



# FortiNAC

## Airwatch MDM Device Integration

Version: 8.x

Date: April 6, 2021

Rev: J

**FORTINET DOCUMENT LIBRARY**

<http://docs.fortinet.com>

**FORTINET VIDEO GUIDE**

<http://video.fortinet.com>

**FORTINET KNOWLEDGE BASE**

<http://kb.fortinet.com>

**FORTINET BLOG**

<http://blog.fortinet.com>

**CUSTOMER SERVICE & SUPPORT**

<http://support.fortinet.com>

**FORTINET COOKBOOK**

<http://cookbook.fortinet.com>

**NSE INSTITUTE**

<http://training.fortinet.com>

**FORTIGUARD CENTER**

<http://fortiguard.com>

**FORTICAST**

<http://forticast.fortinet.com>

**END USER LICENSE AGREEMENT**

<http://www.fortinet.com/doc/legal/EULA.pdf>

# Contents

Overview .....	4
What it Does .....	4
How it Works .....	4
Requirements .....	4
Integration .....	5
Configure Airwatch .....	5
Configure the API Key in AirWatch.....	5
Set Up and Test Notifications (Recommended) .....	5
Configure FortiNAC .....	6
MDM Services .....	6
Captive Portal Configuration .....	9
Allowed Domains .....	9
Events .....	9
Policies .....	10
Mobile Devices.....	11
Troubleshooting Tips .....	12
Related KB Articles.....	12
Debugging.....	12
Appendix .....	13
AirWatch Host/Device Registration Process.....	13
Methods to Export FortiNAC SSL Certificate.....	14
FireFox.....	14
Chrome.....	14
FortiNAC CLI .....	14
Importing Airwatch SSL Certificates to FortiNAC.....	15

# Overview

The information in this document provides guidance for configuring the Airwatch device to be managed by FortiNAC. This document details the items that must be configured.

**Note:** As much information as possible about the integration of this device with FortiNAC is provided. However, the hardware vendor may have made modifications to the device's firmware that invalidate portions of this document. If having problems configuring the device, contact the vendor for additional support.

## What it Does

This integration speeds up the registration process of mobile devices and eliminates the need to install both the FortiNAC agent and the AirWatch Agent on a mobile device.

## How it Works

Mobile devices managed by Airwatch connecting to the network can be registered in FortiNAC using information stored in the AirWatch database. When a rogue host is detected on the network, FortiNAC connects to AirWatch, retrieves the host data from the AirWatch database and registers the host in FortiNAC. AirWatch is polled periodically in order to update records for those hosts that are already registered in FortiNAC. For details, refer to the Appendix topic [AirWatch Host/Device Registration Process](#).

**Note:** If there are multiple FortiNAC systems (PODs) and they are managed with a Network Control Manager (NCM), it is only necessary to configure the integration on one of the FortiNAC Servers. The host records will be propagated, on demand, to the other PODs.

## Requirements

- AirWatch is in place and managing mobile devices
- FortiNAC firmware version 3.x (CentOS) or higher to send notifications to FortiNAC when devices are added to or removed from the AirWatch database

# Integration

## Configure Airwatch

### Configure the API Key in AirWatch

1. Login to AirWatch and navigate to **Menu > Configuration > System Configuration > System >Advanced >API >REST API**. Enable API Access should be checked. The API Key generated is used later in the FortiNAC MDM Services configuration.
2. On the REST API screen, click **Authentication** and make sure **Basic** is selected.
3. Determine the URL to which FortiNAC must connect to access the REST API. This URL is used in the FortiNAC MDM Services configuration. If unknown, contact AirWatch for assistance.
4. Configure a **System Administrator** user in AirWatch to be used by FortiNAC for authentication when requesting data.

**Note:** AirWatch requires a role for each Administrator user. When selecting a role for the Administrator user, make sure that role has permission for REST API.

### Set Up and Test Notifications (Recommended)

Airwatch can be configured to send notifications to FortiNAC when devices are deleted or updated in the Airwatch database. If notifications are not configured in Airwatch, this information will be obtained during the next poll of the MDM. See [MDM Services](#) for details on MDM Polling.

1. Navigate to **Menu > Configuration > System Configuration > System >Advanced >API >Event Notification**.
2. Click **Edit Event Notification** to bring up the dialog box.
3. Enter the following settings into the Event Notification dialog box:
  - Target Name: nsserver
  - Target URL: `https://{nsserver}:8443/api/notifications` (where {nsserver} is the eth0 IP address or hostname of the FortiNAC server)
  - **Note:** In High Availability (HA) configurations, AirWatch must be configured to push data to the hostnames or eth0 IP addresses of both Primary and Secondary Control Servers
  - User Name: nsadminuser
  - Password: nsadminuserpassword
  - Format: Select **XML**
  - Events: Select **all Events**
4. Click **Save**.
5. Browse to `https://{nsserver}:8443/api/notifications` and download the SSL certificate. See Appendix topic [Methods to Export FortiNAC SSL Certificate](#).
6. Import the SSL certificate into Airwatch.
7. Click **Test Connection**. If notifications have been set up correctly, the message **Test is successful** is returned.

# Configure FortiNAC

## MDM Services

Configure a MDM Service to establish a connection with the AirWatch server. MDM Services allows you to configure the connection or integration between FortiNAC and a Mobile Device Management (MDM) system. FortiNAC and the MDM system work together sharing data via an API to secure the network. FortiNAC leverages the data in the MDM database and registers hosts using that data as they connect to the network.

**Important:** Proxy communication is not supported.

1. In the Administrative UI, navigate to **System > Settings > System Communication > MDM Services** and click **Add**.

**Add MDM Service**

MDM Vendor: Air Watch

Name:

Request URL:

User ID:

Password: Show

Identifier:

Enable On Demand Registration

Revalidate Health Status on Connect

Remove Hosts Deleted from MDM Server

Enable Application Updating

Enable Automatic Registration Polling 1 Days

OK Cancel

2. Use the field definitions for the MDM Services in the following table to enter the MDM Service information.

## MDM Services Field Definitions

Field	Definition
<b>MDM Vendor</b>	Name of the vendor of the MDM system.
<b>Name</b>	Name of the connection configuration for the connection between an MDM system and FortiNAC.
<b>Request URL</b>	The URL for the API to which FortiNAC must connect to request data. This will be a unique URL based on your MDM system. <b>Note:</b> Requires the server name (Example: https://services.m3.mydomain.com)
<b>Identifier</b>	A type of key used to identify FortiNAC to the MDM server. This field is not required for all MDM products.  In the case of AirWatch, this is the API Key generated during the AirWatch Configuration. An API key is a unique code that identifies the FortiNAC server to AirWatch and is part of the authentication process for AirWatch.
<b>User ID</b>	User name of the account used by FortiNAC to log into the MDM system when requesting data.
<b>Password</b>	Password for the account used by FortiNAC to log into the MDM system when requesting data.  This field displays only when adding a new MDM connection configuration. It is not displayed in the table of MDM servers.
<b>Enable Automatic Registration Polling (MDM Polling)</b>	Indicates how often FortiNAC should poll the MDM system to collect managed device information. Each time a poll executes, queries are sent to the AirWatch for: <ul style="list-style-type: none"> <li>• The managed device list (one query per 100 entries)</li> <li>• One additional query per each managed device</li> </ul> <p>If <a href="#">AirWatch notifications</a> are configured, set the MDM Poll frequency to <b>1 Day</b>. If notifications are not configured, the frequency can be set higher.</p> <p><b>Note:</b> When choosing an interval, consider the number of queries sent per MDM poll, the size of the AirWatch database and the number of PODs integrated with the same AirWatch system. If the frequency is set too high, AirWatch may not be able to manage the rate of queries from FortiNAC, causing performance issues.</p>
<b>Last Poll</b>	Date and time of the last poll.
<b>Last Successful Poll</b>	Date and time of the last poll that successfully retrieved data.
<b>Create Date</b>	Date that this connection configuration was set up.
<b>On Demand Registration</b>	If enabled, when an unknown host reaches the captive portal, FortiNAC queries the MDM server for information about that host. If the host exists in the MDM server, it is registered in FortiNAC using the data from the MDM server.
<b>Revalidate Health Status On Connect</b>	If enabled, when the host connects to the network FortiNAC queries the MDM server to determine if the host is compliant with MDM policies. <b>NOTE:</b> This setting is disabled by default. When enabled, the MDM may not be able to manage the rate of queries from FortiNAC, causing performance issues. Instead of enabling Revalidate Health Status On Connect, you can enable automatic registration polling to occur once a day, which will also retrieve Health Status, but with less frequency.

<b>Remove Hosts</b>	If enabled, when FortiNAC polls the MDM server it deletes hosts from the FortiNAC database if they have been removed or disabled on the MDM server.
<b>Update Applications</b>	If enabled, when FortiNAC polls the MDM server it retrieves and stores the Application Inventory for hosts that are in the FortiNAC database. <b>NOTE:</b> This setting is disabled by default. When enabled, the MDM may not be able to manage the rate of queries from FortiNAC, causing performance issues.
<b>Last Modified By</b>	User name of the last user to modify the connection configuration.
<b>Last Modified Date</b>	Date and time of the last modification to this connection configuration.

### Right Click Options

<b>Delete</b>	Deletes the MDM Service.
<b>Modify</b>	Opens the Modify MDM Service dialog.
<b>Poll Now</b>	Polls the MDM server immediately.
<b>Show Audit Log</b>	Opens the Admin Auditing Log showing all changes made to the selected item. For information about the Admin Auditing Log, refer to <a href="#">Administration Guide</a> Topic <b>Admin Auditing</b> . <b>Note:</b> You must have permission to view the Admin Auditing Log. See <b>topic Add An Admin Profile</b> in the <a href="#">Administration Guide</a> .
<b>Test Connection</b>	Tests the connection between the selected MDM server and FortiNAC. Error messages indicate which fields are missing or incorrect.

### Buttons

<b>Add</b>	Opens the Add MDM Service dialog.
<b>Modify</b>	Opens the Modify MDM Service dialog.
<b>Export</b>	Exports the data displayed to a file in the default downloads location. File types include CSV, Excel, PDF or RTF. See <b>Export Data</b> in the <a href="#">Administration Guide</a> .
<b>Test Connection</b>	Tests the connection between the selected MDM server and FortiNAC. Error messages indicate which fields are missing or incorrect.
<b>Poll Now</b>	Polls the MDM server immediately.

3. Click **OK** to save.

### Note the following:

- The **Revalidate Health Status On Connect** and **Update Applications** settings are disabled by default. When enabled, the MDM may not be able to manage the rate of queries from FortiNAC, causing performance issues.
- Instead of enabling **Revalidate Health Status On Connect**, you can enable automatic registration polling to occur once a day, which will also retrieve Health Status, but with less frequency.

## Captive Portal Configuration

Navigate to the Content Editor and modify the Portal Configuration content to redirect mobile devices to AirWatch if the device does not have an AirWatch MDM Agent installed.

1. Navigate to **System > Portal Configuration**.
2. Under the **Content Editor** tab, expand **Global** and click **Settings**.
3. Select **Use Configured MDM**.
4. Expand **Registration** and click **MDM Registration**.
5. In the **Content** field, include links to the web sites where users can download the appropriate MDM agent for their device (devices that have an AirWatch Agent should never reach the captive portal). For example, if the user is connecting to the network with an iPhone, there must be a link to the page in the iTunes store where the Apple MDM agent can be downloaded. Refer to Online Help Topic **Portal Content Editor** for additional information.

## Allowed Domains

Devices needing to download an MDM agent must have access to the appropriate web site. Confirm that the necessary web sites are listed in the Allowed Domains view. Unregistered hosts can only navigate to sites listed in Allowed Domains.

Navigate to **System > Settings > Control > Allowed Domains**.

Refer to Online Help Topic **Allowed Domains** for additional information.

**Note:** For AirWatch cloud implementations, add **awada.com** to the list of Allowed Domains.

## Events

Events associated with the AirWatch integration can be enabled and mapped to alarms. Events include:

- MDM Host Created
- MDM Host Destroyed
- MDM Poll Failure
- MDM Poll Success
- MDM Host Compliance Failed
- MDM Host Compliance Passed

Hosts can be marked "at risk" when the host is not in Compliance with an Airwatch policy by using an Alarm mapped to the MDM Host Compliance Failed event.

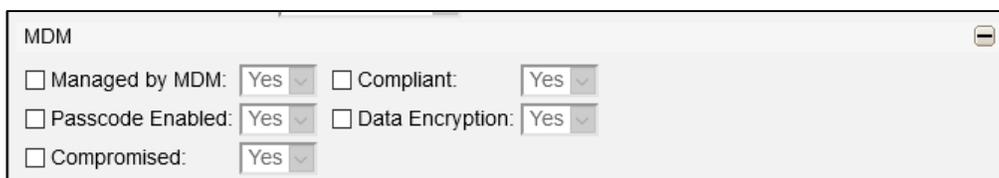
Refer to Online Help Topic **Enable And Disable Events** and **Map Events To Alarms** for additional information.

## Policies

Configure policies to automatically provision network access based upon specific criteria as registered hosts connect to the network. Network Access Policies are comprised of two components:

- **User/Host Profile:** Defines user and/or host data criteria used to assign Network Access Policies. Additional fields that are specific to MDM Services have been added to the host record and can be used as a filter in User/Host Profiles. Refer to **Host View And Search Field Definitions** in the Online Help or the Administration and Operation guide in the [Fortinet Document Library](#) for additional information.

Managed by MDM	FortiNAC registered the host based on data from MDM database.
Compliant	FortiNAC gathered endpoint compliance information from the MDM server and marks the host as compliant with MDM policies or not. <b>Note:</b> Does not list vulnerabilities.
Passcode enabled	Indicates if there is a passcode required to access the endpoint.
Data Encryption	Indicates whether data encryption is enabled on the endpoint.
Compromised	This is an additional field separate from whether it's complaint, if the MDM marks the endpoint as compromised.



The screenshot shows a configuration panel titled "MDM" with a close button in the top right corner. It contains five rows of settings, each with a checkbox and a dropdown menu:

- Managed by MDM:  Yes
- Compliant:  Yes
- Passcode Enabled:  Yes
- Data Encryption:  Yes
- Compromised:  Yes

- **Network Access Configuration:** Specifies the network access value (VLAN or role) to apply when a host matches the associated User/Host Profile.

**Example:** Place all iOS devices on VLAN 10 and all Android devices on VLAN 11.

Apple Network Access Policy:

- User/Host Profiles specifying iOS operating system
- Network Access Configuration specifying VLAN 10

Android Network Access Policy:

- User/Host Profile specifying Android operating system
- Network Access Configuration specifying VLAN 11

Refer to **Network Access Policies** in the Online Help or the Administration and Operation guide in the [Fortinet Document Library](#) for additional information.

## Mobile Devices

**Note:** Hosts cannot register or connect to the network via VPN using the AirWatch MDM Agent. Hosts that need to connect via VPN must have a FortiNAC Agent installed.

- Each managed device must have the AirWatch MDM Agent installed. Refer to the AirWatch documentation for instructions.
- If a device connects to the network and no AirWatch MDM Agent is detected, the FortiNAC captive portal displays a message indicating that no MDM agent has been detected. Links to the appropriate site to download the agent are displayed. Some sample links are preconfigured, however, you must go to the Portal Content Editor and add the links that allow the different device types and operating systems to download the appropriate agent.
- Mobile devices registered using the AirWatch database are registered to a user if that user currently exists in FortiNAC. If the user does not exist in the FortiNAC database the device is registered as a device.
- Additional fields that are specific to MDM Services have been added to the host record and can be used as a filter in User/Host Profiles. Refer to Online Help Topic **Host View And Search Field Definitions** for additional information.
- Mobile devices registered from AirWatch will be assigned one of the following roles:
  - Employee Owned
  - Corporate - Shared
  - Corporate - Dedicated
  - NAC - Default (if not defined in AirWatch)

These roles can be used as a filter in User/Host Profiles. Roles that are defined by AirWatch are not added to the list of possible roles in FortiNAC and will not be available in any drop-down lists used for role assignment.

- FortiNAC also retrieves a list of installed applications for each registered device from AirWatch. Refer to Online Help Topic **Application Inventory** for additional information.

# Troubleshooting Tips

**Symptom:** When attempting to poll MDM, a message similar to the following appears:

```
"Failure: An unknown error occurred. javax.net.ssl.SSLHandshakeException:  
sun.security.validator.ValidatorException: PKIX path building failed:  
sun.security.provider.certpath.SunCertPathBuilderException: unable to find valid certification  
path to requested target"
```

**Solution:** Ensure that the entire certificate path, including any intermediate certificates, are imported to the FortiNAC's keystore. See [Importing Airwatch SSL Certificates to FortiNAC](#).

## Related KB Articles

[Airwatch poll fails with 429 error code](#)

[MDM poll failure with certification path error](#)

[AirWatch MDM poll fails when configured to retrieve application data](#)

[Certificate path error when polling Airwatch](#)

[Airwatch MDM Agent fails to authenticate in isolation](#)

[Unknown Employee and Corporate roles](#)

## Debugging

Enable debugging feature (prints to /bsc/logs/output.master):

```
CampusMgrDebug -name AirWatchServer true
```

```
CampusMgrDebug -name MdmManager true
```

Disable debugging feature

```
CampusMgrDebug -name AirWatchServer false
```

```
CampusMgrDebug -name MdmManager false
```

**Note:** Debugs disable automatically upon restart of FortiNAC control and management processes.

# Appendix

## AirWatch Host/Device Registration Process

When AirWatch and FortiNAC are integrated, the registration process for hosts is as follows:

1. A host connects to the network and is detected by FortiNAC.
2. If the host is running an operating system not supported by AirWatch, it becomes a rogue and goes through the regular registration process (either through the captive portal, Device Profiler or any other registration method configured in FortiNAC).
3. If the host is running one of the operating systems listed below, FortiNAC checks to see if the AirWatch MDM Agent is installed. This requires that On-Demand registration be enabled in the MDM Service record for the AirWatch integration with FortiNAC.
  - Android
  - Apple iOS
  - BlackBerry
  - Mac OS X
  - Symbian
  - Windows Mobile
  - Windows Phone
4. Hosts without the AirWatch MDM Agent are sent to the captive portal where the user is asked to download and install an MDM agent before connecting to the production network.
5. If the host has the AirWatch MDM Agent installed, FortiNAC connects to AirWatch and retrieves the host data from the AirWatch database and registers the host in FortiNAC.
6. If the host is associated with a user in AirWatch that also exists in FortiNAC, then the host is registered to that user.
7. If the user is unknown in FortiNAC, the host is registered as a device.
8. Based on the User/Host Profile that matches the host, a Network Access Policy is applied and the host is placed in the appropriate VLAN.
9. Settings selected for the MDM Service that controls the connection between AirWatch and FortiNAC determine when AirWatch is polled for updated information.

# Methods to Export FortiNAC SSL Certificate

## FireFox

To export certificate to use for other browsers:  
Browse to `https://<appliance name>:8443`  
The message "Your connection is not secure" displays.  
Click the padlock or "i" next to the URL  
Click the > next to the host name  
Click More Information  
Under the Details tab click the Export button.  
Save the file using the format required for Airwatch.

## Chrome

Browse to `https://qa6-74.bradfordnetworks.com:8443`  
Click on the padlock (view site information)  
Click Certificate  
Click Details tab  
Click Copy to File  
Run through the Certificate Export Wizard, save the file using the format required for Airwatch (DER, Base-64, PKCS #7, etc)  
After exporting file, click OK.

## FortiNAC CLI

a. SSH to the FortiNAC Server or Control Server and type  
`echo -n | openssl s_client -connect <appliance name>:8443 | sed -ne '/-BEGIN CERTIFICATE-/,/-END CERTIFICATE-/p' > server.cert`

Example:

```
echo -n | openssl s_client -connect qa6-74.bradfordnetworks.com:8443 | sed -ne '/-BEGIN
CERTIFICATE-/,/-END CERTIFICATE-/p' > server.cert
depth=0 CN = qa6-74.bradfordnetworks.com
verify error:num=18:self signed certificate
verify return:1
depth=0 CN = qa6-74.bradfordnetworks.com
verify return:1
DONE
```

b. ftp or scp file to desired location.  
`ftp <destination ip or name>`  
`scp server.cert root@<location>:/<path>`

## Importing Airwatch SSL Certificates to FortiNAC

If the Airwatch REST API communication is secured using SSL certificates, it may be necessary to import the certificates. This ensures Airwatch will trust communication (such as polling) from FortiNAC. Otherwise, communication may fail.

1. Obtain the leaf SSL certificate used by Airwatch.
2. Copy certificate file to **/bsc/campusMgr/** directory in the FortiNAC Server or Control Server.
3. If file not already in PEM format, convert the file:

```
openssl x509 -inform der -in <DER FORMATTED FILE> -out <PEM FORMATTED FILE>
```

4. Choose a unique alias for the certificate. The alias needs to be unique for each certificate file and should ideally describe why it's there. Examples used below:

```
AWCert
```

5. Import Leaf Airwatch Certificate:

```
keytool -import -alias AWCert -file <AirWatch Certificate File> -keystore  
/bsc/campusMgr/.keystore -storepass ^8Bradford%23
```

6. View the results in the keystore:

```
keytool -list -v -keystore /bsc/campusMgr/.keystore -storepass ^8Bradford%23
```

7. Reboot FortiNAC Server/Control Server:

```
shutdownCampusMgr  
shutdownCampusMgr -kill  
reboot
```



**FORTINET®**



Copyright© 2020 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.