the module filename using Google.
- **Search with Google > MD5:** Performs a search of the module MD5 using Google.
- **Search with Google > SHA1:** Performs a search of the module SHA1 using Google.
- **Search with Google > SHA256:** Performs a search of the module SHA256 using Google.
- **Search with VirusTotalSearch > MD5:** Performs a search of the module MD5 using VirusTotalSearch.
- **Search with VirusTotalSearch > SHA1:** Performs a search of the module SHA1 using VirusTotalSearch.
- **Search with VirusTotalSearch > SHA256:** Performs a search of the module SHA256 using VirusTotalSearch.
- **Open in a Separate View:** Opens the module in a new tab.
- **View Certificate:** Opens the Certificates window.
- **Copy:** Copies the module.

The Modules table includes the following default column headings.

Note: There are a variety of columns you can choose to display using the Column Chooser function. For more information about configuring and customizing tables, see the topic *Tables* in [Main Menu](#).

Column	Description
IIOC Score	The Machine IIOC Score provides a level of confidence that the behavior described in the IIOC was found. Higher scores also denote a greater probability of malicious intent. Also provides a color (green, yellow, orange, red or black) that represents the severity of the threat found in the machine. For more information, see Levels of IIOCs, IIOC Scores, and Risk Score .

Column	Description
Machine Count	Indicates the number of different machines where this module was found. If a module is present on all machines, it may be present on the original installation image, or has been intentionally widely deployed. If a module is only present on one agent, and a thousand agents are checked, it is likely that this module is suspicious and requires more investigation.
Signature	Indicates the presence or absence, validity and source of the signature of this module. Note: In NetWitness Endpoint, all signature information is obtained by a low-level system designed to avoid any malware signature verification bypassing techniques.
Description	Describes the type of module.
Hash Lookup	The classification of the module, based on its hash, when checked against one or more databases.
Risk Score	A data-driven score that ranges from 0 to 100. This score is the output of a machine-learning algorithm and represents the probability of the module being malicious. For more information, see Levels of IIOCs, IIOC Scores, and Risk Score .
Compile Time	Indicates when the module was compiled.
Automatic Bias Status Assignment	Indicates if the module has been automatically assigned a bias status. For more information, see Automatic Status Assignment .

Modules Panes

Note: For more information about configuring and customizing panes, see the topic [Panels in Main Window](#).

The Modules window has four panes to access information or filter the data:

- **Properties** provides information about the properties of a selected module.
- **Module IIOCs** provides information about the InstantIIOCs that were detected against the module and the module's reputation. There is also space for comments.

- **Machines** provides a list of machines that contain a selected module.
 - **Filters** allows you to apply a variety of filters to the modules. It has two tabs, Faceted and Advanced:
 - **Faceted** provides a variety of preset, instant filtering options.
 - **Advanced** is for advanced users who wish to have additional control over the filter options.
- For more information about using filters to sort modules, see [Use Filters to Find Malware](#).

IP List Window

The IP List window displays the complete list of IP/Ports/Protocols entries present in the scan reports under a unique list. The data is aggregated to include the total or sum of each column for the whole environment.

To open the IP List, click **IP List** in the **Main Menu**. The **IP List** window is displayed as shown in the following figure.

IP	Port	Protocol	Domains	Machine Count	Module Count	First Activity	Last Activity
104.16.57.15	443	TCP		1	1	5/8/2015 5:46:42 PM	5/8/2015 5:46:42 P...
104.69.245.206	80	TCP		1	1	5/8/2015 5:46:42 PM	5/8/2015 5:46:42 P...
128.222.70.238	28131	TCP		1	1	5/8/2015 5:46:42 PM	5/13/2015 11:31:2...
128.222.77.177	49155	TCP		1	1	5/8/2015 5:46:42 PM	5/8/2015 5:46:42 P...
128.222.78.12	49155	TCP		1	2	5/11/2015 12:15:44 ...	5/13/2015 11:31:2...
173.194.117.30	443	TCP		1	1	5/8/2015 5:46:42 PM	5/8/2015 5:46:42 P...
173.194.117.66	443	TCP		1	1	5/13/2015 11:31:20 ...	5/13/2015 11:31:2...
173.194.117.69	443	TCP		1	1	5/11/2015 12:15:44 ...	5/11/2015 12:15:4...
173.194.117.72	443	TCP		1	1	5/13/2015 11:31:20 ...	5/13/2015 11:31:2...
173.194.117.78	443	TCP		1	1	5/12/2015 12:45:52 ...	5/12/2015 12:45:5...
173.194.117.82	443	TCP		1	1	5/13/2015 11:31:20 ...	5/13/2015 11:31:2...
173.194.117.86	443	TCP		1	1	5/11/2015 12:15:44 ...	5/12/2015 12:45:5...
173.194.117.87	80	TCP		1	1	5/11/2015 12:15:44 ...	5/11/2015 12:15:4...
173.194.38.169	80	TCP		1	1	5/8/2015 5:46:42 PM	5/8/2015 5:46:42 P...
173.194.38.175	80	TCP		1	1	5/8/2015 5:46:42 PM	5/8/2015 5:46:42 P...
173.194.38.176	80	TCP		1	1	5/8/2015 5:46:42 PM	5/8/2015 5:46:42 P...
173.194.38.181	443	TCP		1	1	5/8/2015 5:46:42 PM	5/8/2015 5:46:42 P...

63 items total

Filter: [Private Address] = 'False' And [LastActivity] >= '5/7/2015 5:30:00 AM'

Properties

Behavior.Network

- Burst Count: 0
- Burst Interval Deviation: 0
- Burst Interval Mean: 0
- Fail Connect Count: 0
- First Activity: 5/8/2015 5:46:42 PM
- IP: 104.69.245.206
- Last Activity: 5/8/2015 5:46:42 PM
- Network Segment: 104.69.245.0
- Port: 80
- Private Address: False
- Total Received: 0 bytes
- Total Sent: 0 bytes
- Trusted Domain: False

General

- Bad Domain: False
- Bad IP: False
- Connection Count: 1
- Domains: 1
- IPV6: 1
- Machine Count: 1
- Module Count: 1
- Protocol: TCP

The **IP List** window is made up of an **IP List** table and a **Properties** pane.

IP List Table

Note: For more information about configuring and customizing tables, see the topic [Tables in Main Window](#).

There are a number of actions available by right-clicking an entry:

- **List Computers with IP Address:** Opens a new tab that contains a list of computers with the selected IP address.

- **Add to Trusted Domains:** Adds the IP address to trusted domains.
- **Edit Trusted Domains:** Opens the **Trusted Domains** dialog in which you can manage trusted domains.
- **Investigate Destination IP with NetWitness:** Investigates the IP address using NetWitness v9.7.
- **Open in NetWitness Investigate:** Analyzes the IP address using RSA NetWitness Suite.
 - If you choose this option, the **NetWitness Investigate** window opens as shown below:

Note: The option **Open in NetWitness Investigate** is available only if you have configured RSA NetWitness Suite through the Monitoring and External Components feature.

- Click the checkboxes to enable or disable the field.
- To edit the query manually, click the URI checkbox and edit the field.
- Click **Investigate**. The selected IP address is further investigated using NetWitness Suite.

The IP List table includes the following default column headings.

Note: There are a variety of columns you can choose to display using the Column Chooser function. For more information about configuring and customizing tables, see the topic *Tables* in [Main Window](#).

Column	Description
IP	The IP address.
Port	The port for the IP.
Protocol	The protocol for the IP.
Domains	Domains associated with the IP.
Machine Count	The number of machines to which the IP connected.
Module Count	The number of modules associated with the IP.
First Activity	The date and time that the IP first connected.
Last Activity	The date and time that the IP last connected.

IP List Panes

Note: For more information about configuring and customizing panes, see the topic *Panes* in [Main Window](#).

The **IP List** window has three panes to access more data.

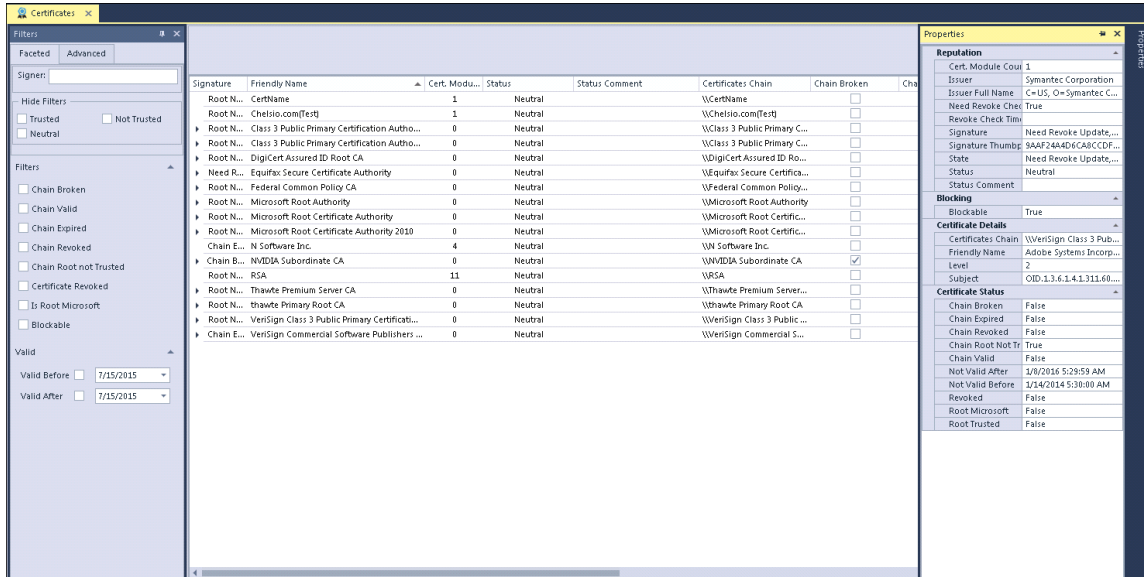
- **Machines:** gives a list of machines with the currently selected IP. If there are more than 10,000 modules for a selected IP, the list displays only the machines for the 10,000 modules with the highest risk score.
- **Modules:** gives a list of Windows and Mac modules with the currently selected IP. This list is limited to 10,000. If there are more than 10,000 modules for a selected IP:
 - For Windows modules, the list displays only the 10,000 modules with the highest risk score.
 - For Mac modules, the list displays only the 10,000 modules with the highest IIOC score.
- **Properties:** has two tabs, **Summary** and **All**, that allow you to access more information about a selected IP.

Certificates Window

The **Certificates** window contains the list of all certificates found in modules or machines. NetWitness Endpoint verifies for certificate revocation daily (at least).

Note: If NetWitness Endpoint isn't able to connect to a certain server for a certain period of time, the status of each certificate will eventually change to Need Revoke Update. In this case, the user needs to use the ConsoleServerSync.exe tool to manually synchronize the certificates. For more information, see [NetWitness Endpoint ConsoleServerSync Tool](#).

To open Certificates, click **Certificates** in the **Main Menu**. The **Certificates** window is displayed as shown in the following figure.



The **Certificates** window is made up of the Certificates table and a number of panes that allow you to filter and view more information about the certificates.

Certificates Table

Note: For more information about configuring and customizing tables, see the topic [Tables in Main Menu](#).

There are a number of actions available by right-clicking an entry:

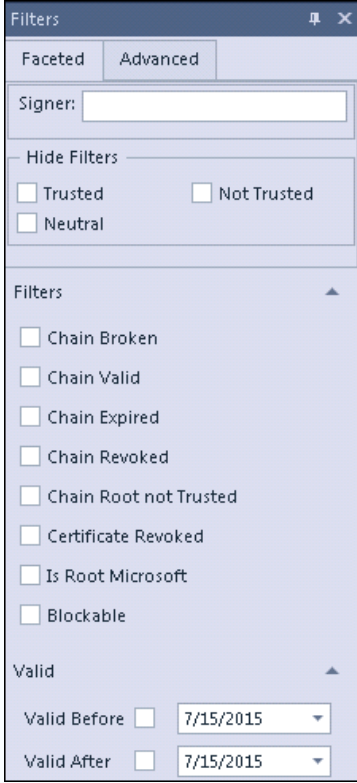
- **Edit Certificate Whitelist Status:** Edit the certificate status.
- **List Windows Modules with Certificates:** Opens a new tab that contains a list of Windows modules with the selected certificate.
- **List Mac Modules with Certificates:** Opens a new tab that contains a list of Mac modules with the selected certificate.
- **List Computers with Certificates:** Opens a new tab that contains a list of the computers with the selected certificate.

Certificates Panes

Note: For more information about configuring and customizing panes, see the topic *Panes* in [Main Menu](#).

Certificates has two panes to filter the machines or access more data:

- **Properties** allows you to view properties of a selected certificate.
- **Filters** allows you to apply a variety of filters to the certificates. It has two tabs, **Faceted** and **Advanced**.
 - **Faceted**

Filters Pane	Option	Description
	Signer	Filter certificates by signer.
	Hide Filters	Check the checkboxes to hide Trusted, Not Trusted, and/or Neutral certificates.
	Filters	Check the checkboxes to filter according to various options.
	Valid	Check the Valid Before and/or Valid After checkboxes and select desired date(s).

- **Advanced:** Is for advanced users who wish to have additional control over the filter options.

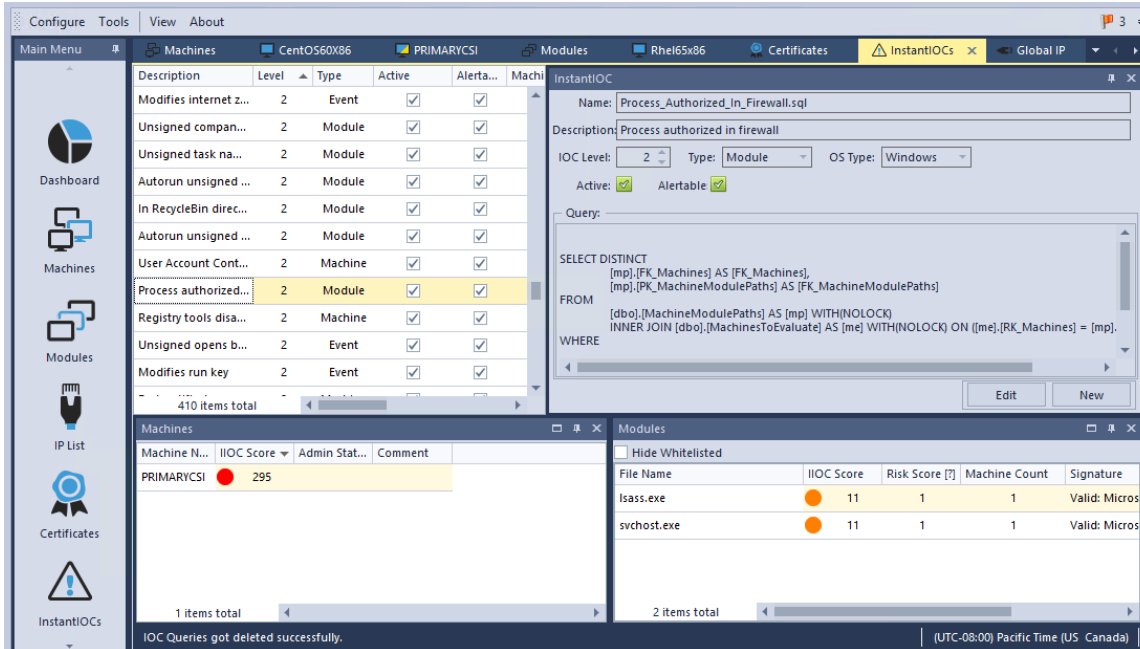
InstantIOCs Window

The **InstantIOCs** window contains the list of all InstantIOCs (Instant Indicators of Compromise) triggered on modules or machines.

InstantIOCs enable security analysts to very quickly query the NetWitness Endpoint database to find files matching specific attributes. They help to reduce the amount of data an analyst must sift through, making it even faster to detect threats in the environment. NetWitness Endpoint comes with more than 200 out-of-the-box InstantIOCs and analysts can easily create their own customized versions.

For more information, see [InstantIOCs](#).

To open InstantIOCs, click **InstantIOCs** in the **Main Menu**. The **InstantIOCs** window is displayed as shown in the following figure.



The **InstantIOCs** window is made up of the InstantIOCs table and a number of panes that allow you to view more information about the IOCs.

InstantIOCs Table

Note: For more information about configuring and customizing tables, see the topic [Tables](#) in [Main Window](#).

Right-clicking an entry allows you to clone the InstantIOC and in certain cases, to delete it.

InstantIOCs Panes

Note: For more information about configuring and customizing panes, see the topic [Panels](#) in [Main Window](#).

The **InstantIOCs** window has three panes to access more data.

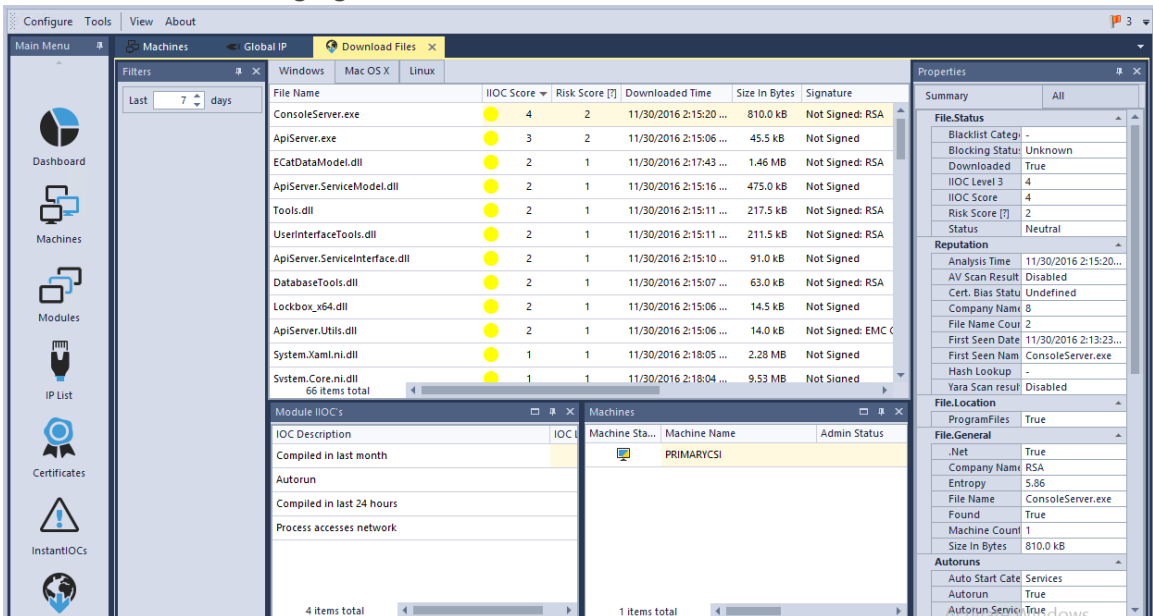
- **Machines:** gives a list of machines with the currently selected IIOC.
- **Modules:** gives a list of modules with the currently selected IIOC. This list is limited to 10,000. If there are more than 10,000 modules for a selected IIOC:
 - For Windows modules, the list displays only the 10,000 modules with the highest risk score.
 - For Mac and Linux modules, the list displays only the 10,000 modules with the highest IIOC score.
- **InstantIIOC:** editing pane gives more information about the selected IIOC and allows you to edit it, activate it or deactivate it, make it alertable or non-alertable, or create a new IIOC.

Note: For more information about editing or creating IIOCs, see [Edit or Create IIOCs](#).

Downloads Window

The **Downloads** window provides information about files downloaded to NetWitness Endpoint.

To open Downloads, click **Downloads** in the **Main Menu**. The **Downloads** window is displayed as shown in the following figure.



Downloads are listed under three main tabs: **Windows**, **Mac OS X**, and **Linux**.

The **Downloads** window is made up of the Downloads table and various panes that allow you to view more information about the selected download.

Downloads Table

Note: For more information about configuring and customizing tables, see the topic *Tables* in [Main Window](#).

There are a number of actions available by right-clicking an entry:

- **Edit Blacklist-Whitelist Status:** Edits the blacklist or whitelist status of the module.
- **List Computers with Module:** Opens a separate tab with a list of computers that contain the selected module.
- **Save Local Copy:** Saves a local copy of the module.
- **Analyze Module:** Opens an **Analyze Module** window that contains various information about the module.
- **Search with Google > MD5:** Performs a search of the module MD5 using Google.
- **Search with Google > SHA1:** Performs a search of the module SHA1 using Google.
- **Search with Google > SHA256:** Performs a search of the module SHA256 using Google.
- **Search with VirusTotalSearch > MD5:** Performs a search of the module MD5 using VirusTotalSearch.
- **Search with VirusTotalSearch > SHA1:** Performs a search of the module SHA1 using VirusTotalSearch.
- **Search with VirusTotalSearch > SHA256:** Performs a search of the module SHA256 using VirusTotalSearch.
- **Open in a Separate View:** Opens the module in a new tab.
- **View Certificate:** Opens the Certificates window.
- **Download to Server:** Downloads the module to the server.
- **Scan with YARA:** Scans the module with YARA.
- **Scan with OPSWAT:** Scans the module with OPSWAT.
- **Scan with OPSWAT and YARA:** Scans the module with OPSWAT and YARA.

The Downloads table includes the following default column headings.

Note: There are a variety of columns you can choose to display using the Column Chooser function. For more information about configuring and customizing tables, see the topic *Tables* in [Main Window](#).

Column	Description
IIOC Score	The Machine IIOC Score provides a level of confidence that the behavior described in the IIOC was found. Higher scores also denote a greater probability of malicious intent. Also provides a color (green, yellow, orange, red, or black) that represents the severity of the threat found in the machine. For more information, see Levels of IIOCs, IIOC Scores, and Risk Score .
Signature	Indicates the presence or absence, validity and source of the signature of this module. Note: In NetWitness Endpoint, all signature information is obtained by a low-level system designed to avoid any malware signature verification bypassing techniques.
Hash Lookup	The classification of the module, based on its hash, from one or more databases.
Machine Count	Indicates the number of different machines where this module was found. If a module is present on all machines, it may be present on the original installation image, or has been intentionally widely deployed. If a module is only present on one agent, and a thousand agents are checked, it is likely that this module is suspicious and requires more investigation.
Error Description	In the event of a download error, the error's details will be displayed here.

Downloads Panes

Note: For more information about configuring and customizing panes, see the topic *Panes* in [Main Window](#).

The **Downloads** window has four panes that allow you to view more data about a selected download:

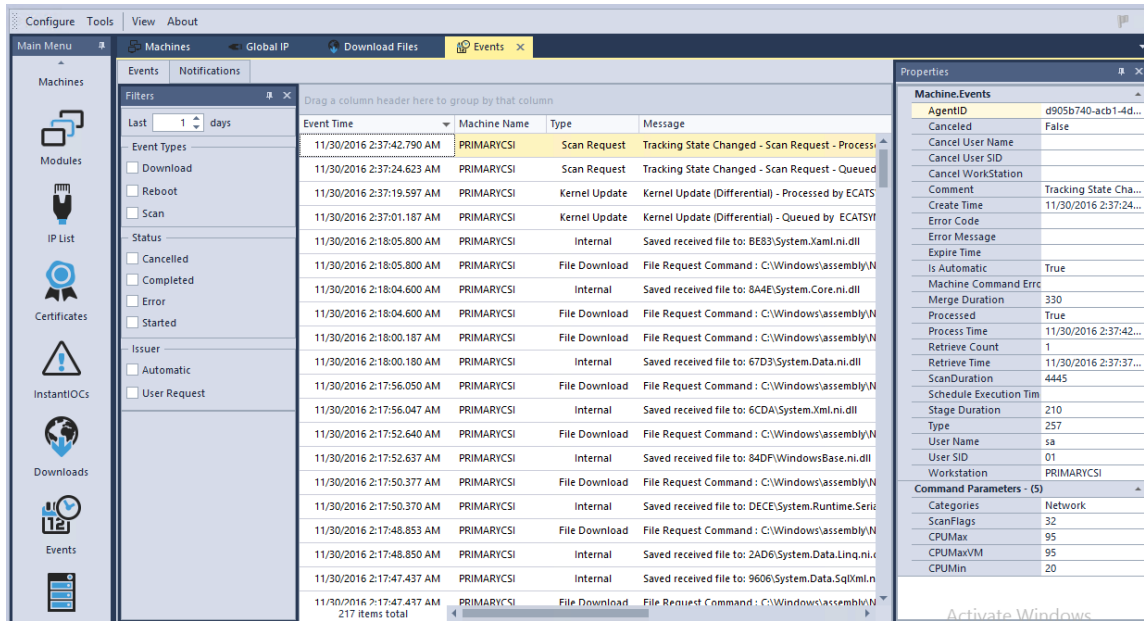
- **Properties** allows you to view properties of a selected download.
- **Filters** allows you to filter the Downloads table according to a selected time frame.

- **Module IIOCs** provides information about any IIOCs that were detected against a selected download.
- **Machines** provides information about machines on which a selected download was found.

Events Window

The **Events** window provides information about NetWitness Endpoint events and notifications related to all agents or the server.

To open Events, click **Events** in the **Main Menu**. The **Events** window is displayed as shown in the following figure.



The **Events** window has two tabs, **Events** and **Notifications**. Each tab has its own table and a Filters pane.

Events displays:

- Queued Commands
- Scan Requests
- Download File Requests (manually or automatically queued)
- Reboot requests
- Debugger tolerance
- Memory Tracker enable/disable
- Agents that retrieve commands

- Agent or Server errors
- Agent Data was saved

Notifications are messages that the user should see as soon as they arrive. Notifications include programmed notifications such as a requested scan being processed.

Note: For more information about activating a scan notification, see the topic [Request an Agent Scan Manually](#).

Notifications also include messages about the environment that are important to users, such as when the SQL Agent Service is not running, or when the server's storage disk is full.

Events Tab: Events Table and Filters Pane

The Events tab displays a table with a list of events for all agents. It provides the Event Time, Machine Name, Type, and Message.

Note: For more information about configuring and customizing tables and panes, see the topics *Tables* and *Panes* in [Main Window](#).

The Events table includes the following default column headings.

Column	Description
Type	The type of event. This may include file requests, scan requests, and uninstall agent requests.
Message	More information about the type of event.
Started	The checkbox is checked if the event started.
Error	The checkbox is checked if the event encountered an error.
Automatic	The checkbox is checked if the event was automatic.
Canceled	The checkbox is checked if the event was canceled.
Completed	The checkbox is checked if the event was completed.

The **Events** tab also consists of a **Filters** pane with various options for filtering events. Events can be filtered to those that occurred within a specified number of days from today, or based on event types, status, and issuer.

Notifications Tab: Notifications Table and Filters Pane

The Notifications tab displays a table with a list of notifications for all agents and the time at which the notification was received.

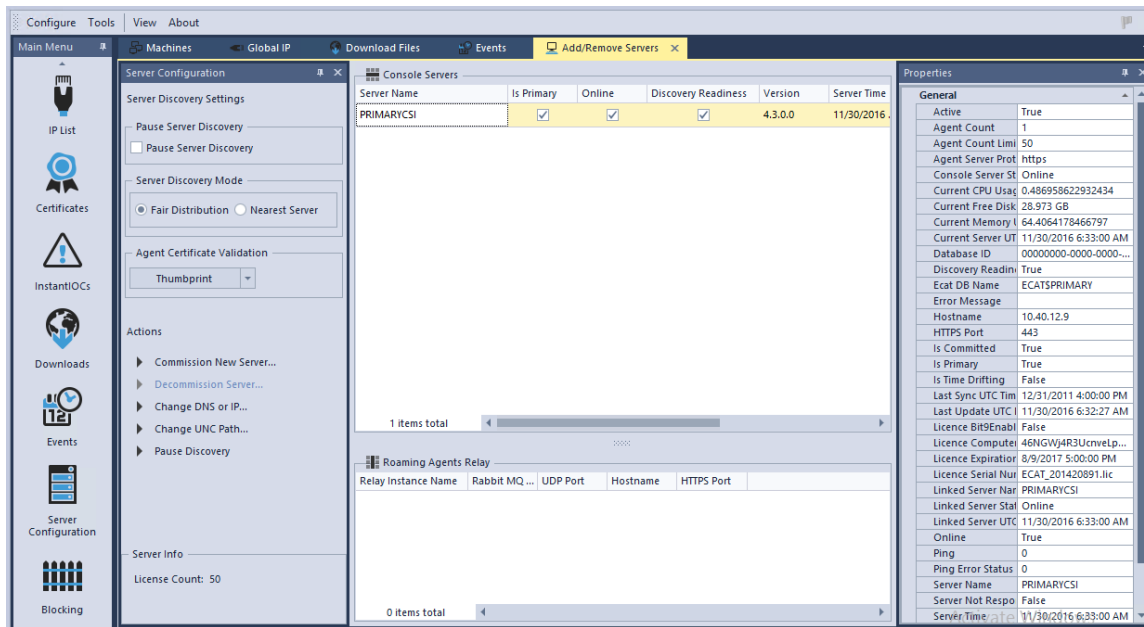
Note: For more information about configuring and customizing tables and panes, see the topics *Tables* and *Panes* in [Main Window](#).

The Notifications tab also consists of a **Filters** pane that allows you to filter the list to those notifications that were made within a specified number of days from today.

Server Configuration Window

The **Server Configuration** window contains the list of all servers connected to NetWitness Endpoint.

To open Server Configuration, click **Server Configuration** in the **Main Menu**. The **Server Configuration** window is displayed as shown in the following figure.



The **Server Configuration** window is made up of the Server Configuration table and a number of panes that allow you to view more information about the servers.

The Cloud Servers pane can be used to configure new cloud servers. Roaming Agent Relay (RAR) is a separate component that provides visibility of endpoints that are disconnected from a corporate network. RAR can be deployed as a cloud service. For information about installing and configuring RAR, see the **RSA NetWitness Endpoint 4.4 Installation Guide** available on [RSA Link](#).

Server Configuration Table

Note: For more information about configuring and customizing tables, see the topic *Tables* in [Main Window](#).

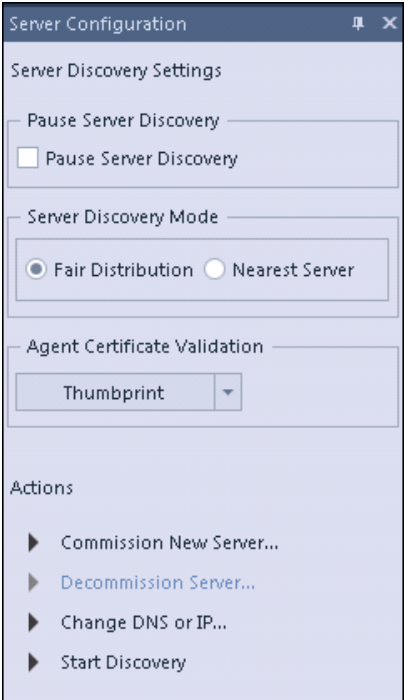
The Server Configuration table includes the following default column headings.

Column	Description
Is Primary	Details if the server is known as the Primary server.
Discovery Readiness	Will allow the server to be connected to by the Agents.
Server Time	Local server time.
Hostname	Name used by the agents to create the connection.

Server Configuration Panes

Note: For more information about configuring and customizing panes, see the topic *Panes* in [Main Window](#).

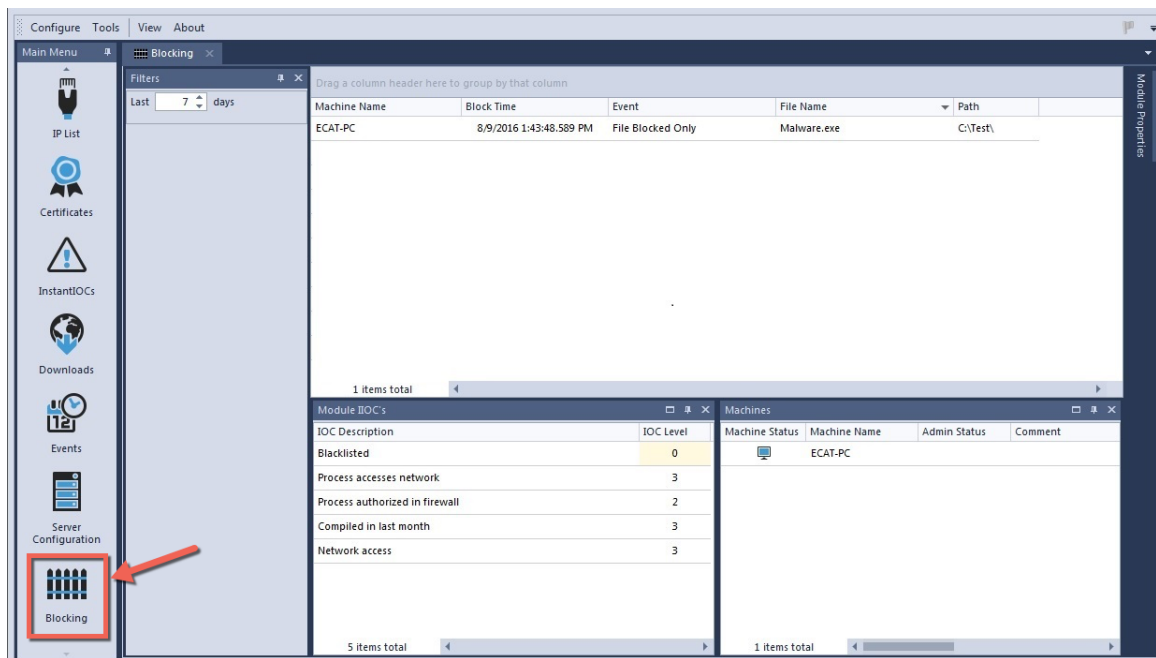
Server Configuration has two panes: **Properties**, which provides more information about a selected server, and **Server Configuration**, which offers a variety of actions to apply to a selected server, as shown below.

Server Configuration Pane	Option	Description
	Pause Server Discovery	This is a global setting that allows the NetWitness Endpoint Admin to pause/resume the server assignments to NetWitness Endpoint agents.
	Server Discovery Mode	<p>Fair Distribution: The primary server attempts to equally distribute the NetWitness Endpoint agents among all the available console servers. Nearest Server: The primary server assigns the closest console server to any agent seeking a server.</p>
	Agent Certificate Validation	<p>May be Thumbprint, Full Chain, or None. Thumbprint: default selection; certificate is generated during installation in the server store and is used when starting the Console Server; server uses the certificate to identify itself and looks for the certificate from the agent; performs direct validation of agent thumbprint; this is the most restrictive option. Full Chain: for customers who have their own certificates they want to use to authenticate agents; looks at root certificate and checks if it is trusted; must go through verification process by checking the trust chain; no revocation checks are performed to allow Console Server to work offline. None: no validation; used for diagnostic purposes only.</p>
<p>Note: The setting selected here is mirrored in the Agent Packager Certificate Validation settings when generated, where it is used by the agent to validate the server certificate. Most likely it will not need to change, but it may be changed if desired. For example, if using full chain for the server certificate you could use thumbprint for the agent.</p>		

Server Configuration Pane	Option	Description
	Actions	One or more actions may be available. Click the desired action to make changes. Actions include Commission New Server, Decommission Server, and Change DNS or IP.

Blocking Window

The **Blocking** window displays the summary of the blocked modules and all events related to blocking within the network, as shown below.



For more information on blocking, see [Blocking System](#).

Tracking Systems

NetWitness Endpoint tracking functionality includes Network Monitoring and Behavior Tracking. While deploying the agent, you can select the following tracking configurations:

- No Monitoring
- Network Monitoring Only
- Full Monitoring and Tracking

(includes both Network Monitoring and Behavior Tracking)

- Full Monitoring, Except Network

Note: Although the performance impact of using trackers is minimal, it is recommended to test the configuration in a test environment before you move it to the production environment of a large-scale deployment.

Note: Full Monitoring and Behavior Tracking is not supported for Linux agents.

No Monitoring

With the No Monitoring option there is no active detection monitoring at all and only normal scan data is available. This option may be useful if you need to investigate or avoid issues.

Note: During a scan, the user mode retrieves all active/listening network connections using the Windows API and reports them to the server, even for agents deployed with the No Monitoring option.

Network Monitoring

Network Monitoring involves a connection analysis that provides statistical information on the network connections since the time of system boot. The data related to network monitoring is found in the Modules table and the IP List.

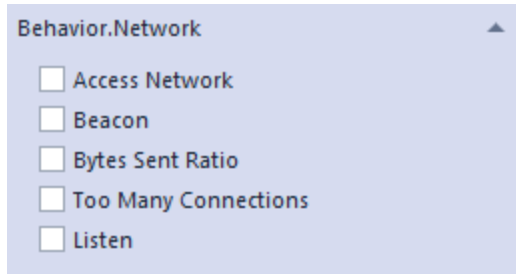
Note: The results of network monitoring are sent to the server with scans.

For each connection, a statistical analysis is performed to determine if it is suspect and potentially related to a command and control (C&C) pattern. When a suspect connection is detected, the module associated with it is assigned a suspect reason, namely, “Too many connections”, “Beacon,” or “Bytes Sent Ratio.” This data is found in the Modules window.

To view Network Monitoring data in the Modules window:

1. From the **Main Menu**, click **Modules**.
2. In the **Modules** table, right-click a column heading and select **Column Chooser** to access a complete list of column options.
3. In the **Customization** dialog box, click the **Behavior.Network** menu arrow.

4. Select the checkboxes to add desired columns (Access Network, Beacon, Bytes Sent Ratio, Listen, Too Many Connections).



5. Close the dialog.

To view Network Monitoring data in the IP List:

1. From the **Main Menu**, click **IP List**.
2. Locate the desired information in the IP List table and in the Summary/All pane.

The following data is available in the IP List.

Property	Description
IP	IP address to which a given process connected or tried to connect. If the system is behind a proxy, the proxy IP is displayed. NetWitness Endpoint does not decode proxy protocols.
Domains	Domain names queried by the process to retrieve the IP address. Note: This is not the reverse lookup address as they most often lead to an address unrelated to the domain accessed, such as Akamai servers.
Bytes sent/received	Total number of bytes sent to and received from this connection.
Connect Count	Number of unique connections (that is, a unique combination of Module/IP/Port/Protocol) initiated by this process.
Burst Count	A burst is a number of consecutive connections ending by at least 15 seconds of inactivity. For example, a malware connecting to its command and control every 3600 seconds (1 hour) and sending multiple collected files each time will generate a single burst per hour even if tens of actual connections are generated.

Property	Description
Burst Interval Mean	The mean time between each burst.
Burst Interval Deviation	Dispersion of burst interval. The more spread apart the bursts, the higher the deviation. The closer the bursts, the lower the deviation. For example, a malware polling every 60 seconds with a standard deviation of 1 or 2 seconds will indicate a very steady polling pattern. Malware using random polling intervals will generate greater values.
Protocol	Internet protocol used. Currently supported values are TCP and UDP.

Full Monitoring and Tracking

Full Monitoring and Tracking includes both Network Monitoring and Behavior Tracking.

The NetWitness Endpoint Behavior Tracking system is an active system that monitors operations and key behaviors related to processes, files, and networks. The Behavior Tracking system allows real-time propagation of suspicious events as they occur and then sends the events to the ConsoleServer automatically without triggering any scan. The events are sent to the ConsoleServer as *.csv files, which are then processed by the database and displayed in the NetWitness Endpoint UI.

For Windows, the system monitors the following behaviors: OpenProcess, CreateRemoteThread, OpenLogicalDrive, OpenPhysicalDrive, ReadDocument, WriteToExecutable, RenameToExecutable, NewIPAddress, Network - incoming, and Network - outgoing. Specifically for machines under containment, the system generates tracking events for IPv4 incoming - allowed or blocked, IPv4 outgoing - allowed or blocked, IPv6 incoming - allowed or blocked, and IPv6 outgoing - allowed or blocked.

For Mac, the system monitors OpenProcess, CreateRemoteThread, WriteToExecutable, RenameExecutable, and CreateAutorun.

The NetWitness Endpoint Behavior Tracking system serves two main purposes:

- To identify the perpetrators of common malware-like behaviors, such as floating code allocation and suspicious thread creation (for more information, see [Floating Code](#)). This is available to allow you to better pinpoint the owner of an action.
- To report common behaviors, such as network activity and inter-process operations, that could be indicative of malware or other threats.

For example, if a malware executes and disappears between scans, the NetWitness Endpoint Behavior Tracking system will identify this behavior.

Tracking events are collected until the next beacon (+15 seconds by default), where the agent will notify the server that it has tracking data to send. On the next cycle (+15 more seconds), the server will request the list of events. Events are typically sent only once (on first occurrence) to avoid overloading the environment. Behavior Tracking events are stored in the main NetWitness Endpoint database and are visible via the NetWitness Endpoint UI's Machine view, in its own pane.

A Behavior Tracking event triggers a limited scan in which just the events (and associated module information) are retrieved for only those categories affected by the event. This is usually done immediately upon receiving the agent status. When a new module is seen by the server for the first time, a scan of the host will be triggered automatically.

If no IIOC's are enabled, then the Tracking events will not impact the endpoint or module score. However, they can still be used for investigative purposes after a breach has been detected.

Full Monitoring, Except Network

This option simply removes network monitoring from the Full Monitoring and Tracking functionality. This option may be useful if you have isolated an issue to the way the Windows agent does its network monitoring and need to disable it. This option is only available for Windows agents.

Note: During a scan, the user mode retrieves all active/listening network connections using the Windows API and reports them to the server, even for agents deployed with the Full Monitoring, Except Network option.

SCAN YOUR NETWORK ENVIRONMENT

There are a variety of scanning options available in NetWitness Endpoint. Agents can either be automatically scanned at the scheduled time set in the NetWitness Endpoint Packager, or they can be manually scanned by request. For more information on scheduling scans automatically, see the topic *Deploying Agents* in the **RSA NetWitness Endpoint Installation Guide**. In addition, there is a database global setting that can automatically request scans for newly connected agents.

The following topics provide additional information on NetWitness Endpoint scanning options:

- [Scan Categories](#)
- [Throttle Agent CPU](#)
- [Download New Modules Automatically](#)
- [Configure Scans for a Machine Group](#)
- [Set Automatic Scan Request](#)
- [Request an Agent Scan Manually](#)
- [Perform a Scan in Standalone Mode](#)
- [NetWitness Endpoint ConsoleServer Logs During a Scan](#)
- [Known Compatibility Issues with Other Antivirus Programs](#)

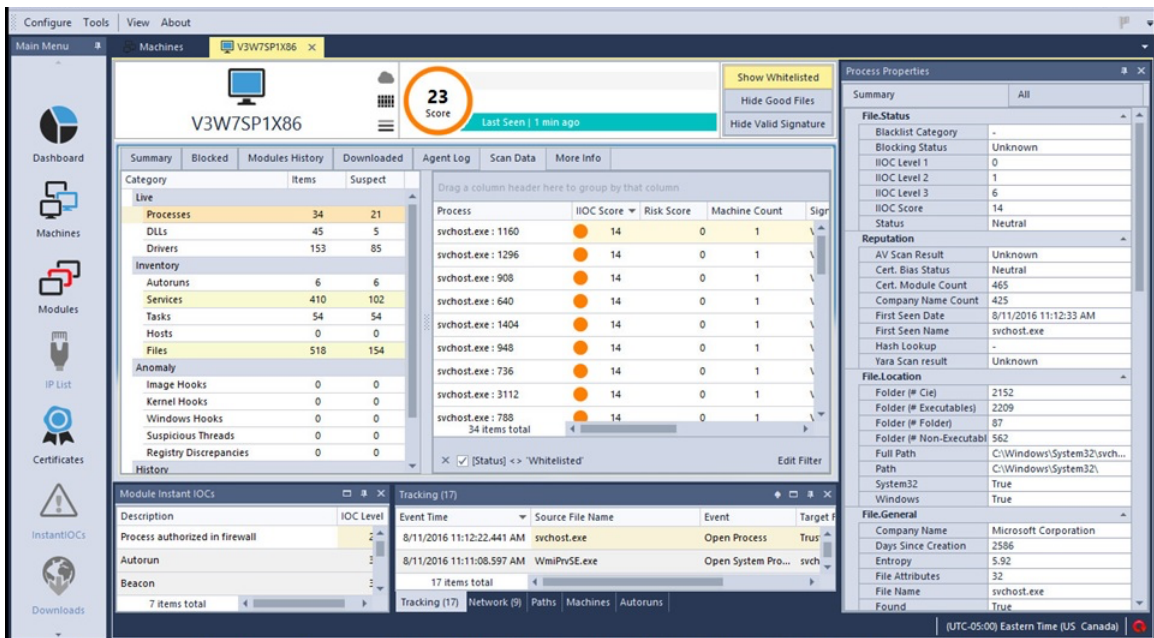
Scan Categories

Categories are the various kinds of things the NetWitness Endpoint agent scans for on the client machine.

Every aspect of each category is scanned multiple times, using different methods, to avoid being bypassed by malware techniques.

The list of categories can be found in the Machine View (click **Machines** in the **Main Menu** and then double-click the machine of interest). Click **Scan Data** to see a list of categories in the options pane on the left.

Clicking a category (say, **DLLs**) will provide a list of instances in the middle pane (such as a list of actual **DLLs**), including threat levels and scores. In the Properties pane is the list of properties of that instance.



Scan categories are specific to the agent machine, according to operating system, as specified in the following topics:

- [Categories \(Windows Machines\)](#)
- [Categories \(Mac OS-X Machines\)](#)
- [Categories \(Linux Machines\)](#)

Categories (Windows Machines)

The categories for Windows machines are divided into four groups, as follows:

Live

- **Processes:** All processes running in the machine at scan time are listed in this category.
- **DLLs:** Dynamic Link Libraries (DLLs) are modules that were loaded by different processes in order to use certain specific functionalities. Only potentially dangerous and non-Microsoft entries are listed in this category.
- **Drivers:** This category will scan and report all the drivers running on the agent's machine at the moment of the scan.

Inventory

- **Autoruns:** All items that are found to be executed at start-up are listed in this category. The list of modules includes all modules automatically started at boot time, login time, or execution time. Any of these techniques could be used to auto-start malware.
- **Services:** All modules that are running as services are listed in this category.
- **Tasks:** All items found in Windows Task Scheduler are listed in this category.
- **Hosts:** All network redirections written in the Host file are listed in this category.
- **Files:** This category contains the list of potentially dangerous and non-Microsoft executable files, as well as any other file found to be hidden.

Anomaly

- **Image Hooks:** Hooks found in executable images (user-mode or kernel-mode): IAT, EAT, Inline.
- **Kernel Hooks:** Hooks found on kernel objects (such as Driver Object [Pointers, IRP_MJ]). This also includes filter devices.
- **Windows Hooks:** Hooks installed using SetWindowsHooksEx().
- **Suspicious Threads:** This category lists all suspicious threads that were found. Suspicious threads are the threads that were found to be floating code or threads whose service table was hooked. The threads could be running either with *user-mode* privileges or with *kernel-mode* privileges. These threads could be used to run malicious code inside a trusted application to execute their own code.
- **Registry Discrepancies:** The Windows registry is a hierarchical database that stores configuration settings and options on Microsoft Windows operating systems. It contains settings for low-level operating system components as well as for applications running on the platform: the kernel, device drivers, services, SAM, user interface, and third party applications all use the registry.

History

- **Network:** An aggregated list of network connections made on the agent machine. See "Network History" in [Analyze Scan Data for a Machine](#) for more information.
- **Tracking:** The NetWitness Endpoint Behavior Tracking system is an active system that monitors operations and key behaviors. See "Full Monitoring and Tracking" in [Tracking Systems](#) for more information.

Parameters

- **Retrieve Master Boot Record:** Selecting this option allows you to capture module metadata of the master boot record, as well as the partition boot record as part of the scan. This is usually done to get the hashes of boot records. Different versions of Windows implement different boot records. Other factors can cause the records to change, such as operating system, language, and disk encryption software. The information will be attached to the files named "MASTER_BOOT_RECORD" and "NTFS_BOOT_RECORD".
- **Reset Agent's Network History:** Selecting this option allows the Windows agents to persist network connection statistics across reboots. This allows the agent to report much more metrics of the complete network. To have more control on the data reported, the scan option is added to clear the connection history. While performing a scan with this option, all prior network statistics are destroyed, and future scans will contain only the new connections collected after this point.

Categories (Mac OS-X Machines)

The following categories, divided into three groups, are supported by the Mac agent scan.

- **Live**
 - **Processes:** Running processes on the Mac.
 - **Loaded Libraries:** Libraries, frameworks, or other dynamically loaded images in the running process. System Frameworks provided by default by the OS are not reported.
 - **Kernel Extensions:** Modules, which are loaded in the Kernel as extensions.
- **Inventory**
 - **Login Items:** Items configured by a user to launch at login time.
 - **Daemons and Agents:** Currently running daemons and agents on the machine.
 - **Hosts:** Entries found in the /etc/hosts file.
 - **Files:** Mach-o format files found on the disk while enumerating the whole file system.
- **History**
 - **Network:** An aggregated list of network connections made on the agent machine. See "Network History" in [Analyze Scan Data for a Machine](#) for more information.
 - **Tracking:** The NetWitness Endpoint Behavior Tracking system is an active system that monitors operations and key behaviors. See "Full Monitoring and Tracking" in [Tracking Systems](#) for more information.

Except for **Login Items** and **Host file** categories, all other categories have Modules and Module Path properties associated with them.

Each unique Mach-o file (SHA256 hash) is referenced as a module. The path on disk where the module resides is Module path.

Additionally a module could be signed, in which case the whole certificate chain is captured and sent to the server. It can be viewed by clicking **Certificates** on the left pane in the NetWitness Endpoint UI.

Categories (Linux Machines)

The following categories, divided into two groups, are supported by the Linux agent scan.

- **Live**
 - **Processes:** All processes running on the Linux agent at scan time.
 - **Loaded Libraries:** Libraries, frameworks, or other dynamically loaded images in the running process.
 - **Drivers:** This category will scan and report all the drivers running on the agent's machine at the time of the scan.
- **Inventory**
 - **Autoruns:** All items that are set to execute at start-up. The list of modules includes all modules automatically started at boot time, login time, or execution time. Any of these techniques could be used to auto-start malware.
 - **Crons:** A type of autorun strategy.
 - **Services:** All modules that are running as services.
 - **Host file entries:** All network redirections written in the Host file.

Throttle Agent CPU

Agent CPU can be throttled to ensure enough CPU is available for the scan and to prevent NetWitness Endpoint from demanding too much from a system that is under heavy use. The NetWitness Endpoint system can be set to automatically download new modules, and the file size of these modules can be limited so that files above a certain size need to be manually downloaded.

When scanning agents, the following Agent CPU values can be throttled:

- **Low CPU Value:** The Low CPU value represents the absolute minimum NetWitness Endpoint will use when there is heavy load on the system. It will not use less than this under

any circumstances. The purpose for this setting is in case a malware has started 100 threads, each consuming a lot of CPU cycles to starve all other processes. NetWitness Endpoint will then increase its priority and ensure it uses the configured minimum amount of CPU.

- **High CPU Value:** The High CPU value is the maximum CPU resources that NetWitness Endpoint will use if the system is idle.
- **VM High Value:** The VM High Value is the value that will be enforced instead of the High CPU value on endpoints running on Virtual Machines. On other systems it will go between Low CPU Value and High CPU Value.

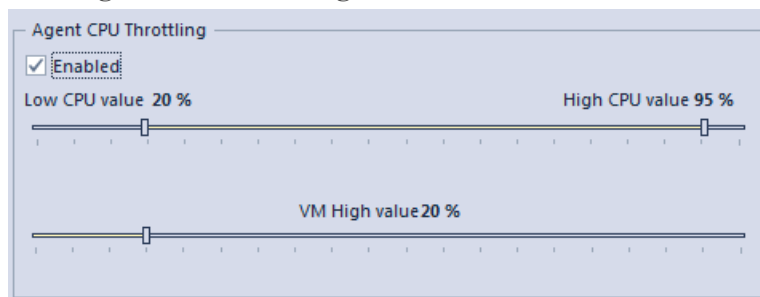
These settings for Agent CPU Throttling are the recommended values:

- **Low CPU value** – 20%
- **High CPU value** – 95% (Note: limiting CPU usage lengthens the amount of time necessary to complete scans; for example, having a maximum usage of 20% could potentially make the scan take five times longer.)
- **VM High value** – 20% to 30%

Note: NetWitness Endpoint scans will only ever use one core; thus, 100% means 100% of one core only.

To enable agent CPU throttling:

1. Click **Configure > Global Parameters**.
2. In the **Agent CPU throttling** section, check the **Enabled** checkbox.

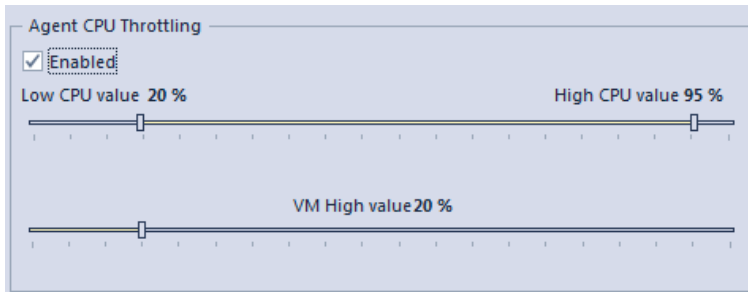


3. Click **OK** or **Apply**.

Note: To disable throttling, uncheck the **Enabled** checkbox.

To edit values for agent CPU throttling:

1. Click **Configure > Global Parameters**.
2. In the **Agent CPU throttling** section, make the desired changes by dragging the value indicators.



Note: Agent CPU Throttling must be enabled in order to modify the values.

3. Click **OK** or **Apply**.

Download New Modules Automatically

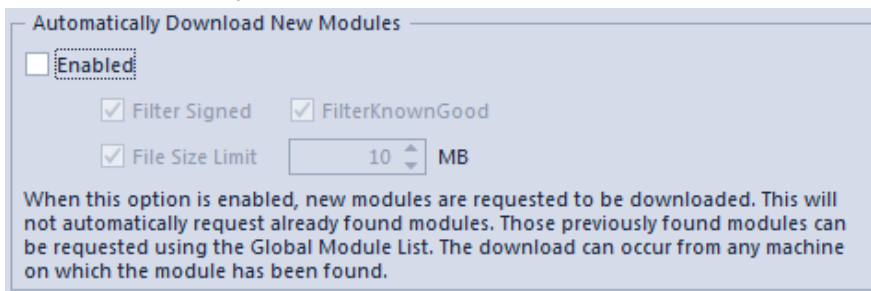
This option is enabled by default, and it ensures that newly found modules are automatically requested to be downloaded. The automatic download option will only download a single copy of each file found. In order to limit the volume of files downloaded, the use of filters is highly recommended. The size of modules to be automatically downloaded should also be limited.

Modules will automatically be scanned by Yara and Metascan when applicable.

Note: If you wish to download previously found modules, they can be requested using the Global Module List. The download can occur from any machine on which the module has been found. It is also possible to request a copy of a module from the Computer pane by right-clicking any file and selecting the **Download to Server** option.

To disable automatic downloading of new modules:

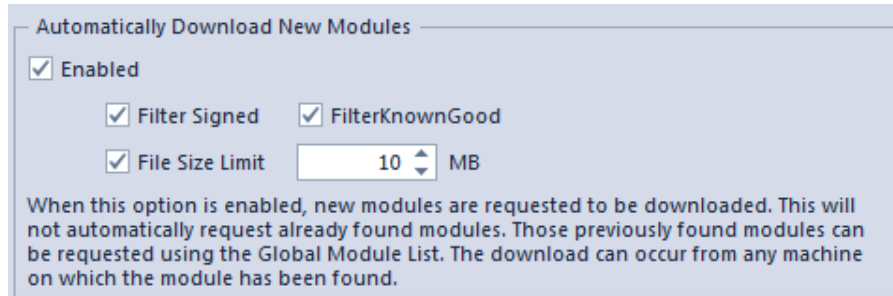
1. Click **Configure > Set Global Parameters**.
2. In the **Automatically Download New Modules** section, uncheck the **Enabled** checkbox.



3. Click **OK** or **Apply**.

To adjust file size limits or add filters:

1. Click **Configure > Global Parameters**.
2. In the **Automatically Download New Modules** section, ensure the **Enabled** checkbox is checked.



3. Do one or more of the following:>
 - Check one or both of the **Filter Signed** or **FilterKnownGood** checkboxes.
 - Remove the file size limit of modules to be automatically downloaded by unchecking the **File Size Limit** checkbox.
 - Adjust the file size limit of modules to be automatically downloaded by clicking the up or down arrows.
4. Click **OK** or **Apply**.

Configure Scans for a Machine Group

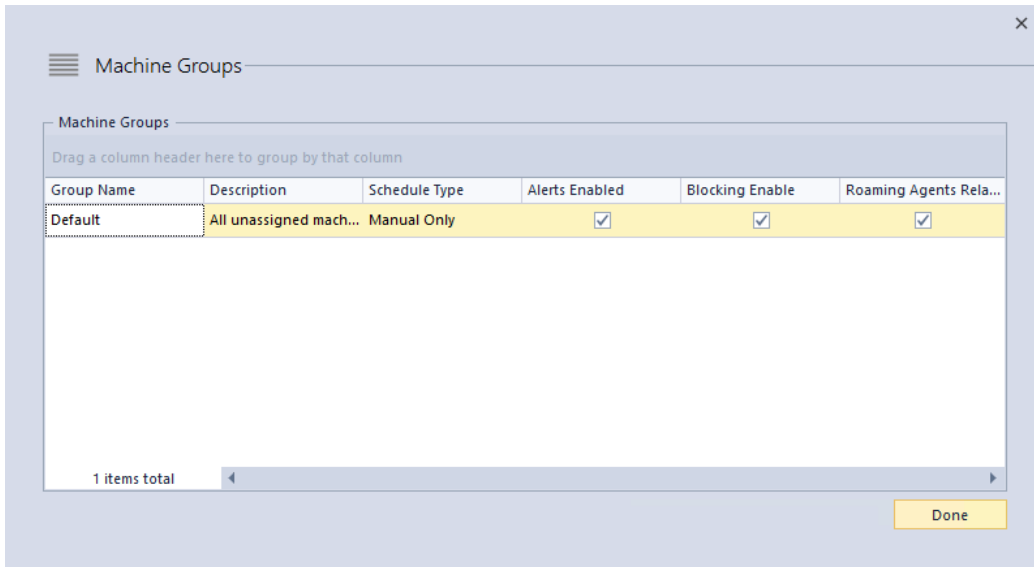
When NetWitness Endpoint is installed, a default machine group is created automatically. Any new system that checks in with NetWitness Endpoint is assigned to this group. NetWitness Endpoint will perform scans of an endpoint based on the type and interval configured under the Machine Groups menu option. You can create as many groups as needed to categorize endpoints in the network. Different types of scans and different scan intervals may be configured for each group.

The machine group named "Default" contains all machines on which the NetWitness Endpoint agent has been installed. Thus, the settings for this group automatically apply to all machines. If you wish to start a scan as soon as a new system first checks in with NetWitness Endpoint, you can set this in the scan configuration for the Default machine group.

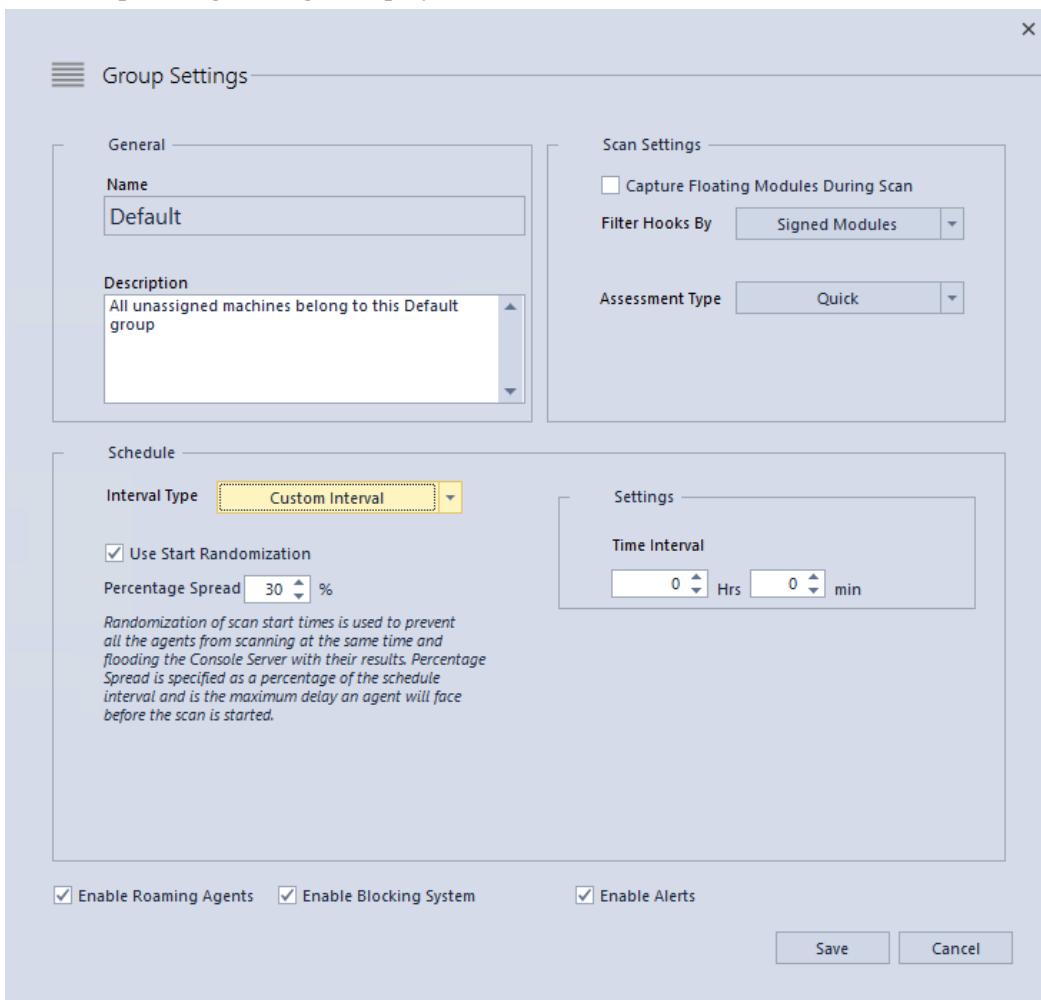
The following procedure describes the process for configuring scans for the Default machine group, which can also be applied to any other machine group you create. For information on adding or deleting machine groups, see the topic [Machine Groups](#).

To configure scans for the Default machine group:

1. On the Top Menu, click **Configure** and then select **Machine Groups**.
The Machine Groups dialog is displayed, as shown below:



- In the Group Name column, right-click on **Default** and select **Edit Group**. The Group Settings dialog is displayed, as shown below:



The Group Settings dialog has three sections:

- **General**, which displays the group name and a description.
- **Scan Settings**, which allows you to configure the type of scan.
- **Schedule**, which allows you to configure the frequency of scans.

3. Configure the desired scan settings according to the following table:

Scan Setting	Description
Capture Floating Modules During Scan	Select the checkbox to enable this option if you want NetWitness Endpoint to capture floating modules during a scan.
Filter Hooks By	Select how you want to filter hooks from the following options: <ul style="list-style-type: none"> • Signed Modules • Whitelisted Certificates • No Filter
Assessment Type	Select the type of scan from the following two options: <ul style="list-style-type: none"> • Quick • Full

4. Configure the desired schedule for performing scans according to the following table:

Schedule Setting	Description
Interval Type: Select the desired interval period between scans from the following options:	
<ul style="list-style-type: none"> • Manual Only 	If you select this option there are no additional settings available.
<ul style="list-style-type: none"> • Custom Interval 	Enter the desired time interval between scans as hours and minutes.
<ul style="list-style-type: none"> • Daily 	Select how the time is specified as either Local to Client, Local to Server, or UTC. Enter the time each day for performing the scan.

Schedule Setting	Description
<ul style="list-style-type: none"> Weekly 	Enter time specifications as detailed for the Daily option and then select the desired day of the week for the scan.
<ul style="list-style-type: none"> Monthly 	Enter time specifications as detailed for the Daily option and then select the numeric day each month that the scan should occur.
Use Start Randomization	
Select the checkbox to enable this option and then enter the desired Percentage Spread.	<p>This percentage represents the time interval over which to spread the individual scans. The randomization percentage is spread over 24 hours, beginning with the time set for the interval type. Percentage Spread can be set from 1% to 60%. For example:</p> <ul style="list-style-type: none"> If you set percentage spread to 50%, the first scan would start at the set time and the last scan would complete 12 hours later. If you set percentage spread to 25% and the start time is 9:00 AM, the first scan would start at 9:00 AM and the last scan would complete 6 hours later at 3:00 PM

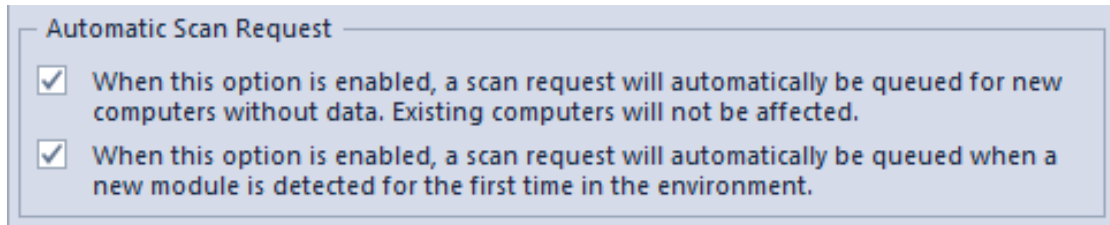
NetWitness Endpoint only retrieves PE files automatically from endpoints during its scans. Alternatively, you can manually request files from one or more systems. Sometimes, during malicious activity on a system, such as password dumping, an adversary will introduce malicious files on a system temporarily to dump passwords and then delete these files. While NetWitness Endpoint will record these events, unless it is scanning the moment the malicious files are introduced and running, it will not get a chance to download these files to the NetWitness Endpoint server. However, NetWitness Endpoint also has an option, which is not enabled by default, that automatically triggers a scan on the endpoint every time a new file is seen by the Behavioral Tracking feature. For more information, see the topic [Set Automatic Scan Request](#).

Set Automatic Scan Request

There is a global setting that ensures NetWitness Endpoint will automatically request a scan when a new agent connects for the first time or when a new module is detected for the first time in the environment. By default, both options are enabled.

To set NetWitness Endpoint to automatically scan new clients:

1. Click **Configure > Global Parameters**.
2. In the **Automatic Scan Request** section, check the desired checkbox or checkboxes.



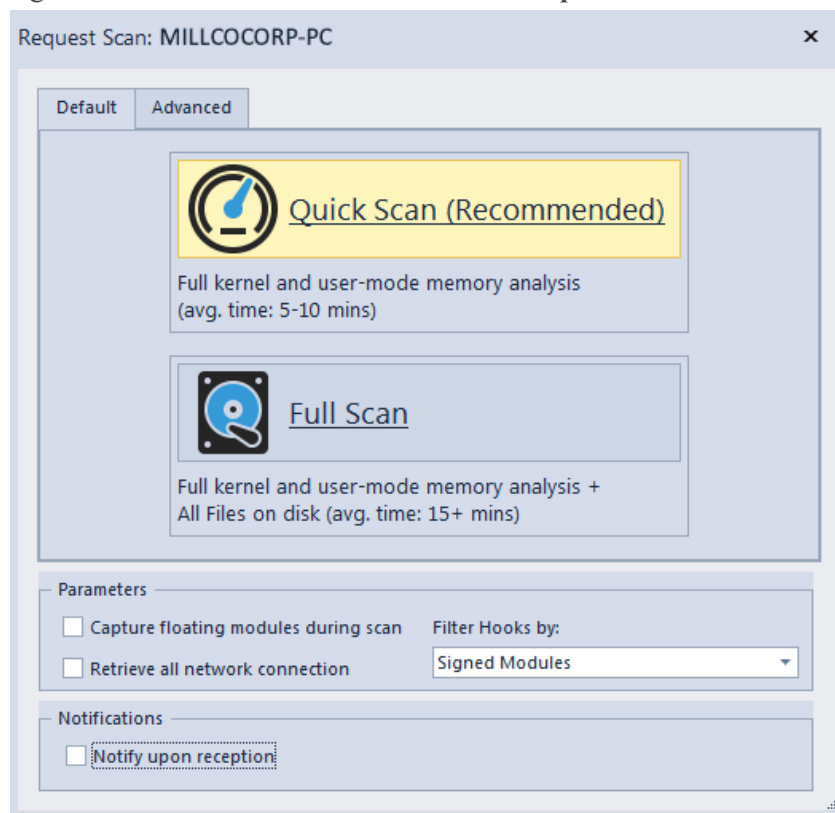
3. Click **OK** or **Apply**.

Note: To disable one or both options, uncheck the desired checkbox or checkboxes.

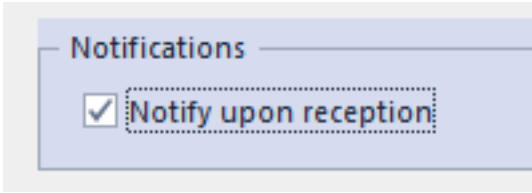
Request an Agent Scan Manually

To scan your network on demand:

1. In the **Main Menu**, click **Machines**.
2. Right-click the desired machine and select **Request Scan** from the drop-down menu.



3. (Optional) Check the **Notify upon reception** checkbox to be notified when the scan has been completed.



4. (Optional) Select desired parameters and filters.
5. Do one of the following:
 - On the **Default** tab, click **Quick Scan**.
 - On the **Default** tab, click **Full Scan**.
 - Click the **Advanced** tab, select the desired options, and click **Proceed**.

Note: For a detailed explanation of every category on the scan, see [Scan Categories](#).

Differences Between Quick Scan and Full Scan

The below table details some differences between Quick Scan and Full Scan.

Quick Scan	Full Scan
Quick scan is the default scan and it includes full kernel and user-mode memory analysis.	Full Scan is similar to quick scan, but it also includes a complete scanning of all the files found on the System disk.
All modules that are found to be active by any NetWitness Endpoint detection method will be retrieved and analyzed. Any module loaded in memory at any time will be analyzed with this method.	The entire drive will be scanned for modules. It is recommended to use only this option while investigating a machine that is expected to be infected and hence some additional information could be found on the disk.

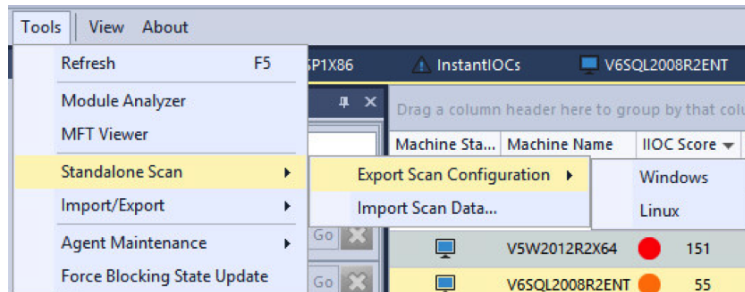
Perform a Scan in Standalone Mode

If the client machine is not connected to a network and cannot communicate with the ConsoleServer, a scan in standalone mode can be performed manually on the client machine. This is achieved by generating a scan configuration file in the NetWitness Endpoint UI, running the scan configuration file on the desired client machine, and then importing the scan output file to the NetWitness Endpoint UI, as described in the following procedures.

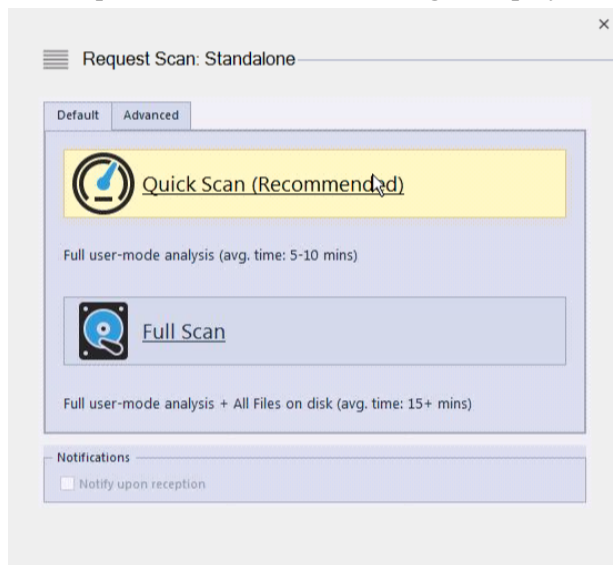
Note: The standalone scan function is supported only for Windows and Linux agents. It is not supported for Mac agents.

Procedure 1: Use the NetWitness Endpoint UI to generate a scan configuration file.

1. Click **Tools > Standalone Scan > Export Scan Configuration** > then select the desired operating system for the client machine, as shown below:



2. The Request Scan: Standalone dialog is displayed, as shown below.



3. Select the desired scan mode from the following options:
 - Click either **Quick Scan** or **Full Scan** on the **Default** tab.
 - If you wish to customize the categories or parameters for your scan, access the **Advanced** tab and select the desired options.
4. Click **Proceed**.

A dialog is displayed requesting you to create a password for the scan configuration file, as shown below:



5. Enter a password for the scan configuration file and click **OK**.

Note: The password must be between 8 and 32 characters. It should be recorded for reference because it will be used later in the process.

5. Navigate to the location where you want to save the file.
6. Enter a filename and click **Save**.
7. Transfer the scan configuration file to the client machine. This can be performed with a USB key or any other kind of media.
8. Install the agent using the same package that would have been used for a normal agent installation.

Note: If the agent is already deployed, it does not need to be reinstalled.

Procedure 2: Start the standalone scan.

1. Open a command prompt on the client machine.
2. Locate the agent executable file in one of the following locations, depending on the agent OS:
 - For Windows: C:\windows\system32
 - For Linux: /opt/rsa/nwe-agent/bin (if agent version is higher than 4.3.0.4)
or /usr/local/ecat (if agent version is lower than or equal to 4.3.0.4)

The executable filename is the name provided in the “NetWitness Endpoint Service Name” field in the NetWitness Endpoint Packager (for Linux agents the value is "ecat-agent" and for Windows agents the default value is "EcatService").

- Run the .exe file in the command prompt using the following syntax:

```
<ECAT Service Name> /password <password> /scanfile <scan config file>
```

>where:

<Ecat Service Name> is the name used in the NetWitness Endpoint Service Name field in the NetWitness Endpoint Packager (see Step 2)

<password> is the password provided to the NetWitness Endpoint UI when generating the scan configuration file and

<scan config file> is the path to the scan configuration file.

For example, the user can enter the command as follows for versions higher than 4.3.0.4:

```
nwe-agent /password
```

```
ecatdemo /scanfile '/home/kslp/desktop/standalone.cfg'
```

OR, for version 4.3.0.4 or lower:

```
ecat-agent /password
```

```
ecatdemo /scanfile '/home/kslp/desktop/standalone.cfg'
```

```
File Edit View Search Terminal Help
[root@localhost kslp]# /usr/local/ecat/ecat-agent -h
*****
* Enterprise Compromise Assessment Tool (ECAT) *
* Copyright 2016 EMC Corporation - All Rights Reserved. *
*****

Usage:
  ecat-agent /help
  - Displays this help.

  ecat-agent /password <password> /scanfile <scan config file>
  - <password>: Password provided on scan config file generation.
  - <scan config file>: Path of the scan config file generated.

[root@localhost kslp]# /usr/local/ecat/ecat-agent /password ecatdemo /scanfile '/home/kslp/Desktop/standalone.cfg'
*****
* Enterprise Compromise Assessment Tool (ECAT) *
* Copyright 2016 EMC Corporation - All Rights Reserved. *
*****

Preparing for stand alone scan...
Scan file /home/kslp/Desktop/standalone.cfg, provided password ecatdemo
Successfully decrypted scan config file...
Loaded configuration...
Running scan with operations 28425063424...
```

- The command window will update as the scan proceeds. When the scan is complete a “Writing data to scanx file...” message is displayed followed by the output scan file location and name, as shown below.

```

Preparing for stand alone scan...
Scan file /home/kslp/Desktop/standalone.cfg, provided password ecatdemo
Successfully decrypted scan config file...
Loaded configuration...
Running scan with operations 28425063424...
Stream=/var/run/dbus/system_bus_socket
Stream=/run/systemd/journal/stdout
Datagram=/run/systemd/journal/socket
Datagram=/dev/log
SequentialPacket=/run/udev/control
Netlink=kobject-uevent 1
DirectoryNotEmpty=/run/systemd/ask-password
OnActiveUsec=30000000
Stream=/var/run/avahi-daemon/socket
Stream=/var/run/rpcbind.sock
PathChanged=/var/lib/rhsm/branded_name
PathExists=/var/lib/rhsm/branded_name
DirectoryNotEmpty=/run/systemd/ask-password
PathExistsGlob=/var/spool/cups/d*
Stream=/var/run/cups/cups.sock
Stream=@ISCSIADM_ABSTRACT_NAMESPACE
Stream=@ISCSIID_UIP_ABSTRACT_NAMESPACE
DirectoryNotEmpty=/run/systemd/ask-password
Stream=/run/lvm/lvmetad.socket
FIFO=/run/dmeventd-server
FIFO=/run/dmeventd-client
Datagram=/run/systemd/shutdown
FIFO=/dev/initctl
OnUnitActiveUsec=86400000000
OnBootUsec=900000000
Completed scan, processing data...
Writing data to scanx file...
Output scan file generated at : /usr/local/ecat/localhost.localdomain-2016-04-14T14:34:19.000.scanx
Take the scanx file and import into ECAT UI->Tools->Standalone Scan->Import Scan Data
[root@localhost kslp]#

```

5. Transfer the scan data result file back to the machine hosting the NetWitness Endpoint UI for the import after the scan is completed.

Procedure 3: Import the standalone scan data.

1. Click **Tools > Standalone Scan > Import Scan Data**.
2. Navigate to the location of the scan data file and click **Open**.
3. Enter the same password that was created earlier in the process.
4. The scan has now been queued and will be processed by the ConsoleServer.

NetWitness Endpoint ConsoleServer Logs During a Scan

At all times, the NetWitness Endpoint ConsoleServer displays a log of events with information concerning the agent connections and transactions.

During a scan the following messages may be displayed:

- **posthello**: Initial communication between the agent and server upon agent's installation.
- **postdataprimer**: Following a scan request, the agent performs a basic set of checks and retrieves the driver list (if this category is part of the scan).

Following the reception of this primary report and if no debugger is found attached, the server sends the decryption key back to the agent so it can continue with the rest of the scan.

- `postdatacomplete`: The agent sends the rest of the scan data. This is where most of the information will be inputted in the database.

All other exception and error messages coming from the NetWitness Endpoint ConsoleServer and SQL are shown in the console log. These include program exceptions, SQL problems, connection errors, and others.

Known Compatibility Issues with Other Antivirus Programs

Sometimes, the NetWitness Endpoint scan process (both Quick scan and Full scan) takes a longer time to complete. This is because of the CPU usage by other antivirus programs (such as Windows Defender, McAfee, Norton, and so on) that may be installed on the agent machines.

To overcome this issue, it is recommended to whitelist the NetWitness Endpoint service in the antivirus program of the agent machine.

To whitelist the NetWitness Endpoint Service in Windows Defender, do the following:

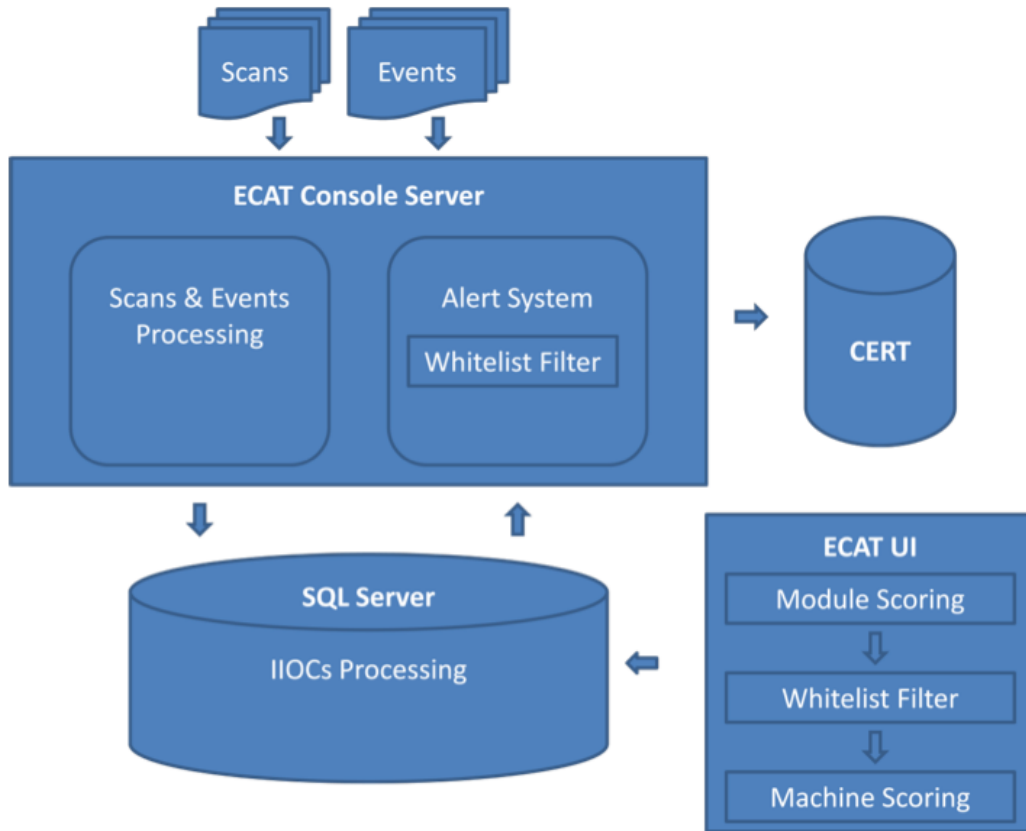
1. Select **Start > Control Panel**.
2. Select **Windows Defender**.
3. Click **Tools > Options**.
4. Select **Excluded files and folders**.
5. Click **Add** and browse for ECATService.exe.
6. Click **OK**.

INSTANTIOCS

With NetWitness Endpoint, Instant Indicators of Compromise (InstantIOCs or IIOCs) are SQL scripts run automatically on the NetWitness Endpoint server as data is processed from the NetWitness Endpoint agents. IIOCs are not looking for specific file-level information such as known-bad MD5 hash, which can be easily modified by attackers. Instead, IIOCs are looking for generic behavior that is typically indicative of malware. By looking for suspicious activity instead of file-level information, NetWitness Endpoint is able to detect new, targeted malware that has never been seen before. The IIOCs included with NetWitness Endpoint enable security analysts to quickly query the NetWitness Endpoint database to find files matching specific attributes. These IIOCs help to reduce the amount of data an analyst must sift through, making it easier and faster to detect threats in the environment. NetWitness Endpoint comes with a wide variety of out-of-the-box IIOCs, and analysts can create their own customized versions.

Description	Level	Type	Active	Alertable	Machine Count	Module Count	Last Executed	Black Listed Count	White Listed Count	User Defined	Error Message
Unsigned writes to...	2	Event	<input checked="" type="checkbox"/>	<input type="checkbox"/>	0	0	03/09/2014 9:42:04 AM	0	0	<input type="checkbox"/>	
Unsigned writes to...	2	Event	<input checked="" type="checkbox"/>	<input type="checkbox"/>	0	0	03/09/2014 9:42:04 AM	0	0	<input type="checkbox"/>	
Unsigned writes to...	2	Event	<input checked="" type="checkbox"/>	<input type="checkbox"/>	0	0	03/09/2014 9:42:04 AM	0	0	<input type="checkbox"/>	
Unsigned writes to...	2	Event	<input checked="" type="checkbox"/>	<input type="checkbox"/>	0	0	03/09/2014 9:42:04 AM	0	0	<input type="checkbox"/>	
No antivirus notific...	3	Machine	<input checked="" type="checkbox"/>	<input type="checkbox"/>	0	0	03/09/2014 9:42:02 AM	0	0	<input type="checkbox"/>	
No firewall notifica...	3	Machine	<input checked="" type="checkbox"/>	<input type="checkbox"/>	0	0	03/09/2014 9:42:02 AM	0	0	<input type="checkbox"/>	
Windows update n...	3	Machine	<input checked="" type="checkbox"/>	<input type="checkbox"/>	0	0	03/09/2014 9:42:02 AM	0	0	<input type="checkbox"/>	
Warning on post r...	3	Machine	<input checked="" type="checkbox"/>	<input type="checkbox"/>	0	0	03/09/2014 9:42:02 AM	0	0	<input type="checkbox"/>	
Hooks registry acce...	3	Module	<input checked="" type="checkbox"/>	<input type="checkbox"/>	0	0	03/09/2014 9:42:03 AM	0	0	<input type="checkbox"/>	
Duplicate section n...	3	Module	<input checked="" type="checkbox"/>	<input type="checkbox"/>	1	10	03/09/2014 9:42:03 AM	0	0	<input type="checkbox"/>	
Empty section name	3	Module	<input checked="" type="checkbox"/>	<input type="checkbox"/>	0	0	03/09/2014 9:42:03 AM	0	0	<input type="checkbox"/>	
Compiled in last m...	3	Module	<input checked="" type="checkbox"/>	<input type="checkbox"/>	1	25	03/09/2014 9:42:02 AM	0	0	<input type="checkbox"/>	
No file description	3	Module	<input checked="" type="checkbox"/>	<input type="checkbox"/>	1	1	03/09/2014 9:42:03 AM	0	0	<input type="checkbox"/>	
Autorun	3	Module	<input checked="" type="checkbox"/>	<input type="checkbox"/>	1	152	03/09/2014 9:42:03 AM	0	0	<input type="checkbox"/>	
File access denied	3	Module	<input checked="" type="checkbox"/>	<input type="checkbox"/>	0	0	03/09/2014 9:42:03 AM	0	0	<input type="checkbox"/>	
Beacon	3	Module	<input checked="" type="checkbox"/>	<input type="checkbox"/>	1	2	03/09/2014 9:42:03 AM	0	0	<input type="checkbox"/>	
Network access	3	Module	<input checked="" type="checkbox"/>	<input type="checkbox"/>	1	9	03/09/2014 9:42:03 AM	0	0	<input type="checkbox"/>	
Bytes sent ratio	3	Module	<input checked="" type="checkbox"/>	<input type="checkbox"/>	1	1	03/09/2014 9:42:03 AM	0	0	<input type="checkbox"/>	
High connection c...	3	Module	<input checked="" type="checkbox"/>	<input type="checkbox"/>	1	1	03/09/2014 9:42:03 AM	0	0	<input type="checkbox"/>	
Image mismatch	3	Module	<input checked="" type="checkbox"/>	<input type="checkbox"/>	0	0	03/09/2014 9:42:03 AM	0	0	<input type="checkbox"/>	
Temporary directory	3	Module	<input checked="" type="checkbox"/>	<input type="checkbox"/>	0	0	03/09/2014 9:42:03 AM	0	0	<input type="checkbox"/>	
File not found	3	Module	<input checked="" type="checkbox"/>	<input type="checkbox"/>	1	145	03/09/2014 9:42:03 AM	0	0	<input type="checkbox"/>	
Network listen	3	Module	<input checked="" type="checkbox"/>	<input type="checkbox"/>	1	7	03/09/2014 9:42:03 AM	0	0	<input type="checkbox"/>	
Notification regist...	3	Module	<input checked="" type="checkbox"/>	<input type="checkbox"/>	1	13	03/09/2014 9:42:03 AM	0	0	<input type="checkbox"/>	
Filter device	3	Module	<input checked="" type="checkbox"/>	<input type="checkbox"/>	1	61	03/09/2014 9:42:03 AM	0	0	<input type="checkbox"/>	
Module hidden in ...	3	Module	<input checked="" type="checkbox"/>	<input type="checkbox"/>	0	0	03/09/2014 9:42:03 AM	0	0	<input type="checkbox"/>	
Process access deni...	3	Module	<input checked="" type="checkbox"/>	<input type="checkbox"/>	1	10	03/09/2014 9:42:03 AM	0	0	<input type="checkbox"/>	
AppData directory	3	Module	<input checked="" type="checkbox"/>	<input type="checkbox"/>	0	0	03/09/2014 9:42:03 AM	0	0	<input type="checkbox"/>	
ProgramData direct...	3	Module	<input checked="" type="checkbox"/>	<input type="checkbox"/>	0	0	03/09/2014 9:42:03 AM	0	0	<input type="checkbox"/>	
Packed	3	Module	<input checked="" type="checkbox"/>	<input type="checkbox"/>	0	0	03/09/2014 9:42:04 AM	0	0	<input type="checkbox"/>	
In uncommon direc...	3	Module	<input checked="" type="checkbox"/>	<input type="checkbox"/>	1	37	03/09/2014 9:42:04 AM	0	0	<input type="checkbox"/>	
No file extension	3	Module	<input checked="" type="checkbox"/>	<input type="checkbox"/>	0	0	03/09/2014 9:42:04 AM	0	0	<input type="checkbox"/>	
Uncommon execut...	3	Module	<input checked="" type="checkbox"/>	<input type="checkbox"/>	0	0	03/09/2014 9:42:04 AM	0	0	<input type="checkbox"/>	
Unsigned company...	3	Module	<input checked="" type="checkbox"/>	<input type="checkbox"/>	0	0	03/09/2014 9:42:02 AM	0	0	<input type="checkbox"/>	
Unsigned driver	3	Module	<input checked="" type="checkbox"/>	<input type="checkbox"/>	0	0	03/09/2014 9:42:04 AM	0	0	<input type="checkbox"/>	

IIOC queries are run on the NetWitness Endpoint Server so results come back very quickly, and you can even query data from disconnected endpoints because the latest information from all endpoints is maintained in the NetWitness Endpoint database.



In NetWitness Endpoint, the IIOC SQL scripts query the database containing the scan data and monitored events that have been sent from each user agent deployed in the environment. All data available in the database can be used when creating an IIOC, and it mainly consists of:

1. Scan data
 - Live (processes, DLLs, Drivers)
 - Inventory (Autoruns, Services, Tasks, Hosts, Files, Registry Configuration)
 - Anomaly (Hooks, Suspicious Threads, Registry Discrepancies)
2. Monitors
 - File Monitor
 - Registry Monitor
 - Process Monitor
 - Thread Monitor

- Object Monitor
- Network Monitor

Note: IIOCs use current machine data, which consists of last scan data and events identified by the NetWitness Endpoint Behavior Tracking system.

Additional information about IIOCs is provided in the following topics:

- [Levels of IIOCs, IIOC Scores, and Risk Score](#)
- [Types of IIOCs](#)
- [Persistent and Non-Persistent IIOCs](#)
- [Active IIOCs](#)
- [Edit or Create IIOCs](#)
- [Whitelist Machine IIOCs](#)

Levels of IIOCs, IIOC Scores, and Risk Score

To enable users to efficiently prioritize suspicious endpoints and investigate, NetWitness Endpoint provides a scoring mechanism based on the behavior that was seen. Each endpoint will have an aggregated suspect score, which is calculated based on the suspect scores of all modules found. The suspect scores are calculated based on the IIOCs that triggered. The IIOCs have pre-assigned threat levels based on the perceived threat from the detected suspicious behavior. See the following sections for more detail.

IIOC Levels

IIOCs are looking for generic behavior that is typically indicative of malware, and there are different levels of IIOCs based on how suspicious the behavior is considered. IIOCs have four possible levels, ranging from 0 to 3.

IIOC Level	Severity Number	Severity Color	Description
CRITICAL	0	Black	Confirmed infection
HIGH	1	Red	Highly suspicious activity
MEDIUM	2	Orange	Activity might be suspicious
LOW	3	Yellow	More informational, but could be suspicious

Module IIOC Scores

A module IIOC score (0-1024) is calculated by counting the number of L0, L1, L2, and L3 IIOCs triggered by a module and applying bitwise operations. Here is a figure to represent the mapping between IIOC levels and the module scores.

Level	L0	L1			L2				L3		
Bit	11	10	9	8	7	6	5	4	3	2	1
Range	1024	128-1023			8-127				0-7		
Max IOCs	1	7			15				7		

We can see from the above mapping that the module score only accounts for a maximum of 7 IIOCs for Level 1, a maximum of 15 IIOCs for each of Level 2, and a maximum of 7 IIOCs for Level 3.

The following table gives more information:

Score	Name	Color	Description
0	Clean	Green	No IIOCs have been triggered on this object.
1-7	Low	Yellow	One or more IIOCs of Level 3 have been triggered on this object. Level 3 IIOCs are informative and potentially linked to minor malware behavior.
8-127	Medium	Orange	One or more IIOCs of Level 2 plus one or more IIOCs of Level 3 and have been triggered on this object. Level 2 IIOCs are good indicators of abnormal activity but might lead to false positives.
128-1023	High	Red	One or more IIOCs of Level 1 plus one or more IIOCs of Level 2 and Level 3 have been triggered on this object. Level 1 IIOCs are high indicators of compromise.
1024	Critical	Black	One or more IIOC of Level 0 (critical) has been triggered. Needs immediate attention.

Note: When a module triggers at least one IIOC Level 0 (critical), it immediately gets a score of 1024, the highest score possible.

Calculate the Module IIOC Score

You can manually calculate the score using the following formula:

$$\text{MIN}((\text{MIN}(\text{L3}, 7) + (\text{MIN}(\text{L2}, 15) * 8) + (\text{MIN}(\text{L1}, 7) * 128) + (\text{MIN}(\text{L0}, 1) * 1024)), 1024)$$

Note: This formula is used to ensure that an IIOC level never gets overridden by a lower one: A module triggering a single IIOC of level 1 will always score higher than a module triggering multiple IIOCs of level 2.

Machine IIOC Scores

A machine IIOC score is aggregated based on the module scores. It is calculated using the same bitwise operations as for the module score, but instead of applying it on the IIOCs having triggered on a module, it is applied on the distinct IIOCs (that is, the same IIOC will only count once for a machine) having triggered on a machine.

Note: IIOCs on whitelisted modules are excluded before calculating the machine score. Therefore, IIOCs on whitelisted modules will not affect a machine score even though those modules have a score.

Risk Score

A risk score is a data-driven score that ranges from 0 to 100. This score is the output of a machine-learning algorithm and represents the probability of the module being malicious.

The components that factor into the risk score are (in order of priority):

1. Machine Learning Model
2. Module Status (Whitelisted, Blacklisted)
3. Certificate Status (Whitelisted, Blacklisted)
4. IIOC Level 0
5. Reputation
6. OPSWAT
7. YARA

A score of 100 corresponds to a known bad file, while a score of 0 corresponds to a known good file. The risk score is updated every 30 seconds on average.

There is a hierarchy for how the risk score may be overridden, as following:

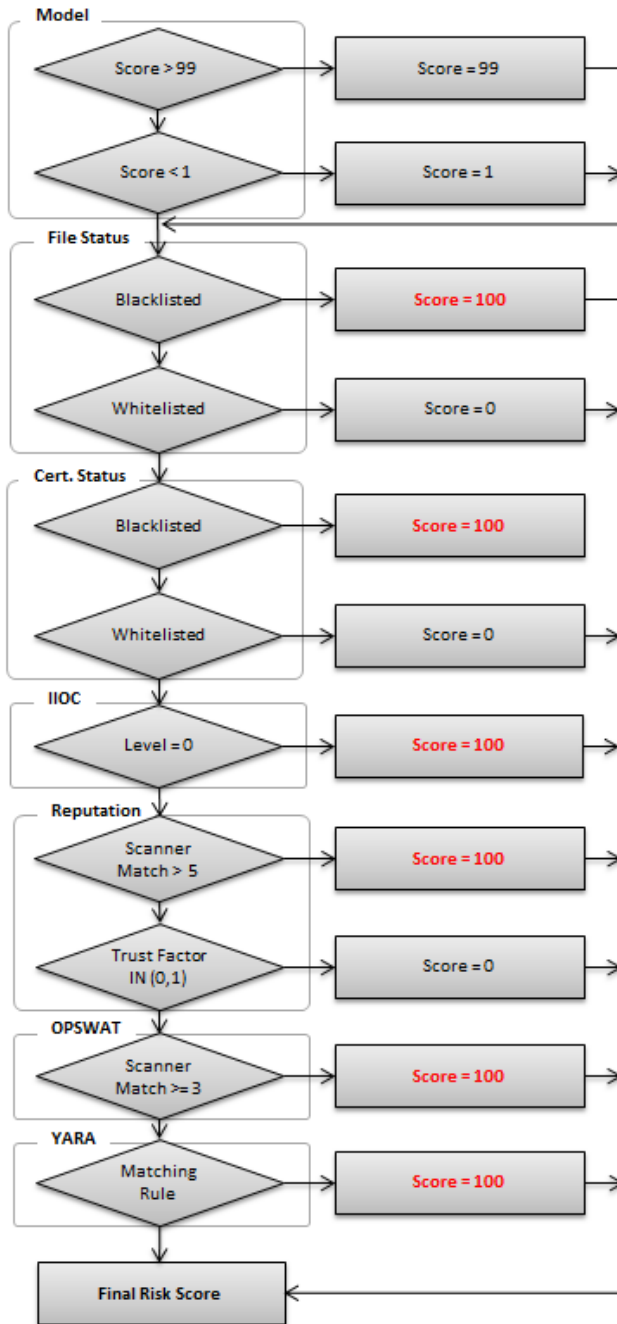
1. If file is blacklisted, risk score is overridden with 100.
2. If file is whitelisted, risk score is overridden with 0.
3. If certificate is blacklisted, risk score is overridden with 100 (for modules with this certificate).
4. If certificate is whitelisted, risk score is overridden with 0 (for modules with this certificate).
5. For modules with IIOC Level 0, risk score = 100

6. If module was scanned by reputation service and scanner match > 5 , then risk score = 100
7. If module was scanned by reputation service and trust factor in $(0, 1)$, then risk score = 0
8. If module was scanned by OPSWAT and scanner match ≥ 3 , then risk score = 100
9. If module was scanned by YARA and rule was matched, then risk score = 100

The priority of these rules is reflected in the diagram shown below.

The blacklisting/whitelisting rule has the highest priority. For example, if a file was whitelisted and also reported as infected by YARA, the risk score would be 0 because the whitelisting rule has a higher priority.

The following flow diagram illustrates the risk score override process.



Differences between IIOC Score and Risk Score

Both IIOC score and risk score use IIOCs that are triggered on modules to generate a score. Both scores have their own strengths and weaknesses.

The IIOC score is based on human-defined weights (that is, IIOC level) to compute the score, whereas the risk score (for Windows machines) is based on weights determined by a model trained on both blacklisted and whitelisted modules.

The strength of the IIOC score is that it is adaptive and takes into account user-defined IIOCs as well as adjustments made on IIOCs level. Hence, the analyst has good control over the score. The IIOC score can be more powerful with capable hands and with the whitelisting facility. However, the weakness is that it considers all IIOCs of the same level to be equal. This generates more noise than desirable.

The strength of the risk score is that it provides more granularity and is more precise. It does not rely completely on the IIOC level defined, but rather sets its own levels for each IIOC according to the data on which it was trained. However, the weakness is that it needs to have seen malware trigger an IIOC to account for it in the score. Hence, it can fail to detect malware if the behaviors were not present in the data used for training the model.

To summarize, the IIOC score captures a wider range of behaviors (that is, higher sensitivity), whereas the risk score is more precise.

Types of IIOCs

IIOCs can be categorized by type, which can be an important consideration when analyzing IIOC results. The following sections provide more details on the different types of IIOCs.

Event IIOCs

Event IIOCs describe the behavior of a module. This data comes from the tracking module in the NetWitness Endpoint agent itself. The agent is monitoring the behavior of the running modules and looking for certain behaviors that are relayed to the NetWitness Endpoint server through its tracking data. The NetWitness Endpoint agent has the following behavior monitors:

- File Monitor
- Registry Monitor
- Process Monitor
- Thread Monitor
- Object Monitor
- Network Monitor

The following figure shows the events that triggered the Event IIOC "Mounting Remote Share with Explicit Credentials," as displayed in the Scan Data tab for a machine:

The screenshot shows the NetWitness Endpoint interface for machine AD1. The 'Scan Data' tab is active, displaying a table of events. A red box highlights two entries:

Event Time	Source Module File Name	Target Process File Name	Target Command Line
7/15/2015 4:25:29.614 PM	cmd.exe	net.exe	net use x: \\10.20.30.5\c\$ "P@ssw0rd" /user:besadmin
7/15/2015 4:25:29.692 PM	conhost.exe	net.exe	net use x: \\10.20.30.5\c\$ "P@ssw0rd" /user:besadmin

Summary statistics from the interface:

- Registry Discrepancies: 0 Suspect
- History: 102
- Network: 102
- Tracking: 151 Suspect
- Total: 151 items total

Administrative Status: 143 Score (Last Seen Just Now)

Machine IIOCs

Machine IIOCs describe aspects of the host machine such as User Account Controls (UAC) being disabled or the Hosts file containing Fully Qualified Domain Names (FQDNs). This information comes from scan data. These IIOCs are useful for examining machines that might have had configuration settings changed, and that are not standard in the environment. This could indicate malicious activity or users abusing their privileges.

The following figure indicates that the Machine IIOC "User Account Controls (UAC) disabled" (a level 2 IIOC, which will add between 8 and 127 to the IIOC score) has been triggered on three machines:

IIOC Name	Level	Category	Checked	Unchecked	Score	Count
User Account Controls (UAC) disabled	2	Machine	<input checked="" type="checkbox"/>	<input type="checkbox"/>	3	0
Limited User Account (LUA) disabled	2	Machine	<input checked="" type="checkbox"/>	<input type="checkbox"/>	3	0
Suspicious SVCHOST running	1	Machine	<input checked="" type="checkbox"/>	<input type="checkbox"/>	0	0
Registry tools disabled	2	Machine	<input checked="" type="checkbox"/>	<input type="checkbox"/>	0	0
Task manager disabled	2	Machine	<input checked="" type="checkbox"/>	<input type="checkbox"/>	0	0

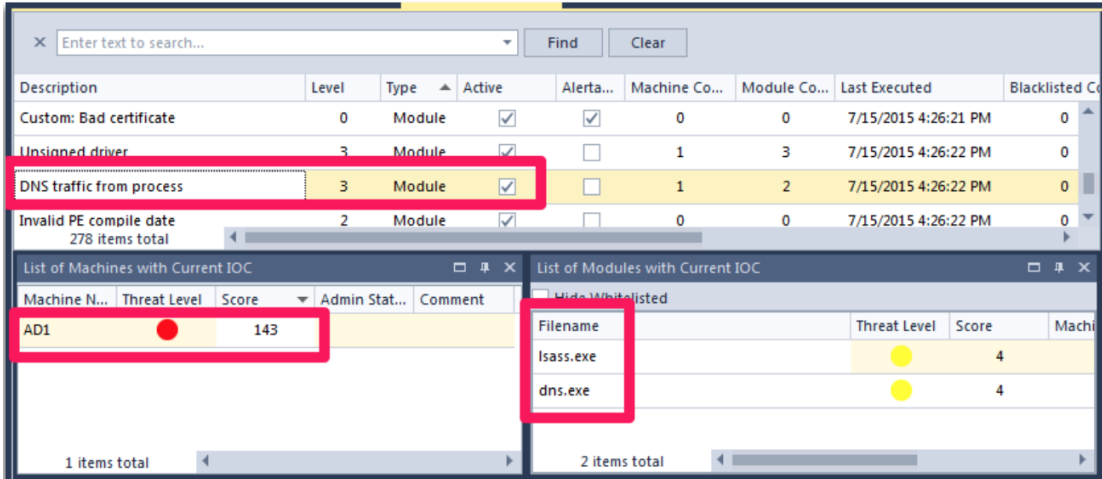
Machine N...	Threat Level	Score	Admin Stat...	Comment
WIN7-VICTIM	●	447		
ECAT	●	159		
CORP08912...	●	151		

Module IIOCs

Module IIOCs describe technical aspects of a module and are generated from scan data. Scan data includes the following aspects of the running machine:

- Live (processes, DLLs, drivers)
- Inventory (autoruns, services, tasks, hosts, files, registry)
- Anomaly (hooks, suspicious threads, registry discrepancies)

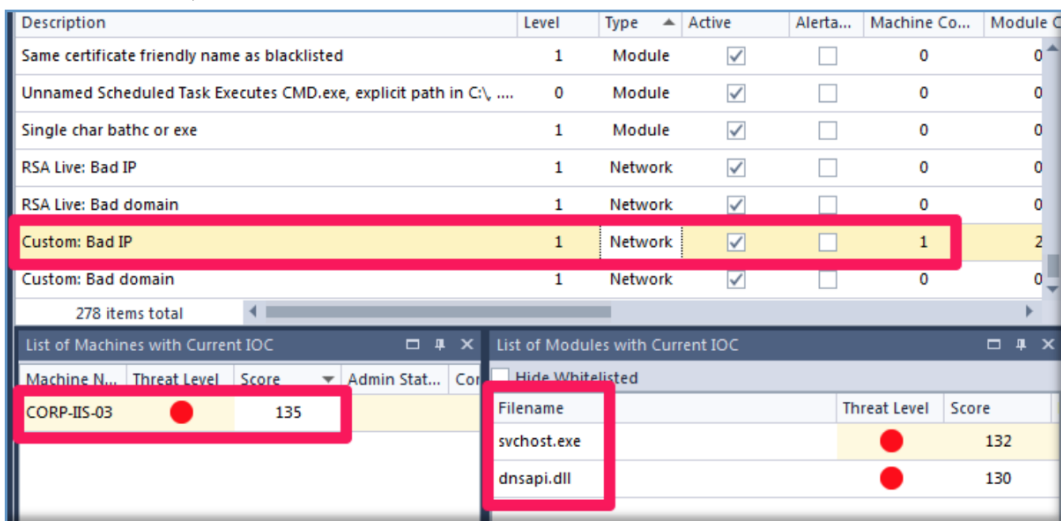
The following figure illustrates a Module IIOC. This particular IIOC is titled "DNS traffic from process" (a Level 3 IIOC, which means it will add between 1 and 8 to the IIOC score). There is one machine on which at least module has performed DNS resolution. On that machine there are actually two modules that have performed DNS resolution.



Network IIOCs

Network IIOCs are generated from the tracking data gathered in near real-time by the NetWitness Endpoint agent. They compare the IPs and domains connected to and resolved to a blacklist specified under Tools > Import/Export > Checksums > IP and Domains, as well as blacklist data from RSA's Live content distribution system.

The following figure illustrates that on the machine "CORP-IIS-03," there are two modules that have made network traffic to IPs that have been imported and flagged as bad IPs. This particular IIOC is Level 1, which will increase the IIOC score to between 128 and 1023.



Persistent and Non-Persistent IIOCs

It is important to understand the difference between Persistent IIOCs and Non-Persistent IIOCs.

Persistent IIOCs

Persistent IIOCs are those IIOCs that, once they have triggered on an object (machine or module), will never be discarded on this object except for Event Type `IIOC`. This allows the user to get a complete picture of the object to which the IIOC relates. The more information you have on a module when investigating it, the better, as this helps you to better answer the question, “What is this module capable of?” Even though a module might not have exhibited a behavior (for example, hooking) in the last week, this does not mean it will never exhibit that behavior. In other words, if the module did something once in its life on one machine, it can do it again in the future on any other machine.

Note: Once Event Type `Persistent IIOC` triggers, it remains triggered for the number of days set in configuration. Remove Tracking Events older than the number of days defined in the Database Maintenance configuration in the User Interface.

Non Persistent IIOCs

Once a Non-Persistent IIOC triggers, it remains triggered while the condition remains in at least one of the machines.

Here are some examples of IIOCs where this applies:

- All user-generated IIOCs
- Machine IIOCs (for example, Firewall disabled, UAC disabled)
- Environmental IIOCs (for example, Present on fewer than X machines)
- Status IIOCs (for example, Blacklisted, Bad Module, Bad Certificate)
- Time-dependent IIOCs (for example, Compiled last month, Created last month)

Non-persistent IIOCs are cleared after triggering conditions are no longer present. For example, a non-persistent Event IIOC is cleared after all the tracking events that caused the IIOC to be triggered are removed by database maintenance. After non-persistent IIOCs are reset, they may be triggered again.

Active IIOCs

An active IIOC means that the IIOC will be processed during the IIOC processing phase. An IIOC needs to be active in order for it to trigger and detect the given behavior on objects during monitoring or scanning. Inactive IIOCs can be seen as exploratory or as work-in-progress IIOCs.

To activate/deactivate an IIOC:

1. In the **Main Menu**, click **InstantIOCs**.
2. Select the IIOC you wish to enable/disable.
3. In the **InstantIOC** pane, click **Edit**.
4. Check or uncheck the **Active** checkbox, as desired.
5. Click **Save**.

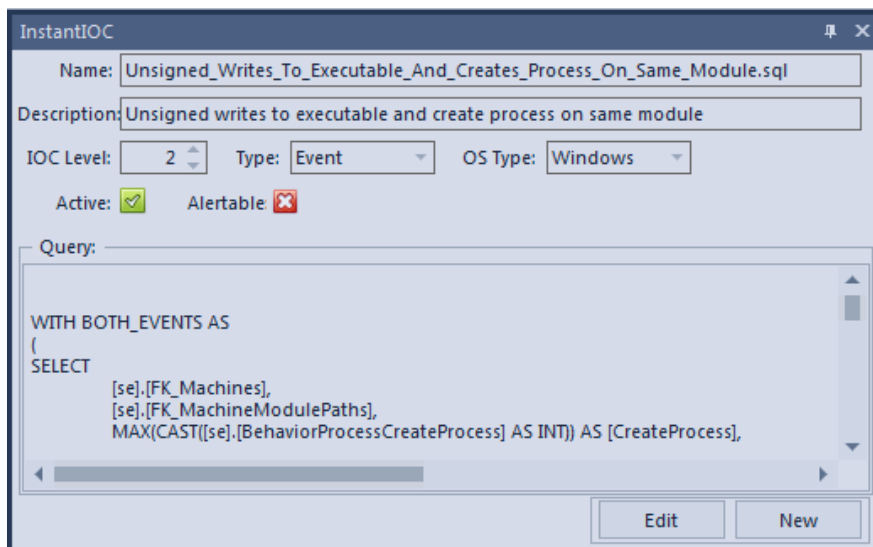
Edit or Create IIOCs

IIOCs provide tremendous flexibility and customization options for analysts.

Edit IIOCs

NetWitness Endpoint users can edit IIOCs using the IIOC editor.

Note: It is not possible to simply modify default IIOCs because these may be updated when installing service packs. If a default IIOC almost answers your need, you may clone the IIOC (by right-clicking the IIOC) and then modify the copy. This prevents your customized IIOC from being overwritten in future updates.



The screenshot shows the InstantIOC editor window. The Name field contains "Unsigned_Writes_To_Executable_And_Creates_Process_On_Same_Module.sql". The Description field contains "Unsigned writes to executable and create process on same module". The IOC Level is set to 2, Type is Event, and OS Type is Windows. The Active checkbox is checked, and the Alertable checkbox is unchecked. The Query field contains the following SQL query:

```
WITH BOTH_EVENTS AS
(
SELECT
  [se].[FK_Machines],
  [se].[FK_MachineModulePaths],
  MAX(CAST([se].[BehaviorProcessCreateProcess] AS INT)) AS [CreateProcess],
```

At the bottom right of the window are "Edit" and "New" buttons.

To edit an IIOC:

1. In the **Main Menu**, click **InstantIOCs**.
2. Right-click the IIOC you wish to edit, and select **Clone**.

3. In the **InstantIOC** pane, make the desired edits.
4. Click **Save**.

Change the Level of an IIOC

If you find that an IIOC score is too high, you may change its level:

To change the level of an IIOC:

1. In the **Main Menu**, click **InstantIOCs**.
2. Select the IIOC you wish to change.
3. In the **InstantIOC** pane, click **Edit**.
4. Change the level in the **IOC Level** field.
5. Click **Save**.

Create Your Own IIOCs

There are two ways you can create an IIOC:

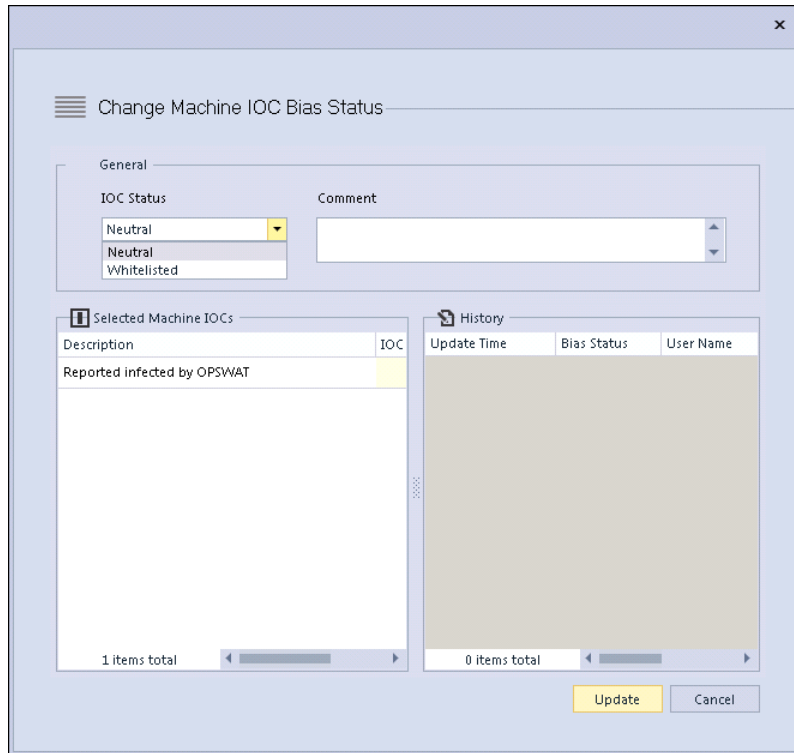
- Combine existing IIOCs using the user interface.
- Use SQL. This approach is for the advanced user with a good knowledge of SQL.

Whitelist Machine IIOCs

You can change the status of a machine IIOC to Neutral or Whitelisted from the Machine View. This option can be used if you consider an IIOC to be trusted and do not want the machine score to be impacted by this IIOC.

To whitelist a machine IIOC:

1. From the **Main Menu**, open **Machines** and select the desired machine.
The Machine View window is displayed.
2. From the Machine IIOCs displayed at the bottom of the window, identify the IIOC that will be whitelisted.
3. Right-click the IIOC you want to whitelist, and select **Change Machine IOC Bias Status**.
The **Change Machine IOC Bias Status** dialog is displayed.



4. From the **IOC Status** drop-down, select **Whitelisted**.
5. Add any comment in the **Comment** box (Optional).
6. Click **Update**. The IIOC status is changed to **Whitelisted**.

A whitelisted IIOC will not be considered while calculating the machine score. Also you will notice that the overall machine score is reduced.

INVESTIGATE RESULTS

Once you have completed the process of scanning the endpoint machines and collecting information on modules, you can begin investigating the scan results.

The first step in investigating scan results is to eliminate modules that have been trusted. A module can be classified as whitelisted, blacklisted, or graylisted. A completely clean computer will have a score of 0 after all false positives are eliminated.

There are a number of NetWitness Endpoint options and tools available to aid in investigating results, as listed below:

- [Investigation Best Practices](#)
- [Review Modules](#)
- [Whitelisting and Gold Images](#)
- [Use Filters to Find Malware](#)
- [Use IIOCs to Find Malware](#)
- [Analyze Files](#)
- [Analyze Scan Data for a Machine](#)
- [Trojan Functionality and API Calls](#)
- [Access the Module Analyzer](#)
- [Edit Module Status](#)
- [Forward to Malware Analysis](#)
- [Baselining](#)
- [Checksums](#)

Investigation Best Practices

When investigating scan results in NetWitness Endpoint, there are some best practices and tips that may help you to more efficiently identify and isolate problems.

As a general rule, you should perform at least some if not all of the following actions on a daily basis:

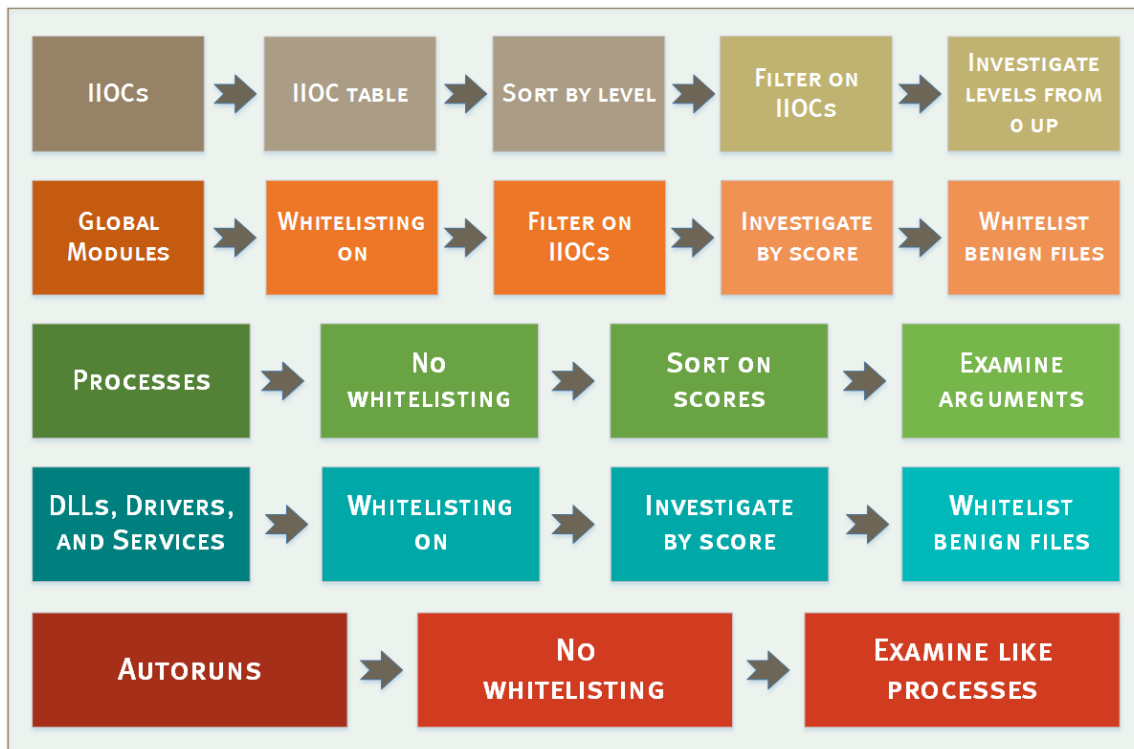
- Analyze IIOC hits (for more information see the topic [Use IIOCs to Find Malware](#)).
- Hunt for malicious files in the Global Modules window using the various behavior filters. For more information, see the topic [Use Filters to Find Malware](#).
- Investigate modules with high scores and whitelist/blacklist them. For more specific information on investigating modules, see the topics [Review Modules](#) and [Analyze Files](#).
- Develop YARA signatures for any malicious files found in the endpoints.
- Whitelist any files found to be benign during analysis. For more information, see the topic [Whitelisting and Gold Images](#).
- Research the latest threats reported by security companies in the form of blogs, research papers, or flash reports, and translate any knowledge gained from these sources into IIOCs or Yara signatures.

Any suspicious files or malware identified during the analysis should be investigated further by reviewing the endpoint's MFT, log files (such as event logs or web logs, if applicable), and registry hives.

You should also set up a virtual environment where malware analysis can be performed. This environment should be completely isolated from the Internet or the company network. It should also have a local instance of NetWitness Endpoint set up so that you can observe what footprint the malware being analyzed leaves on the system and how NetWitness Endpoint categorizes it. This type of analysis can also be used to create new IIOCs for NetWitness Endpoint.

Investigation Process Flows

The following process flows show the recommended approaches for investigating different types of items in NetWitness Endpoint.



Additional guidance and detailed information on analyzing NetWitness Endpoint scan findings are provided in the topics [Analyze Scan Data for a Machine](#) and [Analyze Files](#).

Recommended Column Configurations

The following table lists the recommended columns to use when investigating different types of items in the Global Modules table. For information on how to configure table columns and access the Column Chooser, see the topic [Main Window](#). For more information on the Global Modules table, see the topic [Modules Window](#).

File Analysis Columns	Tracking Analysis Columns	Tasks Analysis Columns	Autoruns Analysis Columns
Filename	Source Module Filename	Source Module Filename	Source Module Filename
File Size	Event	Event	Event
Machine Count	Target Module Filename	Target Module Filename	Target Module Filename
Packed	Target Module Path	Target Module Path	Target Module Path

File Analysis Columns	Tracking Analysis Columns	Tasks Analysis Columns	Autoruns Analysis Columns
Signature	Source Command Line	Arguments	Arguments
Full Path	Hidden	Registry Path	Registry Path
Days Since Compilation	File Creation (\$SI)	File Creation (\$SI)	File Creation (\$SI)
Section Names	File Creation (\$FN)	File Creation (\$FN)	File Creation (\$FN)
Hidden			
File Creation (\$SI)			
File Creation (\$FN)			

Review Modules

There are a number of places where you can access a list of modules and review associated information:

- Main Menu > Modules
- Main Menu > IP List
- Machine View > Summary Tab
- Machine View > Downloaded Tab
- Machine View > Scan Data Tab

Note: To access the Machine View, double-click a machine in the Machines list. For more information, see [Machine View](#).

Each row in the list of modules is color-coded according to the module status:

- **Whitelisted** refers to a module that is manually marked as safe. Whitelisted modules have a green threat level. The module will not be considered suspicious during the suspect index calculations, although the module retains its threat level, score, and suspect reason information. For more information, see [Whitelisting and Gold Images](#).

- **Blacklisted** refers to a module that is marked as suspicious, such as when a virus is found by OPSWAT Metascan. Blacklisted modules are highlighted in red.
- **Graylisted** refers to a module that is put aside for later review. Graylisted modules are highlighted in gray. The module will be considered whitelisted when the suspect index is processed. It will behave as a whitelisted module with a different color that will not be hidden when the **Hide whitelisted** option is selected.
- **Neutral** refers to a module that has not been given a status by the user. (Its status is unchanged from the scan.)

The Modules list includes the following column headings.

Column	Description
IIOC Score	<p>The score is a numeric identifier used to indicate the machine’s level of potential compromise.</p> <p>Each suspicious behavior is given a weight. Suspicious behavior includes unknown modules, hidden files, hooks, and other results extracted from the NetWitness Endpoint agent’s analysis.</p> <p>The score is the sum of all suspicious behaviors in all the machines where the module was found. For example, if the score is 4 on one machine and 15 on another machine, and if these suspect reasons are the same, the score will be at least 15. If the suspect reasons are not the same, the score could be higher (for example, 19).</p> <p>This measurement is a very good indicator of a module requiring attention. Nevertheless, it is not an exact measurement, and even legitimate modules can have a score. This is when the whitelisting mechanism proves to be extremely useful.</p> <p>Whitelisting a module will not change the score or threat level of a module, but it will affect the overall score of the machine.</p> <p>On the other hand, blacklisting a module will increase the suspect reasons for that particular module, further increasing the module's score.</p>
Machine Count	<p>Indicates the number of different machines where this module was found. If a module is present on all machines, it may be present on the original installation image, or has been intentionally widely deployed. If a module is only present on one agent, and a thousand agents are checked, it is likely that this module is suspicious and requires more investigation.</p>

Column	Description
Signature	<p>Describes the presence, absence, validity, and source of the digital signature of this module.</p> <p>The information reports who has digitally signed the module and if the signature was verified or not. Since it is fairly easy to insert a trusted root into a Windows system and sign malware code with it to make it look as if it comes from Microsoft or another trusted source, NetWitness Endpoint implements the whole validation process at the server level.</p> <p>The hash, the whole certification chain, and the catalogue information are gathered from the machine and sent to the server. NetWitness Endpoint performs an online check with Microsoft, VeriSign, and other trusted root authorities for CRL (Certificate Revocation Lists) and validation. If the module is not signed by a trusted root or if the whole certification chain cannot be validated, NetWitness Endpoint flags the module accordingly.</p>
Hash Lookup	The classification of the module, based on its hash, from one or more databases.
Risk Score	A data-driven score that ranges from 0 to 100. This score is the output of a machine-learning algorithm and represents the probability of the module being malicious. For more information, see Levels of IIOCs, IIOC Scores, and Risk Score
Compile Time	Tells when the module was compiled.
Automatic Bias Status Assignment	Indicates if the module has been automatically assigned a bias status. For more information, see Automatic Status Assignment .

Floating Code

Floating code can be defined as a section of executable code found in memory that cannot be associated to any known driver, process, or DLLs. It is also a common hiding technique used by rootkits to avoid being traced. Floating code in kernel memory is not attached to any known driver, while floating code in user process memory cannot be linked to any loaded DLLs.

The presence of floating code is typical and may indicate that a malware is using an existing trusted process to conceal its presence.

Example of Kernel Floating Code

A kernel driver rootkit loads, allocates a block of kernel memory, copies the executable code in that block, and starts a system thread pointing to it. It then unloads from memory and wipes itself from the disk, leaving no traces of its presence.

User-Mode Floating Code

User-mode floating code has been known and used for years by malware. Typically, a malware allocates a block of memory (VirtualAllocEx) into a target process (for example, Internet Explorer), copies the code, and starts a remote thread pointing to the code. The running code then resides inside Internet Explorer and its connections are thought to be legitimate.

Another example of floating code is MetaSploit/Meterpreter. The MetaSploit framework can be used to craft a specially formed PDF file that will trigger a buffer overflow into unpatched versions of Acrobat Reader. The Meterpreter code is executed and then connects back to the attacker's system. In this case, the code uses the running Acrobat thread to be executed.

Floating code can also be created by loading a DLL through a method called reflective DLL loading. This method uses a program to inject a DLL (stored as an encrypted resource) into a process (that is, from kernel space) without dropping a file or triggering an OS notification. NetWitness Endpoint can locate and identify these memory loaded DLLs.

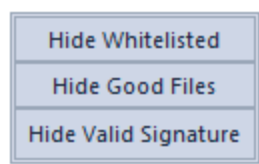
In NetWitness Endpoint, floating code blocks are clearly identified and can be found in the Process DLLs list. When a floating DLL is found, its Process Environment Block (PEB) information is hashed in order to identify copies of the same module across the entire environment.

Hide Certain Files

Hiding certain files, particularly whitelisted files, known good files, or files with a valid signature, allows users to focus on only those files that may present a risk.

To hide whitelisted files, known good files, or files with a valid signature:

1. Open the desired machine.
2. Click one or more of the following buttons to the right of the **Machine Identification** section:
 - **Hide Whitelisted**
 - **Hide Good Files**
 - **Hide Valid Signature**



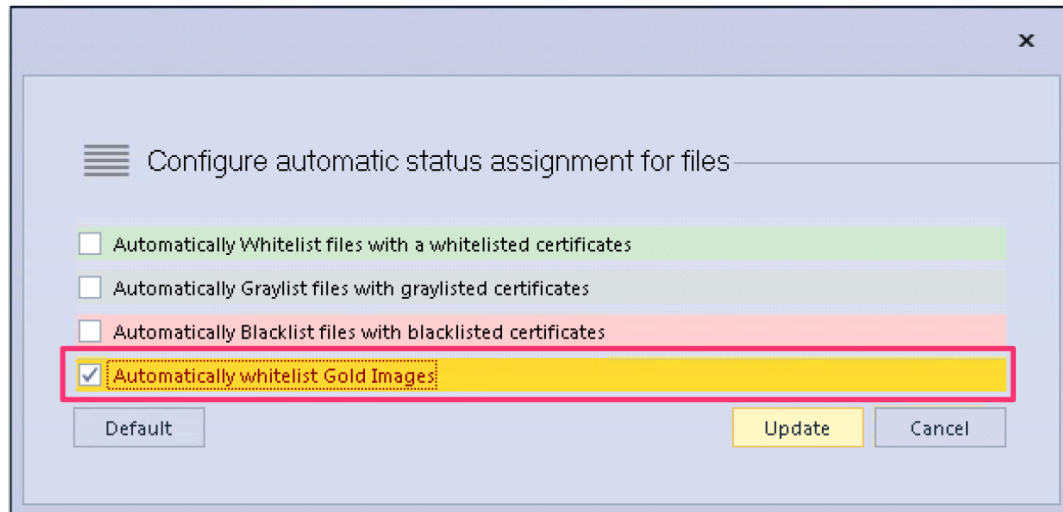
Whitelisting and Gold Images

As you use NetWitness Endpoint on a daily basis, you should spend some time categorizing files by either whitelisting or blacklisting them. If your company has a standard workstation or server build (commonly referred to as a Gold Image), you should deploy NetWitness Endpoint on this standard build, run a full scan, and then whitelist everything manually.

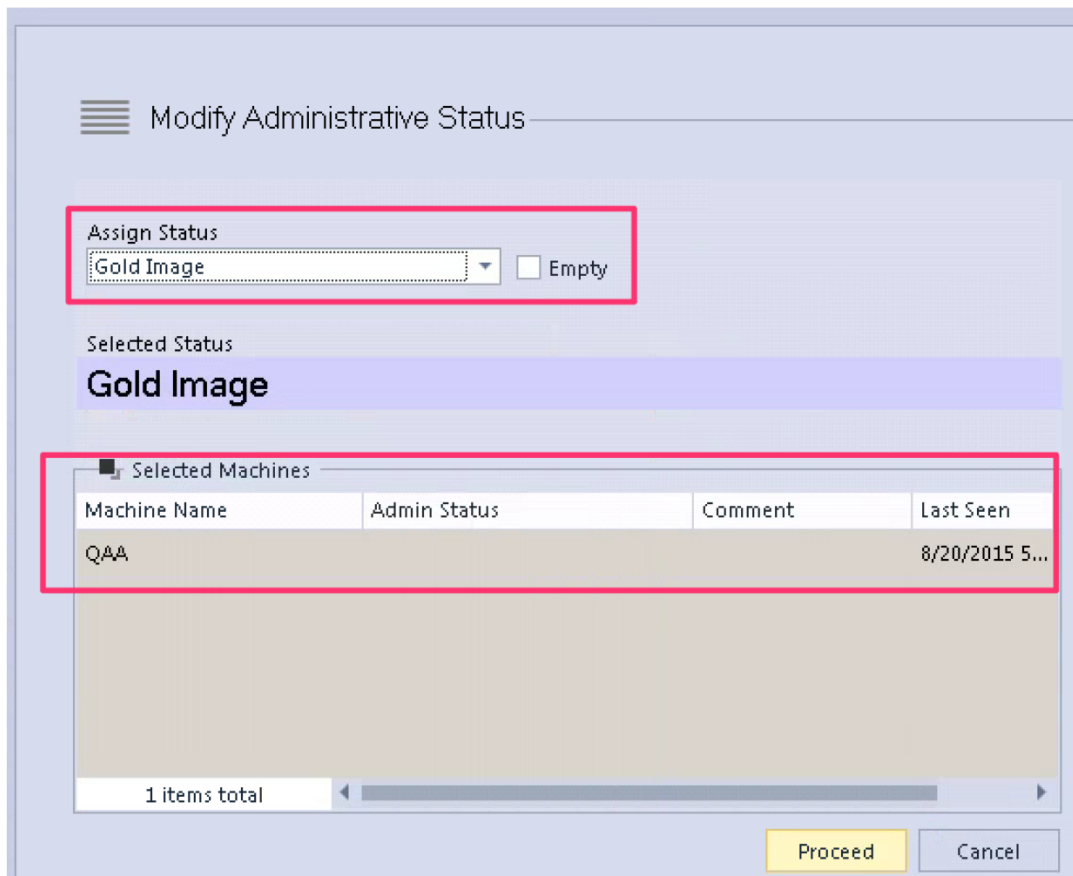
You can also automate the whitelisting of Gold Image systems by following these steps:

1. Install the NetWitness Endpoint agent on a Gold Image machine.
2. From the NetWitness Endpoint UI, start a full scan of the Gold Image machine and wait for the scan to complete.
3. From the NetWitness Endpoint UI, open the **Configure** menu and select **Automatic Status Assignment**.

The Configure automatic status assignment for files dialog is displayed, as shown below:



4. Select **Automatically whitelist Gold Images** as shown above and click **Update**.
5. In the **Machines Window**, right-click on the Gold Image machine and select **Modify Status**.
The Modify Administrative Status dialog is displayed, as shown below:



6. In the **Assign Status** drop-down list, select **Gold Image**, as shown above. The name of the Gold Image machine should be listed in the **Selected Machines** pane.
7. Click **Proceed**.
The Gold Image machine will be automatically whitelisted.
8. After the above steps have been completed, you should turn off the **Automatically whitelist Gold Images** option (step 4) to prevent you from accidentally whitelisting other systems. If that feature is turned on, and you accidentally assign the Gold Image status to the wrong system, all files under that system will also be whitelisted.

Whitelisting has many benefits for analyzing files:

1. Whitelisting saves time. When you spend time analyzing a file and determine that it is benign or malicious, you can preserve that analysis time by categorizing the file accordingly (as either whitelisted or blacklisted).
2. Whitelisting reduces the number of files you have to review and allows you to focus only on newly created files.

3. If a Gold Image is available you can whitelist it, which then greatly reduces the number of files you have to review.

When whitelisting a file or group of files, you should always add a comment as to why the file was whitelisted, such as "VirusTotal clean" or "Analyzed and looks clean" or "File is a component of X application" and so on. Doing so allows future analysts to know what logic was used to deem a file clean.

Sometimes it is easier to whitelist files in groups rather than individually. You can group files for whitelisting on the basis of a few criteria. For example, you can sort files by signature and whitelist all files signed by a trusted vendor such as Google or Apple, as shown in the figure below:

Drag a column header here to group by that column

Filename	Compile Time	Score	Machine Co...	Signature	▲ Filesize	Description	Pac
diskWiper.dll	8/22/2014 7:44:01 PM			Valid: VMware, Inc.	22.2 kB	VMware Tools di...	
vmware-unity-helper.exe	3/26/2011 12:05:30 ...	0	1	Valid: VMware, Inc.	174.6 kB	VMware Unity H...	
vmplayer.exe		2	1	Valid: VMware, Inc.	3.89 MB	VMware Player	
vm3dum64.dll		1	3	Valid: VMware, Inc.	288.1 kB	VMware SVGA 3...	
vnetlib64.dll		0	1	Valid: VMware, Inc.	908.6 kB	VMware networ...	
glib-2.0.dll		0	1	Valid: VMware, Inc.	766.6 kB	GLib	
liblber.dll		0	1	Valid: VMware, Inc.	138.7 kB		
vmware-rem...		1	1	Valid: VMware, Inc.	4.61	Trusted files based on signature...	
libeay32.dll		0	1	Valid: VMware, Inc.	1002.6 kB	OpenSSL Shared...	
sigc-2.0.dll		0	1	Valid: VMware, Inc.	55.1 kB	The Typesafe Cal...	
libldap_r.dll		0	1	Valid: VMware, Inc.	254.6 kB		
libcds.dll		0	1	Valid: VMware, Inc.	106.6 kB		
libcurl.dll		3	1	Valid: VMware, Inc.	338.6 kB		
vmdkShellE...		0	1	Valid: VMware, Inc.	60.2 kB	VMware Workst...	
zip.exe	7/17/2006 7:53:19 PM	0	1	Valid: VMware, Inc.	139.7 kB		
vmwarebase.dll	2/26/2013 2:44:12 AM	0	1	Valid: VMware, Inc.	3.99 MB	VMware base lib...	
vnetlib64.dll	3/25/2011 11:59:04 ...	0	1	Valid: VMware, Inc.	946.1 kB	VMware networ...	
vmPerfmon.dll	3/26/2011 12:23:02 ...	0	1	Valid: VMware, Inc.	525.1 kB	vmwarePerfmon ...	
zip.exe	7/17/2006 7:53:19 PM	0	1	Valid: VMware, Inc.	139.7 kB		

In addition to whitelisting and blacklisting files, NetWitness Endpoint also provides a graylist category. You can use this category however you deem appropriate. Analysts sometimes use this category to mark files that need a deeper analysis to determine if they are to be whitelisted or blacklisted. You can also use it to mark files that may be used for both legitimate and malicious purposes. For example, psexec.exe is a legitimate tool used by many administrators to execute files remotely. However, many hackers also use this tool when moving laterally from system to system. Therefore, rather than whitelisting this file, you may want to graylist it so that you can see the context under which it is used to ensure that it is not for malicious purposes.

Use Filters to Find Malware

NetWitness Endpoint leverages the SQL database to facilitate analyzing the information gathered by the NetWitness Endpoint agent quickly in a number of unique ways. This is accomplished through three main functions: faceted filtering, the table filter editor, and InstantIOCs (IIOCs).

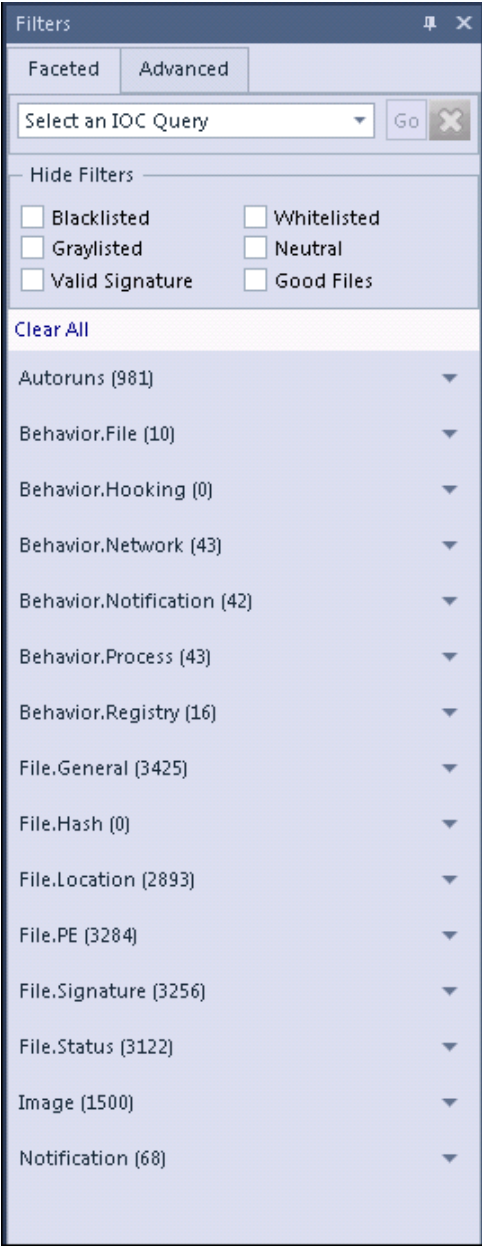
Faceted Filtering

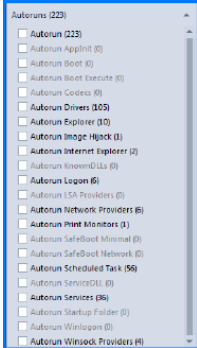
The faceted filtering options in the Global Modules list greatly facilitate identifying certain module types and behaviors. By combining filters of both the behavior aspects of the module from the Event Tracking category, as well as the typical categories of behavior that NetWitness Endpoint determines during its regular scans of the endpoint, you can efficiently identify modules of interest. For example, locating hidden files inside a temp directory can be done quickly and easily.

A useful analysis approach to the Global Modules list is to apply various filters to the data to identify suspicious/malicious files. Any files that are not deemed malicious should be whitelisted. You can use the Hide filters, such as Whitelisted and Good Files, to reduce the amount of data you will have to look at moving forward.

To apply faceted filters:

1. Access the Global Modules list.
2. In the **Filters** pane, shown below, check the checkboxes for the desired options.

Filters Pane	Description
	<p>The modules list will be filtered according to selected options.</p> <p>In the Hide Filters section, check the checkboxes of items you do not want to show in the Modules table. These filters help narrow the list of modules to investigate.</p> <p>Options to show provide a wide variety of categories of behaviors and characteristics to help identify modules that should be investigated. Each option will display the number of modules in the NetWitness Endpoint environment returned when querying on the selected option. Clicking the down arrow to the right of an option expands</p>

Filters Pane	Description
	<p>the option into subcategories, as shown below for the Autoruns option:</p> 

A good filter to start with is Autorun. This filter identifies all files that are set to be automatically loaded when the system is rebooted. You can then combine this filter with another, such as AppData\Local (in the File.Location category), to identify the path of the files.

As you use filters to narrow down your list of suspicious modules, selecting individual files will then display additional relevant information on the module, such all the IIOCs that apply to the module (in the Module IIOCs pane) as well as the machines on which it can be found (in the Machines pane).

Advanced Filtering

The advanced filter query allows you to apply additional query logic to the faceted filter query options.

Opening the Advanced tab in the Filters pane opens a dialog where you can add arguments to your query, as shown in the following figure. Clicking the plus sign lets you add argument lines, and within each argument you can use drop-down lists to make selections.

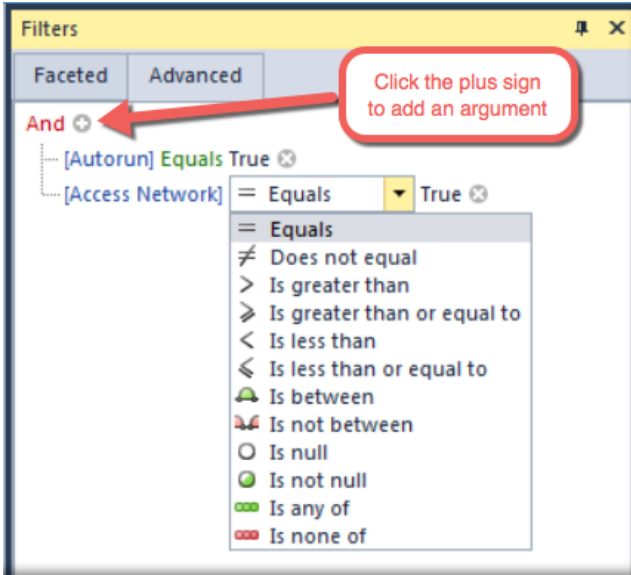
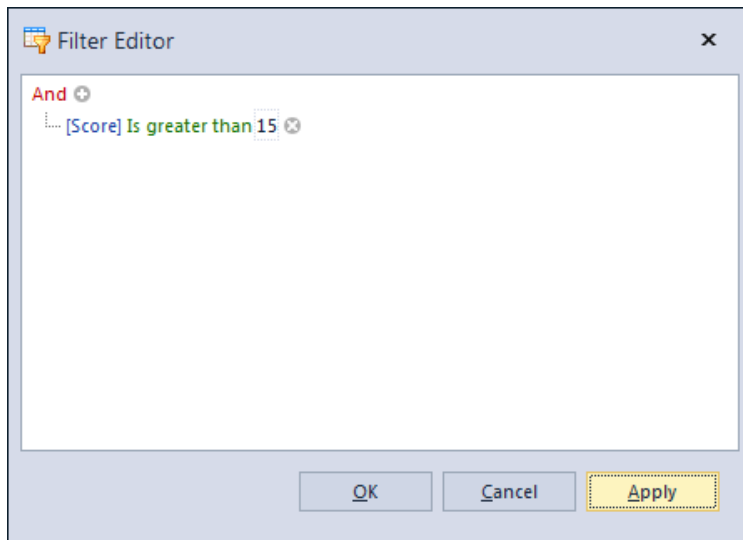


Table Filter Editor

NetWitness Endpoint’s tables offer extremely useful and efficient filtering capabilities. You can create filters from any column available in the list of modules, allowing you to see the desired information more quickly by excluding all irrelevant information from the current view. This allows for more “on the spot” filtering than faceted filtering and can greatly help when developing IIOCs.

To filter a table:

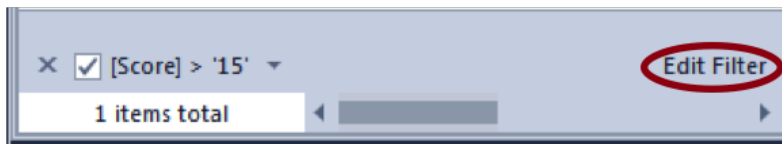
1. Right-click a column header.
2. Select **Filter Editor**.



3. Add desired parameters and click **OK** or **Apply**.

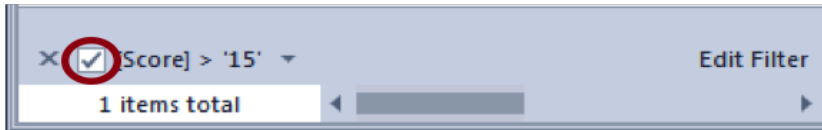
To edit a table filter:

1. Click **Edit Filter**.

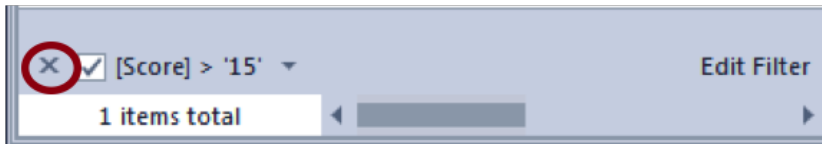


2. Perform desired edits.
3. Click **OK** or **Apply**.

To deactivate a table filter, uncheck the related checkbox at the bottom left of the table:



To delete a table filter, click the **X** associated with the filter at the bottom left of the table:



Use IIOCs to Find Malware

InstantIOCs (IIOCs) provide a way to perform more complex queries of the database, mainly by automating the environment correlation capabilities of NetWitness Endpoint. Applying an IIOC to a list of modules can narrow the list dramatically so you can focus on a specific behavior and locate affected files quickly. For example, applying the "Hidden & Beacon" IIOC identifies instances where the file or directory a process is running from is hidden from the user and the module is contacting the Internet at regular intervals, which is a very strong indication of malware.

Note: For more detailed information on IIOCs, see the topic [Levels of IIOCs, IIOC Scores, and Risk Score](#). For information on investigating by type of IIOC, see the topic [Types of IIOCs](#).

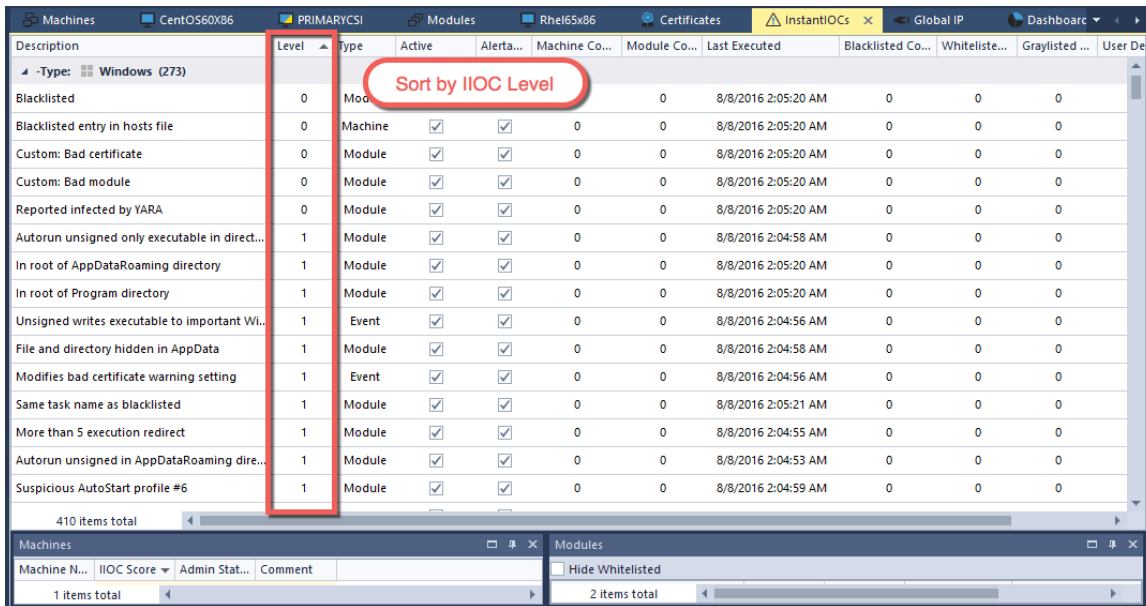
To apply an InstantIIOC:

1. Do one of the following:
 - From the **Main Menu**, open **Machines** and select the desired machine.
 - From the **Main Menu**, open **Modules**.
2. In the Filters pane, click the **Select an IIOC Query** field and select the desired InstantIIOC from the drop-down menu.
3. Click **Go**.

Note: To clear an InstantIOC, click X to the right of the **Select an IOC Query** field.

The Machines or Modules table, depending on what was displayed when applying the IIOC, will update to display only those machines or modules that match the selected IIOC query. You can combine IIOCs and faceted filtering to further refine your results.

Another way to begin your IIOC analysis is to look at the IIOC table (accessed by selecting **InstantIOCs** in the Main Menu). A good place to start is to sort the list of IIOCs by level, as shown in the following figure.



A good IIOC to start with is "Reported infected by YARA." Selecting this IIOC will populate the two panes at the bottom of the screen with the machines that matched the YARA rule and the individual module hits for those machines. Navigating to the "List of Modules with Current IOC" (lower right pane of the figure above) and sorting by Hash Lookup can help you to identify modules that match the YARA rules and investigate new hits that have not been blacklisted. After finding a new hit in YARA, you should investigate those hits on the individual systems to determine how the files got there, when it happened, and if there are any other artifacts of interest around that same time. Many of the IIOCs supplement each other and give more context around the behavior of the module but there are a few that, by themselves, can indicate malicious behavior. The following table explains some of these IIOCs.

InstantIOC	Description
Strong Indication of Malware	
Suspicious SVCHOST running	A running SVCHOST.exe module that is not signed by Microsoft.

InstantIOC	Description
Suspicious services registry entry	An ACCESS DENIED message from an @ImagePath or @ServiceDll entry.
Hidden & Beacon	The file or directory the process is running from is hidden from the user and the module is contacting the Internet at regular intervals.
Suspect thread & Network access	Threads in floating code or threads whose service table was hooked. Could indicate process injection of malicious code that contacts the network.
Floating code & suspect thread	A thread in floating code indicates process injection of malware. PlugX and Duqu 2.0 are two examples of malware that will use this technique to hide from User space tools.
Suspect thread & Hooking	Threads in floating code or threads whose service table was hooked that hooks another module. Could represent rootkit activities.
Floating module in browser process	A module that has no image on disk and is loaded into a browser could represent memory-resident malware from an exploit or code injection from another module.
Unsigned run key present once in environment	An unsigned Registry Run key that is not found elsewhere in the environment. This could represent an advanced adversary with a beachhead in the environment or commodity malware.
Written by blacklisted module	A previously blacklisted module that writes a new module. If there is an ongoing investigation and the malware has been identified this represents the attacker dropping more tools or malware onto the system.
Services in program data	A Windows service should never be run out of the ProgramData directory and is nearly always malicious.

InstantIOC	Description
Unsigned creates remote thread	An unsigned module creating a remote thread is an indicator of code injection. This can be a Trojans method of hiding from User land tools or password dumping if the target process is Isass.exe.
Unsigned copy itself as autorun	This is indicative of a dropper entrenching itself in the filesystem and then registering an autorun mechanism.
Unsigned writes executable to startup directory	This is indicative of a dropper entrenching itself in the filesystem by unpacking a Trojan to the startup directory.
Directory hidden	Module exists within a hidden directory, a common way to hide from User land tools.
Good Indication of Malware	
Runs CMD.EXE	There will be many hits for this IIOC. Explorer.exe and vmwaretools.exe will run cmd.exe for legitimate purposes. Other modules running cmd.exe should be examined, especially if they are HTTP daemons, scripting language interpreters like powershell.exe, cscript.exe, or wmiiprsvr.exe.
Runs NET.EXE	Cmd.exe will likely have many hits for this IIOC, but reconnaissance batch files or small executables running recon commands will execute this.
Runs AT.EXE	Indicates possibly lateral movement. If cmd.exe is triggered, you should pivot into the host and examine the Tasks under Scan Data to get the arguments and determine severity.
Unsigned writes executable to UNC	This is indicative of lateral movement in the environment but could also be benign. Examine which binaries were copied over and to what directories on the remote host.

InstantIOC	Description
Autorun unsigned ServiceDLL	Service DLLs are generally digitally signed by the authoring organization. Printer and camera drivers often show up with this IIOC but there shouldn't be many to sort through.
Floating module in OS process	A module that has no image on disk and is loaded into an OS process could represent code injection.
Floating module & Network access	A module in memory that has no image on disk. This could represent memory-resident-only malware. Oftentimes it is an AV product.
Reads document	Many legitimate applications will be reading documents. You should examine the binaries reading the documents as this could indicate packaging and staging of exfil data.

Analyze Files

Whenever you are looking at files, whether they are within a particular machine or in the Global Module list, you can use the following guidelines to aide in determining if a file is malicious or benign. Once you make a determination, you should take the time to whitelist or blacklist these files as doing so cuts down the amount of files to be reviewed in the future, thus preserving the time that was spent analyzing the files. When whitelisting or blacklisting a file, you should provide some comments to briefly describe why the file was categorized this way. For example, "VT clean," or "Component of X program," or "looks clean" can be used to comment a whitelisted file.

When reviewing files in one of the file categories, either within a system's scan results or the Global Module list, you should make use of the filters to hide Whitelisted, Good, and even Valid signature files, while remaining aware that even malware can be digitally signed (more on this further down). More information on reviewing a list of modules is provided in the topic [Review Modules](#)

The analysis criteria discussed in this topic are not meant to be the only indicators to use when analyzing files. Furthermore, you should also keep in mind that there could be malware that is different from what is described here. For every statement made below about malware, there are malicious files that are exactly the opposite of what statement is made. However, as you become familiar with this process you should gain confidence in identifying the majority of malware.

While any one of the indicators listed below would not be suspicious per se, a combination of them would increase the suspect level of a file and should draw your attention. You should remember that more than 99% of the files in the endpoints are benign. Of the handful of files that may be malicious, many of them should be identifiable with one or more of the indicators described below.

When looking at files, you should at least have the following columns visible for analysis (for information on using the table Column Chooser, see *Tables* in the topic [Main Window](#)):

- Filename
- File size
- Machine Count
- Packed
- Signature
- Full Path
- Days Since Compilation (or Compile Time)
- Section Names
- Hidden
- File Creation Time (only available at system level)
- Filename Creation Time (only available at system level)

It is imperative that you follow up on any suspicious or confirmed malicious file finding with a MFT analysis of the system. MFT analysis will provide a complete view of what may have introduced the file under investigation on the system, as well as what other activity occurred before and after the file appeared on the system. However, if the malicious file is introduced after NetWitness Endpoint has already been deployed, the Behavioral Tracking can help answer how the malicious file was introduced on the system.

VirusTotal

A good first step is to right-click on one or more files and select to search VirusTotal (VT) to see if the file has already been submitted. If the file has previously been submitted to VT, you know that someone else has already seen this file. If the file were to be part of an advanced attack that contained command and control (C2) information embedded in the file, then its hash would most likely be unique to your environment and therefore highly unlikely to have been submitted to VT. On the other hand, despite the shortcomings of AntiVirus (AV) programs, if 50+ AV vendors do not flag the file as malicious, that increases your level of confidence that the file is probably clean. Finally, several malicious files used by Advanced Persistence Threat (APT) actors do not have any AV hits during the early days or months of their existence, so other criteria should be used to determine if it is malicious or not, rather than solely relying on

VT.

File Path

Knowing the path of a file is important because sometimes malware authors put the file on directories where there are typically no such files. For example, if a file is at the root of **C:\ProgramData**, this is more interesting than seeing several files in **C:\Program Files***[SomeAppname]* because malicious files are typically standalone files versus a group of files in a legitimate-looking folder. For example, in the following figure, we see multiple files under the IBM folder that also have IBM Corporation in their signature (even though not digitally signed). We also see one file under the user's AppData folder (a common path where malware exists).

Filename	Threat ...	Score	Signature	Full Path
DashboardRaw...	●	1024	Not Signed	C:\Users\...ndregt\AppData\Local\DashboardRawThumbnail\DashboardRa...
[MEMORY_DLL_...	●	144	Not Signed	[MEMORY_DLL_D26362F86639E6713CEC3AE8662883B41406BEA434691C6C59AD...
[MEMORY_DLL_...	●	144	Not Signed	[MEMORY_DLL_D26362F86639E6713CEC3AE8662883B41406BEA434691C6C59AD...
lspush.exe	●	18	Valid: Hemoco Bvba	\\...fp04\Lansweeper\bin\lspush.exe
weathereye.exe	●	11	Not Signed: IBM Corporation	C:\Users\...ndregt\AppData\Local\The Weather Network\weathereye.exe
pcsws.exe	●	11	Not Signed: IBM Corporation	C:\Program Files (x86)\IBM\Client Access\Emulator\pcsws.exe
PdfPro6Hook.exe	●	9	Not Signed	C:\Program Files (x86)\Nuance\PDF Professional 6\PdfPro6Hook.exe
pcswssts.dll	●	9	Not Signed: IBM Corporation	C:\Program Files (x86)\IBM\Client Access\Emulator\pcswssts.dll
Itaswn20.dll	●	9	Not Signed: Lotus Development Cor...	C:\Program Files (x86)\IBM\Client Access\Emulator\Itaswn20.dll
hitmanpro37.sys	●	9	Valid: SurfRight B...	C:\Windows\System32\drivers\hitmanpro37.sys
pcsmgrs.dll	●	8	Not Signed	C:\Program Files (x86)\IBM\Client Access\Mri2924\pcsmgrs.dll
cwbcmsg.dll	●	8	Not Signed	C:\Program Files (x86)\IBM\Client Access\Mri2924\cwbcmsg.dll
cwbsomri.dll	●	8	Not Signed: IBM Corporation	C:\Program Files (x86)\IBM\Client Access\Mri2924\cwbsomri.dll
cwbmsgb.dll	●	8	Not Signed: IBM Corporation	C:\Program Files (x86)\IBM\Client Access\Mri2924\cwbmsgb.dll
cwbinres.dll	●	8	Not Signed: IBM Corporation	C:\Program Files (x86)\IBM\Client Access\Mri2924\cwbinres.dll
mfeavfk.sys	●	8	Valid: McAfee, Inc.	C:\Windows\System32\drivers\mfeavfk.sys

Filename

Sometimes, even the filename can be very telling of a file's character. If a file is named **svch0st.exe**, **svchost.exe**, or **svchosts.exe**, it should immediately draw your attention since someone is obviously trying to mimic the legitimate Windows file named **svchost.exe**. On the other hand, if a file has a random-looking filename, then it should also draw your attention since many Trojans write random filenames when dropping their payloads to prevent an easy search across the endpoints in the network based on filename. An example of this is shown below:

Filename	Threat Level	Score	Machine Count	Full Path
vbcchinstya.exe	●	1024	1	C:\Users\...ero\AppData\Roaming\{1C068C18-BB40-4600-D000-8528DDD7FD}\vbcchinstya.exe
[FLOATING CODE]	●	139	0	[FLOATING CODE]
btwdins.exe	●	130	13	C:\Program Files\ThinkPad\Bluetooth Software\btwdins.exe
AcroRd32.exe	●	130	134	C:\Program Files (x86)\Adobe\Reader 10.0\Reader\AcroRd32.exe
iexplore.exe	●	130	1763	C:\Program Files (x86)\Internet Explorer\iexplore.exe
rrcmd.exe	●	130	10	C:\Program Files (x86)\Lenovo\Rescue and Recovery\rrcmd.exe

Machine Count

The frequency of a file in the endpoints can be used to make a determination of whether it is a file of interest or not. For example, if a file exists on 200 systems on a 4,000-endpoint network, that would mean that 200 systems in the network have that same exact (by hash) file, and are infected. This is highly unlikely, unless the network is dealing with a worm that replicates itself automatically.

File Size

A good number of Trojans are less than 1 MB in size, and of these a great number of them are less than 500 KB. So, file size can also be used as an indicator when assessing a file.

Packed

A file with high entropy will get flagged as packed. A packed file means that it is likely compressed to reduce its size (or to obfuscate malicious strings/configuration information). If a file is packed it should draw your attention, especially if it also matches several of the other criteria described in this topic.

Signature

If a file is digitally signed by a trusted vendor, such as Google, Apple, Oracle, among others, you should feel comfortable whitelisting it. Ensure that the term "Valid:" is in the signature column before doing so, as shown below.

Filename	Threat Level	Score	Machine C...	Signature	Filesize	Description	Ha
myAgtSvc.exe	●	399	687	Valid: McAfee, Inc.	289.5 kB	Managed Services Agent	L
myAgtSvc.exe	●	395	22	Valid: McAfee, Inc.	289.0 kB	Managed Services Agent	L
mcsshield.exe	●	389	440	Valid: McAfee, Inc.	197.1 kB	McAfee On-Access Scanne...	L
mcsshield.exe	●	263	839	Valid: McAfee, Inc.	236.8 kB	McAfee On-Access Scanne...	L
WmiPrivSE.exe	●	259	222	Valid: Microsoft Windows	364.0 kB	WMI Provider Host	L
mcsshield.exe	●	259	362	Valid: McAfee, Inc.	199.5 kB	McAfee On-Access Scanne...	L
mcsshield.exe	●	259	4	Valid: McAfee, Inc.	199.1 kB	McAfee On-Access Scanne...	L
McShield.exe	●	259	1431	Valid: McAfee, Inc.	177.2 kB	On-Access Scanner service	L
mcsshield.exe	●	258	124	Valid: McAfee, Inc.	743.2 kB	McAfee Scanner service	L
Scan64.Exe	●	257	1377	Valid: McAfee, Inc.	12.3 kB	VirusScan On-Demand Sc...	L
JavaSetup8u45 (3).exe	●	151	1	Valid: Oracle America, Inc.	548.6 kB	Java Platform SE binary	L

Drag a column header here to group by that column

Trusted Vendor therefore, Whitelist

Days Since Compilation (or Compile Time)

The compile time is found within each Portable Executable (PE) file in its PE header. This timestamp is rarely tempered with, even though an adversary can easily change it before deploying to a victim's endpoint. This timestamp can be indicative of a newly created file that has been introduced to the environment. You may also compare this timestamp against the file's reported Created Time on the system. If a file was compiled a few days ago, but the timestamp of the file on the file system indicates that it was created a few years ago, then you could be dealing with a case of time stamping.

Section Names

Every PE file should have section names. If they are missing or have strange or random names, this may be indicative of a malicious file. However, if you determine that a file is malicious and its section names contain a section name that is unusual, you can leverage this information by looking for other files across the endpoints that have the same section name. Some packers create section names with the packer name, thus exposing the fact that the file has been packed with that packer. For example, the UPX packer names file sections UPX0, UPX1, and so on.

Hidden

While many files are hidden in Windows by default, when combined with other indicators, such as the file path, this condition could raise the level of suspicion for a file.

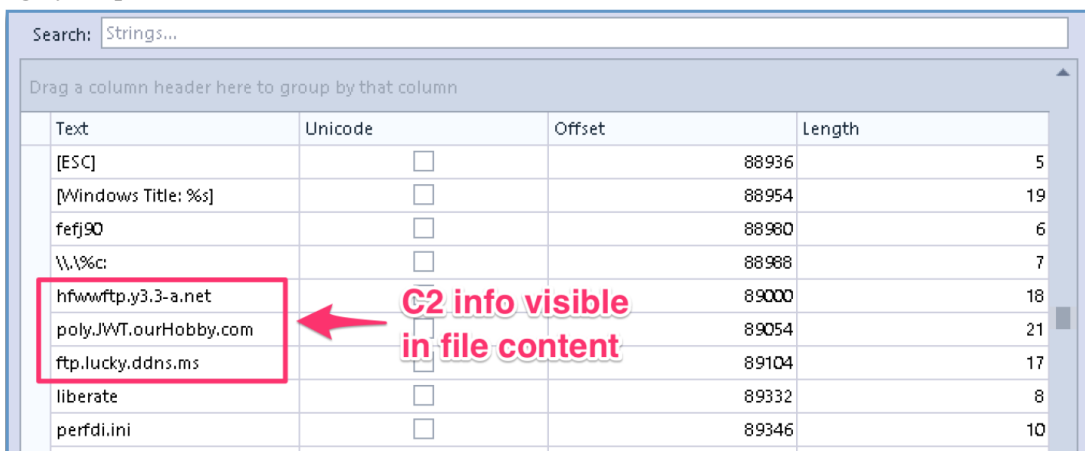
Created Times

By viewing both the \$FN Created time and \$SI Created time, you can confirm when a particular file was created on the endpoint. If there are major discrepancies between these two timestamps, then further investigation is needed.

File Content

You should look at the content of any suspicious file to further analyze it. You can access the Analyze Module feature by right-clicking on the file and selecting **Analyze Module** (for more information, see [Access the Module Analyzer](#)). When reviewing strings, look for obvious malicious strings. Accurately spotting these malicious strings does require some experience with analyzing malware. However, there are certain general criteria that may help you get started:

- If the file contains C2 information in the form of domain names or IP addresses, then that is highly suspicious, as shown below.



Search: Strings...

Drag a column header here to group by that column

Text	Unicode	Offset	Length
[ESC]	<input type="checkbox"/>	88936	5
[Windows Title: %s]	<input type="checkbox"/>	88954	19
fefj90	<input type="checkbox"/>	88960	6
\\A%c:	<input type="checkbox"/>	88968	7
hfwwwftp.y3.3-a.net	<input type="checkbox"/>	89000	18
poly.JWT.ourHobby.com	<input type="checkbox"/>	89054	21
ftp.lucky.ddns.ms	<input type="checkbox"/>	89104	17
liberate	<input type="checkbox"/>	89332	8
perfdi.ini	<input type="checkbox"/>	89346	10

- If you see company names within the file you can use these to do research on the company and the type of software it makes, then determine if there is legitimate use of that software in your environment.
- For some of the Trojans that communicate over HTTP, the adversary embeds static HTTP headers in the malicious file. An example from an actual Trojan is shown below.

00007A40	4D 6F 7A 69 6C 6C 61 2F 34 2E 30 20 28 63 6F 6D	Mozilla/4.0 (com
00007A50	70 61 74 69 62 6C 65 3B 20 4D 53 49 45 20 37 2E	patible; MSIE 7.
00007A60	30 3B 20 57 69 6E 64 6F 77 73 20 4E 54 20 36 2F	0; Windows NT 6.
00007A70	31 3B 20 54 72 69 64 65 6E 74 2F 34 2E 30 33 29	1; Trident/4.0;)
00007A80	00 00 00 00 21 61 78 65 6C 3A 20 46 61 63 6C 65	!axel: Faile
00007A90	64 20 74 6F 20 49 00 00 00 00 00 00 00 00 00 00	d to InternetOpe
00007AA0	6E 41 2C 20 25 64 00 00 00 00 00 00 00 00 00 00	nA, %d.
00007AB0	41 63 63 65 70 74 0A 20 2A 21 2A 0D 0A 51 63 63	Accept: /* Acc
00007AC0	65 70 74 2D 4C 61 6E 67 75 61 67 65 3A 20 6E 6E	ept-Language: en
00007AD0	2D 75 73 0D 0A 41 63 63 65 70 74 2D 45 6E 63 6F	-us Accept-Enco
00007AE0	64 69 6E 67 3A 20 67 7A 69 70 2C 20 64 65 66 6C	ding: gzip, defl
00007AF0	61 74 65 0D 0A 00 00 00 21 61 78 65 6C 3A 20 46	ate !axel: F
00007B00	61 69 6C 65 64 20 74 6F 20 49 6E 74 65 72 6E 65	ailed to Interne
00007B10	74 4F 70 65 6E 55 72 6C 41 2C 20 75 72 6C 3A 20	tOpenUrlA, url:
00007B20	25 73 2C 20 25 64 2E 0D 0A 00 00 00 21 61 78 65	%s, %d. !axe

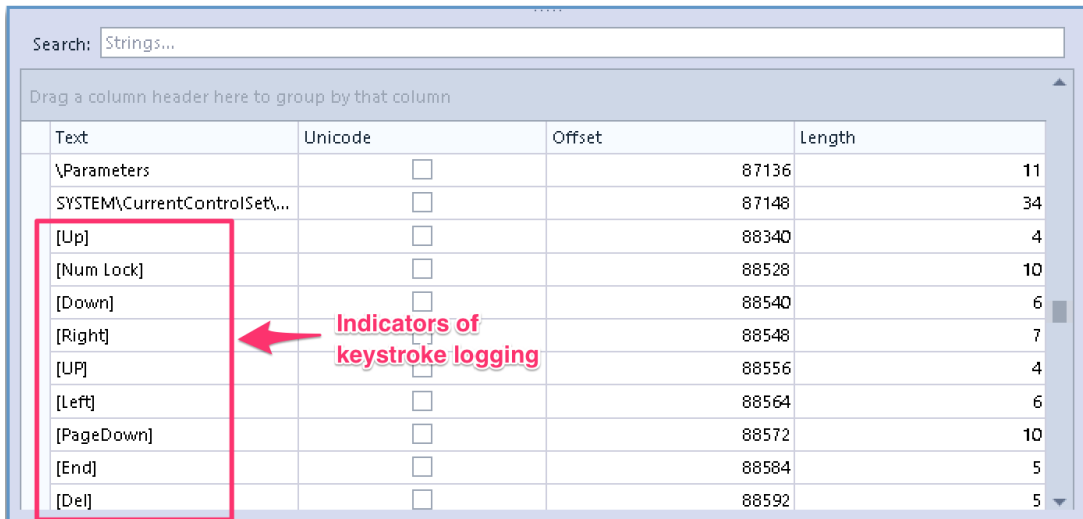
Components of a HTTP header

- Every time you see the string "cmd.exe" within a file you are investigating you should wonder why it is there. From the malware perspective, the presence of the string "cmd.exe" could be there for remote shell functionality or to execute files on the system either automatically or on demand. An example of a Trojan running several commands to collect information from the system is shown below.

00007C00	6F 20 61 78 65 6C 2E 00 0D 0A 00 00 21 69 6E 66	o axel. !inf
00007C10	6F 00 00 00 63 6D 64 2E 65 78 65 20 2F 63 20 73	o cmd.exe /c s
00007C20	79 73 74 65 6D 69 6E 66 6F 00 00 00 25 73 5F 31	ysteminfo %s_1
00007C30	00 00 00 00 63 6D 64 2E 65 78 65 20 2F 63 20 69	cmd.exe /c i
00007C40	70 63 6F 6E 66 6F 67 70 65 6C 6E 6E 6E 6E 6E 6E	pconfig /all
00007C50	25 73 5F 32 00 00 00 00 63 6D 64 2E 65 78 65 20	%s_2 cmd.exe
00007C60	2F 63 20 74 61 73 6B 6C 69 73 74 20 2F 76 00 00	/c tasklist /v
00007C70	0A 46 61 69 6C 65 64 20 74 6F 20 47 65 74 46 69	Failed to GetFi
00007C80	6C 65 41 74 74 72 69 62 75 74 65 73 41 20 6F 66	leAttributesA of
00007C90	20 72 65 74 75 72 6E 20 66 69 6C 65 2E 00 00 00	return file.

Using cmd.exe to collect information

- If you see unprintable keyboard keys listed within the file, such as: [F1], [F2], [Page Up], [Enter], [Esc], and so on, this may be indicative of a keystroke logger.



Search: Strings...

Drag a column header here to group by that column

Text	Unicode	Offset	Length
\Parameters	<input type="checkbox"/>	87136	11
SYSTEM\CurrentControlSet\...	<input type="checkbox"/>	87148	34
[Up]	<input type="checkbox"/>	88340	4
[Num Lock]	<input type="checkbox"/>	88528	10
[Down]	<input type="checkbox"/>	88540	6
[Right]	<input type="checkbox"/>	88548	7
[UP]	<input type="checkbox"/>	88556	4
[Left]	<input type="checkbox"/>	88564	6
[PageDown]	<input type="checkbox"/>	88572	10
[End]	<input type="checkbox"/>	88584	5
[Del]	<input type="checkbox"/>	88592	5

Indicators of keystroke logging

- When looking at a file you can also focus on the section names and look for strange names. Also, if the file is packed, this should raise your suspicion to some degree. The example below shows a file that is packed and has strange section names. More importantly, this file has parameters that would register this DLL in the registry, effectively entrenching it there. Common packer artifacts for UPX will be sections with the names .UPX0 or .UPX1, and VMProtect will use .VMP1 or .VMP2, and so on.

Analyze Module

Image Information

Architecture	I386/x86
Characteristics	Executable, 32-bit, DLL
Checksum	853414
Entry Point	0x001be000
Imported DLLs	0 imported functions in 0 DLLs
Section Names	,.rsrc ,.idata , , aqxjep, onesnxz
Valid PE	True

Packing Detection

Entropy	7.8937848586167227
Entry point Found	True
Image Likely Packed	True

Search: Strings...

Drag a column header here to group by that column

Text	Unicode	Offset	Length
M01V	<input type="checkbox"/>	803788	5
paXul	<input type="checkbox"/>	804472	5
DC@R	<input type="checkbox"/>	804676	4
CNBSD4.DLL	<input type="checkbox"/>	804752	10
DllCanUnloadNow	<input type="checkbox"/>	804763	15
DllGetClassObject	<input type="checkbox"/>	804779	17
DllRegisterServer	<input type="checkbox"/>	804797	17
DllUnregisterServer	<input type="checkbox"/>	804815	19
PSQV	<input type="checkbox"/>	805409	4
cb1	<input type="checkbox"/>	805461	4

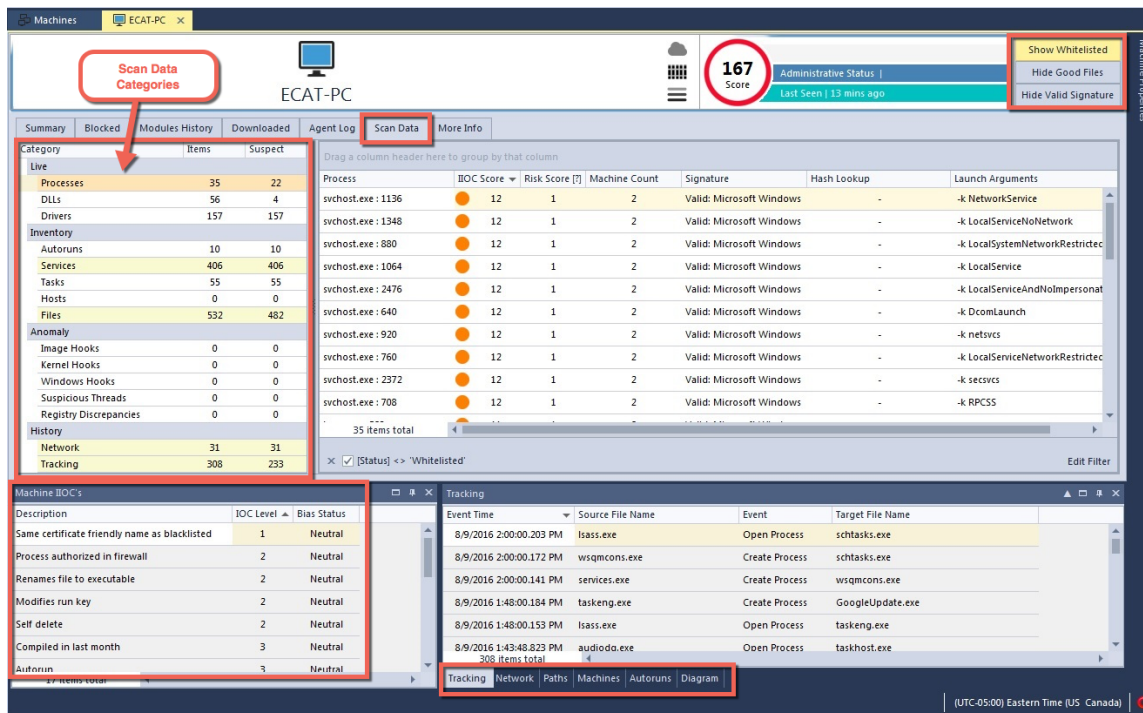
Strange looking section names

High entropy, i.e. likely packed file

The only legible strings. These parameters are executed when DLL is registered in registry with regsvr32.exe

Analyze Scan Data for a Machine

The Scan Data tab in the [Machine View](#) for a selected machine presents a breakdown of scan results, sorted by category, and tracking information for that machine, as shown in the following screen.



The following sections provide some guidelines for investigating each scan data category.

Processes

This category identifies all processes that were running when NetWitness Endpoint last scanned the system. This is only a snapshot in time and will most likely be different from scan to scan. When reviewing processes it is important to see the Launch Arguments and to NOT hide Good or Whitelisted files. Even legitimate files can be used for malicious purposes, so it is important to view all of them to determine accurately if there is any malicious activity.

For example, `rundll32.exe` is a legitimate Windows executable that is categorized as a Good file; however, an adversary may use this executable to load a malicious DLL. Therefore, when viewing processes, you need to be aware that `rundll32.exe` is running and view its arguments.

Similarly, the command line versions of the RAR and 7zip utilities are part of legitimate software; however, if the adversary was using one of these utilities to archive files for exfiltration when NetWitness Endpoint was scanning the system, you would be able to determine that exfiltration activity is occurring by simply looking at the arguments.

If you want to see more details for a particular process, you can request a process memory dump by right-click on a process and selecting **Dump Full Process Memory** (available for Windows machines only). The process memory dump is stored on the agent machine temporarily before being transferred automatically to the server. The memory snapshots are stored on the NetWitness Endpoint Server under the `Server\Files\Machines\ subdirectory. Note that the process memory dump may take a fair amount of disk space and also may fail if the agent system goes offline/asleep during the request or if the agent kernel driver fails to load.`

DLLs and Drivers

When reviewing DLLs and Drivers, you should hide Whitelisted and Good files, and even Valid Signatures, except that you should be aware that even malware can be digitally signed. The remaining files can be analyzed using the criteria described in the topic [Analyze Files](#).

Autoruns

The Autotuns category is similar to the Process category. You should Not hide any files from view, and should also ensure that the Arguments and Registry Path are visible to determine if anything suspicious has been entrenched in the system.

Services

You can leverage the filtering of Whitelisted and Good Files when analyzing this category.

Tasks

This category is also similar to Processes, and you should not hide any files from view. Additionally, you should make sure the Arguments column is visible. Below you can see an example where the legitimate Windows file **rundll32.exe** has been scheduled as a job to load a malicious DLL file with a random-looking name (**tdfyx.oja**):

Category	Items	Suspect	Filename	Arguments	Threat Level	Score	Signature	Machine Count
Inventory								
Autoruns	38	7						
Services	372	75						
Tasks	16	7	Rundll32.exe	tdfyx.oja,lmwykznx	2	2	Valid: Micro...	796
Hosts	0	0	Sc.exe	config upnphost s...= auto	2	2	Valid: Micro...	900
Files	677	283	Sc.exe	start sppsvc	2	2	Valid: Micro...	900
Anomaly			playsnlsrv.dll		1	1	Valid: Micro...	906
Image Hooks	0	0			1	1	Valid: Micro...	906
Kernel Hooks	0	0			1	1	Valid: Micro...	906
Windows Hooks	0	0			1	1	Valid: Micro...	906
Suspicious Threads	0	0			1	1	Valid: Micro...	880
Registry Discrepancies	0	0			1	1	Valid: Micro...	869
History					1	1	Valid: Micro...	896
Network	349	309			1	1	Valid: Micro...	896
Tracking	537	75			1	1	Valid: Micro...	896

Hosts

This category lists the entries found in the Windows host file:

C:\WINDOWS\system32\drivers\etc\hosts. This file can be abused for malicious purposes. For example, malware can add entries here for AV domain or search engine domain names to resolve to the loopback address so that the system will be unable to reach them. The following screen shows an example of an infected hosts file.

Summary	Downloaded	Agent Log	Scan Data	More Info	Infected host with 1000s of entries in Hosts file		
Category	Items	Suspect	Drag a column header to a different column				
Live							
Processes	129	85	Host Name	IP	Status		
DLLs	399	168	1001namen.com	127.0.0.1	Neutral		
Drivers	184	143	www.1001namen.com	127.0.0.1	Neutral		
Inventory							
Autoruns	51	50	100888290cs.com	127.0.0.1	Neutral		
Services	494	305	www.100888290cs.com	127.0.0.1	Neutral		
Tasks	32	32	www.100sexlinks.com	127.0.0.1	Neutral		
Hosts	15492		100sexlinks.com	127.0.0.1	Neutral		
Files	869	378	10sek.com	127.0.0.1	Neutral		
Anomaly							
Image Hooks	0	0	www.10sek.com	127.0.0.1	Neutral		
Kernel Hooks	695	682	www.1-2005-search.com	127.0.0.1	Neutral		
Windows Hooks	0	0	1-2005-search.com	127.0.0.1	Neutral		
Suspicious Threads	1	1	123fporn.info	127.0.0.1	Neutral		
Registry Discrepancies	1	0	010402.com	127.0.0.1	Neutral		
History							
Network	445	444	00hq.com	127.0.0.1	Neutral		
Tracking	7210	4293	www.00hq.com	127.0.0.1	Neutral		
			www.123fporn.info	127.0.0.1	Neutral		
			www.123movie download.com	127.0.0.1	Neutral		
			123simsen.com	127.0.0.1	Neutral		
			15492 items total				

Files

This category shows a full list of files found on the selected machine since NetWitness Endpoint was installed. You can filter Whitelisted and Good files to reduce the number of files to view. You can then analyze the remaining files using the criteria outlined in the topic [Analyze Files](#).

Image Hooks

These are hooks found in executable images (user-mode or kernel-mode): IAT, EAT, Inline.

Kernel Hooks

These are hooks found on kernel objects, for example, Driver Object (Pointers, IRP_MJ). This also includes filter devices.

Window Hooks

These are hooks installed using User32!SetWindowsHooksEx API.

Suspicious Threads

This category lists all suspicious threads that were found. Suspicious threads are threads whose service table was hooked. The threads could be running with either user-mode or kernel-mode privileges. These threads could be used to run malicious code inside a trusted application to execute their own code.

Registry Discrepancies

The Windows registry is a hierarchical database that stores configuration settings and options on Microsoft Windows operating systems. It contains settings for low-level operating system components as well as for applications running on the platform: the kernel, device drivers, services, SAM, user interface, and third-party applications all use the registry.

Network History

This category provides an aggregated list of network connections made on the agent machine. The list is filtered to focus on the most important connections while maintaining a reasonable database load. Statistics on the number of connections and intervals between connections are available for each item. Domain names are provided when possible, but cannot be guaranteed due to the strict timing involved.

Note: When reviewing scan results in this category you may notice some network connections being made by ECATService.exe to Microsoft sites and internal corp network using RPC Protocol. This is normal behavior and is not a cause for concern.

Event Tracking

The NetWitness Endpoint Behavior Tracking system is an active system that monitors operations and key behaviors. See "Full Monitoring and Tracking" in [Tracking Systems](#) for more information.

Trojan Functionality and API Calls

Trojans vary in functionality and complexity; however, most Trojans have one or more of the following types of functionality:

- File system traversal or manipulation
- Process enumeration, termination, or creation
- Registry enumeration or manipulation
- Network access
- GUI access

- Remote shell
- File upload or download
- Keystroke logging

This type of functionality is typically accomplished through Application Program Interface (API) calls, which are functions exported by various Windows DLLs. If the malicious file is not packed (or compressed), these types of API calls are visible to the analyst and a combination of them should raise the suspicion level of the file being analyzed. Some of the Trojan functionality listed above can be mapped to the the following types of API calls:

API Calls	Possible Trojan Functionality
GetSystemDirectoryA GetDriveTypeA GetLocalDrives DeleteFileA FindNextFileA FindFirstFileA CreateFileA WriteFileA CopyFileA	File system traversal and file manipulation such as creating, editing, deleting, or searching for files
TerminateProcessA Process32First Process32Next ShellExecuteA CreateProcessA	Process termination, enumeration, and creation
RegSetValueExA RegDeleteKeyA RegCreateKeyExA RegOpenKeyExA RegQueryInfoKeyA RegCloseKeyA	Registry enumeration or manipulation

API Calls	Possible Trojan Functionality
RegisterServiceCtrlHandlerA CreateServiceA StartServiceA QueryServiceStatus SetServiceStatus OpenSCManagerA	Windows service enumeration, creation, or configuration
InternetReadFile InternetOpenA InternetConnectA InternetOpenUrlA InternetConnectA HttpSendRequestA HttpOpenRequestA	HTTP-related API calls

Access the Module Analyzer

You can use the Module (or File) Analyzer and string search functions to retrieve and view detailed information about a downloaded module or any other module locally accessible by the NetWitness Endpoint UI.

Note: If the file is on the machine but was not yet downloaded, it can be queued for download.

To analyze a downloaded module:

- Do one of the following:
 - From the **Main Menu**, click **Downloads**.
 - From the **Machine View**, select the **Downloaded** tab.
 - Select the module to be downloaded.

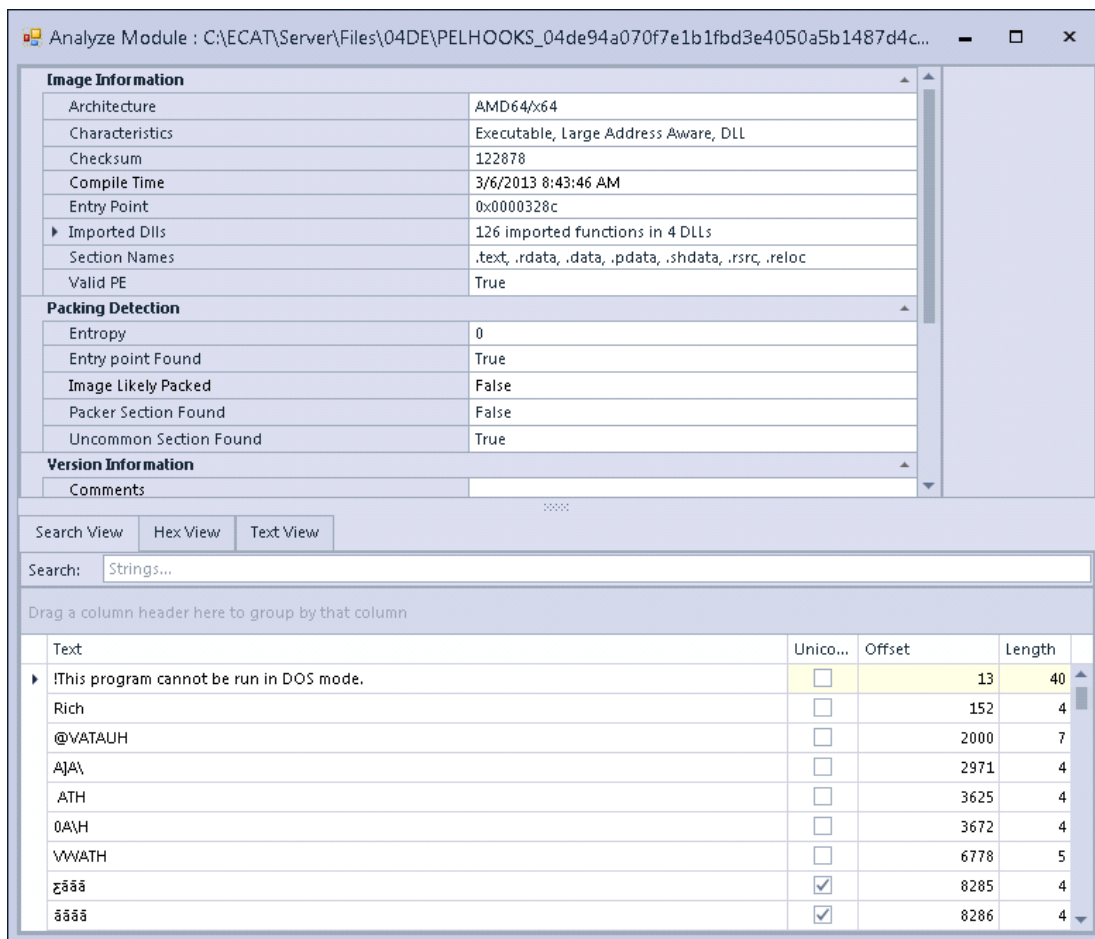
Note: Downloaded modules have the Downloaded flag set to “True” in the Module Properties pane. You can enable the Downloaded column in a table of modules by right-clicking the column headings to access the Column Chooser. Use the File.Status drop-down to select Downloaded as a column heading.

- Right-click the selected module and select **Analyze Module**.
The **File Analyzer** dialog is displayed and the file can be investigated.

3. Enter text in the **Search** field to perform a string search, and press ENTER.
You can navigate through the results using the arrow buttons or by pressing ENTER.

To analyze a saved module (locally accessible by NetWitness Endpoint UI):

1. Select **Tools > Module Analyzer**.
2. Do one of the following:
 - Navigate to the location of the file.
 - Enter a **File name**.
3. Click **Open**.
The **PE File Analysis** dialog box is displayed and the file can be investigated.
4. Enter text in the **Search View** field to perform a string search, and press ENTER.
You can then navigate through the results with the arrow buttons or by continuing to press ENTER.
5. To view the results, use the **Hex View** and **Text View** tabs to view the results in Hex format and Text format. The following figure is an example of a **File Analyzer** dialog. The table below the figure provides details about the types of information given in the File Analyzer dialog.



Field	Description
-------	-------------

Image Information

Architecture	The native machine architecture this image was compiled for (I386/x86, AMD64/x64).
Characteristics	A collection of information about the properties as indicated by the PE header of the file. It may include: No Relocation, Executable, No Live Number, No Symbols, Obsolete: Aggressive Memory Trim, Large Address Aware, Obsolete: Bytes Reversed (Low), 32-Bit, No Debug Info, Run From Swap (Removable), Run From Swap (Network), System File, DLL, Single CPU, Obsolete: Bytes Reversed (High).
Checksum	The image checksum as indicated by the PE.

Field	Description
Entry Point	The software entry point (the address where the code will start its execution).
Imported DLLs	A collection of all the functions imported from different DLLs.
Section Names	Shows all the section names found on the file. The list can include: .text, .data, .rsrc, .rdata, code, .tls, among others.
PackingDetection	
Entropy	The entropy of the image data, excluding the PE headers. It is a measure that could determine if the contents are packed (compressed or encrypted).
Entry Point Found	Indicates if the entry point address is found within a code section.
Image Likely Packed	Indicates if the image is most likely packed, based on section names found and on entropy.
Packer Section Found	Indicates if a known packer section name was found in this image.
Uncommon Section Found	Indicates if an unusual section name was present in this image.
Version Information	
Comments	The comments associated with the file, as indicated in the version resource of the file.
Company	The company that produced the file, as indicated in the version resource of the file.
Debug Mode	Specifies whether the file contains debugging information or was compiled with debugging features enabled, as indicated in the version resource of the file.

Field	Description
File Description	The description of the file, as indicated in the version resource of the file.
File Version	The file version, as indicated in the version resource of the file.
Internal Name	The internal name of the file, as indicated in the version resource of the file.
Language	The default language string for the version info block, as indicated in the version resource of the file.
Legal Copyright	The copyright notices that apply to the specified file, as indicated in the version resource of the file.
Legal Trademarks	The trademarks and registered trademarks that apply to the file, as indicated in the version resource of the file.
Original Name	The name of the file when it was created, as indicated in the version resource of the file.
Product	The name of the product this file is distributed with, as indicated in the version resource of the file.
Product Version	The version of the product this file is distributed with, as indicated in the version resource of the file.

Edit Module Status

You can edit the status of a module to be either whitelisted, blacklisted, or graylisted. Changing a status will impact all machines on which that module was found.

Note: Normally, only modules marked as suspect should have their status changed, although the system will not block the whitelisting of non-suspicious files. Whitelisting a non-suspicious module will not modify a machine score; however, blacklisting a non-suspicious module will.

To edit a module's status:

1. Do one of the following:

- Click **Modules** in the **Main Menu**.
 - Double-click the machine, access the **Summary** tab, and select the module.
2. Do one of the following:
 - Right-click the selected module or modules and select **Edit Whitelist/Blacklist Status**.
 - Select one or more modules and press **CTRL+B** to access the **Edit Blacklist-Whitelist Status** dialog.
 3. Click the **Module Status** drop-down arrow and select a status.
 4. (Optional) Edit the comment.
 5. (Optional) Change the certificate status by checking the **Change Certificate Status** checkbox and selecting the desired status from the drop-down menu.
 6. Click **Yes**.

Forward to Malware Analysis

Malware Analysis is a component of the RSA NetWitness Suite. The files retrieved by NetWitness Endpoint can be forwarded to the sandbox of your choice for further analysis. This topic provides information about forwarding suspicious files or modules to Malware Analysis (MA) for consumption and further analysis.

The Forward to Malware Analysis option is used to perform further analysis of the infected files using NetWitness Suite Malware Analysis. The Forward to Malware Analysis option is available only for downloaded modules. One or multiple downloaded modules can be selected for analysis using Malware Analysis. Once the suspicious files or modules are sent to Malware Analysis, further investigation can be done by logging into NetWitness Suite and accessing the Malware Analysis service.

The infected files/modules can be sent for analysis only if they meet the requirements of NetWitness Suite for consumption. For example, the file extension must be correct, and the file must be copied to the correct watched folder in the file share.

The supported file formats are:

- PE32 executable (.EXE), or Library (.DLL)
- Portable Document Format (.PDF)
- Office Documents (.DOC, .DOCX, .RTF, .XLS, .XLSX, .PPT, .PPTX)
- Archive and Quarantine Formats: ZIP (.ZIP) as a container. No nesting of archives.

Once the files are forwarded for analysis, they will be placed in the directory as a zip archive [with or without the password "infected"]. If required, the archive will be broken into multiple zip files if the collective size of the selected modules exceeds the limit of 100 MB.

The Forward to Malware Analysis process consists of the following steps:

1. Configure Forward to Malware Analysis
2. Perform Forward to Malware Analysis

To use this feature, make sure that:

- NetWitness Suite is installed and configured.
- Malware Analysis service is installed and configured.

Configure Forward to Malware Analysis

After installing and configuring NetWitness Suite and Malware Analysis service, you must configure NetWitness Endpoint to enable communication with Malware Analysis.

To configure Forward to Malware Analysis:

1. Share the watch directory with the NetWitness Endpoint UI machine and provide read-write access. The watch directory of Malware Analysis installation is located at `/var/lib/rsamalware/spectrum/infectedZipWatch/watch`.

Note: For more information about the watch folder, see Malware Analysis guide.

2. Make sure that the NetWitness Endpoint UI has access to the shared folder (watch directory).

Note: One way of sharing the folder is to mount the shared watch directory as a drive on the NetWitness Endpoint UI machine. Follow the standard windows procedure to map the network drive (<http://windows.microsoft.com/en-in/w...#1TC=windows-7>).

Perform Forward to Malware Analysis

To perform Forward to Malware Analysis, do the following:

1. From the **Main Menu**, click **Modules**.
The **Modules** window is displayed.
2. Locate a module that has been downloaded.

Note: Downloaded modules have the Downloaded flag set to "True" in the Module Properties pane. You can enable the Downloaded column in a table of modules by right-clicking the column headings to access the Column Chooser. Use the **File.Status** drop-down to select "Downloaded" as a column heading.

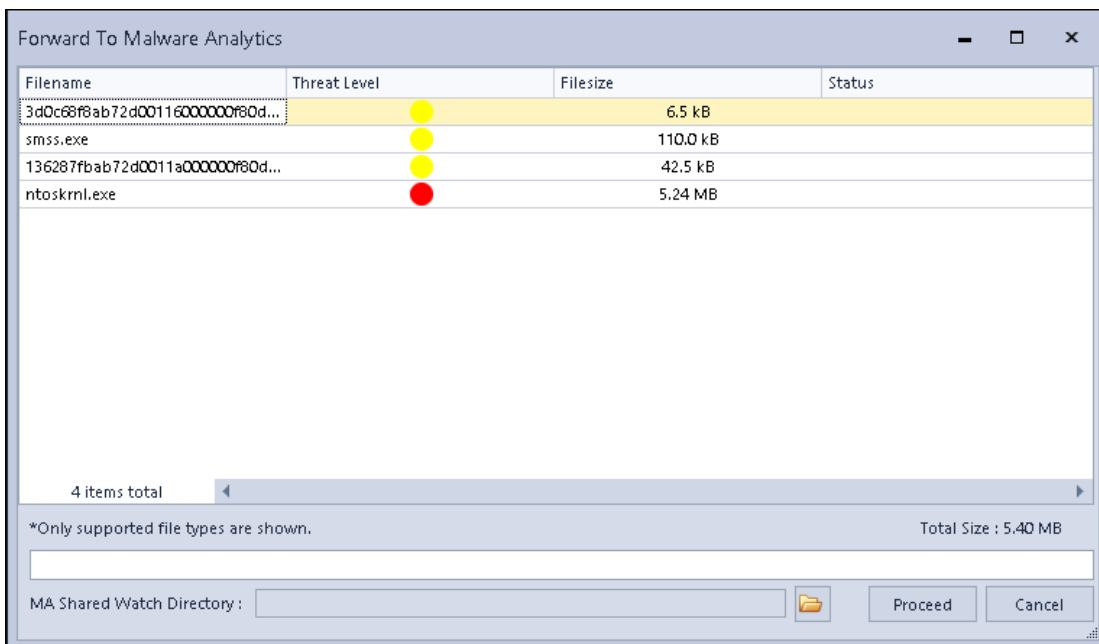
3. Do one of the following:

- Right-click a module in the Modules list.
- Select multiple modules by holding CTRL or SHIFT and right-click within the selection.

Note: The Forward to Malware Analysis can also be accessed by right-clicking the modules from the Global Downloads tab, the Machine Scan Data tab, the Machine Summary tab, or the Machine Downloaded tab.

4. Select **Malware Analysis**.

The **Forward to Malware Analytics** window is displayed as shown below.



5. Select the location of the file share where the MA watch directory is shared.

6. Click **Proceed**.

- The file is dropped into a watched file share for Malware Analysis to consume.
- Malware Analysis consumes the file and creates an on-demand job in the Scan Jobs List.

7. Log on to Malware Analysis. For more details about using Malware Analysis, refer to the following topics of NetWitness Suite Malware Analysis document:

- Upload Files for Malware Scanning
- Upload Files from a Watched Folder
- View Detailed Malware Analysis of an Event

Baselining

You can use a baseline system that represents the environment you want to assess. This speeds up the assessment process by automatically whitelisting all modules on the standard system. This is only possible in a freshly installed, clean system.

A computer can be used as a baseline at any time during an assessment.

To set up a machine as a baseline:

1. Install the NetWitness Endpoint agent on a clean computer.
2. Request a full scan and wait for the results.
3. Ensure hooks to be whitelisted have been assigned to a module.

Note: You must assign inline hooks and suspicious threads to modules to be able to give them a bias. Since hooks cannot be hashed for an MD5 to be recognized, they may have different behavior signatures on different systems. For more information, see the topic [Assign Hooks to Modules](#).

4. Manually whitelist files in the Files category with a score higher than 0.

Note: If the corporate environment contains more than one standard system configuration (for instance, Windows XP and Windows 7 machines), you may establish as many baseline computers as required.

Checksums

A checksum is a simple error detection method that ensures the integrity of a file after it has been transmitted from one storage device to another on the same network. NetWitness Endpoint uses the technique of checksums to import different types of files. NetWitness Endpoint supports importing regular files or files in STIX (Structured Threat Information eXpression) format. For more information about STIX, see <http://stix.mitre.org/>.

Note: A sample STIX file (ECAT_STIX_Sample.xml) is available at the location `C:\ECAT\Server`.

You can import the following types of files using checksums:

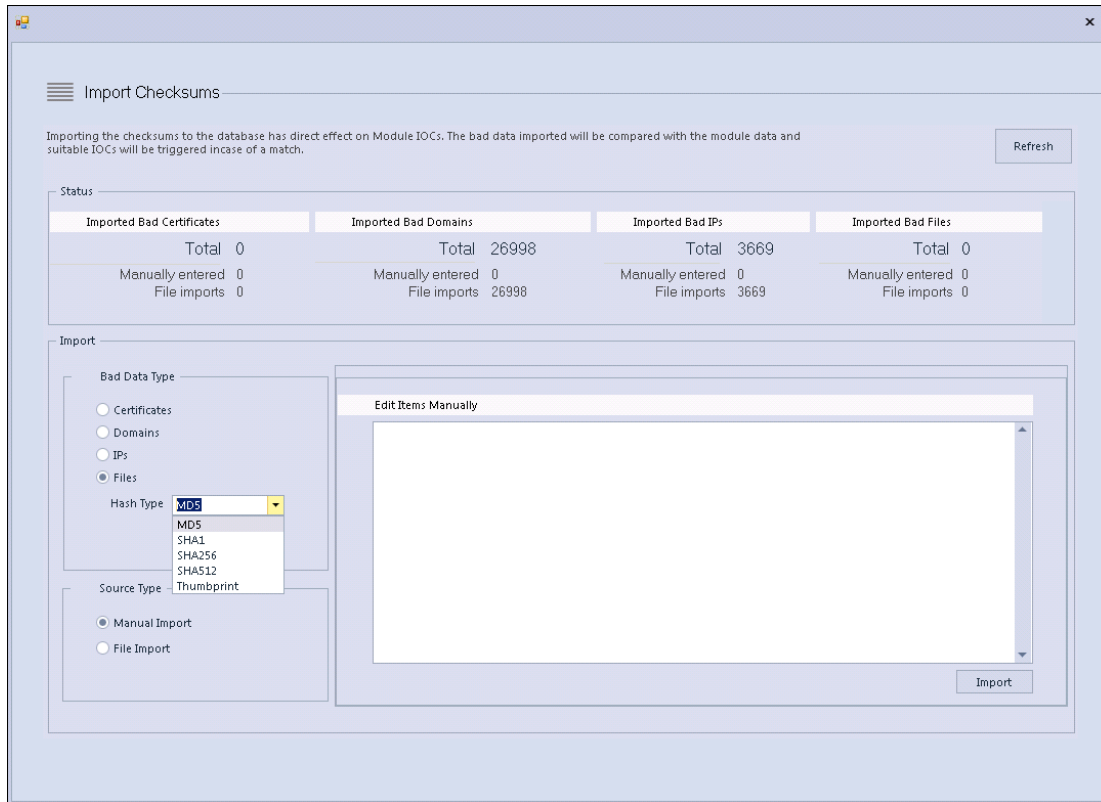
- [Bad Certificates](#)
- [Bad Domains](#)
- [Bad IPs](#)
- [Bad File Hashes](#)

Import Checksums

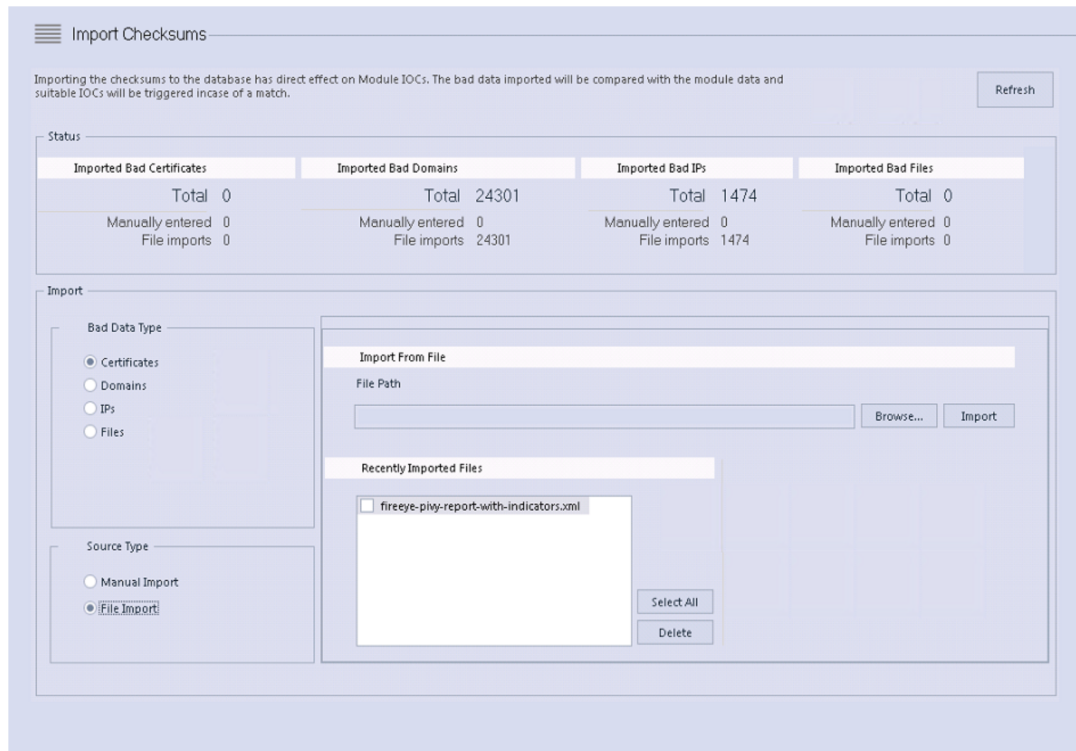
To import checksums, do the following:

1. Go to **Tools > Import/Export > Checksums**.

The **Import Checksums** window is displayed.



2. Select the type of bad data to be imported using the radio button. By default, the option "Certificates" is selected.
3. Select the type of import using the radio button.
 - If you select **Manual Import**, you must manually enter the details of the selected data type in the given space.
 - If you select **File Import**, the **Import Checksums** window is refreshed with additional options to import the file.



Click **Browse** and select the file.

Note: The file to be imported can be a regular file or a STIX file. The import function automatically detects which type of file to import.

4. Click **Import**.

The checksum is imported to the database. The imported checksums have direct impact on the IIOC of the module.

Bad Certificates

You can import bad certificates by adding checksums.

Import Bad Certificates

To import bad certificates:

1. Click **Tools > Import/Export > Checksums**.
The **Import Checksums** window is displayed.
2. From the type of data, select **Bad Certificates** using the radio button.

3. Select the type of import using the radio button.
 - If you select Manual Import, you must manually enter the details of bad certificates in the given space.
 - If you select File Import, the **Import Checksums** window is refreshed with additional options to import the file.
 - a. Select either regular file or STIX file by using the radio button.
 - b. Click **Browse** and select the file.

Note: You can import multiple entries by separating the thumbprints with a space, comma, or a new line.

4. Click **Import**.

The bad certificates are imported to the database.
5. Verify the checksums are imported:
 - If you do not receive an error message, then your checksums are imported successfully. You can verify the number of checksums currently entered using the **Status** tab.
 - If there is an error with the checksums, a warning message is displayed prompting you to continue. If you choose to continue, the erroneous checksums will be removed from the import window, and only the correct checksums are imported.

Note: Imported certificates are listed in the Import/Export window until they are removed.

Bad Domains

You can import bad domains by adding checksums.

Import Bad Domains

To import bad domains:

1. Click **Tools > Import/Export > Checksums**.

The **Import Checksums** window is displayed.
2. From the type of data, select **Bad Domains** using the radio button.
3. Select the type of import using the radio button.
 - If you select Manual Import, you must manually enter the details of bad domains in the given space.

- If you select File Import, the **Import Checksums** window is refreshed with additional options to import the file.
 - a. Select either regular file or STIX file using the radio button.
 - b. Click **Browse** and select the file.

Note: For manual import, you can import multiple entries by separating the domains with a space, comma, or a new line.

4. Click **Import**.

The bad domains are imported to the database. You can verify the number of domains currently entered by accessing the **Status** tab.

Note: Imported domains are listed in the Import/Export window until they are removed.

Bad IPs

You can import Bad IPs by adding checksums.

Import Bad IPs

To import bad IPs:

1. Click **Tools > Import/Export > Checksums**.

The **Import Checksums** window is displayed.

2. From the type of data, select **Bad IPs** using the radio button.

3. Select the type of import using the radio button.

- If you select Manual Import, you must manually enter the details of bad IPs in the given space.
- If you select File Import, the **Import Checksums** window is refreshed with additional options to import the file.
 - a. Select either regular file or STIX file by using the radio button.
 - b. Click **Browse** and select the file.

Note: For manual import, you can import multiple entries by separating the thumbprints with a space, comma, or a new line.

4. Click **Import**.

The bad IPs are imported to the database.

5. Verify the checksums are imported:
 - If you do not receive an error message, then your IPs are imported successfully. You can verify the number of IPs currently entered using the **Status** tab.
 - If there is an error with the checksums, a warning message is displayed prompting you to continue. If you choose to continue, the erroneous IP(s) will be removed from the import window, and only the correct IP(s) are imported. The IPs that are partially correct will have the correct range imported.

Note: Imported IPs are listed in the Import/Export window until they are removed.

Bad File Hashes

You can import file hashes by adding checksums.

Import Bad File Hashes

To import bad file hashes:

1. Click **Tools > Import/Export > Checksums**.
The **Import Checksums** window is displayed.
2. From the type of data, select **Files** using the radio button and select the **Hash Type** using the drop-down options.
3. Select the type of import using the radio button.
 - If you select Manual Import, you must manually enter the details of bad files in the given space.
 - If you select File Import, the **Import Checksums** window is refreshed with additional options to import the file.
 1. Select either regular file or STIX file by using the radio button.
 2. Click **Browse** and select the file.

Note: You can import multiple entries by separating the thumbprints with a space, comma, or a new line.

4. Click **Import**.
The bad file hashes are imported to the database.
5. File Hashes will continue to be listed.

6. Verify the checksums are imported:

- If you do not receive an error message, then your file hashes are imported successfully. You can verify the number of file hashes currently entered using the **Status** tab.
- If there is an error with the checksums, a warning message is displayed prompting you to continue. If you choose to continue, the erroneous file hashes will be removed from the import window, and only the correct file hashes are imported.

Note: Imported file hashes are listed in the Import/Export window until they are removed. To view them, you will need to access them by hash type, using the drop-down menu.

REMEDiate RESULTS

NetWitness Endpoint provides two powerful tools for addressing and investigating scan results that may present a threat to your enterprise.

- You can [Use the Blocking System](#) to block or quarantine infected or malicious modules across the enterprise.
- You can [Use Machine Containment](#) to isolate individual machines from the network, allowing an analyst to investigate possible threats within a machine real-time while the threat is still active.

Use the Blocking System

The NetWitness Endpoint Blocking System allows analysts to block or quarantine infected or malicious modules across the enterprise. The Blocking System is enabled by default, but a user can disable it if desired.

Note: Currently the Blocking System is supported only for Windows agents; it is not supported for Mac or Linux agents. Also, during installation, the Windows Agent must be packaged in the Packager with Advanced > Settings > Monitoring Mode set to Full Monitoring (the default value).

The NetWitness Endpoint Blocking System is a powerful tool that can protect an enterprise in a variety of ways:

- Stop or reduce the spread of identified malware, such as viruses, trojans, rootkits, worms, spyware, and adware.
- Identify attempted breach points to aid in deeper analysis; all events are time-stamped allowing analysts to trace backward to identify the entry point.
- Allow analysts to know if the situation is under control, for example, is it contained, partially contained and still progressing, are there unprotected endpoints.
- Remove nuisance software, such as adware, which can potentially mask real malware.
- For malware that loads into memory and then injects code (which NetWitness Endpoint will detect), blocking the loader will terminate it if it is currently running and prevent it from loading in the future, thus stopping all actions possible by the loader. However, a reboot is required to remove already injected code.

Caution: When making the decision to block a module, the user should consider the possibility that blocking the module could render systems or software unusable. The user should first complete appropriate testing before using this option.

Currently, the following module types can be blocked: .EXE, .COM, .SYS, .DLL, .SCR, .OCX.

Note: You will not be able to block certain modules, such as modules that are signed by Microsoft or RSA or modules larger than 100 MB. See the [Troubleshooting](#) topic for a workaround to the 100 MB module size limit.

If an analyst blocks a module that is currently running, NetWitness Endpoint will attempt to disable it. If an attempt is made to download a blocked module at the endpoint, the download will complete successfully but further access to the module will be blocked and an Access Denied message will display.

As a precaution, when blocking is enabled, if a module that the user is attempting to block is present on at least 50 machines, a warning message will be displayed and the user will be unable to complete the blocking action. This setting can be configured in the Global Parameters dialog (see below), but extreme caution should be exercised in changing this parameter. If a module has been found on at least 50 machines, it could be a vital component of the system, in which case blocking it could have unintended consequences.

The following remediation actions are provided by the Blocking System:

- **Block Only:** This option blocks a module from being written on the disk or loaded to the memory.
- **Block & Quarantine File:** This option blocks the module and moves it to the quarantine folder (C:\ProgramData\EcatService\Role-Based Access Control.

Note: The <Name> folder is an eight-letter name based on the service name, and is identical across the environment.

Enable/Disable the Blocking System

The Blocking System is enabled by default. To disable the Blocking System, use any one of the following options:

Note: For the Blocking System to work, it must be enabled in Global Parameters as well as for Machine Groups.

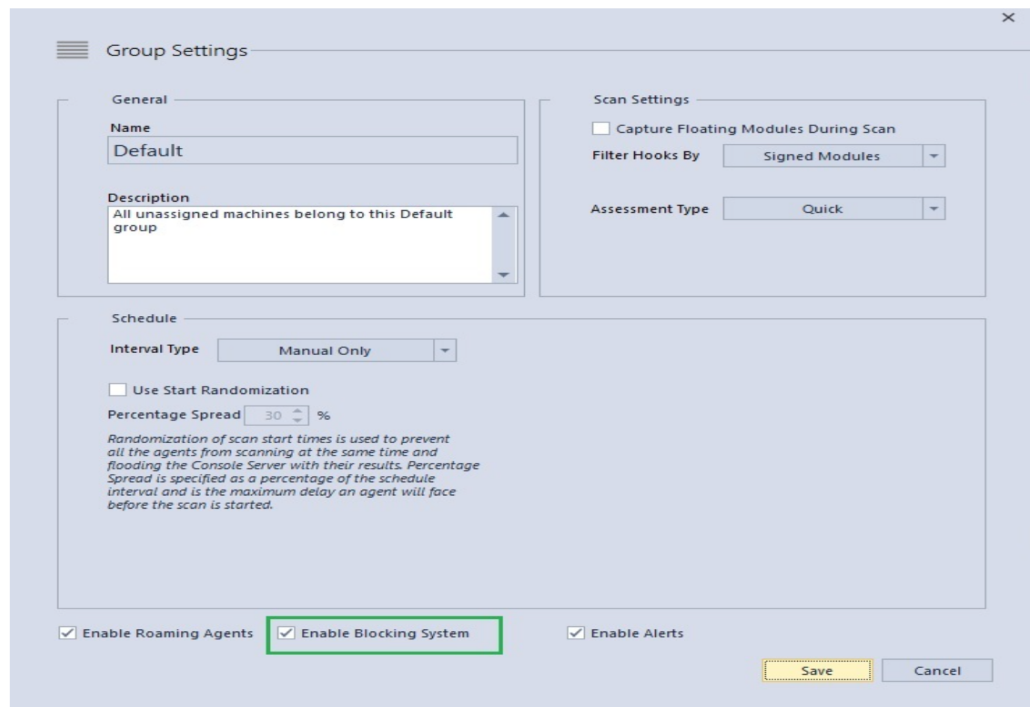
1. Using Global Parameters:
 - a. Click **Configure > Global Parameters**.



- b. To disable the blocking system, uncheck the "Enable Blocking System" checkbox.
- c. To enable the blocking system, select the "Enable Blocking System" checkbox.
- d. To change the default number for the number of affected systems at which point blocking is prevented, edit the number in the list box. Consider the implications carefully before changing this number as it could potentially affect a vital component of the system. The default value is 50.
- e. Click **OK**.

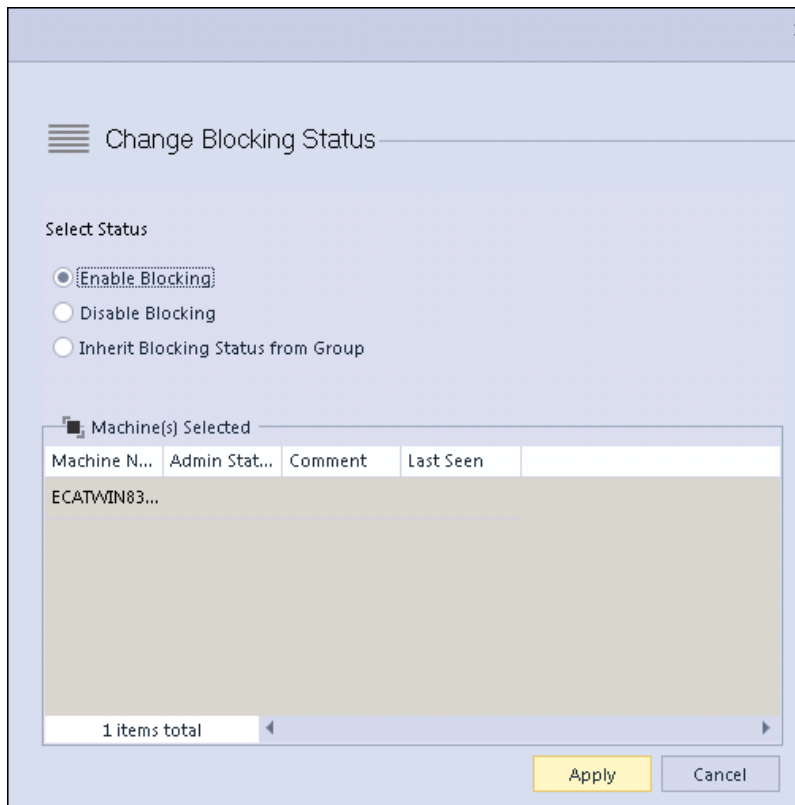
2. Using Machine Groups:

- a. Click **Configure > Machine Groups**.
- b. To disable the blocking system, right-click on **Group** and select **Edit Group**, then uncheck "Enable Blocking system" checkbox and click **Save**.
- c. To enable the blocking system, right-click on **Group** and select **Edit Group**, then check "Enable Blocking system" checkbox and click **Save**.



3. Using the Machine View:

- a. Right-click the machine and select **Blocking System**.



- b. To disable the Blocking System, select the "Disable Blocking" radio button.
- c. To enable the Blocking System, select the "Enable Blocking" radio button.
- d. You also have the option of selecting the "Inherit Blocking Status from Group" radio button, which simply means the machine will follow the selection made for the machine group to which it is assigned. This option is the initial default selection for a machine.
- e. Click **Apply**.

Identify and Block Modules

To identify the modules to be blocked, do the following:

1. Perform a scan on the agent machines (If not done already). For more information, see [Scan Your Network Environment](#).
2. Analyze the scan results and identify the malicious modules. For more information, see [Investigate Results](#).
3. Change the status of the suspicious module to either blacklisted or graylisted. See the topic [Edit Module Status](#).

Note: A module cannot be blocked using the Blocking System without first changing its status to either blacklisted or graylisted.

To block a module using the Blocking System in the NetWitness Endpoint UI:

1. Do one of the following:
 - Click **Modules** in the **Main Menu**.
 - Double-click the machine, access the **Summary** tab, and select the module.
2. Do one of the following:
 - Right-click the selected module and select **Edit Whitelist/Blacklist Status**.
 - Select one or more modules and press **CTRL+B** to access the **Edit Blacklist-Whitelist Status** dialog box.
3. The **Edit Status** window is displayed as shown below:

The screenshot shows the 'Edit Status (Malware.exe)' dialog box. It is divided into several sections:

- General:** Contains a 'Module Status' dropdown menu set to 'Blacklisted' and a 'Category' dropdown menu set to 'Generic Malware'. Below these is a 'Comment' text area.
- Remediation Action:** A checked checkbox is followed by two radio button options: 'Block Only' (selected) and 'Block & Quarantine File'.
- Certificate Status:** A dropdown menu is set to 'Blacklisted' with an ellipsis button to its right.
- History:** A table with columns for 'Status', 'Update Time', 'User Name', and 'Comment'. The table is currently empty, with a status bar at the bottom indicating '0 items total'.

At the bottom of the dialog are 'Update' and 'Cancel' buttons.

4. From the **Module Status** drop-down, change the module status to **Blacklisted/Graylisted** (if not already done).
5. From the **Category** drop-down, select the appropriate category based on the type it belongs to:

- Generic Malware
 - APT: APT (Advanced Persistent Threats) is a set of stealthy and continuous computer hacking processes, often orchestrated by humans targeting a specific entity.
 - Attacker Tool
 - Unidentified
 - Ransomware: This is a type of malware that prevents or limits users from accessing their system. This type of malware forces its victims to pay the ransom through certain online payment methods in order to grant access to their systems, or to get back their data.
6. Select the type of remediation action:
- **Block Only:** If you select this option, the module is blocked but remains in that location.
 - **Block & Quarantine File:** If you select this option, the module is blocked and moved to the Quarantine folder (**C:\ProgramData\EcatService\xxx**) on the server and can be accessed only by the user with appropriate permissions. For more information about roles and permissions, see [Role-Based Access Control](#).
7. Click **Update**.

The module gets blocked from the agent machine(s) and the status is updated in the **Machine View** window.

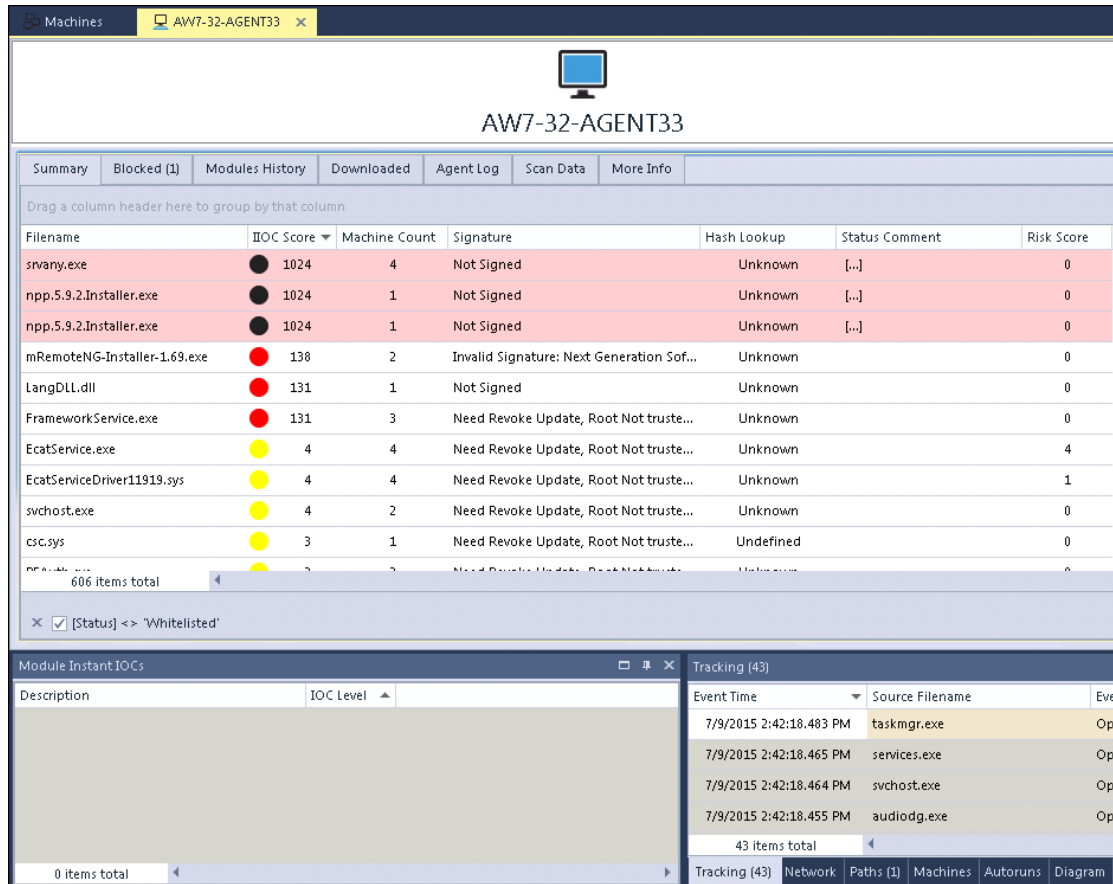
Note: The IIOC score of the blacklisted blocked module is changed to 1024 and the color is changed to black.

Note: Blocking operations can be resource-intensive, and are processed automatically once every 24 hours. If you want the blocking action to take effect sooner, from the Tools menu, select **Force Blocking State Update**. However, RSA recommends that you do not perform this action more than once per day.

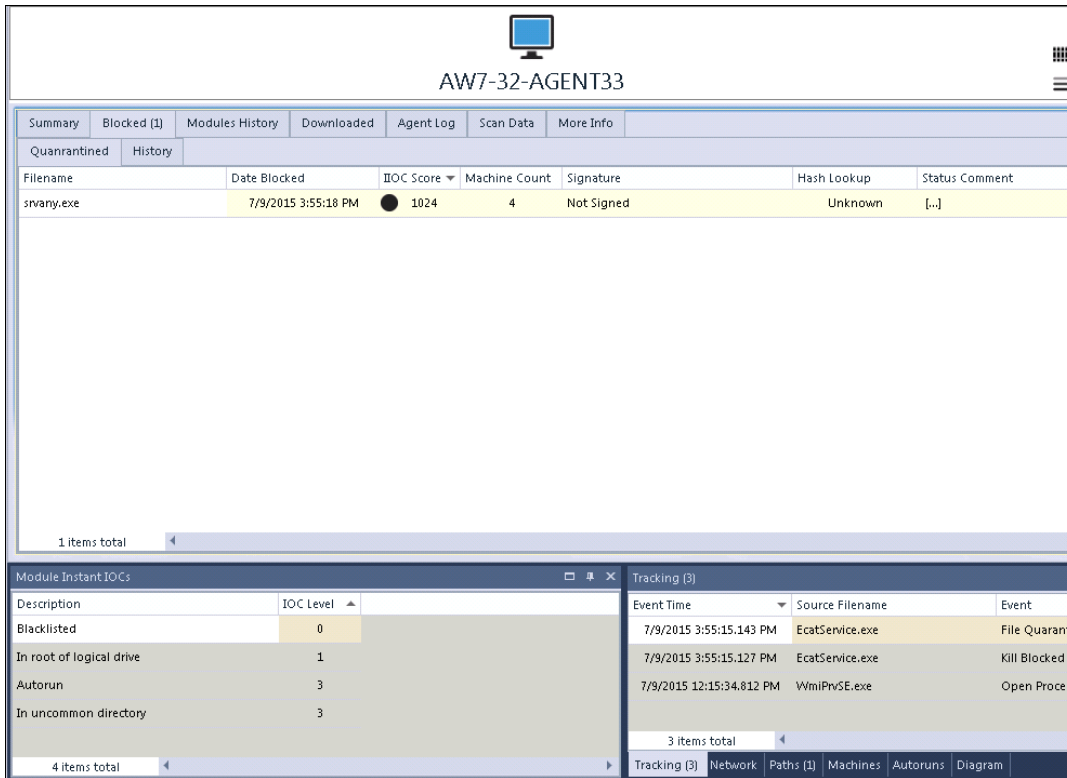
View Blocked Modules

To view the list of blocked modules and blocked history for a particular machine, do the following:

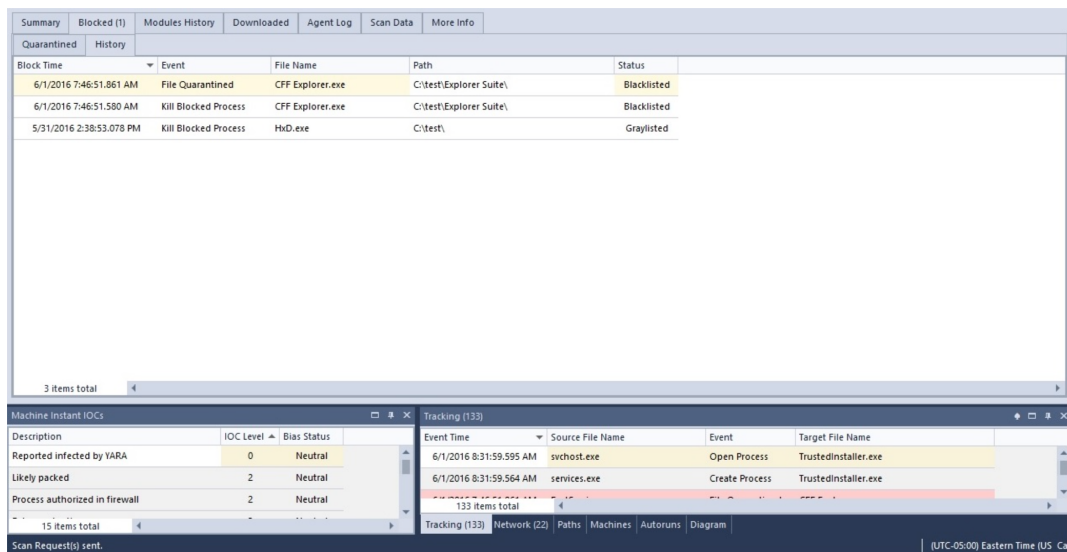
1. Open the **Machine View** window as shown below:



2. Click the **Blocked** tab.
The **Blocked** window is displayed, showing details of the blocked modules.
3. There are two tabs within the **Blocked** window:
 - The **Quarantined** tab displays the list of modules that are quarantined for a particular machine as shown below:



- The **History** tab displays the history of the blocked modules as well as quarantined modules for a particular machine as shown below:



4. Right-clicking the module from the **Blocked** tab provides various options including "Restore from Quarantine".

Restore Blocked Modules

You can restore the quarantined module and move it back to the appropriate location for usage. To do so, you must first change the blocking status of the module from the **Edit Blacklist-Whitelist Status** window.

To restore quarantined modules:

1. From the Machine View window, select the **Blocked** tab.
The **Blocked** window is displayed.
2. Select the **Quarantined** tab.
3. Right-click the module to be restored and select **Edit Blacklist-Whitelist Status**.
4. Remove the blocking option and change the module status back to Neutral or Whitelisted.
5. Click **Update**.
6. Go back to the **Machine View** and select **Quarantined** tab from the **Blocked** window.
7. Right-click the module to be restored and select "Restore from Quarantine".
The module is deleted from the quarantine folder and restored back to the server.

Unblock a Blocked Module

If you block a module by mistake or for any other reason, you can remove the blocked status by doing the following:

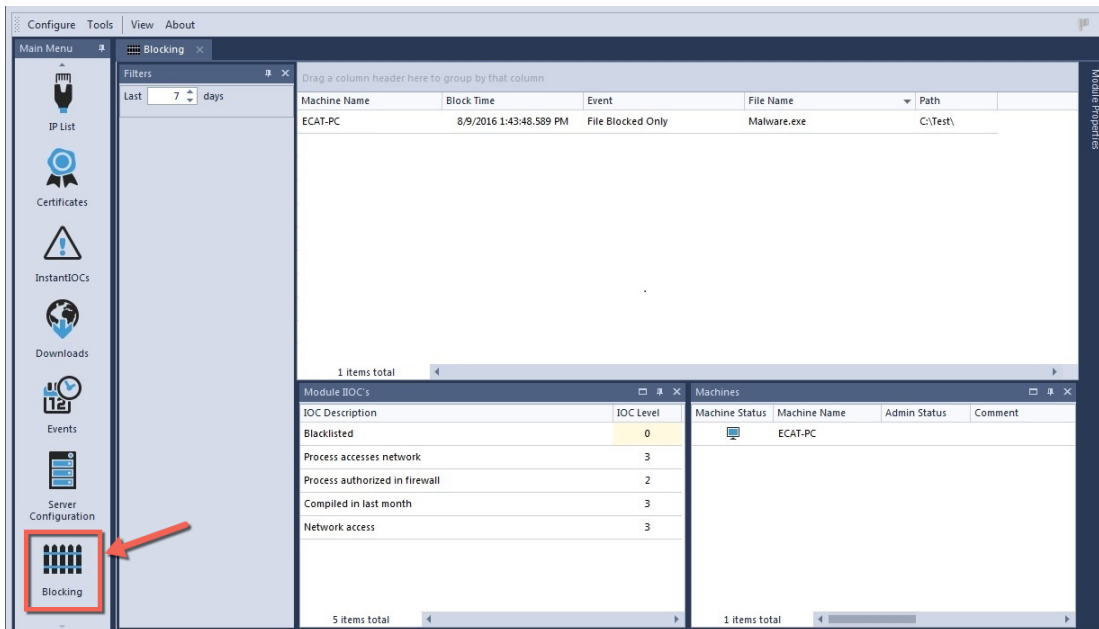
1. Right-click the required module and select **Edit Whitelist/Blacklist Status**.
2. Uncheck the **Remediation Action** checkbox and remove the blocked status.
3. Change the Module Status to either Neutral or Whitelisted.
4. Click **Update**.
The module gets unblocked and the status is updated in the **Machine View** window.

Note: Due to the periodic syncing of files, it may take several minutes for the unblocking action to take effect. If you want the unblocking action to take effect immediately, from the Tools menu, select **Force Blocking State Update**.

View Global Blocking

To view global blocking or the blocking events within the entire network, do the following:

1. Click **Blocking** in the Main Menu.
2. The **Blocking** window is displayed as shown below:



The **Blocking** window displays the summary of the blocked modules and all events related to blocking within the network.

Performance Considerations

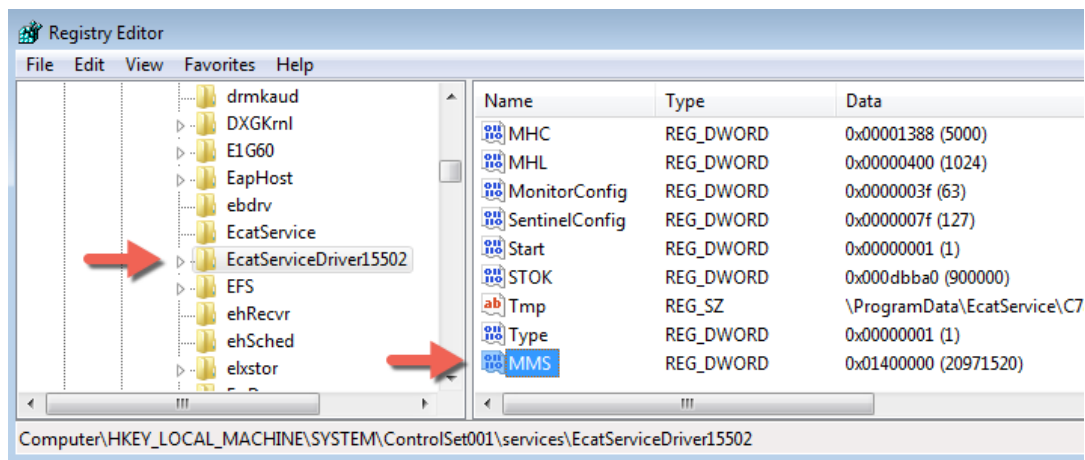
The blocking system works by comparing hashes of executable files with known bad hashes. An attempt is made to keep the impact of hashing to a minimum. But if blocking is not required, you can disable the blocking system to remove this overhead completely.

The NetWitness Endpoint agent maintains a cache of executable module hashes to reduce the load over time. As the NetWitness Endpoint agent detects a new modules loaded for execution, they are added to the cache. The hash is not computed again unless the module changes. This process does not consider non-executable modules such as MS Office modules, or any other document, or data modules. When the Blocking System is activated, the hash cache will be created. This is likely to cause load on the agent machine for a few minutes, but does not affect overall performance. Apart from the initial hashing, there will be a minor impact when a new program is run for the first time. When the program or feature is used for the second time, the hash is sourced from the cache and the impact is not significant. Also, the hash cache is kept across reboots.

Troubleshoot Blocking

If you are unable to block a file, the following items should be verified:

- Check that blocking is enabled on the environment (Global Parameters setting), for the machine group, and for the machine (these are all the default settings when installing NetWitness Endpoint). Also, during installation the Agent must be packaged in the Packager with Advanced>Settings>Monitoring Mode set to Full Monitoring (the default value).
- Check whether file is MS or RSA signed. These files cannot be blocked.
- Check if there is a MS or RSA signed file on another machine that shares the same path.
- Check if the file is larger than 100 MB. By default, the system will not block files over 100 MB. There is a workaround available to change the maximum file size of the blocking mechanism:
 1. Boot the machine in safe mode.
 2. In the Registry Editor, create a new DWORD entry named "MMS" with the maximum file size value (in bytes) in "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EcatServiceDriver#####", replacing "EcatService" with your service name, and ##### with the active driver number. The following example shows how a 20 MB max size is set:



3. Reboot the machine in normal mode.
- Check if the number of instances of the file is more than 50 (or whatever number is configured in Global Parameters, as described above).
 - Check whether there is any kernel mode agent downtime in progress. The kernel mode agent must be running to block a file.
 - Check whether the file is a Memory DLL, which cannot be blocked.

Use Machine Containment

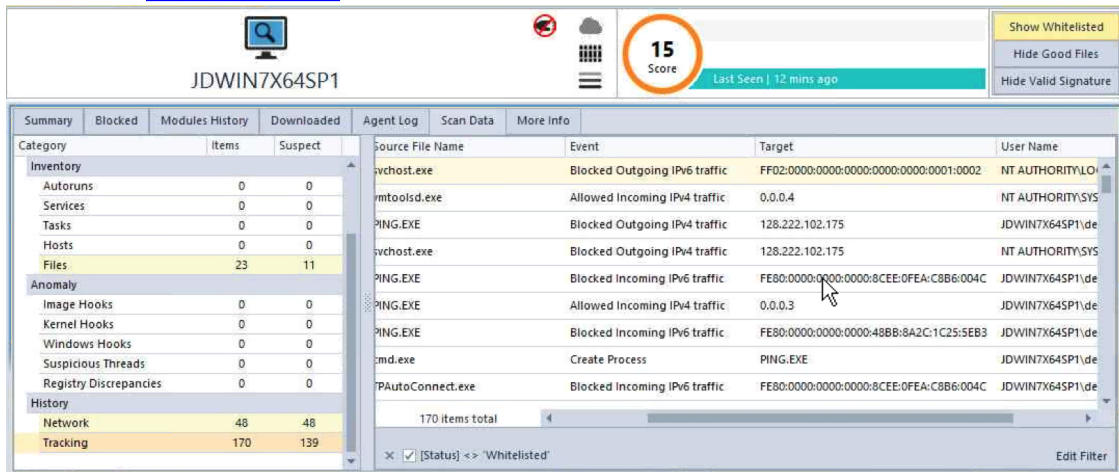
The NetWitness Endpoint Machine Containment feature allows an analyst to apply containment to a machine that may be compromised. Applying containment blocks the ability of a machine to connect to the network, allowing the analyst to observe the malware in action while protecting the larger environment. Analysts are able to control the spread of an attack and investigate the malware behavior post-containment. When a machine is contained, only NetWitness Endpoint connections are allowed from any process on the machine. For more information on how to apply containment, see [Turn Containment On or Off](#).

Note: Machine containment is currently available only for Windows machines (version 6.0 and above, for more information, see [Supported Machines for Containment](#)); it is not available for Linux or Mac machines. Also, users must be assigned either L2 or Administrator permissions to use any of the machine containment functionality.

For the analyst:

- NetWitness Endpoint retains full visibility on the processes/modules in the contained machine:
 - In particular, new modules, spawned after containment, will also be visible to the analyst, and will be contained.
 - Attempted network connections will be monitored and reported on as usual.
 - Specifically for network connections, the analyst will have the ability to distinguish between free connections, connections made through the exceptions mechanism, NetWitness Endpoint blocked connections, and unsuccessful connections for other reasons.
- The analyst will be able to quickly identify contained machines:
 - The faceted filter in the Machines table will include "Contained" as a local filter, along with Online, Offline, and Platform Type (Windows, Mac, Linux).
 - In the Machines table, "Contained" and "Containment Supported" are optional columns.
- Containment-related tracking events are added to the Events table and shown in the Machine View for the contained machine, as shown below. In addition to the network connections mentioned above, the system captures the username for the account owning the process that initiated or accepted a tracked connection, and the PID of the process involved in a tracked communication, regardless of direction. For additional information on containment tracking

events, see [Tracking Systems](#).



From the malware point of view:

- Containment manifests itself as network unavailable; malware will be unable to tell the difference between a cable unplugged and a contained machine.
- Allowed connections through the exclusion mechanism will be experienced in the same way as free connections; malware will be unable to tell the difference between a free connection and a connection allowed through an exclusion. For information on the exclusion list, see [Edit Containment Exclusion List](#).
- There will be no visible artifacts that malware can interrogate to find out if the machine is contained or not.

For the end user, when a machine is isolated, the end user will experience the process as if his or her workstation was unplugged from the network.

Note: Machine containment should be used only as a short-term solution for investigation and remediation. Machines should not be kept under containment for extended periods.

Supported Machines for Containment

There are some exclusions that apply to which machines can be placed under containment.

Machine containment is supported under both of the following conditions:

- Windows machines running NetWitness Endpoint agent version 4.3 or later, packaged with either full monitoring mode enabled or full user mode plus modern network tracking (beta)

- Windows machines running the following versions:

Operating System	Version Number
Windows 10	10.0
Windows Server 2016	10.0
Windows 8.1	6.3
Windows Server 2012 R2	6.3
Windows 8	6.2
Windows Server 2012	6.2
Windows 7	6.1
Windows Server 2008 R2	6.1
Windows Server 2008	6.0
Windows Vista	6.0

Machine containment is not supported for any of the following conditions:

- Mac machines
- Linux machines
- Microsoft Windows machines running Windows versions older than 6.0
- Machines running NetWitness Endpoint agent older than 4.3
- Machines running NetWitness Endpoint agent 4.3, but packaged without full monitoring or full plus modern network tracking (beta) enabled
- Machines connecting through the RAR server

Note: If a contained agent leaves the network, that agent will remain contained, and incapable of connecting anywhere (even through RAR), until they connect to the home network through a wired connection.

Note: For containment to work properly, all ConsoleServers must be configured with either the IP address or a fully qualified DNS name. Containment will not work properly if a ConsoleServer is configured with a partial DNS name. If you enter a partial DNS name, agent machines will go offline and a manual agent uninstall and reinstall will be required.

Turn Containment On or Off

You can turn machine containment on or off through the right-click menu for a machine in either the Machines table or the Machine View window.

To turn containment on:

1. Do one of the following:
 - Locate and select the machine you wish to contain in the Machines table.
 - Open the Machine View for the machine you wish to contain.
2. Right-click and select **Containment > Start Containment**.
A confirmation message displays.

Note: If containment is not supported for the selected machine, the Start Containment option is disabled and a message is displayed that indicates why it is not supported for this machine.

3. Click **OK** to confirm applying containment to the selected machine.
The status for applying containment displays at the bottom of the Machines table, initially as "Containment Pending" followed by "Containment Enforced" to indicate that containment was applied successfully to the selected machine.


You can continue to view the contained machine and the machine will continue to send data to the NetWitness Endpoint system. However, none of the executables on the contained machine will be able to initiate or accept external connections.

Whenever there is at least one contained machine in the network, a warning message is displayed at the top of all tables. For more information, see [Configure Containment Warning Message](#).

To turn containment off:

1. In the Machines table, locate and select the machine for which you wish to discontinue containment.
2. Right-click and select **Containment > Stop Containment**.
A confirmation message is displayed.
3. Click **OK** to confirm removing containment for the selected machine.
The status for removing containment is displayed at the bottom of the Machines table as "Releasing Containment" followed by "Not Contained."

Alternate method to turn containment off:

1. Open the Machine View for the contained machine.
2. Click the containment indicator  at the top right section of the Machine View window.

The previously contained machine will now be able to send and receive data from the network and accept external connections.

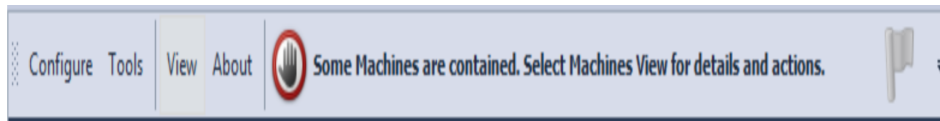
Note: Uninstalling, updating, or overwriting an agent will also remove containment.

For more information on viewing containment status for machines, see the following topics:

- [Machines Window](#)
- [Machine View](#)

Configure Containment Warning Message

When at least one machine is under containment, a message appears at the top of all tables, warning the user that some machines are isolated, as shown below:



This message appears even when these machines are not connected to the network. It will also display for machines currently pending containment or pending release.

If you do not want this message to appear, it can be turned off through the menu customization window in NetWitness Endpoint, as illustrated below:



In the above illustration, the numbers indicate the path through the menus to reach the menu customization window (step 4). The checkmarks indicate menu items currently visible. If you click to uncheck the containment message, it will be removed from the user interface until it is re-enabled using the same process.

Edit Containment Exclusion List

The NetWitness Endpoint containment feature includes a containment exclusion list, which you can modify by adding IP addresses. When exclusions are added, incoming and outgoing connections on those IP addresses are allowed, and behave in a similar fashion as if containment was not in place.

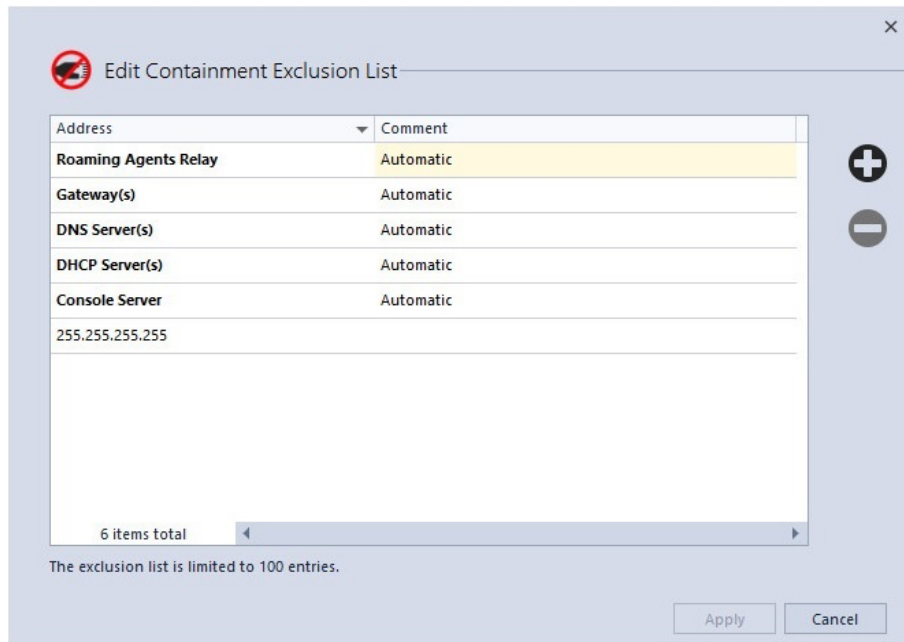
Default exclusions are added automatically for all connections required by NetWitness Endpoint, such as the RAR server and Console Server, as well as gateways, fully qualified DNS servers, and DHCP servers. The containment exclusion list allows an analyst to make exceptions to containment rules, so as to allow for monitoring connections and continued observation of lateral movement intentions. This list is managed globally for all contained machines.

Note: When entering an exclusion for an IPv6 address, you must also include any required multicast addresses, depending on your specific network configuration, as described below.

To add an exclusion to the containment exclusion list:

1. In the **Configure** menu, select **Containment...**

The Edit Containment Exclusion List dialog is displayed, as shown below:



2. Click the plus sign on the right side of the dialog to add a new IP address to the list.

The Add New IP Address dialog is displayed, as shown below:

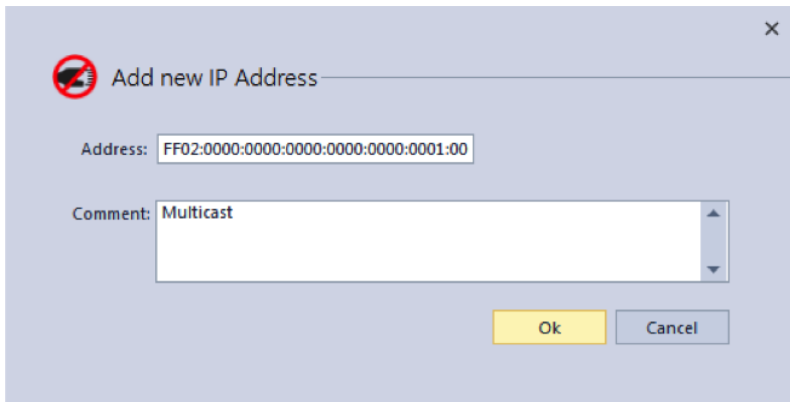


3. Enter the IP address, along with an optional comment (up to 1024 characters).

4. Click **OK**.

The IP address is now added to the exclusion list.

5. If adding an IPv6 connection, you will also need to add to the exclusion list any multicast addresses required for your network configuration. To do this simply repeat the previous steps for each required multicast address. An example is shown below:



To edit an IP address in the exclusion list:

1. Right-click the desired IP address and select **Edit**.
The Edit IP Address dialog is displayed.
2. Edit the information for the selected IP address.
3. Click **OK**.

To delete an IP address in the exclusion list:

1. Select the desired IP address.
2. Click the minus sign on the right side of the dialog.
A confirmation dialog is displayed.
3. Click **OK** to confirm deleting the selected IP address.

Note: The entries in bold at the top of the containment exclusion list (the comment field contains "Automatic") are default entries for required NetWitness Endpoint connections. These entries cannot be modified or deleted.

Note: The containment exclusion list is limited to a total of 100 IP addresses. After the 100th IP address is added, the plus sign will be grayed out.

COMMUNITY SOURCES FOR MODULE ANALYSIS

NetWitness Endpoint provides a variety of options for consulting outside sources of information when analyzing modules, as explained in the following topics:

- [File Reputation Service](#)
- [RSA Live Connect](#)
- [Search Modules with Online Services](#)
- [Analyze Modules with OPSWAT Metascan or YARA](#)

File Reputation Service

NetWitness Endpoint utilizes an online file reputation service to check the reputation of every module identified by the NetWitness Endpoint agents in your network. The validation is performed through RSA Live against an extensive database of known files that is updated in real-time, so files are checked against the very latest information.

Prerequisite: To use the file reputation service, you must first configure an RSA Live account by going to **Configure > Monitoring and External Components** and selecting to add an RSA Live connection. For more information see [RSA Live](#).

Modules are validated according to the following criteria:

1. Modules with the highest risk score are validated first.
2. Modules with the following characteristics are excluded from validation:
 - Modules signed by Microsoft or RSA
 - Modules with whitelisted certificates
 - Whitelisted modules
 - Blacklisted modules
 - Modules no longer present in the environment

After the file reputation service is enabled and the initial validation is complete, new modules added to the database are automatically validated according to the same criteria.

The NetWitness Endpoint UI displays module validation results in the Hash Lookup column in the Modules table and when viewing module and scan data information in the Machine View window for a selected machine. The possible validation values are:

- **Unknown:** The service could not find the hash queried.
- **Good:** The sample is considered to be goodware.
- **Suspicious:** The sample is suspected to be malicious.
- **Malicious:** The sample is labelled as malicious.
- **"-":** The sample was not submitted to the reputation service yet.

Note: If the NetWitness Endpoint Console Server is disconnected from the internet, you can download file reputation information using the ConsoleServerSync.exe tool, as explained in [NetWitness Endpoint ConsoleServerSync Tool](#).

RSA Live Connect

The RSA Live Connect service allows NetWitness Endpoint users to enhance malware detection and analysis with community information aggregated from other participants in the Live Connect service. The service provides access to statistics on hash reputation within the community, dates first/last seen, and proportions of decisions made by analysts within the community.

To enable such statistics, the following non-identifiable information is shared:

- Module hashes for files that are whitelisted, blacklisted, or graylisted
- Modules identified as risky by NetWitness Endpoint's behavior analytics
- IIOC matches on those files
- External network connections (to IP addresses and domains outside the current NetWitness Endpoint domain)

Customer-identifiable information, including internal connection information, will not be shared.

To participate in this community, you must have an RSA Live account and enable participation in the service through the RSA Live configuration dialog in Monitoring and External Components. For more information, see [RSA Live](#).

Once the Live Connect service is enabled, it immediately begins uploading information into the Live Connect service and retrieving information for matching modules. New information is then exchanged every 30 seconds.

Information retrieved from the Live Connect service displays in a Live Connect Information section of the Properties pane for a selected module, as shown below:

Live Connect Information	
# File Occurrer	1617
% Blacklisted	9.45
% Customer Occ	20.65
% Graylisted	None
% Neutral	Only You
% Whitelisted	None
First Time Seen	7/20/2016 6:44:55 ...
Last Updated	8/3/2016 6:01:41 AM
Risk	Unsafe
Risk Reason	File Blacklisted

File information included in the Properties pane indicates:

- **# File Occurrences:** The number of times the file appears in the community systems (for example, if one customer has the file on 1,000 endpoints, then total occurrences will be 1,000).
- **% Blacklisted:** The percentage of customers out of those that have the file who have marked it as blacklisted.
- **% Customer Occurrences:** The percentage of customers out of all customers registered in the Live Connect service that have reported having the file.
- **% Graylisted:** The percentage of customers out of those that have the file who have marked it as graylisted.
- **% Neutral:** The percentage of customers out of those that have the file who have marked it as neutral.
- **% Whitelisted:** The percentage of customers out of those that have the file who have marked it as whitelisted.
- **First Time Seem:** The first time the file (MD5) appeared in the Live Connect community.
- **Last Updated:** The last time the Live Connect community updated information on modules. By default, NetWitness Endpoint updates module status every 7 days.
- **Risk:** Live Connect provides the following risk ratings: Safe, Unknown, or Unsafe.
- **Risk Reason:** The reason for setting a file as Unsafe. This can be one or more of the following:
 - Communication to Unsafe Domain
 - Communication to Unsafe IP

- Downloaded from Unsafe Domain
- Downloaded from Unsafe IP
- File Blacklisted
- Static Analysis
- Suspicious Behavior

If the Live Connect service is enabled but then at some point disabled, all previously downloaded information will persist in the NetWitness Endpoint database and continue to display in the Properties pane for matching modules.

If the Live Connect service is never enabled, the Properties pane will still contain a Live Connect Information section, but the fields will not contain any information, as shown below:

Live Connect Information	
# File Occurrences	0
% Blacklisted	None
% Customer Occurrence:	None
% Graylisted	None
% Neutral	None
% Whitelisted	None
First Time Seen	
Last Updated	Waiting to download
Risk	Unknown
Risk Reason	

Search Modules with Online Services

You can use Google to search for matches according to the MD5 or the name of the module to research the legitimacy of the file.

To search a module with an online service:

1. From the **Main Menu**, click **Modules**. Alternatively, double-click a machine in the Machines List.
2. Right-click the module and select the **Search with** option associated with the desired online services (Google, VirusTotalSearch).
 - If the option **Offline Search** is **disabled**, a browser window will open with a search for that module's MD5.
 - If the option **Offline Search** is **enabled**, NetWitness Endpoint will generate an HTML file in the server folder with all modules to search. This file can then be copied and the modules can be searched on a computer with Internet access.

Note: Offline Search can be selected from **Configure > Internet Search Options**.

The following figure shows an Offline Search HTML Page.

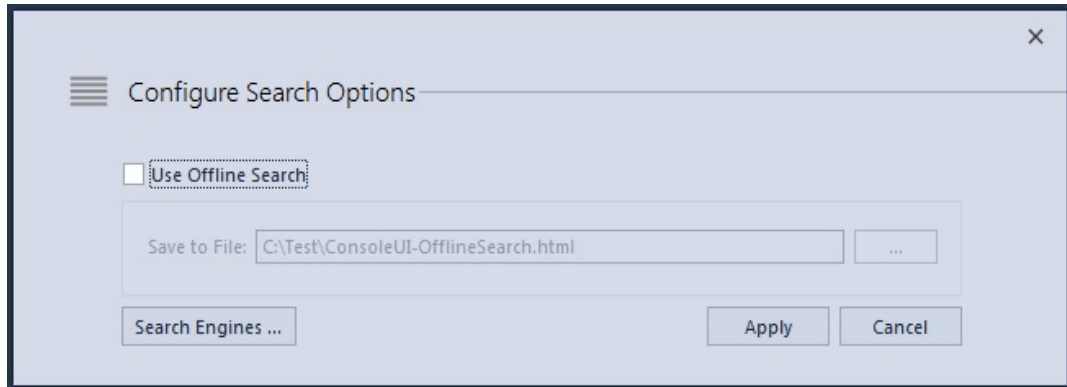
Name	Md5	Size	Search by MD5	Search by Name
m scorlib.ni.dll	1) 87E1E8A5135908AF80C184413AEB8AA1	2) 11 49 08 16	3) http://www.google.com/search?hl=en&q=87E1E8A5135908AF80C184413AEB8AA1	4) http://www.google.com/search?hl=en&q=m scorlib.ni.dll
System.ni.dll	5) 2FF632103A9FFE7C8BA4E8B55F743EC1	6) 79 73 88 8	7) http://www.virustotal.com/latest-report.html?resource=2FF632103A9FFE7C8BA4E8B55F743EC1	8) http://www.virustotal.com/latest-report.html?resource=System.ni.dll
System.Xml.ni.dll	9) 4DCC6849BF4C24FE34FD4EA69219D525	10) 54 53 31 2	11) http://www.checkfilename.com/SearchResults.aspx?SearchText=4DCC6849BF4C24FE34FD4EA69219D525	12) http://www.checkfilename.com/SearchResults.aspx?SearchText=System.Xml.ni.dll
System.Core.ni.dll	13) BF401586E76B7EADA0628D6733998E0	14) 22 95 29 6	15) http://fileadvisor.bit9.com/services/extracto.aspx?md5=BF401586E76B7EADA0628D6733998E0	16) http://fileadvisor.bit9.com/services/extracto.aspx?filename=System.Core.ni.dll

Add a New Search Engine

The default internet search options are Google and VirusTotalSearch. If required, you can configure new search engines by doing the following:

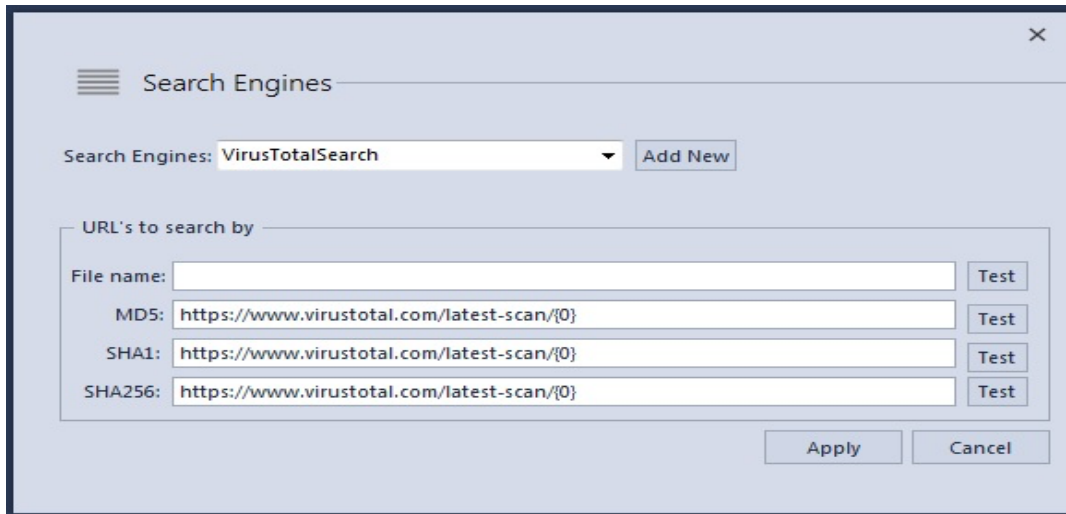
1. Click **Configure > Internet Search Engines**.

The **Configure Search Options** window is displayed as shown below:



2. Click **Search Engines**.

The **Search Engines** window is displayed as shown below:



3. Click **Add New** to add a new search engine.
4. Provide a name for the new search engine and click **OK**.
5. Enter the URLs and click **Apply**.
The new search engine is added to the list of Search Engines.

Analyze Modules with OPSWAT Metascan or YARA

To analyze a module with either OPSWAT Metascan antivirus or YARA rules, the module's download status must be downloaded.

To manually analyze a module:

1. Do one of the following:
 - From the **Main Menu**, click **Downloads**.
 - From the **Machine View**, select the **Downloaded** tab.
 - Select the module to be downloaded.

Note: Downloaded modules have the Downloaded flag set to “True” in the Module Properties pane. You can enable the Downloaded column in a table of modules by right-clicking the column headings to access the Column Chooser. Use the File.Status drop-down to select Downloaded as a column heading.

2. Right-click the module to analyze it and select the **Scan with** option that contains the available analyzers (that is, OPSWAT, YARA, or both).

Note: If no analyzers are installed, the option is disabled and a message is displayed.

The results of the analysis can be viewed in the **AV Scan Result** and **YARA Scan Result** columns in the properties of a selected module. The time of the last analysis performed on the module will be shown on the **Analysis Time**, also found in the properties of the module.

Note: To know at a glance if a module was scanned and when it was scanned, the **Analysis Time** column can be set to be displayed on the Global Module List or any category data grid. Also, to check whether the file was found to be infected, the **AV Scan Result** and **YARA Scan Result** columns can be displayed.

Reputation	
Analysis Time	7/22/2015 12:05:12...
AV Definition I	130536327179098...
AV Description	Found Infected o...
AV First Threat	Suspicious
AV Scan Result	Infected
AV Version	5
Cert. Bias Statu	Undefined
Company Nam	1
File Name Cou	1
First Seen Date	7/22/2015 12:04:32...
First Seen Nam	libcurl.dll
Hash Lookup	Unknown
Yara Definition	643895181337233
Yara Scan resul	Clean

The following figure shows a module list with OPSWAT and YARA results.

Filename	IOC Score	Machine C...	Size In Bytes	Analysis Time	AV Version	Yara Scan Desc...	Hash Look...	Risk Score	Compile Time	First Seen ...	AV Scan Re...	Automatic ...	AV Descript...
FrameworkService.exe	134	19	101.3 kB		0		Unknown	0	10/17/2007 5...	7/22/2015 1...	Unknown	<input type="checkbox"/>	
AM_Delta_Patch_1.203.125...	130	1	4.06 MB		0		Unknown	0	7/24/2015 2...	7/25/2015 3...	Unknown	<input type="checkbox"/>	
avgmfapoc.exe	130	1	5.84 MB		0		Unknown	0	10/17/2014 1...	7/22/2015 1...	Unknown	<input type="checkbox"/>	
STAFEnv.bat	130	1	0.5 kB		0		Unknown	4	7/22/2015 1...		Unknown	<input type="checkbox"/>	
svany.exe	130	24	8.0 kB	7/23/2015 5...	5		Unknown	0	4/19/2003 6...	7/22/2015 1...	Clean	<input type="checkbox"/>	
simplexmllrpc.py	129	11	3.4 kB	7/22/2015 2...	5		Unknown	0		7/22/2015 2...	Clean	<input type="checkbox"/>	
avgdiagex.exe	128	1	2.78 MB		0		Unknown	0	10/17/2014 1...	7/23/2015 3...	Unknown	<input type="checkbox"/>	
libcurl.dll	128	1	276.5 kB	7/22/2015 1...	5	I...	Unknown	1	5/14/2014 7...	7/22/2015 1...	Infected	<input type="checkbox"/>	Found Infe...
libaprutil-1.dll	128	1	196.5 kB	7/22/2015 1...	5		Unknown	1	5/14/2014 5...	7/22/2015 1...	Infected	<input type="checkbox"/>	Found Infe...
libapricomv-1.dll	128	1	26.5 kB	7/22/2015 1...	5		Unknown	1	5/14/2014 5...	7/22/2015 1...	Infected	<input type="checkbox"/>	Found Infe...
ssleay32.dll	128	1	261.0 kB	7/22/2015 1...	5		Unknown	1	5/14/2014 7...	7/22/2015 1...	Infected	<input type="checkbox"/>	Found Infe...
libapr-1.dll	128	1	146.0 kB	7/22/2015 1...	5		Unknown	1	5/14/2014 5...	7/22/2015 1...	Infected	<input type="checkbox"/>	Found Infe...
avgemcc.exe	128	1	653.5 kB		0		Unknown	0	10/17/2014 1...	7/22/2015 1...	Unknown	<input type="checkbox"/>	
avgnsx.exe	128	1	1.02 MB		0		Unknown	0	10/17/2014 1...	7/22/2015 1...	Unknown	<input type="checkbox"/>	

Module IOC's (3)		Machines (1)	
IOC Description	IOC Level	Machine Sta...	Machine Name
Modifies services ImagePath	1		
Network access	3		
DNS traffic from process	3		

Machine Sta...	Machine Name	Admin Status	Comment
	WIN7SP086		

Note: There may be YARA rules that generate errors in NetWitness Endpoint, regardless of which version of YARA you are using. When this occurs, NetWitness Endpoint automatically disables YARA. To remedy this, you will need to remove the incompatible rules and re-enable YARA.

MANAGE MODULES

Modules consist of files and relevant information collected during an assessment. You can view all modules of all assessed machines in the Modules table, or you can view modules for a specific agent in the Machine View for that agent.

To maintain the database size at a viable level, NetWitness Endpoint uses automatic filtering on some categories, based on the digital signature of the file. If the file is signed by a Microsoft Root Authority, it is automatically excluded from the following module categories:

- Files
- Autoruns
- Network
- Windows Hooks
- Kernel Hooks
- DLLs

A variety of procedures are available for managing modules within NetWitness Endpoint, as detailed in the following topics:

- [Automatic Status Assignment](#)
- [Update Certificates](#)
- [Assign Hooks to Modules](#)
- [MFT Viewer](#)
- [View the Machine List for a Module](#)
- [Download Modules](#)
- [Export Blacklist-Whitelist Files](#)
- [Import Blacklist-Whitelist Files](#)

Automatic Status Assignment

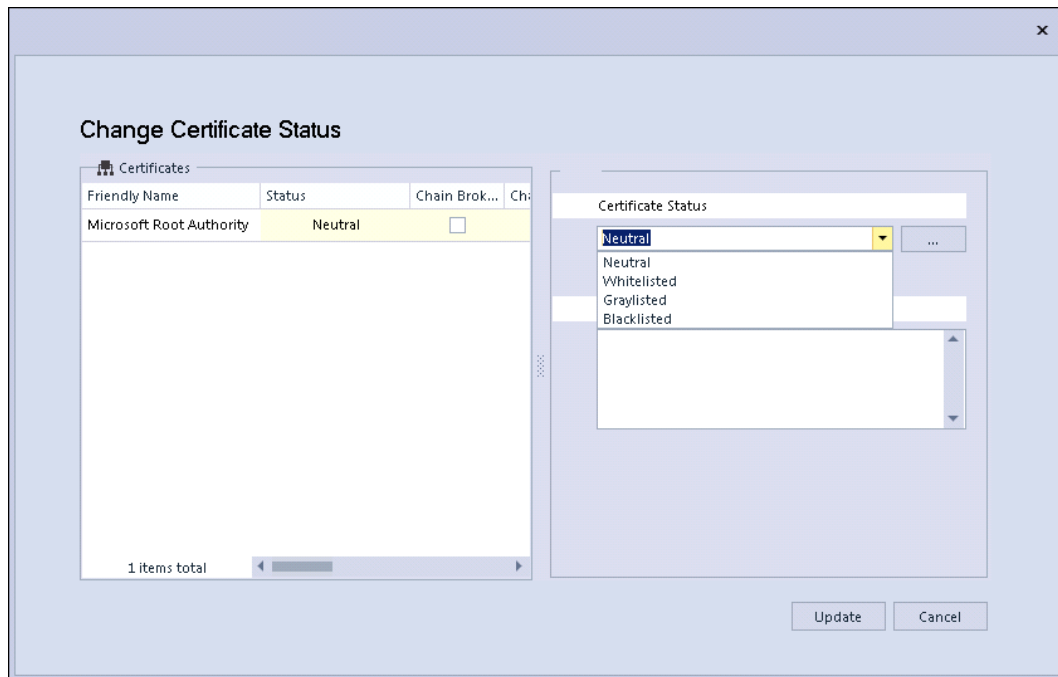
Automatic Status Assignment enables you to automatically assign a status (such as Whitelisted, Blacklisted, or Graylisted) to a module based on the status of the certificate used to sign the module. You can assign a status to the certificate signed by certain trusted vendors and this status can be automatically applied to all modules that use these certificates. For example, if you consider Microsoft a trusted vendor, you can set the status for the certificates signed by Microsoft as Whitelisted. Further, you can configure automatic whitelisting for the modules that are signed by these whitelisted certificates. Similarly, you can also set the certificates as Neutral, Blacklisted, or Graylisted.

The configuration of automatic status assignment for modules is a two-step process. The first step is to edit/update the status of the certificates and the second step is to configure automatic whitelisting for modules based on the status of the certificates.

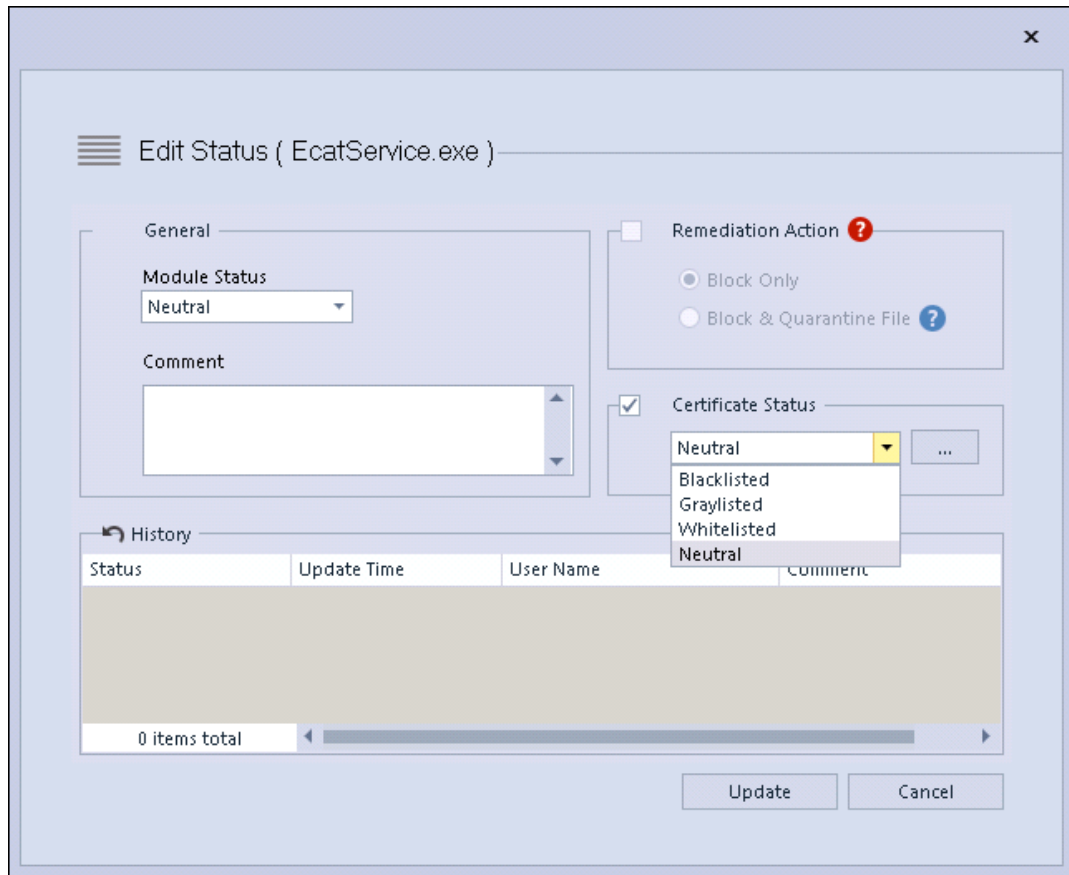
Change Certificate Status

You can change the status of the certificates by using any one of the following options:

1. Using the **Certificates** Main Menu:
 - a. From the **Main Menu**, click **Certificates**.
The **Certificates** window is displayed.
 - b. Right-click the required certificate and select **Edit Certificate Whitelist Status**.
The **Change Certificate Status** window is displayed as shown below:



- c. In the **Certificate Status** drop-down, select a status. To know more about each status, see the topic [Review Modules](#).
 - d. Click **Update**.
The status of the certificate is updated.
2. Using the **Modules** Main Menu:
- a. From the **Main Menu**, click **Modules**.
 - b. Right-click the selected module/modules and select **Edit Whitelist/Blacklist Status**.
The **Edit Status** dialog is displayed as shown below:



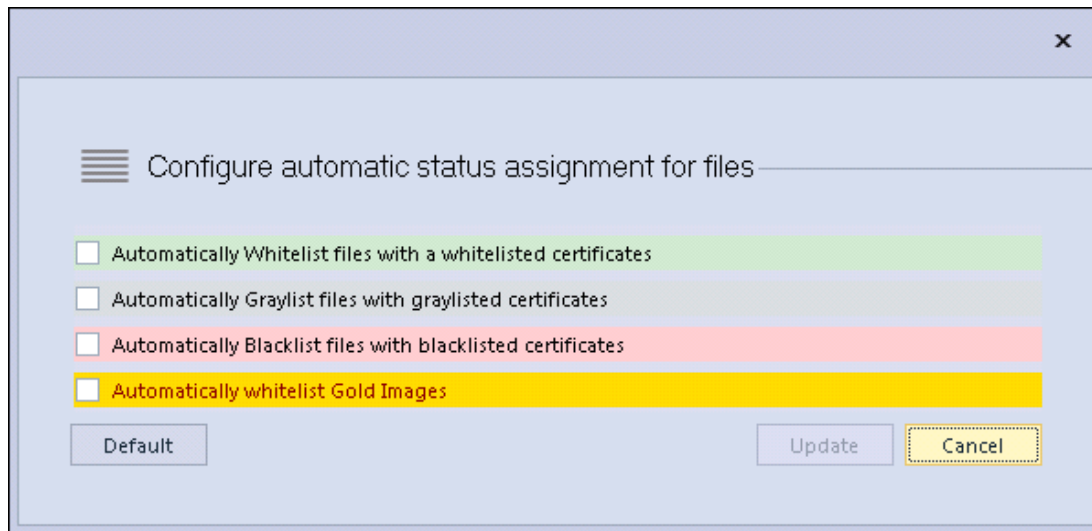
- c. Select the **Certificate Status** check-box and choose from the drop-down options.
- d. Click **Update**. The status of the certificate is updated accordingly.

Configure Automatic Status Assignment

To configure automatic status assignment of modules, do the following:

1. Click **Configure > Automatic Whitelisting**.

The **Configure Automatic Status Assignment** dialog is displayed as shown below:



2. Select the check-box based on the required options. For example, if you select "Automatically Whitelist files with a whitelisted certificates", all modules with whitelisted certificates will be whitelisted.
3. Select **Default** to use the default options. By default, the following options are enabled:
 - Automatically Graylist files with graylisted certificates
 - Automatically Blacklist files with blacklisted certificates
4. Click **Update**.
Automatic status assignment is configured.

Note: For more information about the **Automatically whitelist Gold Images** option, see the topic [Whitelisting and Gold Images](#).

Update Certificates

ECAT will automatically import trusted root certificates to overwrite existing certificates bearing the same name.

Certificates need to be imported when the **Signature** column says “**needs signature revoke update**.” This last message means that NetWitness Endpoint cannot confirm that the signature root authority is valid or has been revoked. Importing certificate and revocation lists will clear this message and replace it with the validity of the certificate (valid or revoked). Certificates need to be updated when unknown authorities appear or after two weeks to force an update to the **CRLs** (Certificate Revocation Lists).

Note: To update the CRLs, NetWitness Endpoint ConsoleServer must have working Internet access.

To import trusted root certificates:

1. Click **Configure > Update Certificates**.
2. Click **Yes** in the **Import Trusted Roots** dialog box.

Assign Hooks to Modules

NetWitness Endpoint organizes modules into scan categories. However, some categories, such as inline hooks, may not be assigned to a module due to the complex mechanisms that malware uses to hide.

If NetWitness Endpoint is not able to locate the module responsible for the hook, the hook to support must be manually assigned. For example, McAfee sets IAT hooks on multiple functions, but they point to floating code (for more information, see [Floating Code](#)). When the originator is found, a manual relationship is established between **mcafee.exe** and the hooks. For more information concerning hooks, see [Scan Categories](#).

To assign hooks to a module:

1. From the **Machines** List, double-click the machine.
2. From the **Categories** pane, select the required hook category (image hooks, kernel hooks).
3. Right-click the hook in the hook table on the right and select **Assign Module**.
4. Select a module from the list and click **OK**.

MFT Viewer

You can view the full MFT (Master File Table) of a remote computer and the metadata of every file (deleted or not) on the remote disk.

To view the full MFT of a remote computer on the remote disk:

1. Right-click the desired machine in the **Machines** list and select **Forensics > Request MFT**.
2. Click **Proceed** in the **Request MFT** dialog box. The MFT will be compressed by the NetWitness Endpoint agent and transferred to the server. Once this is done, it will be visible in the machine's **Downloaded** pane.
3. Right-click the file and select **Download and Open MFT**. The MFT Viewer will parse the MFT file and display every available file in a tree view similar to the one in Windows Explorer. The **Deleted Files** tab contains a sequential list of all deleted files.

Note: As with other modules, NetWitness Endpoint allows you to download the file to any desired path by right-clicking the file and selecting **Save Local Copy**.






To view a previously downloaded MFT:

1. Click **Tools > MFT Viewer**.
2. Specify the file path and partition letter to which the MFT belongs.
3. Click **Open**.

View the Machine List for a Module

From the Machine View or from the Modules tab, you can view a list of machines for the module.

The **Machine Count** column on the Modules list tells on how many systems the module was found.

Filename	IOC Score ▼	Machine Count	Signature	Size In Bytes	Description	Hash Look...	Risk Score
SearchProtocolHost.exe	 0	1	Need Revok...	160.5 kB	Microsoft ...	Good	0
SearchFilterHost.exe	 0	1	Need Revok...	84.5 kB	Microsoft ...	Good	0
taskhostex.exe	 0	6	Need Revok...	52.5 kB	Host Proce...	Good	0
SUSPEND-VM-DEFAULT...	 0	1	Not Signed	459 bytes		Unknown	0
RESUME-VM-DEFAULT...	 0	1	Not Signed	457 bytes		Unknown	0

To open and view a list of machines with a module:

1. Do one of the following:
 - Locate the module, right-click it, and select **List Computers with Module**.
 - In the **Main Menu**, click **Modules**, select the module, and consult the **Machines** pane to see which machines have the module.
2. Double-click a row to open the machine in the main window.

Download Modules

Suspicious modules can be downloaded to the NetWitness Endpoint server to perform a more intensive scan.

Downloaded modules are automatically scanned by several antivirus engines with OPSWAT Metascan, and can also be analyzed with the PE file analyzer, as well as any other desired tool.

The scan result is stored in the module's comments. If one of the Metascan antivirus engines reports the file as malware, it will affect the suspect reasons information as well as raise the score of the file. Infected files are automatically blacklisted.

The files are stored on the server in the **/server/Files** subdirectory. The filename is based on the timestamp of the downloaded file and the existing filename. An underscore is added to the extension to avoid executing the file unintentionally.

The download status of a file could be any of the following:

- Not Downloaded
- Queued (the download was requested but not yet received)
- Downloaded

Automatically Download New Modules

You can set NetWitness Endpoint to automatically download new modules, which will automatically request new modules to be sent from the client machines. All modules are requested with no exceptions. Therefore, this option should be used with caution since it could cause a very high traffic level on the network.

A filter can be applied to the new files to be automatically downloaded. Files with a valid signature or with a known hash can be excluded from the automatic process and downloaded manually at a later time.

Note: This option will not automatically request modules that had been previously found by other scans. Only new modules from new scans will be downloaded automatically. To request modules that are already in the database but not downloaded, see *Manually Downloading Modules* below.

The download can be requested from any machine on which the module has been found.

To set NetWitness Endpoint to automatically download modules:

1. Click **Configure > Global Parameters**.
2. Locate the **Automatically Download New Modules** section.
3. Check the **Enabled** checkbox.
4. Click **OK** or **Apply**.

Note: This is a global database setting. If multiple administrators modify the setting, only the last setting will be effective.

Manually Download Modules

Modules that were not downloaded can be queued manually for an examination.

To manually download a module:

1. Click **Modules** in the **Main Menu**. Alternatively, double-click a **machine** and select the module.
2. Right-click the module and select **Download to Server**.
3. Click **Proceed** in the **Download to Server** dialog box.

Retrieve Downloaded Modules

You can retrieve a downloaded module and save it to your hard drive. Downloaded modules are stored in the server in the `/server/Files` subdirectory. The filename is based on the downloaded file's timestamp and existing filename. An underscore is added to the extension to avoid executing the file unintentionally.

To retrieve a downloaded module:

1. Do one of the following:
 - Open **Downloads** from the **Main Menu**.
 - Open a machine and access the **Downloaded** tab.
 - Locate a downloaded module.
2. Right-click the desired module and select **Save Local Copy**.
3. Navigate to the desired location of the file and click **Save**.

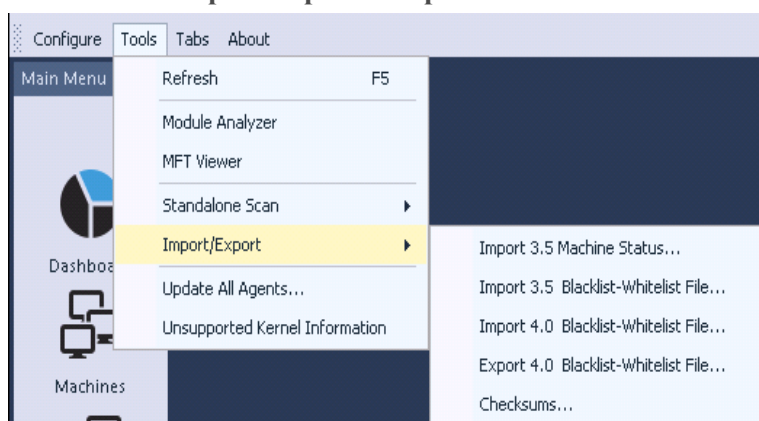
Export Blacklist-Whitelist Files

You can export a blacklist-whitelist file and save it to your hard drive. The file will be saved in .xml format.

This is useful if you need the data at a later date, for example, to restore your database after it has been cleared. It can also be used to share the whitelisting information between two different instances of NetWitness Endpoint.

To export a blacklist-whitelist file:

1. Click **Tools > Import/Export > Export 4.0 Blacklist-Whitelist File**.



2. In the **Select file to Export** section, select the file to export.
3. Navigate to the location where you want to save the file and enter a **File name**.

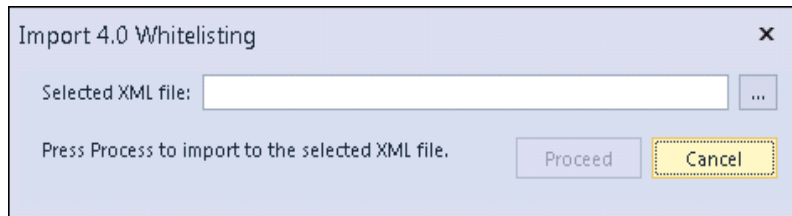
4. Select **Save as type**.
5. Click **Save**.

Import Blacklist-Whitelist Files

You can import a previously exported blacklist-whitelist file. The file should be in .xml format. Importing this list will automatically set the modules' status and the comments to the ones stored on the .xml.

To import a blacklist-whitelist file:

1. Make sure that the file to import is from NetWitness Endpoint Version 3.5 or later.
2. Click **Tools > Import/Export > Import 4.0 Blacklist-Whitelist File**.



3. Navigate to the location of the file and enter a **File name**.
4. If requested, select **File of type**.
5. Click **Proceed**.

MANAGE AGENTS



An agent runs on a machine (for example, a Windows desktop, laptop, or server), which it scans for information. This machine is the target of the assessment. All assessed machines are listed in the Main Menu under **Machines**.







The following topics provide information and procedures for managing machines:

- [Agent Status Icons](#)
- [Modify Machine Status](#)
- [Modify Machine Comments](#)
- [Machine Groups](#)
- [Perform a Full Memory Dump](#)
- [Reboot a Machine](#)
- [Kernel Adaptation System](#)
- [Update an Agent](#)
- [Change Agent Server](#)
- [Uninstall Agents and Remove Agents from the Database](#)

Agent Status Icons

Throughout the NetWitness Endpoint UI, each agent is represented as a color-coded icon according to its status. Hovering over an icon with the mouse displays a tooltip with the status description.

Icon	Description
	Install Error
	Machine Offline

Icon	Description
	Machine Offline - Driver Error
	Machine Online
	Machine Online - Driver Error
	Machine Requires Reboot
	Online Scanning
	Online Scanning - Driver Error

Some of the driver errors can be resolved by using the Kernel Adaptation System. For more information, see [Kernel Adaptation System](#).

Modify Machine Status

You can modify the administrative status of a machine. The status is used as a marker when an assessment is performed by multiple NetWitness Endpoint UI users at the same time. A status only has a visual impact. No score is modified.

The following table lists some of the default available statuses, their corresponding row color in the list of machines, and their description.

Status	Color	Description
None	White	Machine doesn't have a status assigned to it.
Under Investigation	Gray	Machine is under investigation.

Status	Color	Description
Infected	Red	Machine is infected.
Verified	Green	Machine has been completely assessed.
Skipped	Gray	Assessment of this machine was begun but was then put aside for later review.
Test	Indigo	Machine is in testing phase.

To modify a machine's status:

1. Do one of the following:
 - Right-click the machine in the Machines list.
 - Select several machines by holding CTRL or SHIFT, then right-click within the selection.
2. Select **Modify Status**.
3. Select the required status from the drop-down menu.
4. Click **Proceed**.

To edit administrative status descriptions or colors:

1. Click **Configure > Administrative Status**.
2. Select the desired status from the list and click **Modify**.
3. Modify the text and/or color as desired.
4. Click **OK**.

To add or remove administrative status options:

1. Click **Configure > Administrative Status**.
2. Do one of the following:
 - To add an administrative status, click **Add New**. Enter color and text, and click **Add**.
 - To delete an administrative status, click **Delete**.

Modify Machine Comments

You can modify any comments made for a machine.

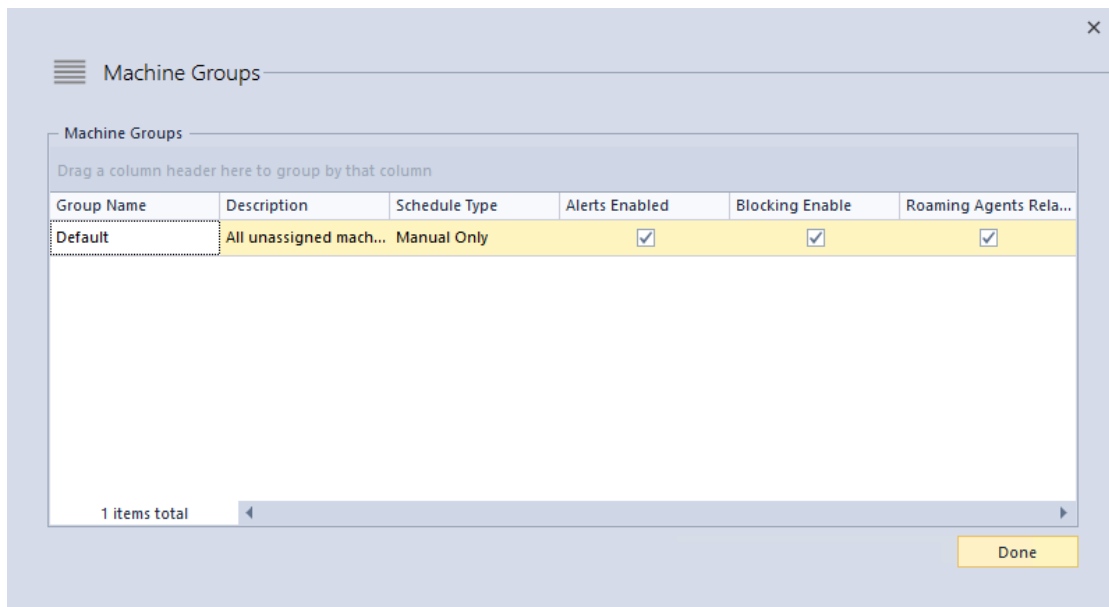
To modify comments:

1. Do one of the following:
 - Right-click the machine in the **Machines** list.
 - Select several machines by holding CTRL or SHIFT, then right-click within the selection.
2. Select **Modify Comment**.
3. Enter the comment and click **Proceed**.

Machine Groups

Any computer or server (physical or virtual) that has a NetWitness Endpoint agent running is called a “machine” in the NetWitness Endpoint UI. A machine group is a logical group of machines. Each machine is part of a machine group. By default, every machine is part of the “Default” machine group. Each machine group has specific properties that the NetWitness Endpoint administrator can define.

To view the list of machine groups: Click **Configure** in the Top Menu and select **Machine Groups**. The Machine Groups dialog is displayed, as shown below:



The Default machine group will always be listed and the settings for this group automatically apply to all machines in the network on which a NetWitness Endpoint agent has been installed. Additional information about the group also displays such as the schedule type for running scans and whether Alerts or Blocking as been enabled for the group.

To edit settings for the Default machine group:

1. From the Machine Groups dialog, in the Group Name column, right-click on **Default** and select **Edit Group**.

The Group Settings dialog is displayed, as shown below:

2. You can edit the settings for running scans for the Default group. For more information, see [Configure Scans for a Machine Group](#).
3. You can select whether to enable the following options for all machines in the group:
 - **Enable Roaming Agents:** Select to enable the Roaming Agents Relay for machines in this group. You must have also installed and configured the NetWitness Endpoint Roaming Agents Relay (RAR) to use this option. For more information, see *Step 14: (Optional) Deploy Roaming Agents Relay* in the RSA NetWitness Endpoint 4.4 Installation Guide.
 - **Enable Blocking System:** Select to enable the Blocking System for machines in this group. For more information, see [Remediate Results with the Blocking System](#).
 - **Enable Alerts:** Select to enable the alerting function for machines in this group. For more information, see [Manage Alerts](#).

You can create additional groups as needed to categorize machines in the network. To create a new group:

Note: A machine can only belong to one machine group at any given time. If you create a new machine group and assign machines to it, those machines will no longer belong to the Default machine group.

1. From the Machine Groups dialog, in the Group Name column, right-click on **Default** and select **Add Group**.
The Group Settings dialog is displayed.
2. Enter a name and description for the new group.
3. Select desired settings as previously described for editing the Default group.

To delete a group: From the Machine Groups dialog, in the Group Name column, right-click on a group name and select **Delete Group**. A dialog displays to confirm the deletion process. This option is not available for the Default group.

Once you have created machine groups, you can individually add or remove machines from any machine group except the Default group:

- To add a machine to a group: In the **Machines** list, right-click a machine, and select **Configuration Group > Add Machine to Group**. (Note: a machine can only belong to one machine group at any given time.)
- To remove a machine from a group: In the **Machines** list, right-click the machine you wish to remove, and select **Configuration Group > Remove from Group**.

Perform a Full Memory Dump

A full memory dump provides a more in-depth investigation of the machine.

Caution: Ensure you have enough disk space on the server. The memory dump is equivalent to the size of the machine's physical RAM.

Note: The **Request Memory Dump** option does not work if the Windows 10 Device Guard feature is enabled.

To perform a full memory dump:

1. Do one of the following:
 - Right-click the machine in the **Machines** list.
 - Select several machines by holding CTRL or SHIFT, then right-click within the selection.
2. Select **Forensics > Request Memory Dump**.
3. Click **Request** to confirm you want to perform a full memory dump.

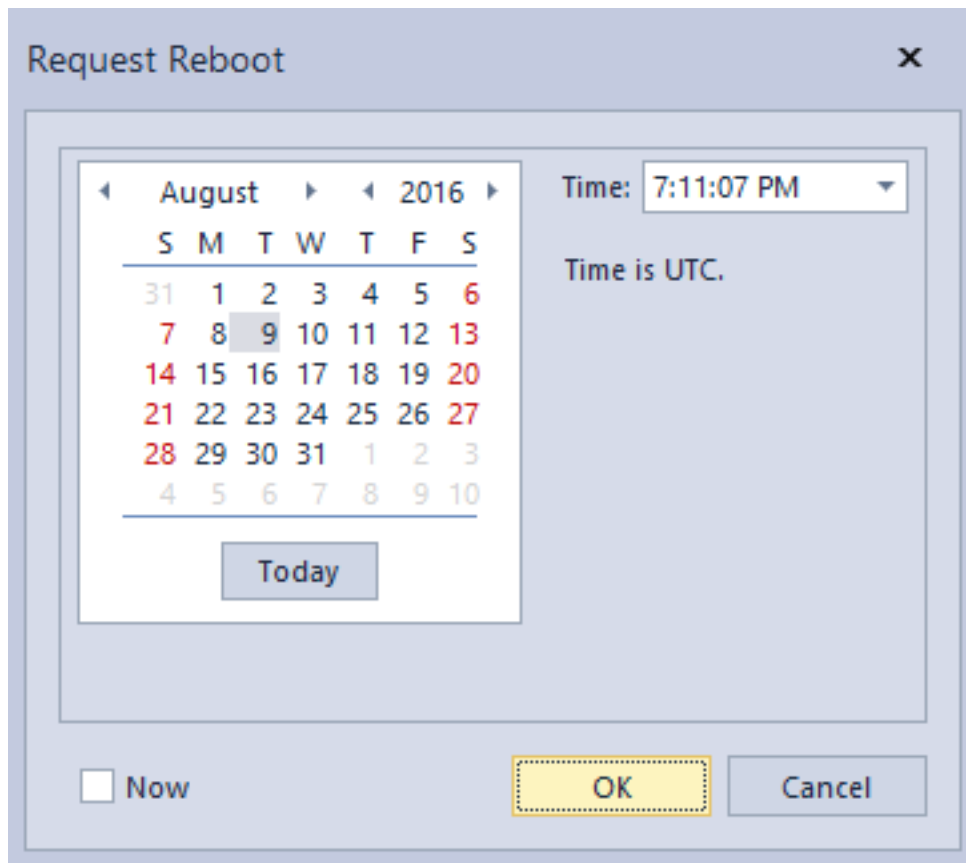
The memory snapshots are stored on the NetWitness Endpoint Server under the `\Server\Files\Machines\<Client-Name>\<Client-Name_Date-Taken>.raw` subdirectory.

Note that the full memory dump will also consume a large amount of disk space on the agent machine before it is automatically transferred to the server. Additionally, the memory dump can take a long time to complete and may fail if the agent system goes offline/asleep during the request or if the agent kernel driver fails to load.

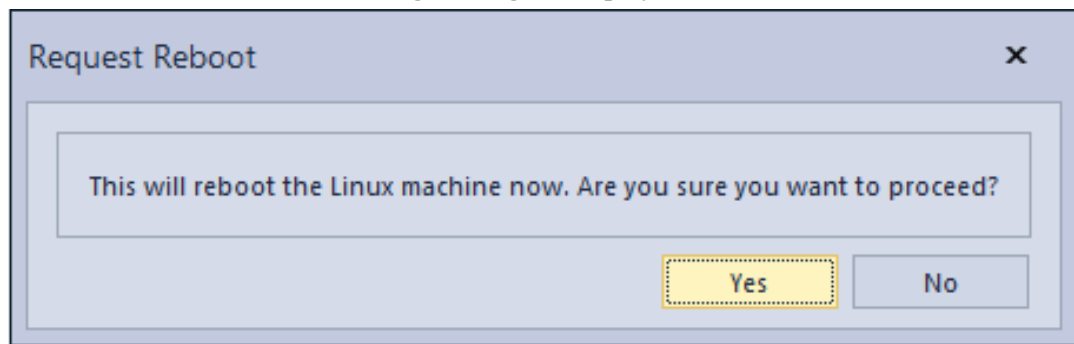
Reboot a Machine

To reboot a machine:

1. In the **Machines** list, right-click the machine.
2. Select **Advanced > Reboot**.
 - For a Windows or Mac machine, the Request Reboot dialog is displayed, as shown below



- For a Linux machine, the following message is displayed:



3. For a Windows or Mac machine, do one of the following:
 - Choose a date and time for rebooting the machine and then click **OK**.
 - Click the **Now** checkbox to reboot the machine immediately and then click **OK**.
4. For a Linux machine, click **Yes** to proceed with the reboot.

Kernel Adaptation System

This topic provides information about using the Kernel Adaptation System to maintain stability of the NetWitness Endpoint agents in case of unknown or unsupported Windows kernels. This is only applicable for Windows agents.

The NetWitness Endpoint Windows agent uses a number of kernel-specific mechanisms to gather information critical to the analyst. To provide a safe operating environment, the details are only extracted from known versions of the operating system. The agent installer provides the agent with all the necessary information required to run correctly on the active operating system of an endpoint, provided it is a supported version. However, an unknown Windows kernel version may be encountered in the following cases:

- Windows update service patches are applied after the installation of the Windows agent
- If an unsupported version of the Windows kernel is installed on an agent


The former usually happens during a patch update cycle (which occurs every Tuesday) or through a critical update released by Microsoft and distributed periodically by the IT administrator. In such cases, the NetWitness Endpoint agent reverts to a fallback mode, reducing its level of analysis and providing only the basic information.

The Kernel Adaptation System provides greater stability to the NetWitness Endpoint agent by eliminating the dependency of installing product updates when new kernels are found. The new kernel update takes place automatically through RSA Live and is available free of cost to all customers subscribed to NetWitness Endpoint.

Using the Kernel Adaptation System requires minimal user intervention as most of the process is automatic, except for identifying unsupported kernels and setting up RSA Live.

To set up RSA Live, see [RSA Live](#).

Identify Unsupported Kernels

When NetWitness Endpoint detects unsupported kernels on a Windows agent, the affected system displays the  icon. Additionally, the system's "Machine.ECAT.DriverErrorCode" property is set to "0xe0010014".

Kernel Update Process

When an unsupported kernel is identified in the system, the NetWitness Endpoint Server connects to liveecat.rsa.com and sends the following information in a .CSV file:

- Kernel File Name
- Compilation Time for the Kernel File
- Size of the Kernel File
- Flag: Always 1

There is no visible information that is sent through this system at any given time. Once the above information is received, the NetWitness Endpoint team is notified. The NetWitness Endpoint team updates the supported kernels database with the required information and updates the liveecat.rsa.com server. The NetWitness Endpoint server polls this server every 30 minutes and automatically retrieves the updated kernel database ("KernelData.csv"). When next connected, the Windows agents receive the required update and load the NetWitness Endpoint driver. In most cases, the entire process takes place automatically and is not visible to the user.

Waiting Time for Kernel Update

Generally, the maximum wait time is 24 hours during standard business days, but in some cases it may exceed this time. If the update takes more than 24 hours, please contact RSA Customer Support.

Kernel Updates for NetWitness Endpoint Server without Internet Connection

For certificates and RSA Live feed import, use the ConsoleServerSync.exe tool, as described in [NetWitness Endpoint ConsoleServerSync Tool](#).

Update an Agent

You may update one agent, a set of agents, or all agents to the latest version of the NetWitness Endpoint agent.

Updating an agent can be done using any one of the following three methods:

- Using the NetWitness Endpoint UI
- Using Agent Installer
 - Command Line
 - Double-click
- Any other Deployment Tools

Note: This can also be done with deployment software.

Note: If an agent is currently under containment, updating, overwriting, or uninstalling that agent will remove machine containment.

Update an Agent Using the NetWitness Endpoint UI

Updating an agent is a three-step process:

1. Generate the installer on the server machine.
2. Queue the update on the NetWitness Endpoint UI.
3. Wait for the agent to confirm the update.

Note: Make sure that you generate the installer on a machine where the proper certificates are installed (ones that match the certificates from ConsoleServer).

Upon successful completion of an update, the installation date on the computer list will be updated, though a refresh might be needed to see it. In addition, the events pane will show the result of the update. This is true for the client events pane and the global events pane.

To update an agent:

1. Generate a new agent installer.

Note: The new agent should have the same service name as the original.

2. Open the **Machines** list from the **Main Menu**.
3. Right-click the machine and select **Agent Maintenance > Update Agent**. (Alternatively, several agents can be selected by holding CTRL or SHIFT. All selected agents will then be updated simultaneously.)
4. Navigate to the location of the generated file, select the desired file, and click **Proceed**.
The Update Agent window will then display the package file information.
5. Click **Update**.

Note: The installation date on the computer list will be updated when an update was successfully applied, though a refresh might be needed to see it.

To update all agents:

1. Generate a new agent installer.

Note: The new agent should have the same service name as the original.

2. Select **Tools > Agent Maintenance > Update All Agents**.
3. Under **Update package**, navigate to the location of the generated file, select the desired file, and click **Proceed**.

The Update Agent window will then display the package file information.

4. Click **Update**.

Update an Agent Using Agent Installer

To update an agent using Agent Installer, simply double-click the agent installer and follow the instructions or use the command-line option. Instructions for using the command line option to update agents are provided in the topics for deploying each type of agent in the RSA NetWitness Endpoint 4.4 Installation Guide.

Note: If you get an error while updating the agent by using other methods, it is recommended to use the command-line option to update the agent.

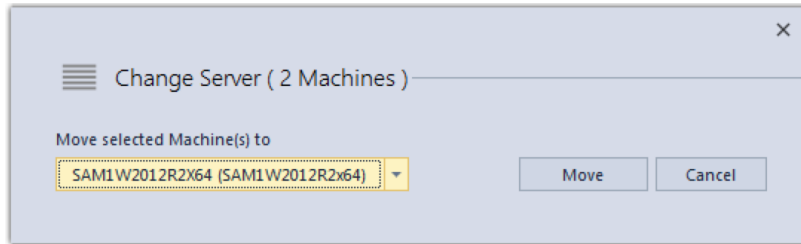
Change Agent Server

With the multi-server environment, you can now change the server associated with the agents from one Console Server to another based on your requirement. NetWitness Endpoint supports changing the server for agents during any of the following scenarios:

- When the current Console Server is no longer available for some reason.
- When the Administrator wants to balance the Console Server load manually.
- When the NetWitness Endpoint agents want to report to the Primary Console Server when the current Console Server is not accessible for extended period of time.

To change an agent server:

1. Open the **Machines** list from the Main Menu.
2. Do one of the following:
 - Right-click on the machine and select **Agent Maintenance > Change Server**.
(Alternatively, several agents can be selected by holding CTRL or SHIFT. Selected agents will then be updated simultaneously).
 - Select **Tools > Agent Maintenance > Change Server**.
3. The **Change Server** dialog is displayed as shown below:



4. Select the required Console Server from the available options in the drop-down list.
5. Click **Move**.
The NetWitness Endpoint agent is moved to the new server and receives the new server details.

Uninstall Agents and Remove Agents from the Database

If you uninstall the agent, there is no way for the server to know whether the agent has been uninstalled or is offline.

Note: A deleted agent's modules remain in the Module List, and the **Machine Count** column may display 0 if the deleted agent was the only one with the module.

License counts are based on the number of reports in the database. Uninstalling a machine allows it to remain in the server, and it still counts as a license. To free a license, you need to remove a machine from the database.

Note: If you remove a machine from the database, but you didn't first uninstall the agent, then a new report will be created the next time the agent connects. This means that to ensure a machine will no longer affect the database, the user needs to first uninstall the agent and then remove the agent from the database.

To free a license:

1. Uninstall the agent.
2. Remove the agent from the database.

To uninstall an agent:

1. Do one of the following:
 - Right-click the machine in the **Machines** list.
 - Select several machines by holding CTRL or SHIFT, then right-click within the selection.
2. Select **Agent Maintenance > Uninstall Agent**.
3. Click **Proceed** to confirm you want to delete the agent.

Note: If an agent is currently under containment, uninstalling, overwriting, or updating that agent will remove machine containment.

To remove an agent from the database:

1. Do one of the following:
 - Right-click the machine in the **Machines** list.
 - Select several machines by holding CTRL or SHIFT, then right-click within the selection.
2. Select **Advanced > Remove Selection from the Database**.
3. Click **Yes** to confirm you want to delete the agent.

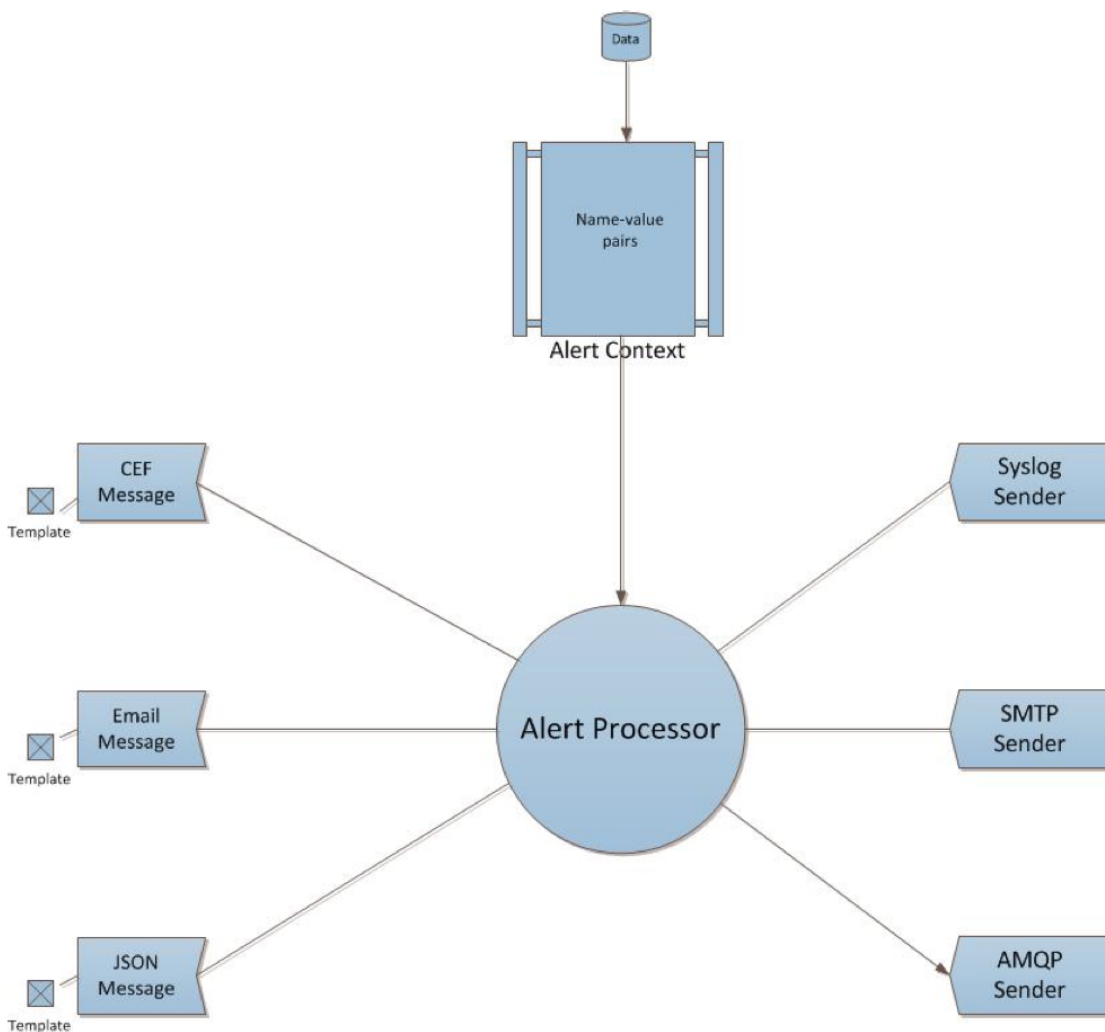
MANAGE ALERTS

This topic provides information about how alerts are generated and configured in NetWitness Endpoint.

You have the ability to generate alerts (Syslog and SMTP) if IIOCs are triggered. If you have selected an IIOC to be alertable, then if behavior is detected that matches the IIOC (indicating a potential indicator of compromise), an alert will be generated.

Note: An IIOC triggered on a whitelisted object will not generate an alert.

The following figure shows a high level overview of how alerts are generated in NetWitness Endpoint.



Types of Alerts

There are four types of IIOC alerts defined:

- **Machine.** This alert indicates that a machine has been identified as exhibiting suspicious behavior. The alert will contain details about the identified machine.
- **Module.** This alert indicates that a module (for example, a file, a .dll, or a .exe) has been identified as suspicious. The alert will contain details about the identified module.
- **Network.** This alert indicates that there has been suspicious Internet activity (traffic) seen.
- **Event.** This alert represents any other suspicious activity detected by NetWitness Endpoint that does not fall into the above three categories.

Note: In reality, there are only two objects to which an IIOC can be assigned, Machines and Modules. Events and Network are simply categories that help you define IIOCs that are really Module IIOCs.

Alert Fields

The table below lists all the alerting fields for each of the IIOC types.

Machine	Module	IP	Event	Enabled by default for CEF and AMQP?
agentid (unique ID of agent)	agentid (unique ID of agent)	agentid (unique ID of agent)	agentid (unique ID of agent)	Y
shost (hostname of agent)	shost (hostname of agent)	src (source IP address)	shost (hostname of agent)	Y

Machine	Module	IP	Event	Enabled by default for CEF and AMQP?
src (IP address of agent)	src (IP address of agent)	shost(source hostname)	src (IP address of agent)	Y
smac (mac address of agent)	smac (Mac address)	smac (mac address of agent)	smac (mac address of agent)	Y
	fname (filename)		fname (source module name)	Y
	fsize (size of file in bytes)		fsize	Y
	fileHash (sha1sum of file)		fileHash (source module hash)	Y
instantIOCName (The InstantIOC name)	instantIOCName (The InstantIOC name)	instantIOCName (The InstantIOC name)	instantIOCName (The InstantIOC name)	Y
instantIOCLevel	instantIOCLevel	instantIOCLevel	instantIOCLevel	Y
rt (last scan time)			rt (last scan time)	Y

Machine	Module	IP	Event	Enabled by default for CEF and AMQP?
machineScore				Y
userOU				Y
machineOU				Y
deviceDnsDomain (domain of the agent)				Y
user (last known logged on user on the agent)				Y
	OPSWATResult=< short description>			Y
	YARAResult=< short description>			Y
	ReputationResult=<possible values are unknown, good, suspicious, or malicious>			Y
	moduleScore			Y

Machine	Module	IP	Event	Enabled by default for CEF and AMQP?
	moduleSignature=< short description>			Y
		dst (destination IP address)		Y
		dhost (hostname of destination, if known)		Y
		start (timestamp of start of activity)		Y
		end (timestamp of end of activity)		Y
		destinationDnsDomain (destination domain name, if known)		Y
			sourceModule	Y
			targetModule	Y
gatewayip	gatewayip	gatewayip	gatewayip	N
remoteip	remoteip	remoteip	remoteip	N

Machine	Module	IP	Event	Enabled by default for CEF and AMQP?
os (Operating system)	os (Operating system)	os (Operating system)	os (Operating system)	Y
	timezone	timezone	timezone	N
	sha256sum			N
	md5sum			Y
		protocol		Y
		port		Y
		totalsent		Y
		totalreceived		Y
		useragent		N
		filename		Y

Users can enable or disable any of the fields for CEF and AMQP messages (AMQP is the protocol used to send alerts to the RSA NetWitness Suite Incident Management component). This can be done by editing the ConsoleServer.exe.config file, which is located at the Master ConsoleServer install path. If this file is edited, the RSAECATServer service needs to be restarted for this to take effect. The sections of the config file that controls this are shown below.


```
<MachineAlertFields>
  <add key="agentid" value="True"></add>
  <add key="shost" value="True"></add>
  <add key="src" value="True"></add>
  <add key="smac" value="True"></add>
  <add key="instantIOCName" value="True"></add>
  <add key="instantIOCLLevel" value="True"></add>
  <add key="rt" value="True"></add>
  <add key="machineScore" value="True"></add>
  <add key="userOU" value="True"></add>
  <add key="machineOU" value="True"></add>
  <add key="deviceDnsDomain" value="True"></add>
  <add key="suser" value="True"></add>
  <add key="gatewayip" value="False"></add>
  <add key="remoteip" value="False"></add>
  <add key="os" value="True"></add>
  <add key="timezone" value="False"></add>
</MachineAlertFields>

<ModuleAlertFields>
  <add key="agentid" value="True"/>
  <add key="shost" value="True"/>
  <add key="src" value="True"/>
  <add key="smac" value="True"/>
  <add key="fname" value="True"/>
  <add key="fsize" value="True"/>
  <add key="fileHash" value="True"/>
  <add key="instantIOCName" value="True"/>
  <add key="instantIOCLLevel" value="True"/>
  <add key="OPSWATResult" value="True"/>
  <add key="YARAResult" value="True"/>
  <add key="ReputationResult" value="True"/>
  <add key="moduleScore" value="True"/>
  <add key="machineScore" value="True"/>
  <add key="moduleSignature" value="True"/>
  <add key="gatewayip" value="False"/>
  <add key="remoteip" value="False"/>
  <add key="os" value="True"/>
  <add key="timezone" value="False"/>
  <add key="sha256sum" value="False"/>
  <add key="md5sum" value="True"/>
</ModuleAlertFields>
```

```

<IPAlertFields>
  <add key="agentid" value="True"></add>
  <add key="shost" value="True"></add>
  <add key="src" value="True"></add>
  <add key="smac" value="True"></add>
  <add key="instantIOCName" value="True"></add>
  <add key="instantIOCLLevel" value="True"></add>
  <add key="dst" value="True"></add>
  <add key="dhost" value="True"></add>
  <add key="start" value="True"></add>
  <add key="end" value="True"></add>
  <add key="destinationDnsDomain" value="True"></add>
  <add key="gatewayip" value="False"></add>
  <add key="remoteip" value="False"></add>
  <add key="os" value="True"></add>
  <add key="timezone" value="False"></add>
  <add key="protocol" value="True"></add>
  <add key="port" value="True"></add>

  <add key="totalsent" value="True"></add>
  <add key="totalreceived" value="True"></add>
  <add key="useragent" value="False"></add>
  <add key="filename" value="False"></add>
</IPAlertFields>
<EventAlertFields>
  <add key="agentid" value="True"></add>
  <add key="shost" value="True"></add>
  <add key="src" value="True"></add>
  <add key="smac" value="True"></add>
  <add key="fname" value="True"></add>
  <add key="fsize" value="True"></add>
  <add key="fileHash" value="True"></add>
  <add key="instantIOCName" value="True"></add>
  <add key="instantIOCLLevel" value="True"></add>
  <add key="rt" value="True"></add>
  <add key="sourceModule" value="True"></add>
  <add key="targetModule" value="True"></add>
  <add key="gatewayip" value="False"></add>
  <add key="remoteip" value="False"></add>

  <add key="os" value="True"></add>
  <add key="timezone" value="False"></add>
</EventAlertFields>

```

Users can also customize the list of fields that are part of the Email alert. For more information, see the topic *Email Templates* in [Configure Alerts](#).

Alert Destination

Alerts from NetWitness Endpoint are sent to the following destinations in the following formats.

Note: The Incident Management Broker refers to a component of RSA NetWitness Suite.

Destination	Format	Protocol
Email user	Email	SMTP
Syslog server	Common Event Format	TCP/UDP syslog
Incident Management Broker	JSON	AMQP

Alertable Flags

There are three controls in NetWitness Endpoint that must be satisfied before an alert is triggered. The settings for these controls are at the following levels:

- InstantIOC's alertable flag
- Machine Group's alertable flag
- Destination's alertable flag

InstantIOC's Alertable Flag

Each InstantIOC has an alertable attribute that must be enabled, or else no alerts for this IIOC will be generated. By default, this flag is enabled only for a select few IIOCs.

To enable/disable InstantIOC's alertable flag:

1. In the **Main Menu**, click **InstantIOCs**.
2. Select the desired InstantIOC.
3. In the **InstantIOC** pane, click **Edit**.
4. Check or uncheck the **Alertable** checkbox to enable or disable alerting.
5. Click **Save**.

Note: Some IIOCs may generate a lot of alerts if enabled. As a best practice, you may want to begin testing the alerting functionality with L0 and L1 IIOCs.

Machine Group's Alertable Flag

Each machine is part of a machine group. By default, every machine is part of the "Default" machine group. Each machine group has an alertable flag. This setting allows users to enable/disable alerts from machines at the group level.

To enable/disable a Machine Group's alertable flag:

1. Click **Configure > Machine Groups**.
2. Select the desired machine group.

3. Right-click the machine group, and select **Edit Group**.
4. Check or uncheck the **Enable Alerts** checkbox to enable or disable alerting.
5. Click **Save**.

Destination's Alertable Flag

Syslog server, SMTP server, and Incident Management broker (a component of RSA NetWitness Suite) are the three possible alert destinations in NetWitness Endpoint. You can enable/disable alerting at this level.

To enable/disable the Destination's alertable flag:

1. Click **Configure > Monitoring and External Components**.
2. Check or uncheck the checkbox in the **Enable** column to enable or disable alerts for the component.

Configure Alerts

In NetWitness Endpoint, you can configure three kinds of alerts: Syslog alerts, Incident Management alerts, and Email (SMTP) alerts.

Note: NetWitness Endpoint will trigger a configured alert notification only once, regardless of whether the notification is received successfully by the configured receiver.

In this section, the following processes are explained:

- Configure Syslog Alerts
- Configure Incident Management Alerts
- Configure Email (SMTP) Alerts
- Email Templates
- Test Connectivity
- Modify or Delete an External Component
- Temporarily Disable Alerting

Configure Syslog Alerts

NetWitness Endpoint also has the capability to send Syslog messages to a Syslog server, including RSA Security Analytics, RSA NetWitness for Logs, ArcSight, and others. The message is based on RFC 3164, modified to correspond to ArcSight (CEF) standards, but can be received by any appropriate listener.

Multiple Syslog servers may be added to NetWitness Endpoint. Alerts will be sent to each Syslog server. The act of just adding Syslog servers is not sufficient for NetWitness Endpoint to send alerts. Alerts must be enabled at the Machine Group level and the IIOC must be marked alertable. The messages will be triggered by a score threshold.

Fields that are sent as part of the alert can be customized. For more information, see the topic Alert Fields in [Types of Alerts](#).

Prerequisite: You will need the Syslog server name or IP address, port, and protocol (TCP or UDP).

To configure Syslog alerts:

1. Click **Configure > Monitoring and External Components**.

The **External Components Configuration** window is displayed.

2. From the Components listed, select **SYSLOG Server** and click + to add a new Syslog component.

3. Enter the following fields:

- Instance Name: Enter a unique name to identify the Syslog server.
- Server Hostname/IP: Enter the Host DNS or IP address of the Syslog server.
- Port: Enter the port number.
- Protocol: Select either TCP or UDP using the radio button.

Note: The port is generally 514 for UDP and 1468 for TCP.

4. Click **Save**.

The Syslog server entry is displayed in the Monitoring and External Components list.

Note: Syslog alerts are in CEF alert format.

CEF Alert Format

Main message (values are separated by spaces):

[<PRI>] [TIMESTAMP] [HOSTNAME] [CUSTOM MESSAGE]

Option	Description
<PRI>	<132> (Hardcoded) a (facility*8)+severity where: Facility.Local0=16 Severity.Warning=4

Option	Description
TIMESTAMP	Syslog Timestamp, in the format: mm dd hh:mm:ss
HOSTNAME	Name of the machine that emitted the Syslog

Custom message (values are separated by "|" character):

```
[<CEF HEADER>:<VERSION>] | [DEVICE VENDOR] | [DEVICE PRODUCT] | [DEVICE VERSION] | [SIGNATURE ID] | [NAME] | [SEVERITY] | [EXTENSION]
```

The tables below describe the possible values of these fields.

Field Name	Machine	Module	IP	Event
<CEF HEADER>:<VERSIO N>	CEF:0	CEF:0	CEF:0	CEF:0
DEVICE VENDOR	RSA	RSA	RSA	RSA
DEVICE PRODUCT	RSA ECAT	RSA ECAT	RSA ECAT	RSA ECAT
DEVICE VERSION (This will change on every version of NetWitness Endpoint)	4.3	4.3	4.3	4.3
SIGNATURE ID	MachineIO C	ModuleIO C	IPIOC	SuspiciousEventIO C
NAME	EcatAlert	EcatAler t	EcatAler t	EcatAlert

Field Name	Machine	Module	IP	Event
SEVERITY:	1	1	1	1
Emergency = 0, Alert = 1, Critical = 2, Error = 3, Warning = 4, Notice = 5, Information = 6, Debug = 7.				

Extensions are in the form of **name=value** pairs separated by spaces. If either the **name** or **value** itself contains a space, it's escaped by **<space>** as shown below.

```
fileName=c:\Program<space>Files\RSA
```

Examples of CEF Messages

- Machine Alert

```
05-02-2014 18:23:23 Local0.Warning 127.0.0.1 May 02 18:23:23 INENDEBS1L2C
CEF:0|RSA|RSA
ECAT|4.0.0.33063|MachineIOC|EcatAlert|1|agentid=26C5C21F-4DA8-3A00-437C-AB7444987430
shost=INENDEBS1L2C src=192.168.1.1 smac=11-11-11-11-11-11-11-11
instantIOCName=TestIOC instantIOCLLevel=3 rt=05/02/2014<space>12:53:23
machineScore=1-2-3-4
userOU=CN\=Surname,<space>Alice,OU\=Engineering,OU\=IN<space>TestCity<space>RSA,OU\=
TestCountry,OU\=International<space>Users,DC\=corp,DC\=example,DC\=com
machineOU=CN\=MACHINENAME,OU\=Servers,DC\=corp,DC\=example,DC\=com
deviceDnsDomain=example.com suser=example\alice os=Windows<space>7
```

- Module Alert

```
05-02-2014 18:23:23 Local0.Warning 127.0.0.1 May 02 18:23:23 INENDEBS1L2C
CEF:0|RSA|RSA
ECAT|4.0.0.33063|ModuleIOC|EcatAlert|1|agentid=26C5C21F-4DA8-3A00-437C-AB7444987430
shost=INENDEBS1L2C src=192.168.1.1 smac=11-11-11-11-11-11-11-11 fname=filename.exe
fsize=23562
fileHash=de9f2c7f<space>d25e1b3a<space>fad3e85a<space>0bd17d9b<space>100db4b3
instantIOCName=TestIOC instantIOCLLevel=3 OPSWATResult=OPSWAT<space>result<space>here
YARAResult=N<space>YARA<space>rules<space>matched ██████████ moduleScore=1-2-3-4
moduleSignature=ABC<space>Inc. os=Windows<space>7
md5sum=0x00000000000000000000000000000000
```

- IP Alert

```
05-02-2014 18:23:23 Local0.Warning 127.0.0.1 May 02 18:23:23 INENDEBS1L2C
CEF:0|RSA|RSA
ECAT|4.0.0.33063|IPIOC|EcatAlert|1|agentid=26C5C21F-4DA8-3A00-437C-AB7444987430
shost=INENDEBS1L2C src=192.168.1.1 smac=11-11-11-11-11-11-11-11
instantIOCName=TestIOC instantIOCLLevel=3 dst=192.168.1.1 dhost=host.example.com
start=05/02/2014<space>12:53:23 end=05/02/2014<space>13:53:23
destinationDnsDomain=example.com os=Windows<space>7 protocol=http port=80
totalsent=2345 totalreceived=12345
```

- Event Alert

```
05-02-2014 18:23:23 Local0.Warning 127.0.0.1 May 02 18:23:23 INENDEBS1L2C
CEF:0|RSA|RSA
ECAT|4.0.0.33063|SuspiciousEventIOC|EcatAlert|1|agentid=26C5C21F-4DA8-3A00-437C-AB74
44987430 shost=INENDEBS1L2C src=192.168.1.1 smac=11-11-11-11-11-11-11-11
fname=filename.exe fsize=23562
fileHash=de9f2c7f<space>d25e1b3a<space>fad3e85a<space>0bd17d9b<space>100db4b3
instantIOCName=TestIOC instantIOCLLevel=3 rt=05/02/2014<space>12:53:23
sourceModule=Source.dll targetModule=Target.dll os=Windows<space>7
```

Configure Incident Management Alerts

Alerts can be sent to the RSA Security Analytics Incident Management solution. The act of just adding an Incident Management (IM) broker is not sufficient for NetWitness Endpoint to send alerts. Alerts must be enabled at the Machine Group level and the IIOC must be marked alertable.

Fields that are sent as part of the alert can be customized. For more information, see *Alert Fields* in the topic [Types of Alerts](#). For information about Incident Management Integration, see *Incident Management Integration* in the topic [RSA NetWitness Suite Integration](#).

Configure Email (SMTP) Alerts

The act of just adding an SMTP server is not sufficient for NetWitness Endpoint to send alerts. Alerts must be enabled at the Machine Group level and the IIOC must be marked alertable. Also, the email server must be configured to be open-relay.

The format of the email body can be customized. For more information, see the topic *Email Templates* below.

Prerequisites: You will need the following SMTP details:

- The SMTP server hostname or IP address
- The SMTP port
- Sender's email ID (should be anonymous email ID)
- A list of email recipients

To configure Email alerts:

1. Click **Configure > Monitoring and External Components**.
The **External Components Configuration** window is displayed.
2. From the Components listed, select **SMTP Configuration** and click + to add a new SMTP component.
3. Enter the following fields:
 - Instance Name: Enter a unique name to identify the SMTP server.
 - Server Hostname/IP: Enter the hostname of the SMTP server.
 - Port: Enter the port number.

Note: The port is generally 25.

4. Provide the required information in the Email Address fields.
5. Add one or more recipients.
6. Click **Save**.

Email Templates

Email alerts from NetWitness Endpoint can be customized by the user. There are email templates for each of the IIOC alerts. The email templates can be found at the Master ConsoleServer installation path. For example:

C:\Program Files (x86)\RSA\ECAT\Server

The templates are in the form of an XML file, which is listed below.

Alert Type	Template Filename
Machine	machine_ioc_email_template.xml
Module	module_ioc_email_template.xml
IP	ip_ioc_email_template.xml
Event	event_ioc_email_template.xml

The file is an HTML file that the user can customize. Any word in the file enclosed within "{" and "}" is a variable that is replaced by the real value. For more information about the variables, see *Alert Fields* in the topic [Types of Alerts](#).

The RSAECATServer service needs to be restarted for the changes to take effect.

Caution: The variables must be one of the alert fields or else the RSAECATServer service will not start.

Test Connectivity

After a Syslog server, an IM broker, or an SMTP server are added to NetWitness Endpoint, you may send test alerts to test connectivity.

To test connectivity:

1. Click **Configure > Monitoring and External Components**.
The **Configure External Components** window is displayed.
2. From the Components listed on the left options pane, select the external component you want to test.
3. Click **Test Settings**.
4. Go to your component and verify that four messages, one for each alert type, were received.

Note: For SYSLOG, there will be four CEF messages. For IM Broker, there will be four AMQP messages. For SMTP, there will be four emails.

Note: For Test Settings to work properly, make sure that API Server is running as an application or a service.

Modify or Delete an External Component

The process is the same for any external component.

To modify or delete an external component:

1. Click **Configure > Monitoring and External Components**.
The **Configure External Components** window is displayed.
2. Select the external component you wish to modify or delete.
3. To edit the component, click **Edit** and make the changes.
4. To delete the component, click minus sign (-) on the left options pane or the main window.
5. Save the settings by closing all the dialog boxes.

Temporarily Disable Alerting

You may disable alerting for a particular external component.

To disable alerting:

1. Click **Configure > Monitoring and External Components**.
2. Locate the external component you wish to temporarily disable.
3. Uncheck the checkbox under the **Enable** column.

Note: If you wish to enable alerting, check the **Enable** checkbox.

MANAGE USERS

NetWitness Endpoint provides the following user management functionality:

- Pre-configured roles - There are four roles created automatically during NetWitness Endpoint installation. Additional custom roles can also be added. For more information see [Role-Based Access Control](#).
- User Management - NetWitness Endpoint Admin users can perform a variety of user management tasks such as creating users and assigning roles. For more information, see [Manage Users and Roles](#).
- User management control is available through the NetWitness Endpoint UI and the associated SQL database.

Role-Based Access Control

Role-based access control in NetWitness Endpoint allows NetWitness Endpoint Administrators to more precisely control what information each user can access and manipulate by assigning a specifically configured role to each NetWitness Endpoint user.

Note: By default, all users who are assigned a "sysadmin" SQL role will be assigned the NetWitness Endpoint Admin role. NetWitness Endpoint considers it a best practice to limit this to just one user as this user is responsible for accepting End User License Agreements (EULAs) and therefore also has legal responsibilities.

With role-based access control, access to each module, dashlet, and view within the NetWitness Endpoint UI is restricted based on the role and the permissions assigned to that role. The roles determine what users can do. A role has permissions assigned to it and you must assign a role to each user. The user then has permission to do what the role allows.

Pre-Configured Roles

To simplify the process of creating roles and assigning permissions, there are pre-configured roles in the NetWitness Endpoint UI. These pre-defined roles are added during NetWitness Endpoint installation. After installation, the admin user can also add customized roles based on specific requirements. There are two permanent roles that cannot be modified or deleted: ECAT Admin and ECAT Read-Only.

The following table lists each pre-configured role and the permissions assigned to it. The ECAT Admin user will have all the permissions. A subset of permissions is assigned to each of the other roles.

Role	Permission
ECAT Admin	<p>Full system access. The System Administrator role is granted all permissions by default.</p> <div style="border: 1px solid green; padding: 5px;"> <p>Note: NetWitness Endpoint recommends that there be only one user with the ECAT Admin role. Also, to perform all functions available to this role, the user must also be assigned "sysadmin" privileges in SQL.</p> </div>
ECAT Read-Only	All the actions in which a user can view data.
L1 Analyst	Read-Only access plus the following basic task areas: basic scan, edit module status, forensics, import/export, module actions, scan groups, UI related
L2 Analyst	L1 Analyst tasks plus the following task areas: analyze (such as with SA), certificates, configuration, IIOC, remediation (which includes containment), scan with external, schedule time specification, server configuration discovery

Role Permissions

Users assigned to a role can only access the NetWitness Endpoint tasks and information according to the permissions assigned to the role. In addition to the pre-configured roles installed automatically, ECAT Admin users can also create custom roles. For more information on creating roles and viewing role permissions, see the topic [Manage Users and Roles](#). When an NetWitness Endpoint user logs in to NetWitness Endpoint, menu items and actions not permitted by that user's assigned role are disabled or grayed-out. The permissions granted to the current user's assigned role can be viewed by clicking **About** in the NetWitness Endpoint top menu.

The following table describes in detail the 18 permissions available to assign to user roles:

Role Permission	Description
Agent Maintenance – Update or uninstall agents	Grants the user the ability to update the deployed endpoint agents to a newer version or remove the deployed agent from the endpoint.

Role Permission	Description
Analyze – Analyze with NetWitness Suite, analyze a module	Allows the analyst access to the Analyze Module detail window for a selected module. If NetWitness integrations are configured, the user will be permitted to access the Analysis functionality with those tools.
Basic Scan – Request or cancel a scan	Allows the user to request a scan of a single endpoint or group of endpoints. Any of the available scan types (Full, Basic, or Quick) are allowed. This user may also cancel a previously requested scan of an endpoint.
Certificates – Flag a certificate vendor as trusted, remove trusted flags, edit trusted status, edit trusted domains	Allows the user to modify the trusted state of module certificates and domains.
Configure – Configure connection, time zones, internet search engines, monitoring & external components, global parameters, administrative status, machine groups, update certificates	Allows the user to configure various global settings applicable to the Console Server. This is traditionally a permission reserved for the NetWitness Endpoint Administrator.
Edit Module Status – Edit Blacklist/Whitelist status, edit trusted domains, modify status, modify comments, modify modules to block	Allows users to access the Edit Blacklist/Whitelist status dialog found when right-clicking on a module. From here, users may modify its whitelist and blacklist status, attach comments to a module, or adjust blocking settings for that module.

Role Permission	Description
Forensics – Request files, request MFT, request full memory dump, reboot endpoint	Allows a user to perform more invasive tasks upon an endpoint. The user may request arbitrary files and directories by path or request a Master File Table (MFT) from the endpoint, which would contain the layout of the entire file system and a list of its contents. This user may also request a snapshot of the current state of the endpoint’s RAM and reboot the endpoint.
IIOC – Modify IIOCs: Clone, delete, edit, create new	Allows for the maintenance and management of the defined IIOCs. The user may clone an IIOC to use it as the basis for a new one, delete or edit an existing IIOC, or create a new IIOC. This management setting is typically reserved for an administrator, high-level analyst, or threat intelligence specialist.
Import/Export – Export to Excel, standalone scan - export scan configuration, standalone scan – import scan data, import/export blacklist/whitelist file, RSA Live, Checksum	Allows the user to import or export various configurations and data via the UI. The user may also obtain and import RSA Live information through the offline Console Server Sync tool.
Module Related Tools – Module Analyzer, MFT Viewer, Search with File Advisor, Google & Virus Total, Open in new module view, View certificates	Allows a user to gain additional visibility into various modules. With this permission, the user may open the module analyzer, use the MFT viewer to request files from an endpoint, perform various external searches against the modules (such as with Google and Virus Total), and view certificates associated with the module.
Module Actions – Add to trusted domains, download to server, save a local copy, assign module	Allows the user to request a module be downloaded to the Console Server or, for a module already downloaded, save a copy of the module to the local system. With this permission, users may assign floating code to a particular module within the Scan Data tab.

Role Permission	Description
Remediation – Reboot, remediate, show diagnostics, remove selection from database, module blocking and machine containment	This permission provides access to the endpoint management and diagnostic tasks found in the Advanced menu after right-clicking on an endpoint. The user may reboot the endpoint, remove an endpoint from the database, and add the diagnostic tab to the display. Additionally, the user may configure blocking of individual modules and machine containment throughout the environment.
Scan Groups – Configure groups, add machine to group, remove machine from a group	Allows the user to configure machine group settings, including adding or removing endpoints from machine groups.
Scan with External – Scan with YARA or OPSWAT	Allows the user to scan a downloaded module with one of the supported external scanners. YARA is an open-source scan tool typically configured upon NWE deployment. OPSWAT is a third-party commercial AV tool installed separately.
Schedule Time Spec – Local to client, local to server, UTC	When scheduling scans via Machine Groups, allows a user scheduling a scan to determine what time zone is used – the time zone local to the client, local to the server, or UTC. UTC is the default time zone if this permission is not granted.
Server Configuration – Commission new server, change DNS or IP, Decommission server, configure cloud	Provides access to the settings within the Server Configuration window of the main menu. Within this window, users may add servers to a Multi-Server Architecture, modify hostnames/IP addresses of currently configured servers, and add or remove RAR servers from the configuration. This permission is commonly reserved for the administrator performing initial set-up of the NetWitness Endpoint services.
Server Configuration Discovery – Start or pause discovery	Server discovery is the act of allowing new endpoints to be recognized by and added to the current Console Server. This permission allows the user to pause this discovery, thus preventing new endpoints from being added.

Role Permission	Description
UI Related – Copy data, copy data with header, access dashboard, configure skins	Allows the user basic access to the UI. This permission allows the user to view and adjust the dashboard, apply various skins to the UI, and copy endpoint data displayed in the UI.

Manage Users and Roles

This topic provides information about accessing NetWitness Endpoint user information and performing the user management tasks that can be performed by a NetWitness Endpoint Administrator.

Note: By default, all users who are assigned a "sysadmin" SQL role will be assigned the ECAT Admin role and these users will not be displayed in the **Users** tab of the **Security** window. NetWitness Endpoint considers it a best practice to limit this to just one user as this user is responsible for accepting EULAs and therefore also has legal responsibilities.

Access User and Role Information

You can perform various user management tasks from the **Users** or **Roles** tabs, as follows:

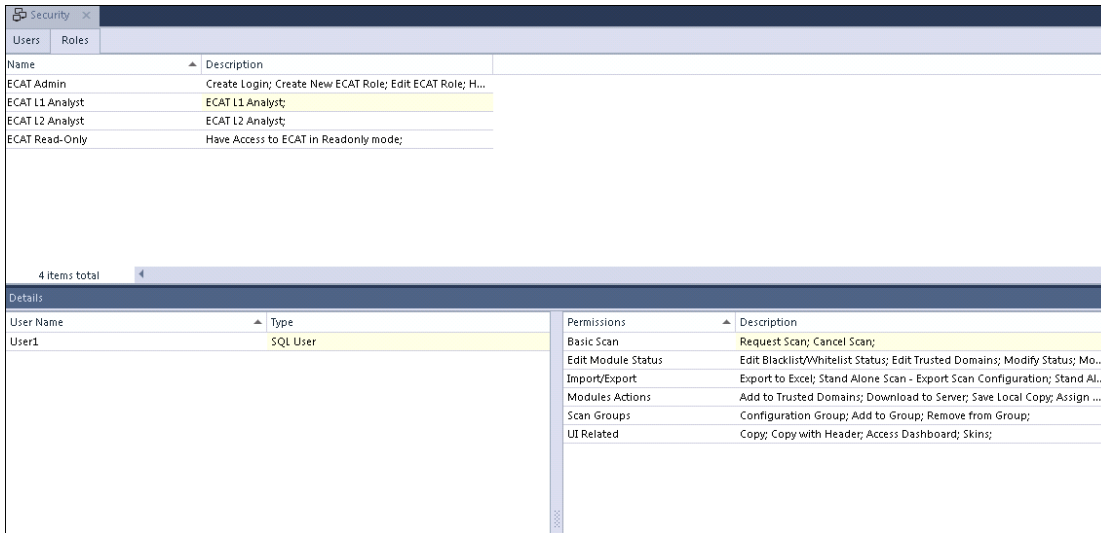
- From the top menu, select **Configure > Manage Users and Groups**.
The **Security** window is displayed, which contains the **Users** and **Roles** tabs.
- The **Users** tab lists all NetWitness Endpoint users (SQL users and Microsoft users), as shown below:

Security	
Users	
Name	Type
User1	SQL User
User2	SQL User

2 items total

Details	
Name	Description
ECAT L1 Analyst	ECAT L1 Analyst;
ECAT Read-Only	Have Access to ECAT in Readonly mode;

- By selecting a user, the details for that user are displayed at the bottom of the window. By default, any user is automatically assigned the "ECAT Read-Only" role.
 - You can add roles to the user by right-clicking the user and selecting **Add to Role**.
 - For other user management tasks that can be performed using the **Users** tab, see the *Perform User Management Tasks* section below.
3. The **Roles** tab displays the pre-configured and customized roles, as shown below:



- You can create and manage roles and permissions by right-clicking and selecting the option.
- By selecting a role, the details of that role are displayed at the bottom of the window. The left pane displays the users associated with that role and the right pane displays the permissions assigned to that role.
- For other user management tasks that can be performed using the **Roles** tab, see the *Perform Role Management Tasks* section below.

Note: The permissions do not display for the ECAT Admin or the ECAT Read-Only roles.

Perform User Management Tasks

The administrator can perform the following user management tasks from the **Users** tab:

1. Create SQL User
2. Add SQL User

3. Add Windows User
4. Remove User
5. Add to Role
6. Remove from Role
7. Reset Password

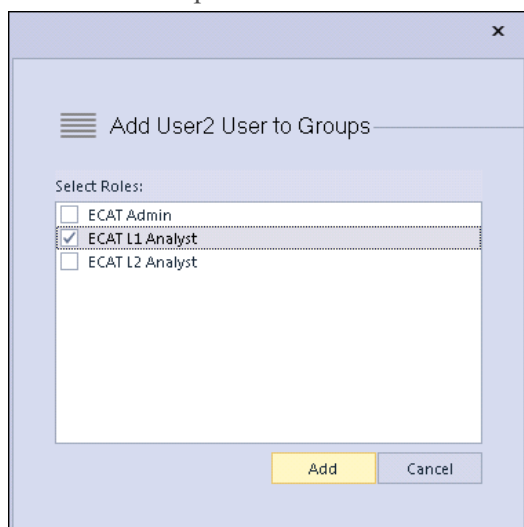
To perform user management tasks:

1. From the top menu, select **Configure > Manage Users and Groups**.
The **Security** window is displayed.
2. Select the **Users** tab. The following options are available by right-clicking:
 - **Create SQL User** - This option allows you to create a SQL user.
 - **Add SQL User** - This option allows you to add an existing SQL user.
 - **Add Windows User** - This option allows you to add an existing Windows user. The Username must be in the format Domain\Username.

Note: Only users with SQL "sysadmin" privileges or ECAT Admin users created by users with SQL "sysadmin" privileges are able to create other users.

- **Remove User** - This option allows you to delete the user.
- **Add to Role** - This option allows you to add the user to an existing role. You can also add multiple roles to a single user.

NOTE: Although the option is available to assign the ECAT Admin role to a user, NetWitness Endpoint recommends restricting this role to just one user.



- **Remove from Role** - This option allows you to remove one or more roles from the selected user.
- **Reset Password** - This option allows you to reset the password for the selected SQL user. You do not need to know the previous password to perform this function. Windows users will need to contact their System Administrator to reset a password.

Note: SQL users may reset their own passwords using the Reset Password link on the NetWitness Endpoint Login dialog.

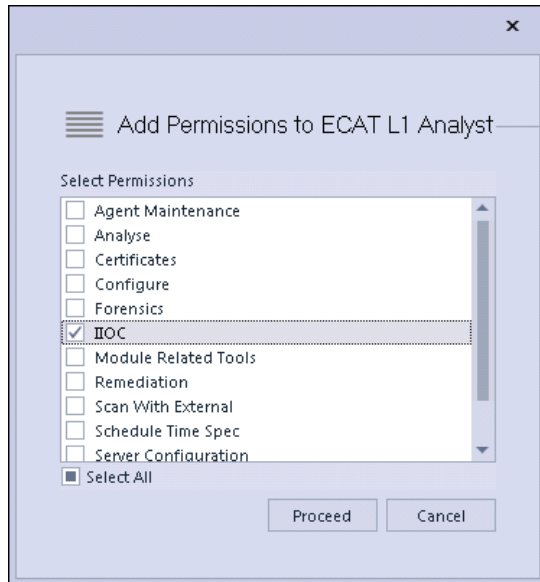
Perform Role Management Tasks

The administrator can perform the following role management tasks from the **Roles** tab:

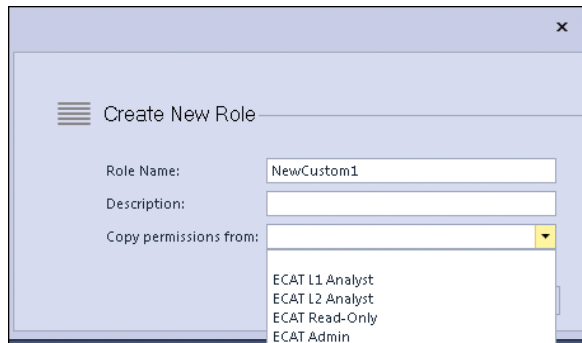
1. Add User(s)
2. Remove User(s)
3. Add Permission(s)
4. Remove Permission(s)
5. Create Role
6. Delete Role

To perform role management tasks:

1. From the top menu, select **Configure > Manage Users and Groups**.
The **Security** window is displayed.
2. Select the **Roles** tab. The following options are available by right-clicking:
 - **Add User(s)** - This option allows you to add one or more users to the selected role.
 - **Remove User(s)** - This option allows you to remove one or more users from the selected role.
 - **Add Permission(s)** - This option allows you to add new permissions to the selected role. This option is disabled for "ECAT Admin" and "ECAT Read-Only" roles.



- **Remove Permission(s)** - This option allows you to remove permissions from the selected role. This option is disabled for "ECAT Admin" and "ECAT Read-Only" roles.
- **Create Role** - This option allows you to create a new custom role.



The **Copy permissions from** drop-down option allows you to copy permissions from an existing role to the new role. You can then further customize the new role by adding or removing the associated permissions as described above.

- **Delete Role** - This option allows you to delete the selected role. This option is disabled for "ECAT Admin" and "ECAT Read-Only" roles. Any users that were assigned to the deleted roll will still have the default "ECAT Read-Only" role privileges.

MONITORING AND EXTERNAL COMPONENTS

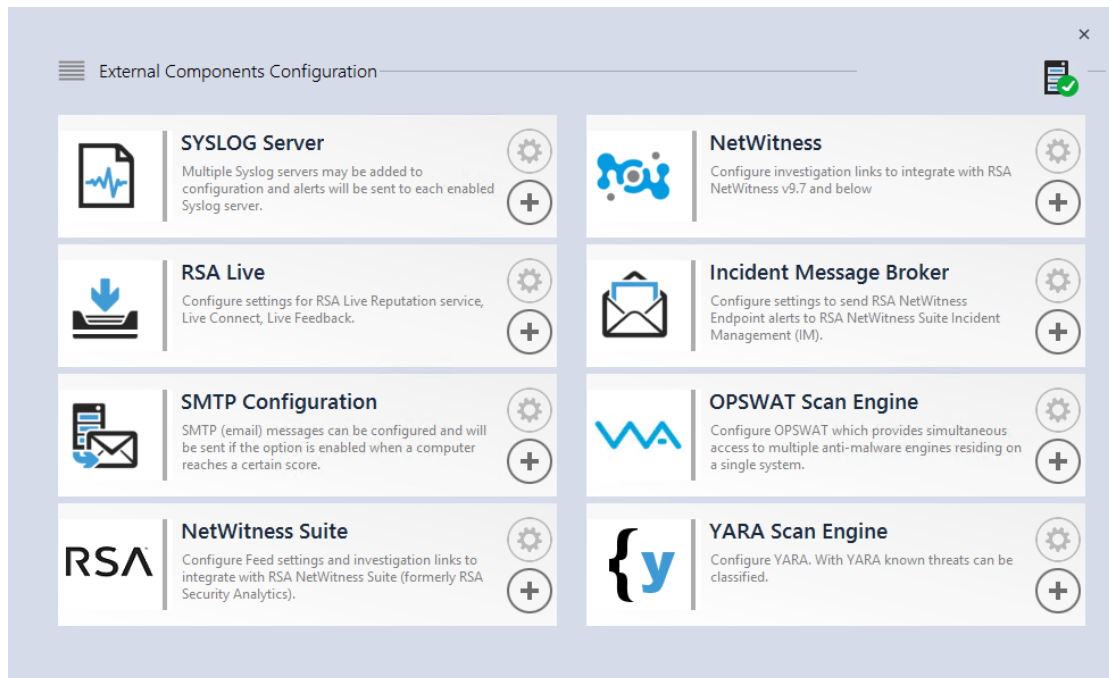
This topic provides information about how to configure monitoring and external components. You can configure the following external components:

- [RSA NetWitness Suite Integration](#)
- [NetWitness Suite Endpoint Meta Integration](#)
- [RSA Live](#)
- [RSA NetWitness v9.7](#)
- [SMTP](#)
- [OPSWAT Scan Engine](#)
- [YARA Scan Engine](#)

Configure External Components

To configure External Components:

1. Click **Configure > Monitoring and External Components**.
The **External Components Configuration** window is displayed.



2. To add a component:
 - a. Click + next to the component to be added.
 - b. Enter the required details.
 - c. Click **Save**. The component is added to NetWitness Endpoint.
3. To edit a component:
 - a. Click the settings button next to the component.
 - b. Click **Edit** and make the required changes.
 - c. Click **Save**.

RSA NetWitness Suite Integration

This topic is relevant if you have NetWitness Endpoint and NetWitness Suite (previously System Analytics) products. You must have a basic understanding of NetWitness Suite and how to access NetWitness Suite documentation on [RSA Link](#).

NetWitness Suite is a security-monitoring platform that combines network monitoring, traditional log-centric SIEM, forensics, and big data management and analytics. You can configure NetWitness Endpoint with NetWitness Suite to provide additional information on the network activities. With this integration, analysts investigating network connections in NetWitness Endpoint can directly query NetWitness Suite for more detailed information about the network connection.

NetWitness Endpoint regularly runs Indicator of Compromise (IOC) queries on new scan data, which are collected and stored in the database. Whenever NetWitness Endpoint identifies a potential IOC it generates an alert, which is reported to the user or sent to an external system. For more information about Alerts, see [Manage Alerts](#).

One such external system is NetWitness Suite, which can accept NetWitness Endpoint alerts. NetWitness Suite can further assist security analysts in investigating the IOCs detected by NetWitness Endpoint.

Integrate NetWitness Endpoint with NetWitness Suite

You can configure the NetWitness Endpoint integration with NetWitness Suite from the NetWitness Endpoint UI, as described in the following sections. For configuration within NetWitness Suite, refer to the NetWitness Suite documentation on [RSA Link](#).

There are three types of integration points for NetWitness Endpoint data to be sent to NetWitness Suite:

- RSA Feed Integration
- Syslog Integration
- Incident Management Integration

RSA Feed Integration

The NetWitness Endpoint Server generates a .CSV file after scanning the agents. The .CSV file contains information about all scanned agents. This metadata is exported to NetWitness Suite for further analysis.

The following table shows the fields included in the .CSV file.

Column #	NetWitness Endpoint Feed Fields	Description	Column Name in NetWitness Suite (Meta Key Name)
1	MachineName	Host name of the Windows agent	alias.host
2	LocalIp	IPv4 address	index
3	RemoteIp	Far end IP as seen by the router	stransaddr

Column #	NetWitness Endpoint Feed Fields	Description	Column Name in NetWitness Suite (Meta Key Name)
4	GatewayIp	IP of the gateway	gateway
5	MacAddress	MAC address	eth.src
6	OperatingSystem	Operating system used by the Windows agent	OS
7	AgentID	Agent ID of the host (unique ID assigned to the agent)	client
8	ConnectionUTCTime	Last time the agent connected to NetWitness Endpoint server	ecat.ctime
9	Source Domain	Domain	domain.src
10	ScanUTCTime	Last time the agent was scanned	ecat.stime
11	Machine Score	Score of the agent indicating the suspicion level	risk.num
12	UserName	User name of the client machine	Username

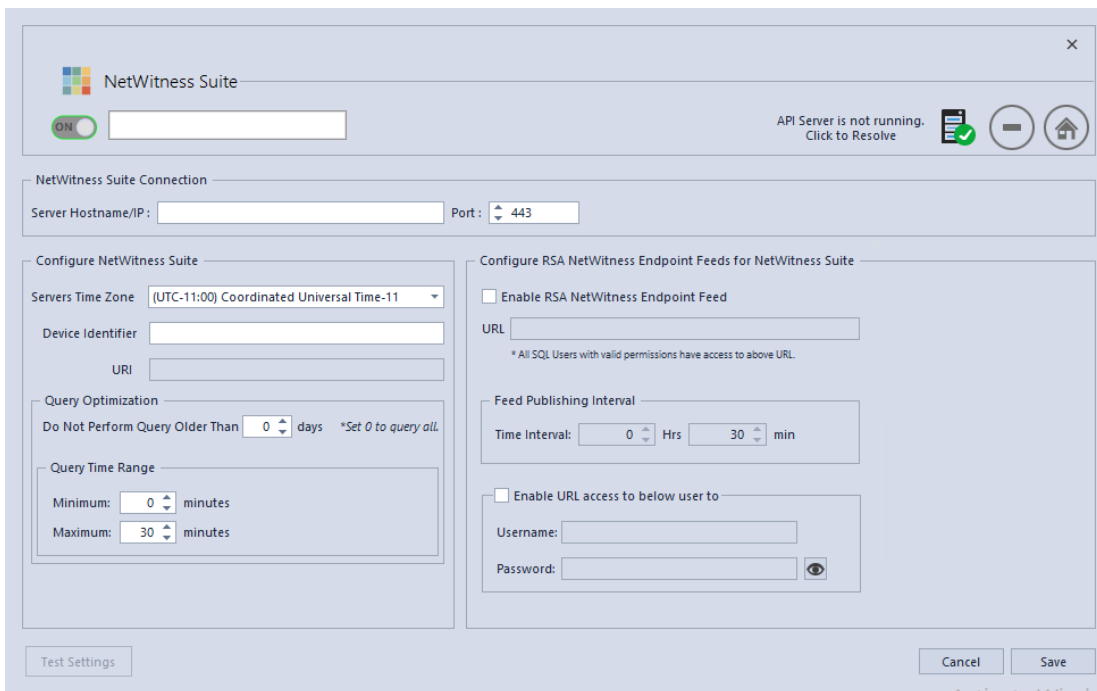
To set up integration of the NetWitness Endpoint .CSV file feed with NetWitness Suite:

1. Configure .CSV feed in NetWitness Endpoint.
2. Export the NetWitness Endpoint CA certificate from the NetWitness Endpoint ConsoleServer and import it into the NetWitness Suite trust store.
3. Configure the feed in NetWitness Suite (edit the index file of the concentrator to add the custom meta keys of NetWitness Endpoint).
4. Create a recurring feed in NetWitness Suite Live.

Configure the .CSV Feed in NetWitness Endpoint

To configure the .CSV feed:

1. Click **Configure > Monitoring and External Components**.
The **External Components Configuration** window is displayed.
2. From the Components listed, select **NetWitness Suite** and click + to add a new NetWitness Suite component.



3. In the NetWitness Suite dialog, next to **ON**, enter a unique instance name.
4. Enter the Server Hostname or IP address of the NetWitness Server.
5. The default port number is 443. Update the field if needed.
6. Configure the additional settings on the **Configure NetWitness Suite** and **Configure NetWitness Endpoint Feeds for NetWitness Suite** panes.
7. In the **Configure NetWitness Suite** pane, enter the fields appropriately.

Note: The Device Identifier is your NetWitness Suite concentrator device ID. You can find the Device Identifier in NetWitness Suite when you look up a Concentrator or Broker in **Investigation > Navigate > <Concentrator or Broker Name>**. The Device Identifier is the number in the URL after "investigation." For example, in the URL `https://<IP address>investigation/319/navigate/values`, the Device Identifier is "319."

8. In the **Configure NetWitness Endpoint Feeds for NetWitness Suite** pane, do the following:

- a. Check the **Enable NetWitness Endpoint Feed** checkbox.
 - b. Enter a username and password for a SQL user previously configured for NetWitness Endpoint. This will be used later by NetWitness Suite to retrieve the feed. If necessary, you can create a new SQL user in the NetWitness Endpoint UI by selecting **Configure > Manage Users and Roles**, then right-clicking and selecting **create sql user**.
 - c. Select your **Feed Publishing Interval**.
9. Click **Save** and **Close** the dialog.

Export the NetWitness Endpoint CA Certificate from the NetWitness Endpoint ConsoleServer

To export the NetWitness Endpoint CA certificate to the NetWitness Suite trust store:

1. Export the NetWitness Endpoint Server CA certificate. To export the NetWitness Endpoint CA certificate using mmc, see the topic *Exporting Certificates from the ConsoleServer Machine* in "Step 4: Backup Primary Server Certificates" of the *RSA NetWitness Endpoint 4.4 Installation Guide*.
2. Import the CA certificate to the NetWitness Suite trust store. For further details on importing the certificate into NetWitness Suite, see RSA NetWitness Suite documentation on [RSA Link](#).

To edit the index file of the concentrator, see NetWitness Suite documentation on [RSA Link](#).

For more detailed directions for creating a recurring feed, see the *RSA NetWitness Endpoint Integration Guide*, available on [RSA Link](#).

Syslog Integration

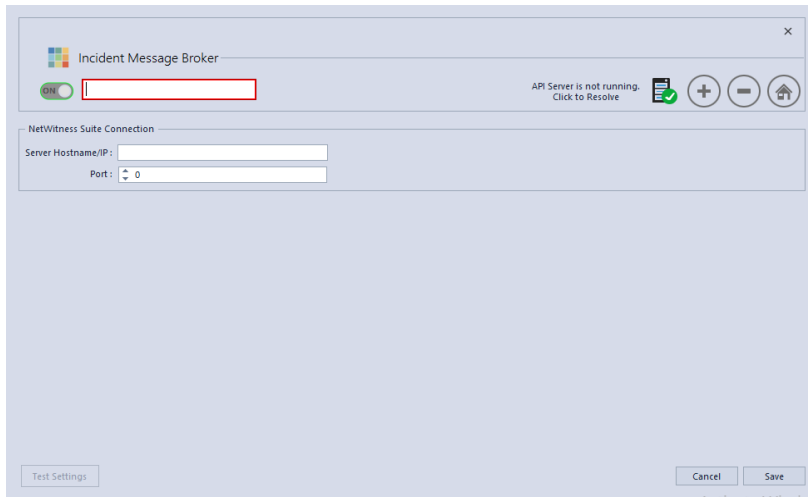
For information about Syslog integration, see *Configuring Syslog Alerts* in the topic [Configure Alerts](#).

NetWitness Respond Integration

NetWitness Endpoint alerts can also be sent to NetWitness Respond (previously called Incident Management) .

To configure NetWitness Respond integration:

1. Click **Configure > Monitoring and External Components**.
The **External Components Configuration** window is displayed.
2. From the Components listed, select **Incident Message Broker** and click + to add a new IM component.



3. Enter the following fields:
 - Instance Name: Enter a unique name.
 - Server Hostname/IP: Enter the Host DNS or IP address of the IM broker (NetWitness Server).
 - Port number: The default port is 5671.
4. Click **Save**.
5. Navigate to the `ConsoleServer.exe.config` file in `C:\Program Files\RSA\ECAT\Server`.
6. Modify the virtual host configurations in the file as follows:


```
<add key="IMVirtualHost" value="/rsa/system" />
```

Note: In NetWitness Suite 11.0, the virtual host is `/rsa/system`". For version 10.6.x and below, the virtual host is `/rsa/sa`".
7. Restart the API Server and ConsoleServer.
8. To set up SSL for Respond Alerts, perform the following steps in the NetWitness Endpoint Primary ConsoleServer to set the SSL communications:
 - a. Export the NetWitness Endpoint CA certificate to .CER format (Base-64 encoded X.509) from the personal certificate store of the local computer (without selecting the private key). To export the NetWitness Endpoint CA certificate using mmc, see the topic Exporting Certificates from the ConsoleServer Machine in "Step 4: Backup Primary Server Certificates" of *RSA NetWitness Endpoint 4.4 Installation Guide*.

Note: When referring to the *Exporting Certificates from the ConsoleServer Machine* topic, follow steps 1 to 10 and select **No, do not export the private key**. Click **Next** and choose .CER format to export. Continue to follow steps 13 to 20.

- b. Generate a client certificate for NetWitness Endpoint using the NetWitness Endpoint CA certificate. (You **MUST** set the CN name to **ecat**. Run cmd.exe console with Administrator rights)

```
makecert -pe -n "CN=ecat" -len 2048 -ss my -sr LocalMachine -a
sha1 -sky exchange -eku 1.3.6.1.5.5.7.3.2 -in "NWECA" -is MY -ir
LocalMachine -sp "Microsoft RSA SChannel Cryptographic Provider" -
cy end -sy 12 c:\client.cer
```

Note: In the previous code sample, if you upgraded to version 4.3 (or later) from a previous version and did not generate new certificates, you should substitute "ECATCA" for "NWECA".

Or, if your current operating system has PowerShell version 5.1 or later, you can use the following code sample:

```
PS C:\> New-SelfSignedCertificate -KeyExportPolicy Exportable -
Subject "CN=ecat" -KeyAlgorithm RSA -KeyLength 2048 -
CertStoreLocation "cert:\LocalMachine\My" -HashAlgorithm SHA256 -
KeySpec KeyExchange -TextExtension @("2.5.29.37=
{text}1.3.6.1.5.5.7.3.2,1.3.6.1.5.5.7.3.1") -Provider "Microsoft
RSA SChannel Cryptographic Provider" -KeyUsage DigitalSignature,
KeyEncipherment, KeyAgreement -Signer (Get-ChildItem -Path
Cert:\LocalMachine\My\ -DnsName NweCA) -NotAfter (Get-Date).AddYears
(5); Export-Certificate -Cert (Get-ChildItem -Path
Cert:\LocalMachine\My\ -DnsName ecat) -FilePath C:\Client.cer
```

- c. Make a note of the thumbprint of the client certificate generated in step b. Enter the thumbprint value of the client certificate in the **IMBrokerClientCertificateThumbprint** section of the **ConsoleServer.Exe.Config** file as shown.

```
<add key="IMBrokerClientCertificateThumbprint"
value="896df0efacf0c976d955d5300ba0073383c83abc"/>
```

9. On the NetWitness Server, copy the NetWitness Endpoint CA certificate file in .CER format (from step a) into the import folder: `/etc/pki/nw/trust/import`.
10. Issue the following command to initiate the necessary Chef run:
- ```
orchestration-cli-client --update-admin-node
```
- This appends all of those certificates into the truststore.

- Restart the RabbitMQ server:

```
systemctl restart rabbitmq-server
```

The NetWitness Endpoint account should automatically be available on RabbitMQ.

- Import the `/etc/pki/nw/ca/nwca-cert.pem` and `/etc/pki/nw/ca/ssca-cert.pem` files from the NetWitness Server and add them to the Trusted Root Certification stores in the NetWitness Endpoint Server.

## NetWitness Suite Endpoint Meta Integration

The NetWitness Endpoint Meta Integration with the NetWitness Suite (version 10.6.5 or later) offers customers that have both products a way to more easily take advantage of their products in a single user interface. With this feature, users can collect meta from selected machines where NetWitness Endpoint agents are deployed. The NetWitness Endpoint Meta Integrator converts the data and sends it to the NetWitness Suite Log Decoder. The meta can then be viewed in the associated NetWitness Suite Concentrator and also in NetWitness Suite Investigate.

**Note:** In version 11.1, you can also configure the NetWitness Endpoint 4.4.0.2 Console Server to collect meta from an Endpoint Hybrid or Endpoint Log Hybrid machine. For more information, see [Integrating the Endpoint 4.4.0.2 or Later Console Server with an Endpoint Hybrid or Endpoint Log Hybrid](#).

## Meta Integrator Installation

During NetWitness Endpoint installation, the Meta Integrator is installed by default with the ConsoleServer and is installed to the same location (default location is `C:\Program Files\RSA\ECAT\Server`). The Meta Integrator is controlled through the `MetaIntegrator.jar` file, which requires that you also have Java JRE version 8 update 131 or later installed as well. Log files related to the Meta Integrator are stored in the same location.

**Note:** Only Java JRE version 8 and its updates are supported. Java JRE versions 9 or later are not supported.

During the installation for either the NetWitness Endpoint Primary Server or Secondary Server, if you select the option to run the server as a service, the Meta Integrator will also be installed to run as a service. Once installed, the Meta Integrator service will be displayed as "RSA NWE Meta Service" in the list of services.

**Note:** It is not necessary to install the Meta Integrator as a service to use this functionality. If you did not install it as a service, see the [Enable the Meta Integrator](#) section below for configuration options.

If you did not select to run the NetWitness Endpoint server as a service during installation but want to create the RSA NWE Meta Service at a later time, navigate to the NetWitness Endpoint server folder (default location is C:\Program Files\RSA\ECAT\Server) and run the following command in the command prompt: `MetaService.exe /install`.

If you want to make changes to the NWE Meta Service after installation, such as the default port, do the following:

1. Stop the RSA NWE Meta Service.
2. Go to the NetWitness Endpoint server folder (default location is C:\Program Files\RSA\ECAT\Server).
3. Open the `MetaService.exe.config` file.
4. To change the default port listened to by the Meta Integrator JAR file, edit the value in the "metaintegratorPort" field.
5. To change the logging level, edit the value in the "metaintegratorLogLevel" field. Applicable values are "INFO", "DEBUG", and "ERROR".
6. Restart the RSA NWE Meta Service.

To uninstall the RSA NWE Meta Service, navigate to the NetWitness Endpoint server folder (default location is C:\Program Files\RSA\ECAT\Server) and run the following command in the command prompt: `MetaService.exe /uninstall`.

**Note:** You must enable the Meta Integrator manually as it is disabled by default following installation of NetWitness Endpoint, as described below.

## Enable the Meta Integrator

Enabling the Meta Integrator requires three separate configurations, as described in the following sections.

### Enable/Disable the Meta Integrator on the NetWitness Endpoint ConsoleServer

You must enable the Meta Integrator on the ConsoleServer and specify the IP address of the NetWitness Suite Log Decoder you are using for the integration to be complete. You can enable or disable the Meta Integrator using command line parameters in the ConsoleServer configuration file. This is also where you set the directory for the JSON files generated by the CSV to JSON converter, which can be used for debugging purposes.

**Note:** In a NetWitness Endpoint multi-server environment, the Meta Integrator must be enabled on all servers, primary and secondary.

To enable the Meta Integrator:

1. Using the command prompt, go to the NetWitness Endpoint server folder.
2. Enter the following command: `ConsoleServer.exe /nw-investigate enable`.
3. As shown below, you will be prompted to enter certain details. You can select to use default values for some of the entries according to the comments shown in the prompt.

**Note:** Be sure to specify an existing and valid NetWitness Suite user at this prompt.

```

Administrator: C:\Windows\system32\cmd.exe

C:\Program Files\RSA\ECAT\Server>ConsoleServer.exe /nw-investigate enable
Enter the below required details to configure NetWitness Investigate
Logdecoder IP:10.4.1.15
Logdecoder Port (Default 56202 for SSL. Press Enter to use default port):
Log decoder Rest Port(Default 50102. Press Enter to use default port) :
Log decoder Rest Username:admin
Log decoder Rest Password:*****
(Optional. Use only for debug) Enter folder location where converted jsons are t
o be written. Press Enter to ignore.

Enter the base Uri for Meta integrator. Default is http://localhost:7058. Press
Enter to use default (Change this only if Meta integrator is running on a differ
ent port)

17 11:34:38:8369 Connecting to database (local) on ECAT$PRIMARY ...
17 11:34:39:4600 Done.

C:\Program Files\RSA\ECAT\Server>_

```

4.

Once the Meta Integrator is enabled, and if running as an application (not as a service), if you want to change the port number and logging level, do one of the following:

- To change only the port number, run the command: `java -Dserver.port=<Port number here> -jar MetaIntegrator.jar`
- To change both the port number and logging level, run the command: `java -Dserver.port=<Port number here> -Dlogging.level.ROOT=<Value here> -jar MetaIntegrator.jar`.

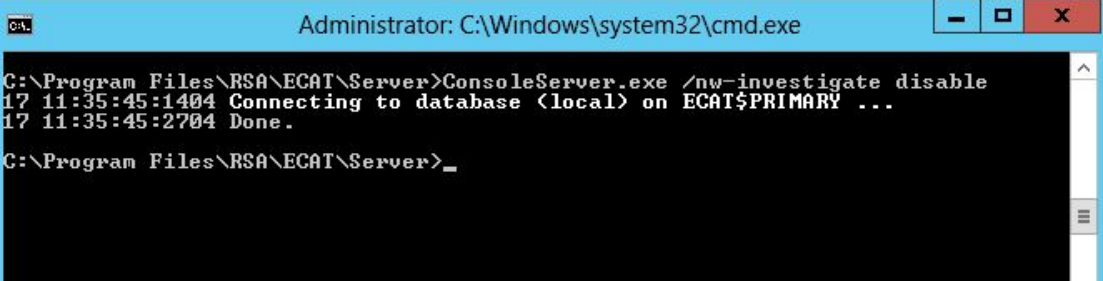
For example: `java -Dserver.port=8000 -Dlogging.level.ROOT=DEBUG -jar MetaIntegrator.jar`.

**Note:** If a web proxy is configured on the system, you may need to add an exception for the NWE Meta Service to successfully connect to Log Decoder. Refer to "Configure Proxy Settings of ConsoleServer" in the *NetWitness Endpoint 4.4 Installation Guide*.



To disable the Meta Integrator:

1. Using the command prompt, go to the NetWitness Endpoint server folder.
2. Enter the following command: `ConsoleServer.exe /nw-investigate disable`.



```
Administrator: C:\Windows\system32\cmd.exe
C:\Program Files\RSA\ECAT\Server>ConsoleServer.exe /nw-investigate disable
17 11:35:45:1404 Connecting to database (local) on ECAT$PRIMARY ...
17 11:35:45:2704 Done.
C:\Program Files\RSA\ECAT\Server>_
```

For help with the ConsoleServer configuration options:

1. Using the command prompt, go to the NetWitness Endpoint server folder.
2. Enter the following command: `ConsoleServer.exe -help`. A list of all available command options is displayed in the command prompt window.

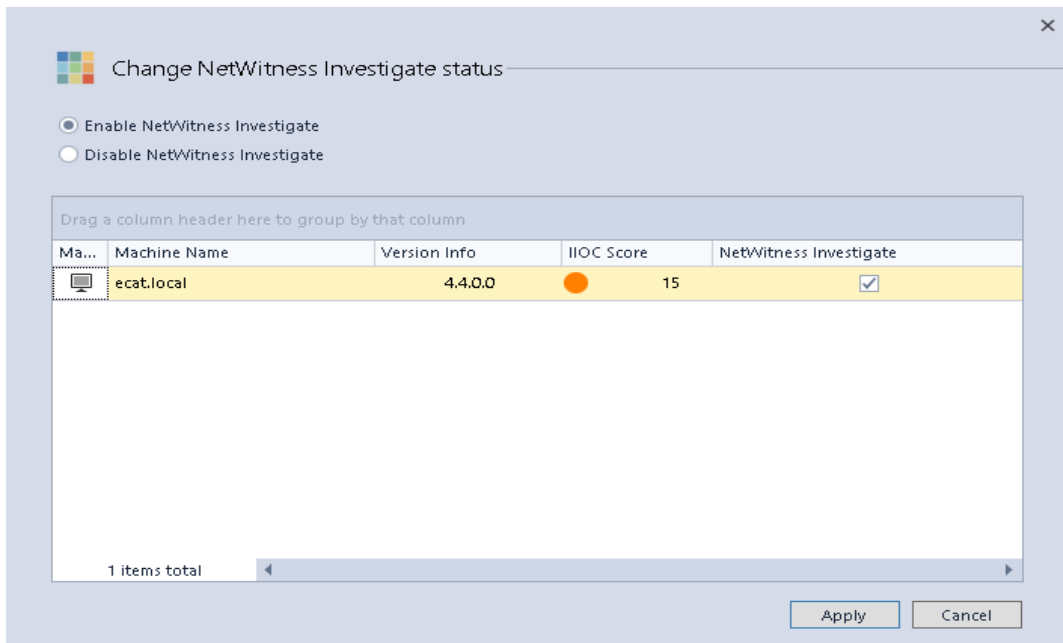
### **Enable/Disable Meta Collection for Individual Agents**

Once the Meta Integrator is enabled, you must individually select and activate meta collection for NetWitness Endpoint agents. The Meta Integration Status column in the Machines table indicates whether meta is currently being collected for each machine.

To enable/disable meta collection for an agent:

1. In the Machines table, select one or more machines, then right-click and select **NetWitness Investigate....**

The Change NetWitness Investigate status dialog is displayed, listing the machine(s) selected in the Machines table.



2. Do one of the following:
  - Click the **Enable NetWitness Investigate** option to enable this feature on the selected machine(s).
  - Click the **Disable NetWitness Investigate** option to disable this feature on the selected machine(s).
3. Click **Apply**.
4. Any currently in-progress meta integration downloads will finish before the status change is completed.
5. The following status messages will display in the bottom left corner of the Machines table:
 

Changing NetWitness meta integration status...

NetWitness meta integration status change succeeded.

### Add Firewall Rule to the NetWitness Suite Log Decoder

For NetWitness Suite to receive the NetWitness Endpoint metas successfully, you must add a firewall rule to the Log Decoder server. Without this firewall rule, the Log Decoder will drop all meta received from the NetWitness Endpoint ConsoleServer.

To add the firewall rule (for RHEL/CentOS 6):

1. On the NetWitness Suite Log Decoder machine, locate the `/etc/sysconfig/iptables` file.
2. Add the following two lines to the file before the COMMIT keyword:
 

(For non-SSL traffic)

```
-A INPUT -p tcp -m multiport --ports 50202 -m comment --comment "4
```

```

NWE Meta Integrator LogDecoder Port" -j ACCEPT
(For SSL traffic)
-A INPUT -p tcp -m multiport --ports 56202 -m comment --comment "4
NWE Meta Integrator LogDecoder SSL Port" -j ACCEPT

```

**Note:** If the NetWitness Suite Log Decoder is running RHEL/CentOS 7, you do not need to create this firewall rule.

## Meta Configuration File

You can control and manipulate the meta shared with NetWitness Suite through a configuration file. The `metakeysconfiguration.xml` file is installed to the same location as NetWitness Endpoint and the Meta Integration file (see above). The metakey configuration file defines all of the data elements collected from the agents and specifies which of the elements can be shared with the NetWitness Suite. A portion of the configuration file is shown in the following figure.

```

1 <!--All keys are case sensitive
2 Order mentioned here in the file is important. This will be the order in which meta will be present within the session-->
3 <metakeysconfiguration>
4 <category id="common" enabled="true"> <!--Retain it as true always-->
5 <mapping njsonidentifier="Category" metakey="category" datatype="Text" enabled="true"/>
6 <mapping njsonidentifier="mvecallbackid" metakey="mve.callback_id" datatype="Text" enabled="true"/>
7 <mapping njsonidentifier="machineAgentId" metakey="id_unique" datatype="Text" enabled="true"/>
8 <mapping njsonidentifier="machineName" metakey="devicehostname" datatype="Text" enabled="true"/>
9 <mapping njsonidentifier="networkInterfaces.ipv4" metakey="hostip" datatype="IPv4" enabled="true"/>
10 <mapping njsonidentifier="networkInterfaces.macAddress" metakey="smacaddr" datatype="MAC" enabled="true"/>
11 </category>
12 <category id="autorun" enabled="true">
13 <mapping njsonidentifier="registryPath" metakey="directory" datatype="Text" enabled="true"/>
14 <mapping njsonidentifier="type" metakey="autorun_type" datatype="Text" enabled="true"/>
15 <mapping njsonidentifier="launchArguments" metakey="query" datatype="Text" enabled="true"/>
16 <mapping njsonidentifier="filepath.path" metakey="directory" datatype="Text" enabled="true"/><!--filepath here means - look
17 <mapping njsonidentifier="file.firstFilename" metakey="filename" datatype="Text" enabled="true"/><!--file here means - look
18 <mapping njsonidentifier="file.checksumSha256" metakey="checksum" datatype="Text" enabled="true"/><!--file here means - look
19 <mapping njsonidentifier="file.checksumSha1" metakey="checksum" datatype="Text" enabled="true"/><!--file here means - look
20 <mapping njsonidentifier="file.checksumMd5" metakey="checksum" datatype="Text" enabled="true"/><!--file here means - look
21 </category>
22 <category id="certificate" enabled="true">
23 <mapping njsonidentifier="subject" metakey="cert_subject" datatype="Text" enabled="true"/>
24 <mapping njsonidentifier="friendlyName" metakey="cert_common" datatype="Text" enabled="true"/>
25 <mapping njsonidentifier="issuer" metakey="cert_ca" datatype="Text" enabled="true"/>
26 </category>

```

As you can see in the above figure, the metakey configuration file is divided into categories, with more specific mapping elements within each category. All categories and elements are initially enabled by default. With the exception of the first category (`id = "common"`), which should always be enabled, you can disable any other categories or individual mapping elements, as follows:

- To disable an entire meta category, change its `enabled` tag to `"false"` (see red outline in the above figure).
- To disable a specific mapping element, change its `enabled` tag to `"false"` (see blue outline in the above figure).

You can also modify the metakey configuration file in other ways, such as changing metakey names or format types.

**Note:** Whenever you modify the metakey configuration file, you must restart the Meta Service for the configuration changes to take effect.

## Agent Meta Collection

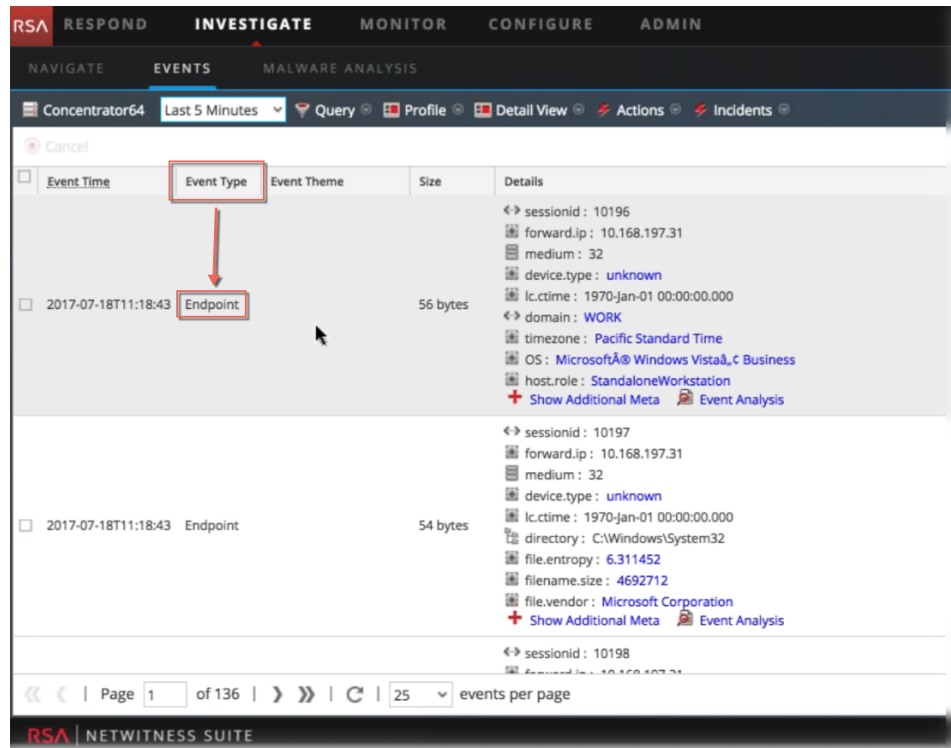
When the Meta Service is enabled, subsequent agent scans will be used to collect meta from all active NetWitness Endpoint agents that have been enabled for meta collection. However, depending on the operating system (Windows, Linux, OS-X), some of the metakeys will have different values. Tracking data will also be sent with the meta to the NetWitness Suite and be viewable with the other meta.

## View Agent Meta in NetWitness Suite

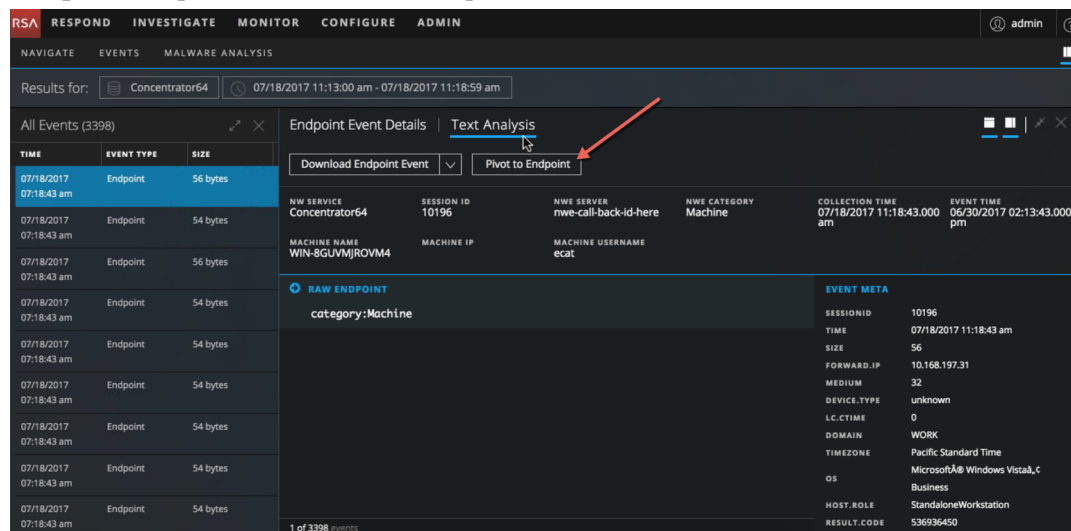
For users that have both NetWitness Suite 10.6.5 (or later) and NetWitness Endpoint 4.4 (or later) installed (and have enabled the Meta Service), you can view the NetWitness Endpoint meta in NetWitness Suite, as follows:

1. Log in to NetWitness Suite.
2. Go to **INVESTIGATE**.
3. In the **Navigate** view, select the Concentrator that aggregates data for the Log Decoder specified when you enabled the NetWitness Endpoint Meta Service.
4. Go to the **Events** view to see the NetWitness Endpoint meta. You can easily identify meta collected from NetWitness Endpoint agents as it will have an event type of "Endpoint", as

shown below.



5. You can continue to investigate Endpoint events using the event analysis tools available in NetWitness Suite.
6. When viewing endpoint event details for a specific machine, you can click **Pivot to Endpoint** to open the NetWitness Endpoint Thick Client, as shown below.



7. When the NetWitness Endpoint Thick Client opens, it will automatically show the Machine View for the specific machine for which you were viewing events in NetWitness Suite Investigate.

## **Integrating the Endpoint 4.4.0.2 or Later Console Server with an Endpoint Hybrid or Endpoint Log Hybrid**

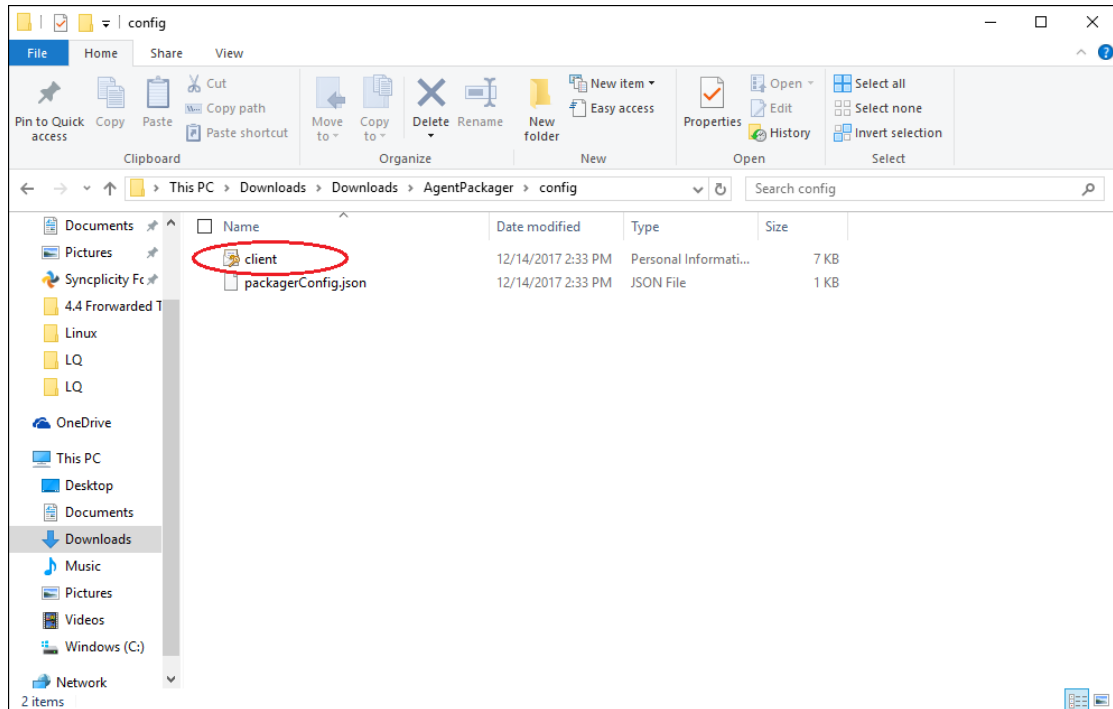
The NetWitness Endpoint 4.4.0.2 or later agents data are available in the Investigate > Hosts and Files view, and you can view the NetWitness Endpoint metadata in the **Investigate > Navigate and Event Analysis** view. For this option, make sure the NetWitness Endpointserver is configured for meta forwarding. This integration includes the following steps:

- [Configuring the Client Certificate on the NetWitness Endpoint 4.4.0.2 Console Server](#)
- [Enabling the Metadata Forwarding in the NetWitness Endpoint 4.4.0.2](#)
- [Enabling Machines to Forward Metadata from the NetWitness Endpoint 4.4.0.2 to the NetWitness Endpoint Server](#)

### **Configuring the Client Certificate on the NetWitness Endpoint 4.4.0.2 Console Server**

The NetWitness Endpoint 4.4.0.2 Console Server must use the same client certificate that the NetWitness Endpoint11.1 agents use to forward the metadata to the Endpoint Server.

1. Download the agent packager. For more information, see *Endpoint Insights Agent Installation Guide* *Endpoint Agent Installation Guide*.
2. Extract **AgentPackager.zip** and from the Config folder, obtain the client certificate.
3. Copy the client certificate to the NetWitness Endpoint 4.4 Console Server.

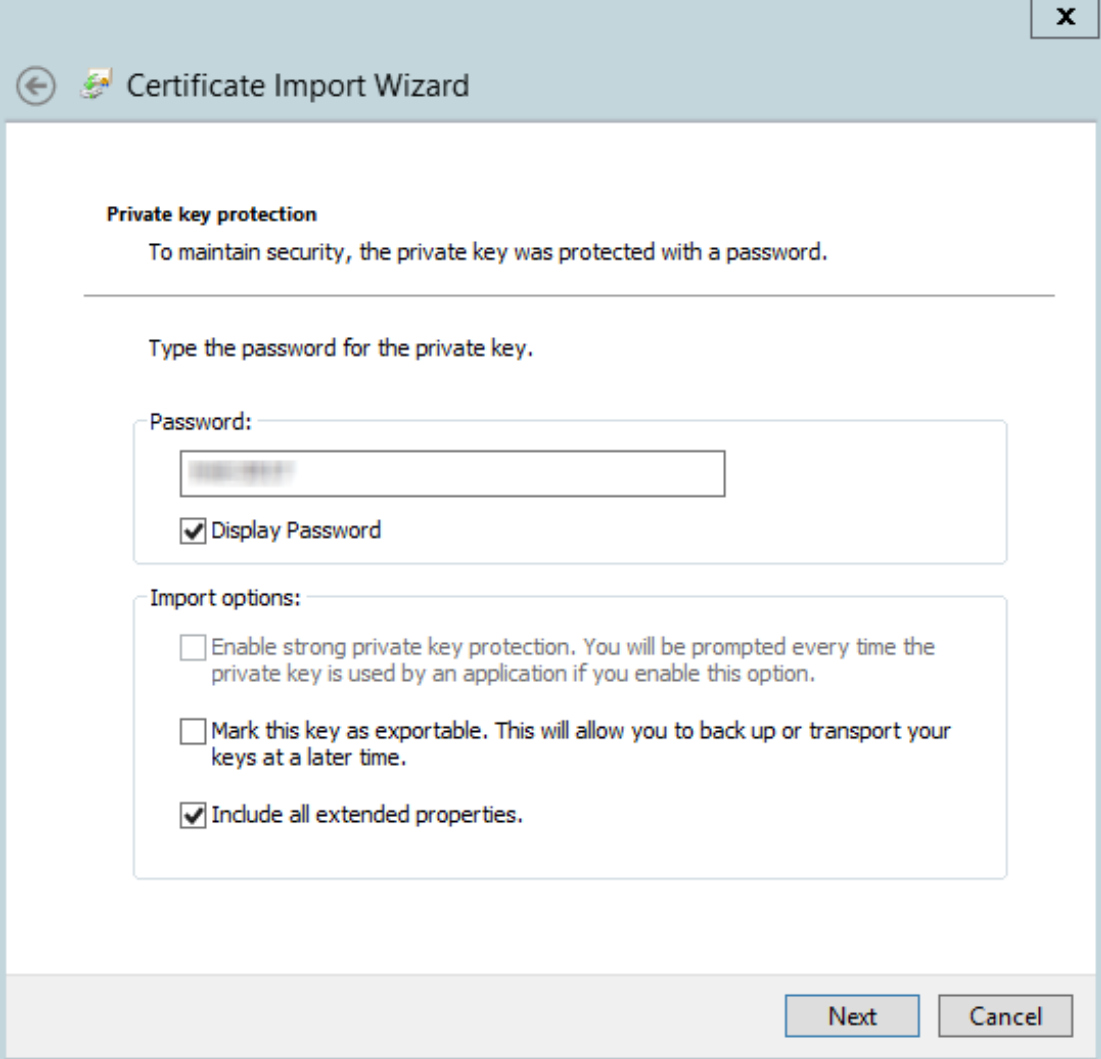


4. Double-click on the **client** file.  
The **Certificate Import Wizard** dialog is displayed.
5. Select the store location as **Local Machine** and click **Next**.



6. Browse the file you want to import and click **Next**.
7. Enter the same password used while generating the agent packager.

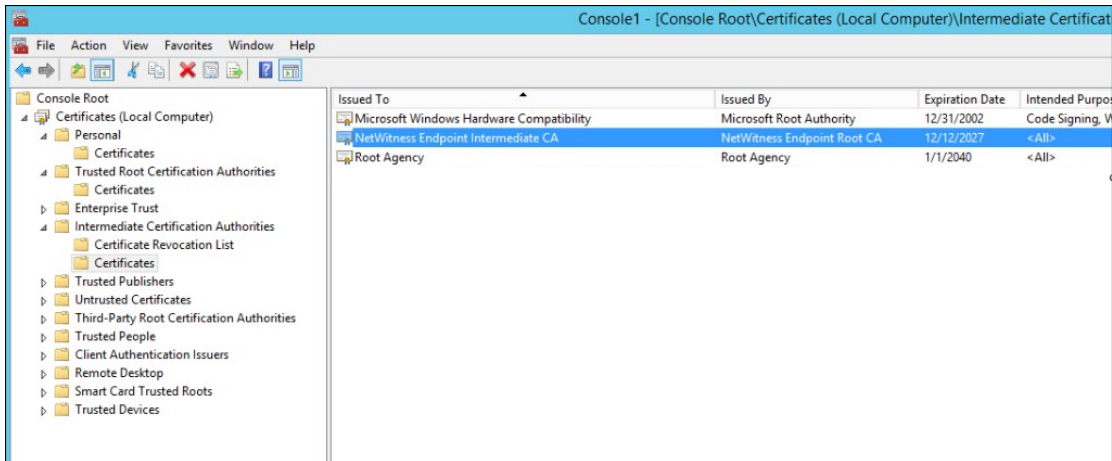




The image shows a 'Certificate Import Wizard' dialog box. The title bar includes a back arrow, a certificate icon, and the text 'Certificate Import Wizard', along with a close button (X). The main content area is titled 'Private key protection' and contains the following text: 'To maintain security, the private key was protected with a password.' Below this is a horizontal line and the instruction 'Type the password for the private key.' There is a 'Password:' label followed by a text input field containing a masked password. Below the input field is a checked checkbox labeled 'Display Password'. Underneath is an 'Import options:' section with three checkboxes: 'Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option.' (unchecked), 'Mark this key as exportable. This will allow you to back up or transport your keys at a later time.' (unchecked), and 'Include all extended properties.' (checked). At the bottom right, there are 'Next' and 'Cancel' buttons.

8. Click **Next** and **Finish**.

The certificate is listed under **Personal, Intermediate Certificate Authorities > Certificate** and **Trusted Root Certification Authorities** in the Console Server.



### Enabling the Metadata Forwarding in the NetWitness Endpoint 4.4.0.2

To enable the metadata forwarding for the selected NetWitness Endpoint 4.4.0.2 agents, run the following command:

```
ConsoleServer.exe /nw-investigate set-endpointdecoder baseuri <ENDPOINT HOST> certificate rsa-nw-endpoint-agent filepath c:\Json
```

```
C:\Program Files\RSA\ECAT\Server>ConsoleServer.exe /nw-investigate set-endpointdecoder baseuri https://... certificate rsa-nw-endpoint-agent
14 06:34:37:4979 Connecting to database (local) on ECAT$PRIMARY ...
14 06:34:37:5099 WARNING: Using SA authentication...
14 06:34:37:5139 Done.
C:\Program Files\RSA\ECAT\Server>
```

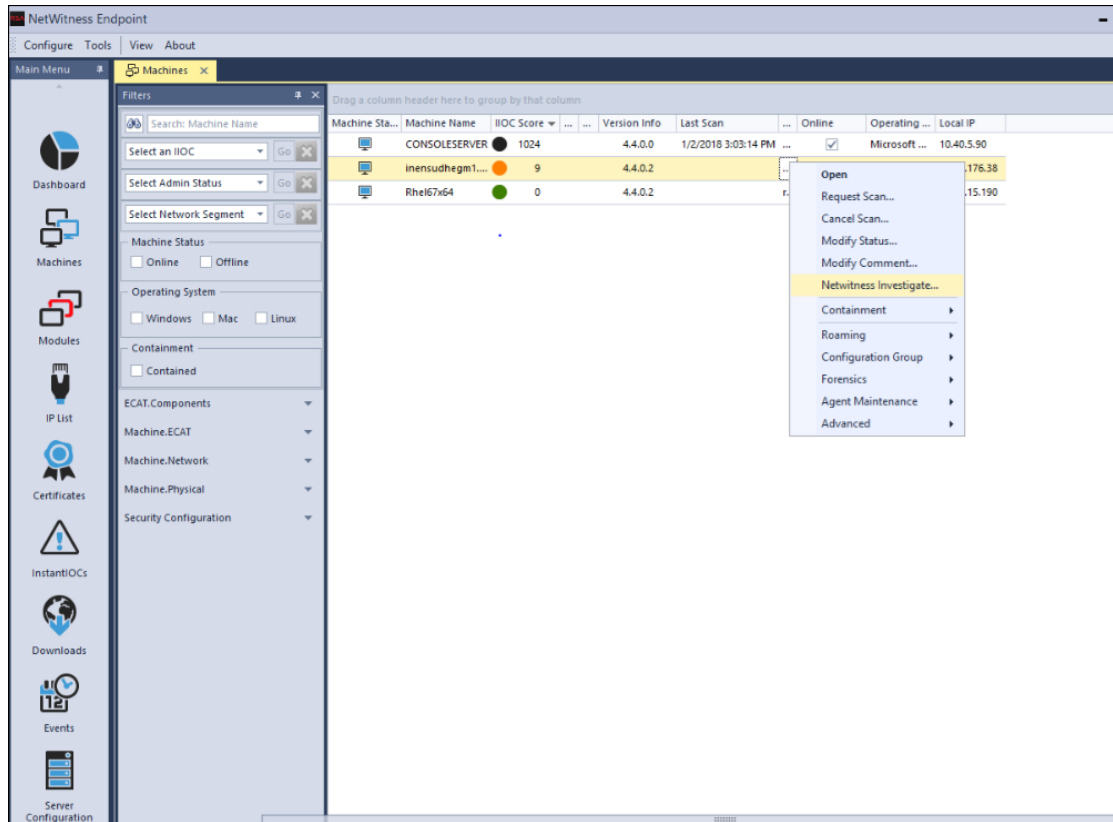
For example:

```
ConsoleServer.exe> /nw-investigate set-endpointdecoder baseuri
https://10.255.255.255 certificate rsa-nw-endpoint-agent filepath
c:\Json
```

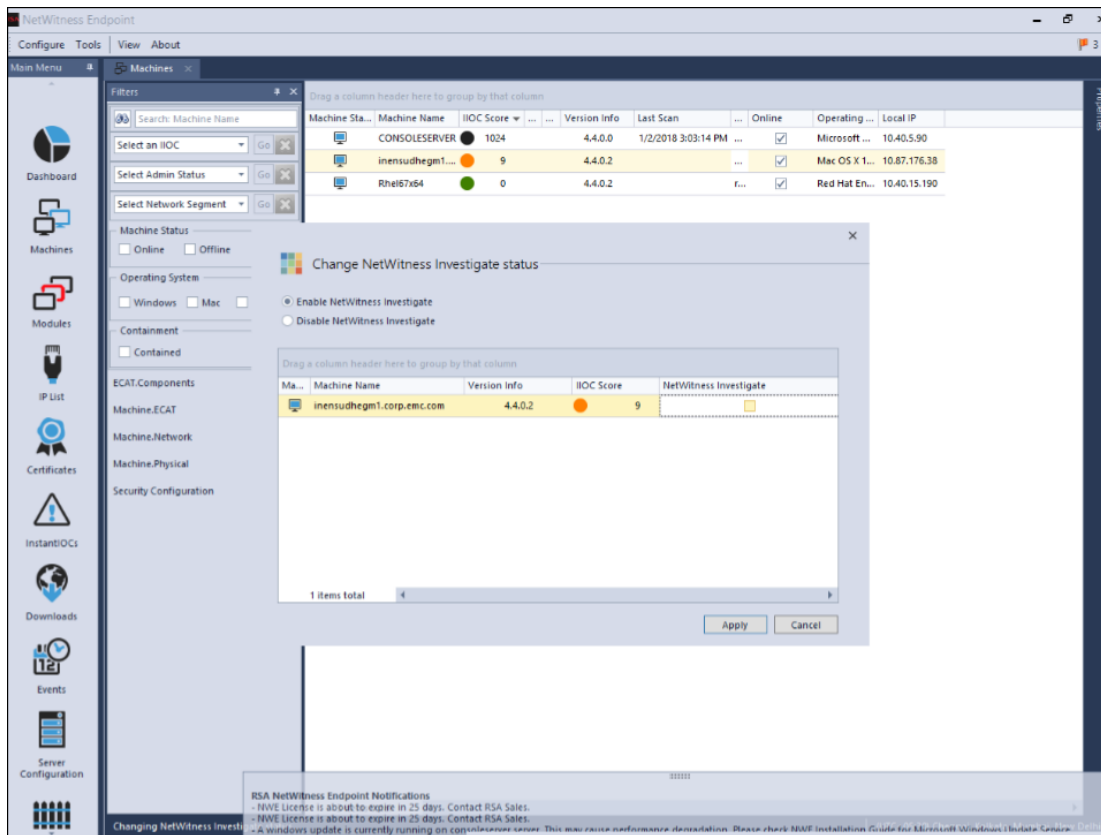
### Enabling Machines to Forward Metadata from the NetWitness Endpoint 4.4.0.2 to the NetWitness Endpoint Server

After you enable the Metadata Forwarding using any one of the above options, perform the following to enable the machines to forward metadata.

1. Open the NetWitness Endpoint 4.4.0.2 user interface.
2. Click **Machines** from the left panel. The list of available machines are displayed.



3. Select machines for which you want to forward metadata to the NetWitness Endpoint Server.
4. Right-click and select the **NetWitness Investigate** option.  
The Change NetWitness Investigate Status dialog is displayed.



5. Select the **Enable NetWitness Investigate** option.
6. Click **Apply**.
7. To verify if the **Enable NetWitness Investigate** option is enabled, repeat step 4.

For more detailed information on viewing and analyzing endpoint events in NetWitness Suite, see the *NetWitness Suite 11.0 Investigation and Malware Analysis User Guide*, available on [RSA Link](#).

## RSA Live

RSA Live is a threat intelligence delivery system that benefits your security team by reducing the time it takes to identify, assess, and respond to incidents. RSA partners with the most trusted and reliable providers in the security community, along with RSA FirstWatch, to deliver, correlate, and illuminate the most pertinent information to your organization and fuse it with your network and log data in real time.

NetWitness Endpoint can be configured to receive feeds from RSA Live. Several feeds in RSA Live contain suspicious domains and IP addresses. Several IIOC's defined within NetWitness Endpoint can benefit from these feeds from an intelligence perspective.

**Note:** You must have an RSA Live account to use the NetWitness Endpoint [File Reputation Service](#) or the [RSA Live Connect](#) service.

**Note:** NetWitness Endpoint does not publish any feeds into RSA Live. It is only a consumer of feeds.

## Configure RSA Live in NetWitness Endpoint

The following is required before you can configure RSA Live in NetWitness Endpoint:

- An RSA Live account. If you do not have an account, you can request one by clicking the link provided in the RSA Live dialog, as shown below.
- The NetWitness Endpoint ConsoleServer should be able to connect to <https://cms.netwitness.com>.

To configure RSA Live in NetWitness Endpoint:

1. Go to **Configure > Monitoring and External Components**.  
The **Configure External Components** window is displayed.
2. From the Components listed, select **RSA Live** and click + to add a new Live component.  
The RSA Live dialog is displayed, as shown below.

**RSA Live**

ON

**RSA Live Settings**  
[If you do not have a RSA Live account, click here to create one](#)  
 Username:  Server Hostname/IP:   
 Password:  Port:

**RSA Services**  
 Reputation service  OFF Live Connect Threat Intelligence Service (Beta)  OFF

**RSA Live Subscribed Feeds**  
 Refresh Interval:  Hour(s)

| Feed Name              | Subscribed               | Count | Error Message | Last Updated           |
|------------------------|--------------------------|-------|---------------|------------------------|
| Malware Domain List    | <input type="checkbox"/> | 0     |               | 01-01-0001 00:00:00... |
| Malware Domains        | <input type="checkbox"/> | 0     |               | 01-01-0001 00:00:00... |
| Malware IP List        | <input type="checkbox"/> | 0     |               | 01-01-0001 00:00:00... |
| RSA FirstWatch APT ... | <input type="checkbox"/> | 0     |               | 01-01-0001 00:00:00... |
| RSA FirstWatch APT ... | <input type="checkbox"/> | 0     |               | 01-01-0001 00:00:00... |
| RSA FirstWatch Com...  | <input type="checkbox"/> | 0     |               | 01-01-0001 00:00:00... |
| RSA FirstWatch Com...  | <input type="checkbox"/> | 0     |               | 01-01-0001 00:00:00... |
| 14 items total         |                          |       |               |                        |

3. Enter your RSA Live account credentials.

**Note:** If you do not have an RSA Live account, click the link provided, which takes you to the RSA Live Registration Portal. Follow the specific directions for NetWitness Endpoint customers. Once you have an account, return to this dialog and enter your new credentials.

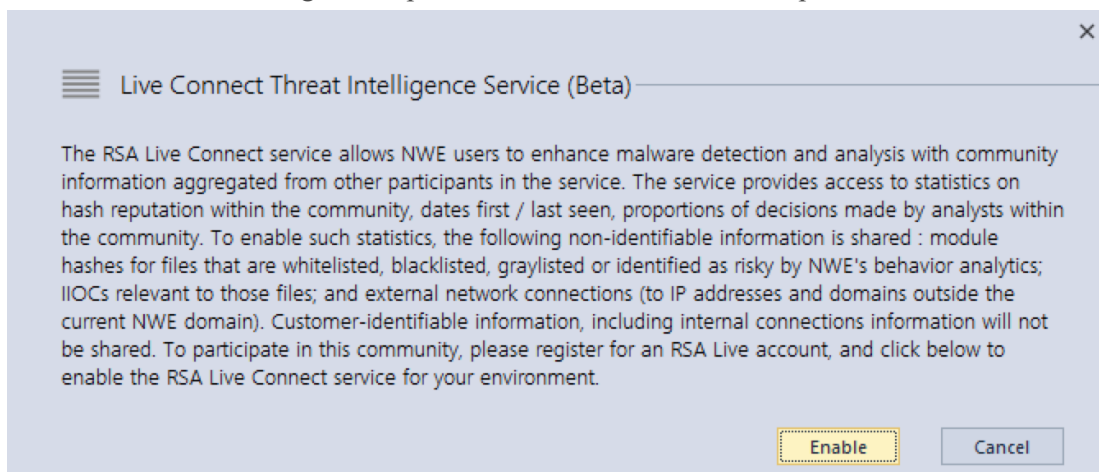
**Note:** If you are using NetWitness Endpoint version 4.4, but not NetWitness 10.x or 11.x, you must contact RSA Customer Support and open a customer support case to get an RSA Live account.

4. Enter the Server Hostname and Port values.

**Note:** The host value is generally **cms.netwitness.com**. The port is generally **443**.

5. To use the NetWitness Endpoint file reputation service to validate modules, set the **Reputation service** control to **ON**. This option is not available unless you have entered your RSA Live credentials. For more information, see [File Reputation Service](#).
6. To use the RSA Live Connect service, set the **Live Connect Threat Intelligence Service (Beta)** control to **ON**. This option is not available unless you have entered your RSA Live Credentials.

A popup window is displayed that explains the purpose of this service and how it is used to enhance the threat intelligence capabilities within NetWitness Endpoint, as shown below:



You must click **Enable** on the popup message to activate this service. If you click **Cancel** or the **X** in the upper right corner, the service is not activated, the message closes, and the control is returned to the **OFF** position.

To disable the Live Connect service, set the **Live Connect Threat Intelligence Service (Beta)** control to **OFF**.

For more information, see [RSA Live Connect](#).

7. To activate subscriptions, select the feeds that NetWitness Endpoint should import from RSA Live by selecting the corresponding checkboxes.
8. Enter an appropriate interval.

**Note:** The recommended interval is 24 hours. This means that NetWitness Endpoint will connect to RSA Live every 24 hours to update the imported data.

9. Click **Save**.  
The component is now added to NetWitness Endpoint and the subscriptions are activated.
10. To validate the connectivity, select the newly added component and click **Test Settings**.

**Note:** If all settings are correct, a **Passed** message is displayed.

11. Click **Apply**.

### Connect RSA Live through Proxy

After configuring RSA Live, it is important to check the following settings:

1. Make sure that the machine where the NetWitness Endpoint Primary ConsoleServer is installed is able to connect to <https://cms.netwitness.com>. This can be tested by typing the URL [https://cms.netwitness.com/alfresco/service/SDK\\_1\\_1/search?title=RSA](https://cms.netwitness.com/alfresco/service/SDK_1_1/search?title=RSA) in the IE Browser of the ConsoleServer machine and providing the live credentials.
2. The NetWitness Endpoint UI must be able to connect to the NetWitness Endpoint ConsoleServer machine (NOT <https://cms.netwitness.com>). This can be verified by typing **https://<hostname or IP>:9443/ecat/liveconfig** (hostname or IP, whichever was provided during installation of the NetWitness Endpoint ConsoleServer) in the IE Browser. If the connection is successful, you will be prompted to enter the credentials. If the connection fails due to proxy settings, do one of the following:
  - Add the IP addresses and hostnames of both the NetWitness Endpoint UI and ConsoleServer in the exception list of both the NetWitness Endpoint UI and ConsoleServer machines.
  - Bypass the proxy server by enabling Bypass proxy server for local addresses and connect using the hostname instead of the IP address or the Fully Qualified Domain Name (FQDN). For more information, see <http://support.microsoft.com/kb/262981>.

## Select Available Feeds from RSA Live

The RSA Live dialog lists all currently available feeds. This list may change as RSA Live adds or removes feeds as necessary. To select one or more feeds, click to select the checkbox in the Subscribe column for each desired feed. To select all feeds, click **Select All** above the list of available feeds.

**Note:** None of the feeds are enabled by default in NetWitness Endpoint. When a feed is enabled, the NetWitness Endpoint ConsoleServer connects to RSA Live (<https://cms.netwitness.com>) and periodically downloads feed data into the NetWitness Endpoint system.

## Deploy RSA Live Feeds Offline

If you are not connected to the internet, you can deploy the feeds offline by using the ConsoleServerSync.exe tool. For more information, see [NetWitness Endpoint ConsoleServerSync Tool](#).

## RSA NetWitness v9.7

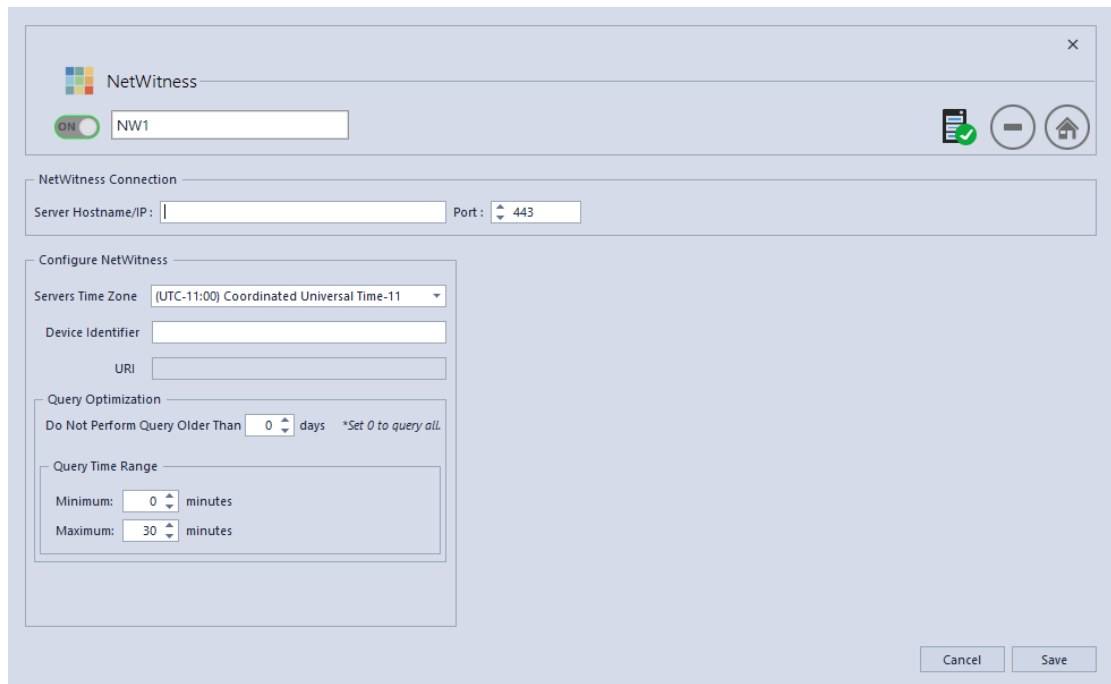
RSA NetWitness v9.7 (a previous version of RSA NetWitness Suite) is a network security monitoring platform that provides visibility and situational awareness about what's happening on the network. You can configure NetWitness Endpoint to connect directly to NetWitness v9.7 in order to provide additional information about network activities.

When investigating Network Connections in NetWitness Endpoint, you can right-click a particular connection and select **Investigate Destination IP with NetWitness** or **Investigate Source and Destination IP with NetWitness**. This request will automatically query the RSA NetWitness database and open directly into the NetWitness Investigator screen with the query results. From there, the analyst can drill down to gain more insight into that network connection.

To configure RSA NetWitness:

1. Go to **Configure > Monitoring and External Components**.  
The **Configure External Components** window is displayed.
2. From the Components listed, select **NetWitness** and click + to add a new NetWitness component.





3. Enter the fields relevant to NetWitness configuration:

- Instance Name
- Host DNS or IP
- Port
- Servers Time Zone
- Device Identifier
- URI

**Note:** Refer to the RSA NetWitness documentation for more information on these fields.

4. (Optional) To optimize the queries you should customize these parameters:

- Minimum Query Time Range: Automatically increases the time range submitted in the queries to circumvent the time difference between the NetWitness Endpoint database and the NetWitness database.
- Maximum Query Time Range: Automatically decreases the time range of the query to the given value to limit the scope of the submitted queries.

- **Do Not Perform Query Older Than:** This parameter prevents the execution of queries that are defined as too old.

5. Click **Save**.

The component is now added to NetWitness Endpoint.

## SMTP

NetWitness Endpoint will send SMTP (email) messages when a computer reaches a certain score, if the option is enabled. For more information, see *Configuring Email (SMTP) Alerts* in the topic [Configure Alerts](#).

## OPSWAT Scan Engine

OPSWAT Metascan (now called Metadefender Core) is an advanced multi-scanning software engine that may (optionally) be used with NetWitness Endpoint. It combines unique technologies and multiple anti-malware engines from market leaders (such as CA, ESET, AVG, and others) and improves the likelihood of catching malware on downloaded modules.

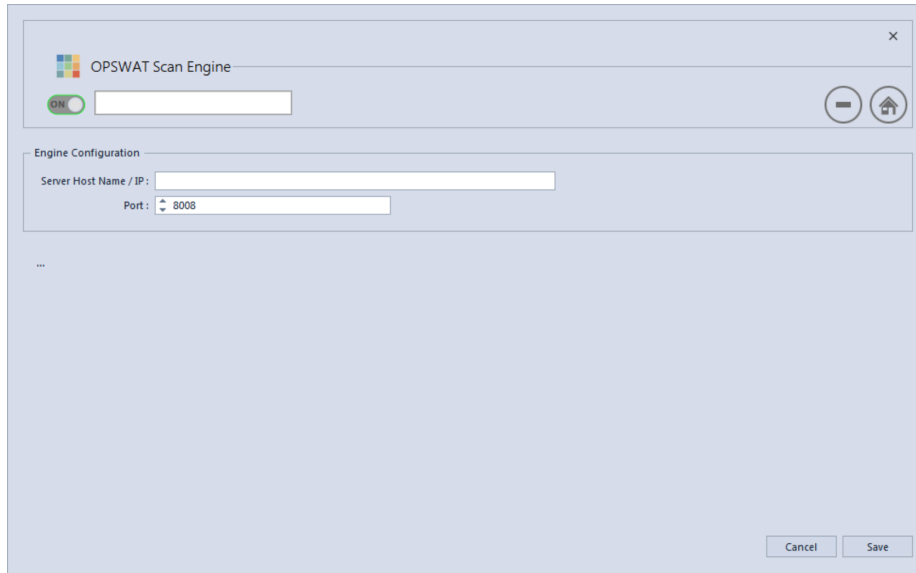
**Note:** Before configuring OPSWAT you must have previously installed the OPSWAT Metascan executable on the same machine as the NetWitness Endpoint ConsoleServer or on another server on the same LAN. For more information, see *Step 9: (Optional) Install Metascan* in the RSA NetWitness Endpoint 4.4 Installation Guide.

To configure OPSWAT Metascan in NetWitness Endpoint:

1. Go to **Configure > Monitoring and External Components**.

The **Configure External Components** window is displayed.

- From the Components listed, select **OPSWAT Scan Engine** and click + to add a new OPSWAT component. The OPSWAT Scan Engine dialog is displayed, as shown below:



- Set the control to **ON**. You can also optionally enter a name for the OPSWAT Scan Engine.
- Enter the **Server Host Name / IP** address for the server on which OPSWAT is installed. If it is installed on the same machine as the NetWitness Endpoint ConsoleServer, you can enter "(local)".
- A default value is entered automatically for the **Port Value**, but this may be changed.
- Click **Save**.

## YARA Scan Engine

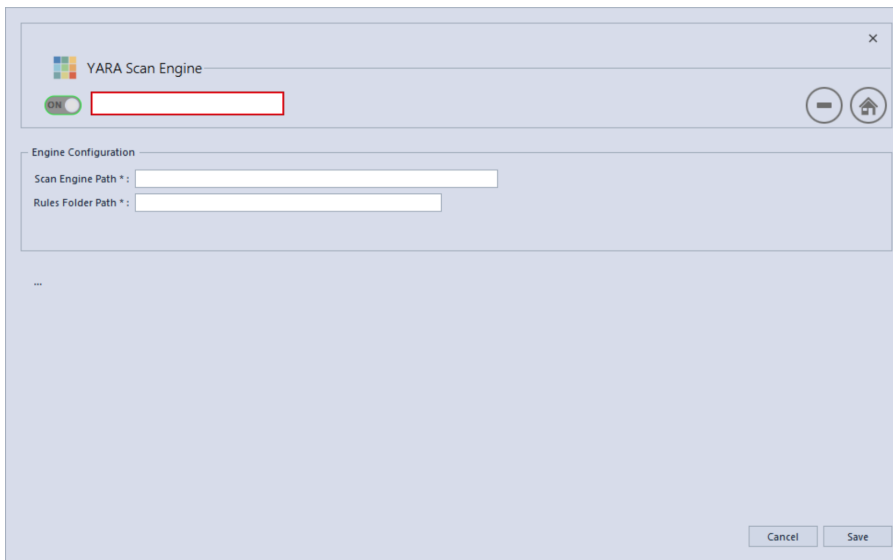
YARA is an open source static analysis tool that may (optionally) be used with NetWitness Endpoint. It uses a set of custom rules to help identify and classify known threats on downloaded modules.

**Note:** Before configuring YARA you must have previously installed the YARA executable on the same machine where the NetWitness Endpoint ConsoleServer is running.

To configure YARA in NetWitness Endpoint:

- Go to **Configure > Monitoring and External Components**.  
The **Configure External Components** window is displayed.

- From the Components listed, select **Yara Scan Engine** and click + to add a new YARA component. The YARA Scan Engine dialog is displayed, as shown below:



- Set the control to **ON**. You can also optionally enter a name for the YARA Scan Engine.
- Enter the **Scan Engine Path**. This should be the path to the YARA executable file. This path may be either absolute or relative to the location of the ConsoleServer.
- Enter the **Rules Folder Path**. This should be the path to the YARA folder containing the rules to be used. This path may be either absolute or relative to the location of the ConsoleServer.
- Click **Save**.

**Note:** There may be YARA rules that generate errors in NetWitness Endpoint, regardless of which version of YARA you are using. When this occurs, NetWitness Endpoint automatically disables YARA. To remedy this, you will need to remove the incompatible rules and re-enable YARA.

# REFERENCES

---

This section is a collection of reference information that pertains to using NetWitness Endpoint.

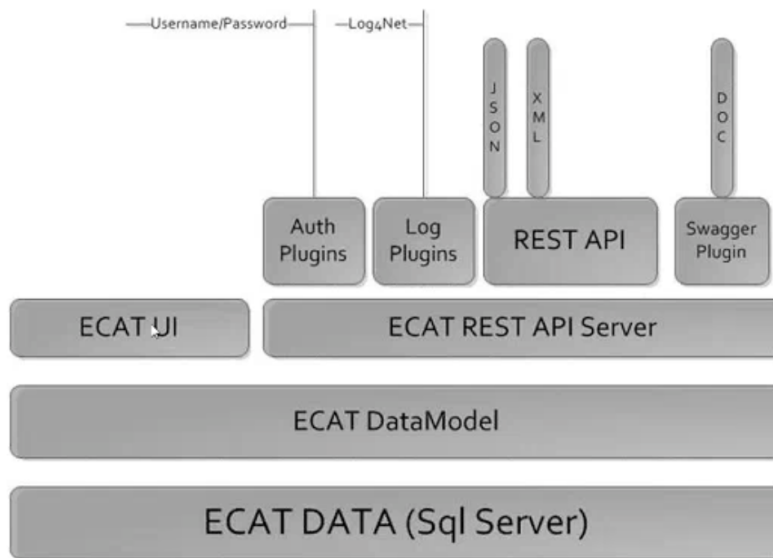
## Topics Covered:

- [REST API Server](#)
- [NetWitness Endpoint ConsoleServerSync Tool](#)
- [Live Feedback](#)
- [NetWitness Endpoint UI URL Commands](#)
- [List of Host and Service Ports](#)
- [Troubleshooting](#)

## REST API Server

This topic provides detailed information about configuring and using the REST API's for NetWitness Endpoint using the NetWitness Endpoint API Server.

The NetWitness Endpoint REST API Service exposes the REST APIs to third-party developers. The API Server is installed automatically during NetWitness Endpoint Primary ConsoleServer installation as a Windows Service called "RSA ECAT API Server". The following diagram provides a high-level architecture for the REST API Service in NetWitness Endpoint.

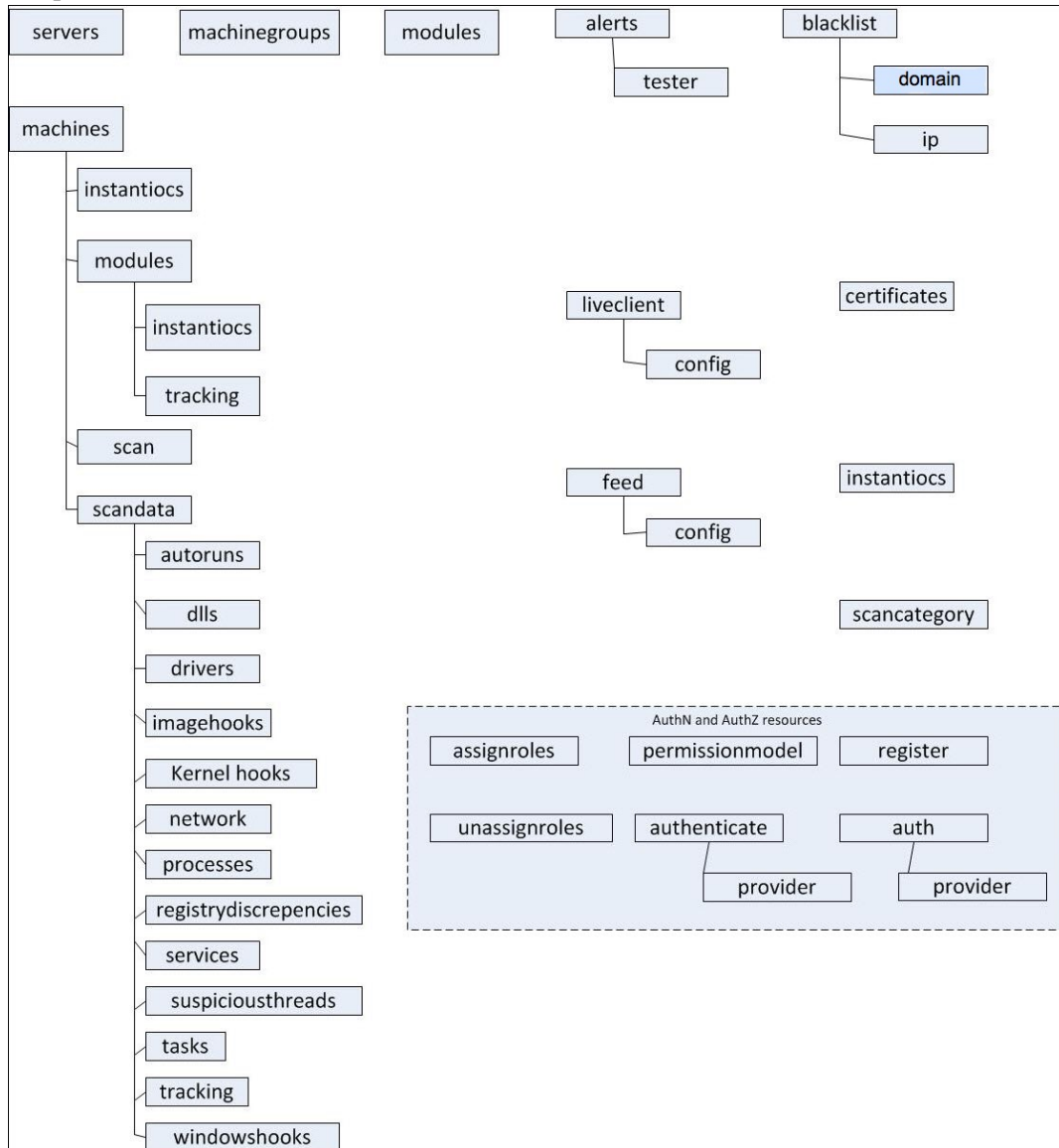


The following topics provide more detailed information about the NetWitness Endpoint REST API Server:

- [REST Resources Architecture](#)
- [Start/Stop the API Server](#)
- [Data Format and HTTP Verbs](#)
- [Authentication and Authorization](#)
- [API Self-Discovery Using HATEOAS](#)
- [Pagination](#)
- [Debugging and Logging](#)
- [Managing the API Server DB Connecting User](#)
- [Tuning the API Server](#)

## REST Resources Architecture

The following diagram shows the REST resources supported for the API. You will notice that the architecture strongly reflects the flow of information as it is rendered in the NetWitness Endpoint UI.



## Start/Stop the API Server

You must use the Windows Service Control Manager to start and stop the NetWitness Endpoint API Server service. Once the service is started, you can access the Swagger-based interactive API Documentation for more information on the REST APIs.

The link to the API documentation is as follows:

`https://<servername>:9443/api/v2/swagger-ui/`

**Note:** The NetWitness Endpoint UI uses the NetWitness Endpoint API Server, so the service should be kept running at all times. As a best practice you should set the API Server to restart automatically after a failure using the server properties dialog.

## Data Format and HTTP Verbs

### Root Endpoint

All APIs can be accessed using HTTPS as follows: *https://<servername>:<port>/api/v2*.

### Data Format

The API service supports both JSON and XML data formats. However, the support for XML is limited.

You can use one of the following two ways to define the headers and format in URL:

1. **HTTP-Headers:** Use either of the following in the request headers:
  - Accept: application/xml
  - Accept: application/json
2. **Format:** Use either of the following query parameter in every HTTP request:
  - ?format=json
  - ?format=xml

**Note:** RSA recommends that you use JSON format as there is limited support for XML.

### HTTP Verbs

The API server uses the appropriate HTTP verbs for each action. The table below provides the description of HTTP verbs:

| Verb   | Description                                                                                     |
|--------|-------------------------------------------------------------------------------------------------|
| GET    | Used to retrieve resources.                                                                     |
| POST   | Submits data to be processed by the identified resource.                                        |
| PUT    | Create or update a resource.                                                                    |
| DELETE | Delete a resource.                                                                              |
| HEAD   | Can be issued against any resource to get just the HTTP header info. (Currently not supported). |



| Verb    | Description                                                                          |
|---------|--------------------------------------------------------------------------------------|
| PATCH   | Used for updating resources with partial data. (Currently not supported).            |
| OPTIONS | Returns the methods supported by the identified resource. (Currently not supported). |

## Authentication and Authorization

### Authentication

To authenticate to the API Server, you must use a valid username and password. The following usernames are supported:

- SQL-SA usernames created using the NetWitness Endpoint UI.
- Custom usernames created using the `/register` APIs.

### Authentication Type

The API Server supports two types of authentication, namely:

- HTTP-Basic authentication
- Forms-based authentication

RSA recommends that new clients use the Forms-based authentication. Support for HTTP-Basic authentication exists only for backward compatibility, as SA-Feeds (as a client) connect using Basic Authentication.

### HTTP-Basic Authentication

To login using a browser, enter the username and password in the pop-up dialog box. For any programmatic usage, ensure that you use the appropriate method that supports Basic Authentication.

### Forms-based Authentication

To authenticate using the Forms-based authentication, use the `POST /auth/credentials` API. For example:

```
POST auth/credentials
{
 "UserName": "guest",
 "Password": "guest",
 "RememberMe": true
}
```

The response to this request is something similar to below:

Headers:

```
Transfer-Encoding: chunked
Content-Type: application/json; charset=utf-8
Vary: Accept
Server: Microsoft-HTTPAPI/2.0
Set-Cookie: ss-id=IwlyVei3QJveXR2acNdn;path=/
Set-Cookie: ss-
pid=4sp04LxaTeb8iJUWH9Ex;path=/;expires=Tue,
17 Apr 2035 09:00:12 GMT
Set-Cookie: ss-
opt=perm;path=/;expires=Tue, 17 Apr 2035 09:00:12 GMT
Set-Cookie: X-
UAId=1007;path=/;expires=Tue, 17 Apr 2035 09:00:12 GMT
X-Powered-By: ServiceStack/4.038 Win32NT/.NET
Date: Fri, 17 Apr 2015 09:00:12 GMT
```

Body:

```
{
 UserId: "1007"
 SessionId: "4sp04LxaTeb8iJUWH9Ex"
 UserName: "guest"
 ResponseStatus: {}
}
```

All API calls that require authentication must send the cookies as a part of the request headers, such as:

```
Cookie: ss-id=IwlyVei3QJveXR2acNdn; ss-
pid=4sp04LxaTeb8iJUWH9Ex; ss-opt=perm; X-UAId=1007
```

If you are using any compliant HTTP REST client (like a browser, or any C# or JAVA programmable client), cookies are automatically included.

## Create Custom Usernames Using /register API

For better security, RSA recommends using the SQL-SA usernames created using the NetWitness Endpoint UI for the REST clients. In situations where this is not possible, you can create your own users that can be managed by the API Server. Note that this feature is disabled by default. To enable this feature, you must configure the following settings in the **ApiServer.exe** file located in the folder **C:\ECAT\Server**.

For example, in **C:\ECAT\ApiServer.exe**, set the "RegistrationFeature" value to TRUE as follows:

```
<appSettings>
 <add key="RegistrationFeature" value="true"></add>
</appSettings>
```

On restarting the API-Server, /register APIs will be available.

The user (either SQL-SA or Windows Authentication user) connecting to the API Server database (referred to as the API Server DB connecting user) **MUST** have at a minimum the "ECAT\_ROLE\_Readonly" permission for this functionality. This can be configured in the NetWitness Endpoint UI using the option **Configure > Manage Users and Roles**. The maximum privileges of the custom users that you create is limited to the maximum privilege of the API Server DB connecting user. For more information about the Admin user and other permissions, see [Managing the API Server DB Connecting User](#).

**Note:** The API Server DB connecting user is the value of <DbSaUser> for SQL-SA authentication and Windows users for Integrated Authentication.

## API Server Admin User

The API Server admin user assigns NetWitness Endpoint Role-Based Access Control (RBAC) permissions to the new users. The admin user is created by default at the time of installation.

- Username: admin
- Password: This has to be set using the following command:

```
ApiServer.exe /setadminpswd A_Strong_Password
```

After setting the password, restart the server.

The admin user can now make REST calls and has all the privileges of the API Server DB connecting user in terms of NetWitness Endpoint RBAC permissions. The main purpose of this user is to create custom REST clients when the user is unable to create SQL-SA users for REST clients.

To create a new user:

1. Log off from the REST client and register a new user by using the following command:

```
POST https://localhost:9443/register
```

2. Log on as the admin user and assign a role to the newly created user using the following steps:
  - a. Log on as admin:  
POST <https://localhost:9443/auth/credentials>
  - b. Assign roles:  
POST <https://localhost:9443/assignroles/>
  - c. Unassign roles:  
POST <https://localhost:9443/unassignroles/>
  - d. Log off as admin:  
POST <https://localhost:9443/auth/logout>

For details about the data to be passed in the request, see the Swagger documentation that can be accessed from <https://<servername>:9443/api/v2/swagger-ui/>.

For details about different roles and permissions, see the *Authorization* section below.

## Authorization

APIs that access privileged NetWitness Endpoint resources require authorization. The API server uses the NetWitness Endpoint RBAC authorization concept for naming its roles and permissions.

To get information about the APIs that require authorization and the type of roles/permissions, use the following:

```
GET /permissionmodel/
```

The ECAT Admin user is responsible for assigning the roles/permissions appropriately. Clients without appropriate permissions will receive a 403 error code.

For SQL-SA users, the roles/permissions are managed through the NetWitness Endpoint UI. For custom usernames, roles/permissions are managed by the `/register` API.

## API Self-Discovery Using HATEOAS

To enable auto-discovery of the next logical resource, some APIs use the popular HATEOAS mechanism. The resource that supports this mechanism has a Links list where each element of the list contains two items:

- `rel`: indicates the relationship
- `href`: indicates the URI of the related next logical resource

For example, the `machines/{GUID}/scandata` resource contains many sub-resources. To ease the application development for such huge objects, the HATEOAS linking approach is available.

A `GET` request on `machines/5163a596-6a4d-5a7c-2be8-0f73fd9a1fff/scandata` provides the following output, indicating how to find the next logical nodes:

```
{
 "Guid": "5163a596-6a4d-5a7c-2be8-0f73fd9a1fff",
 "MachineName": "244APP43",
 "Links": [
 {
 "rel": "Services",
 "href": "https://244app43:9443/api/v2/machine...ndata/services"
 },
 {
 "rel": "Processes",
 "href": "https://244app43:9443/api/v2/machine...data/processes"
 },
 {
 "rel": "DLLs",
 "href": "https://244app43:9443/api/v2/machine...scandata/dlls"
 },
 {
 "rel": "Drivers",
 "href": "https://244app43:9443/api/v2/machine...andata/drivers"
 },
 {
 "rel": "Autoruns",
 "href": "https://244app43:9443/api/v2/machine...ndata/autoruns"
 },
 {
 "rel": "Tasks",
 "href": "https://244app43:9443/api/v2/machine...scandata/tasks"
 },
 {
 "rel": "Image Hooks",
 "href": "https://244app43:9443/api/v2/machine...ata/imagehooks"
 },
 {
 "rel": "Kernel Hooks",
 "href": "https://244app43:9443/api/v2/machine...ta/kernelhooks"
 },
 {
 "rel": "Windows Hooks",
 "href": "https://244app43:9443/api/v2/machine...a/windowshooks"
 },
 {
 "rel": "Suspicious Threads",
 "href": "https://244app43:9443/api/v2/machine...piciousthreads"
 },
 {
 "rel": "Registry Descrepancies",
 "href": "https://244app43:9443/api/v2/machine...ydiscrepancies"
 }
]
}
```

```
 },
 {
 "rel": "Network Traffic",
 "href": "https://244app43:9443/api/v2/machine...andata/network"
 }
]
}
```

## Pagination

The results of certain APIs are in the form of List objects. For example, GET /machines/ would return the list of all machines. To prevent huge data transfer, Pagination is supported for all APIs that return a list.

By default, only 50 items will be returned per page.

You can control the number of pages by using the following two query string parameters:

- page=nn
- per\_page=nn

For example, the following query will return 20 items per page:

[https://244app43:9443/api/v2/machine...=1&per\\_page=20](https://244app43:9443/api/v2/machine...=1&per_page=20)

The links of the other pages and the total number of pages will be supplied through HTTP headers as per RFC: <http://tools.ietf.org/html/rfc5988#page-6>.

For example, the machines object containing 1000 elements will have the link headers as shown below for the 5th page:

Link:

```
https://244app43:9443/api/v2/machine...=5&per_page=20; rel=self",
<https://244app43:9443/api/v2/machine...=6&per_page=20>; rel="next",
<https://244app43:9443/api/v2/machine...50&per_page=20>; rel="last",
<https://244app43:9443/api/v2/machine...=1&per_page=20>; rel="first",
<https://244app43:9443/api/v2/machine...=4&per_page=20>; rel="prev"
```

In addition, the "X-Total-Count" HTTP header contains the total number of items. For example: X-Total-Count: 1000.

## Debugging and Logging

The REST API server uses the friendly Log4Net for creating logs and the level of logging can be controlled using the `ApiServer.exe.config` file.

You can access the **C:\ECAT\API\ApiServer.exe.config** file and edit the logging parameters as required. For better performance, make sure to bring down the logging during deployment of your application. After making changes, you must restart the RSA ECAT API Server service for the changes to take effect.

```
<log4net>
 <root>
 <level value="INFO"></level>
 <appender-ref ref="RollingFileAppender"></appender-ref>
 </root>
 <appender name="RollingFileAppender"
type="log4net.Appender.RollingFileAppender">
 <file value="apiserver.log"></file>
 <appendToFile value="true"></appendToFile>
 <rollingStyle value="Size"></rollingStyle>
 <maxSizeRollBackups value="5"></maxSizeRollBackups>
 <maximumFileSize value="10MB"></maximumFileSize>
 <staticLogFileName value="true"></staticLogFileName>
 <layout type="log4net.Layout.PatternLayout">
 <conversionPattern value="%date [%thread] %level -
%message%newline"></conversionPattern>
 </layout>
 <filter type="log4net.Filter.LevelRangeFilter">
 <levelMin value="DEBUG"></levelMin>
 <levelMax value="FATAL"></levelMax>
 </filter>
 </appender>
</log4net>
```

## Managing the API Server DB Connecting User

This topic provides information about managing the admin user to access the NetWitness Endpoint Microsoft SQL database and perform other actions.

The API Server must have access to the NetWitness Endpoint SQL database. Therefore, the admin user for the REST API server **MUST** have access to the ECAT\$PRIMARY database. This admin user is referred to as the API Server DB Connecting User. For security reasons, RSA recommends following the principal of least privileges.

This admin user can either be a Windows user or a SQL-SA user. This choice is made during the installation of this feature and can be modified later:

- **Windows User**

For a Windows user, this will be the "RunAs" user of the Windows Service. This credential can also be used to access the NetWitness Endpoint database.

- **SQL-SA user**

Similar to the NetWitness Endpoint ConsoleServer, the API Server can also be configured to

use a SQL-SA credential to access the database. The username is in the **ApiServer.exe.config** file as shown below:

```
<add key="DbSaUser" value="alice"/>
```

The password of the "DbSaUser" user is stored in the NetWitness Endpoint lockbox. It can be modified post installation by using the following command:

```
C:\ECAT\API>ApiServer.exe -setdbpswd PassSecret
```

This admin user must have all the permissions that your REST client will ever be assigned. The REST clients will have a subset of the privileges that are assigned to this user based on the roles/permissions that are assigned from the /register API.

The API Server DB connecting user (either SQL-SA or Windows Authentication user) **MUST** have at the minimum "ECAT\_ROLE\_Readonly" permissions for this functionality. This can be assigned using the option **Configure > Manager Users and Groups** in the NetWitness Endpoint UI. Some API's require additional permissions and these permissions can be viewed by performing the following REST call:

```
GET /permissionmodel
```

For example, from your browser, open the page <https://<apiserver>:9443/api/v2/permissionmodel>.

## Tuning the API Server

You can tune the REST API Server by editing the **ApiServer.exe.config** file. All parameters are under the <appSettings> section. After making changes, you must restart the RSA ECAT API Server service for the changes to take effect.

The following table provides the description of the configuration options available via the **ApiServer.exe.config** file:

Name and Default Value	Description
<add key="RegistrationFeature" value="true"/>	User Registration Feature. If disabled, the /register API will not be available and users will not be able to register new accounts. These accounts are maintained at the ServiceStack layer and not the database. If this option is disabled, the users will be able to login using the SQL-SA account.
<add key="SupportForSQLSAUsers" value="true"/>	To enable/disable SQL-SA users. If disabled, users will not be able to authenticate using SQL-SA accounts.



Name and Default Value	Description
<pre>&lt;add key="CacheRefreshIntervalInSecs" value="60"/&gt;</pre>	<p>The refresh interval of the global cache in seconds. The global cache contains some of the most commonly used objects. These objects will be refreshed from the database every 60 seconds by default.</p>
<pre>&lt;add key="ProviderTimeout" value="120000"/&gt;</pre>	<p>This is the timeout for querying an object from the database in milliseconds</p>

## NetWitness Endpoint ConsoleServerSync Tool

NetWitness Endpoint administrators can use the ConsoleServerSync tool to update time-sensitive information when automatic updates are not possible, such as when a NetWitness Endpoint ConsoleServer is used in an isolated environment and is not connected to the Internet. The external information being updated changes constantly so it is important to keep the NetWitness Endpoint database as up-to-date as possible. The ConsoleServerSync tool facilitates collecting and organizing the necessary information from the Internet into one or more files that can then be uploaded to the NetWitness Endpoint database, thereby synchronizing the data. This helps to ensure that the NetWitness Endpoint system stays up-to-date. The types of information that can be updated through the ConsoleServerSync tool include:

- **Trusted certificate roots and Certificate Revocation Lists (CRLs).** Certificates are found in modules and machines. NetWitness Endpoint verifies for certificate revocation daily. If NetWitness Endpoint is not able to verify certificates for a certain period of time, the status of affected certificates changes to Need Revoke Update. When this happens you must use the ConsoleServerSync tool to manually synchronize the certificates. For more information on certificates, see [Certificates Window](#).
- **RSA Live feeds.** RSA Live is a threat intelligence delivery system that contains suspicious domains and IP addresses, among other types of information, which is beneficial for several NetWitness Endpoint IIOCs. For more information on RSA Live feeds, see [RSA Live](#).
- **Kernel data.** When NetWitness Endpoint identifies unsupported kernels, the NetWitness Endpoint team updates the supported kernels database as well as the livecat.rsa.com server, which then feeds updated kernel information back to the NetWitness Endpoint server. Agents are then updated automatically during the next connection. When the NetWitness Endpoint Console Server cannot connect to the internet, these automatic updates do not occur and

therefore must be done manually. For more information on kernel data, see [Kernel Adaptation System](#).

- **Reputation data for modules.** The NetWitness Endpoint Reputation Service automatically sends hash information to RSA Live for all files discovered by agents to verify whether if any file is known malware or a legitimate file. When the NetWitness Endpoint Console Server cannot connect to the internet, this automatic file verification does not occur and therefore must be done manually. For more information see [File Reputation Service](#).

To use the ConsoleServerSync tool, you must be able to run the executable file from a machine with access to the Internet. Also, to retrieve information from RSA Live, you must have an RSA Live account, as described in the topic [RSA Live](#).

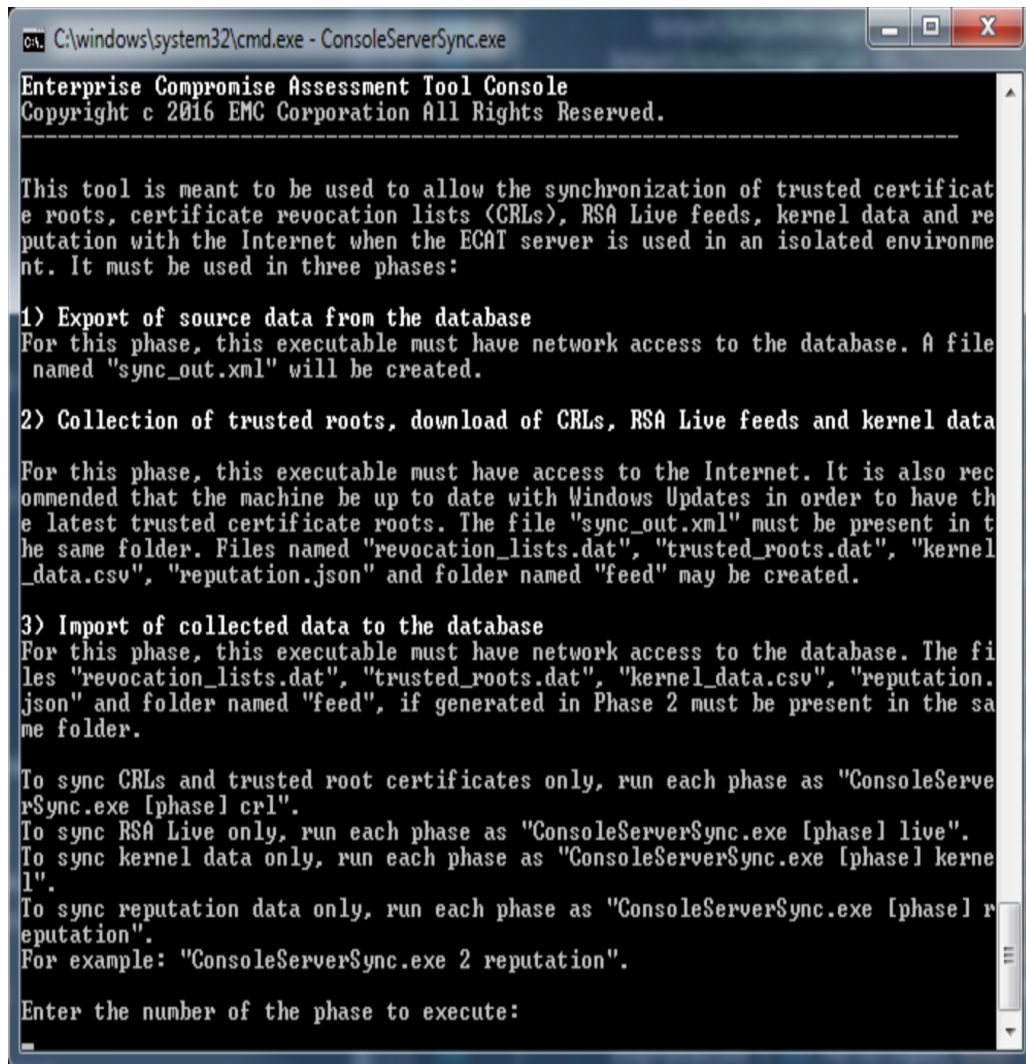
There are three phases to using the ConsoleServerSync tool:

- Phase 1: Export source data from the NetWitness Endpoint database
- Phase 2: Collect trusted roots, CRLs, RSA Live feeds, and kernel and reputation data
- Phase 3: Import collected data to the NetWitness Endpoint database

## Phase 1

To perform Phase 1 for the ConsoleServerSync tool, do the following:

1. Locate the **ConsoleServerSync.exe** file, which was automatically installed with the NetWitness Endpoint server. The default location is: C:\ECAT\Server.
2. Run the **ConsoleServerSync.exe** file from the command prompt.  
Information about how to use the ConsoleServerSync tool is displayed, similar to what is shown below:



```
C:\windows\system32\cmd.exe - ConsoleServerSync.exe
Enterprise Compromise Assessment Tool Console
Copyright c 2016 EMC Corporation All Rights Reserved.

This tool is meant to be used to allow the synchronization of trusted certificate
roots, certificate revocation lists (CRLs), RSA Live feeds, kernel data and re
putation with the Internet when the ECAT server is used in an isolated environme
nt. It must be used in three phases:

1) Export of source data from the database
For this phase, this executable must have network access to the database. A file
named "sync_out.xml" will be created.

2) Collection of trusted roots, download of CRLs, RSA Live feeds and kernel data
For this phase, this executable must have access to the Internet. It is also rec
ommended that the machine be up to date with Windows Updates in order to have th
e latest trusted certificate roots. The file "sync_out.xml" must be present in th
e same folder. Files named "revocation_lists.dat", "trusted_roots.dat", "kernel
_data.csv", "reputation.json" and folder named "feed" may be created.

3) Import of collected data to the database
For this phase, this executable must have network access to the database. The fi
les "revocation_lists.dat", "trusted_roots.dat", "kernel_data.csv", "reputation.
json" and folder named "feed", if generated in Phase 2 must be present in the sa
me folder.

To sync CRLs and trusted root certificates only, run each phase as "ConsoleServe
rSync.exe [phase] crl".
To sync RSA Live only, run each phase as "ConsoleServerSync.exe [phase] live".
To sync kernel data only, run each phase as "ConsoleServerSync.exe [phase] kerne
l".
To sync reputation data only, run each phase as "ConsoleServerSync.exe [phase] r
eputation".
For example: "ConsoleServerSync.exe 2 reputation".

Enter the number of the phase to execute:
```

3. In the tool window, at the **Enter the number of the phase to execute:** prompt, type:

1

This will extract source data to sync all four types of data at once.

4. Press ENTER.

You will be prompted for the password to connect to the NetWitness Endpoint database server. If this is your first time using the tool or the tool is unable to find the database, you will be prompted for the NetWitness Endpoint database server name and the NetWitness Endpoint database server user name in addition to the password. These database connection parameters are stored in the **ConsoleServerSync.exe.config** file and are automatically reused each time the ConsoleServerSync tool is launched. If you enter incorrect information or need to change the stored parameters for any reason, you can do one of the following:

- Edit the **ConsoleServerSync.exe.config** file to update the information and then relaunch the ConsoleServerSync tool. For more information see the Update Connection Parameters section below.
  - Delete the **ConsoleServerSync.exe.config** file and then relaunch the ConsoleServerSync tool. A new config file is generated automatically and you will be prompted to enter all of the NetWitness Endpoint database server connection parameters again.
5. Once Phase 1 is successfully executed, a file named **sync\_out.xml** is created in the same location as the **ConsoleServerSync.exe** file. This file contains the source data for all four types of data.

## Phase 2

To perform Phase 2 for the ConsoleServerSync tool, do the following:

1. Copy the **ConsoleServerSync.exe** and **sync\_out.xml** files to the same folder on a machine that has access to the Internet. This machine should be up-to-date with Windows Updates to have the latest trusted certificate roots.
2. Run the **ConsoleServerSync.exe** file from the command prompt.
3. In the tool window, at the **Enter the number of the phase to execute:** prompt, type:  
2
4. Press ENTER.  
Prompts for connecting to RSA Live will display.
5. Enter your RSA Live connection information. The server name and port are provided, but you must enter your username and password. If you do not have a username or password for RSA Live, you need to create an RSA Live account. For more information see [RSA Live](#).
6. Press ENTER after typing your RSA Live password.  
Additional files are created in the same location as the executable and may include: **revocation\_lists.dat**, **trusted\_roots.dat**, **kerneldata.csv**, and **reputation.json**. A folder named **feed** may also be created.

## Phase 3

To perform Phase 3 for the ConsoleServerSync tool, do the following:

1. Copy the **ConsoleServerSync.exe** file to a machine that has network access to the NetWitness Endpoint database. All other files (including the **feed** folder) created during Phase 2 must also be copied to the same location.

2. Run the **ConsoleServerSync.exe** file from the command prompt.
3. In the tool window, at the **Enter the number of the phase to execute:** prompt, type:  
3
4. Press ENTER.  
You will be prompted for the password to connect to the NetWitness Endpoint database server. For more details see step 4 for Phase 1 above.
5. Once Phase 3 is successfully executed, all information collected during Phase 2 is uploaded and synchronized to the NetWitness Endpoint database.

### Alternate Command Line Procedure

While most users should use the above procedure, in some cases a user may wish to specify which type of data to sync, rather than automatically syncing all four data types. This is accomplished by specifying the desired data to sync at the time you run the **ConsoleServerSync.exe** file from the command prompt, rather than using the prompt provided in the tool window (shown above).

To use the **ConsoleServerSync.exe** tool from the command prompt, do the following:

1. At the command prompt, run the **ConsoleServerSync.exe** file (as specified in step 2 of Phase 1) but also append one of the following commands, according to which types of information you want to update:
  - To sync only trusted root certificates and CRLs, append:  
1 crl
  - To sync only RSA Live feeds, append:  
1 live
  - To sync only kernel data, append:  
1 kernel
  - To sync only reputation data, append:  
1 reputation
  - To sync a specific combination of types of data at once, enter a "1" followed by each data type name. For example, to sync certificates and kernel data, type:  
1 crl kernel

For example, to sync only reputation data, at the command prompt you would run the following:

```
ConsoleServerSync.exe 1 reputation
```

2. All specified data information is collected in the same **sync\_out.xml** file.
3. Follow the directions above for Phase 2. You also have the option to run Phase 2 from the command line and specify the data type. For example, if you run `ConsoleServerSync.exe 2 reputation`, the tool will download only reputation data. However, if you do not specify the data type, the tool will always download kernel data regardless of what was specified in Phase 1. For example, if you run `ConsoleServerSync.exe 1 reputation`, then run `ConsoleServerSync.exe 2`, you will get both reputation data and kernel data. Depending on what types of data are being updated (as indicated in the **sync\_out.xml** file), additional files are created in the same location.
4. Follow the directions above for Phase 3.

## Updating Connection Parameters

The `ConsoleServerSync` tool must be able to connect to the NetWitness Endpoint database server and thus it requires the correct connection parameters: NetWitness Endpoint database server name, user name, and password. These parameters (except for the server password) are stored in the **ConsoleServerSync.exe.config** file (in the same location as the executable file) and are automatically reused whenever the `ConsoleServerSync` tool is launched (but users are always prompted to enter the database server password). If you need to update the NetWitness Endpoint database connection parameters, one option is to edit the **ConsoleServerSync.exe.config** file. To do so you will need to update the values for "ServerName" and "UserName" as highlighted in the following sample config file:

```
<?xml version="1.0"?>
<configuration>
 <appSettings>
 <clear />
 <add key="ServerName" value="Fire2012R2U1" />
 <add key="InstanceName" value="" />
 <add key="DatabaseName" value="ECAT$PRIMARY" />
 <add key="SQLSecurity" value="y" />
 <add key="UserName" value="ecatadmin" />
 </appSettings>
 <system.net>
 <defaultProxy>
 <proxy usesystemdefault="True"/>
 </defaultProxy>
 </system.net>
</configuration>
```

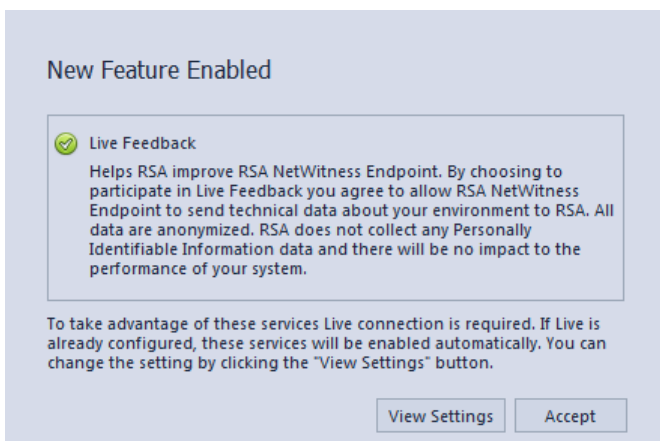
The other option is to just delete the **ConsoleServerSync.exe.config** file. The next time the `ConsoleServerSync` tool is launched, you will be prompted to enter all the NetWitness Endpoint database server connection parameters, which are then stored in a new **ConsoleServerSync.exe.config** file.

## Live Feedback

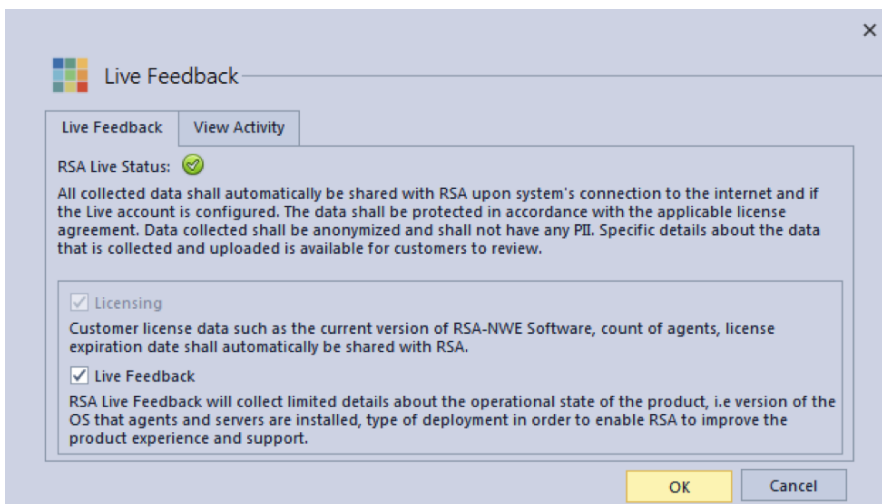
The Live Feedback feature collects NetWitness Endpoint license and relevant information to help improve product experience and support. All data collected is for RSA’s use only and shall be protected in accordance with the applicable license agreement. Furthermore, all collected data will not contain any Personally Identifiable Information.

### Live Feedback Acceptance

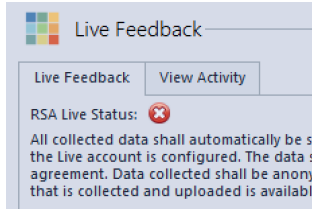
Following an update or new installation to NetWitness Endpoint 4.3 or later, the first time a user with L2 or Admin privileges logs in, that user will be prompted to accept participation in Live Feedback, as shown below:



You can view more information about the feature by clicking **View Settings**, which displays the Live Feedback dialog shown below:



The green checkmark next to RSA Live Status indicates that a Live account is already configured. If a Live account has not been configured, a red X displays instead, as shown below:



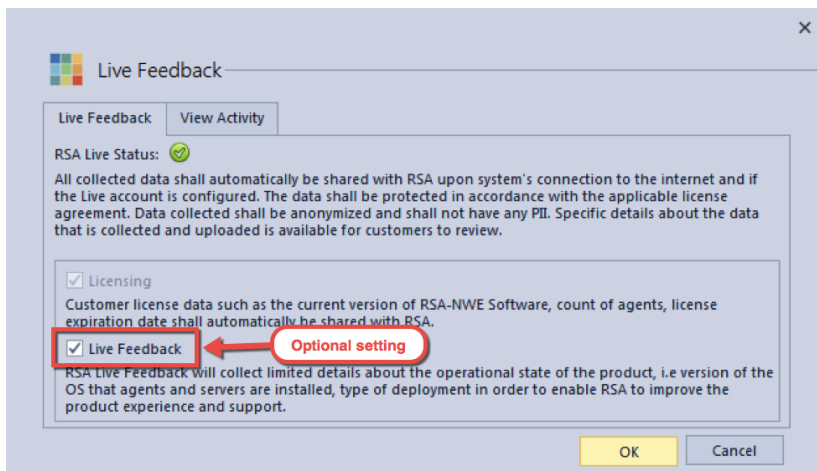
If this is the case, you will need to configure a Live account through the RSA Live feature (Configure > Monitoring and External Components > RSA Live). For more information, see [RSA Live](#). (Note: Live Feedback will still be collected but it will not be uploaded until you have configured your Live account.)

Clicking **OK** or **Cancel** on the Live Feedback dialog will return you to the New Feature Enabled dialog, where you must click **Accept** before continuing to use NetWitness Endpoint.

Licensing information will automatically be shared with RSA upon clicking **Accept** on the New Feature Enabled dialog, the system's connection to the internet, and the Live account configured.

**Note:** You cannot disable the option to share licensing information and you must click **Accept** on the New Feature Enabled dialog, even if you do not currently have a Live account.

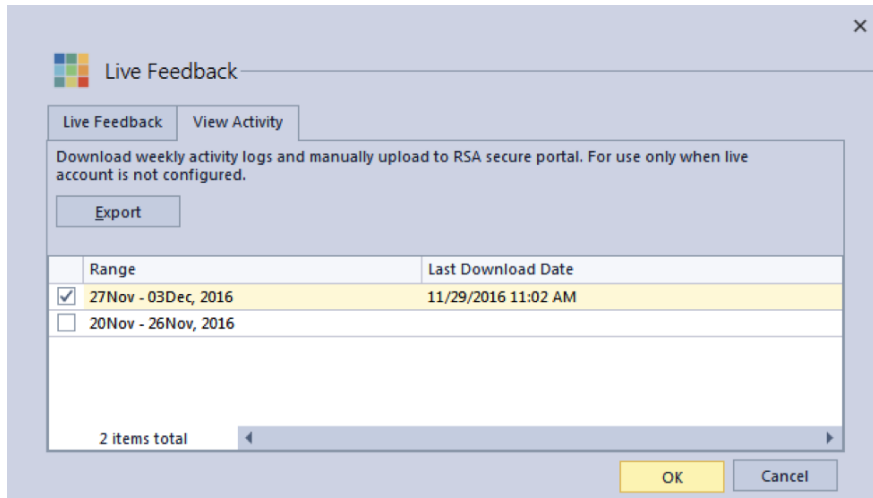
In addition to licensing information, Live Feedback will also collect limited details about the operational state of the product, for example, the OS version for installed agents and the deployment mode and type. Specific details about the data that is collected and uploaded is available for customers to review and is explained in the section, JSON File Structure (see below). This an optional capability and is enabled by default. However, customers who wish not to share data may disable Live Feedback by unchecking the option on the Live Feedback dialog. You can change this setting at will by revisiting the Live Feedback dialog (Configure > Live Feedback), as shown below:





## Viewing Activity

You can view the information collected for a particular week by opening the View Activity tab on the Live Feedback dialog (Configure > Live Feedback), as shown below. You can then select the desired date range from the list displayed and click **Export** to save it to your local disk. The data is in JSON format, and an encrypted file is automatically uploaded to the RSA servers weekly (if you have configured a Live account).



Optionally, if needed, you can manually download Live Feedback data and share it with RSA by uploading it to <https://cms.netwitness.com/telemetry> using your Live credentials.

## JSON File Structure

As previously indicated, all Live Feedback data collected is stored in JSON format. The contents of each JSON file is divided into two sections:

- **Content:** This section contains the details of the deployed instance of NetWitness Endpoint.
- **Checksum:** This section displays the checksum for the Content section in the file. It is used by RSA for an integrity check. For example, "Checksum:  
7D5EB5D5752663BAA5E032F6D4BF8CB0B1E5D23D53CEA605C72F272560028E94"

The Content section of the JSON file contains the following specific details:

- **Version:** The JSON schema version.
- **ProductName:** The name of the product (RSA NetWitness Endpoint)
- **ProductType:** This is the same as the name of the product. It is kept for compatibility purposes.
- **ProductVersion:** The version of the product (for example, 4.4.0.0)

- **ProductInstance:** The GUID of the master (Primary) ConsoleServer. This marks the instance of the product.
- **ActivationKey:** The key used to generate the license for the customer.
- **Components:** The details for all the components in NetWitness Endpoint. These include the master ConsoleServer and the NetWitness Endpoint database, as well as other components depending on your particular configuration. The details for each component are included as follows:
  - *Id:* The unique ID of the component.
  - *Name:* The name of the component (for example, ConsoleServer).
  - *Version:* The version of the component (for example, 4.4.0.0)
  - *Properties:* A list of name-value pairs where "name" is the property name and "value" is the value of that property. For example:

```
{
 "Name": "IsMasterConsoleServer",
 "Value": "1"
}
```
  - A sample Components section from a JSON file is shown below:

```
"Components":
[
 {
 "Id": "4",
 "Name": "Console Server",
 "Version": "4.3.0.0",
 "Properties":
 [
 {
 "Name": "ActiveCloudRelayServerCount ",
 "Value": "1"
 },
 {
 "Name": "IsMasterConsoleServer",
 "Value": "1"
 },
 {
 "Name": "ConsoleServerCount ",
 "Value": "2"
 },
 {
 "Name": "Mode ",|
 "Value": "Fair Distribution"
 }
]
 }
],
```

- **Metrics:** Displays a list of metrics with the usage data for components, as follows:
  - *ComponentId:* The component ID for which metric values are collected. This is the same as the "Id" in the Components section.

- *StartTimeUTC*: The time when the metrics were collected, in EPOCH format.
- *EndTimeUTC*: The time when the metrics collection was completed, in EPOCH format.
- *Stats*: The usage value and usage type statistics for the component.
- A sample Metric section from a JSON file is shown below:

```
{
 "ComponentId": "5",
 "StartTimeUTC": "1479859260000",
 "EndTimeUTC": "1479945540000",
 "Stats":
 [
 {
 "Name": "AgentCount",
 "Value": "2"
 },
 {
 "Name": "AgentCount_For_OS:Microsoft Windows Server 2012 Standard",
 "Value": "2"
 },
 {
 "Name": "AgentCount_For_Version_4300",
 "Value": "2"
 },
 {
 "Name": "AgentCount_Windows",
 "Value": "2"
 },
 {
 "Name": "Agents_Through_CloudRelayServer",
 "Value": "0"
 },
 {
 "Name": "CloudRelayEnabled",
 "Value": "0"
 }
]
}
```

The following is a complete sample of a JSON file:

```

{
 "Content": {
 "Version": "1.0",
 "ProductName": "RSA NetWitness Endpoint",
 "ProductType": "RSA NetWitness Endpoint",
 "ProductVersion": "4.3.0.0",
 "ProductInstance": "51bad80c-8865-408b-add4-c0f8058efe32",
 "ActivationKey": "87kqLchJ1qVDt8PwkDoE0Av8LGYjk=",
 "Components": [
 {
 "Id": "2",
 "Name": "SQL Server",
 "Version": "Microsoft SQL Server",
 "Properties": []
 },
 {
 "Id": "3",
 "Name": "SQL Server",
 "Version": "Microsoft SQL Server",
 "Properties": []
 },
 {
 "Id": "4",
 "Name": "Console Server",
 "Version": "4.3.0.0",
 "Properties": [
 {
 "Name": "ActiveCloudRelayServerCount ",
 "Value": "1"
 },
 {
 "Name": "IsMasterConsoleServer",
 "Value": "1"
 },
 {
 "Name": "ConsoleServerCount ",
 "Value": "2"
 },
 {
 "Name": "Mode ",
 "Value": "Fair Distribution"
 }
]
 },
 {
 "Id": "5",
 "Name": "Console Server",
 "Version": "4.3.0.0",
 "Properties": [
 {
 "Name": "ActiveCloudRelayServerCount ",
 "Value": "0"
 },
 {
 "Name": "IsMasterConsoleServer",
 "Value": "0"
 }
]
 }
]
 }
}

```

```
],
 "Metrics": [
 {
 "ComponentId": "4",
 "StartTimeUTC": "1479859260000",
 "EndTimeUTC": "1479945540000",
 "Stats": [
 {
 "Name": "AgentCount",
 "Value": "2"
 },
 {
 "Name": "AgentCount_For_OS:CentOS Linux 7 (Core)",
 "Value": "1"
 },
 {
 "Name": "AgentCount_For_OS:Mac OS X 10.10",
 "Value": "1"
 },
 {
 "Name": "AgentCount_For_Version_4300",
 "Value": "2"
 },
 {
 "Name": "AgentCount_Linux",
 "Value": "1"
 },
 {
 "Name": "AgentCount_Mac",
 "Value": "1"
 },
 {
 "Name": "Agents_Through_CloudRelayServer",
 "Value": "0"
 },
 {
 "Name": "CloudRelayEnabled",
 "Value": "1"
 },
 {
 "Name": "LinuxAgentCount_For_KernelRelease:3.10.0-327.el7.x86_64",
 "Value": "1"
 }
]
 },
 {
 "ComponentId": "5",
 "StartTimeUTC": "1479859260000",
 "EndTimeUTC": "1479945540000",
 "Stats": [
 {
 "Name": "AgentCount",
 "Value": "2"
 }
]
 }
]
}
```

```

 {
 "Name": "AgentCount_For_OS:Microsoft Windows Server 2012 Standard",
 "Value": "2"
 },
 {
 "Name": "AgentCount_For_Version_4300",
 "Value": "2"
 },
 {
 "Name": "AgentCount_Windows",
 "Value": "2"
 },
 {
 "Name": "Agents_Through_CloudRelayServer",
 "Value": "0"
 },
 {
 "Name": "CloudRelayEnabled",
 "Value": "0"
 }
]
},
"Properties": [
 {
 "Name": "AgentCount_Limit_For_License",
 "Value": "50"
 },
 {
 "Name": "LicenseExpirationDate",
 "Value": "2017-06-29 00:00:00.000"
 },
 {
 "Name": "TotalAgentCount",
 "Value": "4"
 },
 {
 "Name": "Version",
 "Value": "4.3.0.0"
 }
]
},
"Checksum": "7D5EB5D5752663BAA5E032F6D4BF8CB0B1E5D23D53CEA605C72F272560028E94"
}

```

## NetWitness Endpoint UI URL Commands

This topic describes the specifications of a new protocol handler used in the NetWitness Endpoint web UI similar to the RSA NetWitness Suite UI. On activation of the link, a URL with the protocol "ecatui:///..." is capable of launching the NetWitness Endpoint UI on a particular machine in view.

In NetWitness Endpoint, each view is identified with a unique address and the view in the NetWitness Endpoint UI can be triggered by a command. You need to follow a syntax to trigger the view. The keyword identifies the type of view and can be followed by specific details of the view.

### Prerequisites

You must have the NetWitness Endpoint UI installed on your system.

### General Syntax

The general syntax for triggering the view is as follows :

**ecatui:///<keyword>/<details>**

Where,

**ecatui:///** is the standard syntax for the NetWitness Endpoint UI Protocol;

*<keyword>* can be: machines, modules, dashboard, certificate, and so on;

*<details>* can be: name of machine, name of module, general filtering characters ( like \* ), and so on.

**Note:** Agent IDs and IP addresses can be used for machines. File hash values can be used for modules.

The following table lists the different behaviors associated with each case.

Case	Syntax	Behavior
------	--------	----------

Case	Syntax	Behavior
<p><b>Single Machine View</b></p> <p><b>keyword:</b>machines</p> <p><b>details:</b>&lt;name&gt; &lt;agentID&gt; &lt;IPAddress&gt;</p>	<p><a href="#">ecatui:///machines/&lt;name&gt;</a></p> <p><a href="#">ecatui:///machines/&lt;agentID&gt;</a></p> <p><a href="#">ecatui:///machines/&lt;IPAddress&gt;</a></p> <p>Example :</p> <p><a href="#">ecatui:///machines/WIN7SP1X86</a></p> <p><a href="#">ecatui:///machines/10.2.3.69</a></p> <p><a href="#">ecatui:///machines</a></p>	<p>Use this command to open a single machine view that specifies the name or agent ID or IP address.</p> <p>If there are multiple machines of the same name, which is very rare, both machines will be listed in the machine view.</p> <p>Alternate Deprecated Syntax:</p> <p>You can use another syntax that is available for machines:</p> <p><a href="#">ecatui://&lt;name&gt;</a> or <a href="#">ecatui://&lt;agentID&gt;</a> or <a href="#">ecatui://&lt;IPAddress&gt;</a> .</p> <p>This syntax is only applicable for machines and this syntax is used by the RSA NetWitness Suite for its NetWitness Endpoint integration feature.</p>



Case	Syntax	Behavior
<p><b>Multiple Machine View</b></p> <p><b>keyword:</b> machines</p> <p><b>details</b></p> <p>&lt;name&gt;:&lt;name&gt;: &lt;agentID&gt;: &lt;agentID&gt;: &lt;IPAddress&gt;: &lt;IPAddress&gt;:</p>	<p><code>ecatui:///machines/&lt;name1&gt;: &lt;name2&gt;:&lt;name3&gt;:...</code></p> <p><code>ecatui:///machines/&lt;agentID1&gt;: &lt;agentID2&gt;:&lt;agentID3&gt;: ...ecatui:///machines/&lt;IPAddress1&gt;: &lt;IPAddress2&gt;:&lt;IPAddress3&gt;: ...</code></p> <p>Example</p> <p><code>ecatui:///machines/WIN7SP1X86:WIN7SP1Y 67:WIN7SP1Z56 ecatui:///machines/10.2.3.69:192.168.53.23:1 0.2.3.98ecatui:///machines/e6a9bb54-da25- 102b-9a0 3-2db401e887ec</code></p>	<p>Use this command with a combination of names using a separator ":".</p> <p>This command opens a Single Machine view for each valid machine specified. If names are specified more than once, and if the IDs or IPs are invalid, they are ignored.</p>
<p><b>Global Machine View</b></p> <p><b>keyword:</b> machines</p> <p><b>details:</b> *</p>	<p><code>ecatui:///machines/*</code></p>	<p>Use this command to open the global machine view, to view a lists of all machines in the environment.</p>

Case	Syntax	Behavior
<p><b>Modules View</b></p> <p><b>keyword:</b> modules</p> <p><b>details:</b> &lt;name&gt; &lt;hash&gt;</p>	<p><a href="#">ecatui:///modules/</a></p> <p>&lt;name&gt;<a href="#">ecatui:///modules/</a>&lt;hash&gt;</p> <p>Example :</p> <p><a href="#">ecatui:///modules/_ssl.pyd</a></p> <p><a href="#">ecatui:///modules/csrss.exe</a></p> <p><a href="#">ecatui:///modules/70A640CBA334F087D216D13005E98484DE125541A941D669398673243B714189</a></p>	<p>Use this command to open the module mentioned in a separate tabbed view. If multiple modules are of same name, both modules will be listed in the module view.</p>
<p><b>Multiple Modules View</b></p> <p><b>keyword:</b> modules</p> <p><b>details:</b> &lt;name&gt;:&lt;name&gt;:... &lt;hash&gt;:&lt;hash&gt;:...</p>	<p><a href="#">ecatui:///modules/</a>&lt;name1&gt;: &lt;name2&gt;:&lt;name 3&gt;:...</p> <p><a href="#">ecatui:///modules/</a>&lt;hash1&gt;: &lt;hash2&gt;:&lt;hash3 &gt;: ...</p> <p>Example :</p> <p><a href="#">ecatui:///modules/_ssl.pyd:csrss.exe</a></p>	<p>You can combine multiple names/hashes combined with a separator ":". This command opens all the valid modules in a separate tabbed view. Invalid or unavailable module details are ignored.</p>
<p><b>Global Module View</b></p> <p><b>keyword:</b> modules</p> <p><b>details:</b> *</p>	<p><a href="#">ecatui:///modules/</a>*</p>	<p>Use this command to open the global modules view, where the view lists all the modules in the environment.</p>

Case	Syntax	Behavior
<b>Dashboard View</b> <b>keyword:</b> dashboard <b>details:</b> None	<code>ecatui:///dashboard</code>	Use this command to open the dashboard view.
<b>Certificate View</b> <b>keyword:</b> certificate <b>details:</b> None	<code>ecatui:///certificate</code>	Use this command to open the certificate view.
<b>Users View</b> <b>keyword:</b> users <b>details:</b> None	<code>ecatui:///users</code>	Use this command to open the users and groups view.
<b>Blocking View</b> <b>keyword:</b> blocking <b>details:</b> None	<code>ecatui:///blocking</code>	Use this command to open the blocking modules view.
<b>Downloads View</b> <b>keyword:</b> downloads <b>details:</b> None	<code>ecatui:///downloads</code>	Use this command to open the downloaded modules view.

Case	Syntax	Behavior
<b>Events View</b> <b>keyword :</b> events <b>details:</b> None	<code>ecatui:///events</code>	Use this command to open the events and notification view.
<b>Servers View</b> <b>keyword:</b> servers <b>details:</b> None	<code>ecatui:///servers</code>	Use this command to open the server configuration view.
<b>IIOCs View</b> <b>keyword:</b> iiocs <b>details:</b> None	<code>ecatui:///iiocs</code>	Use this command to open the IIOCs view.
<b>Global IP View</b> <b>keyword:</b> globalip <b>details:</b> None	<code>ecatui:///globalip</code>	Use this command to open the Global IP view.

## List of Host and Service Ports

The supported host and service ports for NetWitness Endpoint are as follows:

From Host	To Host	To Ports (Protocol)	Comments
NetWitness Endpoint Server	NetWitness Endpoint SQL Server	1433 (TCP)	Standard SQL communication port (default value)
NetWitness Endpoint Agent	NetWitness Endpoint Server	443 (TCP), 444 (UDP)	Communication from the Agent to the NetWitness Endpoint Server (default values)
NetWitness Endpoint UI	NetWitness Endpoint SQL Server	1433 (TCP)	To view the data in the UI
NetWitness Endpoint UI	NetWitness Endpoint Server	9443 (TCP), 808 (TCP)	For configuring external components and other REST communications
NetWitness Endpoint Server	RSA NetWitness Suite	5671 (TCP), 443 (TCP)	IM integration
RSA NetWitness Suite	NetWitness Endpoint Server	9443 (TCP)	Recurring feed integration
NetWitness Endpoint Server	Log Decoder	514 (TCP/UDP)	For syslog traffic to NetWitness Suite (If using a different syslog vendor, you need to check with the vendor as the TCP port may change.)
NetWitness Endpoint Server	Liveecat.rsa.com; cms.netwitness.com	443 (TCP)	Live integration

From Host	To Host	To Ports (Protocol)	Comments
NetWitness Endpoint	www.microsoft.com	443, 80 (TCP)	Microsoft .NET 4.5 and SQLXML download during the application install
NetWitness Endpoint Server	File share	445, 137, 139	With read/write access rights
NetWitness Endpoint SQL Server	File share	445, 137, 139	With read/write access rights
NetWitness Endpoint UI	File share	445, 137, 139	With read/write access rights; (optional) without this analyst will not be able to inspect a module when running UI from their machine
NetWitness Endpoint Server	Queued Data folder	445, 137, 139	With read/write access rights
NetWitness Endpoint SQL Server	Queued Data folder	445, 137, 139	With read/write access rights
NetWitness Endpoint Server	RAR (Remote Agents Relay)	5671 (RabbitMQ)	Bi-directional communication between NetWitness Endpoint Server and RAR Server
NetWitness Endpoint Agent	RAR (Remote Agents Relay)	443 (TCP), 444 (UDP)	Communication from the Agent to the RAR Server (default values)
	NetWitness Endpoint Server	9443	REST API Interface port (default)

From Host	To Host	To Ports (Protocol)	Comments
NetWitness Endpoint UI, custom client app, or browser	NetWitness Endpoint Server	9443 (HTTPS)	REST API Interface port (default)

## NetWitness Endpoint and Third-Party Antivirus Products

Third-party antivirus products may not always coexist peacefully with RSA NetWitness Endpoint software, the agent in particular. While we cannot advise you on configuration of third-party software, there are a few procedures that can be followed to reduce the conflicts between NetWitness Endpoint and third-party antivirus software. This is intended as a general guideline and is not intended to replace consultation with the antivirus vendor.

### For Machines Running the NetWitness Endpoint Agent

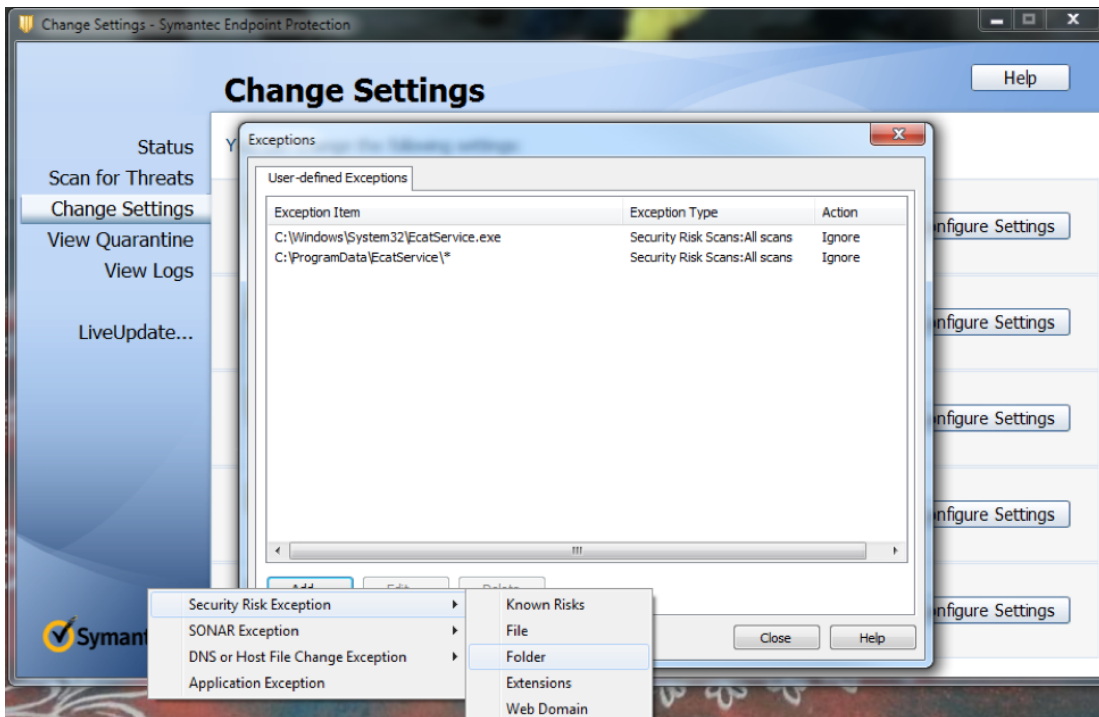
First and foremost, the third-party software needs to "whitelist" the two processes that comprise the NetWitness Endpoint agent. By default, these two processes are named "EcatService" and "EcatServiceDriver" (but alternate names can be specified when the agent installer is built). The third-party software should be configured to ignore `EcatService.exe` (or alternate name) as well as `EcatServiceXXXXX.sys` (the numbers appended to the driver name will vary).

The NetWitness Endpoint agent uses the directory `C:\ProgramData\<<servicename>\` for multiple purposes, including the staging of tracking data and hard links to deleted files (which could be malware) to be transferred to the server. RSA recommends that you configure the third-party antivirus to ignore `C:\ProgramData\EcatService\*` (using the appropriate service name of course) to avoid potential conflicts with third-party antivirus products.

### Example Using Symantec Antivirus to Show the Workflow

The following procedure provides an example workflow for whitelisting NetWitness Endpoint agent files and folders using the Symantec antivirus product.

1. Exclude the NetWitness Endpoint service name and folders from third-party antivirus software.  
Third-party software should be configured to ignore the NetWitness Endpoint service name. By default, the service name is installed as `EcatService.exe` (or alternate name) in location `C:\Windows\System32\EcatService.exe` and ProgramData service name folder `C:\ProgramData\<<servicename>\` (which is used for multiple purposes).



2. Whitelist the NetWitness Endpoint driver file from third-party antivirus software. Third-party software should be configured to whitelist the NetWitness Endpoint driver file EcatServiceXXXXX.sys (or alternate name) located by default in C:\Windows\System32\Drivers\EcatServiceXXXXX.sys (the numbers appended to the driver name will vary) in the following ways:
  - a. Driver file should to be added to third-party software. Customer can whitelist EcatService driver file with SHA256 hash.
  - b. Driver file thumb print should be added to third-party software. If agent is freshly installed or upgraded from one version to another, then you need to check the validity. If the validity expires, then you need to re-upload with newer one.

### For Machines Running the NetWitness Endpoint UI

When a NetWitness Endpoint analyst launches the Module Analyzer, the module being analyzed is copied to the %APPDATA%\local\temp directory on the machine running the UI before it is parsed. It is important to understand that the file is not executed. Third-party antivirus can determine whether or not a file is malicious and quarantine the file before the Module Analyzer can parse it. Whitelisting this directory in your antivirus suite will prevent this from happening, but it does potentially create a blind spot.

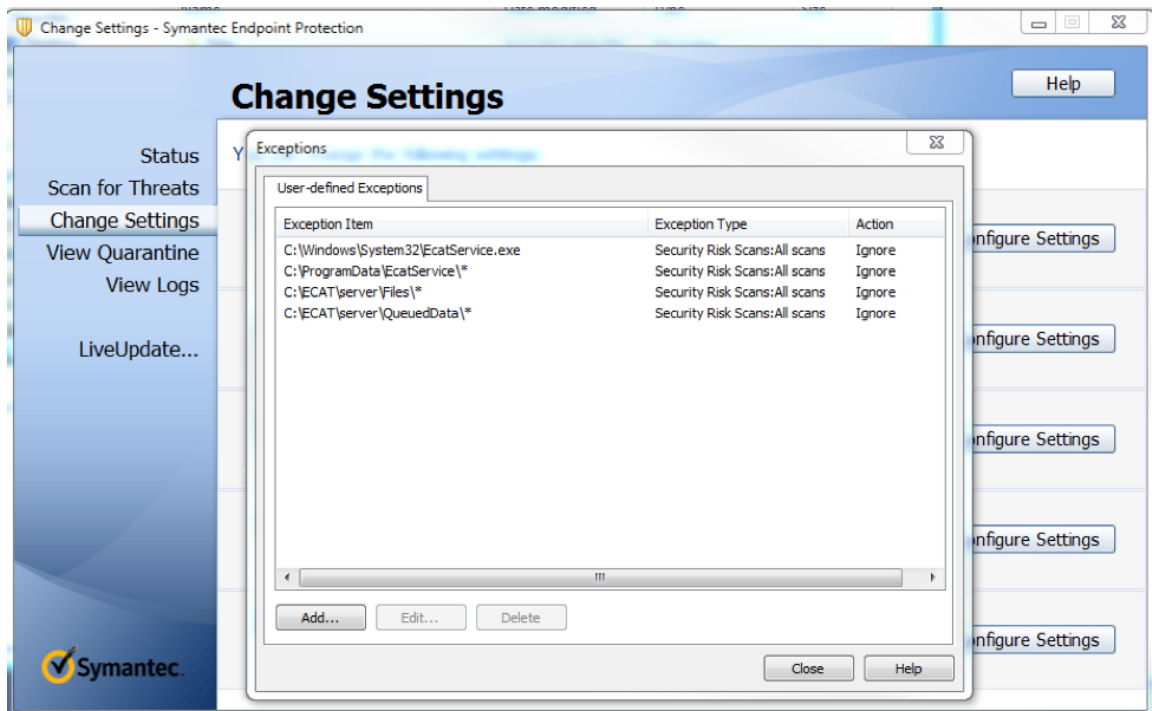


## For Machines Running the NetWitness Endpoint Console Server

The configured files download directory `C:\ECAT\Server` (or different path) must be excluded from third-party antivirus scans. The directory in question is specified in **Configure > Connection > Files UNC Path** in the NetWitness Endpoint UI. For performance reasons only, the following directories can be considered for whitelisting:

- The QueuedData directory
- The folders containing the ECAT\$PRIMARY and tempdb database .mdf and .ldf files

An example of doing this in the Symantec product is shown below.



**Note:** The above workflow might be different for other third-party antivirus vendors. Also, in Symantec, there is no option to add the driver file SHA256 hash or thumb print to whitelist the driver file.

**Note:** If you continue to encounter issues or conflicts with NetWitness Endpoint and third-party antivirus products, please contact [RSA Support](#).

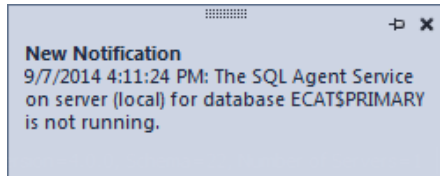
## Troubleshooting

This topic provides information about some common NetWitness Endpoint issues and the troubleshooting steps for these issues.

## 1. Machines don't refresh in the NetWitness Endpoint UI; whitelisting isn't applied to modules; other functions don't seem to work

### Problem:

Even after pressing F5, NetWitness Endpoint features do not seem to refresh. This notification also appears:



### Solution:

A lot of data is managed by SQL Agent jobs. Make sure the SQL Server Agent service is started for your instance of SQL Server.

Service Name	Description	Status	Startup Type
SQL Server (MSSQLSERVER)	Provides stor...	Started	Automatic
SQL Server Agent (MSSQLSERVER)	Executes job...	Started	Automatic
SQL Server Analysis Services (MSSQL)	Supplies online...	Started	Automatic

## 2. The InstallShield says that a port is not available or invalid

### Problem:

The port you selected may be in use on the machine.

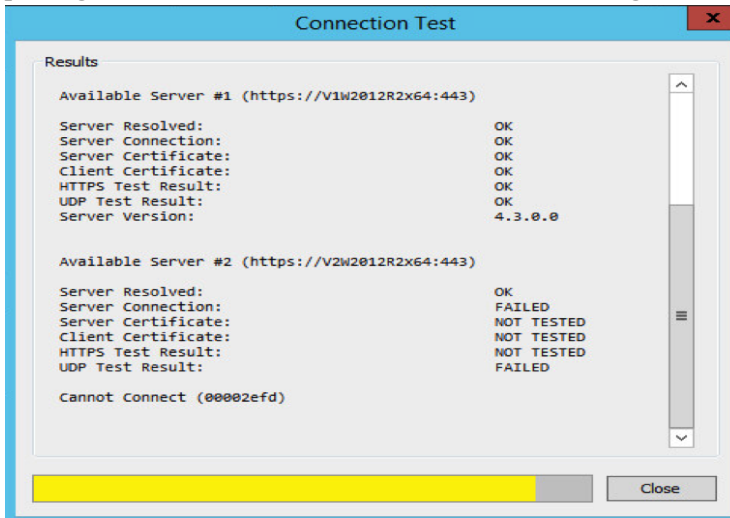
### Solution:

Verify that your previous installation of ConsoleServer is not currently running as a service, or select a different port.

### 3. In the Packager, only half of the Connection Test is succeeding

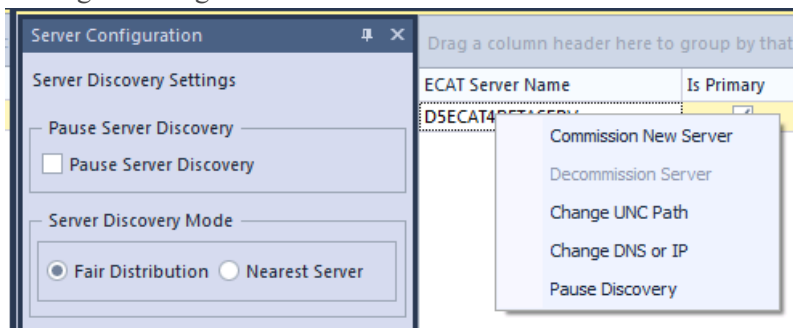
**Problem:**

Because of Server Discovery, the address entered in the Packager is used only to connect to the Primary Server during the initial connection. Afterwards, the Agent or Packager will use the address returned by the Primary Server according to the current setup. A 2<sup>nd</sup> test is made by the packager to confirm that the server is reachable using this address.



**Solution:**

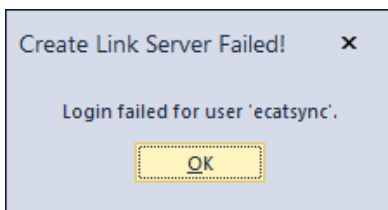
In Server Configuration, change the DNS or IP to something that can be reached by the Packager and Agents.



### 4. Cannot Commission a new Secondary Server: Login failed

**Problem:**

The secondary SQL Server doesn't recognize the password used by the Primary server to connect.



**Solution:**

1. Verify that the user ECATSYNC has the right password on the secondary SQL Server.
2. Verify that the SQL Authentication mode is enabled on the server:
  - Right-click your SQL Server Instance and select **Properties**.
  - Select the **Security option** page and under **Server authentication**, select **SQL Server** and **Windows Authentication** mode.

**5. After installing a new Agent, it doesn't appear in the UI**

**Problem:**

The UI is opened but new Agents don't appear.

**Solution:**

- Verify that ConsoleServer is running and accessible.
- Verify that SQL Agent Jobs are running.
- Press F5 to refresh the Machine List.

**6. After Installing Metascan, the Server Still Says "Antivirus Engine Disabled"**





**Problem:**

After a successful OPSWAT Metascan installation, the server will state:

Starting Antivirus Engine...  
 WARNING: Disabled.

**Solution:**

Enable the Metascan REST Server Service. See *Step 10: (Optional) Install and Configure Metascan* in the **RSA NetWitness Endpoint Installation Guide** for more details.

Name ^	Description	Status	Startup Type
 Metascan	Metascan	Started	Automatic
 Metascan Helper	Metascan ...	Started	Automatic
 Metascan REST	Ensures II...	Started	Automatic
 Microsoft .NET Framework	Microsoft		Manual

Also verify that the AntiVirusConfiguration configuration file setting is correct and truly points to the REST Server. Verify that the Metascan license is still valid (when using a trial, it expires after 30 days).

**7. The Signature Column Says "Need Signature Revoke Update"**

**Problem:**

The Signature column displays "Need Signature Revoke Update". This occurs when the Server couldn't verify the certificate validity for a too long a period of time.

**Solution:**

This means that the certificate expiration could not be validated (or was never checked) or that it has not been validated for more than two weeks (the certificate revocation list should be rechecked). Each different signature URL needs to be updated.

To update them, select **TopMenu > Configure > Update Certificates**, or use the ConsoleServerSync.exe tool. For more information see [NetWitness Endpoint ConsoleServerSync Tool](#).

## 8. The ECAT\_ProcessMergeScanBatches (ECAT\$PRIMARY)] process refuses to start after staging scan files

**Problem:**

If the scan files are not accessible to the database for some reason, they will accumulate in the folder without being consumed by the database.

**Solution:**

Modify the following line in ConsoleServer.exe.config file:

```
<add key="QueuedDataPath" value="{Path accessible to the DB}"></add>
```

Unwanted data will be deleted and new data will be consumed by the database.

## 9. Troubleshooting IM Integration

1. Check if IM is receiving alerts from Reporting Engine, Malware Analysis, or ESA components. Also check to see if there are any issues with NetWitness Endpoint.
2. Make sure that port 5671 is available on the broker machine and check in IP List tables. If not, stop iptables, add entry, and start.
3. Verify if Rabbit MQ server is running; check logs in location `/var/log/rabbitmq/startup_err` log. If there are some errors, then it will show up in `startup_err` as shown below:

```
-rw-r--r--. 1 rabbitmq rabbitmq 4142160 Dec 14 00:01 sa@localhost.log-20141214
-rw-r--r--. 1 root root 0 Dec 17 05:32 shutdown_err
-rw-r--r--. 1 root root 43 Dec 17 05:32 shutdown_log
-rw-r--r--. 1 root root 0 Dec 17 05:35 startup_err
-rw-r--r--. 1 root root 336 Dec 17 05:36 startup_log
-rw-r--r--. 1 rabbitmq rabbitmq 84586589 Dec 19 05:01 sa@localhost.log
```

4. Verify if there are any errors in IM Logs `/opt/rsa/IM/logs/im.log`.
5. Restart IM service if there are any errors and check IM DB connection.

