

# ForeScout CounterACT<sup>®</sup> NIC Vendor Database

**Configuration Guide** 

**Updated December 2017** 



## **Table of Contents**

About the NIC Vendor Database (DB)	3
Requirements	3
NIC Vendors Detected by CounterACT	3
Installation	4
Verify That the Module Is Running	5
Configuration	5
Detecting Endpoints by NIC Vendor	6
Additional CounterACT Documentation	6
Documentation Downloads	7
Documentation Portal	7
CounterACT Help Tools	8

# About the NIC Vendor Database (DB)

The CounterACT<sup>®</sup> NIC Vendor Database (DB) is a Content Module that works with the HPS Inspection Engine to map Network Interface Controllers to their vendors based on their MAC address.

The NIC Vender DB Module provides host properties that let you detect and manage endpoints based on this information.

- NIC vendor names are listed in the **NIC Vendor** host property.
- NIC vendor names can be matched using free-text search tools in the NIC Vendor Value host property.

Policy: 'Antivirus Compliance'>Cor	ndition [	23
Policy: Antivirus Compliance'>Cor NIC Properties  Control C	Indition  NIC Vendor: Indicates the vendor of the NIC based on its MAC Address block value  Meets the following criteria  Does not meet the following criteria  NIC Vendor  Text filter  Name  Select All  OtDB-METRAVIB  1000EYES GMBH  1000EYES GMBH  1000FIO NETWORKS TECHNOLOGY LLC  10NET COMMUNICATIONS/DCA  11WAVE TECHNOLOGY CO,LTD  12SIDED TECHNOLOGY LLC	×
	1394 PRINTER WORKING GROUP     1394 TRADE ASSOCIATION     22974 Items (0 selected)     OK Cancel	

### **Requirements**

This module requires the following CounterACT releases and CounterACT components:

- CounterACT version 8.0
- An active Maintenance Contract for CounterACT devices

### **NIC Vendors Detected by CounterACT**

The HPS NIC Vendor Database identifies NIC vendors by their MAC Address Block as defined by the IEEE Standards Association. This block of the MAC address was previously known as the OUI (Organizationally Unique Identifier). The NIC Vendor DB uses the following MAC Address Block repositories:

MA-L (MAC Address Block Large)

- MA-M (MAC Address Block Medium)
- MA-S (MAC Address Block Small)
- IAB (Individual Address Block)

Each release of this module updates vendor information to reflect changes to these repositories maintained by the IEEE.

The IAB repository is no longer updated by the IEEE. The module uses the last IAB dataset.

# Installation

#### To install the module:

- 1. Navigate to one of the following ForeScout download portals, depending on the licensing mode your deployment is using:
  - Product Updates Portal Per-Appliance Licensing Mode
  - Customer Portal, Downloads Page Centralized Licensing Mode

To find out which licensing mode your deployment is working with, see <u>Identifying Your Licensing Mode in the Console</u>.

- 2. Download the module .fpi file.
- 3. Save the file to the machine where the CounterACT Console is installed.
- 4. Log into the CounterACT Console and select **Options** from the **Tools** menu.
- 5. Select Modules. The Modules pane opens.
- 6. Select Install. The Open dialog box opens.
- 7. Browse to and select the saved module .fpi file.
- 8. Select Install. The Installation screen opens.
- **9.** Select **I agree to the License Agreement** to confirm that you have read and agree to the terms of the License Agreement, and select **Install**. The installation will not proceed if you do not agree to the license agreement.
- The installation will begin immediately after selecting Install, and cannot be interrupted or canceled.
- In modules that contain more than one component, the installation proceeds automatically one component at a time.
- **10.**When the installation completes, select **Close** to close the window. The installed module is displayed in the Modules pane.
  - Some components are not automatically started following installation.

#### Identifying Your Licensing Mode in the Console

If your Enterprise Manager has a *ForeScout CounterACT See* license listed in the Console, your deployment is operating in Centralized Licensing Mode. If not, your deployment is operating in Per-Appliance Licensing Mode.

Select **Options** > **Licenses** to see whether you have a *ForeScout CounterACT See* license listed in the table.

Options				
Search	Q	Licenses Activate, update or deactivate your license for CounterACT features and Extended Module		
© Discovery		Search Q		
> III Licenses		Name         Status           ForeScout CounterACT See         Valid, Capacity exceed	Type ed Perpetual	
Lists		ForeScout CounterACT Control Valid, Capacity exceed	ed Perpetual	
Internal Network		ForeScout Extended Module for Check Point Next Valid, Capacity exceed	ed Perpetual	

Contact your ForeScout representative if you have any questions about identifying your licensing mode.

### Verify That the Module Is Running

After installing the module, verify that it is running.

#### To verify:

- 1. Select Tools>Options and then select Modules.
- 2. Navigate to the module and select **Start** if the module is not running.

### Configuration

No module configuration is required.

# **Detecting Endpoints by NIC Vendor**

The module provides the following host properties that can be used to build policy conditions based on the NIC controllers installed on endpoints.

Policy:'Antivirus Compliance'>Co	ndition	×
NIC	NIC Vendor Value: Indicates a value associated with the NIC Vendor   Mic Vendor Value: Indicates a value associated with the NIC Vendor	
∼ 🔲 Properties	<ul> <li>Does not meet the following criteria</li> </ul>	
✓ ➡ Device Information		
NIC Vendor Value	Any Value 🗸	
NIC Vendor	Match case	
✓ ₩ McAfee ePO		
ePO Agent Last Communi		
🗸 📢 Windows		
Windows SecureConnecto		
✓ ♥ Windows Security		
SMB Signing		
	Evaluate irresolvable criteria as	
	Неір ОК Са	ancel

NIC Vendor	Indicates the vendor of the NIC, based on its MAC Address Block value. To define a matching condition, select <b>Add</b> and then select one or more MAC Address Block values in the NIC Vendor dialog. To detect endpoints with locally administered MAC addresses, select the <b>Locally Administered MAC Address</b> option in the NIC Vendor dialog. This option matches MAC addresses whose Universal/Local bit is set to 1 (local).
NIC Vendor Value	Indicates NIC Vendor values in text format. Use text matching tools to create conditions that match several variants of a vendor name, or look for a specific substring in a name.

### **Additional CounterACT Documentation**

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

- <u>Documentation Downloads</u>
- Documentation Portal
- <u>CounterACT Help Tools</u>

### **Documentation Downloads**

Documentation downloads can be accessed from one of two ForeScout portals, depending on which licensing mode your deployment is using.

- Per-Appliance Licensing Mode Product Updates Portal
- Centralized Licensing Mode Customer Portal
- Software downloads are also available from these portals.

To learn which licensing mode your deployment is using, see <u>Identifying Your</u> <u>Licensing Mode in the Console</u>.

#### Product Updates Portal

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

#### To access the Product Updates Portal:

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

#### **Customer Portal**

The Downloads page on the ForeScout Customer Portal provides links to purchased CounterACT version releases, Base and Content Modules, and Extended Modules, 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. The Documentation page on the portal provides a variety of additional documentation.

#### To access documentation on the ForeScout Customer Portal:

- 1. Go to https://forescout.force.com/support/.
- 2. Select Downloads or Documentation.

### **Documentation Portal**

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

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

#### To access the Documentation Portal:

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

### **CounterACT 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.

#### **CounterACT Administration Guide**

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 **Modules**.
- 2. Select the plugin and then select Help.

#### **Documentation Portal**

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

#### Identifying Your Licensing Mode in the Console

If your Enterprise Manager has a *ForeScout CounterACT See* license listed in the Console, your deployment is operating in Centralized Licensing Mode. If not, your deployment is operating in Per-Appliance Licensing Mode.

Select **Options** > **Licenses** to see whether you have a *ForeScout CounterACT See* license listed in the table.

Options			
Search Search VPN Search General	Q	Licenses Activate, update or deactivate your license for CounterACT features and Search Q	Extended Modul
> III NAC		Name A Status	Туре
1 Licenses		ForeScout CounterACT See Valid, Capacity exce	eded Perpetua
Lists		ForeScout CounterACT Control Valid, Capacity exce	eded Perpetua
> 🌄 Map		ForeScout CounterACT Resiliency Valid	Perpetua
Internal Network		ForeScout Extended Module for Check Point Next Valid, Capacity exce	eded Perpetua

Contact your ForeScout representative if you have any questions about identifying your licensing mode.

### **Legal Notice**

© 2018 ForeScout Technologies, Inc. All rights reserved. ForeScout Technologies, Inc. is a Delaware corporation. A list of our trademarks and patents can be found at <u>https://www.forescout.com/company/legal/intellectual-property-patents-trademarks</u>. Other brands, products, or service names may be trademarks or service marks of their respective owners.

2018-04-10 09:21