# Table of Contents

**About the CounterACT MVM Plugin** ............................................................... 4
  Additional CounterACT Documentation .......................................................... 4

**About this Plugin** .......................................................................................... 4
  Architecture – Concepts and Considerations ................................................... 5
  Concepts ........................................................................................................... 5
  Considerations ................................................................................................. 7
  What to Do ........................................................................................................ 7

**Requirements** ............................................................................................... 7
  CounterACT Software Requirements ............................................................. 8
  Supported Vendor Requirements ..................................................................... 8
  ForeScout Module License Requirements ....................................................... 8
    Requesting a License .................................................................................... 8
    More License Information ............................................................................ 9

**Install the Plugin** .......................................................................................... 9

**Map an SFTP Server to MVM** ..................................................................... 10

**Configure Scan Settings in MVM** ............................................................... 11
  Create CounterACT Scans in MVM ............................................................... 12
  Verify/Configure API Server Port ................................................................. 14

**Using Custom Certificates** ........................................................................... 15

**Configure the Plugin** .................................................................................. 16
  Configuring General MVM Settings ............................................................... 17
  Configuring MVM Enterprise Manager Details .............................................. 17
  Configuring SFTP Details for Scan Results .................................................... 18
  Configuring Advanced MVM Settings ........................................................... 19
  Configuring MVM Scan Engines .................................................................... 20
    Adding MVM Scan Engines ........................................................................ 20
    Mapping CounterACT Devices to MVM Scan Engines ............................... 20
  Configuring MVM Organizations .................................................................... 21
    Adding MVM Organizations ....................................................................... 21
    Assigning MVM Scan Engines to MVM Organizations .............................. 22

**Test the Plugin Configuration** ..................................................................... 23
Create Custom MVM Policies ................................................................. 23
  Detecting Vulnerabilities - MVM Policy Properties .......................... 24
    MVM Applied Tags Property ......................................................... 24
    MVM Connection is UP Property .................................................. 25
    MVM Scan Results Property .......................................................... 25
    MVM Scan Status Property ............................................................ 26
  Managing Vulnerabilities – MVM Policy Actions ............................... 27
    Start MVM Scan Action ............................................................... 27
    Apply MVM Tag Action ............................................................... 28
    Remove MVM Action ................................................................. 29

Displaying MVM Inventory Data .......................................................... 29

Additional CounterACT Documentation .............................................. 30
  Documentation Portal ................................................................. 30
  Customer Support Portal ............................................................. 31
  CounterACT Console Online Help Tools ......................................... 31
About the CounterACT MVM Plugin

McAfee Vulnerability Manager is a vulnerability and assessment product that features vulnerability analysis of your security posture.

The McAfee Vulnerability Manager (MVM) Plugin lets you harness CounterACT’s real-time network visibility for use in vulnerability assessment. The plugin lets you assimilate vulnerabilities management into the larger IT security process. Using the plugin, you can view information gathered from vulnerability scans side by side with other endpoint-related data from a single location. You can also share vulnerability data with other external security-oriented systems, such as SIEM or a central vulnerabilities management database.

Additional CounterACT Documentation

It is recommended that you have a basic understating of CounterACT policy and other basic features when working with this plugin. See Additional CounterACT Documentation for details about how to access information about CounterACT features.

About this Plugin

The plugin lets you integrate CounterACT with the MVM platform so that you can:

- Trigger MVM scan requests from CounterACT based on network activity detected by CounterACT. For example, using CounterACT policies, you can launch a scan on an endpoint following network admission, or if a specific application is installed on the endpoint. See Start MVM Scan Action.
- Use MVM properties to detect MVM scan information, connectivity to the MVM server, and applied MVM tags. For example, you can detect all endpoints that were assigned a critical risk factor. See Detecting Vulnerabilities - MVM Policy Properties.
- Create and apply MVM tags to organize endpoints with similar tags, reducing administrative overhead. For example, you can apply a Windows 7 Enterprise 64bit tag to a group of endpoints using the Apply MVM Tag action. You can then trigger a weekly scan in MVM using the Start MVM Scan action, which will apply to the group of tagged endpoints. See Apply MVM Tag Action and MVM Applied Tags Property.
- Use the CounterACT inventory to see which endpoints have been identified as vulnerable by the plugin. For example, browse the inventory to learn what CVEs have been detected on your network, and acquire information about endpoints with similar findings. See Displaying MVM Inventory Data.
You can create CounterACT reports that provide detailed information about endpoints with specific MVM-detected vulnerabilities. For example you can create a Policy Status Report to display the number of matched and unmatched hosts detected for each MVM policy and sub-policy.

Refer to the CounterACT Console User Manual for more information about the inventory and report features. See Additional CounterACT Documentation for details.

To use the plugin, you should have a solid understanding of MVM concepts, components, functionality and terminology.

Architecture – Concepts and Considerations

This section provides a basic overview of MVM / CounterACT architecture:

- **Concepts** – basic integration concepts.
- **Considerations** – setup details and common network structure issues to keep in mind when you implement this plugin.

**Concepts**

You should be familiar with MVM components when using the McAfee Vulnerability Manager Plugin. Understanding these components is necessary for a successful integration.

**Mapping CounterACT Devices to MVM Scan Engines**

The plugin lets you map CounterACT devices to MVM scan engines in order to share MVM scan data with CounterACT and perform MVM related actions on endpoints detected by CounterACT. MVM scan engines are assigned to MVM organizations. You can access multiple MVM organizations in parallel through the plugin to integrate more than one vulnerability management workspace with CounterACT.

When you create a scan in MVM, you assign a scan engine to perform the scan on a range of defined endpoints. Use the plugin to virtually map a particular CounterACT device to the same range of endpoints covered by a particular MVM scan engine.
Verify that the MVM scan engine is accessible to the IP address range that the mapped CounterACT device handles. You can assign multiple CounterACT devices to the IP address range covered by a single MVM scan engine.

The Start MVM Scan, Apply MVM Tag and Remove MVM Tag actions are only applied to endpoints that are assigned to a CounterACT device mapped to an MVM Scan Engine which is in turn assigned to an MVM Organization. To see IP address assignments to CounterACT devices, select Tools > Options > CounterACT Devices in the Console and review the Assigned IPs.

**Communication with MVM Enterprise Manager**

The MVM Enterprise Manager is the single interface for all API calls to and from all MVM scan engines. A single CounterACT device must be defined as the connecting device for communication between CounterACT devices and the MVM Enterprise Manager. This proxy topology lets the McAfee Vulnerability Manager Plugin control the query rate and requests from CounterACT to the MVM Enterprise Manager. This prevents flooding the MVM Enterprise Manager with API calls from each CounterACT device, ensures more efficient traffic control, and lowers maintenance requirements.

The connecting CounterACT device maintains a message queue for commands that are directed to it from the other CounterACT devices. You can set a time threshold for sending commands so that the connecting CounterACT device can properly manage the queue. See Configuring Advanced MVM Settings for details.

**MVM Scan Results**

MVM scan results are generated by the MVM report service into a network folder that is mapped to an SFTP server. The plugin retrieves detailed scan results from the
CounterACT™ McAfee Vulnerability Manager Plugin

Configuration Guide

Version 1.1.0 and Above

Considerations

Consider the following when mapping CounterACT devices to MVM scan engines:

**Timing:** The plugin is configured to handle network traffic and carry out other tasks with default thresholds. Based on network activity or other requirements, you may need to update these defaults. It is advised to review the scan engine performance over an extended period to optimize settings for reducing scan engine load, on the one hand, and minimizing scan latency on the other. See Configuring Advanced MVM Settings for details.

**Match IP Address Ranges:** Verify that the MVM scan engine is accessible to the IP address range that the mapped CounterACT device handles. See Mapping CounterACT Devices to MVM Scan Engines for details. To see IP address assignments to CounterACT devices, select Tools > Options > CounterACT Devices in the Console and review the Assigned IPs to open the IP Assignment pane. Refer to the section on IP Assignments in the CounterACT Console User Manual for more information.

What to Do

You must perform the following to work with this plugin:

- Verify that requirements are met. See Requirements.
- Download and install the plugin. See Install the Plugin.
- Configure and map an SFTP Server to MVM. See Map an SFTP Server to MVM.
- Configure Scan Settings in MVM. See Configure Scan Settings in MVM.
- Create and store McAfee Foundstone certificates. See Using Custom Certificates.
- Configure MVM connection parameters and plugin settings. See Configure the Plugin.
- Use MVM properties and actions in custom policies. See Create Custom MVM Policies.

Requirements

This section describes:

- CounterACT Software Requirements
- Supported Vendor Requirements
- ForeScout Module License Requirements
CounterACT™ McAfee Vulnerability Manager Plugin   Configuration Guide

CounterACT Software Requirements
The following CounterACT releases can work with this plugin

- CounterACT version 7.0.0, running Hotfix 1.6.1 or above.

Supported Vendor Requirements
The McAfee MVM Plugin supports McAfee Vulnerability Manager Version 7.5 and above.

- Verify that your CounterACT devices and their peered MVM scan engines regularly sync the same NTP server.
- Configure an SFTP server to allow CounterACT to retrieve scan results from MVM Enterprise Manager.

ForeScout Module License Requirements
This plugin is packaged as a ForeScout Module, and requires a module license. When installing the plugin you are provided with a 90-day demo module license.

If you would like to continue exploring the module before purchasing a permanent license, you can request a demo license extension. Consult with your ForeScout representative before requesting the extension. You will receive email notification and alerts at the Console before the demo period expires.

When the demo period expires, you will be required to purchase a permanent module license. In order to continue working with the plugin, you must purchase the license.

Demo license extension requests and permanent license requests are made from the CounterACT Console.

This plugin may have been previously packaged as a component of an Integration Module which contained additional plugins. If you already installed this plugin as a component of an Integration Module, you can continue to use it as such. Refer to the section about module packaging in the CounterACT Console User Manual for more information.

Requesting a License
When requesting a demo license extension or permanent license, you are asked to provide the device capacity requirements. This is the number of devices that you want this license to handle. You must define at least the number of devices currently detected by CounterACT. You can request a license that handles more to ensure that you are licensed for support on additional devices as your deployment grows.

Enter this number in the Devices pane of the Module License Request wizard, in the CounterACT, Console Modules pane.
To view the number of currently detected devices:

1. Select the NAC tab.

2. In the Views pane, select the All Hosts folder. The number in parentheses displayed next to the All Hosts folder is the number of devices currently detected.

More License Information

See the CounterACT Console User Manual for information on requesting a permanent license or a demo license extension. You can also contact your ForeScout representative or license@forescout.com for more information.

Install the Plugin

This section describes how to download and install the plugin.

To install the plugin:

1. Acquire a copy of the plugin in either one of the following ways:
If you are installing a Beta release of this plugin, acquire the plugin .fpi file from your ForeScout representative or contact beta@forescout.com. Otherwise, navigate to the Customer Support ForeScout Modules 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.


5. Select Install. The Open dialog box opens.

6. Browse to and select the saved plugin .fpi file.

7. Select Install.

8. If you have not yet purchased a permanent module license, a message appears indicating that the plugin will be installed with a demo module license. Select Yes and then select Install.

9. An installation or upgrade information dialog box and a license agreement dialog box will open. Accept the license agreement to proceed with the installation.

10. Once the installation is complete, select Close. The plugin is listed in the Plugins pane. The Module Status column indicates the status of your license. See ForeScout Module License Requirements and the CounterACT Console User Manual for information on requesting a permanent license or a demo license extension.

11. Select the plugin and select Start. The Select Appliances dialog box opens.

12. Select the CounterACT devices on which to start the plugin.

13. Select OK. The plugin runs on the selected devices.

Map an SFTP Server to MVM

In order to access scan results for scans initiated by the plugin, you need to configure a remote SFTP server, map the SFTP server to MVM and configure the
relevant settings in the plugin. This ensures that scan results are sent to the designated SFTP server in an asynchronous manner. See Configuring SFTP Details for Scan Results for details.

**To map an SFTP Server to MVM:**
1. Open Foundstone Configuration Manager.
2. Select **Tools > Preferences > Report Server**.

3. Select the **Copy Reports to Network Drive** checkbox.
4. Ensure that the value in the Network Drive field is mapped to the **Server Directory** and **Address** fields in the MVM Plugin. See Configuring SFTP Details for Scan Results for details.

**Configure Scan Settings in MVM**

You must make several initial configurations in McAfee Vulnerability Manager before you can integrate it with the McAfee Vulnerability Manager Plugin.

For example:
- **Set up MVM Organizations.** Any relevant organizations must be defined in MVM before you can integrate them with the McAfee Vulnerability Manager Plugin. You can choose to create dedicated MVM organizations to use with the plugin or use existing MVM organizations. See Adding MVM Organizations for details.

- **Assign user to CounterACT scans.** Assign or create a dedicated MVM user account for CounterACT. This is performed in the Users/Groups section of the MVM Global Admin page. The user needs to have full access permissions to the relevant CounterACT scans.

- **Create CounterACT-dedicated scans.** After you define scans in MVM you can integrate them with the plugin and use them in MVM properties and actions in CounterACT. See Create CounterACT Scans in MVM and Create Custom MVM Policies for details.

- **Verify/Configure API Server Port.** Verify the port number that the plugin uses to connect to the MVM Enterprise Manager. You may choose to edit the default value. See Verify/Configure API Server Port.

### Create CounterACT Scans in MVM

You must define scans in MVM in order to integrate them with the McAfee Vulnerability Manager Plugin and use them in MVM properties and actions in CounterACT. It is recommended that these scans be dedicated to CounterACT.

Some of the scan settings you configure in MVM are overridden by the plugin. While you may need to enter values for these settings in MVM to complete the scan creation process, the actual settings for the scan are taken from the plugin configuration.

**To create a CounterACT scan in MVM:**

1. In the MVM Org Admin view, select **Scans > New Scan.**

2. Select a base setting for your scan and select **Next.**

3. In the Targets tab:
   - Enter a name for the scan. It is recommended to include ‘CounterACT’ in the name to identify the scan.
   - (Optional) Add a description to further identify the scan as relevant to CounterACT. This information is not extracted to the plugin.
− Select a placeholder IP address or range. The value you select here is not used in the scan, because it is overridden by CounterACT settings.
− Select Next.

4. In the Settings tab, select the relevant vulnerability settings.

5. Select Next. The settings should be configured like any other scan. CounterACT extracts these settings as defined in MVM. Consult McAfee Vulnerability Manager Help for more information.

6. In the Reports tab:
− In the Foundscore Type section, select Internal Network.
− In the Reporting Options section, select the XML Report checkbox and clear any other checkboxes in this section.

− Select Next.

7. In the Scheduler tab, perform the following:
In the Activation section, select **Inactive**.

From the Select Engine dropdown menu, select a scan engine.

In the Schedule Type section, select **Immediate**.

The scan engine selected in the Select Engine menu is not used in the scan, because it is overridden by the settings defined in the McAfee Vulnerability Manager Plugin, according to the mapping between CounterACT devices and MVM scan engines. See Mapping CounterACT Devices to MVM Scan Engines for details.

8. Select **Save**.

**Verify/Configure API Server Port**

Verify the port number that the plugin uses to connect to the MVM Enterprise Manager.

**To verify the port:**

1. In the FCM Console, select **Tools > Preferences**.
2. Select the **API Server** tab.
3. In the Incoming Connection section, verify the custom port value. The default value is 3800. This value is needed when configuring the plugin. See Configuring MVM Enterprise Manager Details.
4. (Optional). Select the **Use custom port** checkbox to configure the value. If you change the default value, verify that you do not use a port number that is used for MVM communication. For example, port 3801 is used for communication between the FCM Agent and the Configuration Manager server. Consult McAfee documentation for a complete list of used ports.

### Using Custom Certificates

In order for MVM to validate the CounterACT client connection, you must create custom certificates using the Foundstone Certificate Management Tool, run OpenSSL and generate a certificate with no passphrase, and then store the relevant files in the certificate folder of the Connected CounterACT device.

Have the address or host name of the Connected CounterACT device ready before you begin. See [Configuring MVM Enterprise Manager Details](#).

Perform these tasks before starting the plugin for the first time or when the Connected CounterACT device settings are changed.

Refer to the McAfee Vulnerability Manager SSL and Certificate Management Tools document for more information about using custom certificates.

**To use custom certificates:**

1. Run *Foundstone Certificate Manager.exe* on the server that is running the Foundstone Certificate Management Tool.

2. Select the **Create SSL Certificates** tab.

3. In the Host Address field, enter the address or host name of the Connected CounterACT device.

4. Select **Create Certificate using Common Name**.

5. Type the location for the zip file when prompted by the Save As dialog. This file will contain all generated custom certificates in compressed form.
The passphrase for new custom certificates is generated and displayed in the *Your Passphrase:* box. Copy and save it because you will need this passphrase to decrypt some of the custom certificates.

6. Extract the custom certificates from the zip file to the CertificateStore directory on the MVM server.

   The CertificateStore directory is located in the FCM folder. For example:
   
   C:\Program Files (x86)\Foundstone\FCM\CertificateStore

7. Access the following directory in the Connected CounterACT device:

   /usr/local/forescout/plugin/mvm/cert/

   This directory is automatically created when the plugin is installed.

8. Store the following certificates in the above directory:

   - FoundstoneCAPublicCertificate.pem
   - FoundstoneClientCertificate.pem

**To remove the pass phrase from the private key certificate file:**

1. Run the openssl.exe provided by McAfee.

2. Run the following OpenSSL command in the CertificateStore directory:

   OpenSSL> rsa -in FoundstoneClientCertificate.pem -out ClientKeyNoPass.pem

   The CertificateStore directory is located in the FCM folder. For example:
   
   C:\Program Files (x86)\Foundstone\FCM\CertificateStore

3. Type the saved passphrase for FoundstoneClientCertificate.pem.

4. Run the OpenSSL exit command to end this operation:

   OpenSSL> exit

5. Use SSH to store the following file in the

   /usr/local/forescout/plugin/mvm/cert/ directory of the Connected CounterACT device:

   - ClientKeyNoPass.pem

---

**Configure the Plugin**

Configure the plugin to define the MVM components that the plugin communicates with. These components include the MVM Enterprise Manager, SFTP settings (for scan results), MVM organizations and scan engines. You can assign scan engines to MVM organizations and map CounterACT devices to scan engines.

You can also define settings that manage plugin operational thresholds. For example, configure the volume of requests submitted by CounterACT to the MVM Enterprise Manager.

Before configuring the plugin, review the section on [Architecture – Concepts and Considerations](#).
To configure the plugin:

1. In the CounterACT Console, select **Options** from the **Tools** menu. The Options dialog box opens.

2. Navigate to and select the **Plugins** folder.

3. In the **Plugins** pane, select **McAfee Vulnerability Manager**, and select **Configure**. The McAfee Vulnerability Manager pane opens.

### Configuring General MVM Settings

Use the General tab to configure MVM details, the Connected CounterACT device, SFTP details for scan results and advanced scan processing thresholds.

- **Configuring MVM Enterprise Manager Details**
- **Configuring SFTP Details for Scan Results**
- **Configuring Advanced MVM Settings**

### Configuring MVM Enterprise Manager Details

The MVM Enterprise Manager is the single interface for all API calls to and from all MVM scan engines. A single CounterACT device must be defined as the connecting device for communication between CounterACT devices and the MVM Enterprise Manager.

**To configure MVM Enterprise Manager Details:**

1. In the McAfee Vulnerability Manager pane, select the **General** tab and then select the **MVM-EM** tab.

2. Configure the following connection parameters:

<table>
<thead>
<tr>
<th>Address</th>
<th>IP address of an MVM Enterprise Manager that will act as the single interface for all API calls to and from all MVM scan engines.</th>
</tr>
</thead>
</table>
Port | Port used to access the MVM Enterprise Manager. By default, this is port 3800. See Verify/Configure API Server Port for details.

Connected CounterACT Device | The CounterACT device used to communicate with the defined MVM Enterprise Manager. This CounterACT device manages all communication with the defined MVM Enterprise Manager, including forwarding scan requests submitted to it by other CounterACT devices and dispatching scan results received back to the appropriate CounterACT devices.

---

**Configuring SFTP Details for Scan Results**

Configure SFTP server details to send results from scans initiated by the plugin to a remote SFTP server. The plugin connects to the SFTP server at a predefined interval to check for new scan results.

**To configure SFTP Details for Scan Results:**

1. In the McAfee Vulnerability Manager pane, select the **General** tab and then select the **Scan Results** tab.

2. Configure the following connection parameters:

   **Server Address** | The IP address of the SFTP server.

   **User Name** | The User Name for accessing the SFTP server.

   **Password** | The password for the above user. Retype the password to confirm it.

   **Directory** | The directory of the SFTP server.

   **Report Name Pattern** | (Optional) A report name pattern from MVM for any additional MVM Scan Result reports that you want to send to the SFTP server.
Configuring Advanced MVM Settings

Configure settings that the plugin uses to optimize its processing of scan jobs that it sends to the MVM Enterprise Manager. A scan job is a collection of host scan requests.

To configure advanced MVM Settings:

1. In the McAfee Vulnerability Manager pane, select the **General** tab and then select the **Advanced** tab.

2. Configure the following connection parameters:

| **MVM scan threshold period (seconds)** | The time to wait, in seconds, for new host scan requests. During this time, the plugin receives scan requests and adds them to the scan job queue. When this period expires, the plugin sends the collected scan requests in a scan job to the MVM Enterprise Manager. The default value is 10.
| If the **Minimum Number of Hosts to Expedite Scan Job** value is reached before the **MVM scan threshold period**, this value is not used. |
| **Minimum Number of Hosts to Expedite Scan Job** | The minimum number of host scan requests that, if reached in queue during an **MVM scan threshold period**, triggers the plugin to issue scan jobs. The default value is 10.
| During a collection interval, host scan requests, generated by both policy and manual actions are added by the plugin to its scan job queue. When the queue reaches the value defined in this field, the plugin submits one or more expedited scan jobs, as needed, to the MVM Enterprise Manager.
| If the **MVM scan threshold period** value is reached before the **Minimum Number of Hosts to Expedite Scan Job**, this value is not used. |
Configuring MVM Scan Engines

Use this tab to define scan engines and to map CounterACT devices to scan engines. An MVM scan engine is a service controlled by the MVM Enterprise Manager that performs a defined scan on scan targets. One or more scan engines are assigned to an MVM organization by the global administrator.

Adding MVM Scan Engines

Define scan engines that will perform vulnerability assessment activities on endpoints detected by CounterACT.

To add MVM Scan Engines:

1. In the McAfee Vulnerability Manager pane, select the Scan Engines tab.

2. Select Add.

3. Enter the Engine Name and select OK.
   
The Scan Engine appears in the Engine Name pane.

Mapping CounterACT Devices to MVM Scan Engines

Mapped CounterACT devices communicate with MVM Scan Engines through the Connected CounterACT device. You can map multiple CounterACT devices to a single MVM scan engine.

Verify that the MVM scan engine is accessible to the IP address range that the mapped CounterACT device handles.

You must select Apply after mapping CounterACT devices for the Scan Engines to be updated in the Organizations tab.

To map CounterACT Devices to MVM Scan Engines:

1. In the McAfee Vulnerability Manager pane, select the Scan Engines tab.

2. Select Map....
3. Select a CounterACT device from Available Appliances, select a Scan Engine from Mapped Appliances, and then select Add.

4. Select OK.

Configuring MVM Organizations

Use this tab to define MVM organizations and to assign scan engines to MVM organizations. An MVM organization is a vulnerability management workspace in which scans are created and launched, scan reports are generated and distributed, and tickets are managed.

Adding MVM Organizations

Add MVM organizations in the plugin to define vulnerability management workspaces.

To add MVM Organizations:

1. In the McAfee Vulnerability Manager pane, select the Organizations tab.

2. Select Add.
3. Configure the following connection parameters:

<table>
<thead>
<tr>
<th>Organization Name</th>
<th>The name of the MVM vulnerability management workspace in which scans are created and launched, scan reports are generated and distributed, and tickets are managed.</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Name</td>
<td>The user name associated with the MVM Organization. This user must have public and read table permissions.</td>
</tr>
<tr>
<td>Password</td>
<td>Password for the above user. Retype the password to confirm it.</td>
</tr>
</tbody>
</table>

4. Select OK.

Assigning MVM Scan Engines to MVM Organizations

You can assign one or more scan engines to an MVM organization.

To assign MVM Scan Engines to MVM Organizations:

1. In the McAfee Vulnerability Manager pane, select the Organizations tab.
2. Select Assign....

3. Select a Scan Engine and an Organization and then select Add.
4. Select OK.
Test the Plugin Configuration

This section describes how to perform a configuration test. The test checks the credentials of MVM organizations defined in the plugin.

To run a test:
1. In the McAfee Vulnerability Manager pane, select the Organizations tab.
2. In the Organization pane, select the organization you want to test and select Test.
3. Select Close.

Create Custom MVM Policies

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

Properties
CounterACT policy properties let you instruct CounterACT to detect hosts with specific attributes. For example, create policy that instructs CounterACT to detect hosts running a certain Operating System or with a certain application installed.

Actions
CounterACT policy actions let you instruct CounterACT how to control detected devices. For example, assign detected device to an isolated VLAN or send the device user or IT team an email.

In addition to the bundled CounterACT properties and actions available for detecting and handling endpoints, you can work with MVM related properties and actions to create the custom policies. These items are available when you install the plugin.

For more information about working with policies, select Help from the custom policy wizard.

To create a custom policy:
1. Log in to the CounterACT Console.
2. On the Console toolbar, select the Policy tab. The Policy Manager opens.
3. Select Add to create a policy.
Detecting Vulnerabilities - MVM Policy Properties

This section describes the properties that are made available when the McAfee Vulnerability Manager Plugin is installed.

For example, you can use MVM properties in custom policies to detect the current MVM risk rating results and then you can organize endpoints into CounterACT groups with critical, high, medium, low or no risk ratings. You can then use these groups in CounterACT policies to control endpoints by applying relevant actions according to risk levels. For example, you can assign endpoints with critical risk ratings to an isolated VLAN.

To access MVM properties:

1. Navigate to the Properties tree from the Policy Conditions dialog box.
2. Expand the MVM folder in the Properties tree. The following properties are available:
   - MVM Applied Tags Property
   - MVM Connection is UP Property
   - MVM Scan Results Property
   - MVM Scan Status Property

MVM Applied Tags Property

Indicates tags that were applied to hosts, either by CounterACT or within the MVM Management Console.
MVM Connection is UP Property
Indicates that the plugin can communicate with the MVM server and responds to CounterACT requests.

MVM Scan Results Property
Indicates specific scan results for an endpoint based on an MVM scan template. Endpoints will be marked as unmatched for this property until CounterACT retrieves scan results on the SFTP server. See Configuring SFTP Details for Scan Results for details.

<table>
<thead>
<tr>
<th>Vulnerability Name</th>
<th>The vulnerability synopsis. For example, Microsoft Windows IP Forwarding Enabled Security Bypass Vulnerability.</th>
</tr>
</thead>
<tbody>
<tr>
<td>CVE</td>
<td>The Common Vulnerabilities and Exposures (CVE) ID. For example, CVE-1999-0511.</td>
</tr>
<tr>
<td>Vulnerability Description</td>
<td>The description of the vulnerability.</td>
</tr>
</tbody>
</table>
### Risk Rating
The vulnerability risk rating.
- Low
- Medium
- High
- Critical

### Scan completion time
The date and time when the scan completed.

### Scan name
The scan configuration template name that was used for this scan. For example, Windows Desktop non-intrusive.

### MVM Scan Status Property
Indicates the scan status details on an endpoint for one or more property values or for all property values.

**Scan name**
The scan configuration template name that was used for this scan. For example, Windows Desktop non-intrusive.

**Scan State**
The following statuses exist:
- Canceled
- Canceling
- Complete
- Completing
- Error
- Initializing
- License Violation
- Paused
- Paused for pending
- Pending
- Running Discovery
### Managing Vulnerabilities – MVM Policy Actions

This section describes the actions that are made available when the McAfee Vulnerability Manager Plugin is installed.

**To access MVM actions:**

1. Navigate to the Actions tree from the Policy Actions dialog box.
2. Expand the MVM folder in the Actions tree. The following actions are available:
   - Start MVM Scan Action
   - Apply MVM Tag Action
   - Remove MVM Action

### Start MVM Scan Action

This action lets you trigger a new vulnerability scan to launch when certain policy conditions are met. For example, you can create a policy that detects if certain applications were installed on endpoints or certain registry keys were changed, and trigger the scan when a host meets this condition.

You can automate and optimize the scanning process according to endpoint detection, classification policies and other endpoint properties available in CounterACT. By controlling the frequency and scheduling of scans (using the action’s Schedule tab), you can save valuable network resources and reduce network congestion.

![Start MVM Scan Action](image)

The following parameters are available:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scan Start Time</td>
<td>The start time of the scan.</td>
</tr>
<tr>
<td>Scan Engine ID</td>
<td>The ID of the scan engine that scanned the host.</td>
</tr>
</tbody>
</table>

#### Managing Vulnerabilities – MVM Policy Actions

**To access MVM actions:**

1. Navigate to the Actions tree from the Policy Actions dialog box.
2. Expand the MVM folder in the Actions tree. The following actions are available:
   - Start MVM Scan Action
   - Apply MVM Tag Action
   - Remove MVM Action

**Start MVM Scan Action**

This action lets you trigger a new vulnerability scan to launch when certain policy conditions are met. For example, you can create a policy that detects if certain applications were installed on endpoints or certain registry keys were changed, and trigger the scan when a host meets this condition.

You can automate and optimize the scanning process according to endpoint detection, classification policies and other endpoint properties available in CounterACT. By controlling the frequency and scheduling of scans (using the action’s Schedule tab), you can save valuable network resources and reduce network congestion.

![Start MVM Scan Action](image)

The following parameters are available:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scan Start Time</td>
<td>The start time of the scan.</td>
</tr>
<tr>
<td>Scan Engine ID</td>
<td>The ID of the scan engine that scanned the host.</td>
</tr>
</tbody>
</table>
**Apply MVM Tag Action**

This action lets you apply an MVM tag to an endpoint to group endpoints together logically, reducing administrative overhead. Multiple tags can be applied to an asset, or multiple assets, to help narrow the search when looking for specific assets. For example, using multiple asset tags, administrators can tag all Windows assets that belong to the finance department located in North America. You cannot apply MVM tags to an endpoint that has not been scanned by MVM.

The following parameters are available:

<table>
<thead>
<tr>
<th><strong>MVM Organization Name</strong></th>
<th>The name of the MVM vulnerability management workspace, as defined in the plugin. See Adding MVM Organizations.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>MVM Tag Name</strong></td>
<td>The name of the MVM asset tag. You can use these tags to organize assets within an organization. Tags can be created based on an operating system, department or even location. Multiple tags can be applied to an asset, or multiple assets, to help narrow the search when looking for specific assets.</td>
</tr>
</tbody>
</table>
Remove MVM Action

This action lets you remove an MVM tag that was applied to a host.

![Diagram of Remove MVM Action]

The following parameters are available:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MVM Organization Name</td>
<td>The name of the MVM vulnerability management workspace, as defined in the plugin. See Adding MVM Organizations.</td>
</tr>
<tr>
<td>MVM Tag Name</td>
<td>The name of the MVM asset tag. You can use these tags to organize assets within an organization. Tags can be created based on an operating system, department or even location. Multiple tags can be applied to an asset, or multiple assets, to help narrow the search when looking for specific assets.</td>
</tr>
</tbody>
</table>

Displaying MVM Inventory Data

Use the CounterACT Inventory to view a real-time display of MVM scan results at multiple levels, for example, vulnerability name, risk rating, or scan completion time.

The inventory lets you:

- Broaden your view of the organizational network from endpoint-specific to activity-specific
- View endpoints that have been detected with specific attributes
- Easily track network activity
- Incorporate inventory detections into policies

**To access the inventory:**

1. Select the **Inventory** tab from the Console toolbar.
2. Navigate to the MVM entries.
The following information, based on MVM endpoint properties, is available:

- **MVM Scan Results:** View scan details, including the vulnerability name, CVE, risk rating and scan completion time.

Refer to *Working at the Console>*Working with Inventory Detections* in the *CounterACT Console User Manual* or the Console Online Help for information about how to work with the CounterACT Inventory.

### Additional CounterACT Documentation

For more detailed information about the CounterACT features described here or additional CounterACT features and plugins, 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 and functionality and integrations.
To access the Documentation Portal:
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:
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
1. 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
1. Select Documentation Portal from the Help menu.
Legal Notice

Copyright © ForeScout Technologies, Inc. 2000-2016. All rights reserved. The copyright and proprietary rights in this document belong to ForeScout Technologies, Inc. ("ForeScout"). It is strictly forbidden to copy, duplicate, sell, lend or otherwise use this document in any way, shape or form without the prior written consent of ForeScout. All other trademarks used in this document are the property of their respective owners.

These products are based on software developed by ForeScout. The products described in this document are protected by 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 a valid written agreement signed by you and ForeScout that governs the below ForeScout products and services:

- If you have purchased any ForeScout products, your use of such products is subject to your acceptance of the terms set forth at http://www.forescout.com/eula/;
- If you have purchased any ForeScout products, your use of such products 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 have purchased any ForeScout products, your use of such products is subject to your acceptance of the terms set forth at http://www.forescout.com/eula/;
- 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 an Early Availability Product, the terms applicable to your use of such product are set forth at: http://www.forescout.com/early-availability-agreement/.
  - 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

2016-05-04 10:45