CounterACT™ Afaria MDM Plugin

Configuration Guide

Version 1.7.0 and Above

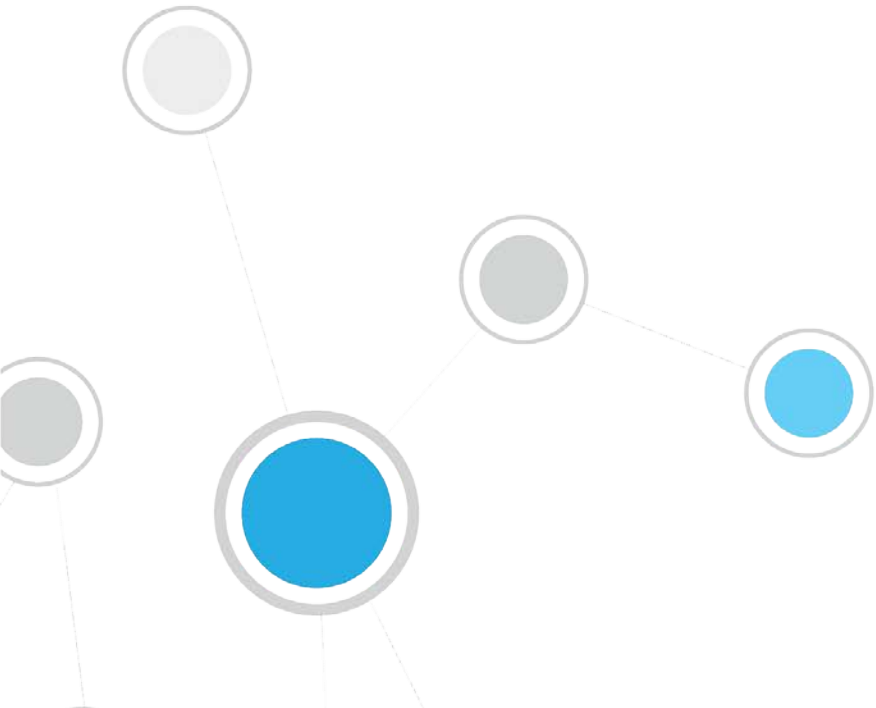


Table of Contents

About Afaria MDM Service Integration

CounterACT integration with the Afaria Mobile Device Management (MDM) service helps IT administrators streamline the process to provision, manage and secure today's expanding suite of smartphones and tablets, all from a single portal. The CounterACT/Afaria integration yields an easy to use platform that includes all of the essential functionality for end-to-end management of mobile devices. Secure and manage applications, documents and devices for global organizations and support both corporate and employee owned devices.

Instead of implementing new security silos that are limited to mobile devices, extend your PC and network security systems to encompass mobile devices.

CounterACT integration with MDM services provides a whole new level of centralized visibility and control of actionable insights for your entire computing landscape.

- ***Secure All Mobile Devices***: Supports all major smartphone and tablet platforms, including iOS and Android, in both Exchange and Lotus Notes environments.
- ***Manage Devices Outside the Corporate Network:*** Leverages integration with MDM services to manage devices even when they are not in the corporate network.
- ***Embrace BYOD***: Provides workflows to discover, enroll, manage and report on employee owned devices as part of your mobile device operation.
- ***Experience simple device enrollment and approval***: Provides a seamless and automatic process of quarantine and enrollment, upon device entry into the corporate network.

About This Plugin

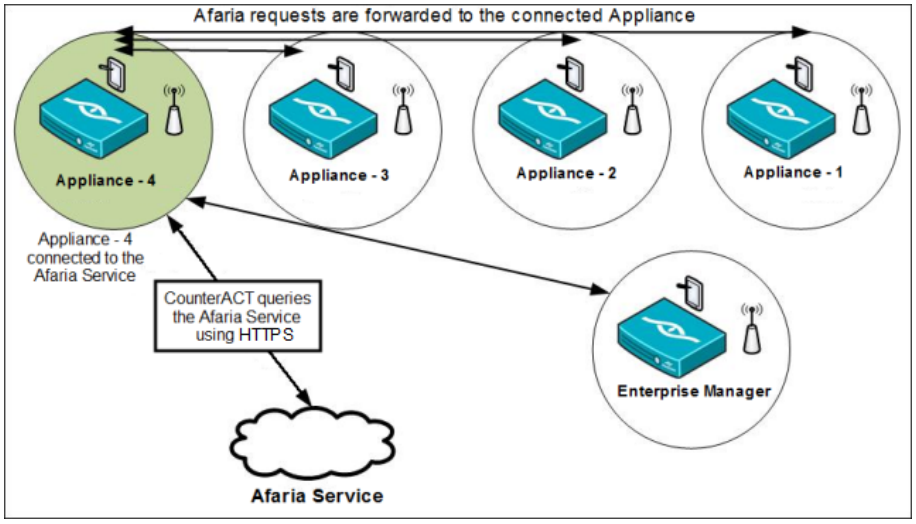
Integration of the Afaria MDM service with CounterACT lets you deliver a comprehensive MDM solution that provides powerful monitoring and enforcement capabilities not available when working solely with the Afaria MDM solution. Use the Afaria MDM plugin to complete the cycle of security by obtaining the following, vital capabilities:

- Automated real-time, continuous detection and compliance of mobile devices the moment they try to connect to your network, including unknown devices.
- Automated real-time, continuous detection and compliance of offsite mobile devices.
- Policy-based, unified NAC enforcement that limits network access based on device type, device ownership, time of day and policy compliance. Policy enforcement includes:
  - Allowing compliant and managed devices to join the network.
  - Limiting network access to a subset of applications and data, blocking access to more sensitive corporate resources.
  - Blocking noncompliant devices or specific types of devices from your network.

- Extends your organization's NAC visibility and control of mobile devices with a CounterACT inventory enriched by information retrieved from the Afaria MDM service.

How It Works

The Afaria MDM Plugin queries the Afaria Service for mobile device attributes, for example core attributes, security and compliance information and network information. All Afaria queries are performed by a single CounterACT Appliance – the *Afaria Connected Appliance* – that is designated for this purpose. The *Afaria Connected Appliance* retrieves information from other CounterACT Appliances and the CounterACT Enterprise Manager and forwards the information to the Afaria Service. Similarly, the Afaria Connected Appliance retrieves information from the Afaria service and forwards it to other CounterACT Appliances and the CounterACT Enterprise Manager.



Continuous Query Refresh

Afaria query mechanisms recheck endpoint attributes at a static frequency—approximately once a day. However, after plugin installation, querying of endpoint properties is based on CounterACT policy *recheck* definitions that define the conditions under which to recheck hosts that match a policy. You can specify:

- How often hosts are rechecked once they match a policy
- Under what conditions to carry out the recheck

Being able to define the *recheck* settings helps you ensure continuous, real-time endpoint evaluation.

The Afaria MDM web service API does not provide CounterACT with the ability to obtain a **last update timestamp** *for an Afaria MDM managed mobile device. Also, the Afaria MDM web service API does not provide the* **force check-in command**. *As a result of these two issues, Afaria provided mobile device information might not necessarily be up-to-date.*

Offsite Device Management

The plugin leverages integration with the Afaria MDM to manage devices even when they are not in the corporate network. The plugin retrieves updated host information for offsite devices through the Afaria MDM service. Offsite endpoints are identified and managed based on their MAC addresses. For more information, see Managing Offsite Devices.

Supported Devices

The following devices are supported by the Afaria MDM Plugin:

- iOS
- Android

For the version(s) of these operating systems that the Afaria MDM supports, refer to Afaria MDM documentation:

http://www54.sap.com/pc/tech/mobile/software/solutions/device-management

Supported Vendor Information

- Afaria MDM Service 7.00.x

Supported Network Infrastructures

- Devices connected to the network via a Wi-Fi connection
- The CounterACT/Afaria MDM service integration is accomplished using either an on-premise, server-based Afaria MDM service or an Afaria MDM cloud service.

Additional Documentation

Refer to Afaria online documentation for more information about the Afaria MDM solution: http://www54.sap.com/pc/tech/mobile/software/solutions/device-management/overview.html

What to Do

This section describes the required actions to establish CounterACT interoperation with the Afaria MDM service:

- Verify that you have met system requirements. See Requirements.
- Define an Afaria User for CounterACT.
- Verify proper Web Service setup on Afaria. See MDM Web Service Verification.

- Install the Plugin.
- Configure and Test the Plugin.
- Create Custom Policies.

Requirements

This section describes:

- CounterACT Software Requirements
- ForeScout Module License Requirements
- Networking Requirements
- Endpoint Requirements

CounterACT Software Requirements

The following product release works with this plugin:

- CounterACT version 7.0.0 with Hotfix 1.3 or above

  It is recommended to install the latest service pack to take advantage of the most current CounterACT updates.

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*.

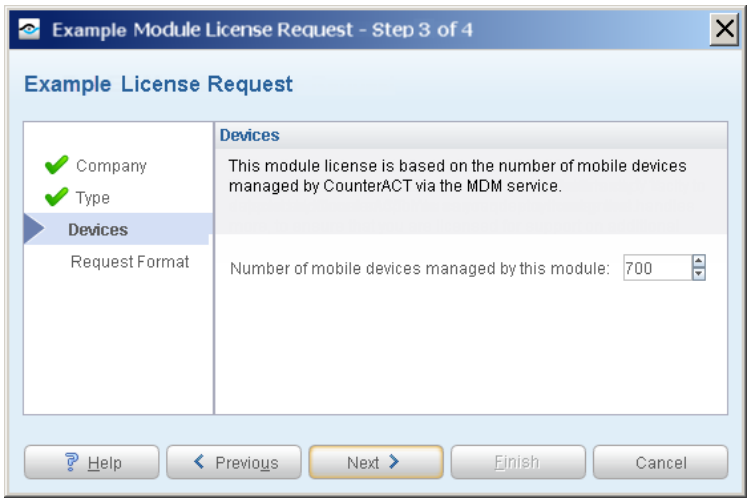
Demo license extension requests and permanent license requests are made from the CounterACT Console.

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 you want the license to support. Licenses for this module are based on the number of mobile devices managed by CounterACT via the MDM service.

Enter this number in the **Devices** pane of the Module License Request wizard, in the CounterACT, Console Modules pane.



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.

Networking Requirements

iOS mobile devices managed by the Afaria service cannot establish a connection to the Afaria service via a proxy. If a proxy is set up to serve your enterprise network, you must open port TCP/5223 to IP address/port 17.0.0.0/8 (the Apple Push Notification Server's IP address/port) on the enterprise firewall. By doing so, the proxy is bypassed when the mobile device accesses the Afaria MDM service.

Endpoint Requirements

Queries to MDM services are based on device MAC addresses. As such, CounterACT must learn device MAC addresses in order to initiate the query process. MAC addresses are learned from any of the following sources:

- Wireless plugin (Client table)
- Packet-Engine (ARP and DHCP traffic)
- L3 switches (ARP table)

Define an Afaria User for CounterACT

CounterACT logs in to the Afaria server using user credentials defined for it in the Afaria MDM service portal. These Afaria user credentials (username and password) are required when configuring the Afaria MDM Plugin in the Console.

To define an Afaria user for CounterACT use

1. In the Afaria service portal, navigate to **Server > Role > Edit**
2. Assign a <role_name> role to the user being defined that includes the following **Remote actions on devices** authorizations:
   - Connection Actions – **Send message**
   - Security Actions – **Delete device data**
   - Security Actions – **Lock**
   - Security Actions – **Remote wipe**
   - Security Actions – **Remove control**
3. In the **Tenant** tab, make sure that the <role_name> role is assigned to the corporate Tenant.
4. In the **Assignments** tab, make sure that the <role_name> role is assigned to the user being defined for CounterACT use.

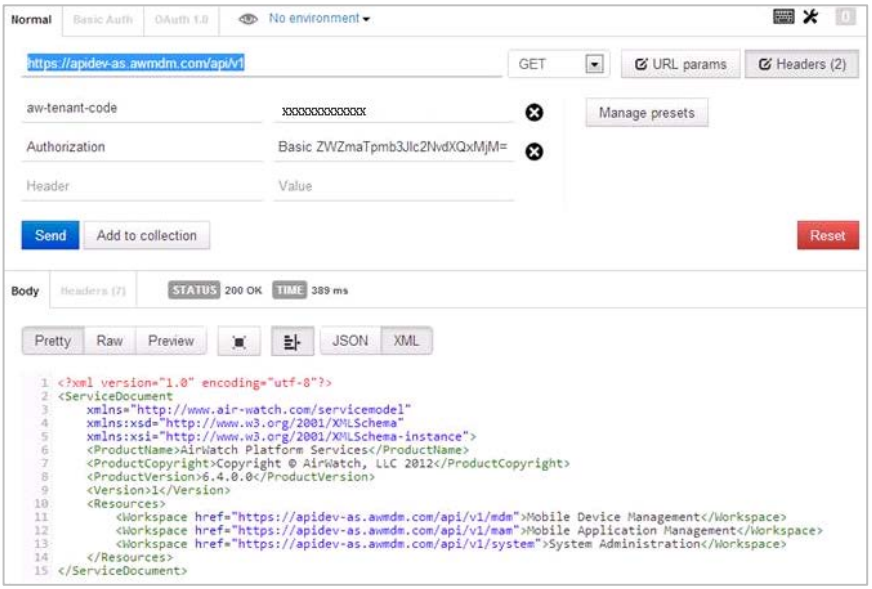
Make sure to record the defined user credentials (username and password); they are necessary for configuring the Afaria MDM Plugin in the Console.

MDM Web Service Verification

This section describes how to verify that the Web Service is properly set up. To verify setup, test REST API calls on the Afaria Server by verifying that the Afaria console supports Web services.

1. Install the Firefox *RESTClient* plugin from the following URL: http://addons.mozilla.org/en-US/firefox/addon/restclient/
2. Launch the *RESTClient* plugin by selecting **Tools -> RESTClient.**
3. In the REST client user interface, do the following:
   - Enter the URL of the REST API on the Afaria server, as follows: https://<*server URL*:*server port*>/ciscoise/mdminfo. Provide the same Afaria server URL and Afaria server port number that will be defined in Configure and Test the Plugin.
   - Define the HTTP header **Authorization** (basic). Provide the same username and password that will be defined in Configure and Test the Plugin.
4. Select **Send**.

   The REST client user interface displays the returned *Response* body; this information is provided in XML format.

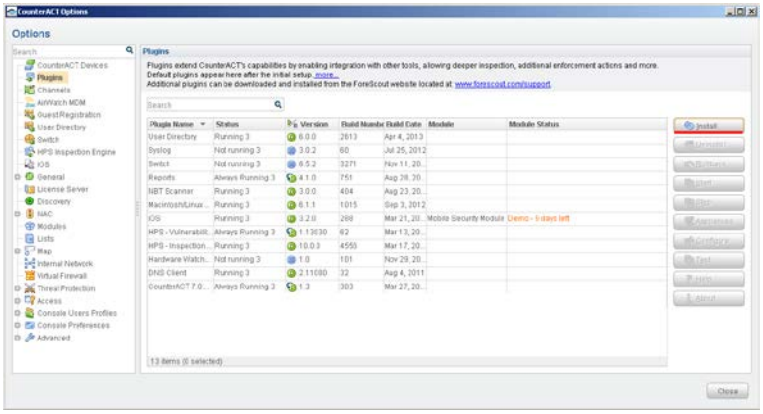


Install the Plugin

This section describes how to install the plugin.

To install the plugin:

1. Acquire a copy of the plugin in either one of the following ways:
   a. If you are installing a Beta release of this plugin, acquire the plugin .**fpi** file from your ForeScout representative or contact beta@forescout.com.
   b. 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 in to 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. 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 time remaining for the demo 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 **Start** to start the plugin. The Select Appliances dialog appears.
12. Select CounterACT Appliances on which the plugin should be started. The plugin must be running on every Appliance that may manage enrolled mobile devices. It is recommended to run the plugin on all Appliances in the environment.
13. Select **OK**. The plugin runs on the selected Appliances.

Once installed, the Afaria MDM Plugin automatically adds an HTTP Redirect exception to the CounterACT NAC Redirect Exception list. CounterACT NAC HTTP redirect exceptions are designed to ensure users can access business essential Internet sites or important files on the Internet while allowing required HTTP blocking and redirection. This exception ensures that devices can enroll with the Afaria service and still receive required HTTP notifications.

Configure and Test the Plugin

This section describes how to configure and test the plugin.

Configure the Plugin

Configure the plugin to enable it to communicate with the Afaria MDM service.

To configure the plugin:

1. In the CounterACT Console, select **Options** from the **Tools** menu.
2. Select **Plugins**.
3. In the Plugins pane, select **Afaria MDM** from the plugin listing and then select **Configure**. The **Afaria MDM** configuration pane opens.
4. In the **Access Afaria Service** tab, do the following:

- In the **Username** field, enter the username that CounterACT must provide to log in to the Afaria server (user credentials previously defined via the Afaria service portal).
- In the **Password** field, enter the password that CounterACT must provide to log in to the Afaria server (user credentials previously defined via the Afaria service portal).
- In the **Retype Password** field, enter the same password as provided in the previous step.
- In the **Afaria Server URL** field, enter the URL that CounterACT must use to communicate with the Afaria service.
- In the **Afaria Server Port** field, enter the port that CounterACT must use to communicate with the Afaria service.
- In the **Afaria Connected Appliance** field's dropdown list, select the CounterACT Appliance to serve as the communication channel between the Afaria service and your CounterACT Enterprise Manager and Appliances. ***The Enterprise Manager must not be selected***.

5. In the **Advanced** tab, do the following:
   - In the **MDM Query Threshold Interval** field, define, in seconds, how frequently the plugin is allowed to query the Afaria service. Use the default value unless otherwise advised.
   - In the **MDM Query Threshold** field, define the maximum number of requests that the plugin is allowed to send to the Afaria service during its allowed, query interval. Use the default value unless otherwise advised.
   - Select **Use a Proxy Server** when a proxy server is in use between the CounterACT ***Afaria Connected*** Appliance and the Afaria service.
     In the **DNS Name or IP Address of the Proxy Server** field, enter either the DNS name or the IP address of the proxy server.
     In the **Port Number** field, enter the required proxy server port.
   - Select **Support Offsite Devices**, if the plugin must handle offsite, mobile devices, these being, mobile devices that are not in the corporate network and the plugin uses the Afaria service to retrieve updated device information and implement CounterACT policy actions.
6. In the **Device to Test** tab's **Device MAC Address** field, enter the MAC address of an Afaria managed mobile device that will be used to test plugin operation. Use only lower case, alphanumeric characters and do not include any colons.
7. Select **Apply** to save your configuration changes.

Test Plugin Communication with the Afaria Service

Test the plugin communication with the Afaria service.

To test the plugin:

1. In the CounterACT Console, select **Options** from the **Tools** menu.
2. Select **Plugins**.

3. In the Plugins pane, select **Afaria MDM** from the plugin listing and then select **Configure**. The **Afaria MDM** configuration pane opens.
4. In the **Device to Test** tab's **Device MAC Address** field, verify that the MAC address of an Afaria managed mobile device is provided; this device MAC address is used to test plugin operation with the Afaria service.
5. In the Options pane, select **Plugins**.
6. In the Plugins pane, select **Afaria MDM** from the plugin listing.
7. Select **Test**.

   Using the configured plugin settings, CounterACT attempts to (a) connect with the Afaria service and (b) retrieve endpoint property values for the specified device.

Create Custom Policies

Create custom policies to detect, manage and remediate Afaria MDM managed mobile devices. Custom policy tools provide you with an extensive range of options for detecting and handling devices. This section describes the policy properties and actions available for use in a policy when the Afaria MDM Plugin is installed.

> *To create useful, effective policies that address the network access control requirements of your organization, you must have a solid understanding of CounterACT policies. See the CounterACT Templates and Policy Management chapters of the Console User Guide.*

Before running a custom policy that handles Afaria MDM managed mobile devices, consider first running any of the following:

- Policies based on the *Asset Classification*, *Mobile Classification*, *iOS Classification* and *Android Classification* templates. Policies based on these templates create groups and classify devices into these groups. Your custom policy can then use these groups to filter and select devices for detection, management and remediation.
- Policies based on the *Corporate/Guest Control* policy template. Policies based on this template create groups and classify devices into these groups. Your custom policy can then use the corporate/guest status of devices to filter and select devices for detection, management and remediation.

Multiple MDM Service Enrollment

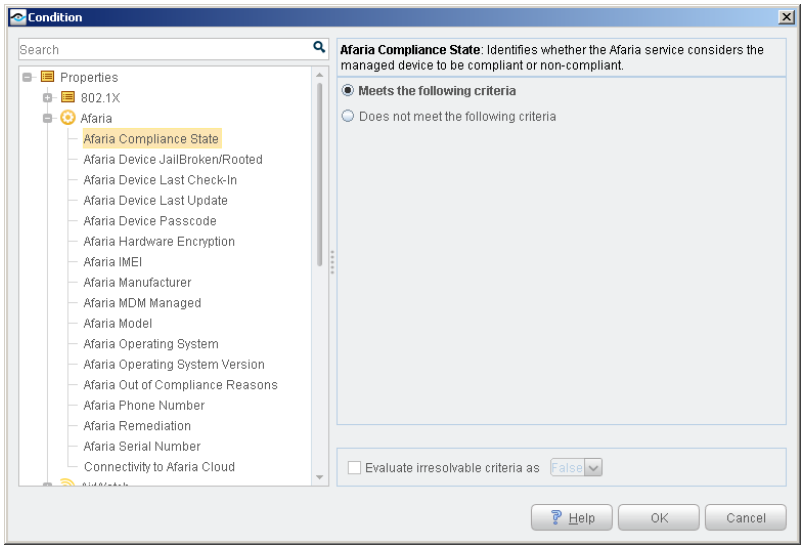
When additional MDM services are active in the network environment, other plugins of the MDM module may be installed. To support these plugins, policies may exist that enroll endpoints in other MDM services. These policies may attempt to enroll endpoints managed by Afaria in their MDM services. When additional plugins of the MDM module are installed, edit MDM enrollment policies to exclude endpoints that are already enrolled in Afaria (or another active MDM service).

For example:

- If MDM services are deployed by network segment, use Scope settings to limit the endpoints examined by each MDM enrollment policy, and exclude segments with Afaria users.
- Add a rule that detects endpoints enrolled in Afaria (for example, using the *Afaria MDM Managed* host property). The policy should not enroll these endpoints in another MDM service.

Detecting Afaria Devices – Policy Properties

CounterACT properties let you detect devices based on information from Afaria. In the Conditions screen, expand the Afaria folder in the Properties tree to use these properties in a policy condition.



The following properties, describing various aspects of an Afaria managed mobile device, are available:

Afaria Compliance State	Identifies whether the Afaria service considers the managed device to be compliant or non-compliant.
Afaria Device JailBroken/Rooted	Identifies a jailbroken iOS device or a rooted Android device.
Afaria Device Last Check-In	The date and time when the Afaria service last communicated with the managed device.
Afaria Device Last Update	The date and time when CounterACT last received an information update about the managed device from the Afaria service.
Afaria Device Passcode	Identifies whether a passcode must be used to unlock the managed device from a locked state.
Afaria Hardware Encryption	Identifies whether encryption is in use (Yes) or not in use (No) in the managed device.
Afaria IMEI	The IMEI number of the managed device.
Afaria Manufacturer	The manufacturer of the managed device.

Afaria MDM Managed	Indicates if the device is registered with the Afaria service.
Afaria Model	The model of the managed device.
Afaria Operating System	The operating system running on the managed device.
Afaria Operating System Version	The version of the operating system running on the managed device.
Afaria Out of Compliance Reasons	The Afaria service's reason for the managed device's non-compliant state.
Afaria Phone Number	The phone number of the managed device.
Afaria Remediation	The Afaria service's recommended remediation action to perform to make the managed device compliant.
Afaria Serial Number	The serial number of the managed device.
Connectivity to Afaria Cloud	Identifies whether CounterACT's most recent communication attempt with the Afaria service was successful (Yes) or not successful (No).

Managing Afaria Devices – Policy Actions

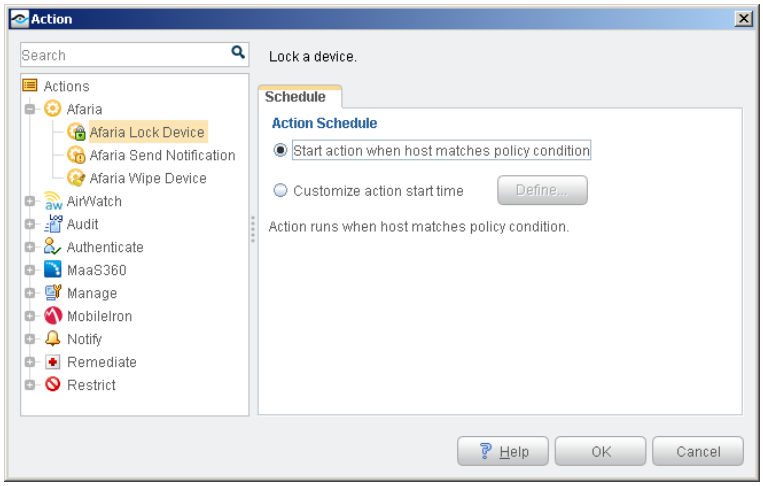
CounterACT policy actions let you apply Afaria service actions to mobile devices based on CounterACT policy detections.

In the Actions screen, expand the Afaria folder in the Actions tree to use Afaria actions in a policy. You can apply the following actions to mobile devices that are detected by a CounterACT policy.

- Afaria Lock Device Action
- Afaria Send Notification Action
- Afaria Wipe Device Action

Afaria Lock Device Action

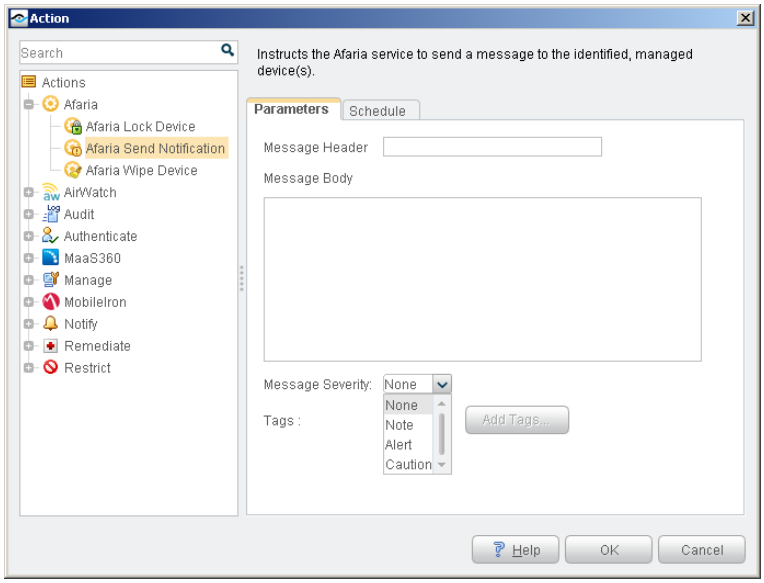
By executing this action, CounterACT instructs the Afaria service to lock the identified managed device(s). You schedule the action’s execution.



Afaria Send Notification Action

By executing this action, CounterACT instructs the Afaria service to send a notification to the identified managed device(s). You define the following action parameters:

- The message header and body content
- The message severity (none, note, alert caution)
- Schedule the action's execution

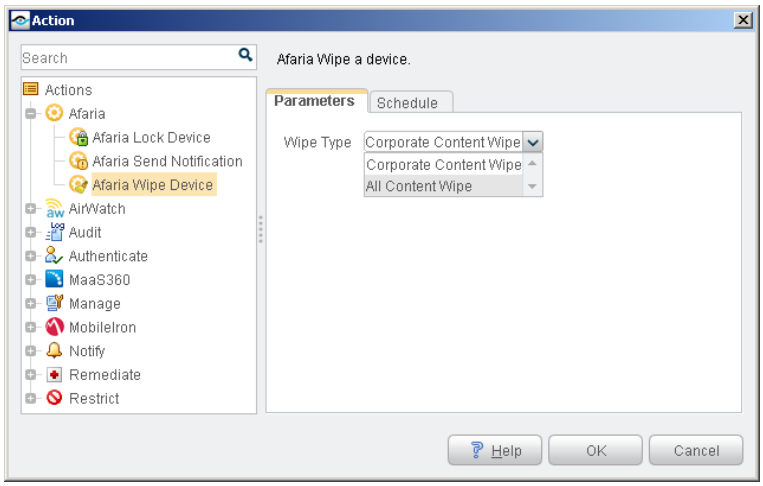


Afaria Wipe Device Action

By executing this action, CounterACT instructs the Afaria service to wipe the identified managed device(s). You define the following action parameters:

- The wipe to perform (only corporate content, all content) header and body content of the message

- Schedule the action's execution



Managing Offsite Devices

When Afaria MDM managed mobile devices are not in the corporate network, the plugin uses the Afaria service to retrieve updated host information and implement CounterACT policy actions.

To configure support for the management of offsite devices:

- Select the **Support Offsite Devices** checkbox, when configuring the plugin. See Configure the Plugin.

Consider the following when you create CounterACT policy conditions and actions that apply to offsite devices:

- CounterACT identifies offsite devices by their MAC address. To manage offsite devices, policies must include devices without a known IP address in their scope.
- All host properties can be evaluated for offsite devices.
- All Afaria MDM Plugin provided actions can be applied to offsite devices. See Managing Afaria Devices – Policy Actions.
- A limited number of general CounterACT actions (that is, those not provided by the Afaria MDM Plugin) can be applied to offsite devices. These actions are:
  - Manage: Add to Group / Classify / Delete host
  - Notify: Send email

Restriction and HTTP redirection actions cannot be applied to offsite devices.

Display Inventory Data

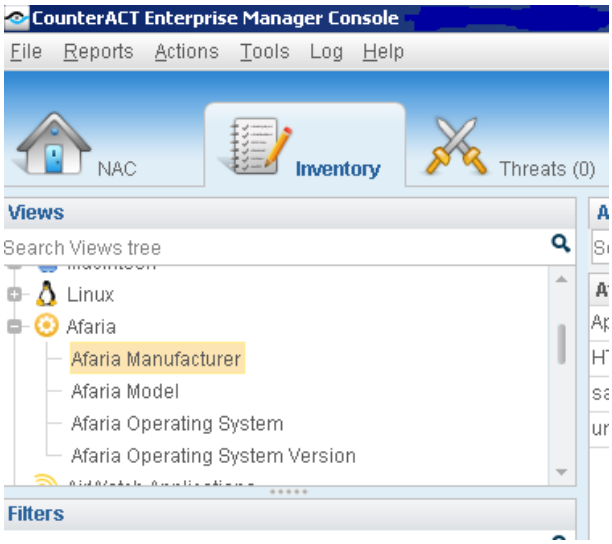
Use the CounterACT Inventory to view a real-time display of Afaria device network activity at multiple levels, for example, software installed, core attributes.

The inventory enables you to:

- Broaden your view of the organizational network from device-specific to activity-specific
- View Afaria MDM managed mobile devices that have been detected with specific attributes
- Easily track Afaria MDM managed mobile device activity
- Incorporate inventory detections into policies

To access the inventory:

1. Select the **Inventory** icon from the Console toolbar.
2. Navigate to the Afaria entries.



The following information, based on Afaria host properties, is available:

- Afaria Manufacturer
- Afaria Model
- Afaria Operating System
- Afaria Operating System Version

For information about how to work with the CounterACT Inventory, refer to either *Working at the Console > Working with Inventory Detections* in the *CounterACT Console User Manual* or the Console, Online Help.

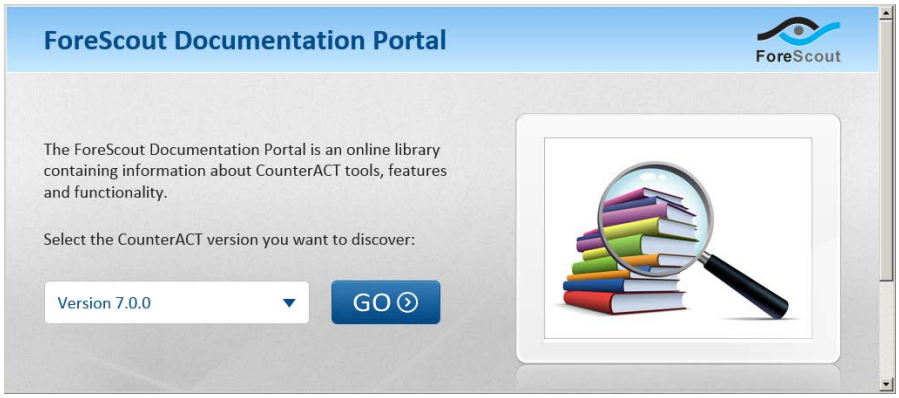
Additional CounterACT Documentation

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:

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, 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

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