CounterACT® Security Policy Templates

Configuration Guide

Version 18.0.1

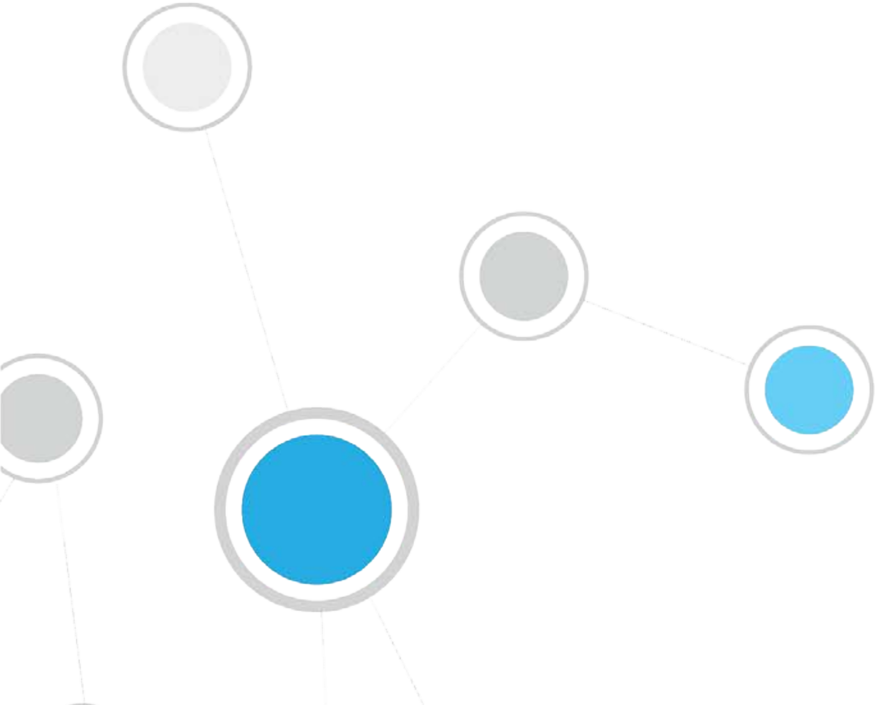


Table of Contents

About Security Policy Templates

Security policy templates use existing ForeScout CounterACT® functionality to detect, evaluate, and respond to vulnerabilities and threats - speeding and simplifying your network response. When this plugin is installed, templates are available in the Policy view of the Console under the *Vulnerability and Response* sub-folder in the Templates tree. Security Policy Templates are named according to the format - *VR + <vulnerability name>*. To work with these templates, it is recommended to:

- Read the release notes, and review policy logic in the Console's Policy view.
- Enable/add mitigation actions to generated policies.

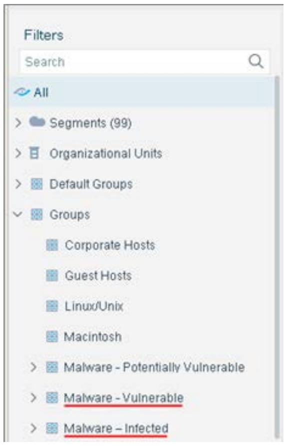
For details of working with CounterACT policies, see the *Console User Manual*.

Review and understand the detection/logic model provided by ForeScout in these templates before you add or edit rules, or make more extensive customizations.

Tracking Vulnerable and Infected Endpoints

In addition to the actions applied by these policies, it is often useful to identify infected and vulnerable endpoints for further tracking and handling. To do this, the plugin creates standard folders in the Groups tree of the Filters pane of NAC and Inventory views.

Templates provided by this plugin use the **Add to Group** action to assign endpoints to the Malware-Vulnerable and Malware-Infected groups.



Supported CounterACT Versions

Customers who work with the following CounterACT versions can install this release:

- 7.0.0

Requirements

- An active Maintenance Contract for CounterACT devices is required.

- HPS Vulnerability DB version 18.0.1 or above.
- Wireless Plugin 1.7.0.2009 or higher is required to work with VR WPA2 KRACK policy templates. You can download and install Wireless Plugin 1.7.0.2009 from the following location: http://updates.forescout.com/support/files/plugins/wireless/1.7.0.2009/1.7.0.2009-17002009/ForeScout-wireless-1.7.0.2009-17002009.fpi
- Advanced Tools Plugin release 2.2.0.1 or above.
- Linux Plugin version 1.1.0 or above for working with the VR Intel SA-00075 AMT/ISM/SBT and VR Intel SA-00086 ME/SPS/TXE security templates
- OS X Plugin version 1.2.0 or above for working with the VR macOS High Sierra Admin Bypass security template.
- Windows PowerShell scripts must be allowed to run on Windows managed endpoints for working with the VR Meltdown and VR Spectre templates.
- To run policy actions on endpoints with Secure Connector installed, Secure Connector must be running as a service.

Installation

To install the plugin:

1. Navigate to the Customer Support, Base Plugins page and download the plugin **.fpi** file.
2. Save the file to the machine where the CounterACT Console is installed.
3. Log into the CounterACT Console and select **Options** from the **Tools** menu.
4. Select **Plugins**. The Plugins pane opens.
5. Select **Install**. The Open dialog box opens.
6. Browse to and select the saved plugin **.fpi** file.
7. Select **Install**.
8. An installation or upgrade information dialog box and a license agreement dialog box will open. Accept the license agreement to proceed with the installation.
9. Once the installation is complete, select **Close**. The plugin is listed in the Plugins pane.

Configuration

No plugin configuration is required.

Policy Templates in This Release

This release provides templates that address the following threats:

- Bad Rabbit Ransomware

- EsteemAudit
- EternalBlue
- GoAhead
- Intel SA-00075 AMT/ISM/SBT
- Intel SA-00086 ME/SPS/TXE
- IoT Reaper
- macOS High Sierra Admin Bypass
- Meltdown
- Petya
- Spectre
- SSL Vulnerability
- WannaCrypt/WannaCry
- WPA2 KRACK

In the Policy creation wizard, these templates are installed under the *Vulnerability and Response* sub-folder in the Templates tree.

Bad Rabbit Ransomware

Policies based on the following template can help you detect and mitigate Bad Rabbit ransomware (a variant of Petya malware).

VR Bad Rabbit

Policies you create with this template evaluate whether the endpoints in the policy scope are vulnerable to Bad Rabbit ransomware. Endpoints not yet infected can be "vaccinated" by running a VBS script on the endpoint that creates a file which prevents infection.

- This policy uses the results of classification to detect endpoints.
  - In environments with Service Pack 2.3.x, verify that the Asset Classification policy is running.
  - In environments with Service Pack 3.0.0 and above, verify that the Primary Classification policy is running. Enable the optional **Add to Group** actions in the policy.
- This policy only evaluates endpoints managed by Remote Inspection or SecureConnector.
- CounterACT must have permission to run a VBS script in the Windows/system root directory (%windir%).

EsteemAudit

Policies based on the following template can help you detect and mitigate the EsteemAudit exploit, which targets Windows endpoints:

VR EsteemAudit

Policies you create with this template use CounterACT properties related to installed Windows files to evaluate a Windows endpoint's vulnerability to EsteemAudit malware, and whether Microsoft patches were installed on the endpoint.

- This policy uses the results of classification to detect endpoints.
  - In environments with Service Pack 2.3.x, verify that the Asset Classification policy is running.
  - In environments with Service Pack 3.0.0 and above, verify that the Primary Classification policy is running. Enable the optional **Add to Group** actions in the policy.
- This policy evaluates all endpoints classified by CounterACT as Windows devices.
- You must install Advanced Tools Plugin release 2.2.3 or above to work with policies created by this template.

EternalBlue

Policies based on the following template can help you detect and mitigate malware that exploits the Eternal Blue vulnerability, such as the WannaCry malware package. Typically Windows endpoints are targeted.

See additional policies that detect specific malware packages such as WannaCrypt/WannaCry.

VR EternalBlue

Policies you create with this template run a script on CounterACT which remotely evaluates whether the endpoints in the policy scope are vulnerable to malware that exploits the Eternal Blue vulnerability (MS17-010), such as the WannaCry malware package.

- This policy uses the results of classification to detect endpoints.
  - In environments with Service Pack 2.3.x, verify that the Asset Classification policy is running.
  - In environments with Service Pack 3.0.0 and above, verify that the Primary Classification policy is running. Enable the optional **Add to Group** actions in the policy.
- This policy evaluates all endpoints classified by CounterACT as Windows devices.
- This policy evaluates both managed and unmanaged endpoints.
- Analysis of SMB responses may not yield a conclusive result on some endpoints.

- You must install Advanced Tools Plugin release 2.2.0.1 or above to work with policies created by this template.

GoAhead

GoAhead httpd 2.5 < 3.6.5, also known as LD_PRELOAD exploit (CVE-2017-17562), is a vulnerability found in the GoAhead web server software in IoT devices that allows Remote Code Execution that can be potentially remotely exploited to hijack gadgets.

VR GoAhead

This policy identifies potentially vulnerable devices and by applying control may be used proactively to prevent security breaches, data leakage and DDoS attacks.

This policy evaluates both managed and unmanaged endpoints. No credentials are required for endpoint login.

Requirements

- CounterACT 7.0.0 with Service Pack 2.3.x or higher.
- Advanced Tools Plugin release 2.2.0.1 or above installed and running.

Intel SA-00075 AMT/ISM/SBT

The policies you create with this template detect Windows and Linux/Unix endpoints with Intel SA-00075 AMT/ISM/SBT vulnerability.

VR Intel SA-00075 AMT/ISM/SBT

This policy only detects vulnerabilities on managed endpoints. This policy provides a third party Intel detection tool. Linux endpoint or server support includes Ubuntu 16.04 LTS and 14.04 LTS or higher.

🗎 *Some tools such as Anti-Virus may prevent the policy from working properly. If this happens, you may need to manually whitelist the "fs_test_00075.exe" and "fs_test_00075_Linux.sh" executables used in the Expected Script Results conditions.*

🗎 *The tool does not support Virtual Machine (VM) environment.*

Requirements

- CounterACT 7.0.0 with Service Pack 2.3.x or higher.
- In environments with Service Pack 3.0.0 and above, your system must be running the Primary Classification policy with Add to Group actions enabled to work with this template.
- In environments with Service Pack 2.3.x your system must be running the Asset Classification policy to work with this template.
- Linux Plugin installed and running

Windows endpoints/servers:

- Microsoft Windows 7, 8, 8.1, or 10
- Local operating system administrative access

Linux endpoints/servers:

- Ubuntu 16.04 LTS and 14.04 LTS.
- Local operating system administrative access
- The Intel® Management Engine Components, specifically: The Intel® Management Engine Interface driver (Intel® MEI).

Intel SA-00086 ME/SPS/TXE

The policies you create with this template detect Windows and Linux/Unix endpoints with Intel SA-00086 ME/SPS/TXE vulnerability.

VR Intel SA-00086 ME/SPS/TXE

This policy only detects vulnerabilities on managed endpoints. This policy provides a third party Intel detection tool.

> *Some tools such as Anti-Virus may prevent the policy from working properly. If this happens, you may need to manually whitelist the "fs_test_00086.exe" and "fs_test_00086_Linux.sh" executables used in the Expected Script Results conditions.*

Requirements

- CounterACT 7.0.0 with Service Pack 2.3.x or above.
- In environments with Service Pack 3.0.0 and above, your system must be running the Primary Classification policy with Add to Group actions enabled to work with this template.
- In environments with Service Pack 2.3.x your system must be running the Asset Classification policy to work with this template .
- Linux Plugin installed and running.

Windows endpoints/servers:

- Microsoft Windows* 7, 8, 8.1, or 10 (Windows* 10S and Windows*10 IOT Core are not supported)
- Windows* 2012 R2 for servers (x64)
- .NET Framework 4.5 or higher
- HECI Driver
- Local operating system administrative access

Linux endpoints/servers:

- Python 2.7 or higher
- Ubuntu LTS 16.0.4 (for client), Redhat 7.2 (for Server)

- Local operating system administrative access

IoT Reaper

Policies based on the following templates use CounterACT remote scanning capabilities to evaluate IoT device vulnerability to the ports and HTTP protocols used by the botnet for download and infection.

- You must install the latest release of the Advanced Tools Plugin to work with this template.

VR IoT Reaper

Use this template in environments that run CounterACT with Service Pack 3.0.0 or above.

This policy scans potential IoT devices for vulnerable ports. Once such a device is detected, CounterACT tests these ports with the HTTP protocol that is used by the botnet for infection. Suspected vulnerable devices are reported by CounterACT.

- Your system must be running the Primary Classification policy to work with this template.

VR IoT Reaper for SP 2.3.x

Use this template in environments that run CounterACT with Service Pack 2.3.x.

This policy scans all devices for vulnerable ports. Once such a device is detected, CounterACT tests these ports with the HTTP protocol that is used for infection. Suspected vulnerable devices are reported by CounterACT.

macOS High Sierra Admin Bypass

The policies you create with this template detect Macintosh endpoints with macOS High Sierra admin bypass vulnerability.

VR macOS High Sierra Admin Bypass

This policy only detects vulnerabilities on managed endpoints.

🗎 *When upgrading from the macOS High Sierra security template version 10.13.0 to 10.13.1, a reboot is required for the patches to complete installation.*

Requirements

- CounterACT 7.0.0 with Service Pack 2.3.x or above.
- In environments with Service Pack 3.0.0 and above, your system must be running the Primary Classification policy with Add to Group actions enabled to work with this template.
- In environments with Service Pack 2.3.x your system must be running the Asset Classification policy to work with this template.
- OS X Plugin installed and running.

- To run policy actions on endpoints with Secure Connector installed, Secure Connector must be running as a service.
- To run policy actions on endpoints with Remote Inspection, the user must have administrator privileges

By default, CounterACT uses the HPS Vulnerability DB Plugin to distribute vulnerability information. For more information about download options supported by CounterACT, see these sections of the HPS Inspection Engine Configuration Guide.

- Distributing Vulnerability Information to Windows Endpoints
- Using Windows Server Update Services (WSUS) or Windows Update
- Windows Update Default Settings

Meltdown

Meltdown breaks the most fundamental isolation between user applications and the operating system. This attack allows a program to access the memory, and thus also the secrets, of other programs and the operating system. Meltdown is described in CVE-2017-5754, see https://meltdownattack.com for more information.

VR Meltdown

The policies you create with this template detect Windows, Linux/Unix and OS X with the Meltdown vulnerability.

This policy only detects vulnerabilities on managed Windows, Linux/Unix and OS X endpoints.

This policy provides a third party Microsoft detection tool. Some tools such as Anti-Virus applications may prevent the policy from working properly. You may need to manually whitelist the *fs_test_SpeculationControl.bat* and *fs_test_pti_Linux.sh* executables used in the Expected Script Results conditions.

Requirements

- CounterACT 7.0.0 with Service Pack 2.3.x or above.
- Linux Plugin or above installed and running. The Linux Plugin should be configured with the user that can run scripts as root.
- OS X Plugin installed and running. OS X Plugin Secure Connector should be deployed as a Service. OS X Plugin Remote Inspection should be configured with the user that can run scripts as root.
- Windows PowerShell scripts must be allowed to run on Windows managed endpoints.

Petya

Policies based on the following template can help you detect and mitigate Petya ransomware.

VR Petya

Policies you create with this template evaluate whether the endpoints in the policy scope are vulnerable to Petya ransomware. Infected endpoints are detected before the terminal reboot phase. Endpoints not yet infected can be "vaccinated" by running a VBS script on the endpoint that creates a file which prevents infection.

- This policy uses the results of classification to detect endpoints.
  - In environments with Service Pack 2.3.x, verify that the Asset Classification policy is running.
  - In environments with Service Pack 3.0.0 and above, verify that the Primary Classification policy is running. Enable the optional **Add to Group** actions in the policy.
- This policy only evaluates endpoints managed by Remote Inspection or SecureConnector.

Spectre

Spectre breaks the isolation between different applications. It allows an attacker to trick error-free programs, which follow best practices, into leaking their secrets. In fact, the safety checks of said best practices actually increase the attack surface and may make applications more susceptible to Spectre. Spectre is described in (CVE-2017-5753 and CVE-2017-5715, see https://meltdownattack.com for more information.

VR Spectre

The policies you create with this template detect Windows, Linux/Unix and OS X with the Spectre vulnerability.

This policy only detects vulnerabilities on managed Windows, Linux/Unix and OS X endpoints.

This policy provides a third party Microsoft detection tool. Some tools such as Anti-Virus applications may prevent the policy from working properly. You may need to manually whitelist the *fs_test_SpeculationControl.bat* and *fs_test_pti_Linux.sh* executables used in the Expected Script Results conditions.

Requirements

- CounterACT 7.0.0 with Service Pack 2.3.x or above.
- Linux Plugin or above installed and running. The Linux Plugin should be configured with the user that can run scripts as root.
- OS X Plugin installed and running. OS X Plugin Secure Connector should be deployed as a Service. OS X Plugin Remote Inspection should be configured with the user that can run scripts as root.
- Windows PowerShell scripts must be allowed to run on Windows managed endpoints.

SSL Vulnerability

The policies you create with this template detect HTTPS servers that are vulnerable to malware that exploits SSL vulnerabilities in managed and unmanaged endpoints. For example, the ROBOT Attack TLS Decryption Vulnerability (Return of Bleichenbacher's Oracle Threat) and the Heartbleed vulnerability.

The Robot Attack TLS Decryption Vulnerability is a 19-year-old vulnerability that allows performing RSA decryption and signing operations with the private key of a TLS server. For more information on the vulnerability, see https://eprint.iacr.org/2017/1189 and https://robotattack.org

Heartbleed is a serious vulnerability in the OpenSSL cryptographic software library that allows stealing the information protected, under normal conditions, by the SSL/TLS encryption used to secure the Internet.

VR SSL

This policy evaluates both managed and unmanaged endpoints. No credentials are required for endpoint login.

🗎 *This policy template can be customized to accommodate different IP address ranges and specific HTTPS ports.*

Requirements

- CounterACT 7.0.0 with Service Pack 2.3.x or above.
- Advanced Tools Plugin release 2.2.0.1 or above installed and running.

WannaCrypt / WannaCry

Policies based on the following template can help you detect and mitigate WannaCrypt/WannaCry ransomware, which targets Windows endpoints.

🗎 *See also the EternalBlue policy template that addresses this vulnerability.*

VR WannaCry

Policies you create with this template use CounterACT properties related to Windows registry keys, running services, and installed files to detect Windows endpoints infected with known variants of WannaCry/WannaCrypt malware.

- This policy uses the results of classification to detect endpoints.
  - In environments with Service Pack 2.3.x, verify that the Asset Classification policy is running.
  - In environments with Service Pack 3.0.0 and above, verify that the Primary Classification policy is running. Enable the optional **Add to Group** actions in the policy.
- This policy only evaluates endpoints managed by Remote Inspection or SecureConnector.
- WannaCrypt malware exploits a vulnerability in SMB connectivity, which was identified by Microsoft and published as MS17-010 in March 2017.

The policy provided in this release check for this vulnerability as part of endpoint evaluation - and can cause download of Microsoft vulnerability information to Windows endpoints.

WPA2 KRACK

Policies based on the following templates classify WiFi connected devices according to KRACK risk, based on the detected software release. Windows managed devices are checked for the Oct 2017 patch. See Remediating WPA2 KRACK on Wireless Controllers and Access Points for details about remediation of Wireless controllers and access points.

- You must install the latest release of the Advanced Tools Plugin to work with this template.
- You must install, configure and run Wireless Plugin 1.8.0 or above to work with this template. Install the latest available release or hotfix.
- This policy uses the results of classification to detect endpoints.
  - In environments with Service Pack 2.3.x, verify that the Asset Classification policy is running.
  - In environments with Service Pack 3.0.0 and above, verify that the Primary Classification policy is running.

VR WPA2 KRACK

Use this template in environments with Service Pack 3.0.0 or above.

VR WPA2 KRACK for SP 2.3.x

Use this template in environments with Service Pack 2.3.x.

- Your system must be running the Mobile Classification policy to work with this template.

Remediating WPA2 KRACK on Wireless Controllers and Access Points

Policies based on the VR WPA2 KRACK and the VR WPA2 KRACK for SP 2.3.x templates use the **WLAN Device Software** property provided by the Wireless Plugin to evaluate vulnerability to WPA2 KRACK malware. Risk is assessed based on the software release on the controller.

- ***For Cisco and Aruba controllers***, policy rules identify vulnerable devices based on currently known information about software releases.
  - Add policy actions to remediate devices that were found to be vulnerable.
  - In the Inventory view, examine policy results per rule.
- ***For controllers of other vendors***, follow this procedure:

  a. Create and run a policy based on one of the templates.

  b. CounterACT populates the Inventory view for the **WLAN Device Software** property.

c. In the Inventory view for this property, review the software releases that CounterACT detected on your controllers. Refer to manufacturer announcements of vulnerability and patch information for these software releases.

d. Use the **WLAN Device Software** property in policies you create to detect and remediate devices that run vulnerable software.

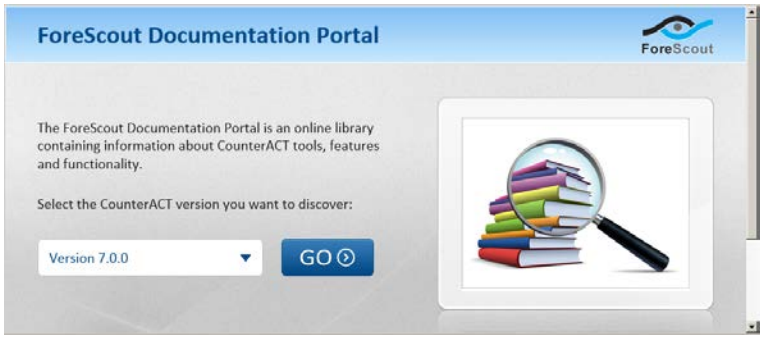
Additional CounterACT Documentation

For more detailed information about the CounterACT features described here or additional CounterACT features and modules, refer to the following resources:

- Documentation Portal
- Customer Support Portal
- CounterACT Console Online Help Tools

Documentation Portal

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



ForeScout Documentation Portal

The ForeScout Documentation Portal is an online library containing information about CounterACT tools, features and functionality.

Select the CounterACT version you want to discover:

To access the Documentation Portal:

1. Go to www.forescout.com/docportal.
2. Use your customer support credentials to log in.
3. Select the CounterACT version you want to discover.

Customer Support Portal

The Customer Support Portal provides links to CounterACT version releases, service packs, plugins and modules as well as related documentation. The portal also provides a variety of How-to Guides, Installation Guides and more. To access the Customer Support Portal, go to:

To access the Customer Support Portal:

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

CounterACT Console Online Help Tools

Access information directly from the CounterACT Console.

Console Help Buttons

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

Console User Manual

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

Plugin Help Files

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

Documentation Portal

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

Legal Notice

These products are based on software developed by ForeScout. The products described in this document may be protected by one or more of the following U.S. patents: #6,363,489, #8,254,286, #8,590,004, #8,639,800 and #9,027,079 and may be protected by other U.S. patents and foreign patents.

Redistribution and use in source and binary forms are permitted, provided that the above copyright notice and this paragraph are duplicated in all such forms and that any documentation, advertising materials and other materials related to such distribution and use acknowledge that the software was developed by ForeScout.

Unless there is another valid written agreement executed by you and ForeScout that governs the ForeScout products and services:

- If you have purchased any ForeScout products or services, your use of such products or services is subject to your acceptance of the terms set forth at http://www.forescout.com/eula/;
- If you have purchased any ForeScout support service (“ActiveCare”), your use of ActiveCare is subject to your acceptance of the terms set forth at http://www.forescout.com/activecare-maintenance-and-support-policy/;
- If you are evaluating ForeScout’s products, your evaluation is subject to your acceptance of the applicable terms set forth below:
    - If you have requested a General Availability Product, the terms applicable to your use of such product are set forth at: http://www.forescout.com/evaluation-license/.
    - If you have requested a Beta Product, the terms applicable to your use of such product are set forth at: http://www.forescout.com/beta-test-agreement/.
    - If you have purchased any ForeScout Not For Resale licenses, such license is subject to your acceptance of the terms set forth at http://www.forescout.com/nfr-license/.

Send comments and questions about this document to: documentation@forescout.com

2018-01-16 16:34