



ForeScout

Core Extensions Module: IOC Scanner Plugin

Configuration Guide

Version 2.4.1



Contact Information

Forescout Technologies, Inc.

190 West Tasman Drive

San Jose, CA 95134 USA

<https://www.Forescout.com/support/>

Toll-Free (US): 1.866.377.8771

Tel (Intl): 1.408.213.3191

Support: 1.708.237.6591

About the Documentation

- Refer to the Technical Documentation page on the Forescout website for additional documentation: <https://www.Forescout.com/company/technical-documentation/>
- Have feedback or questions? Write to us at documentation@forescout.com

Legal Notice

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

2020-07-06 10:01

Table of Contents

About the Forescout IOC Scanner Plugin.....	5
About Certification Compliance Mode	6
About Support for Dual Stack Environments.....	6
Use Cases	6
Broaden the Scope and Capacity of Scanning Activities	6
Use Forescout Policy Actions to Handle Infected Endpoints	7
Perform Enterprise-Wide Forensics.....	8
Threat Information Sharing.....	8
Plugin Tools.....	8
How It Works	9
IOC Detection	10
Best Practices	11
Initial Scan.....	11
Scan for New Threats.....	13
Periodic Scan	13
False-Positive Threat Handling	13
Risk Mitigation	14
Dependencies	15
Configuration of Network-based Observables.....	15
Configuration of Endpoint-based Observables	16
Considerations	16
Malware Removal Limitation	16
Real-Time Detection Limitation.....	16
Process Detection Limitation	16
Detection of Changes Limitation	17
Malware Family Detection Limitation	17
CnC Detection Limitation	17
Suspect DNS Detection	17
Registry Detection	18
Detection and CPU Performance	18
What to Do	19
Requirements.....	19
Upgrade Issues	19
Configure the Plugin.....	20
Ensure That the IOC Scanner Is Running	20
View the IOC Scanner Table	21
IOC Repository Fields.....	21
Manually Add a Threat to the Repository.....	22
Manually Add an IOC to a Threat.....	23
Remove Threats from the Repository	24
Manually Remove Threat Data.....	24
Manage Automatic Removal of Threat Data	25
View Threat IOCs	25

Manually Add a Threat to the Repository.....	26
Manage Threat Exceptions.....	28
IOC Subscribers.....	29
Run IOC Scanner Policy Templates.....	31
CounterACT IOC Hunting Policy Template	31
Create a CounterACT IOC Hunting Policy	32
Percentage of Threat Match Policy Template.....	35
Create a Threat Match Policy.....	35
ATD Specific IOCs Detected Policy Template.....	39
Create a ATD Specific IOCs Detected Policy.....	39
Test the IOC Scanner Policy Workflows.....	43
Create Custom IOC Scanner Policies	46
Properties	46
Actions	46
Detect IOCs – Policy Properties	47
IOC Scan Stats	47
IOCs Detected by CounterACT.....	49
Last Reported IOC.....	50
Last Scan Status	51
Scan Endpoints – Policy Actions.....	52
Scan and Remediate Known IOCs	53
Add Threat Exception.....	55
Manually Add an IOC to a Threat	55
Remove Threats from the Threat Exception Repository	56
Manually Remove Threat Exception Data	57
Display Inventory Information.....	58
Appendix: The DNS Query Extension	59
Configure and Test the Extension	59
Sample Test	60
Detect Endpoints – DNS Query Properties	62
Is a DNS Server	62
DNS Event	63
Core Extensions Module Information	63
Additional Forescout Documentation.....	64
Documentation Downloads	64
Documentation Portal	65
Forescout Help Tools.....	65

About the Forescout IOC Scanner Plugin

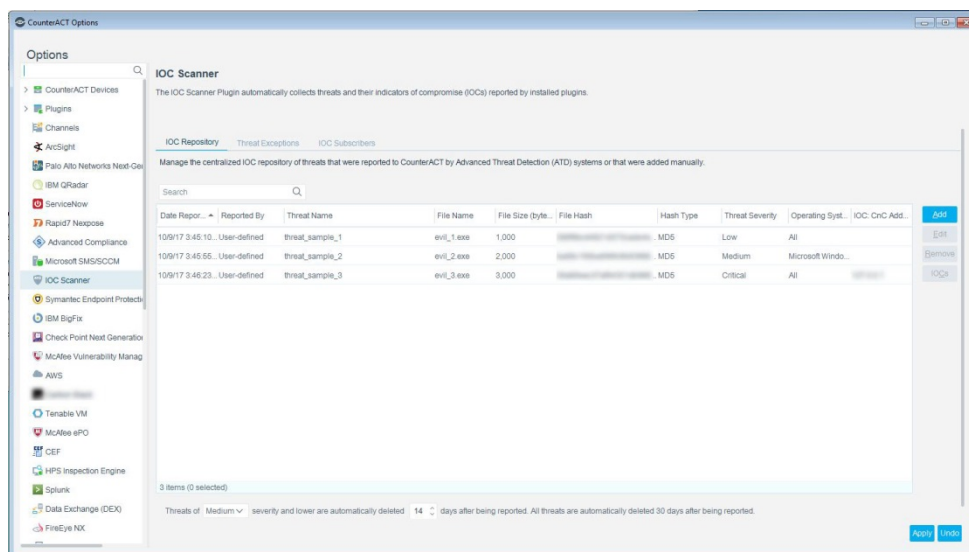
The IOC Scanner Plugin is a component of the Forescout Core Extensions Module. See [Core Extensions Module Information](#) for details about the module.

The IOC Scanner Plugin leverages threat detection and threat prevention mechanisms of third-party systems with the network visibility and enforcement capabilities of the Forescout platform. This lets you accelerate response time, automate workflows, improve operational efficiency, and provide superior security.

The Forescout platform weighs in with its complete real-time visibility and agentless capabilities to fill the void of third-party threat detection and threat prevention systems which may not have full visibility and consequently may overlook important endpoint activity.

Specifically, the plugin serves as:

- A mechanism for scanning all Windows endpoints managed by the Forescout platform for Indicators of Compromise (IOC). See [Scan and Remediate Known IOCs](#).
- A centralized repository of all threats and their IOCs reported to the Forescout platform or added manually. See [View the IOC Scanner Table](#) for details.



- For each threat in the repository, the IOC Scanner Plugin stores the threat file hash and an unordered list of its IOCs.

When scans indicate a threat, you can complete the security cycle by rolling out Forescout policy actions to instantly deny or limit network access, mitigate or remediate endpoints, or notify security teams and endpoints users.

- Third-party threat detection and prevention systems integrate with Forescout through Forescout eyeExtend products. In this document, these third-party systems are referred to as threat intelligence systems.

To use the plugin, you should have a solid understanding of Advanced Persistent Threat (APT) concepts and terminology, and understand how Forescout policies and other basic features work. Additionally, you should understand how to leverage threat intelligence distributed by IOCs.

About Certification Compliance Mode

Forescout Core Extensions Module: IOC Scanner Plugin supports Certification Compliance mode. For information about this mode, refer to the *Forescout Installation Guide*.

About Support for Dual Stack Environments

The Forescout platform detects endpoints and interacts with network devices based on both IPv4 and IPv6 addresses. Scan and Remediate Known IOC actions can be taken on HPS-managed IPv4 and IPv6 endpoints.

Use Cases

This section describes important use cases supported by this plugin.

- [Broaden the Scope and Capacity of Scanning Activities](#)
- [Use Forescout Policy Actions to Handle Infected Endpoints](#)
- [Perform Enterprise-Wide Forensics](#)
- [Threat Information Sharing](#)

Broaden the Scope and Capacity of Scanning Activities

Enhance threat intelligence products by using the intelligent scanning capabilities of the Forescout platform. These capabilities let you achieve sophisticated, actionable high-fidelity scan results.

Broaden the Scope

- When a threat intelligence system detects a new threat and reports it to the Forescout platform, it can automatically scan the network to see:
 - If other Windows endpoints have been infected, including those not monitored by threat intelligence systems.
 - If the malware propagated.
 - If the same threat was propagated or introduced on entry points not monitored by threat intelligence systems, such as email or external devices.

See [Scan for New Threats](#).

- Use the Forescout platform to scan for known threats on Windows endpoints as they attempt to connect to the network. This ensures that infected endpoints are stopped at the threshold of your network. See [Run an Automatic Scan](#).

Enrich Scanning Intelligence

- Scan for one or more specific indications. For example, scan to detect endpoints on which all of the following indications are detected:
 - A specific registry value was set.
 - A specific Mutex IOC was detected.
 - A specific DNS Query IOC was detected.

The screenshot shows a policy configuration window for the IOC Scanner plugin. It includes sections for Name, Condition, and Actions.

Name: search for IOCs relate to Zeus Threat (Mandiant). Description: None. [Edit]

Condition: A host matches this rule if it meets the following condition:
 Advanced view [icon] [icon]

Not	(Criteria)	And/Or	
<input type="checkbox"/>		IOCs Detected by CounterACT - Threat Severity: Critical IOC Type: Registry Key Detection Time NOT: Older than 1 ...		AND	[Add] [Edit] [Remove] [Up] [Down]
<input type="checkbox"/>		ALL IOCs Detected by CounterACT - Threat Severity: Critical Threat File Name: Any Value Threat Reported By: Use...		OR	
<input type="checkbox"/>		IOCs Detected by CounterACT - Threat Severity: Critical Threat File Name: Any Value Threat Reported By: User-def...			

Actions: Actions are applied to hosts matching the above condition.

Enable	Action	Details	
<input checked="" type="checkbox"/>	Add to Group	Add to Group. Schedule: Start=immediately, Occurr...	[Add] [Edit] [Remove]

See [ATD Specific IOCs Detected Policy Template](#).

- Scan endpoints for threats based on specific filters, such as IOC type or severity level. See [ATD Specific IOCs Detected Policy Template](#).
- Evaluate the scan results based on various factors, such as:
 - The severity of the threat detected on the endpoint.
 - The counts and percentages of the IOCs detected on the endpoint of a specific threat. See [IOC Scan Stats](#) for details.

Two policy templates are provided to help enrich your scanning intelligence. See [CounterACT IOC Hunting Policy Template](#) and [ATD Specific IOCs Detected Policy Template](#) for details.


- Continuously monitor all network sessions for all known *DNS Query* IOCs and for the hostname portion of known *CnC Address* IOCs, for example, for a specific malicious URL.

Use Forescout Policy Actions to Handle Infected Endpoints

Complete the security cycle when scans indicate a threat. Use Forescout policies to run policy actions that immediately:

- Contain infected endpoints, for example, by limiting or blocking network access. This prevents lateral movement of the infection to other endpoints.
- Mitigate infected endpoints, for example, by killing suspicious processes.
- Notify stakeholders, for example, by sending the security team an email with details about which threats were detected on which endpoints.
- Perform additional actions, for example, running a vulnerability scan via a vulnerability scanner or triggering a patch update via a patch management system.

See [Create Custom IOC Scanner Policies](#) for details.

 *Use policy actions with caution. It is not uncommon for detected IOCs to be false-positive. See [False-Positive Threat Handling](#).*

Perform Enterprise-Wide Forensics

Use the Asset Inventory to view scan results from different perspectives. For example, run a Forescout policy to identify all endpoints impacted by a specific threat, and then use the Asset Inventory to learn if the threats are location-specific (i.e., emanate from a specific subnet or segment). See [Display Inventory Information](#) for details.

Threat Information Sharing

Use the IOC Scanner Plugin to forward threat intelligence to third-party modules that support this feature.

When a threat intelligence system detects a new threat and reports it to the Forescout platform, it can automatically forward the threat detail to another supported third-party system.

For example, if your network sandbox or Advanced Threat Detection (ATD) solution reports a *GenericThreat105* to the Forescout platform with five unique IOCs, then the Forescout platform can forward those IOCs to your supported Endpoint Detection and Response (EDR) solution so it can hunt for the same threat on each of its managed endpoints. Meanwhile, the Forescout platform keeps a copy of the same threat and IOC and continues threat hunting (as configured) on the network.

Plugin Tools

Plugin tools let you:

- View all threats and their IOCs discovered by threat intelligence systems. See [View the IOC Scanner Table](#).
- [Manually Add a Threat to the Repository](#)
- [Manually Add an IOC to a Threat](#)
- [Remove Threats from the Repository](#)
- [View Threat IOCs](#)
- [Manage Threat Exceptions](#)

- [IOC Subscribers](#)

How It Works

Threat intelligence systems use various methods (including but not limited to: sandbox, heuristics, reverse engineering, and human analysis) to gather real-time indication information regarding malware, threats, zero-day attacks, etc.

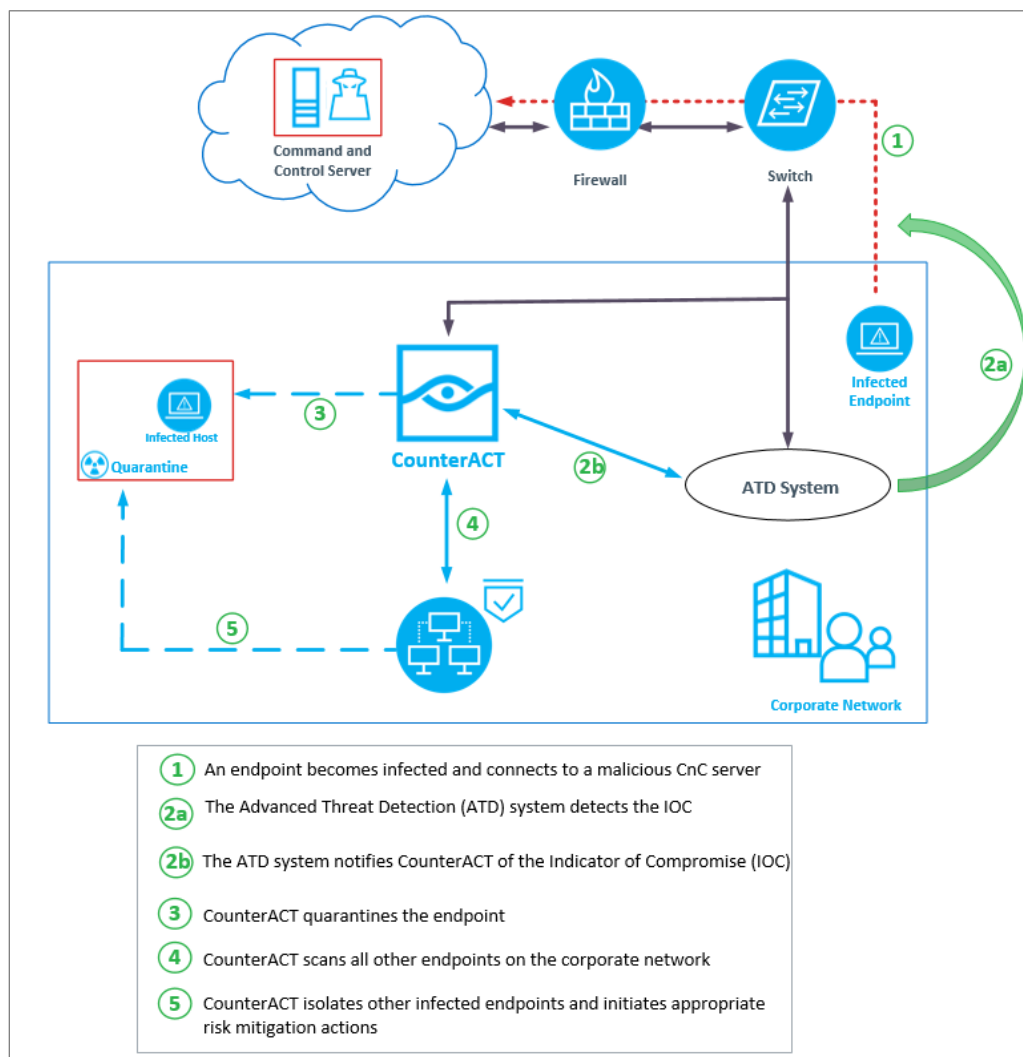
When a threat is detected by a threat intelligence system, the detection system sends the threat details to the Forescout platform. The details may include:

- Source/destination IP address on which the threat was detected
- Timestamp of the event
- Threat name, file name, severity, and hash
- All IOC details identified throughout the lifecycle of the threat

The IOC Scanner Plugin adds the data to the IOC repository, and resolves the data as Forescout properties associated with the endpoint on which the threat was discovered. In addition, the [Last Reported IOC](#) property is resolved on all Windows endpoints for the appropriate threat severity. These properties can be used to trigger policy actions, such as triggering a scan or reacting to scan results.

Low severity threats are deleted from the repository after a pre-configured amount of time. See [Manage Automatic Removal of Threat Data](#) to configure the severity level and number of days.

IOC Detection



The IOC repository includes all IOCs identified by threat intelligence systems throughout a threat's lifecycle. The IOC Scanner Plugin uses this information to detect the same threat on other endpoints. For example, plugin-initiated scans of endpoints can detect IOCs used during a threat infection phase and then trigger appropriate restrictive actions.

- *For each threat in the repository, the IOC Scanner Plugin stores the threat file hash and an unordered list of its IOCs that were provided by threat intelligence system(s). The plugin does not support YARA rules, STIX, OpenIOC or any other format that identifies and classifies malware families.*
- The [Scan and Remediate Known IOCs](#) action scans endpoints for many types of known IOCs, and gives the option of killing processes initiated by IOCs.

■ *Use this option with caution to avoid terminating legitimate processes.*

You can create Forescout policies that trigger appropriate risk mitigation and restrictive actions.

The Forescout platform handles *CnC Address* and *DNS Query* IOCs differently than other IOCs:

- The Forescout platform continuously monitors all network sessions for each known *CnC Address* and *DNS Query* IOC from the time the IOC is added to the IOC repository until it is purged from the repository.
- For other IOC types, the Forescout platform scans endpoints at a specific point in time.

For CNC Address IOCs containing a domain name, the IOC Scanner Plugin tries to resolve the domain automatically. For each successful resolution, the plugin retries this resolution after one minute. If at any point the resolution fails, the plugin retries to resolve this CNC IOC after one hour. This default behavior can be changed by changing the following plugin properties:

- `config.atc.autoresolve_failed_cnc.value` (can be set to 'true' or 'false' depending on whether the user wants turn on turn off the auto-resolution of failed CNCs via the IOC Scanner Plugin.)
- `config.atc.dnsres_failed_period.value` (this is specified in seconds to specify the time interval after which all failed CNCs are resolved by the IOC Scanner Plugin.)


Best Practices

This section describes best practices for scanning Windows endpoints.

- [Initial Scan](#)
- [Scan for New Threats](#)
- [Periodic Scan](#)
- [False-Positive Threat Handling](#)
- [Risk Mitigation](#)

Initial Scan

To detect IOC types other than *CnC Address* and *DNS Query*, a scan must be run. You can scan:

- All endpoints in a specific subnet whenever a new threat is received from a threat intelligence system.
 - Each new endpoint upon admission.
-  *No scan is required to detect CnC Address and DNS Query IOCs because the plugin continuously monitors all network sessions for these IOCs.*

There are two ways to trigger an endpoint scan:

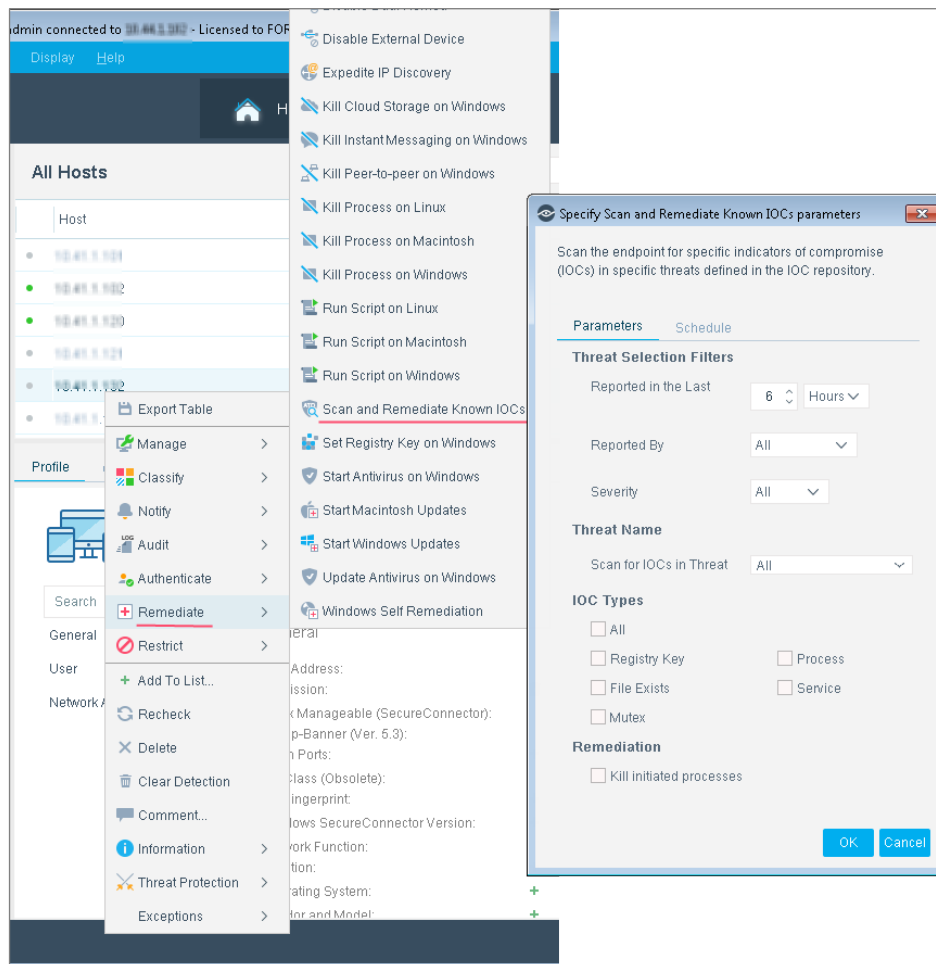
- [Run a Manual Scan](#)
- [Run an Automatic Scan](#)

Run a Manual Scan

Run a manual scan on a specific endpoint.

To run a manual scan:

1. In the Console, Home tab, right-click the endpoint and select **Remediate**. Then select **Scan and Remediate Known IOCs**.



2. In the Specify Scan and Remediate Known IOCs parameters dialog box, enter the scan criteria and then select **OK**. See [Scan and Remediate Known IOCs](#).

Run an Automatic Scan

Use a ForeScout policy to trigger a scan on some or all endpoints in the network. See [Create Custom IOC Scanner Policies](#) for details.

It is recommended to create a policy with the following rules:

- **Main Rule Condition**
 - Network Function: Windows Machine


- **Main Rule Advanced**
 - Recheck unmatched tab: Every 8 hours, Activate on any admission
 - Recheck matched tab: Every 8 hours, Recheck on any admission
- **Sub-Rule Condition**
 - Admission: New Host, Occurred within the last 30 minutes
- **Sub-Rule Action**
 - Scan and Remediate Known IOCs: All Threats reported in the last 8 hours, All IOC Types

Scan for New Threats

It is recommended to create a policy that scans all endpoints, or endpoints not monitored by a threat intelligence system, for newly reported threats that might pose a significant risk to your network. For example, scan endpoints for new Critical threats no more than one hour after a new Critical severity threat is reported. See [Create Custom IOC Scanner Policies](#) for details.

It is recommended to create a policy with the following rules:

- **Main Rule Condition**
 - Network Function: Windows Machine
- **Main Rule Advanced**
 - Recheck unmatched tab: Every 8 hours, Activate on any admission
 - Recheck matched tab: Every 8 hours, Recheck on any admission
- **Sub-Rule Condition**
 - Last Reported IOC: Critical Severity does not meet the criteria: Older than 1 hour
- **Sub-Rule Action**
 - Scan and Remediate Known IOCs: All Critical Severity Threats reported in the last 1 hour, All IOC Types

 *Depending on your corporate needs, you can create similar policies that scan threats of lower severities less frequently.*

Periodic Scan

It is recommended to create a policy that periodically scans all endpoints, or endpoints not monitored by a threat intelligence system, for reported threats that might pose a significant risk to your network. For example, scan endpoints for all Critical threats every 8 hours. See [Create Custom IOC Scanner Policies](#) for details.

False-Positive Threat Handling

Different features of the plugin enable you to focus on the reported threats most likely to compromise your network security.

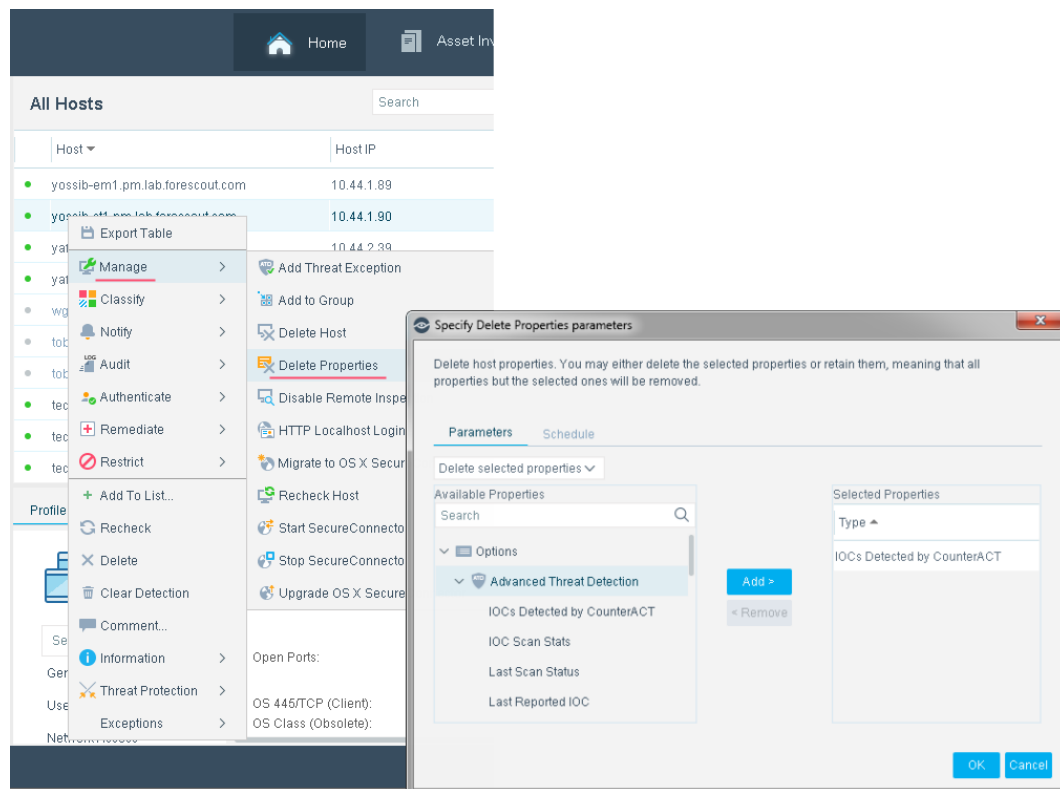
- Narrow your selection of threat filters and IOC types in the [Scan and Remediate Known IOCs](#) action to scan for threats and indications most likely to compromise your network security.
- If a scan indicates the presence of IOCs on an endpoint, isolate the endpoint and then manually review the scan results to determine if the endpoint requires remediation.
- For additional information about the likelihood of a specific threat infection:
 - Use the [IOC Scan Stats](#) property to ascertain how many IOCs the scan detected of a threat of interest, and what percent of its IOCs were detected.
 - Modify and run the [CounterACT IOC Hunting Policy Template](#) to automatically run risk mitigation actions when scan results indicate a likelihood of infection.
- Some reported threats do not indicate a security compromise when detected on a specific endpoint. Use the [Add Threat Exception](#) action to ignore a threat's detection on that endpoint.

Risk Mitigation

When an endpoint is suspected of being infected, it is recommended to:

1. Contain the compromised endpoint in a group created for the severity level of the suspected threat.
2. Use the Forescout platform to automatically isolate endpoints in some or all of the severity groups. For example, isolate all endpoints in the Critical and High Severity group.
3. Manually perform appropriate actions, such as remediation, on each endpoint that was isolated. See [False-Positive Threat Handling](#).
4. When it is determined that it is safe to admit the endpoint to the network, use the Delete Properties action so that the endpoint is no longer marked for remediation or restriction.

In the Console, Home tab, right-click the endpoint, select **Manage** and then select **Delete Properties**.



5. In the Selected Properties field, select the property to be deleted, and select **Remove**.
6. Select **OK**.

Dependencies

IOCs are linked to observables and observables are linked to measurable events or stateful properties which can represent anything from the creation of a registry key on a host (measurable event) to the presence of a *mutex* (stateful property). For the IOC Scanner to function optimally, the Forescout platform must be able to observe and measure events on the network and endpoint.

To ensure that the Forescout platform can measure these network and endpoint events, the following configuration is recommended:

- [Configuration of Network-based Observables](#)
- [Configuration of Endpoint-based Observables](#)

Configuration of Network-based Observables

File Exists, Mutex, Process, Registry Key, Service

The monitor interface of the Forescout platform must be attached to a Mirror, TAP, or SPAN port. This lets the Appliance monitor and track network traffic. Traffic is mirrored to a port on the switch and monitored by the Appliance. When two switches

are connected as a redundant pair, the Appliance must monitor traffic from both switches. No IP address is required on the monitor interface.

For more information, refer to *Setting Up Switch Connections* in the *Forescout Installation Guide*. See [Additional Forescout Documentation](#) for information on how to access the guide.

Configuration of Endpoint-based Observables

File Exists, Mutex, Process, Registry Key, Service

The Forescout platform must be able to manage each endpoint either via Remote Inspection or SecureConnector. For additional information, refer to *Accessing and Managing Endpoints* in the *Forescout Endpoint Module: OS X Plugin Configuration Guide* or the *Forescout Endpoint Module: Linux Plugin Configuration Guide* as well as *Accessing and Managing Windows Endpoints* in the *Forescout Endpoint Module: HPS Inspection Engine Configuration Guide*. See [Additional Forescout Documentation](#) for information on how to access these guides.

In addition, endpoint based indicators are scanned on Microsoft supported Windows operating systems. Windows operating systems beyond the "End of Extended Support" published by Microsoft are not supported. Refer to the following link for details:

<https://support.microsoft.com/en-us/help/13853/windows-lifecycle-fact-sheet>.

Considerations

Consider the following limitations when you use this plugin.

Malware Removal Limitation

The Forescout platform is not designed to remove malware from endpoints. It lets the user kill suspicious processes that are detected in real-time, assisting in containing malware propagation and preventing further damage by the malware.

Real-Time Detection Limitation

The plugin supports periodic and on-demand scanning. A scan reflects what is detected on the endpoint at the time of the scan only. It is not persistent on the endpoint.

Process Detection Limitation

Depending on the type of malicious process reported by a threat intelligence system, the plugin may create a related *File Exists* IOC that can be detected even when the process is not running.

- If the reported malicious process indication is an .exe file, the filename is stored in the IOC repository as two different IOCs:
 - *Process* IOC: The process is detected in real-time if it is running at the time of the scan. Upon detection, it can optionally be killed. However, if a malicious process is short-lived and runs during an interval between scans, the process is not detected.
 - *File Exists* IOC: Even if the process has stopped running or has not run yet, this IOC is detected during a scan, and appropriate actions can be run.
- If the malicious process indication is a loaded .dll file, the filename is stored as a *File Exists* IOC only. This version of the IOC Scanner Plugin does not detect a .dll file loaded by a process.
- This version of the IOC Scanner Plugin detects .exe Portable Executable file types only. If a malicious process indication is a different file type, no IOCs are created for the process, and the process is not detected.

Detection of Changes Limitation

The scan does not track changes made on the endpoint. For example, if malware changes a registry value, a subsequent scan detects the revised registry value, but it cannot detect that the specific registry key was changed from a different value.

Malware Family Detection Limitation

The IOC Scanner Plugin recognizes each threat file hash and an unordered list of its individual IOCs that were provided by threat intelligence systems. The plugin does not support YARA rules, STIX, OpenIOC, or any other format that identifies and classifies malware families.

CnC Detection Limitation

For *CnC Address* (*Command and Control URL*) IOC types, the Forescout platform does not monitor the network for the complete URL value. It monitors only for the hostname portion of the URL provided in the **Destination Address** field.

The [DNS Query Extension](#) enhances detection of *CnC Address* IOCs.

Suspect DNS Detection

The DNS Query Extension detects DNS interactions that reference specific host names of interest. When the extension is installed, the IOC Scanner Plugin initiates DNS monitoring that detects the suspect host name mentioned in the IOC. DNS monitoring also enhances detection of *CnC Address* IOCs. For more information, see [Appendix 1: The DNS Query Extension](#).

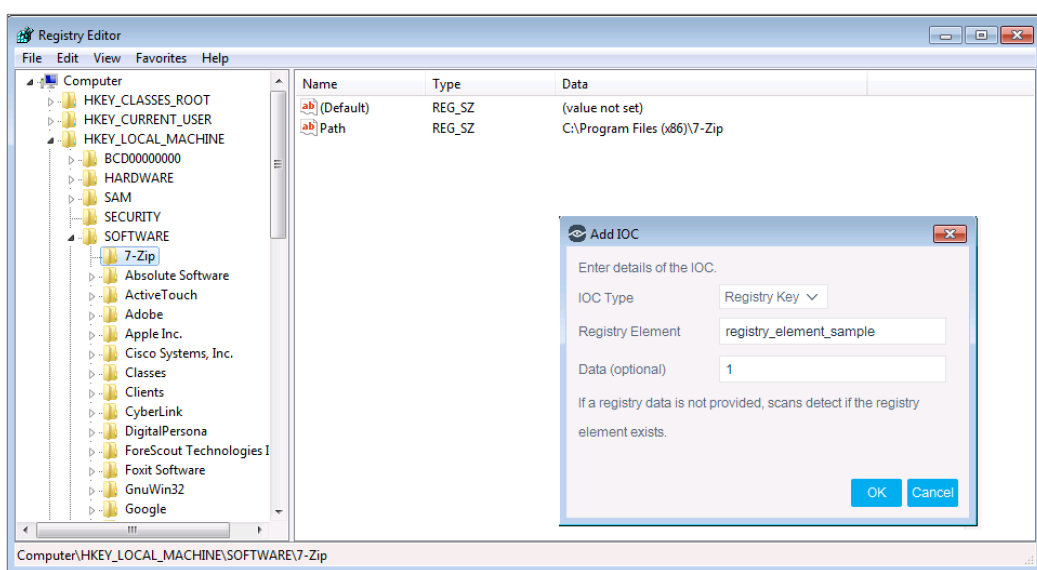
Registry Detection

Registry Keys

The IOC Scanner can scan for the existence of a registry key only, without checking its elements and data. In the example below, you must use the Registry Element **HKEY_LOCAL_MACHINE\SOFTWARE\7-Zip** (including final backslash) and **not** **HKEY_LOCAL_MACHINE\SOFTWARE\7-Zip\ (Default)**.

Registry Elements

To scan for Registry Elements which consist of a Registry Key + Value, use the Registry element: **HKEY_LOCAL_MACHINE\SOFTWARE\7-Zip\Path**. (Without a final backslash)



Data Value

To scan for an exact data value: **HKEY_LOCAL_MACHINE\SOFTWARE\7-Zip\Path** Data: **C:\Program Files\7-Zip** (Without a final backslash)

Detection and CPU Performance

Consider the following CPU performance issues:

- Continuous monitoring of all network sessions for *CnC Address* and *DNS Query* IOCs may negatively impact the Appliance's CPU performance.
- Scanning an endpoint for a large number of IOCs may negatively impact the endpoint's CPU performance.

To purge the IOC repository of threats of lower severities, you can automatically delete them a certain number of days after they were reported to the Forescout platform. See [Manage Automatic Removal of Threat Data](#).

What to Do

You must perform the following to work with this plugin:

1. Verify that system requirements are met. See [Requirements](#).
2. If you are upgrading from an earlier version of IOC Scanner Plugin, see [Upgrade Issues](#).
3. [Configure the Plugin](#). (Optional)
4. [Run IOC Scanner Policy Templates](#) or [Create Custom IOC Scanner Policies](#).
5. [Display Inventory Information](#).

Requirements

The plugin requires the following:

- Forescout version 8.2.1.
- Endpoint Module version 1.2.1 with the HPS Inspection Engine running.
- Core Extensions Module 1.2.1 with the DNS Query Extension Plugin running.
- If you are using Flexx licensing, ensure that you have a valid Forescout eyeControl (ForeScout CounterACT Control) license, to use enforcement actions provided by the component. Refer to the *Forescout Flexx Licensing How-to Guide* for more information about managing Flexx licenses.

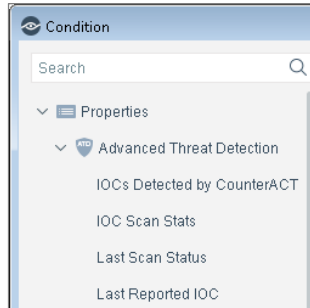
Upgrade Issues

Read this section if you are upgrading to IOC Scanner Plugin version 2.1 from version 2.0.0 or below.

The IOC repository design has been expanded and improved. ***Your existing IOC repository is not compatible with the upgraded design.***

Before upgrading this plugin, the following actions are recommended:


1. For each Advanced Threat Detection Integration solution installed on your system, ensure that you have access to the plugin `.fpi` file for version 2.0.0 Beta 2 or above. Refer to the *Install the Module* section in the configuration guide of each installed Advanced Threat Detection (ATD) solution.
2. Remove and recreate all existing policies that use *Advanced Threat Detection* properties.



3. Uninstall all Advanced Threat Detection Integration solutions lower than version 2.0.0 Beta 2, including the IOC Scanner Plugin (this plugin).
4. For each Advanced Threat Detection Integration solution that you uninstalled in step 3, install the latest release of the Threat Detection Integration Module compatible with IOC Scanner 2.1 or above.

Configure the Plugin

No plugin configuration is required. Once installed, the plugin automatically collects and displays threats and IOCs detected by installed plugins that report threat intelligence information to the IOC repository.

 *Access to Forescout web resources and features may not be enabled by default. Refer to "Define Web Access" in the Forescout Administration Guide.*




Ensure That the IOC Scanner Is Running

After installing the IOC Scanner (and configuring it, if necessary), ensure that it is running.

To verify:

1. Select **Tools > Options > Modules**.
2. In the *Modules* pane, hover over the IOC Scanner name to view a tooltip indicating if it is running on Forescout devices in your deployment.

The name is preceded by one of the following icons:

-  - The IOC Scanner is stopped on all Forescout devices.
-  - The IOC Scanner is stopped on some Forescout devices.
-  - The IOC Scanner is running on all Forescout devices.

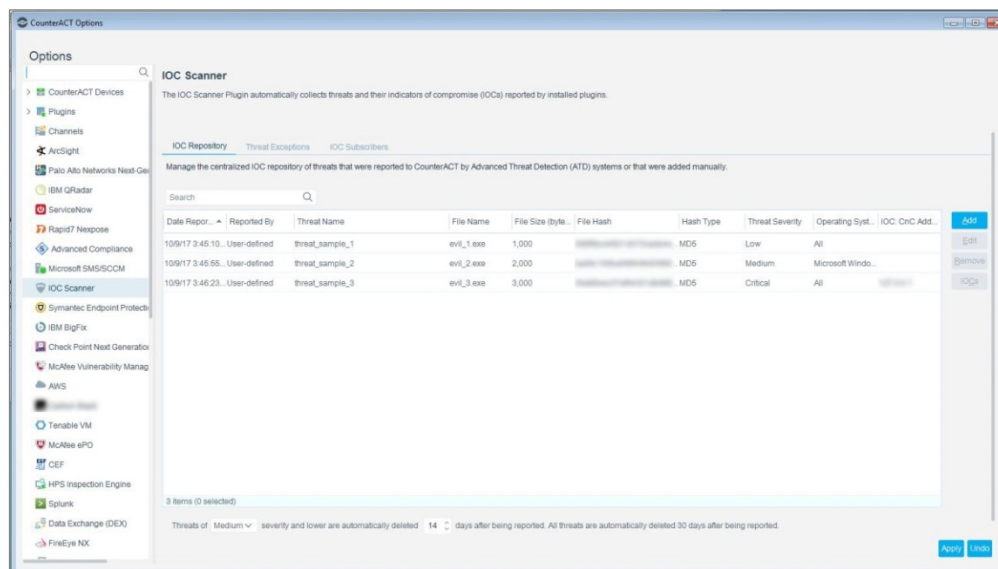
3. If the IOC Scanner is not running, select **Start**, and then select the relevant Forescout devices.
4. Select **OK**.

View the IOC Scanner Table

The IOC Scanner table displays all the threats and IOCs in the IOC repository.

To view the IOC Scanner table:

1. In the Console, select **Options** from the **Tools** menu and go to the **Modules** folder.
2. In the Modules pane, select **Core Extensions > IOC Scanner** and then select **Configure**.



The IOC Repository tab displays the most pertinent information about the IOC.

IOC Repository Fields

Date Reported	The date and time when a threat with this file hash was first reported or manually added to the IOC Scanner Plugin.
Reported By	The threat intelligence system that reported the threat. <i>User-defined</i> indicates that the threat was manually added to the IOC repository and was not reported by a threat intelligence system.
Threat Name	A name used for threat identification purposes only.
File Name	The file name of the threat.
File Size (bytes)	The size of the threat file, in bytes. -1 indicates that no file size was provided by third-party systems.
File Hash	The hash value of the threat file, in hexadecimal format, using lower case characters. This value is used to identify threats in the Scan and Remediate Known IOCs and Add Threat Exception actions. For user-defined threats, this must be a unique identifier. It need not be an actual hash value.

Hash Type	MD5, SHA-1 or SHA-256 hash algorithm for determining the file hash. -None- indicates that the file hash is not an actual hash value.
Threat Severity	Low, Medium, High or Critical threat severity level.
Operating System	The OS (Operating System) for which the threat intelligence system reported the threat. All indicates that the threat was reported for all operating systems.
IOC: CnC Address	Details of the different types of IOCs detected during the lifecycle of the threat.
Threats of XX severity and lower are automatically deleted XX days after being reported.	The level of severity for IOCs to be automatically deleted after a specified number of days. See Manage Automatic Removal of Threat Data . <ul style="list-style-type: none"> Severity level options: Critical, High, Medium (default), and Low. Number of days options: 1-20 days

The Threat Exceptions tab contains the list of threats to be ignored on scans of specific endpoints. See [Manage Threat Exceptions](#).

The IOC Subscribers tab lists all the subscribers that receive IOC notifications. See [IOC Subscribers](#).

Manually Add a Threat to the Repository

You can manually add threats to the IOC repository.

To manually add a threat:

1. In the IOC Scanner pane, IOC Repository tab, select **Add**.

2. Define the following parameters:

Threat Name	Enter any value.
File Name	Enter any value.
File Hash	Enter any unique value not already in the IOC Repository.

3. Define additional parameters as needed. See [IOC Repository Fields](#) for details.
4. Select **OK**, and then select **Apply**.

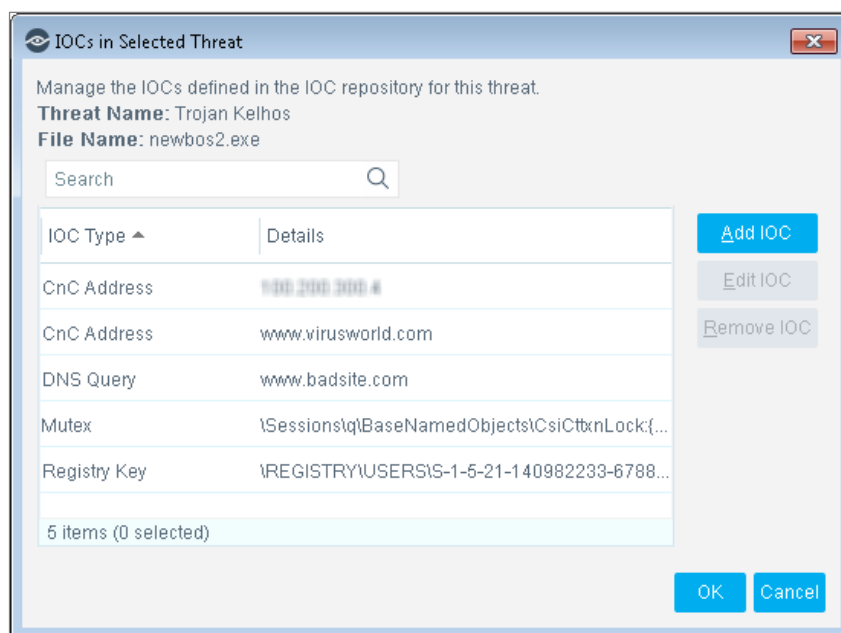
Manually Add an IOC to a Threat

You can manually add IOCs to an existing threat in the IOC repository.

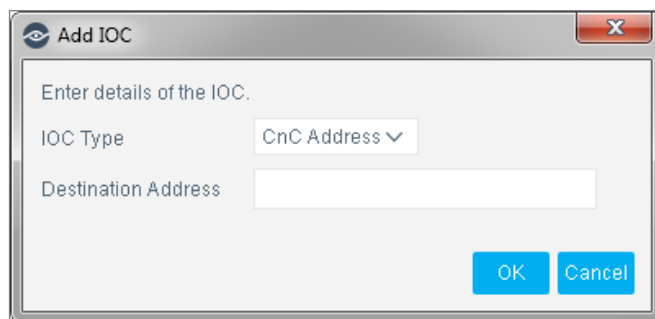
- 📄 *When adding user-defined IOCs, first define a threat. See [Manually Add a Threat to the Repository](#).*

To manually add an IOC to a threat:

1. In the IOC Scanner, IOC Repository tab, select the required threat, and then select **IOCs**.



2. Select **Add IOC**.



3. Enter the details of the threat. For definition of the IOC Types, see [View Threat IOCs](#).
4. Select **OK**.
5. To add another IOC to the threat, repeat steps [2](#) to [4](#).
6. When all the IOCs have been added to the threat, select **OK** in the IOCs in Selected Threat dialog box.

Remove Threats from the Repository

Threats and their IOCs remain in the IOC repository until:

- They are manually removed.
- They are automatically deleted after 30 days.
- A maximum number of 128 threats is reached.

To prevent a negative impact on your Appliance's CPU performance, it is recommended to routinely purge your IOC repository of threats that no longer pose a risk to your network. There are two ways to remove threats from the repository:

- [Manually Remove Threat Data](#)
- [Manage Automatic Removal of Threat Data](#)

Manually Remove Threat Data

You can manually remove individual threats from the IOC repository so that all endpoints are no longer scanned for these threats.

- 📄 *To exempt only specific endpoints from being scanned for a specific threat, see [Add Threat Exception](#).*

To manually remove a threat from the IOC repository:

1. In the IOC Scanner pane, IOC Repository tab, select one or more threats to be removed.
2. Select **Remove**, and in the IOC Scanner pane, select **Apply**.

Manage Automatic Removal of Threat Data

A threat whose severity level is not higher than a specific level can be maintained in the IOC repository a limited number of days only. Threats higher than this severity level are not automatically deleted. An IOC Scanner Plugin global parameter controls how long threats not higher than a specific severity level remain in the IOC repository.

To set the automatic threat deletion parameter:

1. At the bottom of the IOC Repository tab, set the IOC Scanner Plugin global parameters:
 - Select the maximum severity level of threats to be automatically deleted.
 - Set how many days after these threats are added to the repository they are automatically deleted.
2. Select **Apply**.

View Threat IOCs

You can view the details of all IOCs detected during the lifecycle of each threat.

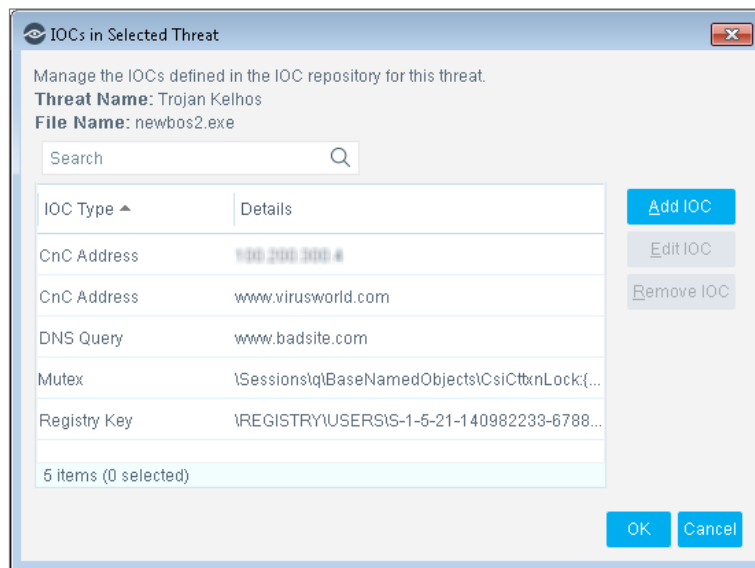
The following IOC types are stored in the IOC repository.

IOC Type	IOC Details
CnC Address (Command and Control URL)	<ul style="list-style-type: none"> Destination Address See CnC Detection Limitation for more information about <i>CnC Address</i> IOCs.
DNS (Domain Name System) Query	<ul style="list-style-type: none"> DNS Name
Process	<ul style="list-style-type: none"> Process Name Process Hash (optional) Process Hash Type See Process Detection Limitation for more information about <i>Process</i> IOCs.
File Exists	<ul style="list-style-type: none"> File Name File Path (optional) <ul style="list-style-type: none"> - If a <i>File Path</i> is not provided, scans detect the file if it is in the local path %PATH%.
Mutex	<ul style="list-style-type: none"> Mutex Name
Registry Key	<ul style="list-style-type: none"> Path Value (optional) <ul style="list-style-type: none"> - If a <i>Value</i> is not provided, scans detect if the registry path exists. - If a <i>Value</i> is provided, scans detect if the value in the registry path matches the value provided. See Registry Detection for Registry scan example.

Service	<ul style="list-style-type: none"> Service <ul style="list-style-type: none"> - Any Windows startup or scheduled system service on the computer.
---------	---

To view threat IOCs:

- In the IOC Scanner pane, IOC Repository tab, select the required threat, and then select **IOCs**.



The details of the selected threat are displayed. See [View Threat IOCs](#) to understand the types of IOCs reported.

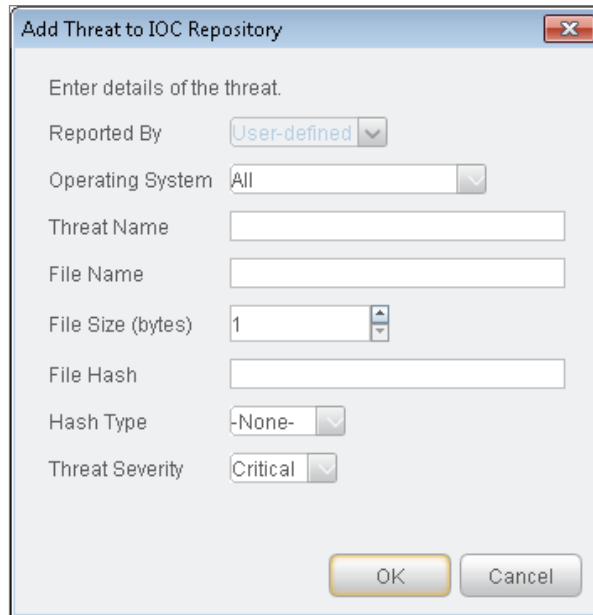
To add an IOC, see [Manually Add an IOC to a Threat](#).

Manually Add a Threat to the Repository

You can manually add threats to the IOC repository.

To manually add a threat to the IOC repository:

- In the IOC Scanner pane, IOC Repository tab, select **Add**.



A dialog box titled "Add Threat to IOC Repository" with a close button (X) in the top right corner. The dialog contains the following fields and controls:

- Enter details of the threat.
- Reported By: User-defined (dropdown menu)
- Operating System: All (dropdown menu)
- Threat Name: (text input field)
- File Name: (text input field)
- File Size (bytes): 1 (spin box)
- File Hash: (text input field)
- Hash Type: -None- (dropdown menu)
- Threat Severity: Critical (dropdown menu)
- OK and Cancel buttons at the bottom right.

2. Define the following parameters:

Threat Name	Enter any value.
File Name	Enter any value.
File Hash	Enter any unique value not already in the IOC Repository.

3. Define additional parameters as needed. See [IOC Repository Fields](#) for details.
4. Select **OK**, and then select **Apply**.

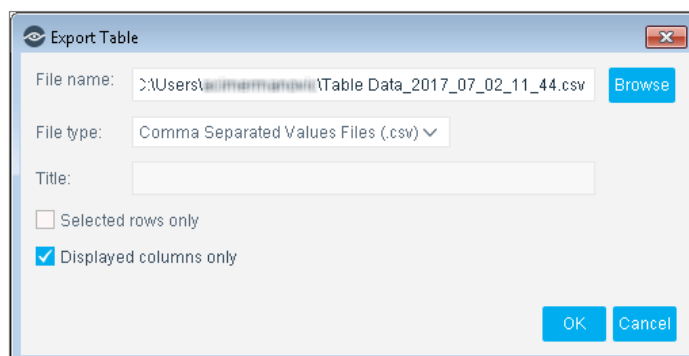
Export IOC Table

You can export threat and IOC information to a CSV or PDF file from:

- the *IOC Scanner* table
- the *IOCs in Selected Threat* table

To export threat or IOC information:

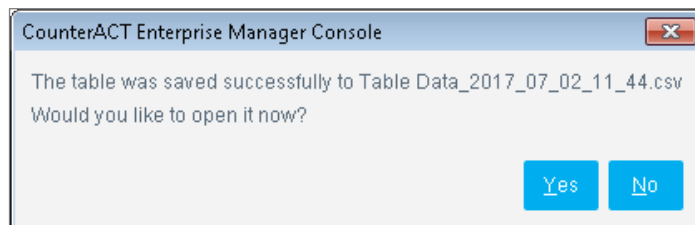
1. Right-click a cell of the IOC Scanner table or the IOCs in Selected Threat table, and select **Export Table**.



A dialog box titled "Export Table" with a close button (X) in the top right corner. The dialog contains the following fields and controls:

- File name: C:\Users\... \Table Data_2017_07_02_11_44.csv (text input field) with a Browse button to its right.
- File type: Comma Separated Values Files (.csv) (dropdown menu)
- Title: (text input field)
- Selected rows only: (checkbox, unchecked)
- Displayed columns only: (checkbox, checked)
- OK and Cancel buttons at the bottom right.

2. Enter the name of the file to which to export the table and select the output file type. For a PDF file, enter a title.
3. Control which information is exported by selecting **Selected rows only** or **Displayed columns only**.
4. Select **OK**.



5. To open the table, select **Yes**. The table is opened in a Microsoft® Excel® spreadsheet or PDF document.

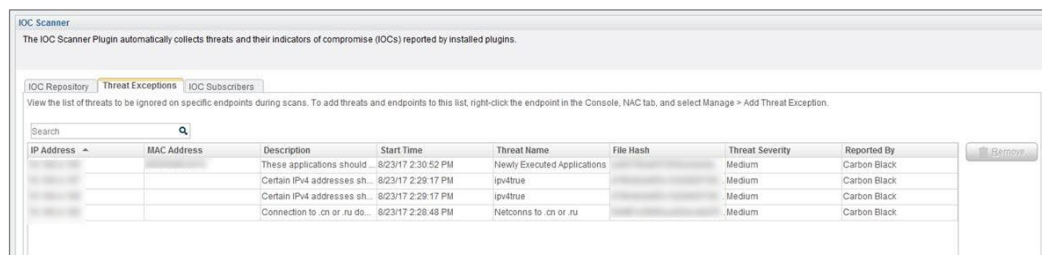
Manage Threat Exceptions

You can trigger the Add Threat Exception action on a given endpoint or on all endpoints so that scans ignore results of specific threats. See [Add Threat Exception](#).

When you no longer want to ignore a threat in the scanning results, you can remove the threat exception from the action.

To manage the scan result threat exceptions:

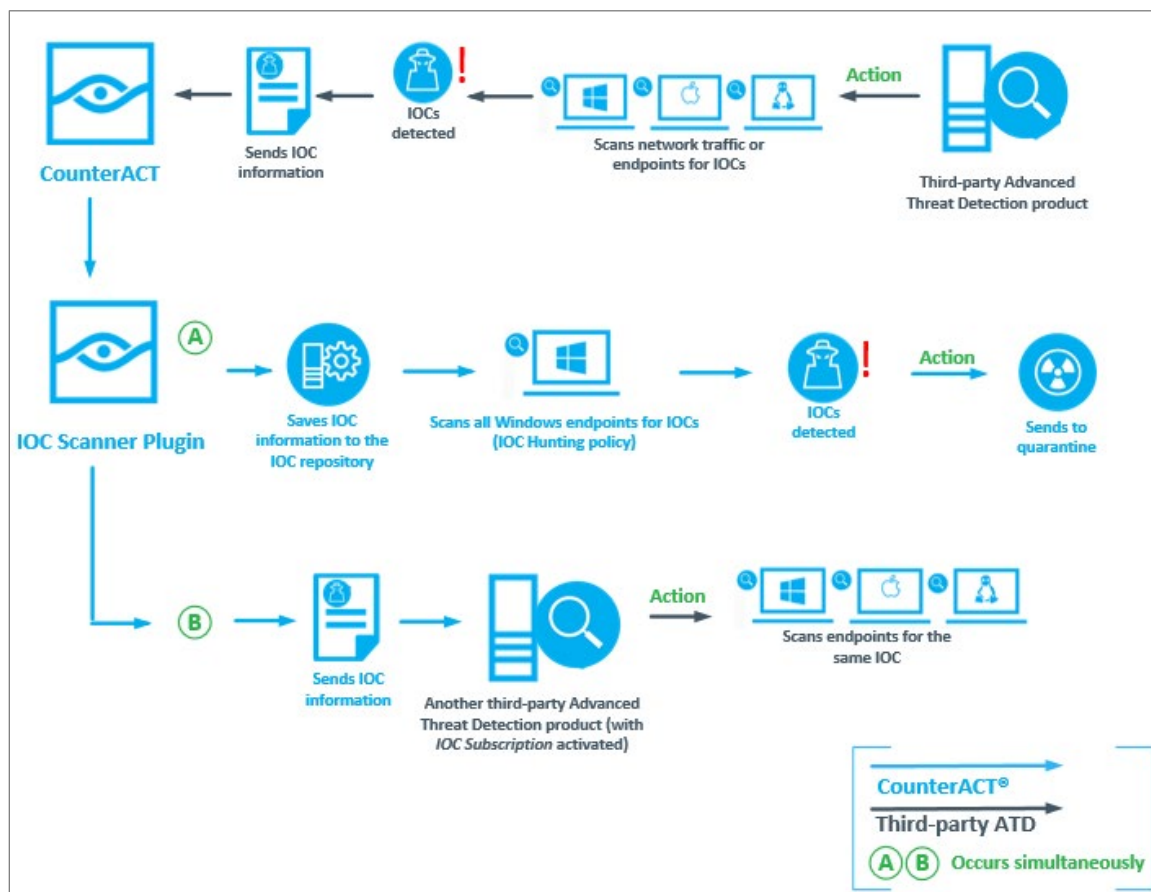
1. In the Console, select **Options** from the **Tools** menu and go to the **Modules** folder.
2. In the Modules pane, select **Core Extensions > IOC Scanner** and select **Configure**. The IOC Scanner pane opens.
3. Select the Threat Exceptions tab. Threats to be ignored on specific endpoints are listed. Each threat is identified by its Threat Identifier value, which consists of:
 - The threat file hash
 - An internal code for the reporting threat intelligence system
 - An internal reference to the operating system (OS) for which the threat was reported




4. To remove one or more threats from the list, select the threat, and then select **Remove**.
5. In the IOC Scanner pane, select **Apply**.

IOC Subscribers

The IOC Subscribers tab lists the threat intelligence plugins that can receive IOC notifications from the Forescout platform (IOC sharing). When a threat intelligence plugin that supports this option is installed, it is automatically added to the IOC Subscribers tab and subscribed to receive all IOC notifications. The threat intelligence plugin then handles received IOCs based on its configuration.



You can choose to register for IOC notifications from All sources (both Advanced Persistent Threat vendors/plugins and User-defined) or User-defined IOCs only, or choose to receive no notifications at all.

 *Plugins that do not support sending or receiving IOC notifications to/from the Forescout platform are not displayed in this tab and are not affected.*

You can also manually update the IOC database by adding user-defined IOCs through the Forescout platform. To provide notification to subscribed plugins in these

cases, there is the need to poll the IOC database upon update (when clicking “Apply”).

The same mechanism is used to report old IOCs to newly registered plugins.

The IOC Subscription notification feature runs on a single Appliance or on multiple Appliances.

To manage IOC sharing between servers:

1. In the Console, select **Options** from the **Tools** menu and go to the **Modules** folder.
2. In the Modules pane, select **Core Extensions > IOC Scanner** and select **Configure**. The IOC Scanner pane opens.
3. Select the IOC Subscriptions tab.
4. Select an item and then select **Edit**.



5. From the Subscribed To drop-down menu, select one of the following options:

ALL	Sends an IOC notification to the Recipient APT plugin from every registered APT plugin that supports this feature, including user-defined IOCs that were manually added. This is the default option.
None	Indicates that IOCs are not to be shared with the selected recipient.
User-defined	Ensures only user-defined (manually added) IOCs are shared with the selected recipient.

6. Select **OK**.
7. In the IOC Scanner pane, select **Apply**. The IOC Scanner Plugin immediately sends the other plugin(s) a notification sharing IOC information.

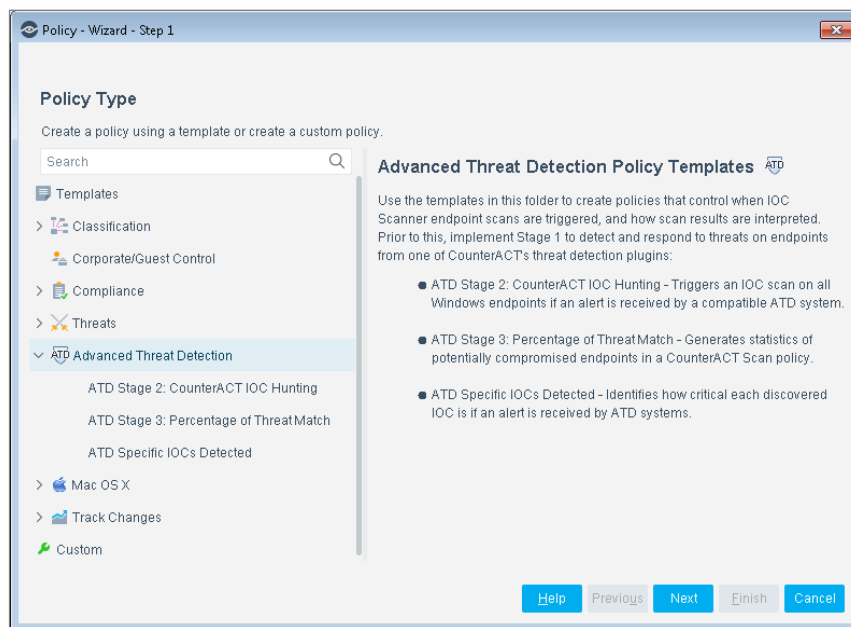
Once the information is sent to the other plugins, it is up to the user of the other plugins to process the IOC information, if that plugin supports IOC notifications.


Run IOC Scanner Policy Templates

This plugin provides policy templates that you can use to manage endpoints on which threats and IOCs were detected. To detect IOC types other than CnC Address and DNS Query, a scan must be run. See [CounterACT IOC Hunting Policy Template](#).

This plugin provides the following policy templates:

- [CounterACT IOC Hunting Policy Template](#) – This policy triggers an IOC scan on all Windows endpoints based on the severity of a threat if an IOC alert is received by a compatible threat intelligence system.
- [Percentage of Threat Match Policy Template](#) – This policy generates statistics of potentially compromised endpoints in a Forescout policy. These statistics show the percentage of IOCs matched to a single threat for detected endpoints, thus indicating the likelihood of infection.
- [ATD Specific IOCs Detected Policy Template](#) – This policy identifies endpoints on which specific IOC details were detected.



 *It is recommended that you have a basic understanding of Forescout policies before working with the templates. Refer to the Forescout Templates and Policy Management chapters of the Forescout Administration Guide. See [Additional Forescout Documentation](#) for information on how to access this guide.*

CounterACT IOC Hunting Policy Template

Use the IOC Hunting policy to trigger an IOC scan on all Windows endpoints based on the severity of a threat if an IOC alert is received by a compatible threat intelligence system.

This template is dependent upon the successful configuration of Threat Intelligence and Endpoint Detection and Response plugins.

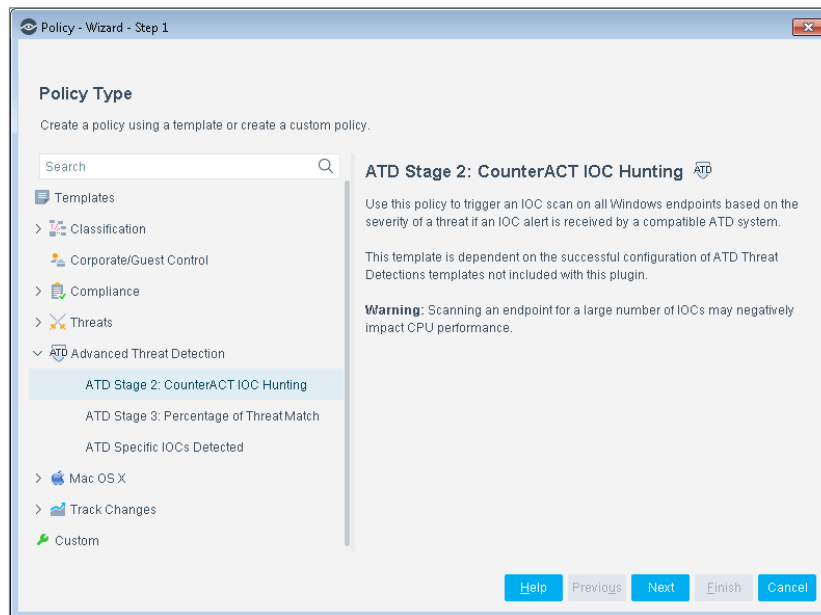
📄 *Scanning an endpoint for a large number of IOCs may negatively impact CPU performance.*

Create a CounterACT IOC Hunting Policy

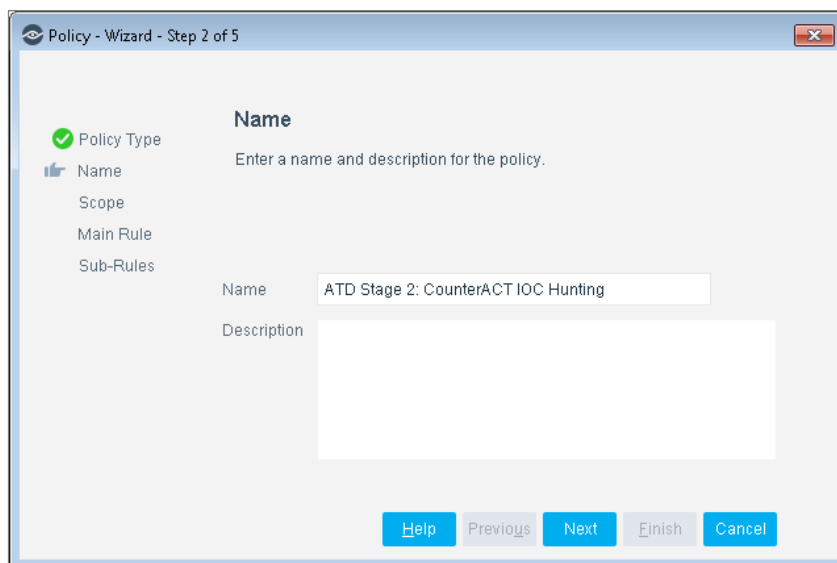
This section describes how to create a policy from the policy template.

To create an IOC Hunting policy:

1. Log in to the Console and select **Policy**.
2. Select **Add** from the Policy Manager. The Policy Wizard opens.
3. Expand the **Advanced Threat Detection** folder and select **ATD Stage 2: CounterACT IOC Hunting**.




4. Select **Next**.



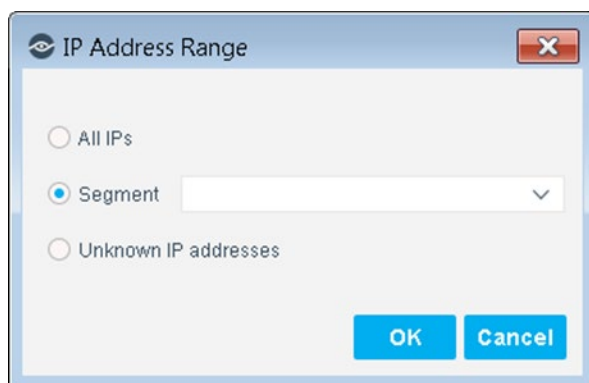
5. Define a unique name for the policy you are creating based on this template, and enter a description.

- Make sure names are accurate and clearly reflect what the policy does. For example, do not use a generic name such as `My_Compliance_Policy`.
- Use a descriptive name that indicates what your policy is verifying and which actions will be run.
- Ensure that the name indicates whether the policy criteria must be met or not met.
- Avoid having another policy with a similar name.

 *Policy names are displayed in the Policy Manager, the Views pane, Reports and in other features. Precise names make working with policies and reports more efficient.*

6. Select **Next**. Both the Scope pane and the IP Address Range dialog box open.

7. Use the IP Address Range dialog box to define which endpoints are inspected.



The following options are available:

- **All IPs:** Include all IP addresses in the Internal Network.

- **Segment:** Select a previously defined segment of the network. To specify multiple segments, select **OK** or **Cancel** to close this dialog box, and select **Segments** from the Scope pane.
 - **Unknown IP addresses:** Apply the policy to endpoints whose IP addresses are not known. Endpoint detection is based on the endpoint MAC address.
8. Select **OK**. The added range is displayed in the Scope pane.
 9. Select **Next**. The Main Rule pane opens.

The main rule of this policy detects endpoints on which any IOC was detected on a Windows machine.

The screenshot shows the 'Policy - Wizard - Step 4 of 5' window. On the left, a sidebar lists the steps: Policy Type, Name, Scope, Main Rule (selected), and Sub-Rules. The main area is titled 'Main Rule' and contains the following sections:

- Condition:** A host matches this rule if it meets the following condition:
 - Criteria: Network Function - Windows Machine
 - Buttons: Add, Edit, Remove
- Actions:** Actions are applied to hosts matching the above condition.
 - Buttons: Add, Edit, Remove
 - Table: No items to display

At the bottom, there are navigation buttons: Help, Previous, Next, Finish, and Cancel.

10. Select **Next**. The Sub-Rules pane opens.
11. Review the sub-rule conditions and actions. See [Sub-Rules](#) for details.
12. Select **Finish** to create the policy.
13. In the Console, select **Apply** to save the policy.

Sub-Rules

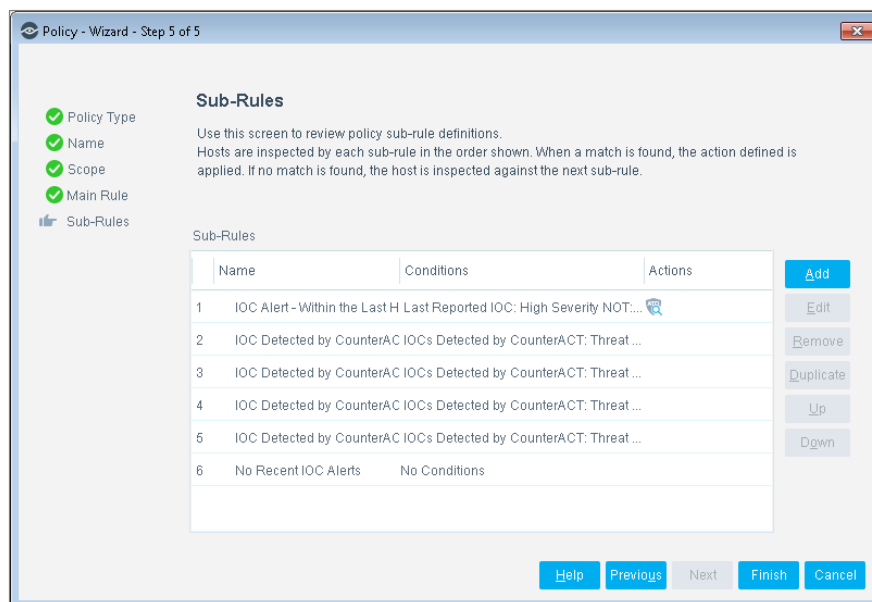
Hosts that match the Main Rule are included in the policy inspection. *Hosts that do not match this rule are not inspected for this policy.*

Sub-rules let you automatically follow up with hosts after initial detection and handling. Creating sub-rules lets you streamline separate detection and actions into one automated sequence.

Sub-rules are performed in order until a match is found. When a match is found, the policy starts to scan all endpoints with no recently identified IOCs. If the endpoint does not match the requirements of the sub-rule, the next rule is examined.


The sub-rules of this policy identify all endpoints with IOCs detected within the last hour. If a new threat is detected, all endpoints are scanned for IOCs contained in the threat:

- IOC Alert – Within the Last Hour
- IOC Detected by CounterACT – Severity Critical
- IOC Detected by CounterACT – Severity High
- IOC Detected by CounterACT – Severity Medium
- IOC Detected by CounterACT – Severity Low
- No Recent IOC Alerts



Percentage of Threat Match Policy Template

Use this policy to generate statistics of potentially compromised endpoints in a Forescout policy. These statistics show the percentage of IOCs matched to a single threat for detected endpoints thus providing the likelihood of infection. Generally speaking, the higher the percentage, the greater the threat.

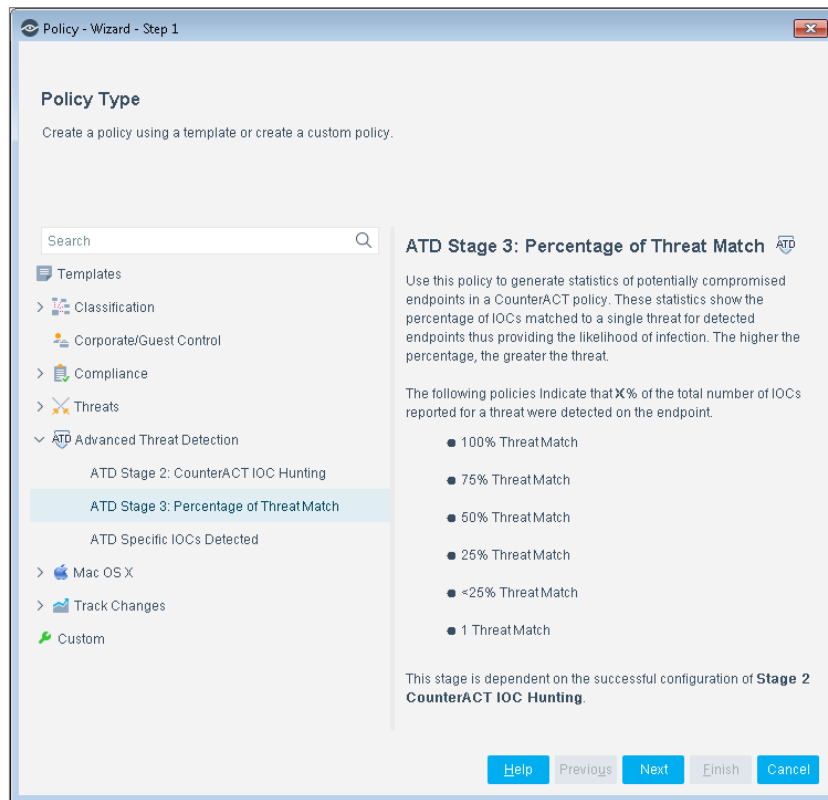
 *Scanning an endpoint for a large number of IOCs may negatively impact CPU performance.*

Create a Threat Match Policy

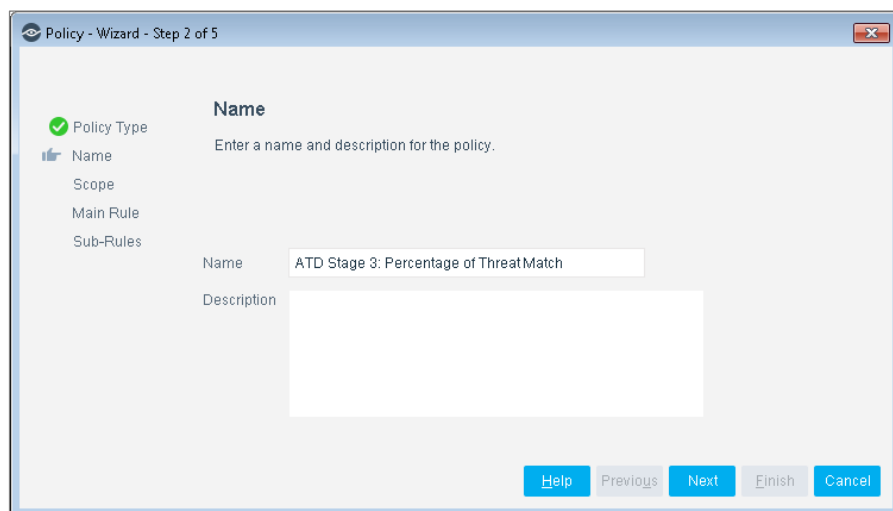
This section describes how to create a policy from the policy template.

To create a Threat Match policy:


1. Log in to the Console and select **Policy**.
2. Select **Add** from the Policy Manager. The Policy Wizard opens.
3. Expand the **Advanced Threat Detection** folder and select **ATD Stage 3: Percentage of Threat Match**.

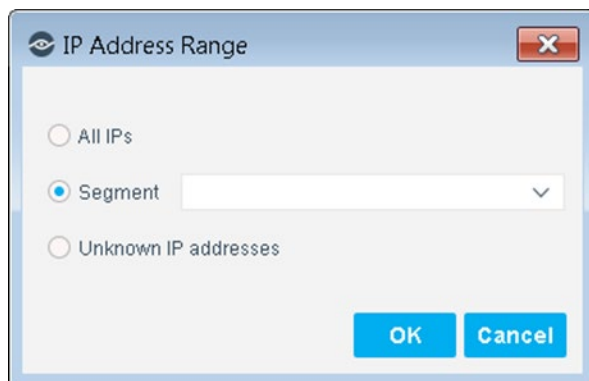


4. Select **Next**.



5. Define a unique name for the policy you are creating based on this template, and enter a description.
 - Make sure names are accurate and clearly reflect what the policy does. For example, do not use a generic name such as `My_Compliance_Policy`.
 - Use a descriptive name that indicates what your policy is verifying and which actions will be run.
 - Ensure that the name indicates whether the policy criteria must be met or not met.
 - Avoid having another policy with a similar name.

 *Policy names are displayed in the Policy Manager, the Views pane, Reports and in other features. Precise names make working with policies and reports more efficient.*
6. Select **Next**. Both the Scope pane and the IP Address Range dialog box open.
7. Use the IP Address Range dialog box to define which endpoints are inspected.



The following options are available:

- **All IPs**: Include all IP addresses in the Internal Network.
 - **Segment**: Select a previously defined segment of the network. To specify multiple segments, select **OK** or **Cancel** to close this dialog box, and select **Segments** from the Scope pane.
 - **Unknown IP addresses**: Apply the policy to endpoints whose IP addresses are not known. Endpoint detection is based on the endpoint MAC address.
8. Select **OK**. The added range is displayed in the Scope pane.
 9. Select **Next**. The Main Rule pane opens.
- The main rule of this policy detects endpoints on which any IOC was detected on a Windows machine.

Policy - Wizard - Step 4 of 5

☒ Policy Type
☒ Name
☒ Scope
☒ Main Rule
☐ Sub-Rules

Main Rule

Use this screen to review policy sub-rule definitions.
 Hosts are inspected by each sub-rule in the order shown. When a match is found, the action defined is applied. If no match is found, the host is inspected against the next sub-rule.

Condition

A host matches this rule if it meets the following condition:

All criteria are True

Criteria
IOCs Detected by CounterACT - Threat Name: Any Value Detection Time NOT: Older than...

Add Edit Remove

Actions

Actions are applied to hosts matching the above condition.

Enable	Action	Details
No items to display		

Add Edit Remove

Help Previous Next Finish Cancel

10.Select **Next**. The Sub-Rules pane opens.

11.Review the sub-rule conditions and actions. See [Sub-Rules](#) for details.

12.Select **Finish** to create the policy.

13.In the Console, select **Apply** to save the policy.

Sub-Rules

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

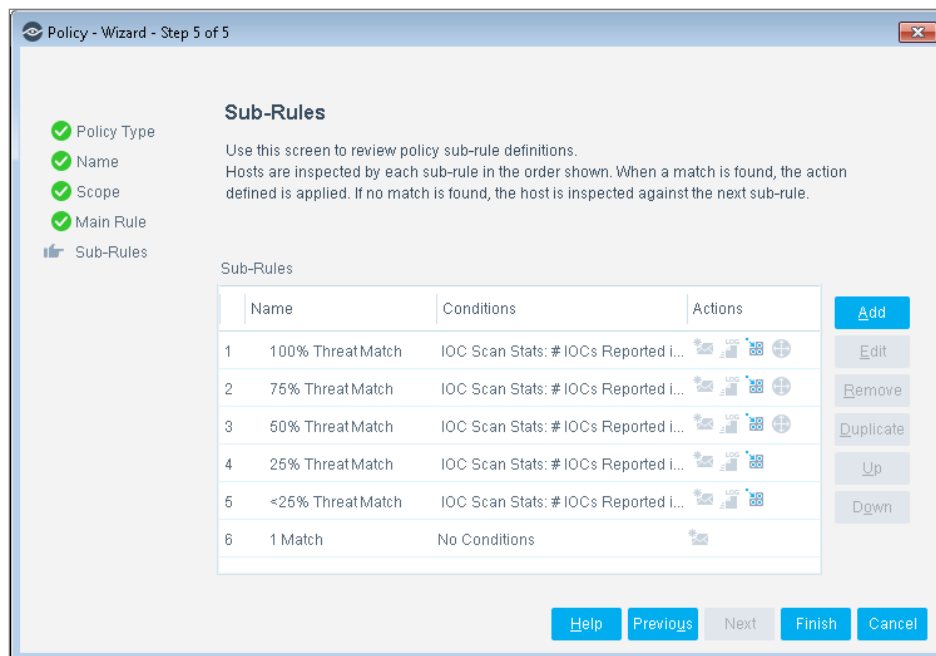
Sub-rules let you automatically follow up with hosts after initial detection and handling. Creating sub-rules lets you streamline separate detection and actions into one automated sequence.

Sub-rules are performed in order until a match is found. When a match is found, the policy sends a notification to the administrator. In addition, an action can be used to log the event to syslog, add endpoints with multiple IOCs detected to a group, and quarantine an endpoint. This action is disabled by default. If the endpoint does not match the requirements of the sub-rule, the next rule is examined.

The sub-rules of this policy sort endpoints by the percent of IOCs matched in a threat:

- 100% Match
- 75% Match

- 50% Match
- 25% Match
- <25% Match
- 1 Match



ATD Specific IOCs Detected Policy Template

Modify this policy template to identify endpoints within the policy scope on which specific IOC details were detected.

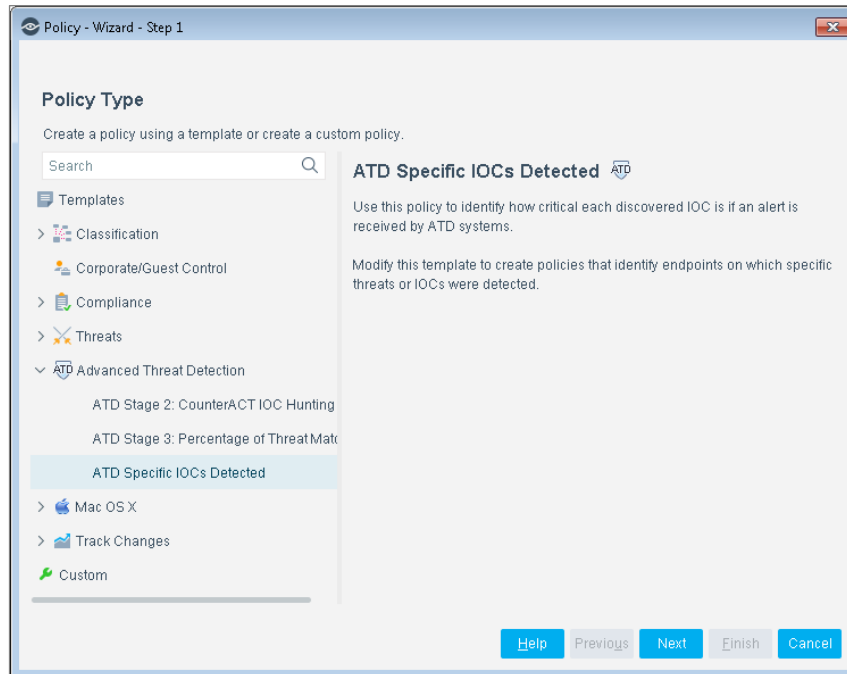
You can add actions to sub-rules. For example, notify the user by email if a specific threat name is detected, or assign the endpoint to a VLAN if a Process IOC is detected.

Create a ATD Specific IOCs Detected Policy

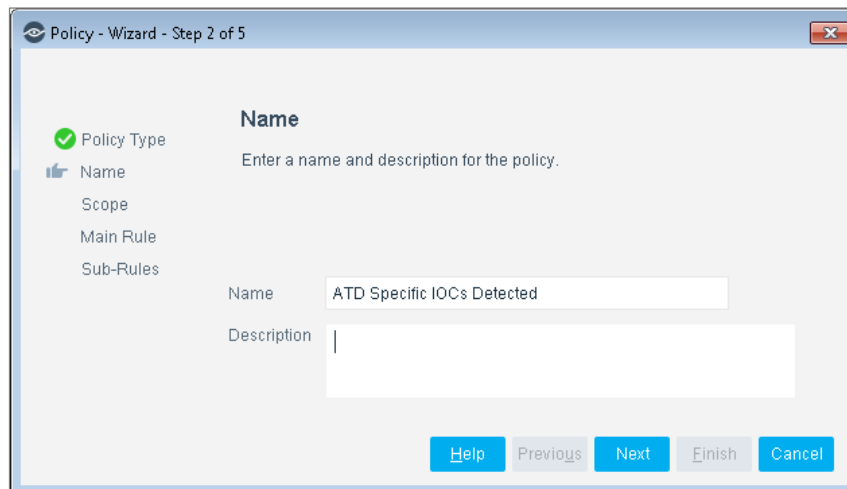
This section describes how to create a policy from the ATD Specific IOCs Detected policy template.

To create the policy:


1. Log in to the Console and select **Policy**.
2. Select **Add** from the Policy Manager. The Policy Wizard opens.
3. Expand the **Advanced Threat Detection** folder and select **ATD Specific IOCs Detected**.



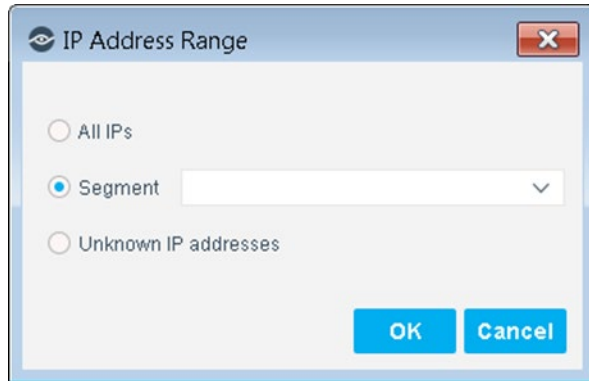
4. Select **Next.**



- 5. Define a unique name for the policy you are creating based on this template, and enter a description.**
- Make sure names are accurate and clearly reflect what the policy does. For example, do not use a generic name such as My_Compliance_Policy.
 - Use a descriptive name that indicates what your policy is verifying and which actions will be run.
 - Ensure that the name indicates whether the policy criteria must be met or not met.
 - Avoid having another policy with a similar name.

 *Policy names are displayed in the Policy Manager, the Views pane, Reports and in other features. Precise names make working with policies and reports more efficient.*

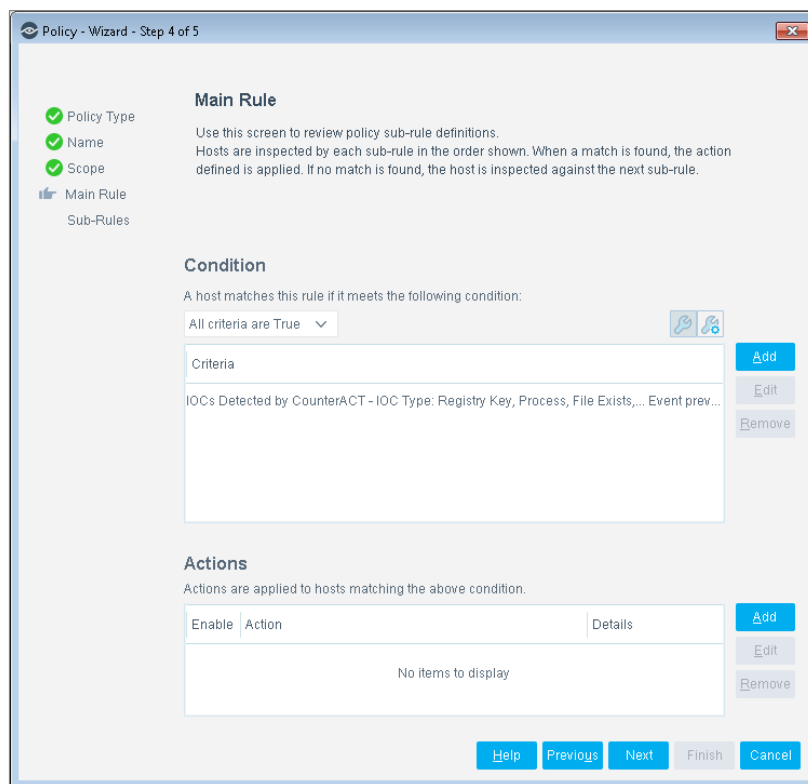
6. Select **Next**. Both the Scope pane and the IP Address Range dialog box open.
7. Use the IP Address Range dialog box to define which endpoints are inspected.



The following options are available:

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

The main rule of this policy detects endpoints on which any threat was detected.



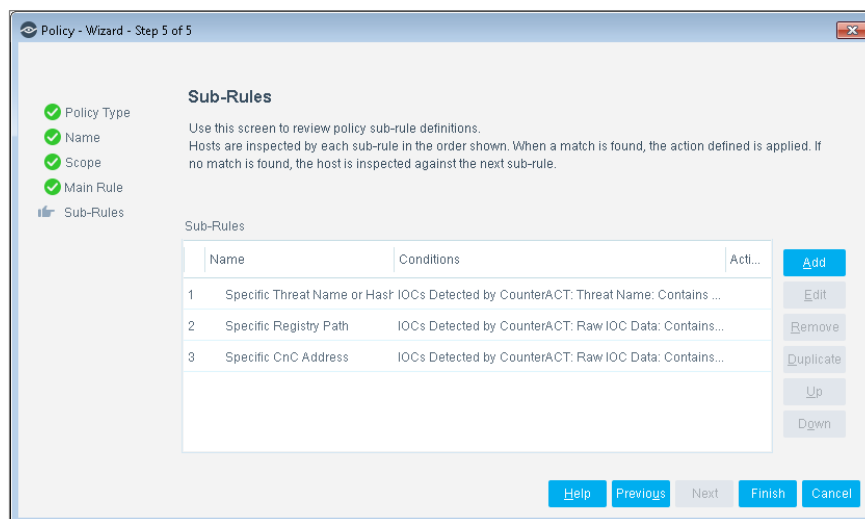
10. Select **Next**. The Sub-Rules pane opens.
11. The sub-rules in this policy template contain sample data. Edit the required sub-rules and remove any unnecessary sub-rules. See [Sub-Rules](#) for details.
12. Select **Finish**.
13. Select **Apply** to save the policy.

Sub-Rules

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

Sub-rules let you automatically follow up with hosts after initial detection and handling. Creating sub-rules lets you streamline separate detection and actions into one automated sequence.

Sub-rules are performed in order until a match is found. When a match is found, the corresponding action is applied to the endpoint. If the endpoint does not match the requirements of the sub-rule, the next rule is examined.



The sub-rules in this policy template contain sample data. Edit or remove each sub-rule to comply with your corporate requirements.

For each required sub-rule:

1. Select the sub-rule and select **Edit**.
2. In the Condition area, select each criterion and select **Edit**.
3. Change the string containing the brackets <> and optionally change other settings to comply with your corporate requirements.

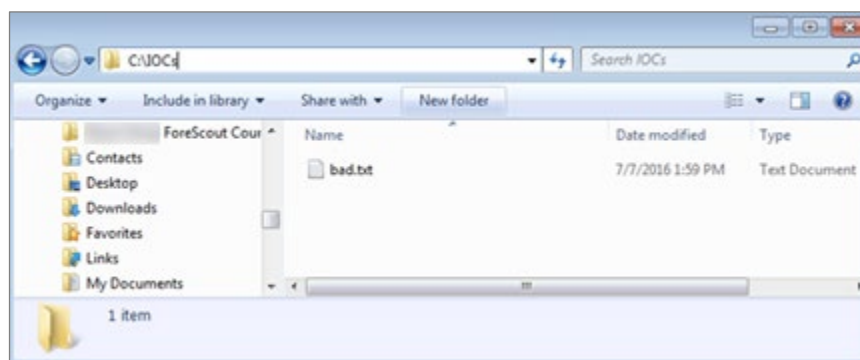
Remove sub-rules not required.

Test the IOC Scanner Policy Workflows

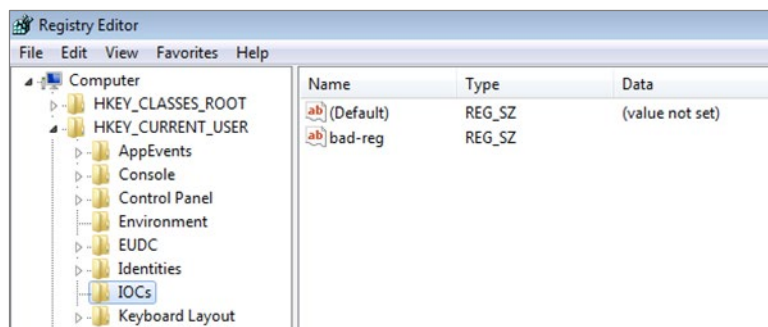
You can test the IOC Scanner policy workflow.

To test the workflow:

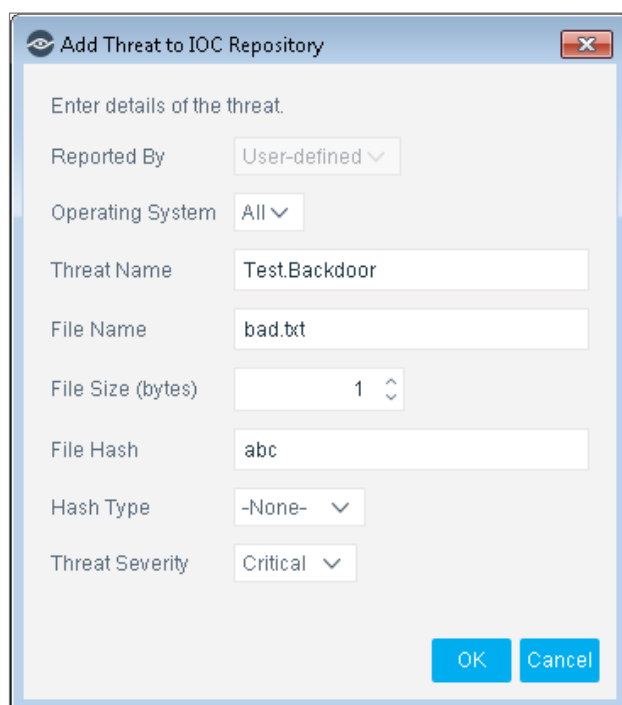
1. Create a dummy observable on a managed Windows host in the path `c:\ioc\` and name it `bad.txt`.



2. Create a fake registry entry in the path `HKEY_CURRENT_USER\IOCs` and name the key string: `bad-reg`:

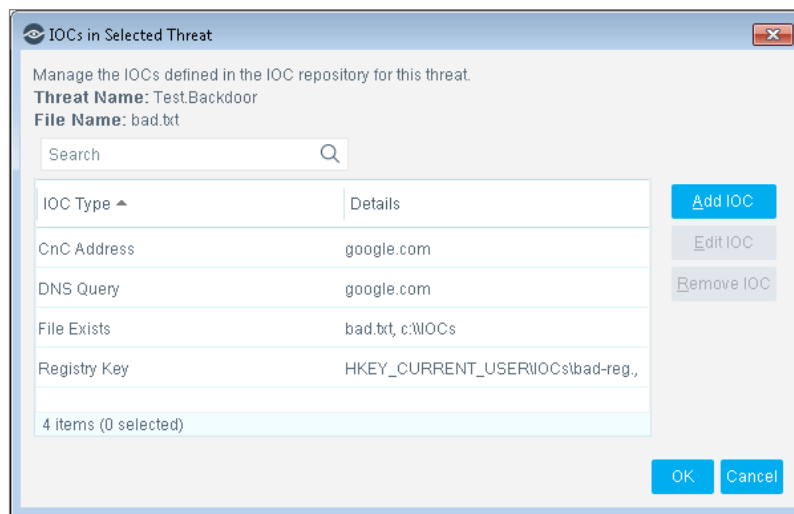


3. Create a fake threat:
 - a. Go to **Options** and select **IOC Scanner**.
 - b. In the IOC Scanner pane, select the IOC Repository tab.
 - c. Select **Add**.

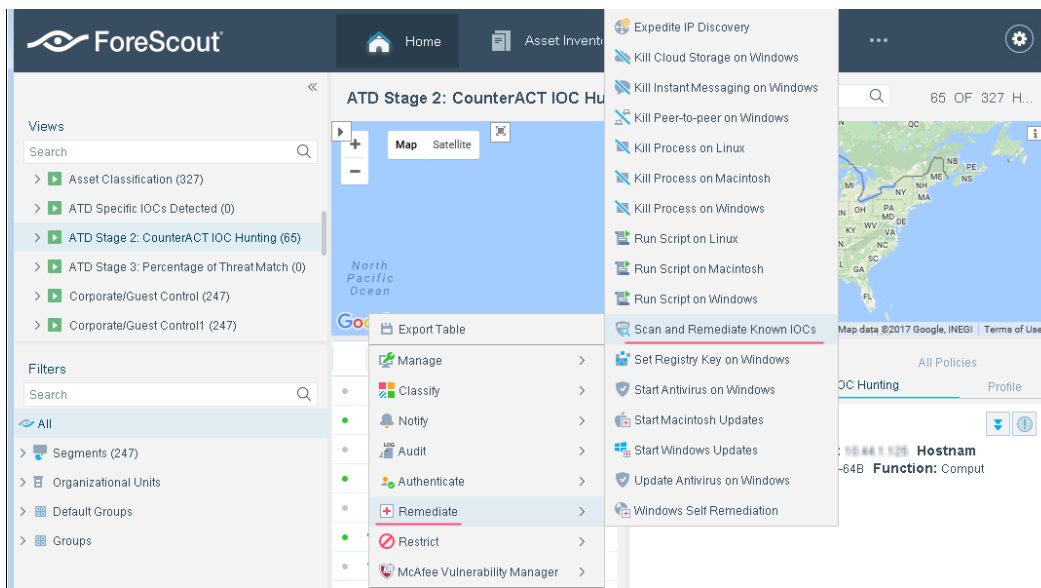


4. Create a fake threat with the following details:
 - Name: **Test.Backdoor**
 - File Name: **bad.txt**
 - File Size: **1**
 - File Hash: **abc (optionally add real MD5 or SHA hash)**
 - Hash Type: **-None-**
 - Threat Severity: **Critical**

5. Select **OK**.
6. Create fake IOCs:
 - a. In the IOC Scanner pane, IOC Repository tab, select the **Test.Backdoor** Threat and then select **IOCs**.
 - b. The IOCs in Selected Threat dialog box opens. Select **Add IOC**.
 - c. Create the following IOCs:
 - File: **bad.txt**
 - Registry Key: **bad-reg**
 - CnC Address: **google.com**
 - DNS Query: **google.com**



7. Select **OK**. In the IOC Scanner pane, select **Apply**.
8. On the endpoint where the IOCs were created, open an internet browser and go to google.com.
9. In the Console, locate the test host, right-click **Remediate** then select **Scan and Remediate Known IOCs**. This launches Stage 2 of the workflow and proceeds through Stage 3.



Create Custom IOC Scanner Policies

Custom policy tools provide an extensive range of options for detecting and handling endpoints. Specifically, you can use the policy to instruct the Forescout platform to apply a policy action to endpoints that do or do not match property values defined in policy conditions.

Properties

Policy properties let you instruct the Forescout platform to detect hosts with specific attributes. For example, create a policy that instructs the Forescout platform to detect hosts running a certain Operating System or having a certain application installed.

Actions

Policy actions let you instruct the Forescout platform how to control detected devices. For example, assign a detected device to an isolated VLAN or send the device user or IT team an email.

You may need to create a custom policy to deal with issues not covered in the IOC Scanner policy templates.

In addition to the bundled Forescout properties and actions available for detecting and handling endpoints, you can work with IOC Scanner related properties and actions to create the custom policies.

For more information about working with policies, select **Help** in the Policy Wizard.

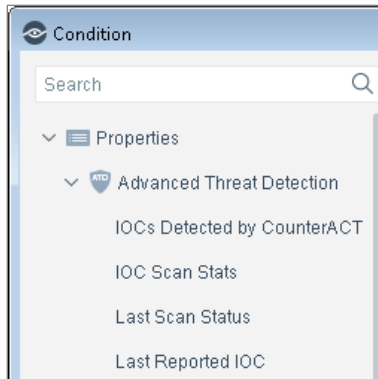
To create a custom policy:

1. Log in to the Console and select **Policy**. The Policy Manager opens.

2. Select **Add** to create a policy.

Detect IOCs – Policy Properties

Policy properties are available when the IOC Scanner Plugin is installed.



To access properties:

1. Go to the Properties tree from the Policy Condition dialog box.
2. Expand the **Advanced Threat Detection** folder in the Properties tree. The following properties are available:
 - [IOC Scan Stats](#)
 - [IOCs Detected by CounterACT](#)
 - [Last Reported IOC](#)
 - [Last Scan Status](#)

IOC Scan Stats

IOC Scan Stats is a composite property that detects the count and percentage statistics of IOCs found during endpoint scans for a selected threat. You can use these statistics to determine the likelihood of the endpoint being compromised by a threat of interest.

When an endpoint is scanned for a threat, the IOC Scanner Plugin calculates:

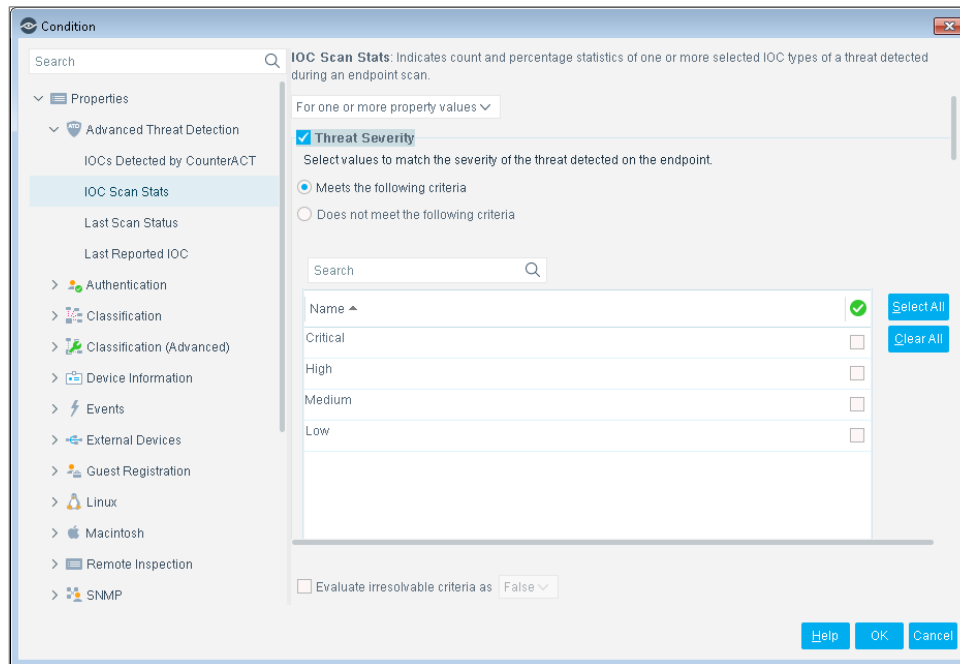
- How many IOCs of each IOC type were detected on the endpoint
- The relationship of the number of detected IOCs to the number of IOCs reported for the threat

See [Sample Statistics Scenario](#) for details.

Only the following IOC types are included in the statistics:

- CnC Address
- DNS Query
- IOCs selected in the [Scan and Remediate Known IOCs](#) action

In addition to working with the property in policies, you can use the Asset Inventory view to see the scan result statistics for each threat. See [Display Inventory Information](#) for more information.



IOC Scan Stats Properties

Threat Severity	The severity (Low, Medium, High or Critical) of the threat whose IOC counts and statistics are required.
IOC Type	Each IOC type to be considered for these statistics. <i>Total of All Types</i> includes all IOCs of all types.
# IOCs Detected of Threat	The number of IOCs of the selected IOC type detected on this endpoint for the selected threat.
# IOCs Reported in Threat	The number of IOCs of the selected IOC type defined in the IOC repository for the selected threat.
% IOCs Detected of Same Type in Threat	Percent of detected IOCs of the selected type out of all IOCs of the same type defined for the selected threat.
% IOCs Detected of All Types in Threat	Percent of detected IOCs of the selected type out of all IOCs of all types defined for the selected threat.
Threat Name	Name of the threat whose IOC counts and statistics are required.
Threat Reported By	The threat intelligence system that reported the threat containing the detected IOC.

Sample Statistics Scenario

In this example, endpoint 1.2.3.4 is scanned for all IOC types in the threat named XYZ.

IOC Type	# IOCs Reported in Threat	# IOCs Detected of Threat	% IOCs Detected of Same Type in Threat	% IOCs Detected of All Types in Threat
CnC Address	4	0	0	0
DNS Query	0	0	0	0
File Exists	4	3	75 (%)	15 (%)
Mutex	0	0	0	0
Process	4	1	25 (%)	5 (%)
Registry Key	4	4	100 (%)	20 (%)
Service	4	2	50 (%)	10 (%)
Total IOCs	20	10	50 (%)	50 (%)

Four scan result statistics values are calculated for each IOC type.

- *# IOCs Reported in Threat*: The threat intelligence system reported that Threat XYZ has four IOCs of each of the following types: Process, Service, File Exists, Registry Key and CnC Address. The total number of IOCs reported is 20.
- *# IOCs Detected of Threat*: Of the IOCs defined in Threat XYZ, the scan detected one Process IOC, two Service IOCs, three File Exists IOCs, and four Registry Key IOCs. The total number of IOCs detected is 10.
- *% IOCs Detected of Same Type in Threat*: For each IOC type, the percent is calculated of $\# \text{ IOCs Detected of Threat} / \# \text{ IOCs Reported in Threat}$.
- *% IOCs Detected of All Types in Threat*: For each IOC type, the percent is calculated of $\# \text{ IOCs Detected of Threat} / \# \text{ Total IOCs Reported in Threat}$.

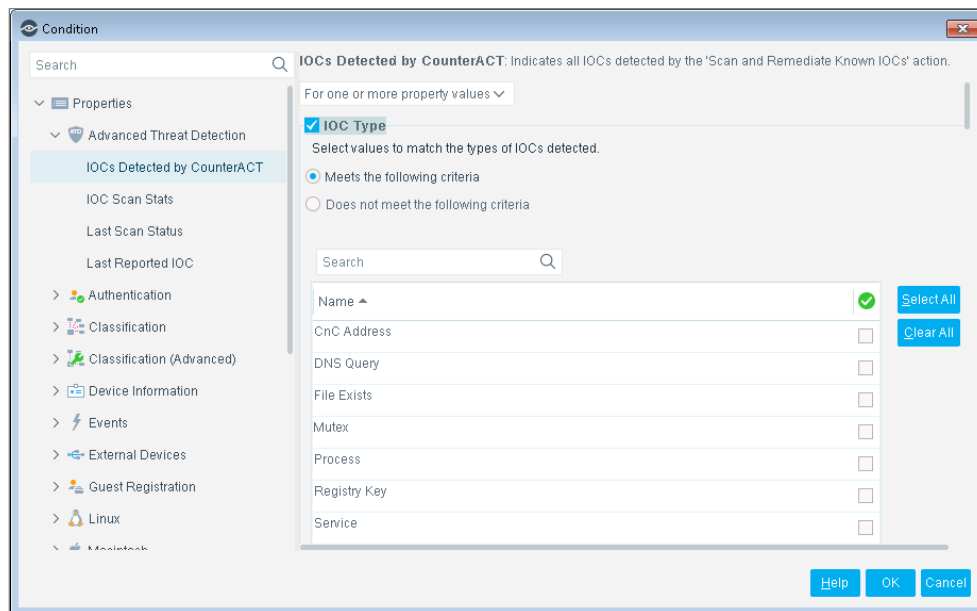
Sample Property Values

If IOC type *Service* and Threat Name *XYZ* are selected in the IOC Scan Stats property, the values to match for the *Service* IOC types are shown on the second row of the [Sample Statistics Scenario](#) table.

- *# IOCs Reported in Threat*: 4
- *# IOCs Detected of Threat*: 2
- *% IOCs Detected of Same Type in Threat*: 50
- *% IOCs Detected of All Types in Threat*: 10

IOCs Detected by CounterACT

This composite property lists all network-based IOCs and all IOCs discovered by the [Scan and Remediate Known IOCs](#) action for a particular endpoint.



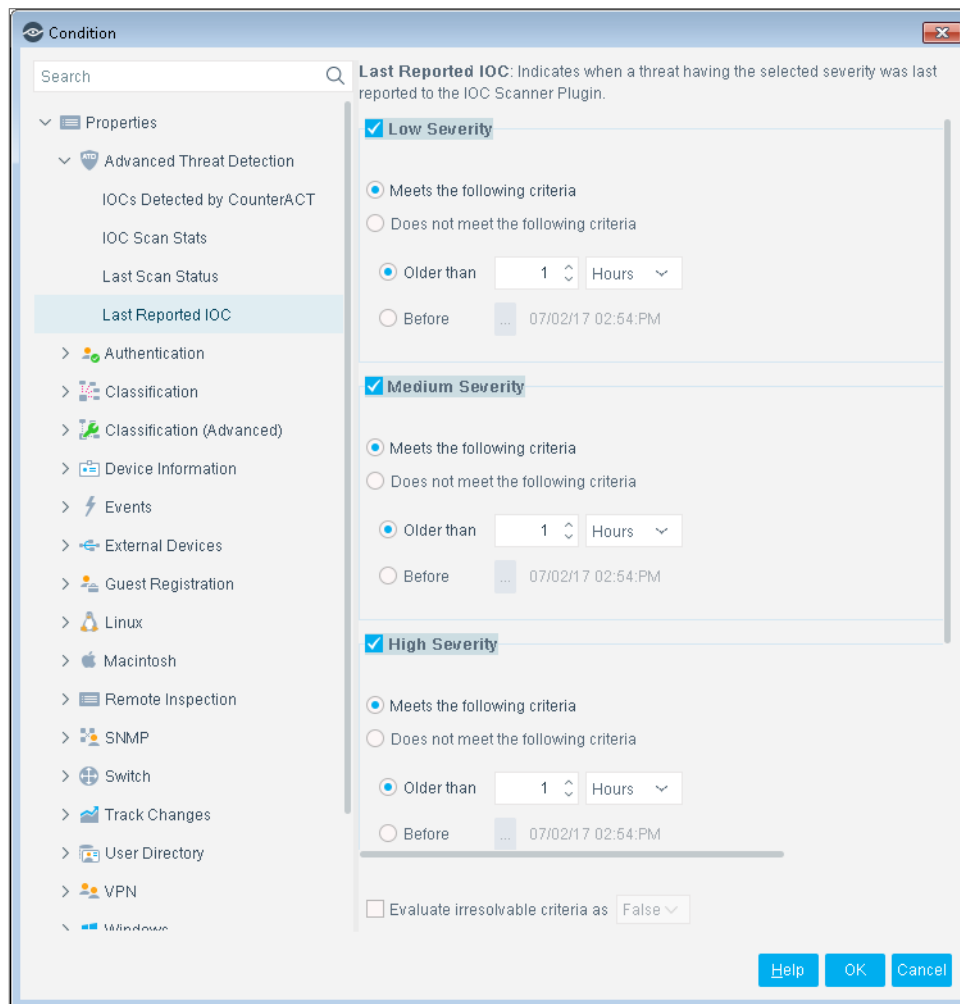
IOCs Detected by CounterACT Properties

IOC Type	The type of IOC detected.
Raw IOC Data	The IOC details reported by the threat intelligence system.
Threat Severity	The severity level of the threat (Low, Medium, High, or Critical).
Threat Name	The name of the threat containing the detected IOC.
Threat File Name	The file name of the detected threat.
Threat File Hash	The file hash of the detected threat.
Threat Hash Type	The hash algorithm of the threat file hash (MD5, SHA-1, or SHA-256).
Threat Reported By	The threat intelligence system that reported the threat.
Operating System	The operating system (OS) for which the threat intelligence system reported the threat.
Detection Time	The time period in which the IOC was detected.

Last Reported IOC

Use the date of the newest threat received by the IOC Scanner Plugin as a policy property to trigger endpoint scans. This property indicates when a threat having the selected severity (Low, Medium, High or Critical) was last reported to the IOC Scanner Plugin from any threat intelligence system on any endpoint in the Forescout network.

Any threat received by the plugin, regardless of the source, causes this property to be updated on all endpoints. Unlike most Forescout properties, the value of this property is the same for all endpoints.



You can use this property in policies to trigger the [Scan and Remediate Known IOCs](#) action on endpoints when new threats are reported by a threat intelligence system. However, if several threats are reported within a short time, it may be inefficient to scan all endpoints each time a new threat is received.

It is recommended to create policies that trigger endpoint scans if the following two conditions are met:

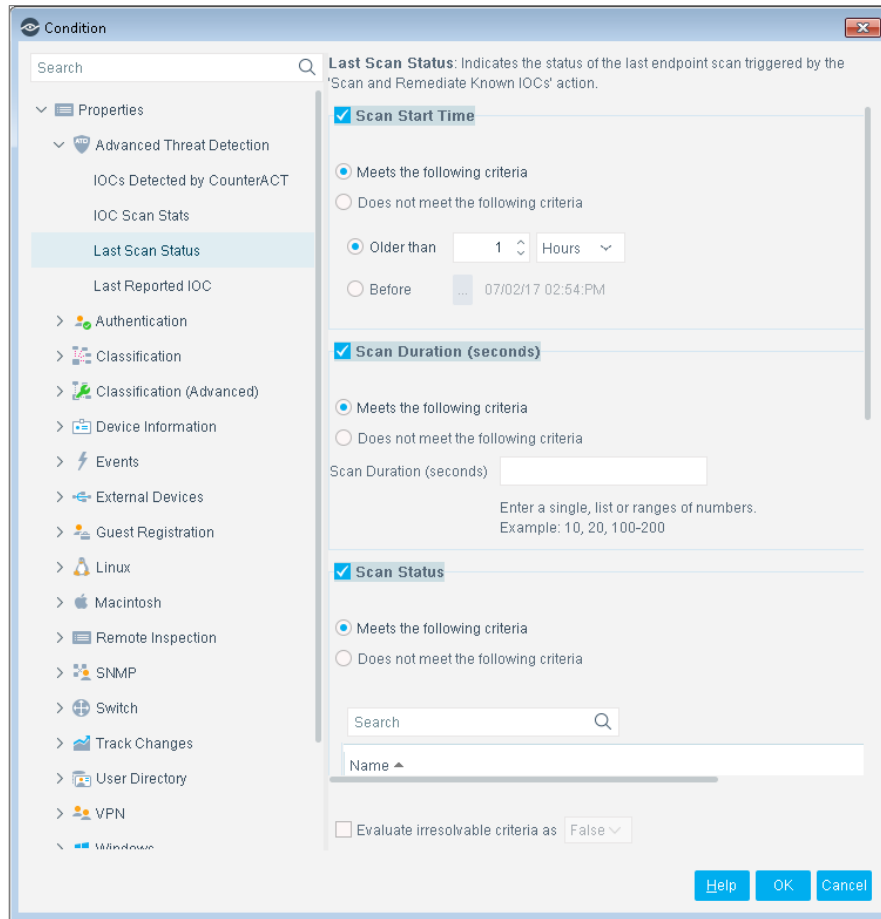
- A threat was reported after the last scan was run.
- A certain period of time has passed since the last scan was run.

All threats reported after last scan was run will be detected in the next scan.

Last Scan Status

This property displays the status of the last [Scan and Remediate Known IOCs](#) action performed on the endpoint.

As soon as a [Scan and Remediate Known IOCs](#) action begins to run, this property's **Scan Start Date** and **Scan Status** fields are populated. The remaining property values are populated upon scan completion.



Last Scan Status Properties

Scan Start Date	The time when the scan started.
Scan Duration (seconds)	The length of time the scan ran, in seconds.
Scan Status	The current status of the scan: <ul style="list-style-type: none"> Failed to run Finished Finished with errors Never scanned No threat exists for selected filters Running
Scan Errors	Errors reported if the scan failed.

Scan Endpoints – Policy Actions

Policy actions let you instruct the Forescout platform how to control detected devices. For example, assign potentially compromised endpoints to an isolated VLAN, or notify the endpoint user or IT team.

In addition to the bundled Forescout actions available for handling endpoints, you can work with the plugin related actions to create custom policies. These actions are available when the plugin is installed.

The following actions are available:

- [Scan and Remediate Known IOCs](#)
- [Add Threat Exception](#)

Scan and Remediate Known IOCs

Network-based threat intelligence systems might not have full visibility of the network, and agent-based systems might not be installed on all endpoints. The IOC Scanner Plugin fills in these gaps by using the data obtained from various threat intelligence systems to scan Windows endpoints discovered and managed by the Forescout platform.

If you are using Flexx licensing, ensure that you have a valid Forescout eyeControl license to use these actions. Refer to the *Forescout Flexx Licensing How-to Guide* for more information about managing licenses.

Use the Scan and Remediate Known IOCs action to scan Windows endpoints for IOCs reported by threat intelligence systems to your IOC repository. Determining which endpoints to scan may depend on the type of installed threat intelligence system, the severity of the threat or other business considerations.

You may want to scan:

- Endpoints on which a threat intelligence system agent is not installed.
- Endpoints on which a threat intelligence system agent cannot be installed.
- Endpoints that are not otherwise covered by a threat intelligence system.

If a threat intelligence system reports a malicious file on an endpoint, you may want to immediately initiate a scan on other endpoints (either a group, or all endpoints) for the reported IOC. Use Advanced Threat Detection properties as policy conditions to trigger the Scan and Remediate Known IOCs action on a given endpoint or on all endpoints when new IOCs are reported.

You can perform scans of varying intensities depending on the severity of the threat. For example, you can perform a scan for all IOCs of a threat with a severity level of High or Critical only.

Scanning involves finding the relevant files and checking their details, such as file hash values, against all IOC details currently listed for the selected threats in the IOC repository. For example, scanning for a threat's *Service* IOCs means checking:


- The hash of the executable behind each of the endpoint's system services
- The hash of each executable set to run on the endpoint at start-up by any user

To enable the list of IOC details used during the scan, ensure that the endpoints scanned by this action can connect back to their managed CounterACT® Appliance using HTTP (port 80/TCP).

The Scan and Remediate Known IOCs action:

- Scans endpoints within the selected scope only.

- Scans only for threats that were reported for all Operating Systems or for the specific OS running on the endpoint.
- Scans for IOCs of selected types defined in threats that:
 - Match the selected filters.
 - Are not in the Threat Exceptions list for that endpoint. See [Add Threat Exception](#).

 *CnC Address and DNS Query IOCs of threats not in the Threat Exceptions list are always detected.*

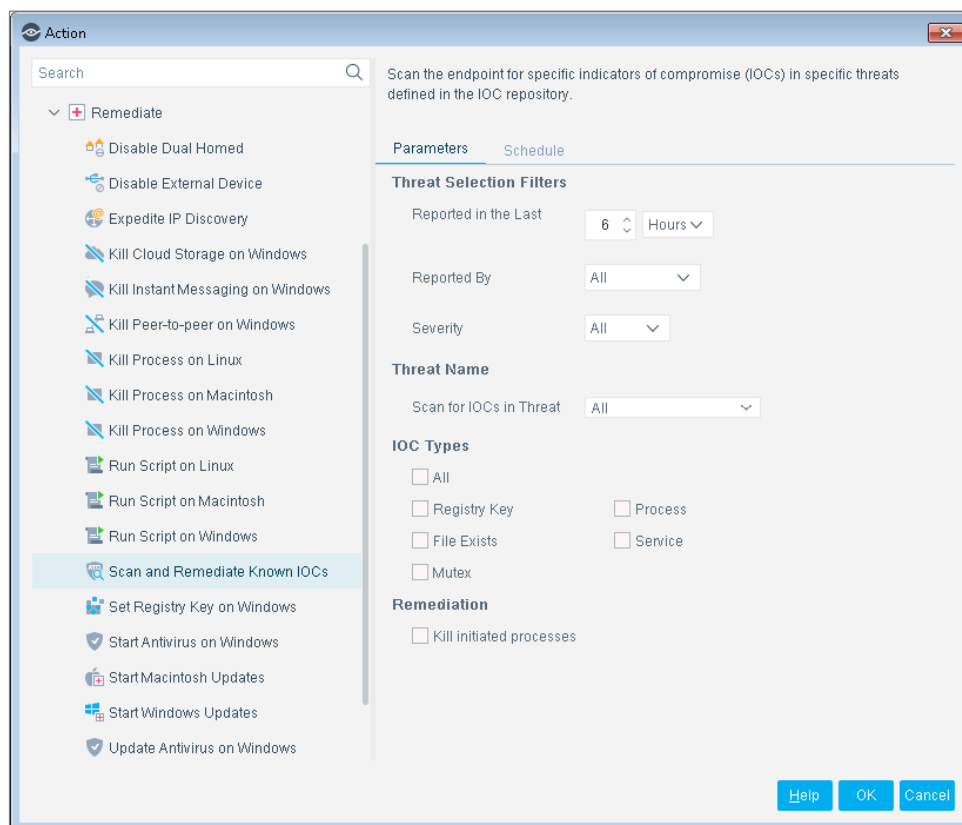
The action also offers the following immediate remediation:

- Kill processes initiated by IOCs detected during the scan.

Use this option with caution to avoid terminating legitimate processes.

To access this action:

1. Go to the Actions tree from the Policy Action dialog box.
2. Expand the **Remediate** folder in the Actions tree, and select **Scan and Remediate Known IOCs**.



Scan and Remediate Known IOCs Properties

Threat Selection Filters	Scan for IOCs defined in threats within the selected filters only. The subset of threats that match the filters is dynamically determined each time the action is run.
Threat Name	Scan for IOCs defined in the selected threat or threats that meet the Threat Selection Filters. Each threat name is followed by the threat file hash.
IOC Types	Scan for the selected IOC types only. See View Threat IOCs . Note: The action always scans the network session for CnC Address and DNS Query IOCs.
Remediation: Kill initiated processes	If an IOC process was initiated on the endpoint, kill the process. <i>Use this option with caution to avoid terminating legitimate processes.</i>

Add Threat Exception

In a typical deployment, some endpoints have legitimate characteristics that match IOCs defined in your IOC repository. These legitimate indications are detected on the endpoints whenever a scan is run. If the threats and the endpoints that produce false-positive scan results are known, the operator can run an action that:

- Deletes the properties on the endpoint of previous scan results of the specified threat.
- Excludes the specified threat in future scans of the endpoint.
- Deletes a threat permanently so that no endpoint is scanned for it.

The Threat Exceptions tab contains the list of threats that are to be ignored on scans of specific endpoints. See [Manage Threat Exceptions](#).

The IOC Subscribers tab lists all the subscribers that receive IOC notifications. See [IOC Subscribers](#).

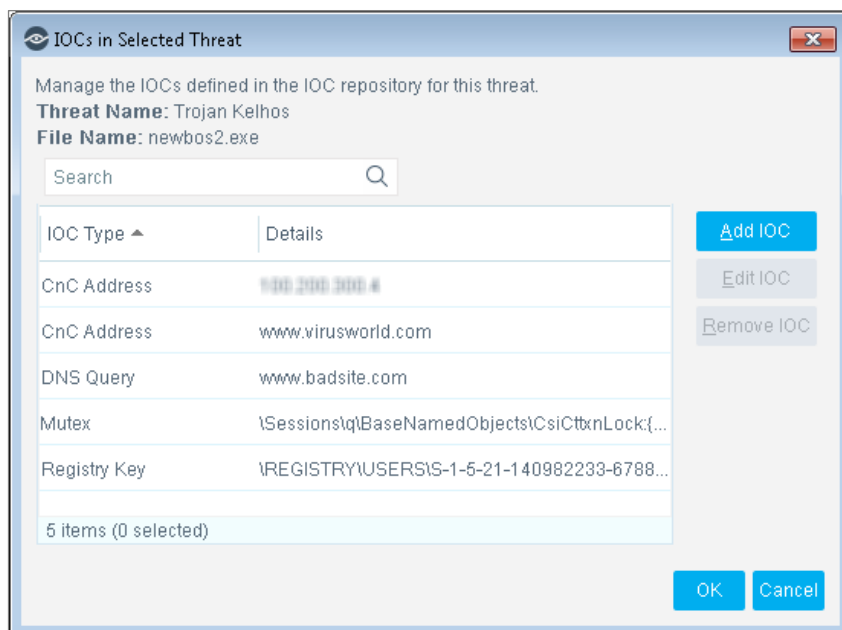
Manually Add an IOC to a Threat

You can manually add IOCs to an existing threat in the IOC repository.

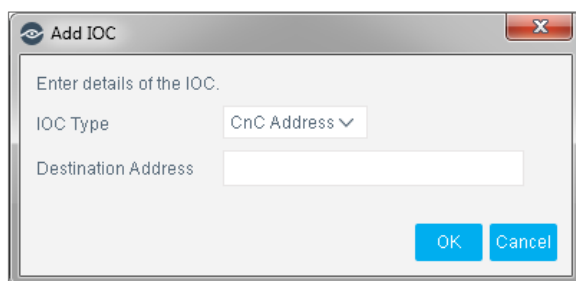
When adding user-defined IOCs, you first need to define the threat. See [Manually Add a Threat to the Repository](#).

To manually add an IOC to a threat:

1. In the IOC Scanner, IOC Repository tab, select the required threat, and then select **IOCs**.



2. Select **Add IOC.**



- 3.** Enter the details of the threat. For definitions of the IOC Types, see [View Threat IOCs](#).
- 4.** Select **OK**.
- 5.** To add another IOC to the threat, repeat steps [2](#) to [4](#).
- 6.** When all the IOCs have been added to the threat, select **OK** in the IOCs in Selected Threat dialog box.

You can also [Remove Threats from the Repository](#).

Remove Threats from the Threat Exception Repository

Threats and their IOCs remain in the IOC repository until:

- They are manually removed.
- A maximum number of 128 threats is reached.

Manually Remove Threat Exception Data

You can manually remove individual threats from the Threat Exceptions repository so that endpoints are no longer scanned for specific threats.

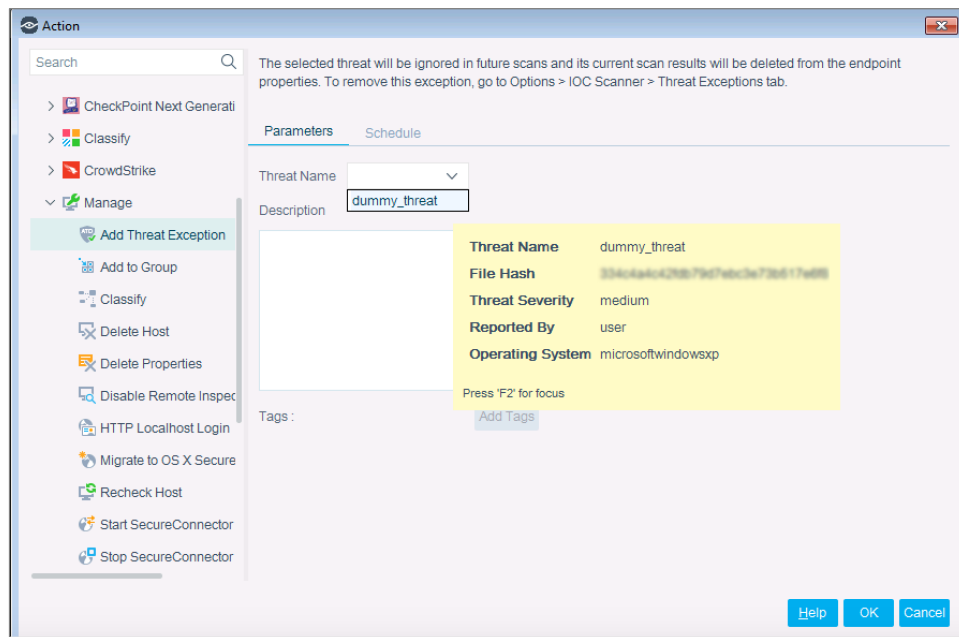
To manually remove a threat:

1. In the IOC Scanner pane, Threat Exceptions tab, select one or more threats to be removed.
2. Select **Remove**, and select **Apply**.

Use Advanced Threat Detection properties as policy conditions to trigger the Add Threat Exception action on a given endpoint or on all endpoints.

To access this action:

1. Go to the Actions tree from the Policy Action dialog box.
2. Expand the **Manage** folder in the Actions tree, and select **Add Threat Exception**.



Add Threat Exception Properties

Threat Name	<p>Select a threat to be ignored in future scans and whose current scan results will be deleted from the endpoint properties. Once the Threat Name is selected and the Parameters tab is saved, the Threat Severity and Threat Identifier are displayed when the user holds the cursor over the Threat Name. The following information is displayed:</p> <ul style="list-style-type: none"> Threat Name Threat Severity Threat Identifier that consists of: <ul style="list-style-type: none"> the threat file hash an internal code for the reporting threat intelligence system an internal reference to the OS for which the threat was reported <p>To remove the threat exception, you must select the same Threat Identifier value in the IOC Scanner, Threat Exceptions tab.</p>
Description	(Optional) Enter a textual description of the exception or a relevant comment.
Tags	To insert endpoint property values in a field, place the cursor in the appropriate field, select Tags and select the appropriate tags.

You can use the IOC Scanner, Threat Exceptions tab to remove this action for a threat. See [Manage Threat Exceptions](#).

Display Inventory Information

Use the Forescout Asset Inventory to view a real-time display of IOC Scanner threat network activity at multiple levels, such as threat names, file names, and severity levels.

The Asset Inventory lets you:

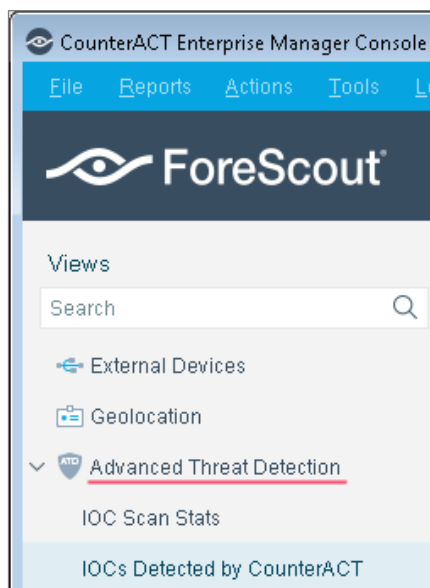
- Broaden your view of the organizational network from device-specific to activity-specific
- View threats and IOCs that have been detected with specific attributes
- Easily track threat activity
- Incorporate inventory detections into policies

The following information, based on plugin related host properties, is available:

- IOC Scan Stats
- IOCs Detected by CounterACT

To access the inventory:

1. In the Console, select **Asset Inventory**.
2. Go to the **Advanced Threat Detection** entries.



Refer to *Working at the Console > Working with Inventory Detections* in the *ForeScout Administration Guide* or the Online Help for information about how to work with the ForeScout Asset Inventory.

Appendix: The DNS Query Extension

The DNS Query Extension detects and parses DNS messages in the network that reference specific host names. The extension does not report other DNS interactions.

The extension provides the **DNS Event** host property that reports details of intercepted DNS messages that reference specific host names of interest. See [DNS Event](#).

Configure and Test the Extension

No configuration is required to work with the extension. Only the test parameters need to be defined.

Run a test to:

- Verify that the Appliance can see DNS traffic.
- See the DNS traffic witnessed in the test time-frame (or within a packet count limit).
- Develop and verify regular expressions to use as policy conditions for the DNS Event Property.

Running a test does not let you:

- See values in the properties (DNS Event, Is DNS Server).

To configure and test the extension:

1. In the Console, select **Options** from the **Tools** menu, and go to the Modules pane.
2. Select **Core Extensions > DNS Query Extension**, and select **Appliances**. The Installed Appliances dialog box opens.
3. Select the Appliance or Enterprise Manager to be configured, and select **Configure**. The DNS Query Extension Enterprise Manager or Appliance Plugin Configuration dialog box opens.
4. Configure the following fields that are used to test the CounterACT device's connection to DNS servers it detects.

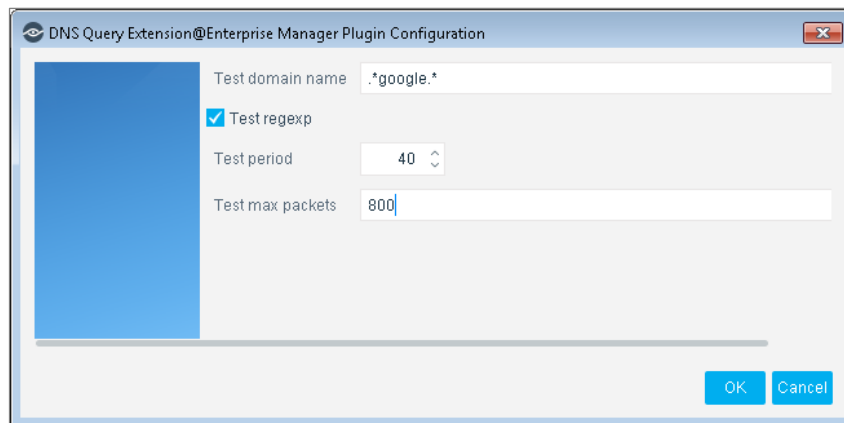
Test domain name	Indicates a domain name used in test queries sent to DNS servers.
Test regexp	Indicates whether the text in the Test domain name field should be evaluated as a regular expression.
Test period	Indicates the maximum time period of the test, in seconds.
Text max packets	Indicates the maximum number of packets that are processed during the test.

5. Select **OK** to configure the CounterACT device with the specified values.
6. Repeat this procedure to configure other CounterACT devices.
7. Select **Test** to test the extension.

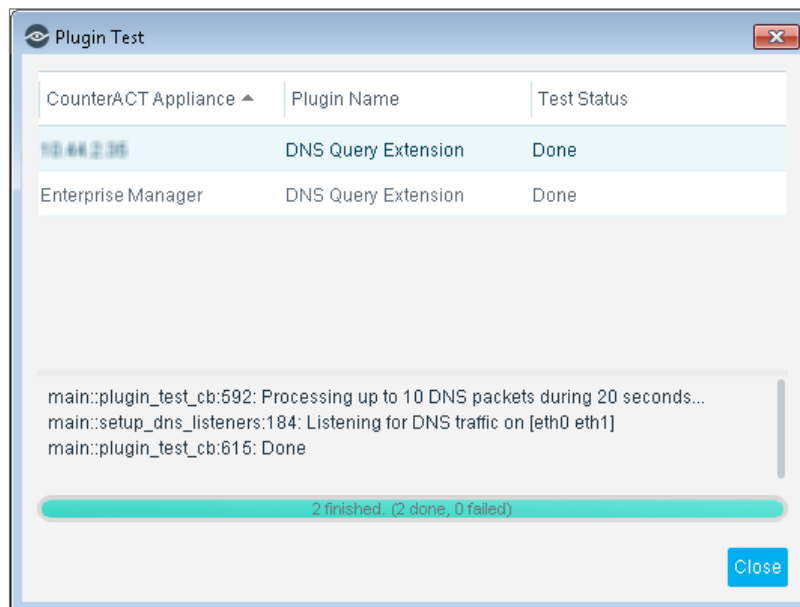
Sample Test

This sample test runs a traffic sniffer (pcap) for a maximum of 40 seconds or until the packet count is reached.

- Test domain name: **.*google.***
- Test regexp: **(Checked)**
- Test period: **40**
- Test max packets: **800**



While capturing, it displays the packets that matched the exact name unless “regex” was selected, in which case it prints all those that constitute a regular expression.



As an example and to generate traffic, open an internet browser and go to ***drive.google.com*** or ***mail.google.com*** on a computer connected to a Forescout monitored network.

The output is as follows:

```
Processing up to 800 DNS packets during 40 seconds...

Listening for DNS traffic on [eth0 eth1]

Name=drive.google.com Type=A Client= endpoint-ip Server= dns-server-ip Response=0
Answers=

<...etc...>

Name=drive.google.com Type=A Client=<client ip> Server=<server ip> Response=1
Answers=drive.google.com. 8 IN A 216.58.210.14.

Name=googlemail.1.google.com Type=A Client=<Endpoint ip> Server=<DNS server ip>
Response=1 Answers=googlemail.1.google.com. 117 IN A 216.58.208.37.

Name=googlemail.1.google.com Type=A Client=<Endpoint ip> Server=<DNS server ip>
Response=1 Answers=googlemail.1.google.com. 117 IN A 216.58.208.37.

Name=drive.google.com Type=A Client=<Endpoint ip> Server=<DNS server ip>
Response=0 Answers=

Name=drive.google.com Type=A Client=<Endpoint ip> Server=<DNS server ip>
Response=0 Answers=

Name=drive.google.com Type=A Client=<Endpoint ip> Server=<DNS server ip>
Response=0 Answers=

Name=drive.google.com Type=A Client=<Endpoint ip> Server=<DNS server ip>
Response=1 Answers=drive.google.com. 293 IN A 216.58.201.238

Name=drive.google.com Type=A Client=<Endpoint ip> Server=<DNS server ip>
Response=1 Answers=drive.google.com. 293 IN A 216.58.201.238

Name=drive.google.com Type=A Client=<Endpoint ip> Server=<DNS server ip>
Response=1 Answers=drive.google.com. 293 IN A 216.58.201.238

Done.
```

Detect Endpoints – DNS Query Properties

This extension provides the following host properties in the Device Information folder:

- [Is a DNS Server](#)
- [DNS Event](#)

You can use these properties in custom policies. See [Create Custom IOC Scanner Policies](#).

Is a DNS Server

This Boolean property indicates if the DNS Query Extension has observed the endpoint accepting and responding to DNS queries.

DNS Event

This composite property indicates the details of DNS messages to and from the endpoint that were intercepted by the DNS Query Extension.

Only messages that reference specific host names of interest are reported. DNS monitoring of a host name is invoked in one of two ways:

- When a *DNS Query* IOC is reported to the Forescout platform, the IOC Scanner Plugin initiates DNS monitoring that detects all DNS interactions that reference the suspect host name mentioned in the IOC.
- When you create a policy condition using the **DNS Event** property provided by the extension, the Forescout platform monitors DNS traffic that matches the host name you specify.

The following information is reported for each DNS message.

DNS Name	Indicates the hostname that the DNS server is asked to resolve.
DNS Query Type	Indicates the Query Type of the DNS message. This is also known as the Request Type, Record Type, or Lookup Type.
DNS Query/Response	Indicates whether this message is the initial query or the response of the DNS Server. Valid string values are "query" and "response".
DNS Zone	In DNS response messages, contains the response message in zone file format.
DNS Address(es)	In DNS response messages, indicates the IP address(es) returned by the DNS server.
DNS Server Address	Indicates the IP address of the DNS server to which the query is addressed.
DNS Monitoring Tag	Indicates the reason that the Forescout platform monitors messaging for the specified hostname. Valid values are: <ul style="list-style-type: none"> ▪ Policy – This hostname is specified in a policy condition using this host property. ▪ ADT - Advanced Threat Detection mechanisms have identified this hostname for monitoring. Both values can be valid simultaneously for a single DNS name.

Core Extensions Module Information

The IOC Scanner plugin is installed with the Forescout Core Extensions Module.

The Forescout Core Extensions Module provides an extensive range of capabilities that enhance the core Forescout solution. These capabilities enhance detection, classification, reporting, troubleshooting, and more. The following components are installed with the Core Extensions Module:

Advanced Tools Plugin
CEF Plugin

Device Data Publisher
DNS Client Plugin

IoT Posture Assessment
Engine

Cloud Uploader	DNS Enforce Plugin	NBT Scanner Plugin
DHCP Classifier Plugin	DNS Query Extension Plugin	Packet Engine
Dashboards Plugin	External Classifier Plugin	Reports Plugin
Data Publisher	Flow Analyzer Plugin	Syslog Plugin
Data Receiver	Flow Collector	Technical Support Plugin
Device Classification Engine	IOC Scanner Plugin	Web Client Plugin

The Core Extensions Module is a Forescout Base Module. Base Modules are delivered with each Forescout release. Upgrading the Forescout version or performing a clean installation installs this module automatically.

Additional Forescout Documentation

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

- [Documentation Downloads](#)
- [Documentation Portal](#)
- [Forescout Help Tools](#)

Documentation Downloads

Documentation downloads can be accessed from the [Technical Documentation Page](#), and one of two Forescout portals, depending on which licensing mode your deployment is using.

- **Per-Appliance Licensing Mode** – [Product Updates Portal](#)
- **Flexx Licensing Mode** – [Customer Support Portal](#)

 *Software downloads are also available from these portals.*

To identify your licensing mode:

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

Technical Documentation Page

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

To access the Technical Documentation page:

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

Product Updates Portal

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

To access the Product Updates Portal:

- Go to <https://updates.forescout.com/support/index.php?url=counteract> and select the version you want to discover.

Customer Support Portal

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

To access documentation on the Customer Support Portal:

- Go to <https://Forescout.force.com/support/> and select **Downloads**.

Documentation Portal

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

To access the Documentation Portal:

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

Forescout Help Tools

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

Console Help Buttons

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

Forescout Administration Guide

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

Plugin Help Files

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

Content Module, eyeSegment Module, and eyeExtend Module Help Files

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

Documentation Portal

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