CounterACT® Microsoft® System Management Server (SMS) System Center Configuration Manager (SCCM) Plugin

Configuration Guide

Version 2.2.5
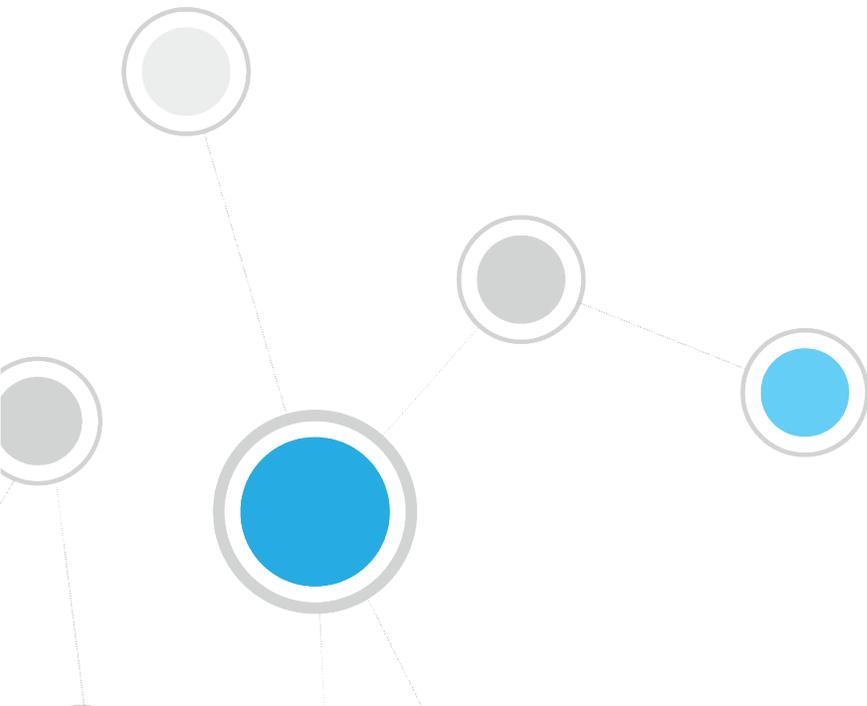
Table of Contents

About the Microsoft SMS/SCCM Plugin

The Microsoft® Systems Management Server (SMS) 2003 and Microsoft® System Center Configuration Manager (SCCM) 2007 and 2012 are servers that collect information from network components and implement software installations and updates.

The SMS/SCCM Plugin lets CounterACT® connect to an SMS or SCCM server for the purpose of:

- Retrieving and displaying advertisement and report information related to SMS/SCCM hosts in CounterACT.

- Updating SMS/SCCM clients with new advertisements, and updating the SMS/SCCM server with new host information.

To use the plugin, you should have a solid understanding of SMS/SCCM concepts, functionality, and terminology.

Concepts, Components, Considerations

Before configuring the plugin you should have a basic understanding of the SMS/SCCM/CounterACT architecture, including concepts, components, and setup considerations.

Concepts

Integration lets you map CounterACT Appliances or the Enterprise Manager to a unique SMS/SCCM server. When several CounterACT devices are mapped to a single SMS server, one CounterACT device functions as a proxy to handle communication between the server and the remaining CounterACT devices. Using a proxy enables the plugin to control the query rate from CounterACT to the SMS/SCCM server, thus ensuring more efficient traffic control.

An option is also available to work with a default server, which can be used to handle CounterACT devices that are not specifically mapped to an SMS/SCCM server. This may happen for example, if new Appliances are registered with an Enterprise Manager, but are not yet assigned to an SMS/SCCM server.

Deployment Options

Deployment can be carried out as follows:

- A unique SMS/SCCM server or server cluster associated with several CounterACT devices.

- Sets of unique SMS/SCCM servers or server clusters associated with several CounterACT devices.

- A single SMS/SCCM server or server cluster associated with a Single Appliance or Enterprise Manager.

You cannot assign several SMS servers to a single CounterACT device.

Components

Connecting CounterACT Device: The Connecting CounterACT device communicates directly with the SMS/SCCM server and handles queries and requests submitted by all the devices assigned to the SMS/SCCM server. In an environment when more than one CounterACT device is assigned to an SMS/SCCM server, the connecting device functions as a proxy between the SMS/SCCM server and other CounterACT devices assigned to it. This means it forwards all requests by other CounterACT devices assigned to the SMS/SCCM server. The Connecting CounterACT device also functions as an Assigned CounterACT device.

Assigned CounterACT Devices: CounterACT devices assigned to a unique SMS/SCCM server. The IP address assignments in these Appliances must also be IP addresses handled by the SMS/SCCM server to which the Appliances are assigned.

Default SMS/SCCM Server: The server to which all CounterACT devices are assigned by default, if they are not explicitly assigned to another SMS/SCCM server.
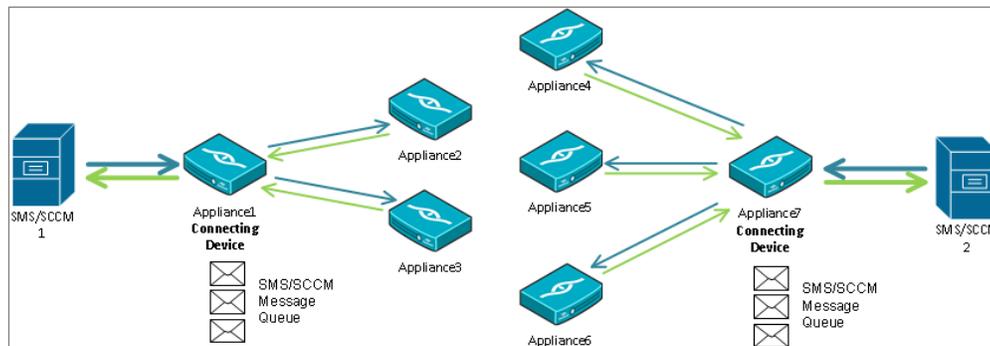
Considerations

Consider the following when mapping CounterACT devices to SMS/SCCM servers:

Match IP Address Ranges: Verify that the SMS/SCCM server/cluster handles the same IP address range as the CounterACT devices assigned to it.

To set IP address assignments to CounterACT devices:

1. Select **Options** from the **Tools** menu and then expand **CounterACT Devices**.

2. Select **IP Assignments**. The IP Assignments pane displays.

3. Select an item and then select **Edit**.

4. Make your settings or select Add to add a new IP address.

5. Select **OK**.

Use This Plugin with the HPS Inspection Engine Plugin: Although SMS/SCCM servers store information that may overlap with the information retrieved by the HPS Inspection Engine Plugin, the Microsoft SMS/SCCM Plugin should not be used as a substitute for the HPS Inspection Engine Plugin because the HPS Inspection Engine Plugin collects information that the SMS/SCCM servers do not.

What to Do

You must perform the following to work with this plugin:

- Verify that requirements are met. See Requirements for details.

- Download and install the plugin. See Install the Plugin for details.

- Define target SMS/SCCM servers, and assign CounterACT devices to them. See Configure the Plugin for details.

- Verify communication with target SMS/SCCM servers. See Test the Plugin.

- Define CounterACT policies that contain SMS/SCCM conditions or actions. See Create Custom Policies for details.

Requirements

- CounterACT version 7.0.0 with Service Pack 2.3.4 or above installed. It is recommended to install the latest service pack to take advantage of the most recent updates.

- Access to the SQL database of SMS/SCCM servers/clusters. The database user account used by CounterACT should have Read Table permission. No write permission is required.

- SMS/SCCM 2003, 2007, or 2012 Inventory Tool for Microsoft Updates SP1 or higher must be installed on the SMS/SCCM site.

- If you are working with policy actions, additional requirements should be addressed. See SMS/SCCM Client Registration Status for more information.

Third-Party Requirements

- When working directly with the SMS/SCCM database, you will need a Microsoft SQL user that belongs to the SMS/SCCM database with read permissions. This is for conducting a *select* query.

Install the Plugin

CounterACT is delivered with several bundled plugins, including this plugin.

New plugin functionality and supporting data may become available independently between major CounterACT version releases. This section describes how to install the plugin when a new plugin version becomes available between releases.

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.

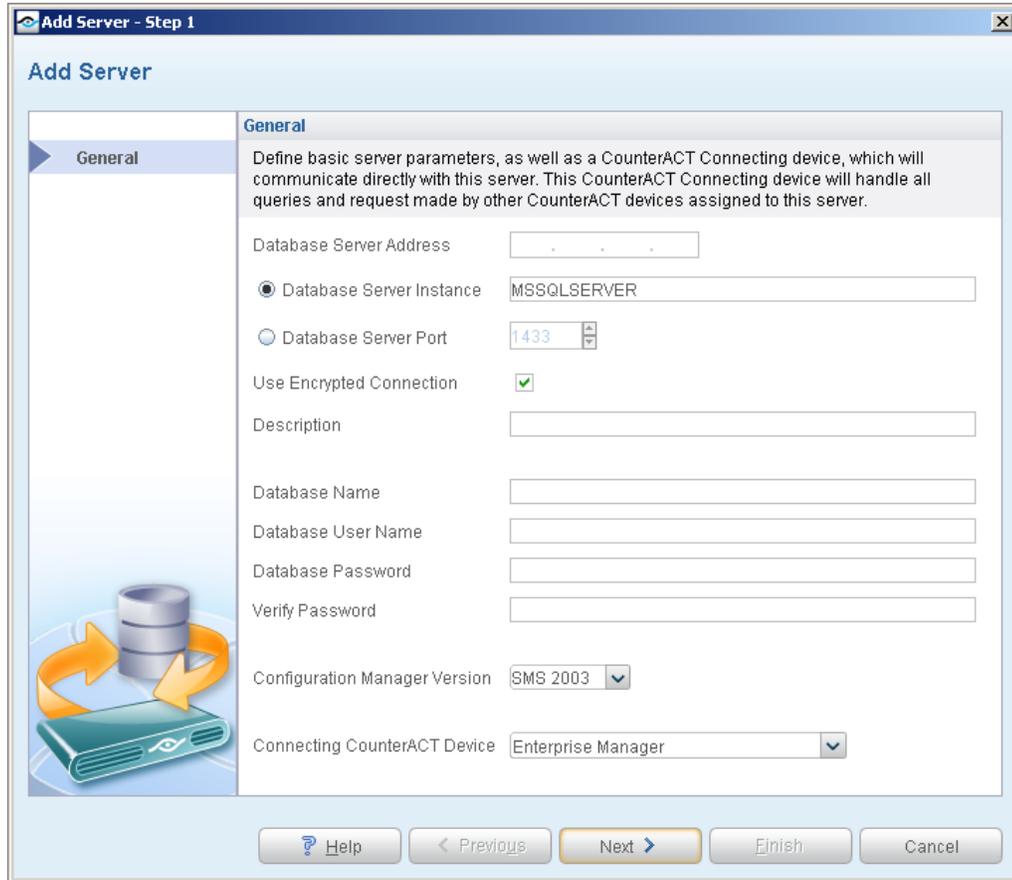9. Once the installation is complete, select **Close**. The plugin is listed in the Plugins pane.

Configure the Plugin

Plugin configuration lets you define target SMS/SCCM servers and map CounterACT Appliances or the Enterprise Manager to a SMS/SCCM server. You can access the SMS/SCCM MSSQL database, which is required for retrieving properties. You can also set advanced parameters, for example you can limit the volume of requests CounterACT submits to the SMS/SCCM server.

See Concepts, Components, Considerations for more information about assigning CounterACT devices to SMS/SCCM servers.

To define SMS/SCCM server targets:

1. Select **Options** from the **Tools** menu and then select the **Plugins** folder.

2. In the Plugins pane, select the Microsoft SMS/SCCM plugin and select the **Configure** button. In the Microsoft SMS/SCCM pane, select **Add** to add a server. The Add Server wizard opens.

3. In the General pane, configure the following connection parameters:

Database Server Address	The IP address of the SMS/SCCM server.
Database Server Instance	The name of the Microsoft SQL Database Server instance to connect to. If you connect using a named instance, the port will be detected automatically. Using a named instance requires UDP connections to the server on port 1434 as well as the port dynamically allocated for the given named instance. The default value is MSSQLSERVER.

Using dynamic ports when connecting with a named instance complicates the connection because the port number may change when the Microsoft SQL server is restarted, requiring changes to the firewall settings. To avoid connection problems through a firewall, configure SQL Server to use a static port.

This parameter is mutually exclusive with **Database Server Port**. |
| **Database Server Port** | The port used to access the SMS/SCCM server (default 1433).

This parameter is mutually exclusive with **Database Server Instance**. |
Use Encrypted Connection	If the SQL connection to the SMS/SCCM server must be encrypted, select the box.
Description	A description of this server connection.
Database	The full name of the target database, for example *SCCM_CM1* or

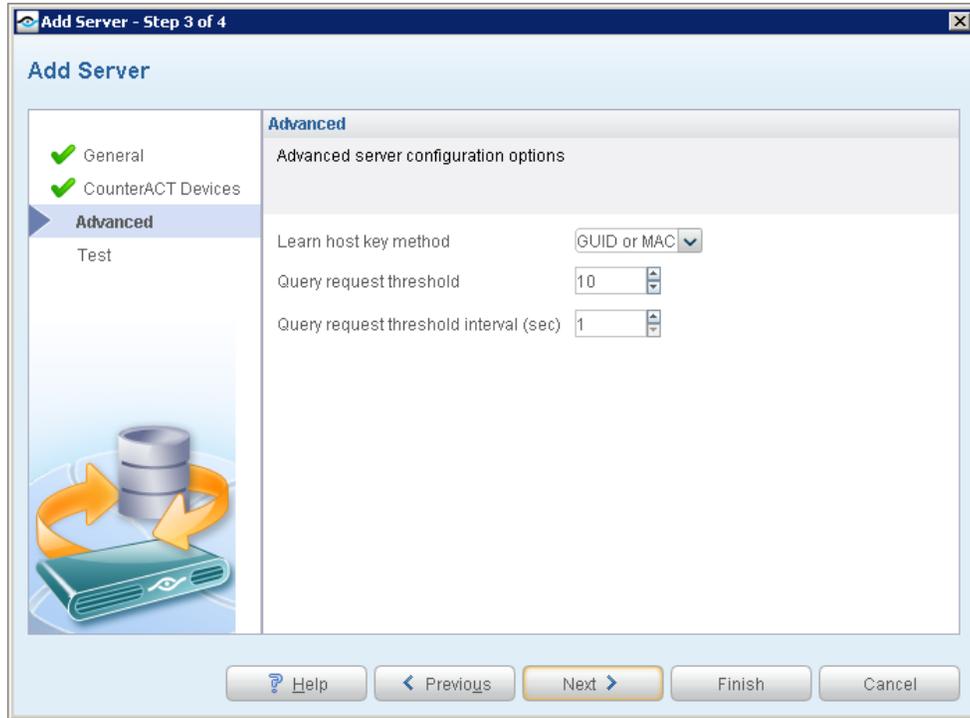| Name	*SMS_db23.*
Database Username	A username for the SQL database of the SMS/SCCM server. This user must have *Read Table* permissions.
	To specify an existing Windows domain user, use the full `DOMAIN\username` format. Windows user login is supported in environments that use NT LAN Manager (NTLM) for authentication. Authentication with Kerberos is not supported.
Database Password	The password for the above user. Retype the password to confirm it.
Configuration Manager Version	The version of the SMS/Configuration Manager that runs on this server.
Connecting CounterACT device	Select the CounterACT device that communicates with the server. This device handles all communication with the target SMS/SCCM server, including requests by other CounterACT devices assigned to this SMS/SCCM server. This device receives SMS/SCCM requests from the other CounterACT devices assigned to this SMS/SCCM target, and passes results to them.

4. Select **Next**. The CounterACT Devices pane opens.
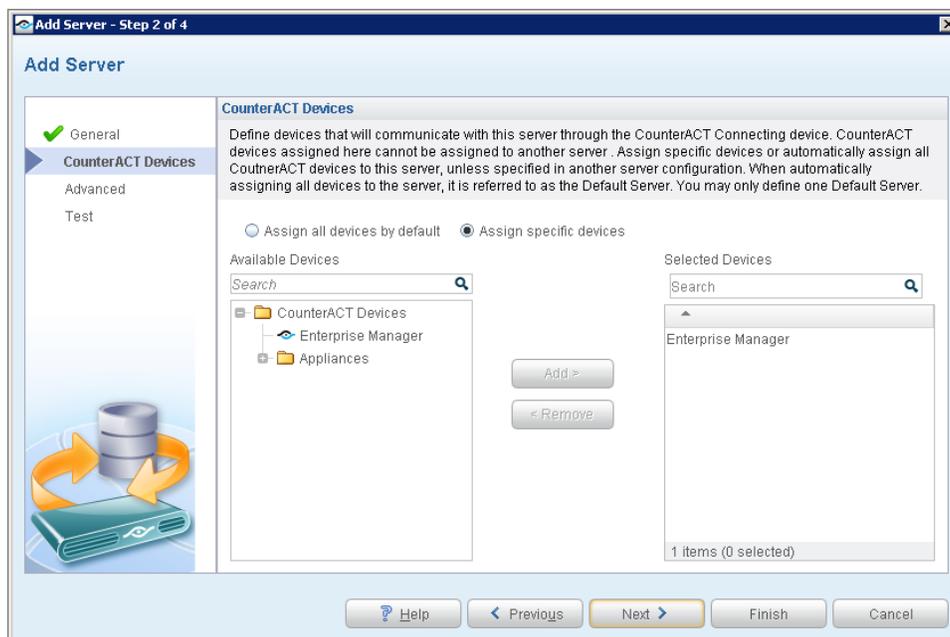
5. Choose one of the following options:

    –   Select **Is Default Server** to make this server the target for all CounterACT devices not assigned to another SMS/SCCM server. Until you define more than one server, this is the only option available.

    –   Select **Assign Devices** to specify CounterACT devices that communicate with this server. Use the Add or Remove buttons to set the selected device.
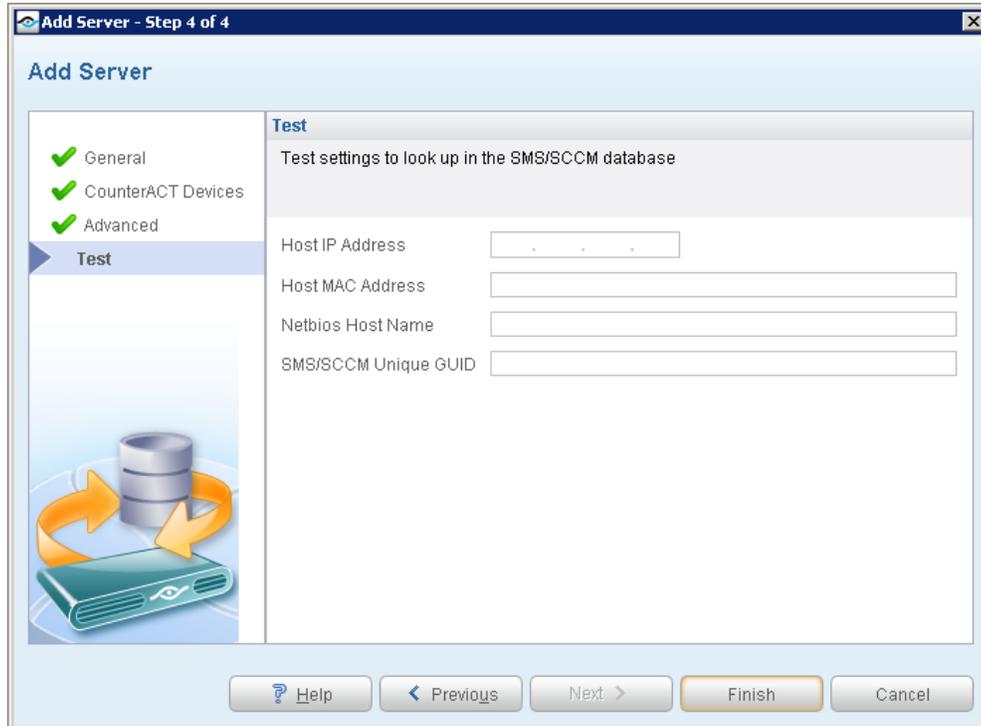
6. Select the **Next** button. The Advanced pane opens.

7. Configure the following advanced features:

Learn host key method	Select the method to use to learn the host key used to look up host properties on the SMS/SCCM server. The following options are available: ▪ GUID Only ▪ GUID or MAC ▪ MAC Only It is recommended to work with the **GUID or MAC** option. To retrieve the GUID the host must be managed by CounterACT (either via remote inspection or using SecureConnector).
Query request threshold	Together, these two parameters regulate the volume of requests submitted to the SMS/SCCM server. **Query request threshold** defines the number of requests that can be submitted over the time period specified by **Query request threshold interval**.
Query request threshold interval	

8. Select **Next**. The Test pane opens.

9. In the Test pane, configure endpoint information that is used to test communication with this server. Data for the endpoints identified by these fields should be present in the database of the target server, but the endpoints do not have to be connected to the SMS/SCCM server for the test.

    Each of these values is tested separately. You can specify one, two, or all values to test the SMS/SCCM query using each type of identifier.

10. Select **Finish**. The server appears in the Microsoft SMS/SCCM pane.

11. (Optional) Repeat this procedure to add other SMS/SCCM servers. In the Microsoft SMS/SCCM pane, select **Edit** to reassign CounterACT devices to each SMS/SCCM server, to change the default SMS/SCCM server, or to change which CounterACT devices handle SMS/SCCM communication.

Test the Plugin

This section describes how to verify that CounterACT can connect to the SMS/SCCM database and retrieve information for a specific host. Test results indicate if the host:

- Has an SMS/SCCM client installed

- Does not have an SMS/SCCM client installed

- Is not known to the SMS/SCCM database

If the database access was enabled in the Add Server wizard, the test verifies that:

— The plugin can access the SMS/SCCMMSSQL database.

— Database query results on the tested host are correct.

Data for the endpoints identified by these fields should be present in the database of the target server, but the endpoints do not have to be connected to the SMS/SCCM server for the test.

To test the plugin:

1. In the Plugins pane, select the Microsoft SMS/SCCM plugin and select **Configure**.

2. From the table in the Microsoft SMS/SCCM pane, select a configured connection to an SMS/SCCM server.

3. (Optional) To review or modify the endpoint information used for the test, select **Edit**. In the Edit SMS Server wizard, select the Test tab. Select **Cancel** or **OK** to exit the wizard.

4. Select **Test**. Confirm the test.

Troubleshooting the Test

This section shows sample error message when the SMS/SCCM credentials are not configured correctly.

If the test returns an error similar to the following example, there is a problem with the server configuration. The IP that was entered may not be an SMS/SCCM server, or the port number entered may be incorrect.

```
DBI connect('host=10.1.8.1;port=1433','wer',...) failed: OpenClient
message: LAYER = (0) ORIGIN = (0) SEVERITY = (78) NUMBER = (41)
Server , database Message String: Server is unavailable or does not exist.
at lib/fstool/commands/SMS/SCCM.pl line 165
Error: Error while executing plugin_test_cb : Unable to connect to server
OpenClient message: LAYER = (0) ORIGIN = (0) SEVERITY = (78) NUMBER = (41)
Server , database
Message String: Server is unavailable or does not exist.
, Quitting
```

If the test returns an error similar to the following example, there is a problem with the user name and password. The user name or password may be incorrect or the user may not have the required permissions.

```
message number=18456 severity=14 state=1 line=0 text=Login failed for user
'wer'.OpenClient message: LAYER = (0) ORIGIN = (0) SEVERITY = (78) NUMBER = 
(46)
Server , database 
Message String: Login incorrect.
 at lib/fstool/commands/SMS/SCCM.pl line 165
Error: Error while executing plugin_test_cb : Unable to connect to server 
Server message number=18456 severity=14 state=1 line=0
text=Login failed for user 'wer'.OpenClient message: LAYER = (0) ORIGIN = 
(0) SEVERITY = (78) NUMBER = (46)
Server , database 
Message String: Login incorrect.
 , Quitting
```

Create Custom Policies

Custom CounterACT policy tools provide you with an extensive range of options for detecting and handling endpoints. Use policies to instruct CounterACT to apply actions to endpoints that match conditions based on host property values.

This section describes the host properties that are made available when this plugin is installed.

Policies, Properties, and Actions

This section provides a brief overview of CounterACT's policy-based tools to detect and handle endpoints. See Create Custom Policies for more detailed information about these features.

Policy rules detect and handle hosts defined in the policy scope. When an endpoint matches the conditions of a rule, the actions of the rule are applied to the endpoint.

Policy conditions examine host properties learned by CounterACT to detect hosts with specific attributes. For example, you can create a policy that instructs CounterACT to detect hosts running a certain operating system or with a certain application installed.

Policy actions let you instruct CounterACT to control detected devices. For example, assign a device that matches the conditions of a rule to quarantine a VLAN or send the device user or IT team an email.
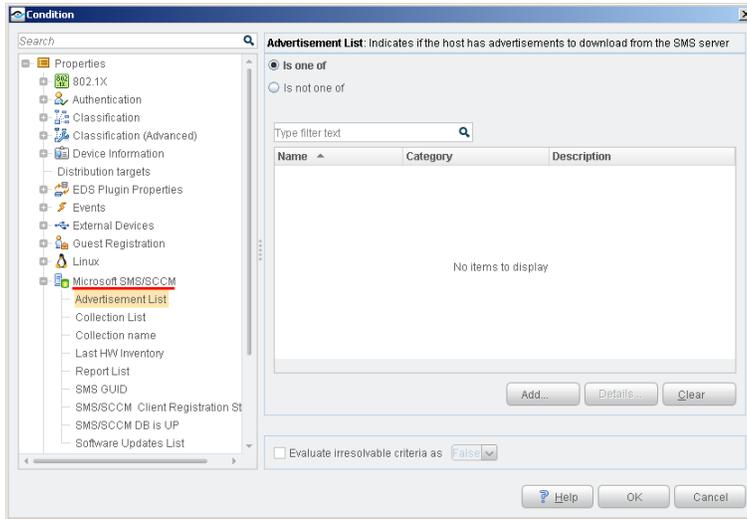
Policy Properties - Detecting Endpoints

The following properties describe attributes that can be discovered by working with custom SMS/SCCM policies. These properties are available when you install the CounterACT SMS/SCCM Plugin.

To access SMS/SCCM properties:

1. Navigate to the Properties tree from the Custom Policy Conditions dialog box.

2. Expand the Microsoft SMS/SCCM folder in the Properties tree. The following properties are available:

   – Advertisement List

- [Collection List](#)
- [Collection name](#)
- [Last HW Inventory](#)
- [Report List](#)
- [SMS GUID](#)
- [SMS/SCCM Client Registration Status](#)
- [SMS/SCCM DB is UP](#)
- [Software Updates List](#)

| Advertisement List	Indicates endpoints that have advertisements to download from the SMS/SCCM server.
Collection List	Indicates endpoints that are members of collections.
Collection name	Indicates endpoints that are members of a specific collection. Wildcards are supported.
Last HW Inventory	Indicates endpoints that reported a hardware inventory event to the SMS/SCCM server before a specified time.
Report List	Indicates endpoints that are members of reports. The plugin only supports reports in which the query is defined according to NetBIOS and with the following format: **SELECT fields FROM tables WHERE sys.Netbios_Name0 = @element_name** or **SELECT fields FROM tables WHERE v_R_System.Netbios_Name = @element_name** Other fixed conditions or SQL commands (such as ORDER) be added after the initial Netbios_Name condition. For example: **SELECT fields FROM tables WHERE sys.Netbios_Name0 = @element_name and table.field = 'fixed_value'**
SMS GUID	Indicates the SMS Client Software GUID of the endpoint

SMS/SCCM Client Registration Status	Indicates the client registration status of the endpoint at the SMS/SCCM server.
SMS/SCCM DB is UP	Indicates that plugin and SMS/SCCM server are connected.
Software Updates List	Indicates endpoints that are members of pending software updates.

Policy Actions - Managing Endpoints

CounterACT actions provide a wide range of tools that assist you in handling SMS/SCCM endpoints.

Get Microsoft SMS/SCCM Updates

Use the *Get Microsoft SMS/SCCM Updates* action to update the SMS/SCCM client with new advertisements and then update the SMS/SCCM server with the new status.
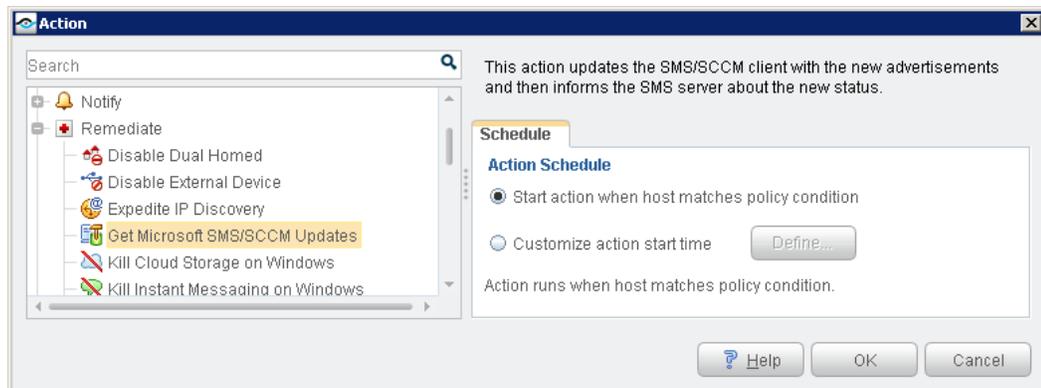
Action Requirements

- SMS/SCCM Advanced client must be installed on the endpoint for the action to work.

- When policy rules use an SMS/SCCM collection property, and the policy implements the *Get Microsoft SMS/SCCM Updates* action and *Assign to VLAN* action, the SMS/SCCM collection should be configured to perform an SMS/SCCM recheck every minute. This ensures that the host moves into production as soon as possible.

- If the policy contains the *Assign to VLAN* action and the *Get Microsoft SMS/SCCM Updates* action, the SMS/SCCM roaming boundaries should be configured to contain the IP ranges of the VLANS that are used in the policy.

- Use the options of the Scheduling tab to customize update retrieval. For example, you can choose the **Customize action start time** option to delay the action.

Using SMS/SCCM

Now that you have established communication between the CounterACT SMS/SCCM Plugin and a server, you can use this to collect information from network components and implement software installations and updates.

Use the CounterACT Inventory tab to view a real-time display of SMS/SCCM updates.

You can browse the inventory to learn what CVEs have been detected on your network, and acquire information about endpoints with similar findings.

Get SMS/SCCM Updates

You can select specific IP addresses to have the SMS/SCCM Plugin get updates.

To get the SMS/SCCM updates:

1. Log in to the CounterACT Console and select the **Home** tab.

2. Navigate to any IP Address and right-click it.

3. Select **Remediate** and then select **Get Microsoft SMS/SCCM Updates**.
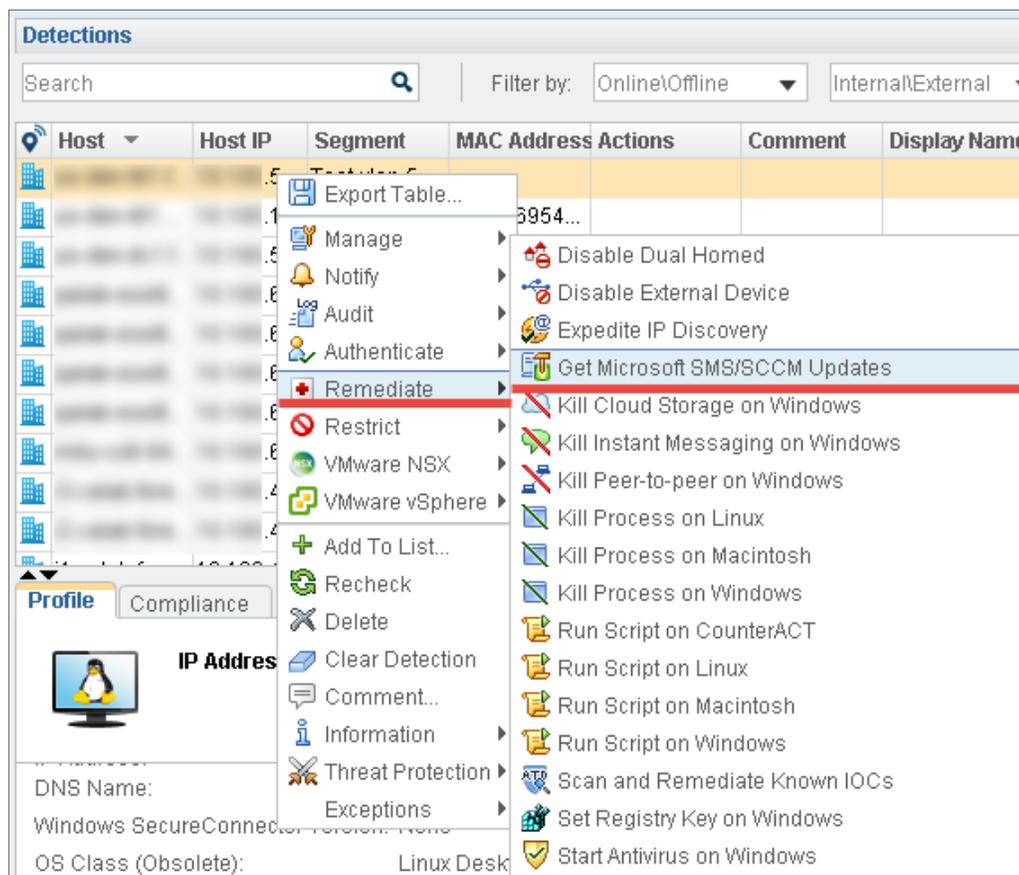
4. The Specify Get Microsoft SMS/SCCM Updates parameters dialog box opens.
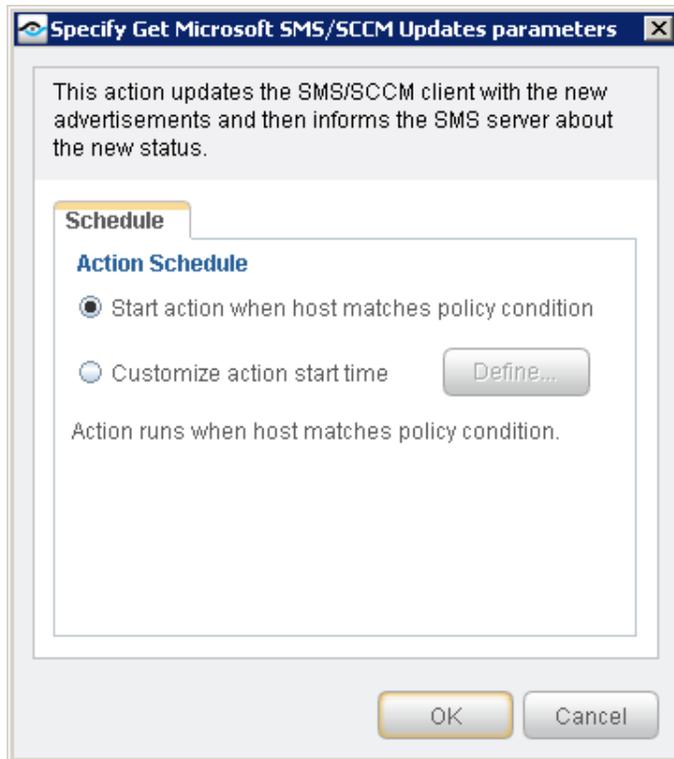
**5.** Set your parameters and then select **OK**.

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.
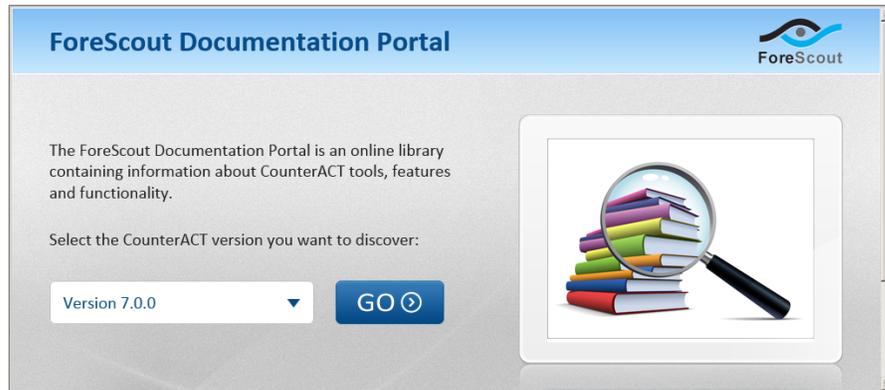
To access the Documentation Portal:

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:

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

- 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 Professional Services, the provision of such services is subject to your acceptance of the terms set forth at http://www.forescout.com/professional-services-agreement/;

- 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

2017-05-23 11:15