

**McAfee Security Connected**  
*Integrating ePO and MVM*



<b>Table of Contents</b>	
<b>Overview</b>	<b>3</b>
<b>User Accounts &amp; Privileges</b>	<b>3</b>
<b>Prerequisites</b>	<b>3</b>
<b>Configuration Steps</b>	<b>3</b>
<b>Optional Configuration Steps for McAfee Risk Advisor 2.7.2</b>	<b>6</b>
<b>Value Add</b>	<b>7</b>

## Overview

Integration between McAfee ePO 5.0.1 and McAfee MVM 7.5. Adds the ability to pull MVM scan data into ePO along with MVM asset information.

## User Accounts & Privileges

Administrative rights to McAfee ePO & MVM.

Access to the Operating Systems, Databases, and Application Consoles.

## Prerequisites

Download the MVM 7.5 ePO Extension.

## Configuration Steps

1. Log in to the ePO Server as administrator (OS Log in)
2. Locate the MVM\_750\_ePO50Extension.zip file.
  - a. Download from the McAfee download site with a valid Grant Number.
3. Unzip the extension file
4. Run Setup.exe
  - a. Once all required applications are found click Next
  - b. Enter the ePO Global Administrator User Name and Password → Next

McAfee Vulnerability Manager ePO Extension 7.5.0

**McAfee**

**Set Administrator Information**

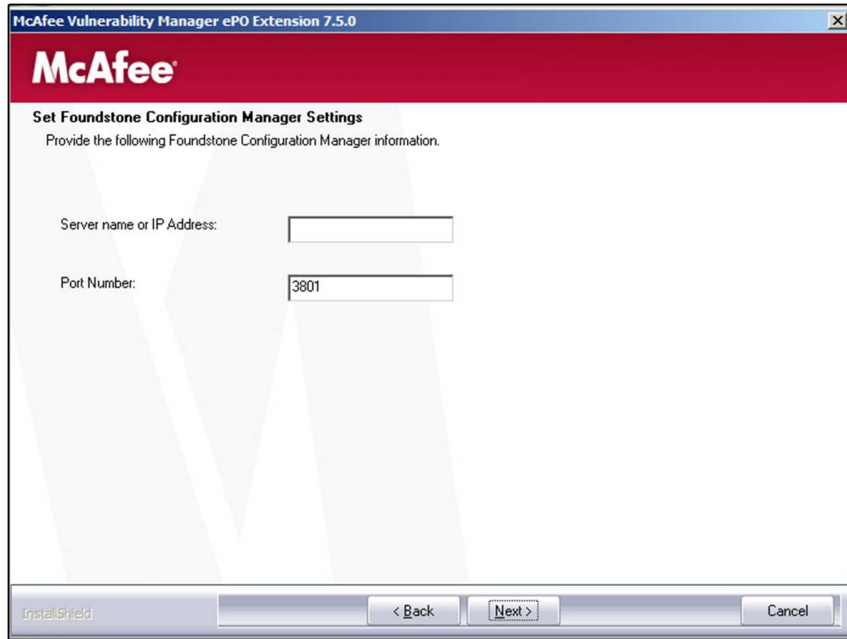
Enter an ePolicy Orchestrator global administrator user name and password. This is required in order to install Vulnerability Manager ePO Extension properly.

User name:

Password:

InstallShield

- c. Enter the IP Address of the MVM Server → Next
- d. Enter the Port Number (default 3801)



The image shows a Windows-style dialog box titled "McAfee Vulnerability Manager ePO Extension 7.5.0". The McAfee logo is at the top. Below it, the text reads "Set Foundstone Configuration Manager Settings" and "Provide the following Foundstone Configuration Manager information." There are two input fields: "Server name or IP Address:" which is empty, and "Port Number:" which contains the value "3801". At the bottom, there are four buttons: "InstallShield" (disabled), "< Back", "Next >" (highlighted), and "Cancel".

- e. Click Next to begin the installation then click Finish
- 5. Log in to the ePO Application Console with the Global Administrator Account



The image shows the login screen for "ePolicy Orchestrator 5.0". The title bar says "Log On to ePolicy Orchestrator". The McAfee logo is in the top right. The main heading is "ePolicy Orchestrator 5.0". There are three input fields: "User name:" (empty), "Password:" (empty), and "Language:" (set to "English" with a dropdown arrow). At the bottom, there is a "Log On" button and a copyright notice: "Copyright 2008-2013 McAfee, Inc. All Rights Reserved."

- 6. Browse to Menu → Registered Servers
- 7. Select New Server

8. Select MVM as the Server type and Enter a Name for the MVM Server → Next

Registered Server Builder	1 Description
<b>Server type:</b>	MVM
<b>Name:</b>	MVM 7.5
<b>Notes:</b>	

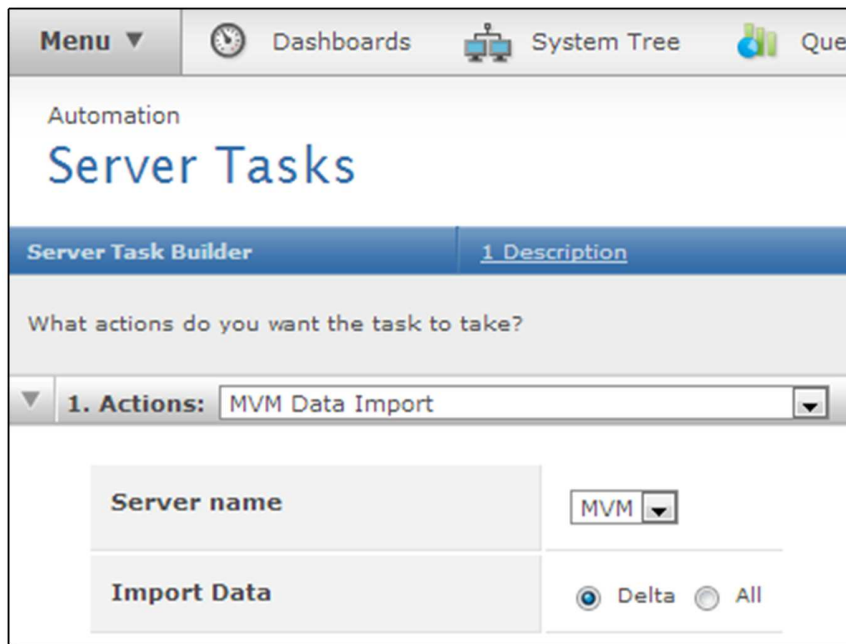
9. Enter the Database IP Address or Host Name for the MVM database
10. Keep Default selected for Server Instance
11. Enter the Database name. (MVM default is faultline)
12. Select Authentication Type Windows Authentication
13. Enter the user name for the Windows Authentication
  - a. Note: Workgroup servers should use the server name\username format.  
Workgroup\username will not work most likely
  - b. Note: Domain servers should use domain\username format
14. Enter the password for the user
15. Select the Organization check box and enter the organization name used for the MVM Server
  - a. Selecting Organization will import all assets discovered by MVM to the ePO server.
  - b. Optional: Select Import assets from ePO data source and Import assets from asset tag (these are not covered in this document)

Registered Server Builder	1 Description	2 Details
<b>Database server:</b>	192.168.1.20	(Host name or IP address)
<b>Server instance:</b>	<input checked="" type="radio"/> Default <input type="radio"/> Instance name: <input type="text"/> <input type="radio"/> Port number: <input type="text"/>	
<b>Require SSL connection:</b>	<input checked="" type="checkbox"/>	
<b>Database name:</b>	faultline	
<b>Authentication type:</b>	<input checked="" type="radio"/> Windows authentication <input type="radio"/> SQL authentication	
<b>User name:</b>	mvm\administrator (For Windows authentication: domain\user)	
<b>Password:</b>	*****	
<b>Confirm password:</b>	*****	
<b>Asset Filters:</b>	<input checked="" type="checkbox"/> Organization: MyCompany <input type="checkbox"/> Import assets from ePO data source: <input type="text"/> <input type="checkbox"/> Import assets from asset tag: <input type="text"/> <input type="checkbox"/> Import only the tagged assets that are unrelated to ePO data sources	

16. Click Test Connection.
17. If the Connection is successful click Save



18. Browse to Menu → Server Tasks
19. Locate the task MVM: Maintain association between MVM and ePO
20. Ensure that task is enabled
21. Click New Task at the bottom of the console
22. Name the task MVM Data Import → Next
23. Select MVM Data Import from the Actions Drop Down
  - a. Select the Server Name
  - b. Select Delta



24. Click Next
25. Schedule the task to run at a desired time → Next → Save

### Optional Configuration Steps for McAfee Risk Advisor 2.7.2

1. Install McAfee Risk Advisor (Not Covered in this document)
2. Deploy the McAfee Application Inventory Agent bundled with MRA 2.7.2
3. Schedule application data collection from the McAfee Application Inventory Agent
  - a. The default policy will collect data from endpoints every day
  - b. Select systems in the system tree then Actions → Application Inventory → Collect Application Data Now to pull data on demand
4. Browse to Menu → Server Tasks
  - a. Enable server task MRA Threat Download and Analysis
  - b. Enable server task MRA Reporting Group Analysis
5. Countermeasure "What-if Risk Analysis" can be measured
6. Browse to Menu → Risk Metrics
7. Apply a countermeasure product → Click Apply and Analyze → Latest "After Analysis" results

- The system will provide metrics on how the system(s) risk score will decrease after deploying products. MVM helps this effort by providing MRA risk information about systems in the environment.

Metrics	Before Analysis	After Analysis
Risk Score for Selected Assets:	12	9.8 ( ↓ -18.25% )
Risk Category:	Low	Low
Number of Threats To Mitigate:	5675	4587

## Value Add

The systems discovered by McAfee Vulnerability Manager using the Discovery Scan and imported to the ePolicy Orchestrator database can be organized using the System Tree groups and subgroups. An efficient and well-organized System Tree can simplify maintenance. This allows administrators to identify unmanaged systems and work towards a fully managed environment more efficiently. Additionally, host vulnerability information is imported the ePolicy Orchestrator dashboards for MVM. This helps administrators consolidate host threat events and host vulnerability information into one console. When McAfee Risk Advisor is installed on the ePolicy Orchestrator Server all host threat events are compared to host vulnerability information so that countermeasure recommendations are available for quick remediation and a path to more comprehensive environment protection.