FortiNAC

MDM Integration

Version: 9.1

Date: December 28, 2023

Rev: S

FORTINET DOCUMENT LIBRARY
http://docs.fortinet.com

FORTINET VIDEO GUIDE
http://video.fortinet.com

FORTINET KNOWLEDGE BASE
https://community.fortinet.com/t5/Knowledge-Base/ct-p/knowledgebase

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

The information in this document provides guidance for configuring integration in order for FortiNAC to manage devices registered using a MDM Server. This document presumes the MDM server is already in place and authenticating devices.

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 MDM server that would 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 that have been registered with the MDM server. Mobile devices connecting to the network can be registered in FortiNAC using the MDM server's host data.

How it Works

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

Supported Devices

The following 3rd party MDM solutions are covered in this document:
Airwatch/Workspace ONE
Citrix Endpoint Management
Google Gsuite
Jamf
Maas360
Microsoft InTune
MobileIron
Nozomi

For the FortiClient EMS solution see FortiClient EMS Device Integration in the Document Library.

Procedure Overview

1. **Configure MDM Device**: Configure the MDM server to communicate with FortiNAC.
2. **Configure FortiNAC**: Configure MDM Services, alarm mappings and policies
3. **Validate**: Verify FortiNAC is behaving as configured for the devices under enforcement.

Important: Proxy communication is not supported.

Multiple PODs controlled by a Control Manager: It is only necessary to configure the MDM integration on one of the FortiNAC Servers. The host records will be propagated on demand to the other FortiNAC Servers.

Configure MDM Device

Configure the MDM server to communicate with FortiNAC. Proceed to the applicable MDM solution:

Airwatch/Workspace ONE
Citrix Endpoint Management
Google Gsuite
Jamf
Maas360
Microsoft InTune
MobileIron
Nozomi

Airwatch/Workspace ONE

Requirements

Supported FortiNAC Engine Version: 8.x and greater

Considerations

- **Versions 9.2.5, 9.4.0 and greater:** Airwatch/Workspace ONE role assignment takes precedence over existing user/host roles in FortiNAC. To configure FortiNAC for user/host roles to take precedence over Airwatch/Workspace ONE assigned roles, see Airwatch/Workspace ONE Role Assignment in Appendix.
- Only Airwatch Basic Authentication is supported.

Configure the API Key in Airwatch/Workspace ONE

1. Login to Airwatch/Workspace ONE 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/Workspace ONE for assistance.
4. Configure a **System Administrator** user in Airwatch/Workspace ONE to be used by FortiNAC for authentication when requesting data.

Note: Airwatch/Workspace ONE 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/Workspace ONE can be configured to send notifications to FortiNAC when devices are deleted or updated in the Airwatch/Workspace ONE database. If notifications are not configured in Airwatch/Workspace ONE, 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/Workspace ONE 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/Workspace ONE.
7. Click **Test Connection**. If notifications have been set up correctly, the message **Test is successful** is returned. Proceed to Configure FortiNAC.

Citrix Endpoint Management

Requirements

- Citrix Endpoint Management is already in place and managing mobile devices.
- Each managed device must have the Citrix Endpoint Management Agent installed. Refer to the Citrix Endpoint Management documentation for instructions.
- Each managed device must be running an Operating System supported by Citrix Endpoint Management. Otherwise, the device becomes a rogue and goes through the regular registration process. Below is the list of supported Operating Systems:
  - Apple iOS
  - Android
  - Windows Phone 8
  - Windows 8
  - Windows Mobile
  - Symbian
- FortiNAC Minimum version: 8.3

Considerations

- Application inventory cannot be retrieved for devices registered based on information from Citrix Endpoint Management.

Configure Citrix Endpoint Management

1. Configure a System Administrator user to be used by FortiNAC for authentication when requesting data.
2. Record the following account information (this will be used when modeling the device in FortiNAC).
   a. Server 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.
   Note: Requires the server name (Example: https://services.m3.mycompany.com)
   b. Identifier - A type of key used to identify FortiNAC to the MDM server.
   c. User ID - User name of the account used by FortiNAC to log into the MDM system when requesting data.
   d. Password - Password for the account used by FortiNAC to log into the MDM system when requesting data.

Google GSuite

When a rogue host is detected on the network, FortiNAC connects to Google GSuite Directory API, retrieves the host data and registers the host in FortiNAC. The GSuite API is polled periodically in order to update records for those hosts that are already registered in FortiNAC.

- Host records are registered and deleted based on the host list returned from GSuite.
- Polling behavior when On Demand Lookup is enabled: Full poll (paged). Stops looking once endpoint is found.
- Duplicate entries and entries with invalid MAC addresses (00:00:00:00:00:00) are not added.
- FortiNAC does not take into account the status of the host (e.g. ACTIVE, DISABLED, DEPROVISIONED) when registering. This means FortiNAC will include all hosts, Active or otherwise, in the database. Consequently, filter results for hosts registered from GSuite may have a higher count that what is reported in GSuite (as GSuite may only list active accounts).

FortiNAC collects the following host data from GSuite:

- Operating System
- Model (Hardware Type)
- Host Name
- Serial Number
- Owner (User)

Requirements

FortiNAC

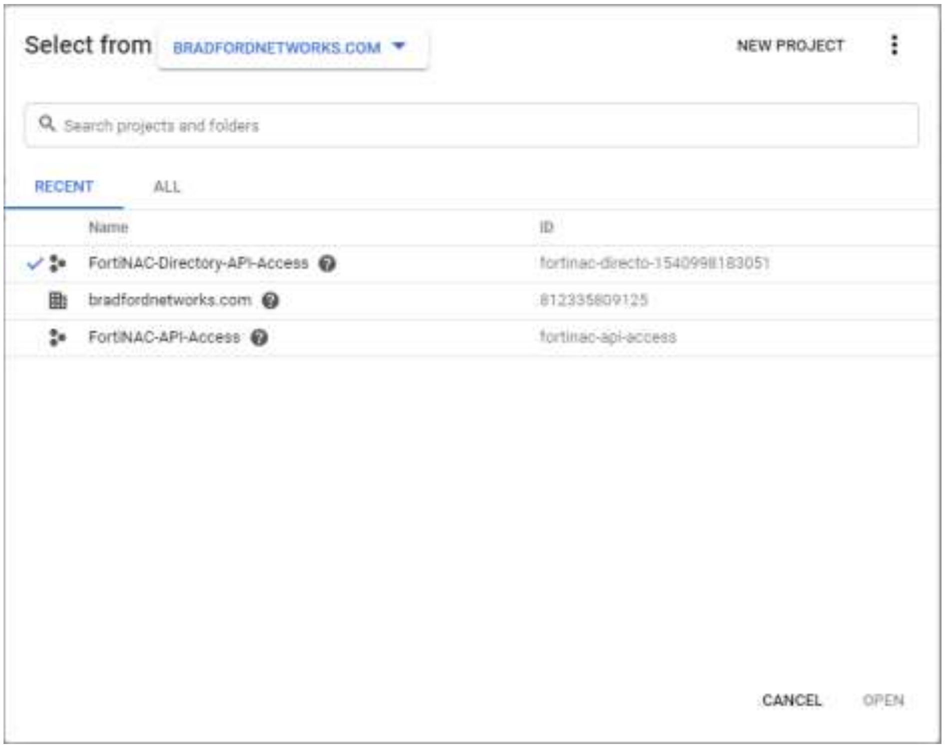
- Supported Engine Version: 8.5.0 and greater
- Recommended Engine Version: 8.8.5 and greater (ID 682244)

Configure Google Developers Console

Log in a Google Account Administrator for the domain. Go to the following web address: https://console.developers.google.com/

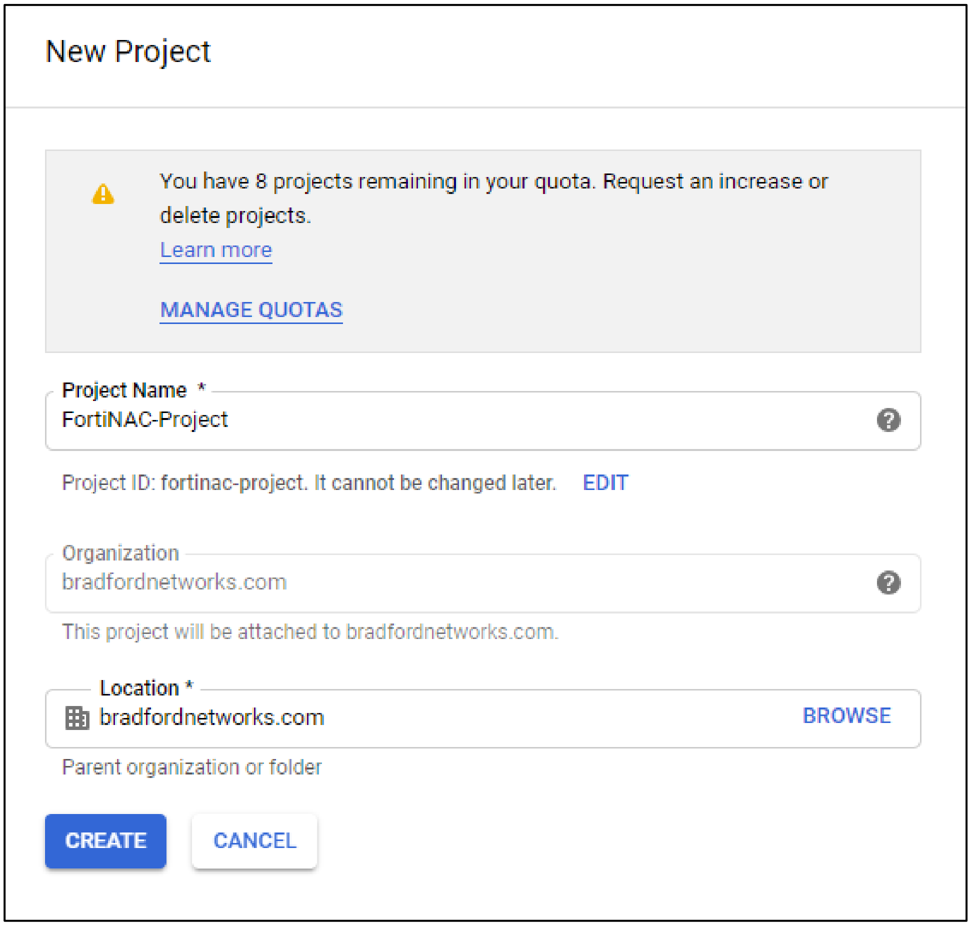
Create A New Project

1. From the dropdown bring up the project management dialog and create a new project with the desired name.



	Name	ID
✓	FortiNAC-Directory-API-Access	fortinac-directo-1540998183051
	bradfordnetworks.com	812335809125
	FortiNAC-API-Access	fortinac-api-access

2. Click **NEW PROJECT.**



New Project

You have 8 projects remaining in your quota. Request an increase or delete projects.

Learn more

MANAGE QUOTAS

Project Name *

FortiNAC-Project

Project ID: fortinac-project. It cannot be changed later. EDIT

Organization

bradfordnetworks.com

This project will be attached to bradfordnetworks.com.

Location *

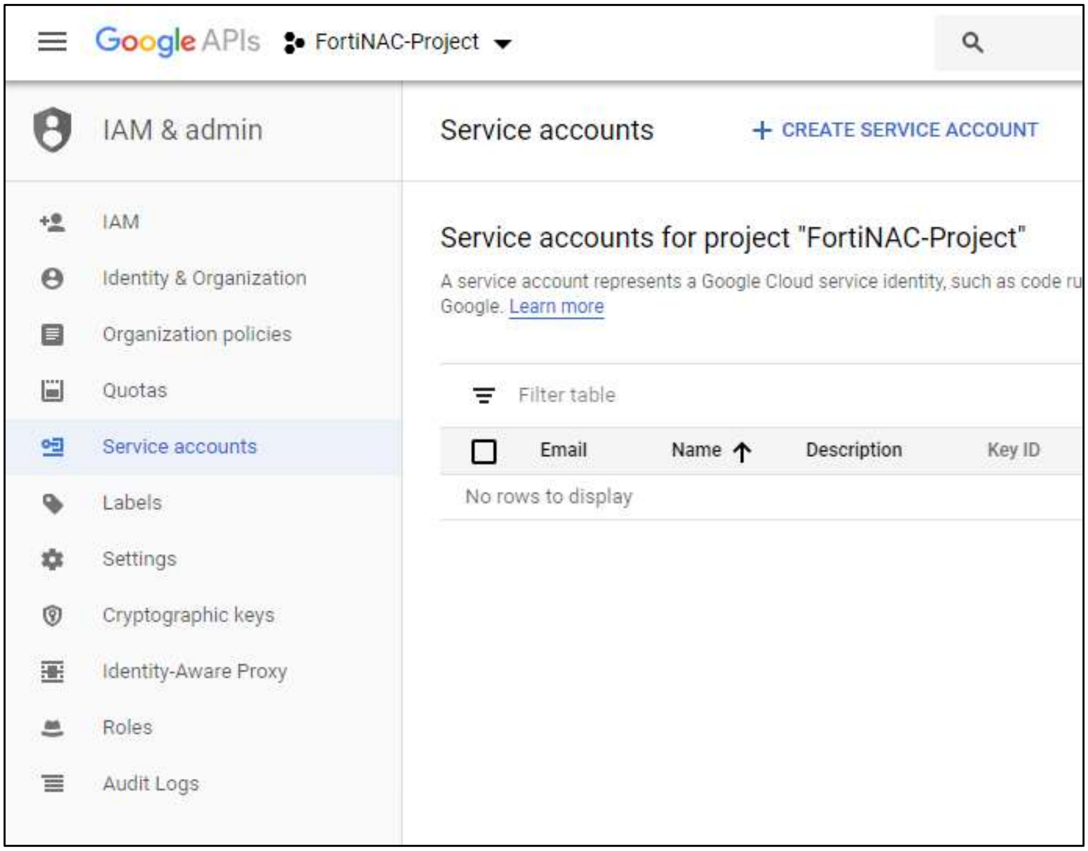
bradfordnetworks.com BROWSE

Parent organization or folder

CREATE CANCEL

3. Click **CREATE**, then select the newly created project by clicking on the dropdown and selecting the project from the project management view.

4. Once the project in created, select the **Service accounts** option on the side menu.



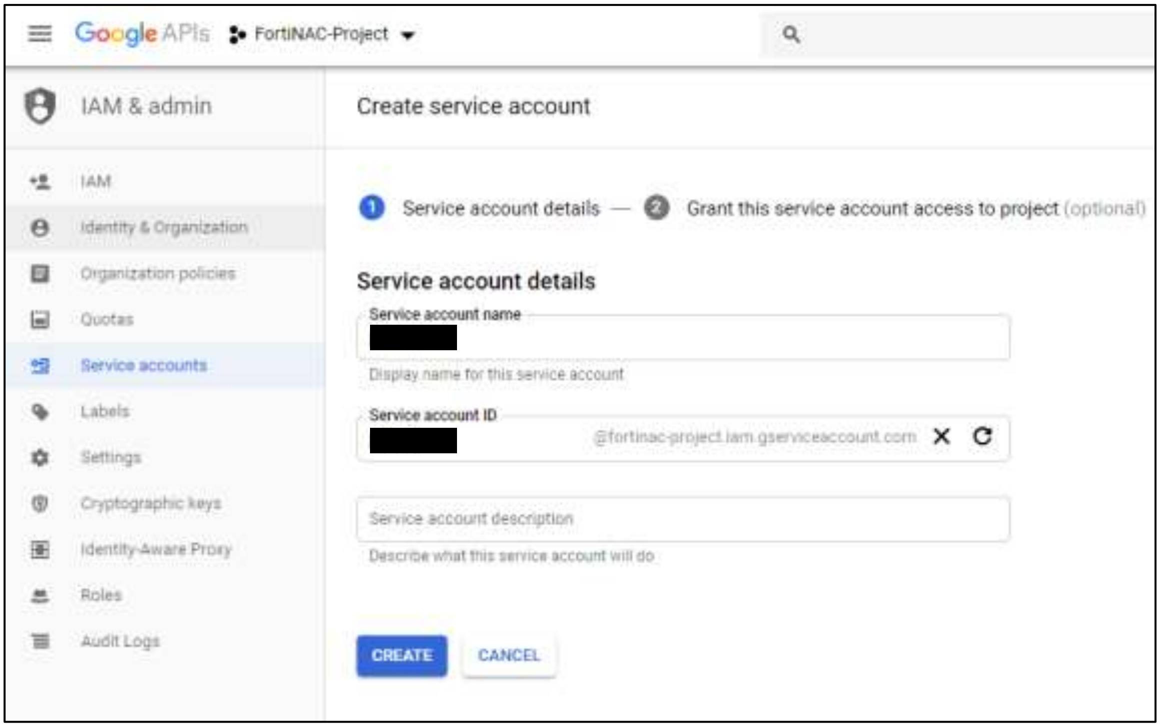
Service accounts for project "FortiNAC-Project"

A service account represents a Google Cloud service identity, such as code ru
Google. Learn more

□	Email	Name ↑	Description	Key ID

No rows to display

5. Click **+ CREATE SERVICE ACCOUNT**.



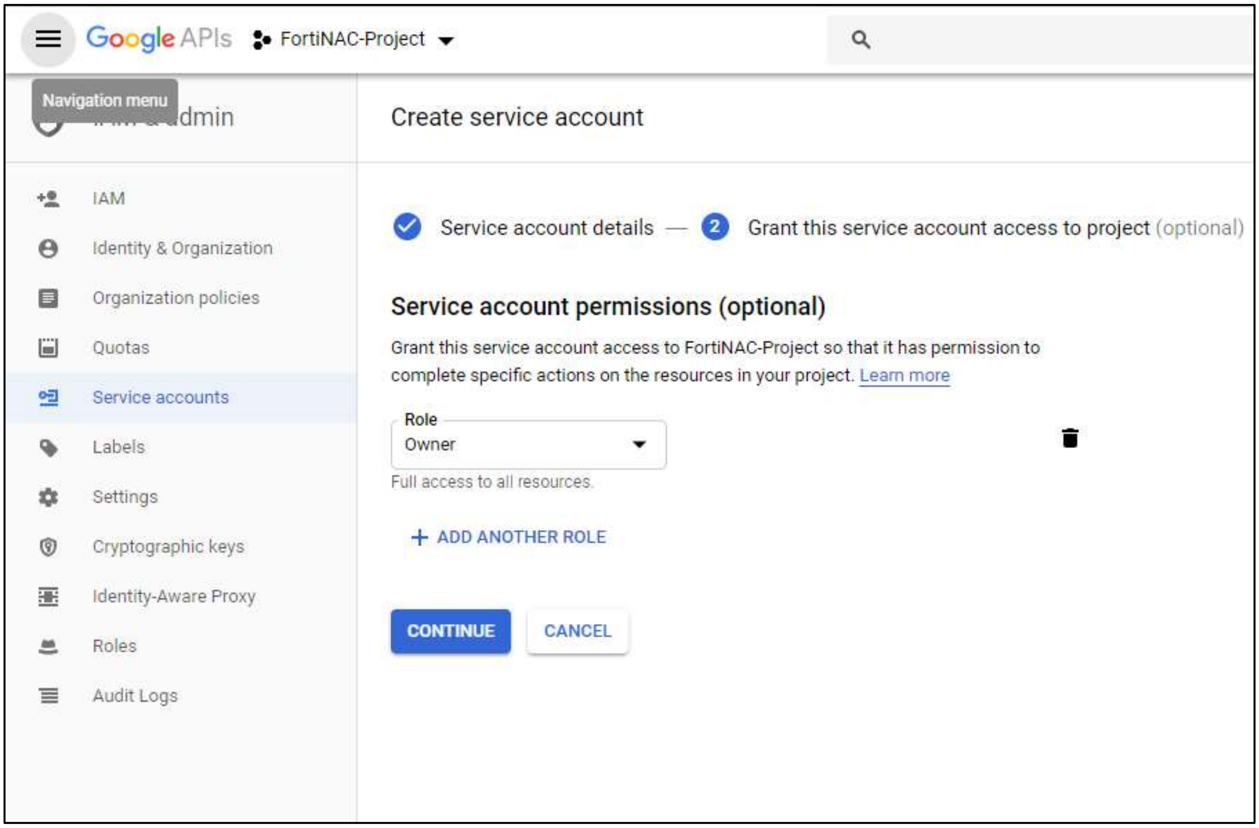
Service account details

Service account name: [redacted]
Display name for this service account

Service account ID: [redacted] @fortinac-project.iam.gserviceaccount.com

Service account description
Describe what this service account will do

6. Give the service account a name and optionally a description and click **CREATE**.



Create service account

Service account details — 2 Grant this service account access to project (optional)

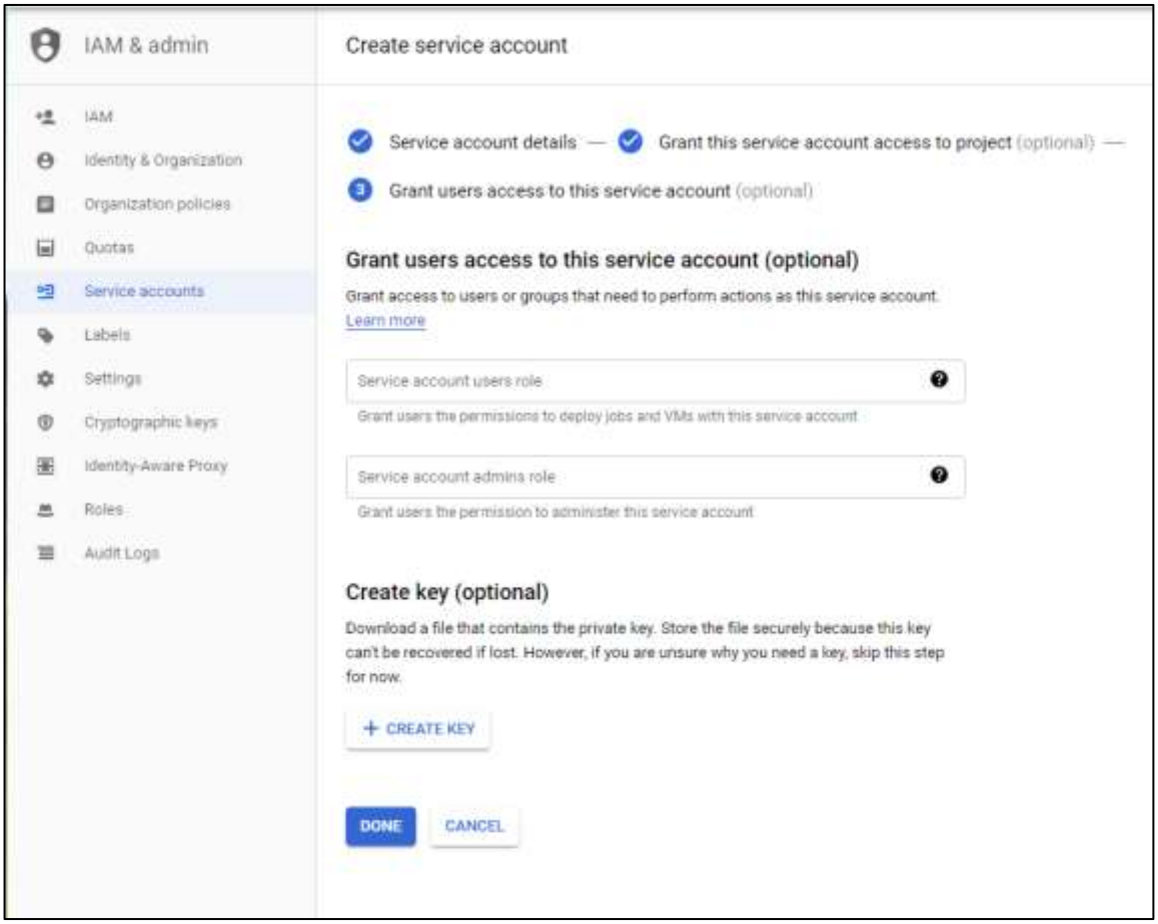
Service account permissions (optional)

Grant this service account access to FortiNAC-Project so that it has permission to complete specific actions on the resources in your project. Learn more

Role: Owner

Full access to all resources.

7. Assign the service account a **Role of Project > Owner** so it has full access to the project. Click **CONTINUE**.



Create service account

Service account details — Grant this service account access to project (optional) — 3 Grant users access to this service account (optional)

Grant users access to this service account (optional)

Grant access to users or groups that need to perform actions as this service account. Learn more

Service account users role

Grant users the permissions to deploy jobs and VMs with this service account

Service account admins role

Grant users the permission to administer this service account

Create key (optional)

Download a file that contains the private key. Store the file securely because this key can't be recovered if lost. However, if you are unsure why you need a key, skip this step for now.

8. Do NOT create the key just yet. Click **DONE** on this screen.

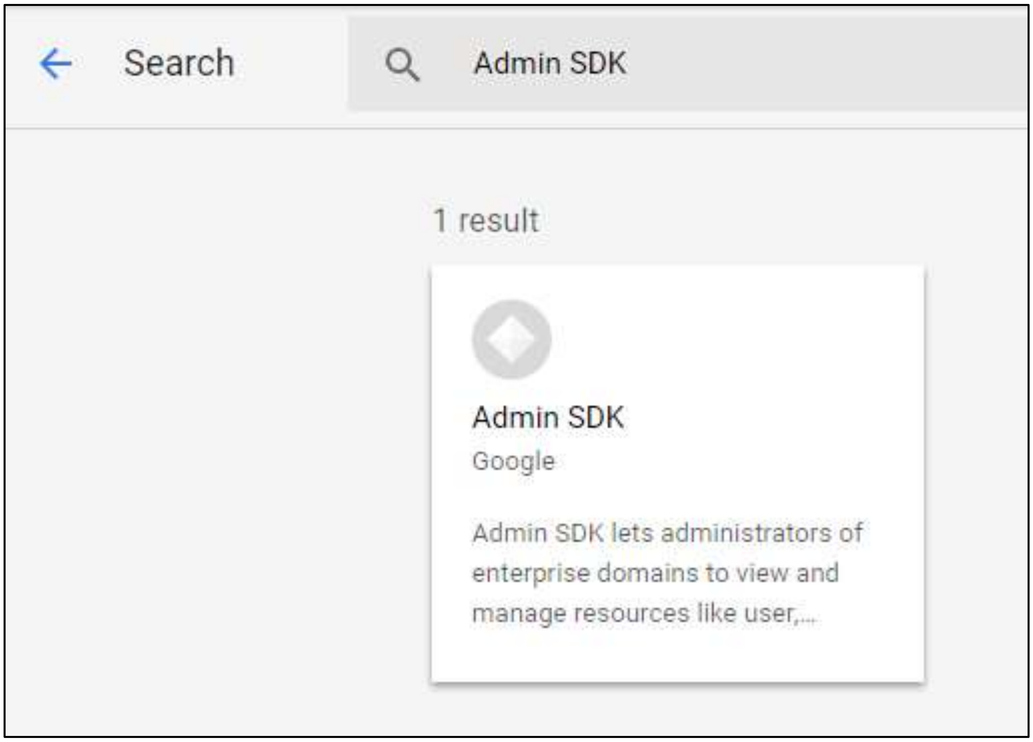
9. Click on the newly created service account in the table, then click **EDIT** from the details view.

10. Under the **KEYS** tab click **ADD KEY > CREATE NEW KEY**. This brings up the Service Account Key creation view.

11. Select the service account, choose **JSON** and click **CREATE**.

12. Download the file. It will be used when configuring FortiNAC.

13. Enable the Admin SDK to access in this project. Click on the top left menu again, and select **APIs & Service > Library**. Search for **Admin SDK** in the search box.



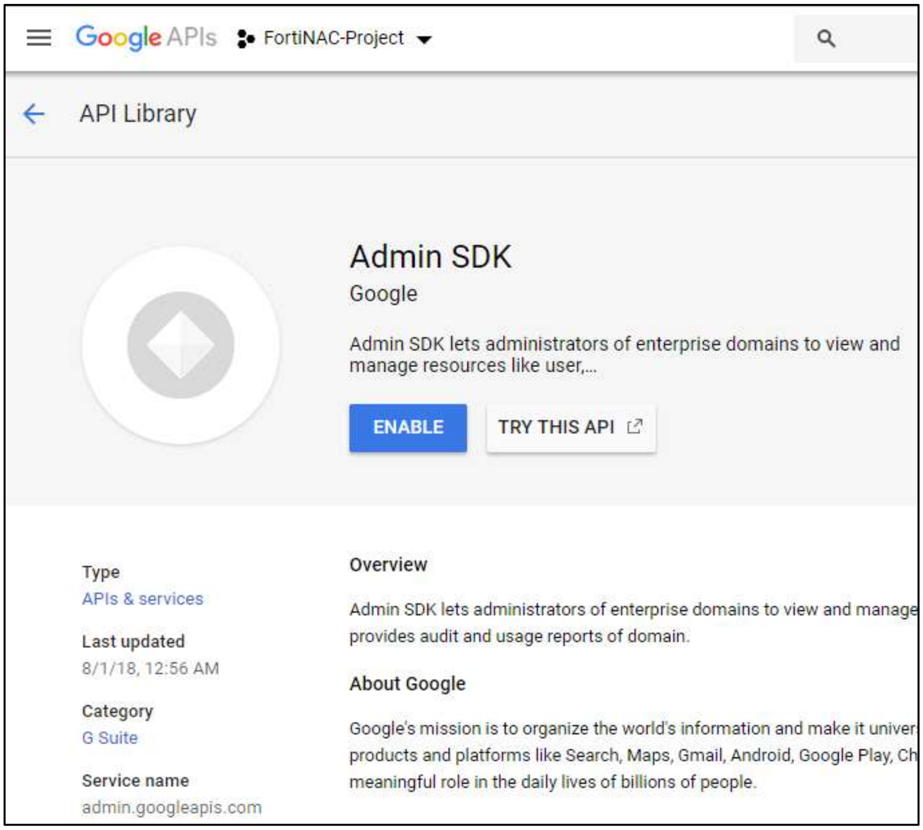
1 result

Admin SDK

Google

Admin SDK lets administrators of enterprise domains to view and manage resources like user,...

14. Then click on it and hit the **ENABLE** button.



Admin SDK

Google

Admin SDK lets administrators of enterprise domains to view and manage resources like user,...

Type

APIs & services

Last updated

8/1/18, 12:56 AM

Category

G Suite

Service name

admin.googleapis.com

Overview

Admin SDK lets administrators of enterprise domains to view and manage

provides audit and usage reports of domain.

About Google

Google's mission is to organize the world's information and make it univer

products and platforms like Search, Maps, Gmail, Android, Google Play, Ch

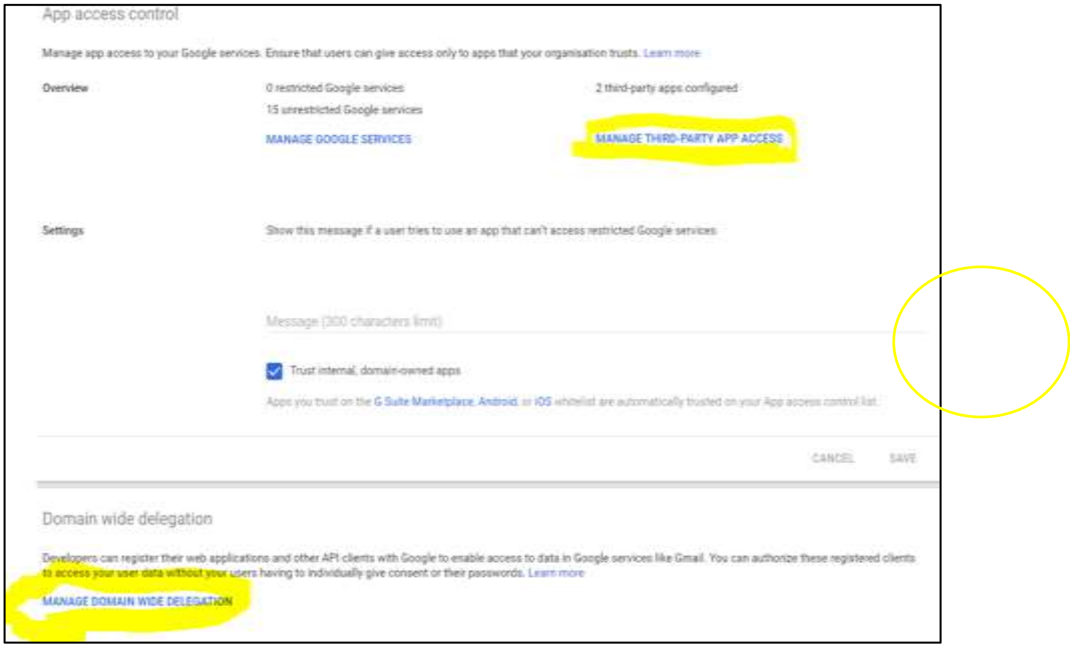
meaningful role in the daily lives of billions of people.

Important: *Do not* click the CREATE CREDENTIALS button in the next view. This has already been done.

Enable API Access to the Service Account

15. Log into https://admin.google.com and on the Home view in the Admin console, click **Security**.

16. At the bottom of the App access control page, select **Manage Domain Wide Delegation**.



App access control

Manage app access to your Google services. Ensure that users can give access only to apps that your organisation trusts. Learn more

Overview

0 restricted Google services
15 unrestricted Google services
MANAGE GOOGLE SERVICES

2 third-party apps configured
MANAGE THIRD-PARTY APP ACCESS

Settings

Show this message if a user tries to use an app that can't access restricted Google services

Message (300 characters limit)

☑ Trust internal, domain-owned apps

Apps you trust on the G Suite Marketplace, Android, or iOS whitelist are automatically trusted on your App access control list.

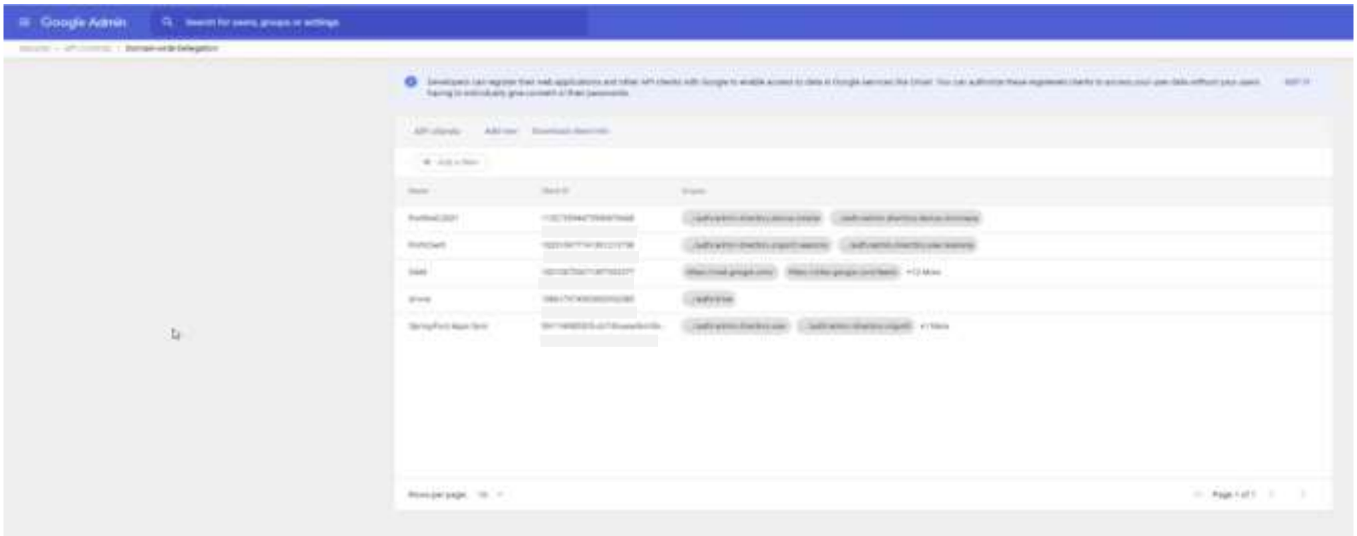
CANCEL SAVE

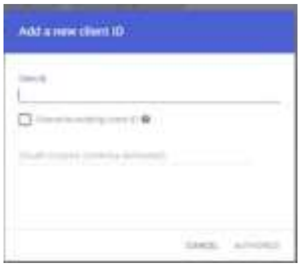
Domain wide delegation

Developers can register their web applications and other API clients with Google to enable access to data in Google services like Gmail. You can authorize these registered clients to access your user data without your users having to individually give consent or their passwords. Learn more

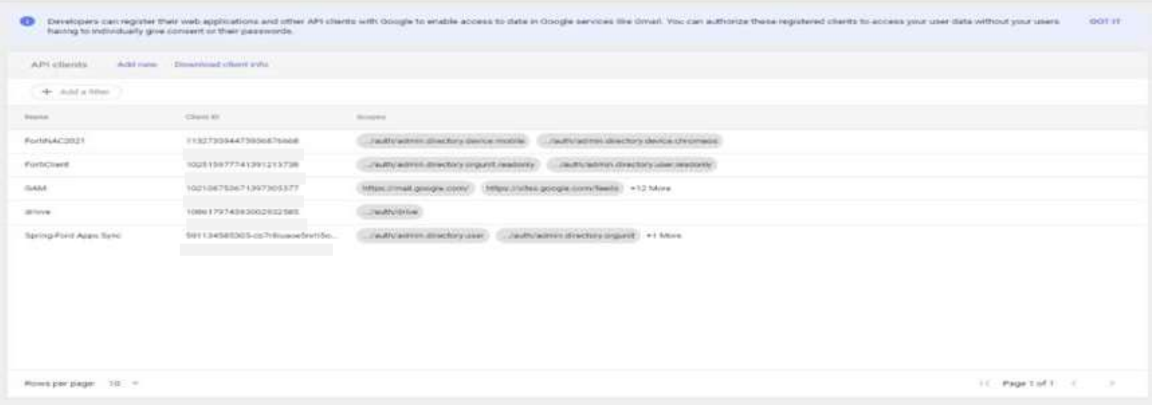
MANAGE DOMAIN WIDE DELEGATION

17. Add a new client ID using the ID copied from the service account created in the developer console.




Add a new client ID
Client ID
□ Overwrite existing client ID
OAuth scopes (comma-delimited)
CANCEL
AUTHORIZE

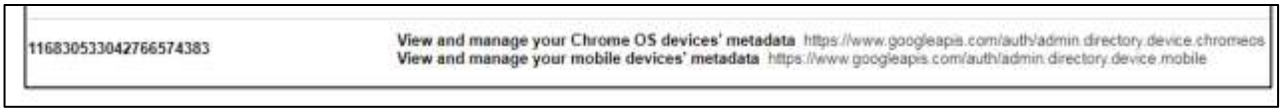
18. Add the scopes to query (Chrome OS devices' metadata and mobile devices' metadata):
    https://www.googleapis.com/auth/admin.directory.device.chromeos
    https://www.googleapis.com/auth/admin.directory.device.mobile



Developers can register their web applications and other API clients with Google to enable access to data in Google services like Gmail. You can authorize these registered clients to access your user data without your users having to individually give consent or their passwords. GOT IT

Name	Client ID	Scopes
FortiNAC2021	[illegible]	.../auth/admin.directory.device.mobile .../auth/admin.directory.device.chromeos
FortiClient	[illegible]	.../auth/admin.directory.orgunit.readonly .../auth/admin.directory.user.readonly
GAM	[illegible]	https://mail.google.com/ https://sites.google.com/feeds +12 More
drive	[illegible]	.../auth/drive
Spring-Ford Apps Sync	[illegible]	.../auth/admin.directory.user .../auth/admin.directory.orgunit +1 More

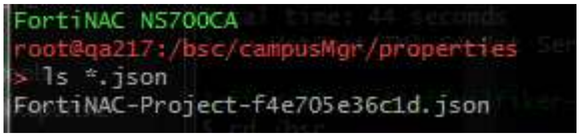
19. The "View and manage your Chrome OS devices' metadata" and "View and manage your mobile devices' metadata" should be listed as the 2 APIs that are accessible using the service account ID.



116830533042766574383 **View and manage your Chrome OS devices' metadata** https://www.googleapis.com/auth/admin.directory.device.chromeos
View and manage your mobile devices' metadata https://www.googleapis.com/auth/admin.directory.device.mobile

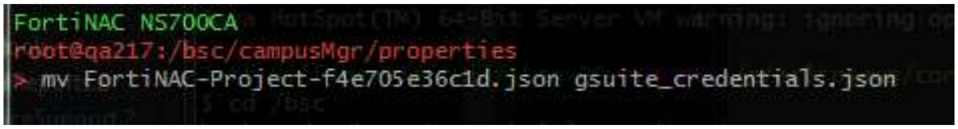
Copy JSON file to FortiNAC

1. Login to the FortiNAC CLI as **root**.
2. Copy the credentials JSON file that was downloaded in the previous step to the **/bsc/campusMgr/properties** directory.



```
FortiNAC NS700CA
root@qa217:/bsc/campusMgr/properties
> ls *.json
FortiNAC-Project-f4e705e36c1d.json
```

3. Rename the file to **gsuite_credentials.json**



```
FortiNAC NS700CA
root@qa217:/bsc/campusMgr/properties
> mv FortiNAC-Project-f4e705e36c1d.json gsuite_credentials.json
```

Proceed to Configure FortiNAC.

Jamf

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
- Polling behavior when On Demand Lookup is enabled: Single device lookup using the MAC address

FortiNAC collects the following host data from Jamf:

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

Requirements

FortiNAC

- Supported Engine Version: 8.8.0 and greater

Jamf

- Supported Server Version: 10.x and greater
- Pro version

Considerations

- Bearer Token authentication is not supported.

Configure Jamf

If not already existing, create an administrator account for API access. This will be used by FortiNAC.

- Read Only access is sufficient
- Password cannot contain "@" character. This can cause authentication failure
- Basic authentication in the Classic API must be enabled (is disabled by default as of version 10.42.0). For details see:
- https://developer.jamf.com/jamf-pro/docs/classic-api-authentication-changes

Proceed to Configure FortiNAC.

Maas360

Requirements

FortiNAC

- Supported Engine Version: 8.0 and greater

Maas360

- Each managed device must have the MaaS360 Agent installed. Refer to the MaaS360 documentation for instructions.
- Each managed device must be running an Operating System supported by the MaaS360. Otherwise, the device becomes a rogue and goes through the regular registration process. Below is the list of supported Operating Systems:
  - Apple iOS
  - Android
  - Samsung
  - BlackBerry
  - Windows Phone
  - Symbian

Configure MaaS360

3. Configure a System Administrator user to be used by FortiNAC for authentication when requesting data.
4. Record the following account information (this will be used when modeling the device in FortiNAC).   In the management UI for the MDM, navigate to **Add Resource > MDM Integration > IBM MaaS360.**

   - Billing Identifier
   - Application Identifier
   - Platform Identifier
   - Application Version
   - Server URL
   - Administrator Identifier
   - Password
   - Access Key

   For additional information, refer to vendor documentation like the following: https://www.ibm.com/support/knowledgecenter/en/SSVLBW_6.1.5/com.ibm.lmc_6.1.5.doc/cfg_AddinganIBMMaaS360MDMresource_t.htm

Proceed to Configure FortiNAC.

Microsoft InTune

When a rogue host is detected on the network, FortiNAC interfaces with the InTune Graph API and retrieves the host data. FortiNAC registers the host if it is already registered with InTune. FortiNAC polls InTune periodically in order to update records for those hosts already registered in FortiNAC.

FortiNAC collects the following host data from InTune:

- Operating System
- Host Name
- Serial Number
- Compliance Boolean
- Model (Hardware Type)
- Type (PC/Android/IOS)
- Owner (User)

Requirements

FortiNAC

- Supported Engine Version: 8.5.0 and greater
- Recommended Engine Version: 8.8.6, 9.1 and greater (Refer to ID 698066 in Release Notes)

Considerations

- Certificate-based authentication is currently not supported.

- Automatic registration for Intune endpoints with only Ethernet adapters
  - Requires version 9.2.5, 9.4.0, F7.2.0 or greater
  - For all other FortiNAC versions.
    - Workarounds:
      - Register using other methods (Captive Portal, etc).
      - Export clients from Intune and import into FortiNAC.
      - Versions 9.1.2, 9.2.0 and greater: Requires the FortiNAC agent to be installed on the client in order to register. As of 9.1.2 and 9.2.0, FortiNAC can use the InTune client serial number to perform a lookup in InTune if necessary. The agent provides the serial number information.
    - Reference KB article 197812.

- As of October 2021, Intune doesn't display Wi-Fi MAC addresses for newly enrolled personally-owned work profile devices and devices managed with device administrator running Android 9 and above.

  Reference
  https://techcommunity.microsoft.com/t5/intune-customer-success/android-12-day-zero-support-with-microsoft-endpoint-manager/ba-p/2621665

  https://docs.microsoft.com/en-us/mem/intune/remote-actions/device-inventory

FortiNAC requires the MAC address information to lookup these devices in InTune. Consequently, these devices will be unable to register to FortiNAC via the MDM.

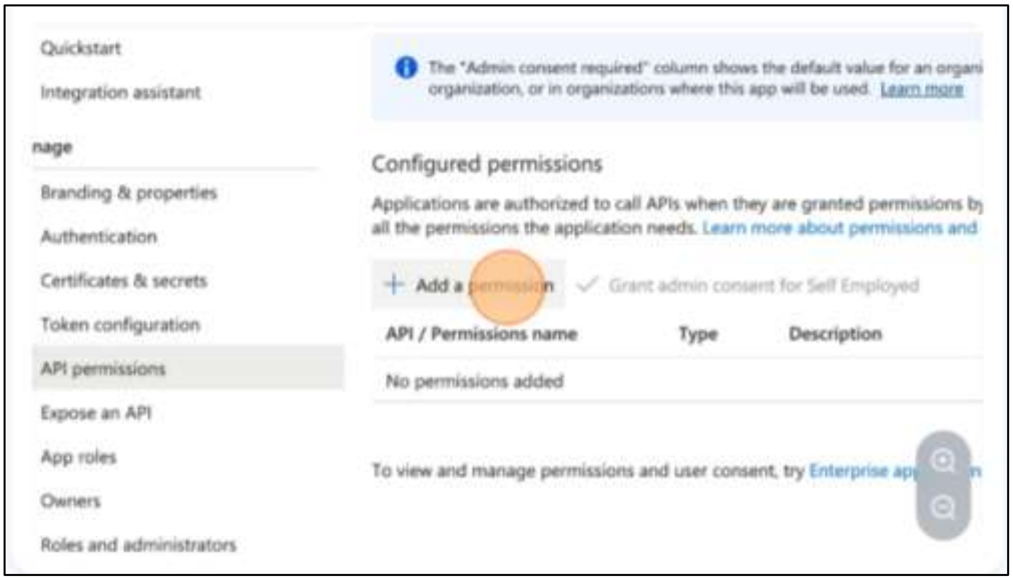
Workaround: Use WPA2 and register the device to the Radius User. Automated registration based upon the user's 802.1x authentication can be enabled on a SSID basis. For details, see **Dot1x Auto Registration** in the Settings table of the **SSID Configuration** section in the Administration Guide.

- There are two types of Applications that can be registered with Azure AD in order to give FortiNAC consent/permission to read MS InTune devices:
    - **Delegated Permissions (Versions 9.1.5, 9.2.2 and lower)**: Appliances with InTune integrations configured with this method will continue to operate as expected in higher versions of code. However, for new service connectors, administrators will be required to register with Application Permissions.

  Application Permissions (Versions 9.1.6, 9.2.3, 9.4 and greater): This is the recommended configuration. Provides a simpler process and better user experience. Allows FortiNAC to run as a background/daemon application and does not require a user delegated permission.

Step 1: Create a New Application Registration for Azure Active Directory

1. From the **Azure Active Directory > App registrations** view, click on **+ New registration**. Enter a unique name for the application (something like "FortiNAC Integration").
2. Select the application within the Azure AD applications portal and give the Application Permissions.
   a. Select the API permissions view and click the **Add a permission** button.



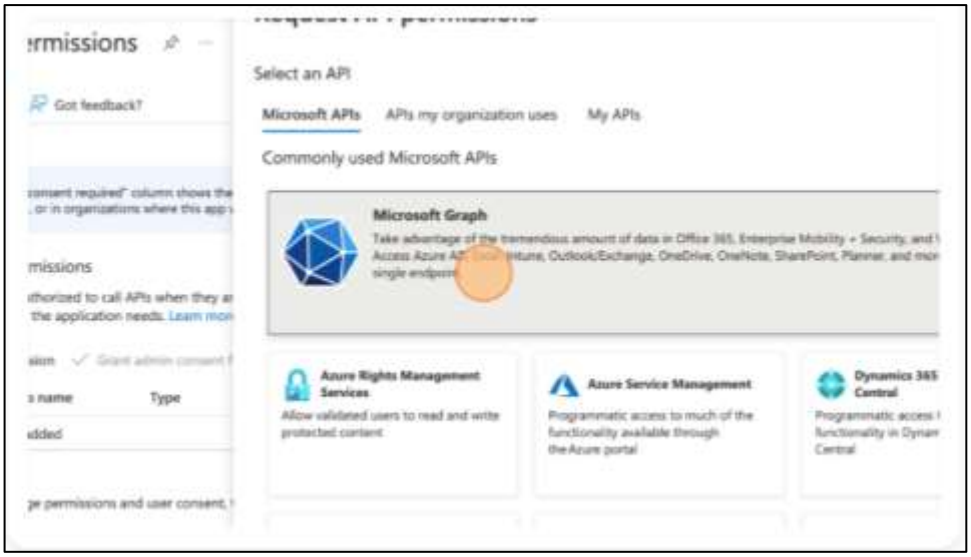
The "Admin consent required" column shows the default value for an organi organization, or in organizations where this app will be used. Learn more

Applications are authorized to call APIs when they are granted permissions by all the permissions the application needs. Learn more about permissions and

API / Permissions name	Type	Description
No permissions added		

To view and manage permissions and user consent, try Enterprise ap n

   b. Select the **Microsoft Graph** APIs.


rmissions
Got feedback?
consent required" column shows the
, or in organizations where this app
missions
thorized to call APIs when they ar
the application needs. Learn mor
sion ✓ Grant admin consent f
s name Type
dded
ge permissions and user consent,
Request API permissions
Select an API
Microsoft APIs
APIs my organization uses
My APIs
Commonly used Microsoft APIs
Microsoft Graph
Azure Rights Management Services
Azure Service Management
Dynamics 365 Central

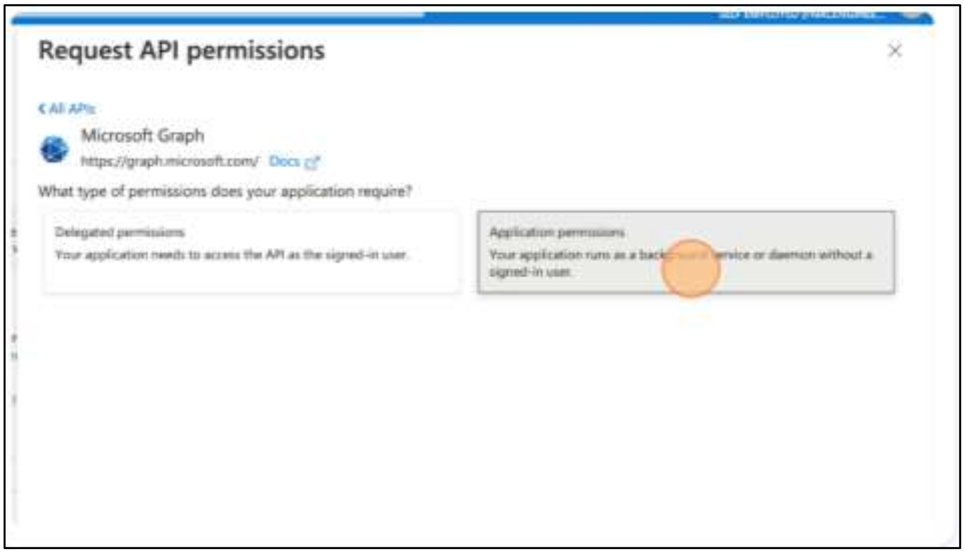
Take advantage of the tremendous amount of data in Office 365, Enterprise Mobility + Security, and \ Access Azure AD, Excel, Intune, Outlook/Exchange, OneDrive, OneNote, SharePoint, Planner, and mor single endpoint

Allow validated users to read and write protected content

Programmatic access to much of the functionality available through the Azure portal

Programmatic access t functionality in Dynam Central

c. Select **Application permissions**.



Request API permissions

‹ All APIs

Microsoft Graph

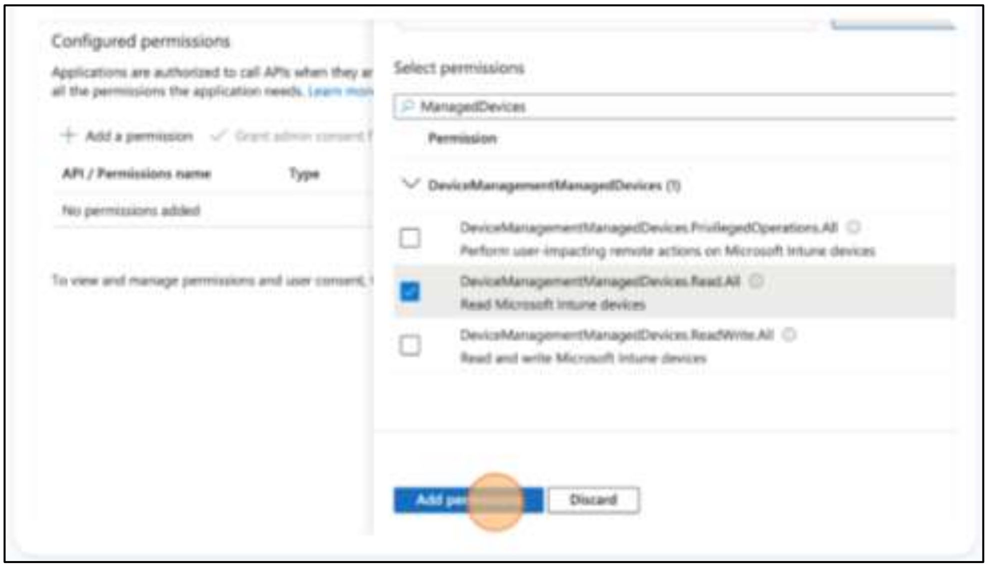
https://graph.microsoft.com/ Docs

What type of permissions does your application require?

Delegated permissions
Your application needs to access the API as the signed-in user.

Application permissions
Your application runs as a background service or daemon without a signed-in user.

d. Click the **Search box** field and search for ManagedDevices. From the search results, select **DeviceManagementManagedDevices.Read.All** to give FortiNAC access to read all MSIntune devices.



Configured permissions

Applications are authorized to call APIs when they ar
all the permissions the application needs. Learn mor

+ Add a permission ✓ Grant admin consent f

API / Permissions name	Type
No permissions added	

To view and manage permissions and user consent,

Select permissions

ManagedDevices

Permission

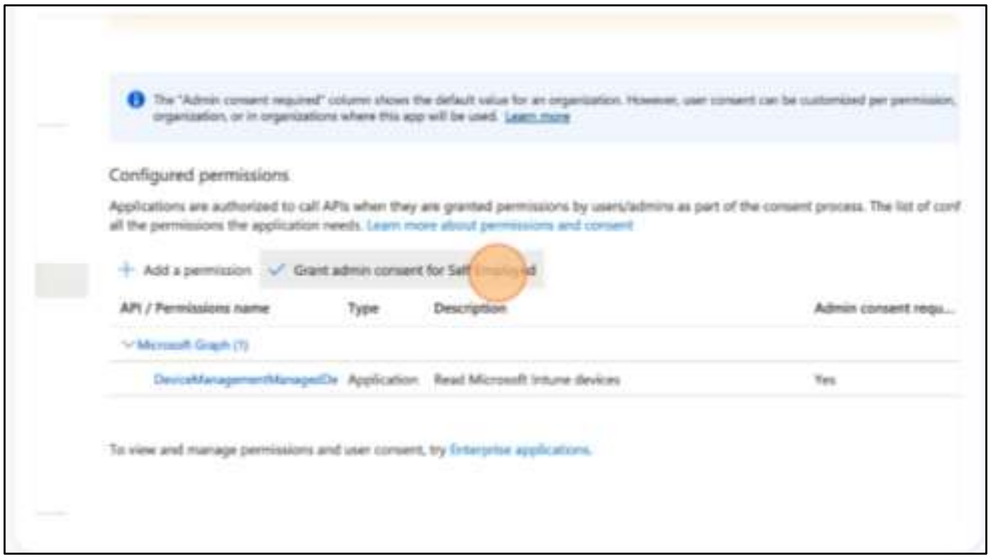
DeviceManagementManagedDevices (1)

☐ DeviceManagementManagedDevices.PrivilegedOperations.All
Perform user-impacting remote actions on Microsoft Intune devices

☑ DeviceManagementManagedDevices.Read.All
Read Microsoft Intune devices

☐ DeviceManagementManagedDevices.ReadWrite.All
Read and write Microsoft Intune devices

e. Click on the **Grant admin consent…** to give FortiNAC admin consent to read MSIntune devices in the background.



The "Admin consent required" column shows the default value for an organization. However, user consent can be customized per permission, organization, or in organizations where this app will be used. Learn more

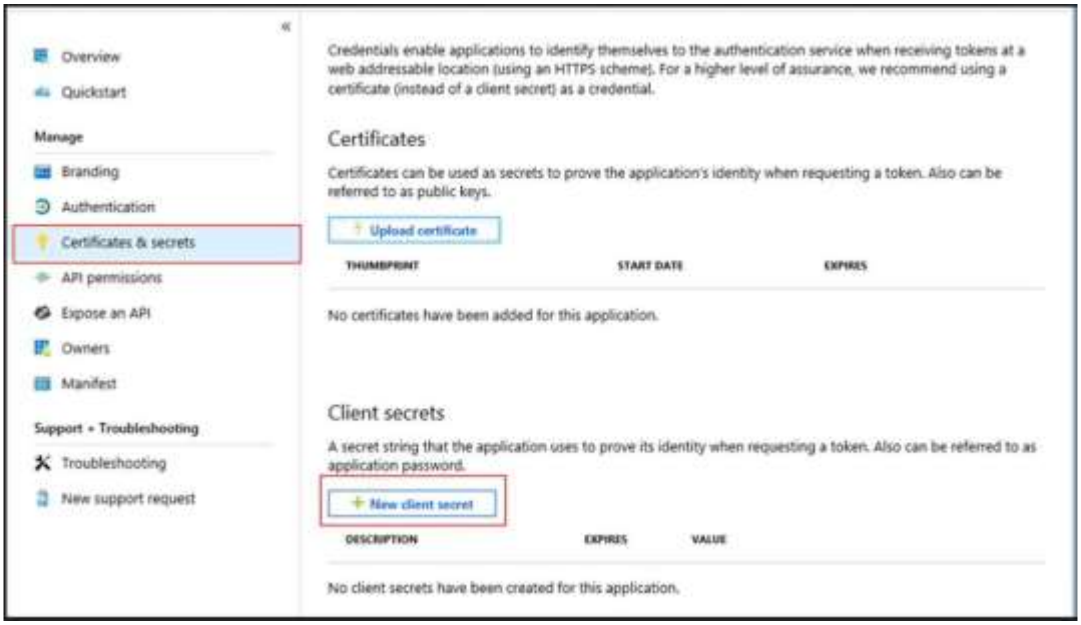
Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of conf all the permissions the application needs. Learn more about permissions and consent

API / Permissions name	Type	Description	Admin consent requ...
∨ Microsoft Graph (1)			
DeviceManagementManagedDe	Application	Read Microsoft Intune devices	Yes

To view and manage permissions and user consent, try Enterprise applications.

f. From **Certificates & Secrets** select **+ New client secret** and create a secret. Copy and store the secret value (not the secret ID). This will be used in FortiNAC configuration.



Credentials enable applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Certificates

Certificates can be used as secrets to prove the application's identity when requesting a token. Also can be referred to as public keys.

THUMBPRINT	START DATE	EXPIRES

No certificates have been added for this application.

Client secrets

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

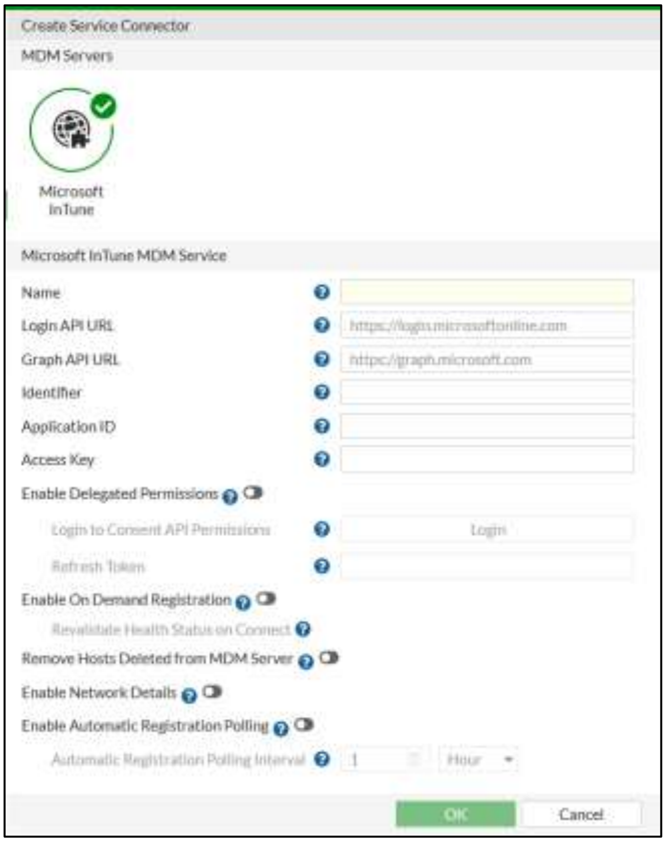
DESCRIPTION	EXPIRES	VALUE

No client secrets have been created for this application.

Step 2: Configure FortiNAC

Configure a MDM Service to establish a connection with the Microsoft InTune Graph API.

1. Navigate to **Network > Service Connectors** and create new **Microsoft InTune** connector.



Create Service Connector

MDM Servers

Microsoft InTune

Microsoft InTune MDM Service

Name

Login API URL: https://login.microsoftonline.com

Graph API URL: https://graph.microsoft.com

Identifier

Application ID

Access Key

Enable Delegated Permissions

Login to Consent API Permissions

Refresh Token

Enable On Demand Registration

Revalidate Health Status on Connect

Remove Hosts Deleted from MDM Server

Enable Network Details

Enable Automatic Registration Polling

Automatic Registration Polling Interval: 1 Hour

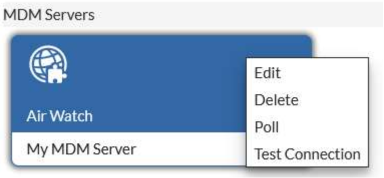
2. Use the field definitions for the MDM Services in the following table to enter the MDM Service information.

MDM Services Field Definitions

Field	Definition
Name	Name of the connection configuration for the connection between an MDM system and FortiNAC.
Login API URL	Default: https://login.microsoftonline.com Can be modified if necessary (e.g.if international domain is required).
Graph API URL	Default: https://graph.microsoft.com Can be modified if necessary (e.g.if international domain is required).
Identifier	Add the Directory (tenant) ID.
Application ID	Add the Application (client) ID.
Access Key	Add the Client Secret Value.
Enable Delegated Permissions	Set to disabled.
Enable 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.
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.
Enable Application Updating	****Leave disabled. Currently not applicable with InTune****
Enable Automatic Registration Polling (MDM Polling)	Indicates how often FortiNAC should poll the MDM system to collect managed device information. Each time a poll executes, queries are sent to the MDM for: • The managed device list (one query per 100 entries) • One additional query per each managed device If MDM notifications are configured, set the MDM Poll frequency to **1 Day**. If notifications are not configured, the frequency can be set higher. **Note:** When choosing an interval, consider the number of queries sent per MDM poll, the size of the MDM's database and the number of PODs integrated with the same MDM. If the frequency is set too high, the MDM may not be able to manage the rate of queries from FortiNAC, causing performance issues.

3. Click **OK** to save.

4. To verify FortiNAC can reach the MDM Server, right-click on the connector and select **Test Connection**.



5. To manually poll the MDM Server, right-click on the connector and select **Poll**.

6. To make any changes to the connector configuration, right-click and select **Edit**.

7. (Versions 9.1.5, 9.2.2 and above): Enable Host by Serial Number lookup. Allows FortiNAC to find hosts by serial number if unable to find by MAC address. Refer to ID 0761623 in Release Notes. In the FortiNAC CLI, login as root and run

globaloptiontool -name persistentAgentSecMgmt.findHostBySerialNumber -set true

Proceed to Events.

MobileIron

When a connection is established between FortiNAC and MobileIron Mobile Device Management (MDM) mobile devices connecting to the network can be registered in FortiNAC based on information stored in the MobileIron database. FortiNAC periodically polls MobileIron to update records for those devices that are registered in FortiNAC. This integration speeds up the registration process and eliminates the need to install both the FortiNAC agent and the MobileIron Agent on a mobile device.

This implementation list assumes that MobileIron is in place and managing mobile devices. The list below outlines the requirements for integrating MobileIron and FortiNAC.

Requirements

FortiNAC

- Supported Engine Version: 8.0 and greater
- Recommended Engine Version: ___ and greater

MobileIron

- Each managed device must have the MobileIron Agent installed. Refer to the MobileIron documentation for instructions.
- Each managed device must be running an Operating System supported by MobileIron. Otherwise, the device becomes a rogue and goes through the regular registration process. Below is the list of supported Operating Systems:
  - Apple iOS
  - Android
  - Mac OSX
  - BlackBerry
  - Windows Phone
  - Symbian

Configure MobileIron

1. Configure a System Administrator user in MobileIron to be used by FortiNAC for authentication when requesting data.
2. The account that is used to access MobileIron must have the API role check box selected.

Proceed to Configure FortiNAC.

Nozomi

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

FortiNAC collects the following host data from Nozomi:

- Type (PC, Android, IOS, Camera, PLC/OT Device)
- Operating System
- Host Name

Requirements

FortiNAC

- Supported Engine Version: 8.6.0 and greater
- FortiNAC PRO License (*only required if parsing IOC SYSLOG events*)
- Certificate used to sign the Nozomi system's certificate is installed in FotiNAC as a trusted certificate*

Nozomi

- Supported Software Version: v19.x and greater
- Valid signed SSL certificate installed in Nozomi system*
- REST API account on Nozomi system

*When using SSL or TLS security protocols for communications between FortiNAC and some servers such as Nozomi, a security certificate may be required. The need for the certificate is dependent upon the configuration of the directory. In most cases, FortiNAC automatically imports the certificate it needs. However, if this is not the case, import the certificate. For instructions, see section Create a keystore for SSL or TLS of the Administration Guide. If certificate is not available, see Communication without SSL Certificate in Appendix.

Proceed to Configure FortiNAC.

Configure FortiNAC

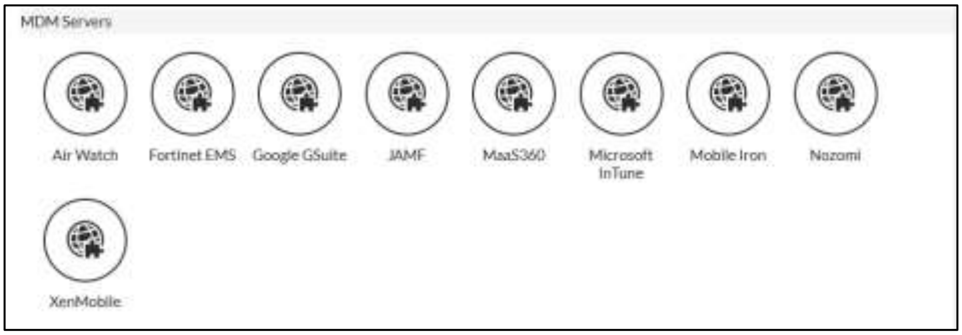
FortiNAC and the MDM system work together sharing data via an API to secure the network. FortiNAC leverages the data in the MDM database and registers hosts using that data as they connect to the network.

MDM Service Connectors

FortiNAC Manager Environments: The MDM Service Connector can be configured either on the FortiNAC Manager or the individual managed FortiNAC servers. For details see MDM services in the Manager Guide.

Configure a MDM Service Connector to establish a connection with the MDM server. MDM Service Connectors are used to configure the connection or integration between FortiNAC and MDM server.

1. In the Administration UI, navigate to **Network > Service Connectors.**
2. Click **Create New.**



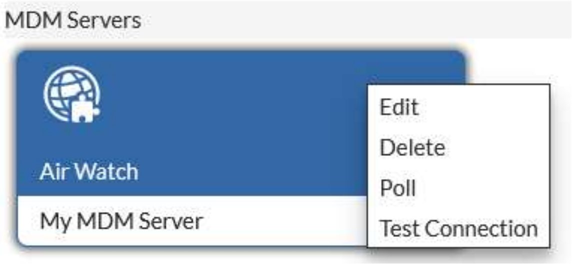
3. Click on the appropriate MDM Server.
4. Use the field definitions for the MDM Service Connector in the following table to enter the MDM Service information. Click **OK** to save.

MDM Service Connector Field Definitions

Field	Definition
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 the MDM system. **Note**: • If secured with SSL certificate, requires the server name as it appears in the certificate. (Example: https://services.m3.mydomain.com) • For some MDMs (such as Jamf), this could be either an on-premise server URL or cloud based URL.
User ID	User name of the account used by FortiNAC to log into the MDM system when requesting data. GSuite: Email address of the Google cloud account used to generate the service account (do not use the email generated for the service account).
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.
Identifier	A type of key used to identify FortiNAC to the MDM server. This field is not required for all MDM products. Airwatch/Workspace ONE, This is the API Key generated during the Airwatch/Workspace ONE Configuration. An API key is a unique code that identifies the FortiNAC server to Airwatch/Workspace ONE and is part of the authentication process for Airwatch/Workspace ONE.
Application ID	Enter the application ID.
Platform ID	Enter the platform version number.
Application Version	Enter the application version number.
Access Key	Enter the application access key (API key).

Enable Automatic Registration Polling (MDM Polling)	Indicates how often FortiNAC should poll the MDM system to collect managed device information. Each time a poll executes, queries are sent to the MDM for: • The managed device list (one query per 100 entries) • One additional query per each managed device If MDM notifications are configured, set the MDM Poll frequency to **1 Day**. If notifications are not configured, the frequency can be set higher. **Note:** When choosing an interval, consider the number of queries sent per MDM poll, the size of the MDM's database and the number of PODs integrated with the same MDM. If the frequency is set too high, the MDM may not be able to manage the rate of queries from FortiNAC, causing performance issues.
Enable 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. Google GSuite: Full (paged) poll is performed. FortiNAC stops looking once the endpoint is found. Jamf: Single device lookup using the MAC address.
Revalidate Health Status On Connect	If enabled, when the host connects to the network FortiNAC queries the MDM server to determine if the host is compliant with MDM policies. **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. 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. • Nozomi: Currently not applicable
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. GSuite: FortiNAC does not remove records based on host status (e.g. ACTIVE, DISABLED, DEPROVISIONED).
Enable 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. • InTune: Currently not applicable • Nozomi: Currently not applicable

The new connector will appear under the MDM Servers section.



5. To verify FortiNAC can reach the MDM Server, right-click on the connector and select **Test Connection**.
6. To manually poll the MDM Server, right-click on the connector and select **Poll**.
7. To make any changes to the connector configuration, right-click and select **Edit**.

Proceed to Captive Portal Configuration.

Captive Portal Configuration

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

1. Navigate to **Portal > 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 MDM 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 Portal Content Editor in the Administration Guide 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.

For a list of recommended domains to add, see Domains to Add to the Allowed Domains List under the Cookbook section of the Document Library.

1. Navigate to **Network > Settings > Control > Allowed Domains**.
2. In the Domains section of the window, click **Add**.
3. Enter the domain name and click **OK**. Repeat to add additional domains.

   - Wildcards such as * cannot be used when entering Domain names.
   - A large domain that contains sub-domains can be entered. For example, if you enter Microsoft.com, users can access all domains for Microsoft. However, if you enter a sub-domain, such as downloads.microsoft.com, then users can only access that specific domain.

4. Click **Save Settings**.

For additional information, see Allowed Domains in the Administration Guide.

Proceed to Events.

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
- MDM Host Compliance Failed
- MDM Host Compliance Passed

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

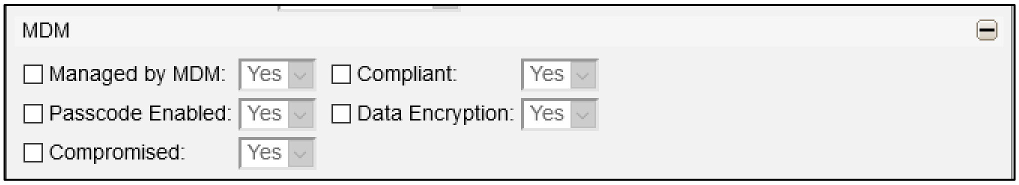
Proceed to Policies.

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 (Applicable MDM's: All)	FortiNAC registered the host based on data from MDM database.
Compliant (Applicable MDM's: Airwatch/Workspace ONE, Fortinet EMS, MS InTune, XenMobile (Citrix), MaaS360, MobileIron)	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 (Applicable MDM's: Airwatch/Workspace ONE, XenMobile (Citrix), MaaS360, MobileIron)	Indicates if there is a passcode required to access the endpoint.
Data Encryption (Applicable MDM's: Airwatch/Workspace ONE, XenMobile (Citrix), MaaS360, MobileIron)	Indicates whether data encryption is enabled on the endpoint.
Compromised (Applicable MDM's: Airwatch/Workspace ONE, XenMobile (Citrix), MaaS360, MobileIron)	This is an additional field separate from whether it's complaint, if the MDM marks the endpoint as compromised.



MDM

□ Managed by MDM: Yes □ Compliant: Yes

□ Passcode Enabled: Yes □ Data Encryption: Yes

□ Compromised: Yes

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

- Devices registered using MDM are registered to a user if the user in the MDM 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.

- **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.

Proceed to Validate.

Validate

Execute the following use cases to verify the MDM integration is performing as expected.

Mobile Devices with Supported Operating Systems (MDM Agent installed)

1. Connect a rogue mobile device to the network (ensure device is registered in MDM and has MDM agent installed).
2. In FortiNAC Administration UI, navigate to **Users & Hosts > Hosts** and search for the device's MAC address – the device's host record should appear and its adapter record should reflect the device being assigned to the FNAC Service Network.
3. FortiNAC queries the MDM server for information about that host and registers using the MDM server information. The On Demand Registration setting determines when FortiNAC queries the MDM server.

   - **On Demand Registration is enabled**: FortiNAC queries the MDM server immediately.

   - **On Demand Registration is not enabled**: FortiNAC waits for the next MDM polling interval.

How the host is registered in FortiNAC

- **Associated username in the MDM matches username in FortiNAC**:
  - Host is registered to that user.
  - Mobile devices registered from Airwatch/Workspace ONE will be assigned one of the following roles:
    - Employee Owned
    - Corporate - Shared
    - Corporate - Dedicated
    - NAC - Default (if not defined in Airwatch/Workspace ONE)

    These roles can be used as a filter in User/Host Profiles. Roles that are defined by Airwatch/Workspace ONE 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.

- **Associated username in the MDM does not match any usernames in FortiNAC**:
  - Host is registered as a device.
  - Host role is set to NAC-Default.

4. FortiNAC should then re-provision the mobile device's network access to the appropriate VLAN or policy dependent upon the Network Access Policy defined. If unexpected results occur, see Troubleshooting.

Mobile Devices with Supported Operating Systems (No MDM Agent)

1. Connect a mobile device that is running one of the Operating Systems supported by the MDM. Ensure the MDM agent is *not* installed.

2. In FortiNAC Administration UI, navigate to **Users & Hosts > Hosts** and search for the device's MAC address – the device's host record should appear and its adapter record should reflect the device being assigned to the isolation network.

3. Open browser on the mobile device - browser should be redirected to the Captive Portal page that directs the user to install the MDM agent.

4. Download and install the agent - host record should update and display as either a registered host to a user (if user record already exists in FortiNAC) or as a device.

5. FortiNAC should then re-provision the mobile device's network access to the appropriate VLAN or policy dependent upon the Network Access Policy defined.

If unexpected results occur, see Troubleshooting.

Mobile Devices with Unsupported Operating Systems

1. Connect a mobile device that is not running one of the Operating Systems supported by the MDM.

2. In FortiNAC Administration UI, navigate to **Users & Hosts > Hosts** and search for the device's MAC address – the device's host record should appear as a Rogue and its adapter record should reflect the device being assigned to the isolation network.

3. If a Device Profiling Rule is not configured to register the device, open browser on the mobile device - browser should be redirected to the Registration Captive Portal page (*not* the MDM Registration page).

4. Register via normal means.

5. FortiNAC should then re-provision the mobile device's network access to the appropriate VLAN or policy dependent upon the Network Access Policy defined.

If unexpected results occur, see Troubleshooting.

Remove Hosts Deleted from MDM Server

1. Disable or delete Host in the MDM*.
2. In a separate window, navigate to **Network > Service Connectors**
3. Right-click on the MDM server connector and click **Poll Now** (or wait for the next polling cycle if Automatic Polling is enabled). The host should disappear from the Host View.

*GSuite: Currently hosts are not removed automatically in FortiNAC.

If unexpected results occur, see Troubleshooting.

Troubleshooting

Related KB Articles

General

Troubleshooting MDM registration issues
Troubleshooting Policies
MDM Poll Failures Due to Invalid Characters

Airwatch/Workspace ONE

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

Use the following KB article to gather the appropriate logs using the debugs below.
Gather logs for debugging and troubleshooting

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

Function	Syntax	Log File

Airwatch/Workspace ONE	`nacdebug -name AirWatchServer true`
	`nacdebug -name MdmManager true`
		/bsc/logs/output.master

Citrix Endpoint Management	`nacdebug -name XenMobileServer true`
	`nacdebug -name MdmManager true`
		/bsc/logs/output.master

Google GSuite	`nacdebug -name GoogleGSuiteServer true`
	`nacdebug -name MdmManager true`
		/bsc/logs/output.master

Jamf	`nacdebug -name JamfServer true`
	`nacdebug -name MdmManager true`
		/bsc/logs/output.master

Maas360	`nacdebug -name MaaS360Server true`
	`nacdebug -name MdmManager true`
		/bsc/logs/output.master

Microsoft InTune	`nacdebug -name MSInTuneServer true`
	`nacdebug -name MdmManager true`
		/bsc/logs/output.master

MobileIron	`nacdebug -name MobileIronServer true`
	`nacdebug -name MdmManager true`
		/bsc/logs/output.master

Nozomi	`nacdebug -name NozomiServer true`
	`nacdebug -name MdmManager true`
		/bsc/logs/output.master

Disable debug	`nacdebug -name <debug name> false`	N/A

Appendix

Airwatch/Workspace ONE Host/Device Registration Process

When Airwatch/Workspace ONE 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/Workspace ONE, 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/Workspace ONE MDM Agent is installed. This requires that On-Demand registration be enabled in the MDM Service record for the Airwatch/Workspace ONE integration with FortiNAC.
   - Android
   - Apple iOS
   - BlackBerry
   - Mac OS X
   - Symbian
   - Windows Mobile
   - Windows Phone
4. Hosts without the Airwatch/Workspace ONE 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/Workspace ONE MDM Agent installed, FortiNAC connects to Airwatch/Workspace ONE and retrieves the host data from the Airwatch/Workspace ONE database and registers the host in FortiNAC.
6. If the host is associated with a user in Airwatch/Workspace ONE 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/Workspace ONE and FortiNAC determine when Airwatch/Workspace ONE is polled for updated information.

Airwatch/Workspace ONE Role Assignment

By default, roles assigned by MDM will take precedence.

Example: Host is assigned MDM role A and also has user role B. When evaluated by FortiNAC for policy assignment, if both MDM and user roles are listed in the user/host profile, policy applied will be based on MDM role (role A).

If this behavior is not desired, FortiNAC can be configured to use user/host roles over MDM assigned roles. Contact Support for assistance if required.

1. In FortiNAC CLI, login as root.
2. Modify file **/bsc/campusMgr/master_loader/.masterPropertyFile**
   Append the following

   ```
   FILE_NAME=./properties_plugin/airWatch.properties
   {
   com.bsc.plugin.airwatch.AirWatchServer.mdmRoles=false
   }
   ```

3. Restart control processes to apply
   restartNAC

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/Workspace ONE.

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/Workspace ONE (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:

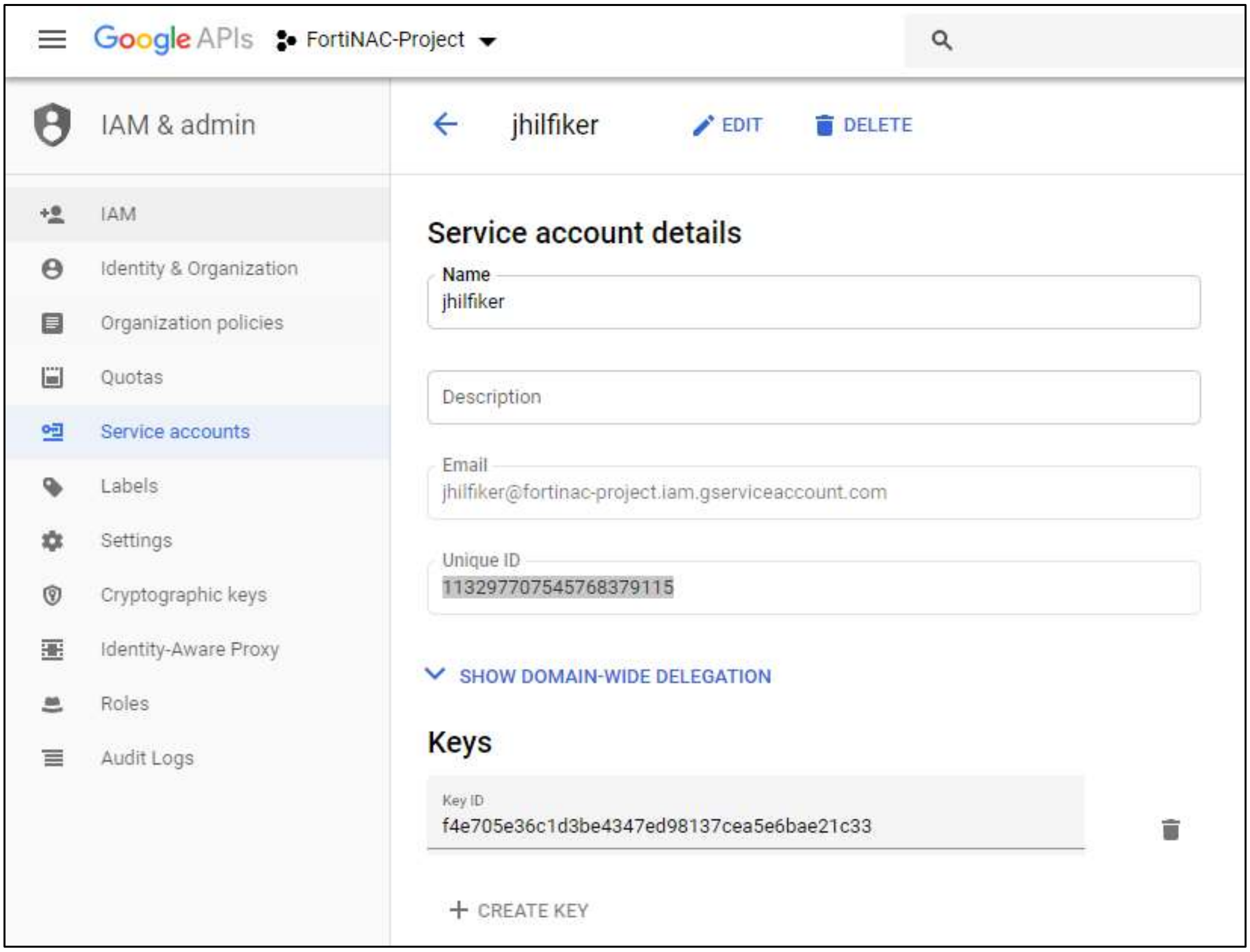
```
echo -n | openssl s_client -connect qa6-74.bradfordnetworks.com:8443 | sed -ne '/-BEGIN CERTIFICATE-/,/-END CERTIFICATE-/p' > server.cert
depth=0 CN = qa6-74.bradfordnetworks.com
verify error:num=18:self signed certificate
verify return:1
depth=0 CN = qa6-74.bradfordnetworks.com
verify return:1
DONE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

b. ftp or scp file to desired location.

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

Enable API Access to the Service Account (Older GSuite UI)

1. Go back to the Service Account view and select your service account. Highlight the Unique ID for your service account and copy it to your buffer.



Service account details

Name: jhilfiker

Description

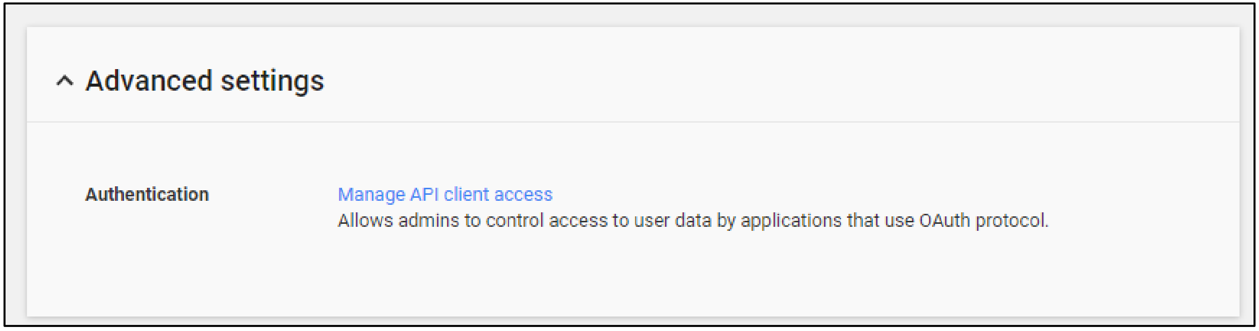
Email: jhilfiker@fortinac-project.iam.gserviceaccount.com

Unique ID: 113297707545768379115

Keys

Key ID: f4e705e36c1d3be4347ed98137cea5e6bae21c33

2. Log into https://admin.google.com on the Home view, click on **Security** then on the security view click on **Advanced Settings**.



Advanced settings

Authentication — Manage API client access
Allows admins to control access to user data by applications that use OAuth protocol.

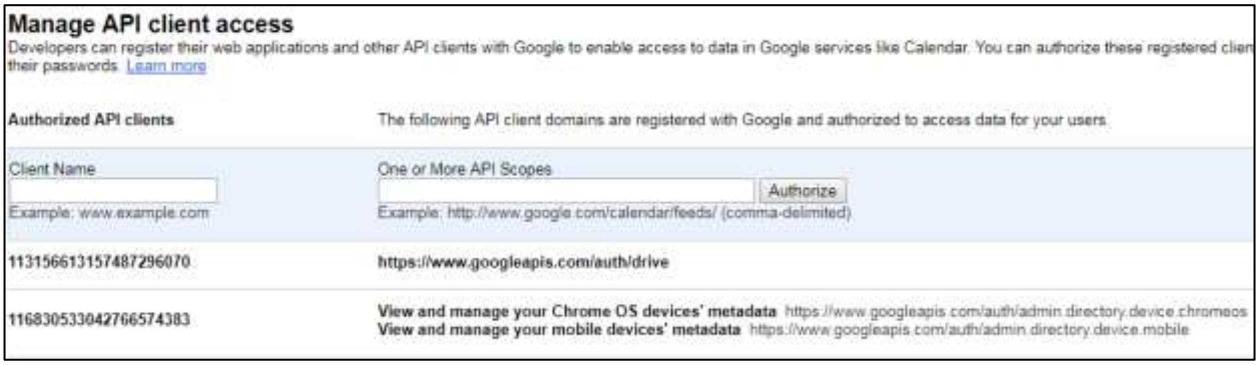
3. Click on **Manage API client access**.

4. Paste in your UniqueID obtained for your service account into the **Client Name** field. Then

add access to the required APIs using this string (copy and paste this exactly into the One or More API Scopes field. **Note:** do not use the “Copy Link Address” option):

```
https://www.googleapis.com/auth/admin.directory.device.mobile,https://www.googleapis.com/auth/admin.directory.device.chromeos
```

5. Then click the **Authorize** button.



Manage API client access

Developers can register their web applications and other API clients with Google to enable access to data in Google services like Calendar. You can authorize these registered clien their passwords. Learn more

Authorized API clients	The following API client domains are registered with Google and authorized to access data for your users.
Client Name Example: www.example.com	One or More API Scopes Example: http://www.google.com/calendar/feeds/ (comma-delimited)
113156613157487296070	**https://www.googleapis.com/auth/drive**
116830533042766574383	**View and manage your Chrome OS devices' metadata** https://www.googleapis.com/auth/admin.directory.device.chromeos **View and manage your mobile devices' metadata** https://www.googleapis.com/auth/admin.directory.device.mobile

6. The “View and manage your Chrome OS devices’ metadata” and “View and manage your mobile devices’ metadata” should be listed as the 2 APIs that are accessible using the service account ID.

Proceed to Configure FortiNAC.

MaaS360 Host/Device Registration Process

When MaaS360 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 that is not supported by MaaS360, it becomes a rogue and goes through the regular registration process, either through the captive portal or 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 MaaS360 MDM Agent is installed. This requires that On-Demand registration be enabled in the MDM Service record for the MaaS360 integration with FortiNAC. See MDM Services below.
   - Apple iOS
   - Android
   - Samsung
   - BlackBerry
   - Windows Phone
   - Symbian

4. Hosts without an 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. Links to the sites where agents can be downloaded must be configured by an Admin user under **Content Editor > Global > Settings > Use Configured MDM and Content Editor > Registration > MDM Registration**.

5. If the host has the MaaS360 MDM Agent installed, FortiNAC connects to MaaS360, retrieves the host data from the MaaS360 database and registers the host in FortiNAC.
   - If the host is associated with a user in MaaS360 that also exists in FortiNAC, then the host is registered to that user.
   - If the user is unknown in FortiNAC, the host is registered as a device.

6. 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.

7. Settings selected for the MDM Service that controls the connection between MaaS360 and FortiNAC determine when MaaS360 is polled for updated information.

Nozomi Communication without SSL Certificate

By default, FortiNAC will not connect to the Nozomi server without a valid certificate installed. If a certificate is not available for install, however, FortiNAC can be configured to connect and ignore certificate validation.

1. In FortiNAC CLI, login as root.
2. Modify file **/bsc/campusMgr/master_loader/.masterPropertyFile**
3. Append the following

```
FILE_NAME=./properties_plugin/nozomi.properties
{
com.bsc.plugin.airwatch.NozomiServer.insecureSSL=true
}
```

4. Restart control processes to apply
   restartNAC

Azure Active Directory Delegated Permissions

This is the original method used. Requires a signed-in user to give FortiNAC permission to use the API when creating an MS InTune service connector. The process was error-prone and involved the user jumping back and forth between the MS Azure portal and the MS InTune connector view.

Existing MS Intune connectors (prior to the change) will have the Enable Delegated Permissions method enabled and will continue to work as before. However, for new service connectors, this button will be disabled and instead will require the user to register the Application with Azure with Application Permissions which is a much simpler process and better user experience.

The following information is for reference.

Configure Azure Active Directory and InTune

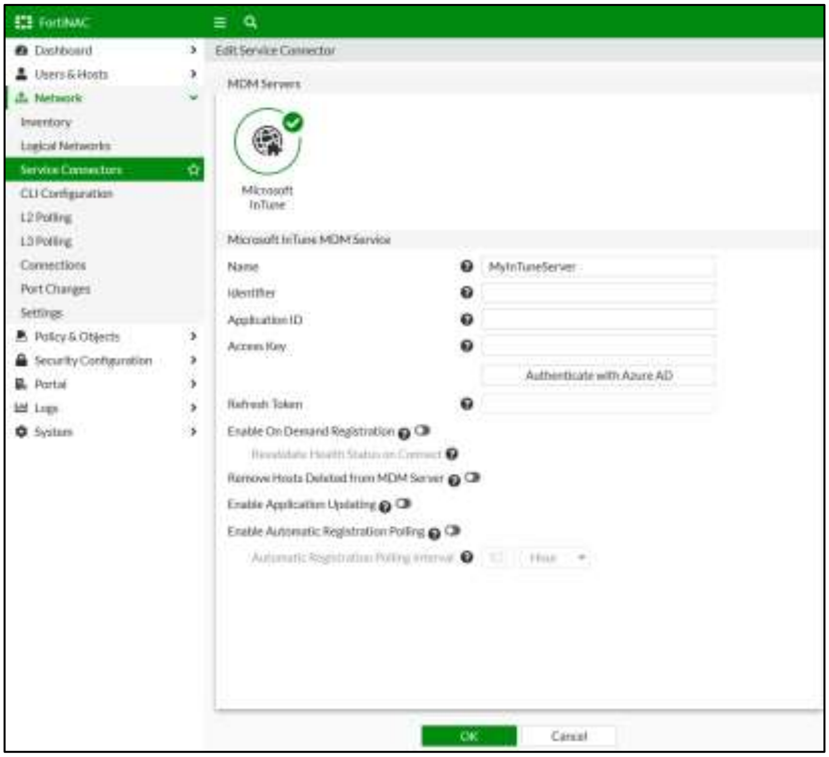
Create a New Application Registration

3. From the **Azure Active Directory > App registrations** view, click on **+ New registration**. Enter a unique name for the application (something like “FortiNAC Integration”).
4. Configure the Redirect URI. This will be used when responding to the authentication request made by FortiNAC in the next section (Configure FortiNAC step 3 - Authenticate With Azure AD).

    a. Leave window open. In a separate browser window, login to the FortiNAC Administration UI. Name used in URL should be the hostname secured by the SSL certificate for the Admin UI. Certificates can be viewed under **Security Configuration > Certificate Management**.

       https://<FortinacDNSHostname>:8443/

    b. Navigate to **Network > Service Connectors.**
    c. Click **Create New.**
    d. Click **Microsoft InTune**.
    e. Populate the **Name** field and click **OK**. The new Fabric Connector should now appear.
    f. Double click on the connector or right-click and select **Edit**.



Edit Service Connector

MDM Servers

Microsoft InTune MDM Service

Name: MyInTuneServer

Identifier

Application ID

Access Key

Refresh Token

Enable On Demand Registration

Revalidate Health Status on Connect

Remove Hosts Deleted from MDM Server

Enable Application Updating

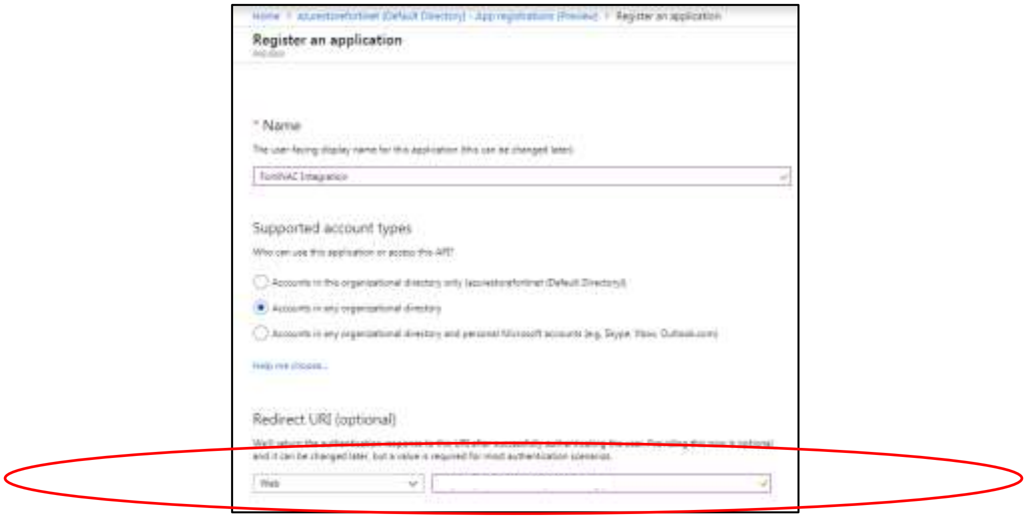
Enable Automatic Registration Polling

Automatic Registration Polling Interval: 12 Hour

g. Copy the entire URL in the browser window and leave window open. The URL should look similar to the following

https://<FortinacDNSHostname>:8443/gui/network/service-connectors/MICROSOFT_INTUNE_MDM/1

h. In the Azure window under **Redirect URI**, select **Web**.
i. In the other field, enter the URL copied in step g.


Home > azurestorefortinet (Default Directory) - App registrations (Preview) > Register an application
Help me choose...

Register an application

* Name

The user-facing display name for this application (this can be changed later).

FortiNAC Integration

Supported account types

Who can use this application or access this API?

○ Accounts in this organizational directory only (azurestorefortinet (Default Directory))

● Accounts in any organizational directory

○ Accounts in any organizational directory and personal Microsoft accounts (e.g. Skype, Xbox, Outlook.com)

Redirect URI (optional)

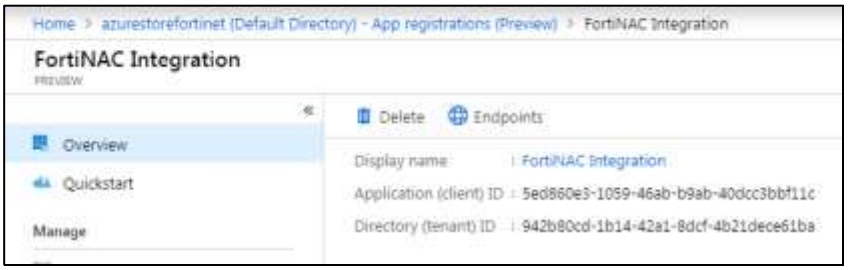
We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Web

Important: If the FortiNAC hostname in the browser URL does not match the hostname entered in the Redirect URI, the authentication attempt will fail because the hostname in the URI does not match the hostname in the request.

High Availability: If FortinNAC is configured for High Availability, enter URI for Primary Server and the URI for the Secondary Server (do not use a shared name).

5. From the Application Registration view, copy down the following (will be used in FortiNAC configuration):
   - **Application (client) ID**
   - **Directory (tenant) ID**



Home > azurestorefortinet (Default Directory) - App registrations (Preview) > FortiNAC Integration

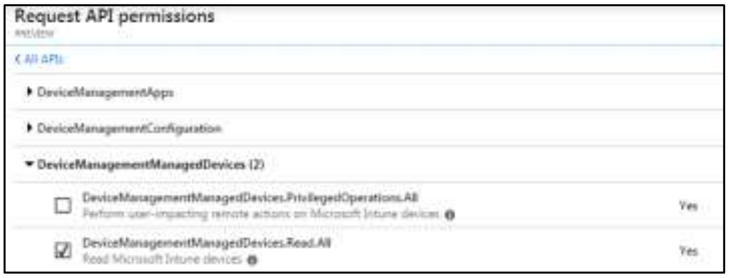
FortiNAC Integration
PREVIEW

Display name : FortiNAC Integration
Application (client) ID : 5ed860e3-1059-46ab-b9ab-40dcc3bbf11c
Directory (tenant) ID : 942b80cd-1b14-42a1-8dcf-4b21dece61ba

6. From **Certificates & Secrets** select **+ New client secret** and create a secret.

7. Review the secret for special characters (specifically colons or question marks). If they are present, generate a new secret. Repeat this process until a secret is generated without these special characters. The Refresh Token generated in the following section may not populate if the client secret contains colons or question marks. This caveat is currently under investigation.
8. Copy and store the secret value (not the ID). This will be used in FortiNAC configuration. **Note:** The secret will be obscured once leaving the view and returning.

9. From **API Permissions** select **+ Add a permission**.
10. Select **Microsoft Graph** > **Delegated permissions**
11. From the list expand **DeviceManagementManagedDevices**
12. Select the following:
    DeviceManagementManagedDevices.Read.All



Request API permissions
PREVIEW

< All APIs

▸ DeviceManagementApps

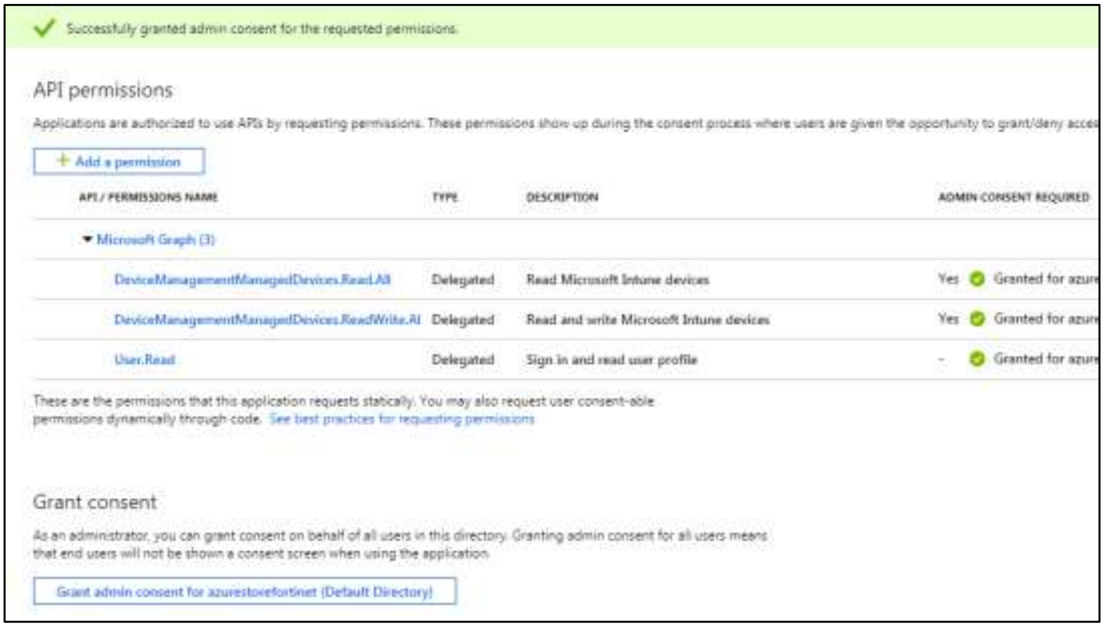
▸ DeviceManagementConfiguration

▾ DeviceManagementManagedDevices (2)

☐ DeviceManagementManagedDevices.PrivilegedOperations.All
Perform user-impacting remote actions on Microsoft Intune devices — Yes

☑ DeviceManagemevitManagedDevices.Read.All
Read Microsoft Intune devices — Yes

13. Grant Consent for the selected API's by selecting the **Grant admin consent for…** button.



✓ Successfully granted admin consent for the requested permissions.

API permissions

Applications are authorized to use APIs by requesting permissions. These permissions show up during the consent process where users are given the opportunity to grant/deny acces

API / PERMISSIONS NAME	TYPE	DESCRIPTION	ADMIN CONSENT REQUIRED	
▾ Microsoft Graph (3)				
DeviceManagementManagedDevices.Read.All	Delegated	Read Microsoft Intune devices	Yes	● Granted for azure
DeviceManagementManagedDevices.ReadWrite.Al	Delegated	Read and write Microsoft Intune devices	Yes	● Granted for azure
User.Read	Delegated	Sign in and read user profile	-	● Granted for azure

These are the permissions that this application requests statically. You may also request user consent-able permissions dynamically through code. See best practices for requesting permissions

Grant consent

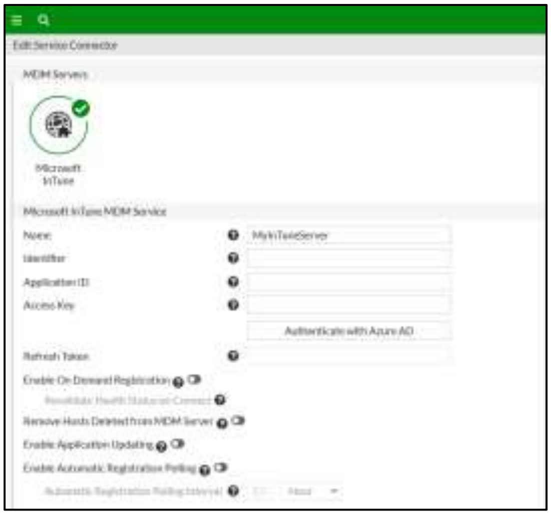
As an administrator, you can grant consent on behalf of all users in this directory. Granting admin consent for all users means that end users will not be shown a consent screen when using the application.

Grant admin consent for azurestorefortinet (Default Directory)

Configure FortiNAC

Configure a MDM Service to establish a connection with the Microsoft InTune Graph API. MDM Services are used 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.

8. Complete configuring the Microsoft Intune Fabric Connector created in the previous section. To return to the view, navigate to **Network > Service Connectors** and double click on the connector.



Name: MyInTuneServer
Identifier:
Application ID:
Access Key:
Refresh Token:
Enable On Demand Registration
Revalidate Health Status on Connect
Remove Hosts Deleted from MDM Server
Enable Application Updating
Enable Automatic Registration Polling
Automatic Registration Polling Interval: Hour

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

MDM Services Field Definitions

Field	Definition
Name	Name of the connection configuration for the connection between an MDM system and FortiNAC.
Identifier	Add the Directory (tenant) ID.
Application ID	Add the Application (client) ID.
Access Key	Add the Client Secret Value.

10. Close any other browser windows that are logged into Microsoft before proceeding.

11. Click the **Authenticate with Azure AD** button. This will launch a dialog that will prompt to log into the Microsoft account.

Important: Use the same admin account used to create the Application within Azure.

This will generate a Refresh Token, and populate it in the Refresh Token field. The Refresh Token will be used by FortiNAC to generate access tokens. These tokens allow FortiNAC to perform API queries for the Graph API.

Note: The Refresh Token may not populate if the client secret contains special characters such as colons and question marks. See step 5 of Create a New Application Registration.

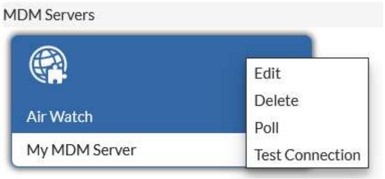
12. Use the field definitions for the MDM Services in the following table to enter the MDM Service information.

MDM Services Field Definitions

Field	Definition
Enable 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.
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.
Enable Application Updating	****Leave disabled. Currently not applicable with InTune****
Enable Automatic Registration Polling (MDM Polling)	Indicates how often FortiNAC should poll the MDM system to collect managed device information. Each time a poll executes, queries are sent to the MDM for: • The managed device list (one query per 100 entries) • One additional query per each managed device If MDM notifications are configured, set the MDM Poll frequency to **1 Day**. If notifications are not configured, the frequency can be set higher. **Note:** When choosing an interval, consider the number of queries sent per MDM poll, the size of the MDM's database and the number of PODs integrated with the same MDM. If the frequency is set too high, the MDM may not be able to manage the rate of queries from FortiNAC, causing performance issues.

13. Click **OK** to save.

14. To verify FortiNAC can reach the MDM Server, right-click on the connector and select **Test Connection**.



15. To manually poll the MDM Server, right-click on the connector and select **Poll**.

16. To make any changes to the connector configuration, right-click and select **Edit**.

17. (Versions 9.1.5, 9.2.2 and above): Enable Host by Serial Number lookup. Allows FortiNAC to find hosts by serial number if unable to find by MAC address. Refer to ID 0761623 in Release Notes. In the FortiNAC CLI, login as root and run

```
globaloptiontool -name persistentAgentSecMgmt.findHostBySerialNumber -set true
```

Proceed to Events.