FORESCOUT

Forescout

Network Module: Rogue Device Detection and Prevention

How-to Guide

Version 1.0

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

Legal Notice

2019-03-05 16:52

Table of Contents

Rogue Device Detection and Prevention Solution

Overview

The Rogue Device Detection and Prevention How-to Guide, version 1.0, provides you with the information necessary to deploy the Forescout rogue device detection and prevention solution in your network. The solution addresses the following rogue device, network security problem:

- MAC Spoofing

The solution monitors Forescout platform-managed switches to identify suspicious MAC spoofing events occurring to endpoints that are connected to these switches. The solution identifies these suspicious events regardless of whether the involved endpoints - the ***spoofing victim*** (legitimate endpoint) and the ***spoofing attacker*** (illegitimate endpoint) - are located on (connected to) the same managed switch or two different, managed switches. Monitoring is continuous. The solution also provides the operator/administrator with the option to take action.

With this solution, Forescout delivers the following value to customers:

- Ensure and demonstrate security compliance
- Reduce the risk of network disruption, due to security incidents/breaches

The solution offers two different methods by which it identifies suspicious MAC spoofing events. The operator/administrator of the Forescout platform, based on their security standards, can activate the use of a single method or both methods. The detection methods are as follows:

- **Detect MAC Address Appearances on Different Ports** – per endpoint connected to a Forescout platform-managed switch, the solution monitors the MAC address appearance at its specific switch location and tracks consecutive changes in/movements of the MAC address switch location. Should a configured threshold of MAC address movements occur within a pre-defined interval, the solution identifies a MAC spoofing event.
- **Detect Changes in Character of Device** - per endpoint connected to a Forescout platform-managed switch, the solution monitors a pre-defined set of fundamental, device properties for changes in their value. Should a configured number of these properties experience a change in value within a pre-defined interval, the solution identifies a MAC spoofing event.

In addition to identifying suspicious MAC spoofing events, the Forescout solution provides:

- Properties containing event-related or action-related information
- A policy template for creating policies to handle identified MAC spoofing events
- Action control
- A Console filter that displays, as a group, the detected endpoints that have been involved in a MAC spoofing event

For Console display purposes, the Forescout platform assigns a unique, fake MAC address to every, detected spoofing attacker.

This document assumes that its readers have a solid understanding of the Forescout Switch Plugin and basic Forescout platform features including properties, policies and actions.

Requirements

The Rogue Device Detection and Prevention solution has the following deployment requirements:

Forescout

The following Forescout version must be running in your Enterprise Manager and your Appliances:

- Forescout 8.1
- (Flexx licensing) A valid Forescout eyeControl (ForeScout CounterACT Control) license, to use enforcement actions provided by the plugin/component. If you do not have this license, these actions will be disabled in the Console. Refer to the *Forescout Flexx Licensing How-to Guide* for more information about managing Flexx licenses and how to request/purchase this license.

Network Module

The following plugins and their version must be running in all your CounterACT devices:

- Rogue Device Plugin, version 1.0
- Switch Plugin, version 8.13

MAC spoofing detection requires the following:

- A minimum of one, running (active) MAC Spoofing Tracking policy or an equivalent policy that resolves the **MAC Spoofing Suspected** property.
- ***Only endpoints that fall within the policy's defined scope are subject to MAC spoofing detection***. Therefore, for each MAC Spoofing Tracking policy or equivalent policy, make sure that you define its scope with the IP segments/IP address range(s) that you require the solution to track and detect.

Core Extensions Module

The following plugin and version is ***optionally*** running in all your CounterACT devices:

- DHCP Classifier Plugin, version 2.2
  - Resolves endpoint property information that the Rogue Device Plugin uses for the **Detect Changes in Character of Device** detection method.

Endpoint Module

The following plugin and version is ***optionally*** running in all your CounterACT devices:

- HPS Inspection Engine, version 11.0
  - Resolves endpoint property information that the Rogue Device Plugin uses for the **Detect Changes in Character of Device** detection method.
  - The Rogue Device Plugin requests the HPS Inspection Engine to verify, via Nmap query, the connection status of endpoints.

Configuration

This section describes both the required and optional configuration for deploying the Rogue Device Detection and Prevention solution. This section addresses the following topics:

Rogue Device Plugin Configuration

The Rogue Device Plugin (RGDP) provides the following options for configuration:

For MAC spoofing detection to function, see MAC Spoofing Detection Requirement .

Option / Field	Description	Sub-Fields
Detect MAC Address Appearances on Different Ports	By default, this option is enabled. Enabling this detection method instructs the plugin to do the following, per endpoint connected to a SWP-managed switch: ▪ Monitor MAC address for its reported appearance at a switch location (IP address, port). ▪ Per MAC address, keep count of consecutive changes (movements) in its switch location.	**Detection Confidence** Select from among the following detection confidence level settings: ▪ *Normal* (***default***) – 3 consecutive MAC address location movements ▪ *High* - 5 consecutive MAC address location movements. 1200 seconds (20 minutes) is the default interval within which the **<n>** consecutive MAC address location movements must occur, in order for the Rogue Device Plugin to determine that these occurrences constitute a MAC spoofing event.

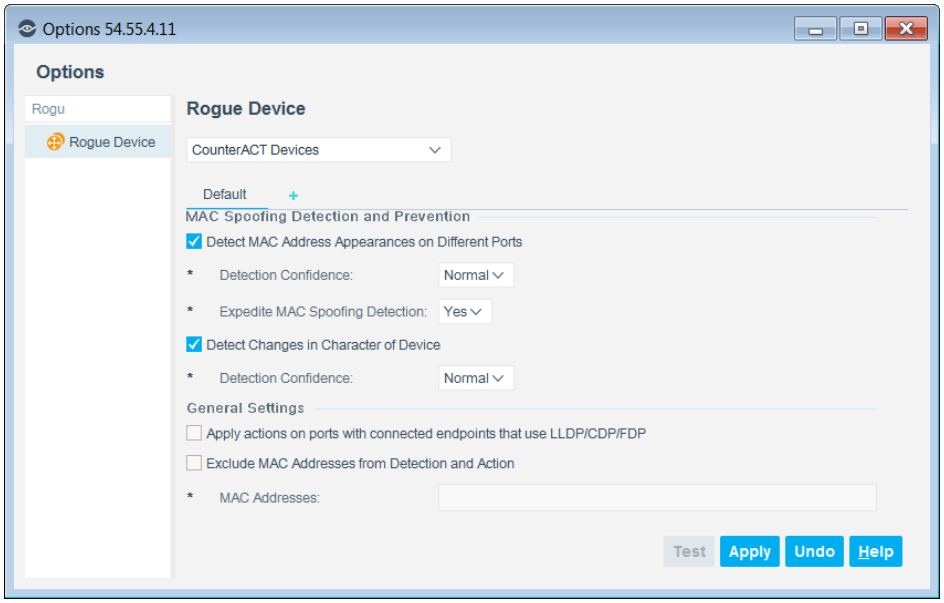
Option / Field	Description	Sub-Fields
	▪ When the plugin identifies that **<n>** consecutive MAC address location movements have occurred within a pre-defined interval, this state results in plugin detection of a MAC spoofing event. In the **Detection Confidence** sub-field, define **<n>**. Forescout recommends enabling the **Expedite MAC Spoofing Detection** option when the RGDP must perform MAC spoofing detection on endpoints that connect to Cisco switches. As needed, enable both this detection method and the following one, as they function independently of each other.	**Expedite MAC Spoofing Detection** Enable this option to permit the RGDP to proactively instruct the SWP to remove an identified MAC address from the MAC Address table of a managed Cisco switch. This option is only supported for SWP-managed Cisco switches and requires specific configuration of the SWP. See section Configuration for Expedite MAC Spoofing Detection. By proactively requesting removal of MAC addresses from a switch's MAC Address table, the RGDP quickens the pace at which it identifies the occurrence of **<n>** consecutive MAC address switch location changes. The RGDP does not have to wait for/rely on the switch to perform its *MAC Address Aging* processing. ***Note***: In network environments that are sensitive about device visibility, if you do not want the plugin to contact certain endpoints by use of the **`ping`** command, you must add such endpoints to the Forescout platform's *Passive Learning* group.
Detect Changes in Character of Device	By default, this option is enabled. Enabling this detection method instructs the plugin to monitor a set of device properties for the occurrence of a change in their value. When the plugin identifies that a change in value occurred in **<n>** properties of a connected endpoint, this state results in plugin detection of a MAC spoofing event. The rationale being that the plugin detected that the endpoint has undergone a change in **<n>** of its fundamental properties, which typically maintain a fixed value.	**Detection Confidence** Select from among the following detection confidence level settings: ▪ *Normal* - a change in value occurred to any 2 of the monitored device properties ▪ *High* (***default***) - a change in value occurred to any 3 of the monitored device properties 600 seconds (10 minutes) is the default interval within which a change in value must occur to the properties, in order for the Rogue Device Plugin to determine that these property value changes constitute a MAC spoofing event. To ensure against false positive, MAC spoofing event detection, the

Option / Field	Description	Sub-Fields
	Note: Detection of a MAC spoofing event does not result when any single, monitored device property undergoes **<n>** changes in value For a list of the default set of plugin-monitored device properties, see Advanced Plugin Configuration. In the **Detection Confidence** sub-field, define the number of monitored device properties, **<n>**, that must undergo a value change. As needed, enable both this detection method and the previous one, as they function independently of each other.	RGDP takes following processing precaution: ▪ Upon the first occurrence of a change in value per MAC address, the RGDP always waits **<m>** minutes to see if the affected MAC address changes/does not change during the waiting period. If the affected MAC address does not change, this confirms for the plugin that the change in value is indeed suspicious and it then starts to track the change in value interval. - For the *Normal* detection confidence level, **<m>** is 90 seconds (1.5 minutes) - For the *High* detection confidence level, **<m>** is 600 seconds (10 minutes)
Apply actions on ports with connected endpoints that use LLDP / CDP / FDP	Enable this option to allow the Switch Plugin to apply, when requested by the Rogue Device Plugin, the *Block Suspected MAC Spoofing* action on ports with connected endpoints, where such endpoints use one of the following discovery protocols: LLDP, CDP or FDP. By default, this option is disabled.	
Exclude MAC Addresses from Detection and Action	Enabling the **Exclude Endpoint MAC Addresses** option causes the **MAC Addresses** field to be available for data entry. By default, the **Exclude Endpoint MAC Addresses** option is disabled.	**MAC Addresses** In the available **MAC Addresses** field, specify the MAC addresses and/or MAC address patterns that you want excluded from rogue device evaluation. ▪ Comma separate multiple entries ▪ Use regular expressions to specify MAC address patterns See also Pre-Defined MAC Address Exclusions. Clearing the **Exclude Endpoint MAC Addresses** checkbox disables use of this option without deleting existing entries from the **MAC Addresses** field.

Option / Field	Description	Sub-Fields
		Note: If a MAC address is excluded only after the endpoint was already determined to be involved in a MAC spoofing event: - The *Block Suspected MAC Spoofing* action cannot be applied on the endpoint - The endpoint's **MAC Spoofing Suspected** property information remains available.

To configure the Rogue Device Plugin, do the following:

1. In the Console, select **Tools** > **Options** > **Modules**.
2. In the Modules pane, expand the **Network** entry and select **Rogue Device**.
3. Select **Configure**. The Rogue Device pane opens.



Pre-Defined MAC Address Exclusions

The following MAC addresses/MAC address patterns, although not entered in the **MAC Addresses** field, are automatically excluded from plugin rogue detection and action processing:

- **`001c7f.*`** - Check Point virtual firewall mac address pattern
- **`0050b6.*`** - docking station MAC address pattern
- **`00249b.*`** - docking station MAC address pattern

If your organization identifies other MAC addresses/MAC address patterns requiring this automatic exclusion, contact Forescout support.

Switch Plugin Configuration

In the Console, you must configure the Switch Plugin (SWP) to manage those switches that require the solution to perform MAC spoofing detection on endpoints that connect to these switches. For information about SWP options mentioned in the following sections, refer to the *Forescout Network Module: Switch Plugin Configuration Guide*.

Configuration for Action Application

Application of Rogue Device Plugin-provided actions requires interaction between the RGDP and the SWP; the RGDP requests the SWP to either block or cancel the block of a managed switch's **<IP address>:<port>**. In order for the SWP to apply these actions on a targeted, managed switch, you are required to configure the SWP with the following option, per managed switch:

- In the CLI pane/tab, enable the **Use CLI** option

Configuration for Expedite MAC Spoofing Detection

Forescout recommends that the RGDP operates using the **Expedite MAC Spoofing Detection** option with managed Cisco switches. Use of this option requires you to configure the SWP with the following the options, per managed Cisco switch:

- In the CLI pane/tab, enable the **Use CLI** option
- In the MAC Permissions section of the Permissions pane/tab, enable the **Write – Enable Actions** option.

Handling SNMP Traps

Forescout recommends that you configure the SWP to handle the SNMP traps sent to it from managed switches. The types of SNMP traps that the SWP handles are:

- Link status traps [Link Up trap, Link Down trap] – sent by all switches
- MAC notification traps - sent only by Cisco switches

In the Console's Edit general parameters window, configure the following Switch Plugin options:

- Enable the **Handle SNMP Traps** option
- In the **Advanced configuration flags** field, configure the **forward_snmp_traps** flag to enable SWP forwarding of SNMP traps

For configuring Cisco switch sending of MAC notification traps, see section Managed Switch Configuration.

Managed Switch Configuration

This section describes the required, managed switch configuration for deploying the Rogue Device Detection and Prevention solution.

Cisco

Forescout recommends that managed Cisco switches send SNMP MAC notification traps to the SWP. You must configure each managed Cisco switch to send MAC notification traps to the SWP. For information about configuring MAC notification

traps on Cisco switches, refer to the *Forescout® Network Module: Switch Plugin Configuration Guide*.

For configuring SWP handling of received MAC notification traps, see section Handling SNMP Traps.

Test

Following your configuration of the Rogue Device Plugin and the Switch Plugin, Forescout recommends that you test each of these plugins.

Policy Evaluation

The Forescout rogue device detection and prevention solution provides the MAC Spoofing Tracking policy template. Use this template to create policies that deal with the endpoints involved in suspected MAC spoofing events.

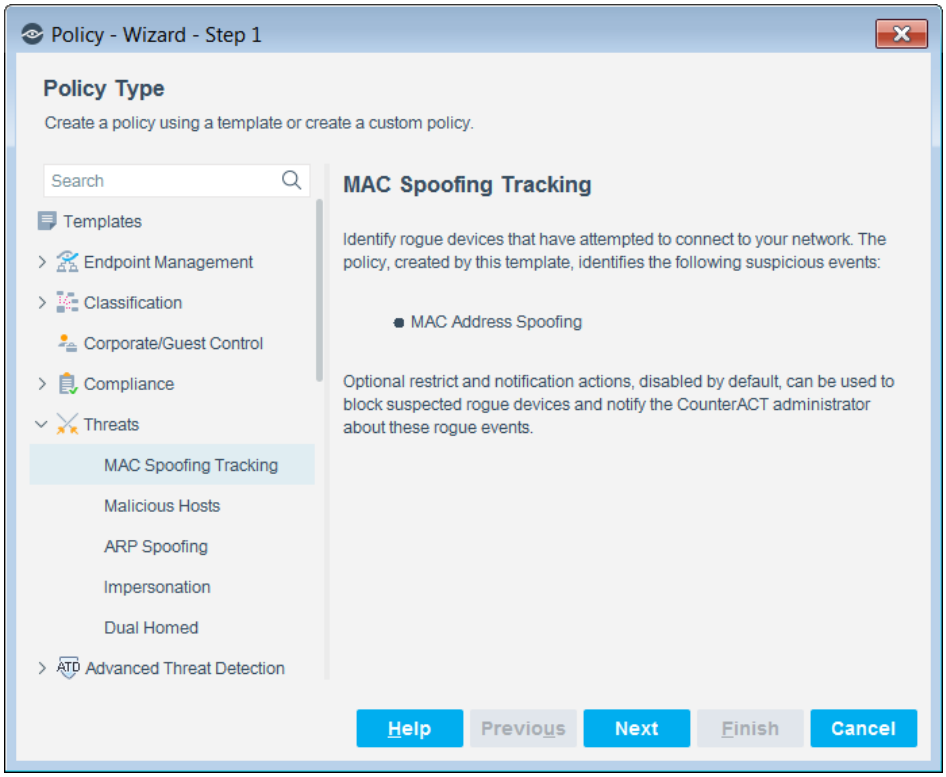
Forescout MAC spoofing detection has the following policy requirements:

- A minimum of one, running (active) MAC Spoofing Tracking policy or an equivalent policy that resolves the **MAC Spoofing Suspected** property.
- ***Only endpoints that fall within the policy's defined scope are subject to MAC spoofing detection***. Therefore, for each MAC Spoofing Tracking policy or equivalent policy, make sure that you define its scope with the IP segments/IP address range(s) that you require the solution to track and detect.

For the properties that the Rogue Device Plugin resolves upon detection of a suspected MAC spoofing event, see Property Resolution.

To access the policy template:

1. Open the Console's **Policy Manager** and select **Add** to open the Policy Wizard.
2. In the Templates tree, navigate to and open **Threats** > **MAC Spoofing Tracking**.



The Policy Wizard then requires you to define the following information:

- Step 2: **Name** (and an optional **Description**)
- Step 3: The policy's scope; the range of IP addresses of the endpoints that the policy targets for evaluation.

  In the **Ranges** column of the Scope page, the default entry is *Hosts without a known IP address* (meaning, Forescout does not know the endpoint IP address). This entry ensures that the policy you create targets spoofing attackers for evaluation, as Forescout assigns a unique, fake MAC address to detected, spoofing attackers but does not assign them an IP address. Select **Add** or **Segments** to add entries to the table.
- Step 4: The **Event Detection Period** - specify the time period when suspicious MAC spoofing events had to have been identified, in order to qualify the endpoints involved in the event for policy evaluation. The defined period globally applies to all policy sub-rules. The default, event detection period is *Detected within the last 1 hour*.

Sub-Rules

The policy uses sub-rules to evaluate endpoints that were involved in a suspected MAC spoofing event and identify those endpoints that match the specified, sub-rule criteria.

The policy includes the following sub-rules:

- Detected Spoofing Attacker
- Detected Spoofing Victim
- Ever Detected as Spoofing Victim

Endpoints that do not match any policy sub-rule means that the plugin has never identified them as being involved in a suspected MAC spoofing event.

Detected Spoofing Attacker

Endpoints matching this sub-rule's condition are the identified *spoofing attacker* in a suspected MAC spoofing event, which the plugin detected within either the defined **Event Detection Period** or the sub-rule's locally defined event detection period. The assigned value of their **MAC Spoofing Suspected** property sub-field **Endpoint Identity** is *Spoofing Attacker*.

When an endpoint matches this sub-rule's condition, the policy then applies all *enabled*, sub-rule actions. The default set of actions for this sub-rule is:

- *Block Suspected MAC Spoofing* – block the detected switch port where the matching endpoint is connected. For details about this action, see Action Control.
- *Send Message to Syslog* – send a message, either a customized one or the default one, to a syslog server. For details about this action, refer to the *Core Extensions Module: Syslog Plugin Configuration Guide*.
- *Send Email* – send an email message to the configured Forescout administrator(s) of the Appliance. For details about this action, refer to the following *Forescout Administration Guide* sections:
  - *Chapter 2: Working the Initial Setup Wizard > Set Up an Appliance from Scratch > Mail*
  - *Chapter 5: Policy Management > Policy Preferences > Email Preferences*

By default, these actions are disabled.

Detected Spoofing Victim

Endpoints matching this sub-rule's condition are the identified *spoofing victim* in a suspected MAC spoofing event, which the plugin detected within either the defined **Event Detection Period** or the sub-rule's locally defined event detection period. The assigned value of their **MAC Spoofing Suspected** property sub-field **Endpoint Identity** is *Spoofing Victim*.

When an endpoint matches this sub-rule's condition, the policy then applies all *enabled*, sub-rule actions. The default set of actions for this sub-rule is:

- *Send Message to Syslog* – send a message, either a customized one or the default one, to a syslog server. For details about this action, refer to the *Core Extensions Module: Syslog Plugin Configuration Guide*.

- *Send Email* – send an email message to the configured Forescout administrator(s) of the Appliance. For details about this action, refer to the following *Forescout Administration Guide* sections:
  - *Chapter 2: Working the Initial Setup Wizard > Set Up an Appliance from Scratch > Mail*
  - *Chapter 5: Policy Management > Policy Preferences > Email Preferences*

By default, these actions are disabled.

Ever Detected as Spoofing Victim

Endpoints matching this sub-rule's condition are the identified *spoofing victim* in a suspected MAC spoofing event, which the plugin *ever* detected; the assigned value of their **MAC Spoofing Suspected** property sub-field **Endpoint Identity** is *Spoofing Victim*.

When an endpoint matches this sub-rule's condition, the policy then applies all *enabled*, sub-rule actions. The default set of actions for this sub-rule is:

- *Send Message to Syslog* – send a message, either a customized one or the default one, to a syslog server. For details about this action, refer to the *Core Extensions Module: Syslog Plugin Configuration Guide*.
- *Send Email* – send an email message to the configured Forescout administrator(s) of the Appliance. For details about this action, refer to the following *Forescout Administration Guide* sections:
  - *Chapter 2: Working the Initial Setup Wizard > Set Up an Appliance from Scratch > Mail*
  - *Chapter 5: Policy Management > Policy Preferences > Email Preferences*

By default, these actions are disabled.

Property Resolution

The Forescout rogue device detection and prevention solution resolves the following properties:

Property	Sub-Field	Description
MAC Spoofing Suspected	**Spoofing Attacker Network Device Address**	IP address of the network device where the illegitimate, spoofing endpoint is located.
	Spoofing Attacker Network Device Port	Port (the physical Ethernet interface information of the port, for example, **eth1/3**) on the network device where the illegitimate, spoofing endpoint is connected.
	Spoofing Victim Network Device Address	IP address of the network device where the legitimate, victimized endpoint is located.

Property	Sub-Field	Description
	Spoofing Victim Network Device Port	Port (the physical Ethernet interface information of the port, for example, **eth1/3**) on the network device where the legitimate, victimized endpoint is connected.
	Endpoint Identity	Identifies each endpoint involved in the suspected MAC spoofing event, using either of the following assignments: ▪ *Spoofing Attacker* (illegitimate endpoint) ▪ *Spoofing Victim* (legitimate endpoint)
	Spoofed MAC Address	The MAC address being spoofed in the suspected MAC spoofing event
	Detection Method	The method that the plugin used to detect the suspected MAC spoofing event. Sub-field provides any of the following values: ▪ *MAC Address Appearances on Different Ports* ▪ *Changes in Character of Device*
	Device Character Changes	Sub-field provides both the original and the changed values of the plugin-monitored properties that, due to their value change, triggered plugin detection of a MAC spoofing event. Changed property values are reported in the following form: **<propertyA value'> -> <propertyA value''>, ... , <propertyZ value'> -> <propertyZ value''>**
MAC Spoofing Suspected – Blocked Locations		The blocked network device location - IP address and port – of either the spoofing attacker, the spoofing victim or both of these involved endpoints. The information is provided in the following form: **<IP address>:<Port>, <IP address>:<Port>** Blocking of network device locations, involved in a suspected MAC spoofing event, is accomplished by applying the *Block Suspected MAC Spoofing* action. For details about this action, see Action Control.

The plugin resolves the **MAC Spoofing Suspected** property upon detection, in your network, of each suspected MAC spoofing event. While the MAC spoofing event remains in effect, the plugin also periodically re-resolves this property.

The plugin resolves the **MAC Spoofing Suspected – Blocked Locations** property as part of its processing of the *Block Suspected MAC Spoofing* action.

In the Forescout Console, find these properties in the **Rogue Device** property group.

Action Control

The Rogue Device Plugin provides the following action to apply control on endpoints:

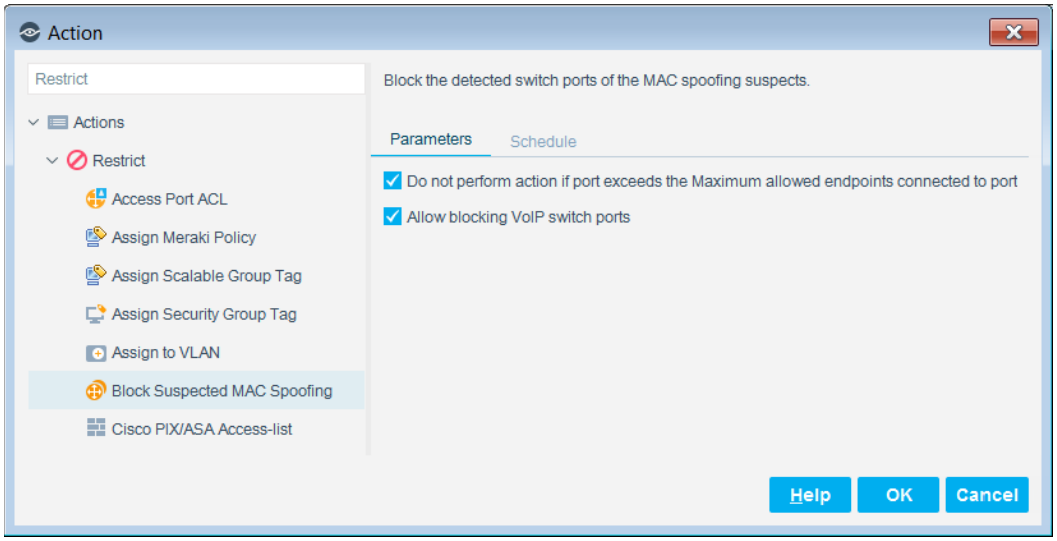
- *Block Suspected MAC Spoofing* - blocks the port of the managed switch to which the targeted endpoint (MAC address) is connected

  As part of action processing, the plugin resolves the **MAC Spoofing Suspected - Blocked Locations** property.

  In the Forescout Console, find this action in the **Restrict** action group.

(Flexx licensing) To use this action, ensure that you have a valid *Forescout eyeControl* license. Refer to the *Forescout Flexx Licensing How-to Guide* for more information about managing licenses.

Action processing requires interaction between the Rogue Device Plugin and the Switch Plugin; the Rogue Device Plugin requests the Switch Plugin to either block or cancel the block of a managed switch's **<IP address>:<port>**. Use the action in policies and manually apply it on detected endpoints.



In the action's Parameter tab, the following options are available for configuration:

Option	Description
Do not perform action if port exceeds the Maximum allowed endpoints connected to port	▪ Enable this option to prevent applying the *Block Suspected MAC Spoofing* action on switch ports that exceed the value defined for the Switch Plugin option **Maximum allowed endpoints connected to port for Block or Assign to VLAN actions**. ▪ Disable this option to allow applying the *Block Suspected MAC Spoofing* action on switch ports that exceed the value defined for the Switch Plugin option **Maximum allowed endpoints connected to port for Block or Assign to VLAN actions**. By default, this option is enabled.

Option	Description
	For information about this Switch Plugin option, refer to the Forescout Switch Plugin Configuration Guide.
Allow blocking VoIP switch ports	▪ Enable this option to allow applying the *Block Suspected MAC Spoofing* action on switch VoIP ports. ▪ Disable this option to prevent applying the *Block Suspected MAC Spoofing* action on switch VoIP ports. By default, this option is enabled. For information about Switch Plugin-managed switches that support VoIP blocking, refer to the Forescout Switch Plugin Configuration Guide.

Policy re-evaluation can cancel the applied action; you can also manually cancel the action. The plugin provides the following cancel action:

- *Undo Rogue Device Block* – removes the block of the port of the managed switch to which the targeted endpoint (MAC address) is connected

  In the Forescout Console, find this action in the **Restrict** action group.

(Flexx licensing) To use this action, ensure that you have a valid *Forescout eyeControl* license. Refer to the *Forescout Flexx Licensing How-to Guide* for more information about managing licenses.

Console Information Display

This section describes the impact of the Forescout rogue device detection and prevention solution on Console information displays, as follows:

- The Home Tab
- The Event Viewer

Home Tab

In the **All Hosts** pane in the Console's **Home** tab, entries of connected endpoints that the RGDP determines to be involved in a MAC spoofing event, display the following distinguishing information:

Detected Endpoint Identity	Column / Field	Information / Description
Spoofing Attacker	**MAC Address**	The entry displays the unique, ***fake*** MAC address of the Spoofing Attacker, which the Forescout platform assigns to the endpoint.
	Comment	The entry displays the following comment: *Note: Detected spoofing attacker. Fake MAC address assigned by Forescout.*

When you select such a table entry, meaning an endpoint determined to be involved in a MAC spoofing event, the following MAC spoofing event information displays in the **Profile** tab:

- The **MAC Spoofing Suspected** property and it sub-fields

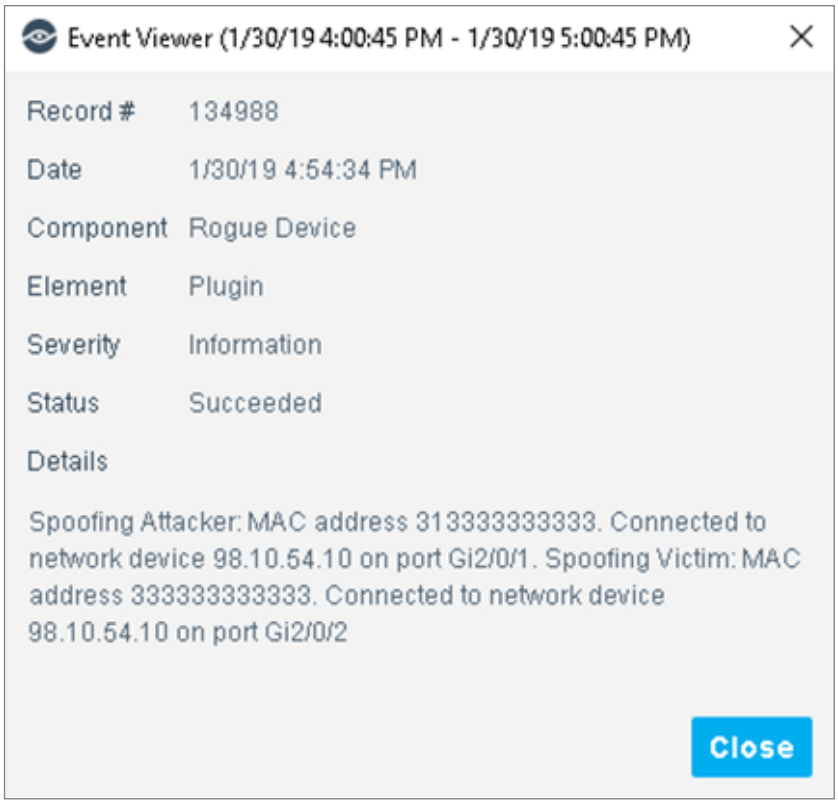
- The **MAC Spoofing Suspected - Blocked Locations** property – info only displays (available) while the *Block Suspected MAC Spoofing* action is applied on the endpoint

For a description of these properties, see Property Resolution.

Event Viewer

For each, detected MAC spoofing event, the RGDP creates an entry in the Console **Event Viewer** that contains the following event information detail:

Detected Endpoint Identity	Information Details	Description
Spoofing Attacker	**MAC Address**	Unique ***fake*** MAC address of the Spoofing Attacker, which the Forescout platform assigns to the endpoint.
	Network Device ▪ IP Address ▪ Port	▪ IP address of the network device where the illegitimate, spoofing endpoint is located. ▪ Port on the network device where the illegitimate, spoofing endpoint is connected.
Spoofing Victim	**MAC Address**	MAC address of the Spoofing Victim.
	Network Device ▪ IP Address ▪ Port	▪ IP address of the network device where the legitimate, victimized endpoint is located. ▪ Port on the network device where the legitimate, victimized endpoint is connected.



Advanced Plugin Configuration

Using the CounterACT device CLI, you can modify plugin processing flag settings to customize the rogue device detection solution to suit your network environment. Customize any of the following:

- Monitored Device Properties
- Detection Confidence Levels
- Detection Intervals

Before modifying processing flag settings, Forescout recommends to first contact our customer support to discuss.

Monitored Device Properties

The detection method **Detect Changes in Character of Device** instructs the Rogue Device Plugin to monitor a set of device properties for the occurrence of a change in their value. The default set of plugin-monitored device properties are as follows:

Device Property	fstool Property Name	Plugin Responsible for Obtaining the Information
DHCP Domain Name	**dhcp_domain_name**	Core Extensions Module: DHCP Classifier Plugin

Device Property	fstool Property Name	Plugin Responsible for Obtaining the Information
DHCP Hostname	**dhcp_hostname**	Core Extensions Module: DHCP Classifier Plugin
DHCP Device OS	**dhcp_os**	Core Extensions Module: DHCP Classifier Plugin
DHCP Vendor Class	**dhcp_vendor_class**	Core Extensions Module: DHCP Classifier Plugin
DHCP Request Fingerprint	**dhcp_req_fingerprint**	Core Extensions Module: DHCP Classifier Plugin
	ipv6_link_local_internal ***Note***: This address information is obtained for connected IPv6 endpoints and is reported, per endpoint, in the Console **Home** tab > **All Hosts** pane along with the endpoint IPv6 address(es).	Network Module: ▪ Switch Plugin ▪ Wireless Plugin
Network Function	**va_netfunc**	Endpoint Module: HPS Inspection Engine
Switch Port PoE Connected Device	**sw_port_poe_desc**	Network Module: Switch Plugin

The following plugin processing flag defines the set of plugin-monitored device properties:

- **config.listen_to_properties.value**

Using the CounterACT device CLI, you can modify this processing flag's setting. Modifications that you make to the set of plugin-monitored device properties remain in effect following both a Rogue Device Plugin upgrade and a Rogue Device Plugin restart.

For plugin monitoring of track changes properties, see also Monitoring of Track Changes Properties.

To modify the set of plugin-monitored device properties:

1. To modify the processing flag per Appliance, do the following:
   a. On the Appliance, log in to the CLI.
   b. Run the following fstool command:
   fstool rogued set_property config.listen_to_properties.value = property= <property_name$_1$>:from=<value/regular expression>:to=<value/regular expression>,...,<property_name$_n$>:from=<value/regular expression>:to=<value/regular expression>
   Make sure the command sets the flag's **from=:to=** value range for all device properties you want monitored.

2. To modify the processing flag for all Forescout devices [Enterprise Manager and all Appliances], do the following:

   a. On the Enterprise Manager, log in to the CLI.

   b. For the Enterprise Manager, run the fstool command provided in the preceding step 1b.

   c. For all Appliances, run the following fstool command:

   fstool oneach –c fstool rogued set_property config.listen_to_properties.value = property=<property_name$_1$>:from=<value/regular expression>:to=<value/regular expression>,...,<property_name$_n$>:from=<value/regular expression>:to=<value/regular expression>

   Make sure the command sets the flag's **from=:to=** value range for all device properties you want monitored.

For example, per Appliance, to set the flag's **from=:to=** value range to **<any value>** for all of the default set of plugin-monitored device properties, the fstool command to run is:

fstool rogued set_property config.listen_to_properties.value = property=dhcp_hostname:from=.*:to=.*,property=nbtdomain:from=.*:to=.*,property=nbthost:from=.*:to=.*,property=sw_port_poe_desc:from=.*:to=.*,property=va_netfunc:from=.*:to=.*,property=va_os:from=.*:to=.*

Monitoring of Track Changes Properties

- Plugin monitoring of track changes properties requires the following configuration:
  - Adding the track changes property to the set of plugin-monitored device properties
  - In the MAC Spoofing Tracking policy or the equivalent policy, which resolves the **MAC Spoofing Suspected** property, add a final sub-rule that evaluates the track changes properties you want the plugin to monitor. This is required because only policy evaluation resolves track changes properties.
- When monitoring track changes properties, the plugin includes the following changes as value changes in any track changes property:
  - From any value <*n*> to the value *Became Irresolvable*
  - From the value *Became Irresolvable* to any value <*n*>

Detection Confidence Levels

Both the **Detect MAC Address Appearances on Different Ports** and the **Detect Changes in Character of Device** detection methods perform their processing using their own detection confidence level. The following plugin processing flags define the detection confidence levels:

- For the **Detect MAC Address Appearances on Different Ports** method
  - **config.normal_mac_spoof_mac_move_to_port_events.value** – defines the number, **<n>**, of consecutive MAC address location movements for the method's *Normal* detection confidence level

  - **config.high_mac_spoof_mac_move_to_port_events.value** – defines the number, **<n>**, of consecutive MAC address location movements for the method's *High* detection confidence level

- For the **Detect Changes in Character of Device** method
  - **config.normal_number_of_properties_changed_required_for_mac_spoof.value** – defines the number, **<n>**, of changes in value that must occur to any of the monitored device properties for the method's *Normal* detection confidence level
  - **config.high_number_of_properties_changed_required_for_mac_spoof.value** – defines the number, **<n>**, of changes in value that must occur to any of the monitored device properties for the method's *High* detection confidence level

Using the CounterACT device CLI, you can modify any of these processing flag's setting. Modifications that you make to processing flag settings remain in effect following both a Rogue Device Plugin upgrade and a Rogue Device Plugin restart.

To modify detection confidence levels, see Modify Detection Confidence Levels and Intervals.

Detection Intervals

Both the **Detect MAC Address Appearances on Different Ports** and the **Detect Changes in Character of Device** detection methods perform their processing using their own detection interval. The following plugin processing flags define the detection intervals:

- **config.mac_to_port_change_threshold_period.value** – defines, in seconds **<s>**, the detection interval for the **Detect MAC Address Appearances on Different Ports** method
- **config.property_change_expiration_period.value** – defines , in seconds **<s>**, the detection interval for the **Detect Changes in Character of Device** method

Using the CounterACT device CLI, you can modify any of these processing flag's setting. Modifications that you make to processing flag settings remain in effect following both a Rogue Device Plugin upgrade and a Rogue Device Plugin restart.

To modify detection intervals, see Modify Detection Confidence Levels and Intervals.

Modify Detection Confidence Levels and Intervals

Modify processing flag settings for *detection confidence level* and/or *detection interval* using the following procedure:

To modify detection confidence level/detection interval:

1. To modify the processing flag per Appliance, do the following:
   a. On the Appliance, log in to the CLI.
   b. Run the following fstool command:
   fstool rogued set_property <processing flag> <n/s>

2. To modify the processing flag for all Forescout devices [Enterprise Manager and all Appliances], do the following:
   a. On the Enterprise Manager, log in to the CLI.
   b. For the Enterprise Manager, run the fstool command provided in the preceding step 1b.
   c. For all Appliances, run the following fstool command:
      `fstool oneach –c fstool rogued set_property <processing flag> <n/s>`

fstool command examples:

- On a single Appliance, run the following command to set its *detection confidence level* processing flag **`config.normal_mac_spoof_mac_move_to_port_events.value`** to the value 1:

  `fstool rogued set_property config.normal_mac_spoof_mac_move_to_port_events.value 1`

- Set the *detection interval* processing flag **`config.property_change_expiration_period.value`** to the value 300 for all Forescout devices:
  – On the Enterprise Manager, run the following command to set the processing flag for the Enterprise Manager:
    `fstool rogued set_property config.property_change_expiration_period.value 300`
  – On the Enterprise Manager, run the following command to set the processing flag for each Appliance:
    `fstool oneach –c fstool rogued set_property config.property_change_expiration_period.value 300`

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 Forescout Resources Page, or one of two Forescout portals, depending on which licensing mode your deployment is using.

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

Software downloads are also available from these portals.

To identify your licensing mode:

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

Forescout Resources Page

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

To access the Forescout Resources Page:

- Go to https://www.Forescout.com/company/resources/, select **Technical Documentation** and search for documents.

Product Updates Portal

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

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

To access documentation on the Forescout Customer Portal:

- 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.

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

To access the Documentation Portal:

- Go to https://updates.forescout.com/support/files/counteract/docs_portal/ and use your customer support credentials to log in.

Forescout Help Tools

Access information 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.

Forescout Administration Guide

- Select **Forescout Help** from the **Help** menu.

Plugin Help Files

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

Online Documentation

- Select **Online Documentation** from the **Help** menu to access either the Forescout Resources Page (Flexx licensing) or the Documentation Portal (Per-Appliance licensing).