FortiNAC

Jamf MDM Integration

Version: 8.8

Date: April 6, 2021

Rev: B

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

FORTINET

Contents

Overview

The information in this document provides guidance for configuring integration in order for FortiNAC to manage devices registered using a Jamf MDM Server.

Note: As much information as possible about the integration of this device with FortiNAC is provided. However, the vendor may have made modifications to the API used to communicate with the Jamf server that would invalidate portions of this document. If having problems configuring the device, contact the vendor for additional support.

What it Does

Jamf is an endpoint management solution that enables scalable and centralized management of Apple mobile devices and personal computers:

- Efficient and effective administration of endpoints
- Designed to maximize operational efficiency and includes automated capabilities for device management and troubleshooting

This integration speeds up the registration process of devices that have been registered with Jamf. Devices connecting to the network can be registered in FortiNAC using host data from Jamf. FortiNAC can also gather application data from the Jamf server to assist in FortiNAC Policy creation.

How it Works

When a rogue host is detected on the network, FortiNAC communicates with Jamf and retrieves the host data. FortiNAC registers the host found on the Jamf server. FortiNAC polls Jamf periodically in order to update records for those hosts already registered in FortiNAC.

FortiNAC collects the following host data from Jamf:

- Type (MacOS/IOS primarily)
- IOS/OSX
- Owner (User)
- Host Name
- Application Data (if configured)

Requirements

- Jamf
  - Pro version
  - Server version 10.X or higher
  - Jamf is in place and registering devices
  - Administrator account for API access
- FortiNAC version 8.8.0 or higher

Jamf Integration

Configure Jamf

If not already existing, create an administrator account for API access (Read Only is sufficient). This will be used by FortiNAC.

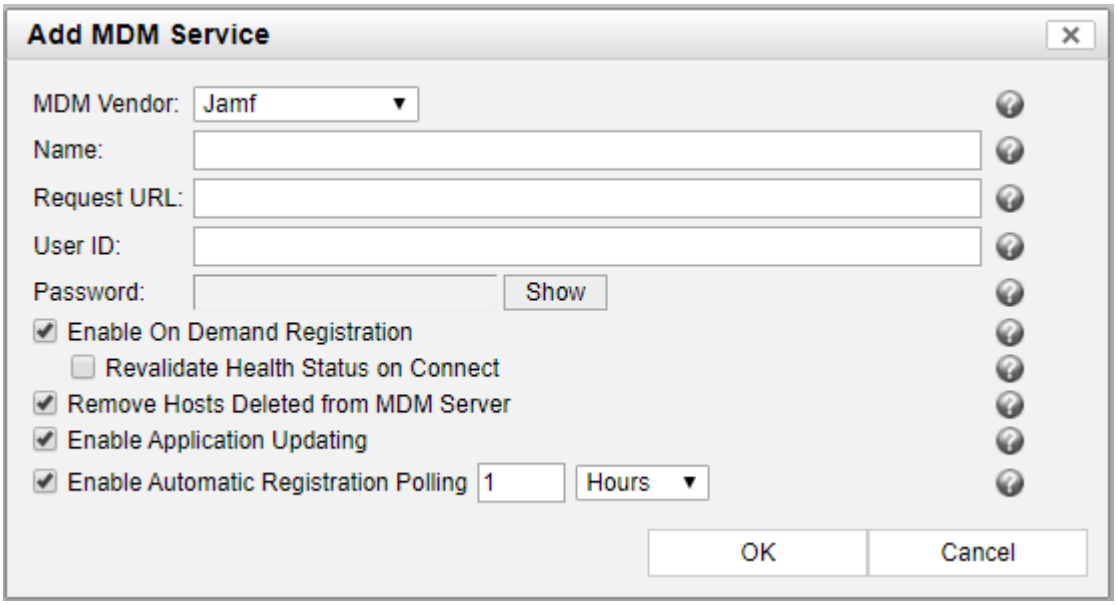
Configure FortiNAC

Configure a MDM Service to establish a connection with the Jamf server. MDM Services are used to configure the connection or integration between FortiNAC and Jamf. FortiNAC and the Jamf system work together sharing data via an API to secure the network. FortiNAC leverages the data in the Jamf database and registers hosts using that data as they connect to the network.

Important: Proxy communication is not supported.

MDM Services

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



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

Note: When integrating Jamf with FortiNAC, if there is more than one FortiNAC with an 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 FortiNAC Servers.

MDM Services Field Definitions

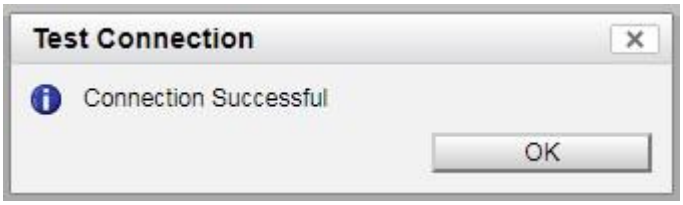
Field	Definition
MDM Vendor	Select **Jamf**
Name	Name of the connection configuration for the connection between an MDM system and FortiNAC.
Request URL	The URL for the API to which FortiNAC must connect to request data. This will be a unique URL based on your MDM system. This will be either the on-prem Jamf server URL or the cloud based Jamf URL.
User ID	User name of the account used by FortiNAC to log into the MDM system when requesting data.
Password	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.
On Demand Registration	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.
Revalidate Health Status On Connect	Not applicable: FortiNAC does not read health information from the Jamf Server.
Remove Hosts Deleted from MDM Server	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.
Application Updating	If enabled, when FortiNAC polls the MDM server it retrieves and stores the Application Inventory for hosts that are in the FortiNAC database. **NOTE**: 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.
Automatic Registration Polling	If enabled, indicates how often FortiNAC should poll the MDM system for information.

MDM Services Field Definitions

Field	Definition
Last Modified By	User name of the last user to modify the connection configuration.
Last Modified Date	Date and time of the last modification to this connection configuration.
Right Click Options	
Delete	Deletes the MDM Service.
Modify	Opens the Modify MDM Service dialog.
Poll Now	Polls the MDM server immediately.
Show Audit Log	Opens the Admin Auditing Log showing all changes made to the selected item. For information about the Admin Auditing Log, refer to section **Admin auditing** of the **Administration Guide** in the Fortinet Document Library for additional information. **Note:** Must have permission to view the Admin Auditing Log. See section **Add an administrator profile** of the **Administration Guide** in the Fortinet Document Library for additional information.
Test Connection	Tests the connection between the selected MDM server and FortiNAC. Error messages indicate which fields are missing or incorrect.
Buttons	
Add	Opens the Add MDM Service dialog.
Modify	Opens the Modify MDM Service dialog.
Export	Exports the data displayed to a file in the default downloads location. File types include CSV, Excel, PDF or RTF. See section **Export Data** of the **Administration Guide** in the Fortinet Document Library for additional information.
Test Connection	Tests the connection between the selected MDM server and FortiNAC. Error messages indicate which fields are missing or incorrect.
Poll Now	Polls the MDM server immediately.

Validate Connectivity

1. Select the EMS and click on the **Test Connection** button. The following message should display:



2. Click the **Poll Now** button at the bottom of the view.
3. Devices from EMS tables should pre-register in the FortiNAC system (if that option was selected).

Events

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

- MDM Host Created
- MDM Host Destroyed
- MDM Poll Failure
- MDM Poll Success

Refer to section **Enable and disable events** and **Map events to alarms** of the **Administration Guide** in the Fortinet Document Library for additional information.

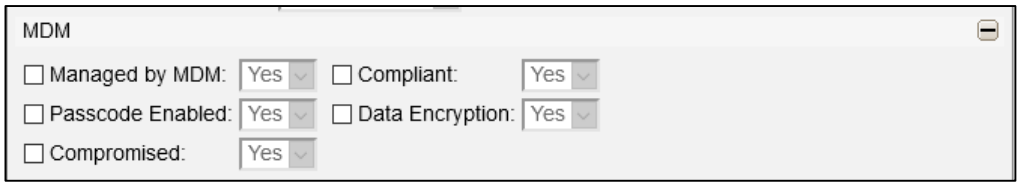
Policies

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 sections **Host View** and **Search and filter options** of the **Administration 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. **Note**: Does not list vulnerabilities.

Passcode enabled	N/A
Data Encryption	N/A
Compromised	N/A



Note the following when determining criteria for User/Host Profiles:

- Devices registered using Jamf are registered to a user if the user in Jamf matches a user in FortiNAC. If the user is not found, the device will be registered as a device and not to a user.
- Devices registered from Jamf are assigned NAC-Default as the role unless the user has a different role set in FortiNAC. If the user has a role, the device inherits the user's role.

- **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 MacOSX devices on VLAN 11.

iOS Network Access Policy:

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

MacOSX Network Access Policy:

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

Refer to section **Network access policies** of the **Administration Guide** in the Fortinet Document Library for additional information.

Validate

Test features enabled in the MDM Service.

On Demand Registration:

1. Connect a device to the network.
2. In FortiNAC Administration UI, navigate to **Hosts > Host View** and search for device by MAC address.
3. If device is already authenticated, FortiNAC should automatically register the device and assign the appropriate network access based upon Network Access Policies.

    - Devices registered using Jamf are registered to a user if the user in Jamf matches a user in FortiNAC. If the user is not found, the device will be registered as a device and not to a user.
    - Devices registered from Jamf are assigned NAC-Default as the role unless the user has a different role set in FortiNAC. If the user has a role, the device inherits the user's role.

Remove Hosts Deleted from MDM Server:

1. Disable or delete Host in Jamf.
2. In a separate window, navigate to **System > Settings > System Communication > MDM Services**
3. Click on the Jamf model and click the **Poll Now** button (or wait for the next polling cycle if Automatic Polling is enabled). The host should disappear from the Host View.

Troubleshooting

Refer to the following KB articles:

Troubleshooting MDM registration issues
https://kb.fortinet.com/kb/microsites/search.do?cmd=displayKC&docType=kc&externalId=FD43815

Troubleshooting Policies
https://kb.fortinet.com/kb/microsites/search.do?cmd=displayKC&docType=kc&externalId=FD42422

Debugging

Enable debugging feature

```
CampusMgrDebug -name JamfServer true
CampusMgrDebug -name MdmManager true
```

Disable debugging feature

```
CampusMgrDebug -name JamfServer false
CampusMgrDebug -name MdmManager false
```

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