CounterACT Aruba ClearPass Plugin

Configuration Guide

Version 1.1.0 and Above

Table of Contents

About the ClearPass Integration **3**

About This Plugin **3**

What to Do 4

Requirements **4**

CounterACT Requirements 4

Aruba ClearPass Requirements 4

Networking Requirements 5

Install the Plugin **5**

Configure the Plugin **6**

Test the Plugin **9**

Create Custom Policies **10**

Detecting Endpoints – Aruba ClearPass Properties 10

Managing Endpoints – Aruba ClearPass Actions 12

Additional CounterACT Documentation **15**

Documentation Portal 15

Customer Support Portal 16

CounterACT Console Help Tools 16

About the ClearPass Integration

The Aruba ClearPass Plugin provides for the interoperation between CounterACT and Aruba ClearPass. Aruba ClearPass is a NAC product in its own right. The purpose of CounterACT working with ClearPass is to achieve a synergy of NAC enforcement; CounterACT detection, via its policies, identifies endpoints that require treatment by ClearPass. CounterACT then instructs the relevant ClearPass server about the treatment to be performed on the identified ClearPass-managed endpoint.

ClearPass servers can be clustered into server groups The ClearPass servers assigned to a ClearPass server group handle NAC enforcement for a specific, organizational group; such groups are established based on business requirements, for example, based on region, function or operation.

About This Plugin

The Aruba ClearPass Plugin instructs a relevant ClearPass server about specific treatment to be performed on a CounterACT detected endpoint that is also being simultaneously managed by Aruba ClearPass.

CounterACT offers the following actions, which result in Aruba ClearPass NAC treatments:

- Assign a ClearPass tag to an Aruba ClearPass managed endpoint
- Delete a ClearPass tag from a Aruba ClearPass managed endpoint

A ClearPass tag consists of a name-value pair.

As part of plugin-initiated actions sent to Aruba ClearPass, CounterACT can also include a request to the ClearPass server to apply a change of authorization (CoA) to the endpoint. Application of the CoA to a detected endpoint forces the endpoint to re-authenticate. ClearPass servers apply the CoA following the success of the plugin-initiated action.

The CounterACT device that interfaces with the ClearPass servers that are members of a ClearPass server group is termed the *Connecting Device*. At any given time, each ClearPass-managed endpoint is handled by only one ClearPass server in a ClearPass server group. That server is termed the *Managing ClearPass Server* of the managed endpoint.

Using syslog messages, Aruba ClearPass informs CounterACT about the following ClearPass-managed endpoint events:

- Confirmations of endpoint RADIUS authentication, which was requested by the Plugin in Aruba ClearPass actions using the *Apply CoA* option.
- When a wireless endpoint comes online
- When a wireless endpoint goes offline

Using syslog messages, Aruba ClearPass provides CounterACT with the following ClearPass-managed endpoint property information:

- Managing ClearPass Server
- ClearPass Server Group
- Status of the Last CoA Request
- Wireless Controller

What to Do

This section describes steps you should take to set up your system when integrating with ClearPass:

1. Verify that you have met the system requirements. See Requirements.
2. Install the Plugin.
3. Configure the Plugin.
4. Test the Plugin.
5. Create policies to handle ClearPass-managed endpoints.

Requirements

This section describes the system requirements for CounterACT-Aruba ClearPass interoperation, as follows:

- CounterACT Requirements
- Aruba ClearPass Requirements
- Networking Requirements

CounterACT Requirements

The following CounterACT version, running its latest hotfix, supports the Aruba ClearPass Plugin:

- 7.0.0

Aruba ClearPass Requirements

Interoperation with the Aruba ClearPass Plugin requires Aruba ClearPass versions 6.3.X.

The Aruba ClearPass administrator must configure the organization's ClearPass servers to send syslog messages to the CounterACT *Connecting Device*s. Using syslog messages, Aruba ClearPass informs CounterACT about specific managed endpoint events and properties.

The plugin performs actions on Aruba ClearPass using the ClearPass web service. For the *Connecting Device*'s HTTPS connection to its ClearPass servers, define the same username and password for all ClearPass servers assigned to a ClearPass server group.

Networking Requirements

Open the following ports on enterprise firewalls to support communication between the CounterACT *Connecting Device* and the group of ClearPass servers with which it interfaces:

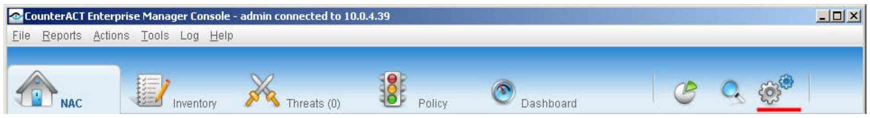
- The port that the *Connecting Device* uses to communicate with its assigned ClearPass servers, which by default is port 443/TCP. Specify this port when you configure the plugin. See Configure the Plugin for instructions on configuring this port value.

Install the Plugin

This section describes how to install the plugin. Install the plugin on all your deployed CounterACT devices; this is accomplished by installing it on the Enterprise Manager, which then ensures that the plugin is installed on all your deployed Appliances.

To install the plugin:

1. Acquire a copy of the plugin in either one of the following ways, as relevant:
   - **a.** If you are installing a Beta release of this plugin, acquire the plugin from your ForeScout representative or contact beta@forescout.com.
   - **b.** Otherwise, navigate to the Customer Support Plugins page and download the plugin.
2. Save the plugin to the machine where the CounterACT Console is installed.
3. Log in to the Console and select the **Options** icon from the CounterACT Console toolbar.


CounterACT Enterprise Manager Console - admin connected to 10.0.4.39
File Reports Actions Tools Log Help
NAC
Inventory
Threats (0)
Policy
Dashboard

4. Navigate to the **Plugins** folder. The Plugins pane opens.
5. In the **Plugins** pane, select **Install**. The **Open** dialog box opens.
6. Navigate to the plugin save location. Select the plugin **`.fpi`**.
7. Select **Install**.

🗎 *If your system is running CounterACT 7.0.0 Hotfix 1.7.1 or above, a license agreement dialog box will open. Accept the license agreement to proceed with the installation.*

Configure the Plugin

This section describes how to configure the Aruba ClearPass Plugin.

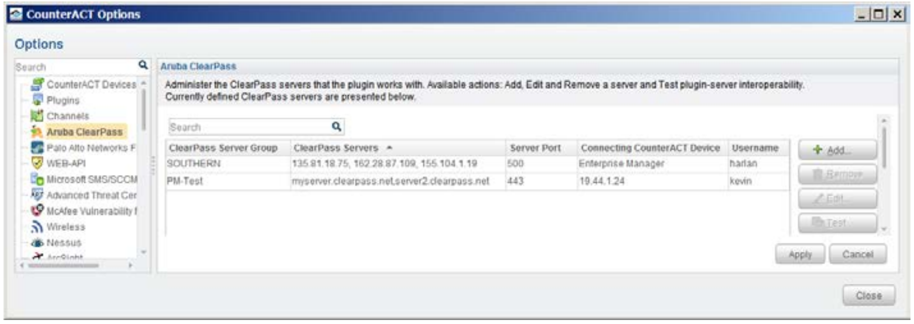
Each ClearPass server group configuration for the plugin defines one or more than one ClearPass server and the CounterACT *Connecting Device* that will interoperate with the group's servers.

CounterACT-ClearPass interoperation imposes the following configuration constraints:

- Both an Enterprise Manager and an Appliance can function as a *Connecting Device*.
- A CounterACT device (Enterprise Manager or Appliance) can only be configured as the *Connecting Device* for a single ClearPass server group.
- Each ClearPass server group can be assigned multiple ClearPass servers.
- Each ClearPass server must only be assigned to a single ClearPass server group.
- Multiple ClearPass server groups can be defined.
- Each ClearPass server group exclusively interfaces with only one CounterACT *Connecting Device*.

To configure the plugin:

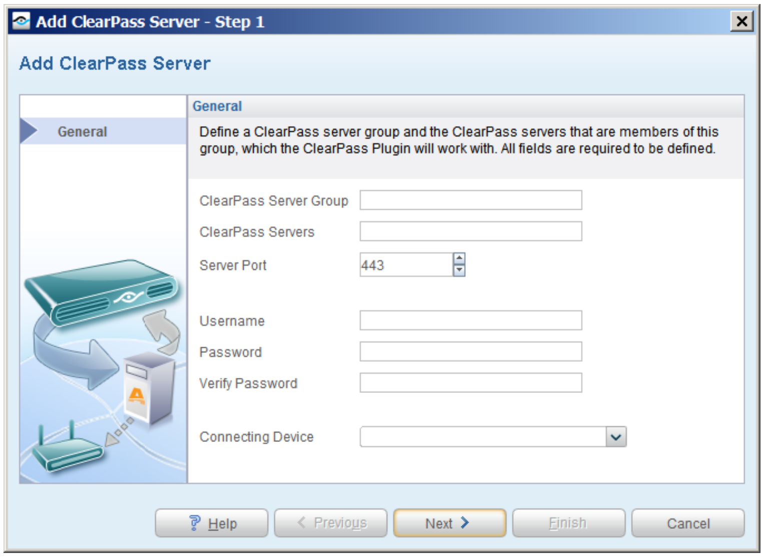
1. In the Console, select **Options** from the **Tools** menu. The **Options** page opens.
2. From the navigation tree, select **Aruba ClearPass**. The **Aruba ClearPass** plugin window opens. The window presents the ClearPass servers configured for interoperation with the plugin.



Administer the ClearPass servers that the plugin works with. Available actions: Add, Edit and Remove a server and Test plugin-server interoperability.
Currently defined ClearPass servers are presented below.

ClearPass Server Group	ClearPass Servers	Server Port	Connecting CounterACT Device	Username
SOUTHERN	135.81.18.75, 162.28.87.109, 155.104.1.19	500	Enterprise Manager	harlan
PM-Test	myserver.clearpass.net,server2.clearpass.net	443	19.44.1.24	kevin

3. Select **Add**. The **General** dialog of the **Add ClearPass Server** wizard opens.



Add ClearPass Server - Step 1

Add ClearPass Server

General

Define a ClearPass server group and the ClearPass servers that are members of this group, which the ClearPass Plugin will work with. All fields are required to be defined.

ClearPass Server Group

ClearPass Servers

Server Port 443

Username

Password

Verify Password

Connecting Device

a. In the **ClearPass Server Group** field, enter the name of the ClearPass server group that receives assignment of the servers defined in the **ClearPass Servers** field.

b. In the **ClearPass Servers** field, enter either the DNS or the IP address of the ClearPass servers that are assigned to the group defined in the **ClearPass Server Group** field. Multiple entries must be comma-separated.

c. In the **Server Port** field, define the port that the *Connecting Device* uses to communicate with its ClearPass servers. By default this is port 443.

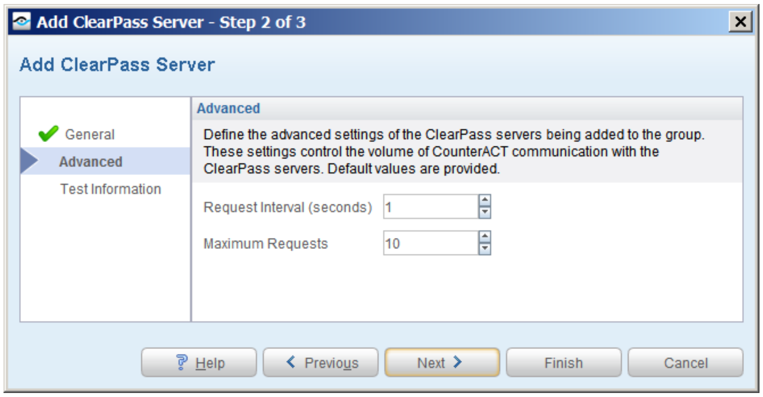
d. In the **Username** field, enter the username that the *Connecting Device* uses to access any member of the ClearPass server group.

e. In the **Password** field, enter the password that the *Connecting Device* uses to access any member of the ClearPass server group.

🗎 *For the Connecting Device's HTTPS connection to a ClearPass server, the same username and password must be in effect for all ClearPass server group members.*

f. From the **Connecting Device** dropdown list, select a CounterACT device. Either an Enterprise Manager or an Appliance can be selected. The selected device interfaces with the ClearPass servers that are assigned to the ClearPass server group.

4. Select **Next**. The **Advanced** dialog opens.



Add ClearPass Server - Step 2 of 3

Add ClearPass Server

Advanced

Define the advanced settings of the ClearPass servers being added to the group. These settings control the volume of CounterACT communication with the ClearPass servers. Default values are provided.

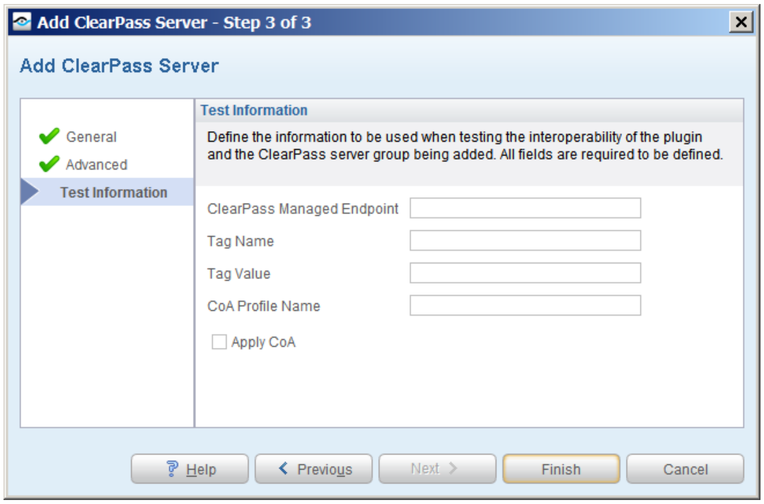
Request Interval (seconds): 1

Maximum Requests: 10

a. In the **Request Interval** field, define the recurring interval, in seconds, during which the *Connecting Device* can send requests to any ClearPass server member of the ClearPass server group.

b. In the **Maximum Requests** field, define the total number of requests that the *Connecting Device* can send, during a request interval, to the ClearPass server members of the ClearPass server group.

5. Select **Next**. The **Test Information** dialog opens.



Add ClearPass Server - Step 3 of 3

Add ClearPass Server

Test Information

Define the information to be used when testing the interoperability of the plugin and the ClearPass server group being added. All fields are required to be defined.

ClearPass Managed Endpoint:

Tag Name:

Tag Value:

CoA Profile Name:

□ Apply CoA

a. In the **ClearPass Managed Endpoint** field, enter the IP address of the ClearPass-managed endpoint that will be used to test the *Connecting Device* interoperation with Aruba ClearPass.

🗎 *Make sure that the provided endpoint is managed by a ClearPass server member of the ClearPass server group.*

b. In the **Tag Name** field, enter the tag name that will be used to test the *Connecting Device* interoperation with Aruba ClearPass with regards to the plugin actions *Assign ClearPass Tag* and *Delete ClearPass Tag*.

c. In the **Tag Value** field, enter the tag value that will be used to test the *Connecting Device* interoperation with Aruba ClearPass with regards to the plugin actions *Assign ClearPass Tag* and *Delete ClearPass Tag*.

d. Select the **Apply CoA** checkbox to test ClearPass server application of a change of authorization to the specified ClearPass-managed endpoint.

e. In the **CoA Profile Name** field, enter the CoA profile name. Aruba ClearPass requires the CoA profile name, in order for a ClearPass server to apply a change of authorization.

6. Select **Finish**.
7. Select **Apply** to save your configuration changes.

Test the Plugin

Test the ability of the plugin to interoperate with the server members of the ClearPass server group. The following interoperation is verified:

- *Connecting Device* HTTPS access to the server members of the ClearPass server group, using the configured username, password and port number.
- Apply of a change of authorization – when testing the application of a change of authorization to the defined ClearPass-managed endpoint, the *Connecting Device* sends a request to each member of the ClearPass server group. Only the *Managing ClearPass Server* of the endpoint will execute requests of this type. By receipt of a confirmation of the successfully applied change of authorization (CoA), the plugin learns the *Managing ClearPass Server* of the endpoint.

🗎 *For the change of authorization test to complete - a re-authentication of the ClearPass-managed endpoint - ensure that the test endpoint attempts to re-connect to the network, after being disconnected.*

- *Assign ClearPass Tag* action - the *Connecting Device* sends a request to the *Managing ClearPass Server* of the endpoint to assign the test tag to the managed endpoint. This action can be executed by all server members of the ClearPass server group.
- *Delete ClearPass Tag* action - the *Connecting Device* sends a request to the *Managing ClearPass Server* of the endpoint to delete the test tag from the managed endpoint. This action can be executed by all server members of the ClearPass server group.

To execute a test of the plugin:

1. In the Console, select **Options** from the **Tools** menu. The **Options** page opens.
2. From the navigation tree, select **ClearPass.** The **ClearPass** plugin window opens.

   The display presents the ClearPass servers configured for interoperation with the plugin.
3. From the display, select a ClearPass server group entry.
4. Select **Test**. The **Testing ClearPass** window opens.

As the test progresses, results display in the window.

Create Custom Policies

Custom CounterACT policy tools provide an extensive range of options for detecting and handling endpoints.

Use a policy to instruct CounterACT to apply a policy action to endpoints that match / do not match property values defined in policy conditions.

Properties

CounterACT properties let you instruct CounterACT to detect endpoints with specific attributes. For example, create a policy that instructs CounterACT to detect those endpoints running a certain operating system or to detect endpoints having a certain application installed.

Actions

CounterACT actions let you instruct CounterACT how to control detected endpoints. For example, assign a detected endpoint to an isolated VLAN or send an email to the endpoint user or IT team.

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

To create a custom policy:

1. Log in to the CounterACT Console.
2. Select the **Policy** icon from the Console toolbar.
3. Create or edit a policy.

In addition to the bundled CounterACT properties and actions available for detecting and handling endpoints, the Aruba ClearPass Plugin provides properties and actions for use in policies.

Detecting Endpoints – Aruba ClearPass Properties

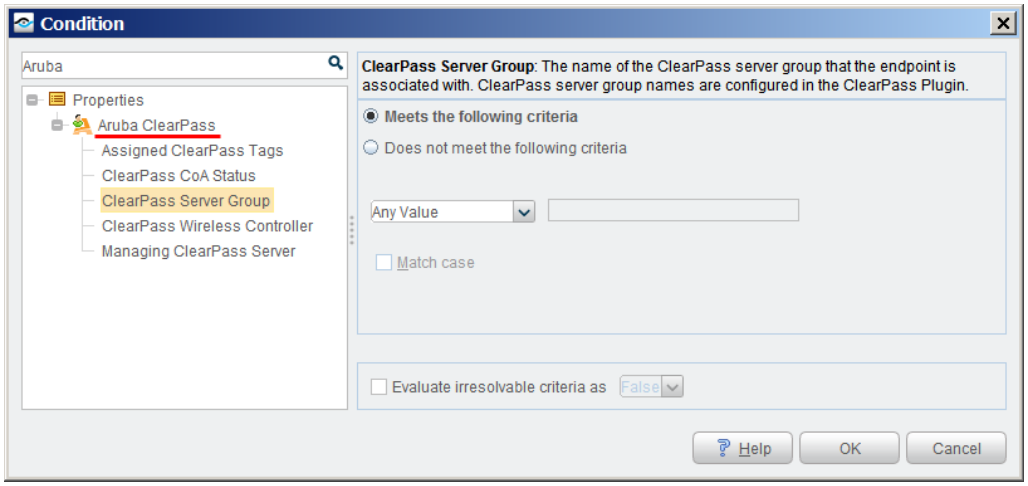
Use policy conditions to evaluate detected endpoints. The Aruba ClearPass Plugin, when installed, provides the following properties to use when evaluating endpoints:

Property	Description
Assigned ClearPass Tags	A semicolon-separated list of assigned tags and their values. For example: tag1=value1;tag2=value2;tag3=value3
ClearPass CoA Status	Status of the most recent change of authorization (CoA) request that was sent to a ClearPass server group.
ClearPass Server Group	Name of the ClearPass server group that the endpoint is associated with. ClearPass server group names are configured in the ClearPass Plugin.

Property	Description
ClearPass Wireless Controller	DNS name of the wireless controller that the endpoint is associated with. If DNS is unavailable, the IP address is provided.
Managing ClearPass Server	IP address of the ClearPass server managing the endpoint. The ClearPass server managing the endpoint is determined based on the receipt of either a syslog message or a response to a successfully applied change of authorization (CoA) request from the ClearPass server.

To access Aruba ClearPass properties:

1. In the **Criteria** pane of either a Policy → Main Rule or a Policy→Sub-Rule, select **Add…**. The **Condition** window opens.
2. In the Properties navigation tree, double-click **Aruba ClearPass**. The ClearPass properties display.



ClearPass Server Group: The name of the ClearPass server group that the endpoint is associated with. ClearPass server group names are configured in the ClearPass Plugin.

● **Meets the following criteria**

○ Does not meet the following criteria

Any Value

□ Match case

□ Evaluate irresolvable criteria as False

In addition to the provided Aruba ClearPass properties, the following CounterACT properties are also relevant to use with Aruba ClearPass managed endpoints:

Property	Description
Authentication Login	An Authentication property. Property identifies endpoints that connected to the network using a specific authentication method. This property offers the relevant criteria **Authentication to ClearPass server**.
Host is online	A Device Information property. Property identifies endpoints as being connected to the network.

To access Authentication and Device Information properties:

1. In the **Criteria** pane of either a Policy → Main Rule or a Policy→Sub-Rule, select **Add…**. The **Condition** window opens.

2. In the Properties navigation tree, double-click any of the following:
   a. **Authentication** - the Authentication properties display.
   b. **Device Information** - the Device Information properties display
3. From the list of Authentication properties, select **Authentication Login**. The **Authentication Login** dialog displays.
4. From the list of Device Information properties, select **Host is online**. The **Host is online** dialog displays.

Managing Endpoints – Aruba ClearPass Actions

CounterACT actions let you instruct CounterACT how to handle detected endpoints. For example, assign detected endpoint to an isolated VLAN or send an email to the endpoint user or the IT team.

The Aruba ClearPass Plugin makes the following actions available for use:

Action	Description
Assign ClearPass Tag	Instruct the ClearPass server, handling the detected endpoint, to assign the specified ClearPass tag to that endpoint. A tag consists of a name-value pair. The action's parameters are as follows (parameters required unless otherwise indicated): ▪ **Tag Name** - tag name to be assigned to the endpoint. ▪ **Tag Value** - tag value to be assigned to the endpoint. ▪ **Apply CoA** (*optional*) - select to instruct the ClearPass server to apply a change of authorization (CoA) to the endpoint following success of the action. Application of the CoA to a detected endpoint forces the endpoint to re-authenticate. ▪ **CoA Profile Name** - A CoA profile name is required by Aruba ClearPass in order for the ClearPass server to apply a change of authorization to an endpoint. When the **Managing ClearPass Server** property is not resolved (contains no information), CounterACT issues this action to all Aruba ClearPass servers assigned to the ClearPass server group. However, if the ClearPass server group is unknown to the plugin, CounterACT issues this action to all Aruba ClearPass servers assigned to all ClearPass server groups.

Action	Description
Delete ClearPass Tag	Instruct the ClearPass server, handling the detected endpoint, to delete the specified ClearPass tag from that endpoint. A tag consists of a name-value pair. The action's parameters are as follows (parameters required unless otherwise indicated): ▪ **Tag Name** - tag name identifying the tag (name-value pair) to be deleted from the endpoint. ▪ **Apply CoA** (*optional*) - select to instruct the ClearPass server to apply a change of authorization (CoA) to the endpoint following success of the action. Application of the CoA to a detected endpoint forces the endpoint to re-authenticate. ▪ **CoA Profile Name** - A CoA profile name is required by Aruba ClearPass in order for the ClearPass server to apply a change of authorization to an endpoint. When the **Managing ClearPass Server** property is not resolved (contains no information), CounterACT issues this action to all Aruba ClearPass servers assigned to the ClearPass server group. However, if the ClearPass server group is unknown to the plugin, CounterACT issues this action to all Aruba ClearPass servers assigned to all ClearPass server groups.

Apply these actions using any of the following ways:

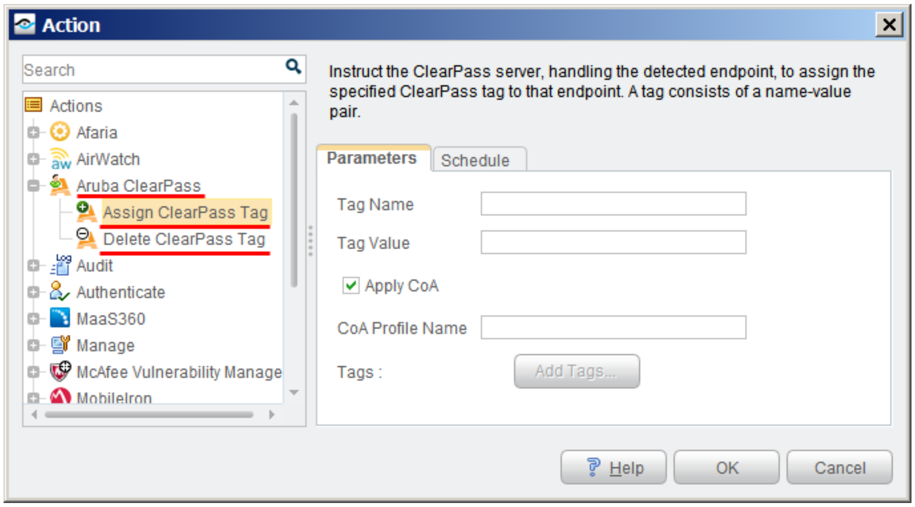
- Incorporate action in a policy
- Manually initiate action for a detected endpoint

To incorporate an Aruba ClearPass Tag action in a policy:

1. In the **Actions** pane of either a Policy → Main Rule or a Policy→Sub-Rule, select **Add…**.

   The **Action** window opens.

2. In the Action navigation tree, double-click **Aruba ClearPass**. The ClearPass actions display.



Instruct the ClearPass server, handling the detected endpoint, to assign the specified ClearPass tag to that endpoint. A tag consists of a name-value pair.

Tag Name

Tag Value

☑ Apply CoA

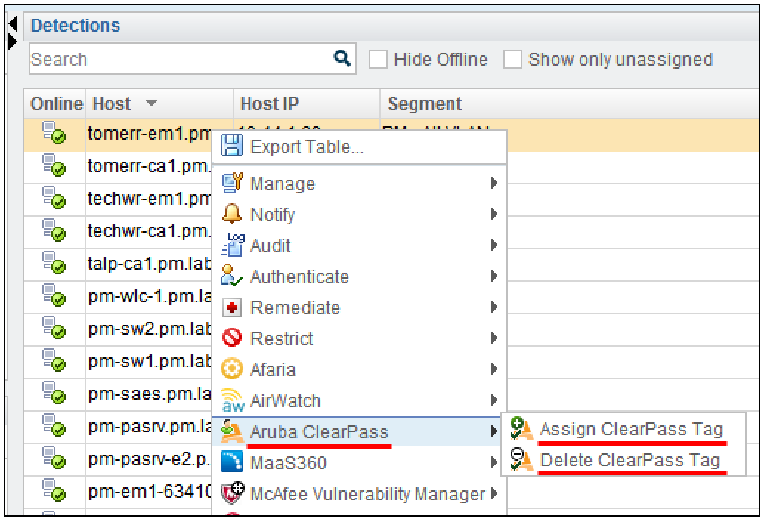
CoA Profile Name

Tags :

3. Select any of the following actions:
   c. **Assign ClearPass Tag**. Continue with step 4.
   d. **Delete ClearPass Tag**. Continue with step 5.
4. If you selected the **Assign ClearPass Tag** action, define the following in the **Parameters** tab:
   a. **Tag Name**
   b. **Tag Value**
   c. Select the **Apply CoA** checkbox (*optional*)
   d. If the **Apply CoA** checkbox is selected, you must enter a **CoA Profile Name**.
5. If you selected the **Delete ClearPass Tag** action, define the following in the **Parameters** tab:
   a. **Tag Name**
   b. Select the **Apply CoA** checkbox (*optional*)
   c. If the **Apply CoA** checkbox is selected, you must enter a **CoA Profile Name**.
6. Select **OK**.

To manually issue an Aruba ClearPass tag action for an endpoint:

1. In the **Detections** pane of the **NAC** tab, right-click an endpoint entry.
2. From the displayed menu, select **Aruba ClearPass**. The ClearPass actions display in a sub-menu.



3. From the sub-menu, select any of the following actions:
   a. **Assign ClearPass Tag**. Continue with step 4.
   b. **Delete ClearPass Tag**. Continue with step 5.

4. If you selected the **Assign ClearPass Tag** action, define the following in the **Parameters** tab:
   a. **Tag Name**
   b. **Tag Value**
   c. Select the **Apply CoA** checkbox (*optional*)
   d. If the **Apply CoA** checkbox is selected, you must enter a **CoA Profile Name**.
5. If you selected the **Delete ClearPass Tag** action, define the following in the **Parameters** tab:
   a. **Tag Name**
   b. Select the **Apply CoA** checkbox (*optional*)
   c. If the **Apply CoA** checkbox is selected, you must enter a **CoA Profile Name**.
6. Select **OK**.

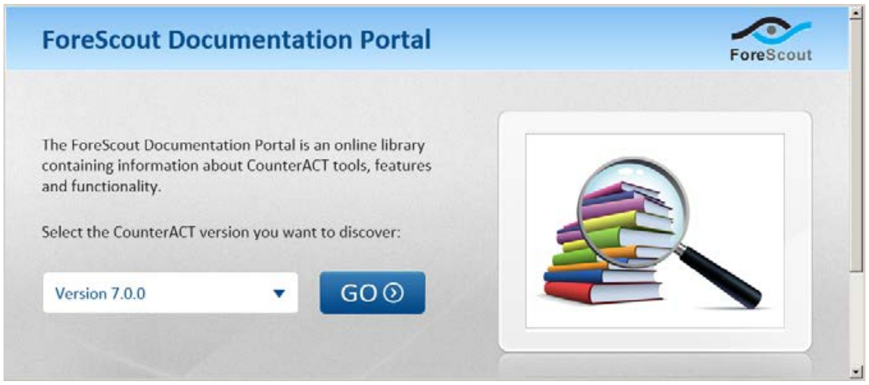
Additional CounterACT Documentation

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

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

Documentation Portal

The ForeScout Documentation Portal is Web-based library containing information about CounterACT tools, features and 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/kb.
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, hotfixes, plugins and modules and their related documentation. The portal also provides a variety of How-to Guides, Installation guides and more.

To access the Customer Portal:

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

CounterACT Console 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. Select **Options** from the **Tools** menu and then select **Plugins**.
2. Select a plugin and then select **Help**.

Documentation Portal

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

Legal Notice

This product is based on software developed by ForeScout Technologies. The products described in this document are protected by U.S. patents #6,363,489, #8,254,286, #8,590,004 and #8,639,800 and may be protected by other U.S. patents and foreign patents.

THIS SOFTWARE IS PROVIDED “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTIBILITY AND FITNESS FOR A PARTICULAR PURPOSE.

All other trademarks used in this document are the property of their respective owners.

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

10/7/2014 15:55:46