



VMDR Mobile

User Guide
Version 1.5.1-0

January 13, 2023

Copyright 2023 by Qualys, Inc. All Rights Reserved.

Qualys and the Qualys logo are registered trademarks of Qualys, Inc. All other trademarks are the property of their respective owners.

Qualys, Inc.
919 E Hillsdale Blvd
4th Floor
Foster City, CA 94404
1 (650) 801 6100



Table of Contents

About this guide.....	3
About Qualys	3
Qualys Support	3
Get Started	4
Configurations	6
EULA Management	6
APNs Certificates	8
What is an APNs Certificate?	8
Pre-requisites to Generate the Certificate	8
Steps to Generate APNs Certificate	8
Organization Info	14
Organization Information	14
Settings	14
Configure Connector	16
VMDR Mobile User Management.....	19
Create VMDR Mobile User	19
Bulk User Upload	21
Importing Users	21
Create a new Tag	24
Mobile Device Inventory	25
Vulnerability Assessment.....	28
Vulnerability Assessment in VMDR Mobile	28
Patch Orchestration	33
Policy Compliance	39
Monitor the Assets	41
Re-evaluation of Controls	42
Dashboards and Reports.....	44
Customizable Dynamic Dashboard	44
Global Dashboard Permissions	44
Reports	45
Appendix.....	47

Renew APNs Certificate 47

About this guide

This user guide helps to get started with VMDR Mobile and use with Cloud Platform.

About Qualys

Qualys, Inc. (NASDAQ: QLYS) is a pioneer and leading provider of cloud-based security and compliance solutions. The Qualys Cloud Platform and its integrated apps help businesses simplify security operations and lower the cost of compliance by delivering critical security intelligence on demand and automating the full spectrum of auditing, compliance and protection for IT systems and web applications.

Founded in 1999, Qualys has established strategic partnerships with leading managed service providers and consulting organizations including Accenture, BT, Cognizant Technology Solutions, Deutsche Telekom, Fujitsu, HCL, HP Enterprise, IBM, Infosys, NTT, Optiv, SecureWorks, Tata Communications, Verizon and Wipro. The company is also a founding member of the [Cloud Security Alliance \(CSA\)](#). For more information, please visit www.qualys.com.

Qualys Support

Qualys is committed to providing you with the most thorough support. Through online documentation, telephone help, and direct email support, Qualys ensures that your questions will be answered in the fastest time possible. We support you 7 days a week, 24 hours a day. Access support information at www.qualys.com/support/.

Get Started

Welcome to the Qualys VMDR Mobile User Guide. Qualys VMDR Mobile offers you a cloud-based solution, to help you secure, monitor, and manage mobile devices (including smart phones and tablets) across your enterprise.

With VMDR Mobile, you can:

- Easily on-board mobile devices (mobile, tablets, iPads) to get compressive visibility into mobile devices details, installed apps, and configurations, even if they are not on VPN or connected to company network,
- Get real-time visibility into vulnerabilities and configuration assessment along with monitoring for potential harmful applications,
- Take remote response actions and seamless patch orchestration for the Android applications' vulnerabilities,
- Evaluate the compliance posture of mobile devices by evaluating against CIS benchmark, NIST mandate, etc,
- Manually hunt the malware that are present on the devices through the SHA-1, SHA-256, and MD5.

We'll help you get started quickly!

Supported Platforms

- Android (Version 4.4.2 and higher)
- iOS (Version 11.0 and higher)

Note: Before the 1.5.1-0 release, iOS version 9.0 and higher were supported. With the 1.5.1-0 release, the iOS supported versions are 11.0 and higher. This is because the iOS QAgent requires cocoaLumberjack Library, and this Library supports iOS 11 and higher versions only.

- iPadOS (Version 13.1 and higher)

Key Benefits of using VMDR Mobile

- Easy on-boarding to get continuous visibility and monitoring of mobile devices. To know more, refer the following:

[Configurations](#)

[VMDR Mobile User Management](#)

[Mobile Device Inventory](#)

- Real-time visibility into latest vulnerabilities and configuration assessment. To know more, refer the following:

[Vulnerability Assessment](#)

Policy Compliance

Monitoring Controls

- Remote response and seamless patch orchestration. To know more, refer the following:

Patch Orchestration

- Real-time evaluations against CIS benchmark, NIST, etc.

Before starting, let's understand different users mentioned in this document:

Admin User - Admin user configures all necessary settings required to enroll the mobile devices, creates VMDR Mobile users, and monitor various dashboards and reports.

VMDR Mobile User - Users added in the VMDR Mobile module/app are considered as VMDR Mobile Users. VMDR Mobile Users are the holders/owners of the mobile devices and are used for the device enrollment.

What are the steps to get started with VMDR Mobile?

- 1) If the devices are enrolled in Intune, then configure Intune Connector to onboard the device seamlessly without end-user intervention. For information on configuring connector, refer [Configure Connector](#).
- 2) To onboard the device through Qualys agent, then setup the following:
 - a. **Optional Step:** Setup End User License Agreement (EULA). For information on setting up EULA, refer [EULA Management](#).
 - b. Configure APNs certificates only if your VMDR Mobile users have iOS devices to enroll. For more information, refer [APNs Certificates](#).
 - c. Create VMDR Mobile users. For detailed steps, refer [Create VMDR Mobile User](#). If you add an email address while creating VMDR Mobile user, the user will receive an email that contains the credentials and enrollment details. VMDR Mobile users have the **Bulk User Upload** option to add multiple users in one go!
 - d. Now, VMDR Mobile users can start enrolling their mobile devices. For more information, refer [Device Enrollment](#). If devices are already enrolled in any EMM, then configure the enrolled to 'Enroll device without VMDR Mobile EMM' for iOS and Android, i.e., select the 'All iOS devices' and 'All Android devices' check-boxes. For more details, refer [Enrollment Settings](#). You can auto-enroll the devices through an automated enrollment process.
- 3) Monitor mobile devices inventory and its security posture using Dashboards and Reports once VMDR Mobile users enroll their devices.

Configurations

This section helps you to create and manage EULA. It also helps you to configure APNs certificates. This section also helps you to configure organization level settings, such as organization information, enrollment settings, application settings, and sync settings.

EULA Management

Your End User License Agreement (EULA) may include the policies and declarations related to the asset management, information access, privacy, Acceptable Use Policy (AUP), reimbursement of expenses, HR policies, non-disclosure of corporate data, etc.

Typically, organization's legal team provides EULA.

Customer's use of the Cloud Services will result in Personal Identifiable Information being processed by Qualys. Customer acts as a the data controller and Qualys acts as a Data Processor. It is Customer's obligation, and Qualys shall not have any obligation, to gather the appropriate consent from every data subject from whom Customer is gathering Personally Identifiable Information through use of the Cloud Services. Customer is required to enter into an end user agreement with each data subject that informs data subject of the data that will be gathered and the use that Customer shall make of such data. Qualys offers provision to define such end user agreement and shall not be deemed to have advised Customer regarding the appropriateness or completeness of such end user agreement.

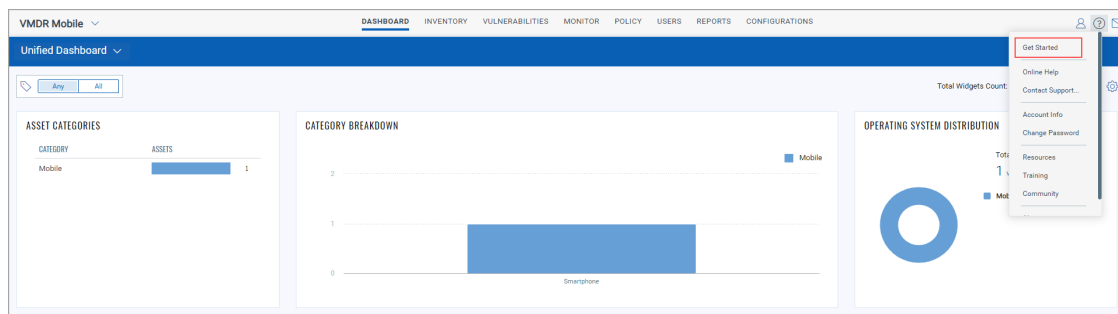
Set up the EULA from the Configuration tab. We are providing you with a provision to add the End User License Agreement text. This step is optional and you can skip it. If EULA is configured, Asset user must accept the EULA before enrolling assets.

Qualys provides you with the ability to configure your own EULA text based on your organization's need and policies. When a EULA is associated with an VMDR Mobile user, the user must accept the EULA at the time of device enrollment.

Note: This is an optional step. You can configure EULA based on your requirement or skip it if not required.

What are the steps to configure a new EULA?

1) Click help icon (question mark icon) and then click **Get Started**.



2) Click **Configure End User License Agreement** to open the Edit EULA page. Provide the EULA text and then click **Save**.

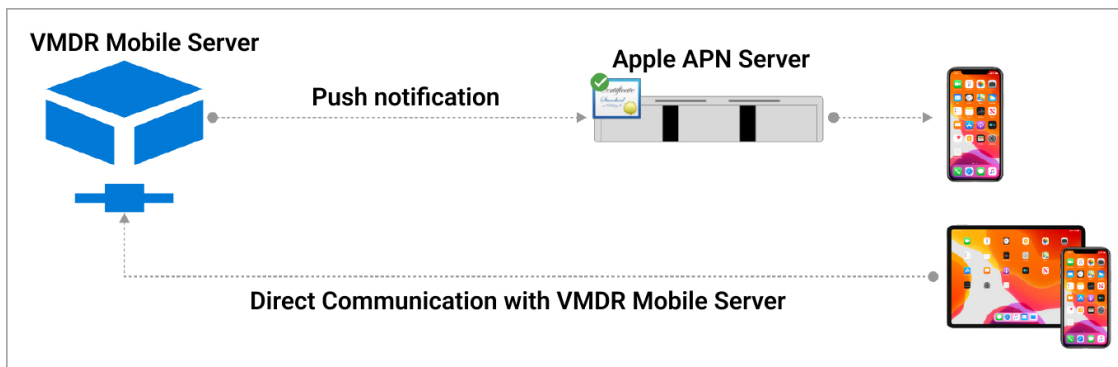
You can also access the EULA from **Configurations > EULA**. You can edit the EULA text using the **Edit** action from the quick action menu.

APNs Certificates

This section is applicable only for iOS devices. For managing iOS devices, you must obtain Apple Push Notification Service (APNs) certificate for secure communication from Qualys VMDR Mobile server with the Apple devices. Qualys VMDR Mobile helps you generate and renew APNs certificates.

What is an APNs Certificate?

VMDR Mobile uses APNs certificate to send notifications to the Apple devices when communication is initiated by the administrator or by the server for requesting information from the devices or, Apps or policies are published on the devices. No data is sent through the APNs service, only the notification.



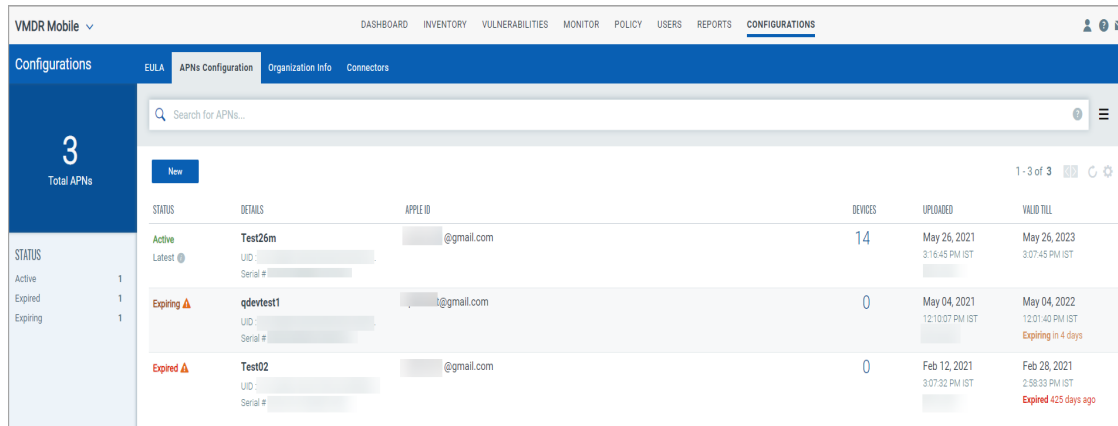
Pre-requisites to Generate the Certificate

- An Apple ID. (You can create it at <https://appleid.apple.com>). Recommended to use the Apple ID which belongs to the organization.
- Mac OS X or Windows workstation with Administrative permissions
- Web browser (Safari, Mozilla Firefox or Chrome are required to work with Apple's website)

Steps to Generate APNs Certificate

- 1) Login to the VMDR Mobile Portal at <https://xxxx.apps.qualys.com>.

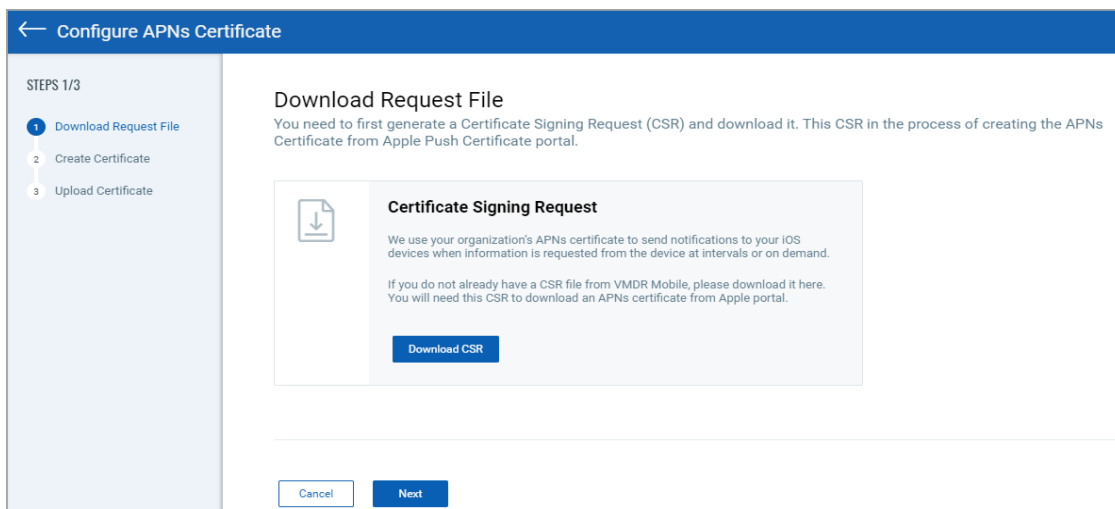
2) Navigate to **Configurations > APNs Configuration** and click **New**.



The screenshot shows the 'Configurations' section of the VMDR Mobile interface, specifically the 'APNs Configuration' tab. A sidebar on the left indicates '3 Total APNs'. The main area contains a table with the following data:

STATUS	DETAILS	APPLE ID	DEVICES	UPLOADED	VALID TILL
Active	Test26m UID: [redacted] Serial #: [redacted]	[redacted]@gmail.com	14	May 26, 2021 3:16:45 PM IST	May 26, 2023 3:07:45 PM IST
Expiring	qdevtest1 UID: [redacted] Serial #: [redacted]	[redacted]@gmail.com	0	May 04, 2021 12:10:07 PM IST	May 04, 2022 12:01:40 PM IST Expiring in 4 days
Expired	Test02 UID: [redacted] Serial #: [redacted]	[redacted]@gmail.com	0	Feb 12, 2021 3:07:32 PM IST	Feb 28, 2021 2:58:33 PM IST Expired 425 days ago

3) Download the Certificate Signing Request (CSR) file and save the file at a known location. Click **Next**.



The screenshot shows the 'Configure APNs Certificate' wizard, Step 1 of 3: 'Download Request File'. The instructions state: 'You need to first generate a Certificate Signing Request (CSR) and download it. This CSR in the process of creating the APNs Certificate from Apple Push Certificate portal.' A 'Certificate Signing Request' box contains a download icon and text: 'We use your organization's APNs certificate to send notifications to your iOS devices when information is requested from the device at intervals or on demand. If you do not already have a CSR file from VMDR Mobile, please download it here. You will need this CSR to download an APNs certificate from Apple portal.' A 'Download CSR' button is present. At the bottom, there are 'Cancel' and 'Next' buttons.

4) Click **Goto Apple Portal** link to go to the Apple Push Certificate Portal (<https://identity.apple.com/pushcert/>).

Qualys Cloud Platform

← Configure APNs Certificate

STEPS 2/3

- 1 Download Request File
- 2 **Create Certificate**
- 3 Upload Certificate

Create Certificate


Name Provide a friendly name for your certificate.

Apple ID Apple ID Note: It can be any Apple ID and need not be an Apple Developer Account.

Get your APNs certificate in 3 easy steps

- Sign in to the Apple Portal
- Upload the Certificate Signing Request (CSR)
- Download the new certificate

For more information download the APNs certificate generation guide. [Learn More](#)



[Goto Apple Portal](#)

5) Log in using corporate Apple ID and password. Click **Create a Certificate**.

Store Mac iPod iPhone iPad iTunes Support

Apple Push Certificates Portal

manmays@gmail.com [Sign out](#)

Get Started

Create a push certificate that enables your third-party server to work with the Apple Push Notification Service and your Apple devices.

[Create a Certificate](#)

FAQ


Learn more about Mobile Device Management
What about OS X Server?

Shop the [Apple Online Store](#) (1-800-MY-APPLE), visit an [Apple Retail Store](#), or find a [reseller](#).

[Apple Info](#) | [Site Map](#) | [Hot News](#) | [RSS Feeds](#) | [Contact Us](#)

Copyright © 2012 Apple Inc. All rights reserved. [Terms of Use](#) | [Privacy Policy](#)

6) Select **I have read and agree to these terms and conditions** check box, and then click **Accept**.

StoreMaciPodiPhoneiPadiTunesSupport

manmays@gmail.comSign out

Apple Push Certificates Portal

Terms of Use

PLEASE READ THE FOLLOWING LICENSE AGREEMENT TERMS AND CONDITIONS CAREFULLY BEFORE DOWNLOADING OR USING THE APPLE CERTIFICATES. THESE TERMS AND CONDITIONS CONSTITUTE A LEGAL AGREEMENT BETWEEN YOUR COMPANY/ORGANIZATION AND APPLE.

MDM Certificate Agreement
(for companies deploying mobile device management for iOS products)

Purpose
Your company, organization or educational institution would like to use the MDM Certificates (as defined below) to enable You to either deploy a third-party commercial, enterprise server software product for mobile device management of iOS products, or deploy Your own internal mobile device management for iOS products within Your company, organization or educational institution. Apple is willing to grant You a limited license to use the MDM Certificates as permitted herein on the terms and conditions set forth in this Agreement.


1. Accepting this Agreement; Definitions

1.1 Acceptance
In order to use the MDM Certificates and related services, You must first agree to this License Agreement. If You do not or cannot agree to this License Agreement, You are not permitted to use the MDM Certificates or related services. Do not download or use the MDM Certificates or any related services in that case.


☐ I have read and agree to these terms and conditions.

[Printable Version >](#)

[Decline](#) [Accept](#)



Shop the [Apple Online Store](#) (1-800-MY-APPLE), visit an [Apple Retail Store](#), or find a [reseller](#).

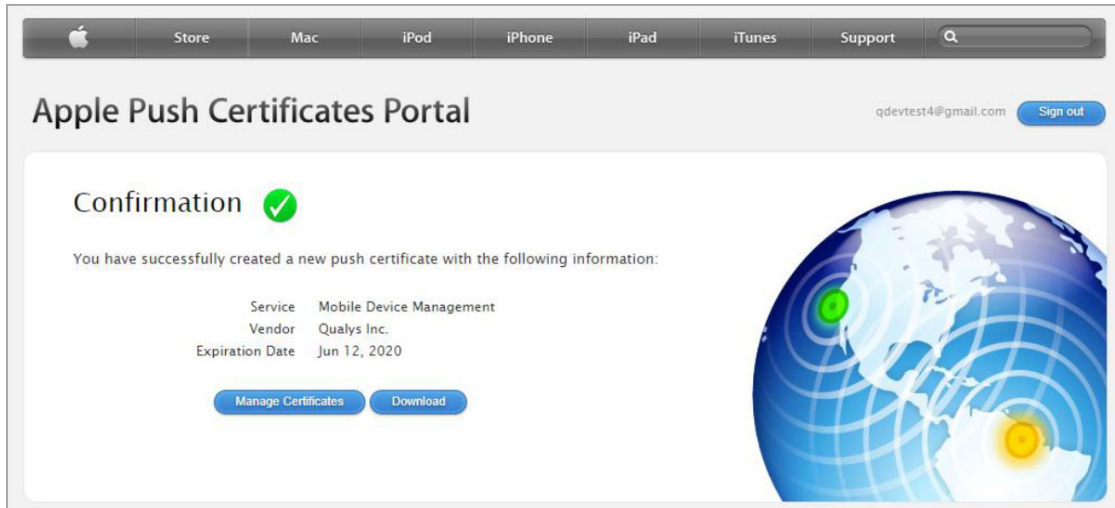
[Apple Info](#) | [Site Map](#) | [Hot News](#) | [RSS Feeds](#) | [Contact Us](#) 

Copyright © 2012 Apple Inc. All rights reserved. [Terms of Use](#) | [Privacy Policy](#)

7) Browse to the location where you saved the Qualys_CertificateSigningRequest.txt file and then upload the certificate file.



8) In the confirmation window, download the PEM file to a known location.



9) Now, go back to your Configure APNs Certificate wizard in the Qualys portal. In the **Create Certificate** tab, enter the **APNs Name** and the **Apple ID** using which, you have generated the PEM file and click **Next**.

The screenshot shows the 'Create Certificate' step (Step 2 of 3) in the Qualys Cloud Platform 'Configure APNs Certificate' wizard. The left sidebar shows the progress: 1. Download Request File, 2. Create Certificate (active), and 3. Upload Certificate. The main content area has a title 'Create Certificate' and two input fields: 'Name' and 'Apple ID'. The 'Name' field has a placeholder text 'Provide a friendly name for your certificate.' The 'Apple ID' field has a placeholder text 'Apple ID Note: It can be any Apple ID and need not be an Apple Developer Account.' Below these fields is a section titled 'Get your APNs certificate in 3 easy steps' with a list of steps: 'Sign in to the Apple Portal', 'Upload the Certificate Signing Request (CSR)', and 'Download the new certificate'. Below the list is a link 'For more information download the APNs certificate generation guide. [Learn More](#)'. To the right of this section is an Apple logo and a button 'Goto Apple Portal'. At the bottom of the wizard are three buttons: 'Cancel', 'Previous', and 'Next' (highlighted with a red border).

10) Upload the certificate file (.pem) that you downloaded from the Apple portal.

The screenshot shows the 'Upload Certificate' step (Step 3 of 3) in the Qualys Cloud Platform 'Configure APNs Certificate' wizard. The left sidebar shows the progress: 1. Download Request File, 2. Create Certificate, and 3. Upload Certificate (active). The main content area has a title 'Upload Certificate' and a subtitle 'Upload APNs certificate you downloaded from Apple push certificate portal.' Below this is a large dashed box for uploading the certificate file. Inside the box is a cloud icon and the text 'Drop file here to attach or [browse](#)'. At the bottom of the wizard are three buttons: 'Cancel', 'Previous', and 'Save'.

11) Enter the Qualys portal password and Click **Save**.

This APNs certificate is now listed in the APNs Configuration tab and you can start using it to manage your Apple devices. The validity of APNs certificate is of 365 days, so you must [Renew APNs Certificate](#) before expiring certificate.

Organization Info

This section helps you to view and edit organization summary and other settings.

Organization Information

This section helps you to configure the organization level information. Sender's address helps to send out any communication or notification from the organization.

Settings

This section helps you to configure various enrollment settings, application settings and sync settings.

Enrollment Settings

Enrollment details are required to enroll the VMDR Mobile user device including ownership of the device, asset communication mode, option to provide mobile number and device enrollment without VMDR Mobile EMM.

The screenshot shows the 'Edit Organization' interface. On the left is a sidebar with 'EDIT MODE' and two options: 'Summary' and 'Settings'. The 'Settings' option is selected. The main content area is titled 'Settings' and contains the 'Enrollment Settings' section. This section includes:

- 'Default Ownership of Assets' with a dropdown menu currently showing 'User Prompt'. Below it, notes state: 'If User Prompt is selected, User will need to choose the Assets Ownership during the enrollment process.' and 'Assets Ownership cannot be changed post enrollment of the asset.'
- 'Default Asset Communication Mode (only for android)' with two radio buttons: 'Push' (selected) and 'Poll'.
- 'Mandate Mobile Number' with two radio buttons: 'No' and 'Yes' (selected). A note below states: 'If checked, User will be required to enter the Mobile Number of the assets being enrolled.'
- A text input field labeled 'Note' with a note below it: 'This Note will be shown to user during Device Enrollment.'
- 'Enroll devices without VMDR Mobile EMM' with two checkboxes: 'All iOS Devices' and 'All Android Devices', both of which are currently unchecked.

For an Android device, you need to choose asset communication mode (Push and Poll) using radio button.

- Push: Qualys server initiates communication with the device when required.
- Poll: Device will communicate to the Qualys server after the specified regular interval. You can set polling interval in [Sync Settings](#).

If you need to enroll devices without VMDR Mobile EMM, select appropriate check-box. You can enroll all iOS devices or Android devices without VMDR Mobile EMM.

Please select the check-boxes if your organization devices are already enrolled in any EMM to enroll iOS devices or Android devices without VMDR Mobile EMM.

Application Settings

This setting allows you to set a default value for Maximum Enrollable Assets field while creating VMDR Mobile users.

Application Settings

Default Maximum Enrollable Assets

Sync Settings

These settings allow you to define various sync intervals like polling interval, asset sync interval and heartbeat interval.

Sync Settings

Recommended values are shown by default. Lowering any of these values will increase battery usage and data consumption on your assets.

Polling Interval (in Minutes) *

Note: Reducing this will increase battery usage and data consumption on asset. Minimum value should be 15 mins.

Asset Sync Interval (in Hours) *

Note: Reducing this will increase battery usage and data consumption on asset.

Heartbeat Interval (in Hours) *

Note: Reducing this will increase battery usage and data consumption on asset.

- Polling Interval (in Minutes): If the device is in poll mode, it will communicate with the server at the time interval as per configuration.

- Asset Sync Interval (in Hours): Device regularly sends the asset update information like new installed apps, change in settings, etc. to the Qualys server as per interval set here.

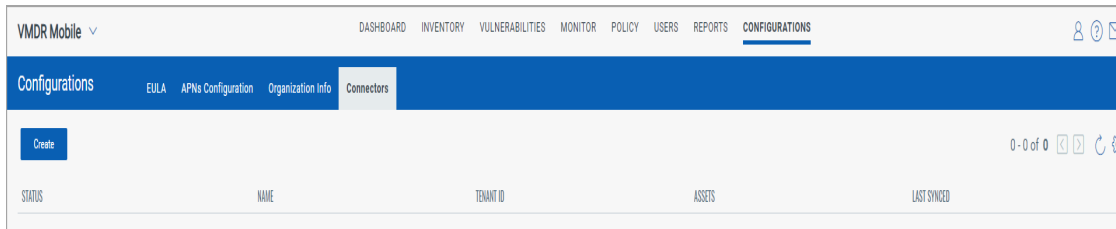
- Heartbeat Interval (in Hours): Device regularly communicates to the Qualys server notifying its status as per interval set here.

Configure Connector

Configure connector to sync the devices which are enrolled in EMM/MDM solution in VMDR Mobile. For now, you can sync only those devices that are enrolled in Intune EMM using connector.

To configure a new connector:

- 1) Navigate to **Configurations > Connectors** sub-tab and click **Create**.



- 2) Enter Name and Description in the **Basic Details** section and click **Next**.

The screenshot shows the 'Create Connector' form. On the left, a sidebar indicates the progress through three steps: 1 Basic Details (active), 2 Authentication Details, and 3 Review and Confirm. The main form area is titled 'Basic Details'. It contains a 'Name' field with a red asterisk, which has 'System' entered. Below it is a 'Description' text area, which is currently empty. A character count '250/250 characters remaining' is visible at the bottom right of the description field. At the bottom of the form, there are 'Cancel' and 'Next' buttons.

- 3) Enter Authentication Details.

Mark device as De-enrolled if the device is de-enrolled from the Intune.

Note: Polling frequency can be set to minimum of 1 hour, that means, after every one hour sync will try to fetch all the devices that are enrolled against the mentioned Tenant ID.

- 4) Click **Next**.

5) Click **Configure** to Review and Confirm the entered details.

The screenshot shows the 'Create Connector' form at the 'Review and Confirm' step. On the left, a sidebar lists the steps: 1 Basic Details, 2 Authentication Details, and 3 Review and Confirm. The main area is titled 'Review and Confirm' and contains two sections: 'Basic Details' and 'Authentication Details'. The 'Basic Details' section shows 'Name' as 'System' and 'Description' as '-'. The 'Authentication Details' section shows 'Tenant ID' as '23', a checkbox for 'Mark device as De-enrolled if devices are de-enrolled from Intune' which is checked, and 'Polling Frequency' set to '4' hours and '0' minutes. At the bottom, there are three buttons: 'Cancel', 'Previous', and 'Configure'.

You will be redirected to the Microsoft portal where all the required permissions are mentioned.

6) Click **Accept**.

The newly created connector will be listed under Connectors sub-tab.

The screenshot shows the 'Connectors' sub-tab in the 'Configurations' section. It features a 'Create' button and a table with the following columns: STATUS, NAME, TENANT ID, ASSETS, and LAST SYNCED. The table contains one row with the status 'Enabled', a Microsoft logo icon, a blurred name, a blurred tenant ID, '2' assets, and a 'Processing' status with a timestamp of 'Aug 06, 2021 3:38:21 PM IST'.

Wait for a while to allow the devices to sync with the new connector. You can also sync manually by selecting the drop-down icon next to the required connector and click **Run**.

This screenshot is similar to the previous one but includes a 'Quick Actions' dropdown menu for the connector. The menu options are 'View Details', 'Edit', 'Delete', and 'Run'. The 'Run' option is highlighted with a red box and a mouse cursor, indicating the manual sync action.

Other actions possible for the existing connectors are **View Details, Edit, Delete**.

The added devices can be searched in Inventory sub-tab.

Note: These devices are enrolled without VMDR Mobile EMM.

VMDR Mobile User Management

VMDR Mobile users are the users who enroll their devices as per email received from the Admin User. Email contains detailed steps to enroll the mobile device. To enroll the device, refer [Device Enrollment](#).

VMDR Mobile offers organizations flexible options to manage and organize VMDR Mobile user accounts. The VMDR Mobile user are the device owners and are different users from that of Portal users.

Navigate to the **Users** tab to see the list of existing users.

STATUS	USER	ASSETS	MODIFIED ON	TAGS
Inactive		2	May 02, 2022 10:45:00 AM IST	Intune
Active		11	Mar 23, 2022 5:06:55 PM IST	Intune
Active		1	Mar 17, 2022 2:24:45 PM IST	

Create VMDR Mobile User

You'll be able to create a new VMDR Mobile user with the following steps:

1) Navigate to the **Users** tab and click **Create User** from the **New** drop-down.

STATUS	USER	ASSETS	MODIFIED ON	TAGS
Inactive		2	May 02, 2022 10:45:00 AM IST	Intune
Active		11	Mar 23, 2022 5:06:55 PM IST	Intune
Active		1	Mar 17, 2022 2:24:45 PM IST	

2) On the **Create New: User** page, enter the user information in the **Personal Information** section and then click **Next**.

The screenshot shows the 'Create New: User' page in the Qualys Cloud Platform. The page has a blue header with the Qualys logo and the text 'Qualys, Cloud Platform'. Below the header is a blue bar with a back arrow and the text 'Create New: User'. The main content area is divided into a sidebar on the left and a main form area on the right. The sidebar shows 'STEPS 1/4' and a list of steps: 1. Personal Information (selected), 2. Assign Tags, 3. User Configuration, and 4. Review & Confirm. The main form area is titled 'Personal Information' and contains several input fields: 'First Name' (John), 'Middle Name' (empty), 'Last Name' (Doe), 'Username' (johndoe, with a green bar indicating 'Username available'), 'Email ID' (jdoe@qualys.com), and 'Contact Number' (empty). At the bottom of the form are 'Cancel' and 'Next' buttons.

3) On the **Create New: User** page, provide following user configurations in the **User Configuration** section.

- EULA: Configure the EULA message you want users to read and accept. For more information, refer [EULA Management](#). EULA configuration is optional. However, if EULA is configured, you need to associate it with the VMDR Mobile user, and the VMDR Mobile user must accept the EULA while enrolling their device.
- Maximum Enrollable Assets: This is the maximum number of assets that can be enrolled for this VMDR Mobile user. The default value for maximum enrollable assets is configured in [Application Settings](#).

- Status: You can create a users in the Active or Inactive state. An active user can enroll devices while inactive users won't be able to enroll the devices.

Qualys Cloud Platform

← Create New: User

STEPS 3/4

- 1 Personal Information
- 2 Assign Tags
- 3 User Configuration
- 4 Review & Confirm

User Configuration

EULA *

Maximum Enrollable Assets *

2

Status

☒ Active ☐ Inactive

Cancel Previous Next

4) Click **Add** and you'll see a user in the list.

Once user is added with valid email address, an email is sent to the user to enroll the device.

Bulk User Upload

VMDR Mobile offers organizations option to upload users in bulk. With this feature, admin can import a CSV file containing list of users in VMDR Mobile.

Importing Users

You'll be able to import users with the following steps:

1) Navigate to the **Users** tab and click **Import from CSV** from the **New** drop-down.

VMDR Mobile

DASHBOARD INVENTORY VULNERABILITIES MONITOR POLICY **USERS** REPORTS CONFIGURATIONS

Users

16 Total Users

Search for Users...

Actions (0) New

Create User

Import from CSV

STATUS	USER	ASSETS	MODIFIED ON	TAGS
Inactive		2	May 02, 2022 10:48:00 AM IST	Intune
Active		11	Mar 23, 2022 5:06:55 PM IST	Intune
Active		1	Mar 17, 2022 2:24:46 PM IST	

1 - 16 of 16

2) You can download a sample template CSV file by clicking 'Download' link from the **Import Users** page.

The screenshot shows the 'Import Users' page in the Qualys Cloud Platform. The page has a blue header with the Qualys logo and 'Cloud Platform' text. Below the header is a sidebar with 'Import Users' and a 'Start' button. The main content area is titled 'File Upload' and includes a sub-header 'You can download the User.csv file template and the system will help you to verify the user's data before uploading it into the system.' There is a 'Download Sample Template' button with a 'Learn More' link. Below this is a dashed box for file upload with a cloud icon and the text 'Drop file here to attach or browse'. At the bottom, there is a checkbox for 'Send asset enrollment details' with a description: 'Your organization is set up to send enrollment details via email. If the email ID is missing for the user, they will not be able to receive the enrollment details.'

To upload users in VMDR Mobile, make sure:

- The file you are uploading must be in CSV format (tab or comma delimited)
- The file must contain 1 row of information for each user that needs to be registered/enrolled
- The first row contains the column titles/attributes
- If mandatory fields are left blank or file contains duplicate data; you will be informed of the line numbers and data that needs to be fixed. Until all errors are cleared, data will not be saved
- Make sure that you have the latest CSV file format. Please refer to the below table in order to fill the correct information in CSV file

Fields	Mandatory / Optional	Validations
Username	Mandatory	Should be alphanumeric and '+', '@', '.', '_', '-' these five characters are allowed. Must be at least 6 characters in length and maximum 250 characters are allowed.
First_Name	Optional	Should be alphanumeric. Must be at least 2 characters in length and maximum 250 characters are allowed.
Middle_Name	Optional	Should be alphanumeric. Must be at least 2 characters in length and maximum 250 characters are allowed.
Last_Name	Optional	Should be alphanumeric. Must be at least 2 characters in length and maximum 250 characters are allowed.

Fields	Mandatory / Optional	Validations
Email_ID	Optional	Must be in standard email format. For example: yourname@yourdomain.com
Contact_Number	Optional	Should be numeric. Must be at least 4 digits in length.
EULA	Optional	If EULA is configured for your organization, then only EULA will be mandatory else optional. It should be alphanumeric and EULA name is case sensitive. It must be at least 6 characters in length. Note: EULA should exist.
Maximum Enrollable Assets	Mandatory	Should be numeric. Must be greater than zero.
Status	Mandatory	Copy and paste the status as mentioned. This field is case sensitive. Status can be Active or Inactive.
Tag	Optional	Should be alphanumeric and Tag name is case sensitive.

If your CSV file is not proper (invalid), you'll see View Errors link to see the Error List page with list of errors in the CSV file. Following is the screen for sample errors:

ROW#	FIRST NAME	MIDDLE NAME	LAST NAME	USERNAME	EMAIL ID	CONTACT NUMBER	EULA	MAX ENROLLABLE / STATUS	TAGS
1		S					testeula	200 Active	tag01,tag02
2		S					testeula	100 Inactive	tag01,tag02

3) Click **Next** after uploading a valid CSV file. Review the user list and click **Import Users** to upload users.

ROW#	FIRST NAME	MIDDLE NAME	LAST NAME	USERNAME	EMAIL ID	CONTACT NUMBER	EULA	MAX. ENROLLABLE / STA	STATUS
1	Anil	Ss	Vighne	AnilVighne...	anilvighne...	-	testeula	200	Act
2	Ankush	Ss	Vighne	Ankush777	avighne@q...	-	testeula	100	Ina

USERNAME	EMAIL ID	CONTACT NUMBER	EULA	MAX. ENROLLABLE / STATUS	TAGS
AnilVighne...	anilvighne...	-	testeula	200 Active	-
Ankush777	avighne@q...	-	testeula	100 Inactive	-

Create a new Tag

You can create a custom tag and associate the required assets to it.

To know more on how to create a tag, click [here](#).

Mobile Device Inventory

Once VMDR Mobile users enroll their mobile devices, it lists under Inventory. Refer [Device Enrollment](#) to enroll the mobile devices. This gives you in-depth visibility of all mobile devices across your enterprise, including their configuration and installed apps.

Select **Asset** to view the assets details and security posture in your inventory. You can use the various metadata filters, group by options and custom query capabilities to find what you are interested in.

The screenshot shows the 'Asset Details' page for an Android Samsung device. The left sidebar contains navigation links: INVENTORY, COMPLIANCE, SECURITY, and MANAGEMENT. The main content area is titled 'Asset Summary' and displays the following information:

- Asset Summary:** Android_samsung, Last Seen: May 11, 2022 5:00 PM IST (a month ago), Status: Enrolled.
- Identification:**
 - Mode: Active
 - Ownership: Corporate - Owned
 - IMEI: [Redacted]
 - MAC Address: 9C:99:6D:D2
 - UUID: 129A5249C49C70220807CD4379BC18846AD49EC
 - Asset ID: 14455641
 - Username: [Redacted]
 - OSF ID: 3944 7x177
 - Enrolled with VMDR Mobile EMM: Yes
 - Qualys Cloud Agent installed: Yes
 - Source: -
- Security Posture:**
 - Vulnerable: Yes
 - Encryption: No Encryption
 - Unauthorized Root Access: No
 - Passcode Present: No
 - Play Protect Enabled: Yes
- Last Location:** A world map showing the last known location. A tooltip indicates: Location unknown, Last Seen: May 11, 2022 05:00 PM.
- Tags:** Intune, SEM.

With quick actions for specific asset, you can view details for the asset, deactivate the asset or send the message.

The asset listing provides a holistic view of all assets with number of vulnerabilities for the asset. It also gives status details with number of assets such as enrolled, de-enrolled and ready for re-enrollment.

- Enrolled: Device is ready for management
- De-enrolled: Corporate data is deleted and device is being not managed
- Ready for Re-enrollment: Device is added but currently not managed

Assets are also segregated based on platforms, ownership, tags and whether it is vulnerable or not.

Click a particular asset to view the asset details.

← Asset Details: **Android_samsung**

Asset Summary

Android_samsung [Link](#)
 Last Seen: May 11, 2022 5:00:13 PM IST (a month ago)
 Status: **Enrolled**

Identification

Mode:	Active
Ownership:	Corporate - Owned
IMEI:	[REDACTED]
MAC Address:	5C:99:60:D2
UUID:	129A5249C49C70220B07CD6379BC188466049EC
Asset ID:	14455641
Username:	[REDACTED]
GSF ID:	3944 7a117f
Enrolled with VMDR Mobile EMM:	Yes
Qualys Cloud Agent Installed:	Yes
Source:	-

Security Posture

Vulnerable:	Yes
Encryption:	No Encryption
Unauthorized Root Access:	No
Passcode Present:	No
Play Protect Enabled:	Yes

Last Location

Location unknown.
Last Seen: May 11, 2022 05:00 PM

Tags

Intune SEM

It includes:

Inventory

- Asset Summary: Summary view with security posture
- System Information: Inventory information which includes specifications and hardware details
- Network Information: Network information which includes the cellular and Wi-Fi information
- Asset Settings: Displays last synced configurations for settings that may make the device vulnerable, such as developer option settings, USB debugging, etc.
- Apps: Get visibility into the list of apps installed on the device

Note: You can uninstall the user installed applications from here.

- CA Certificates: Displays list of CA certificates issued for the device
- Location: Displays device location over the period of time

Security

- Vulnerabilities: Displays vulnerabilities on the device with severity levels and status
- Security Tokens: Displays list of security tokens used in the device

Management

- Actions: Lists various actions that can be performed on the device
- For more information on actions, refer [VMDR Online Help](#).
- Logs: Displays various audit logs, sent messages and diagnostic logs

Vulnerability Assessment

It is a cloud-based service that gives you immediate, global visibility into where your IT systems might be vulnerable to the latest Internet threats and how to protect them. It helps you to continuously identify threats and monitor unexpected changes in your network before they turn into breaches.

Vulnerability Assessment in VMDR Mobile

On enrollment, the vulnerability scanning is done for each mobile device. Within a couple of minutes, the vulnerability is evaluated, and you can see the detected vulnerabilities. We have best coverage of vulnerabilities of Android and iOS, it includes:

Device vulnerabilities include vulnerable OS versions with CVEs details. We cover OS vulnerabilities from 2016 to the latest for Android and iOS, which helps you secure from the attacks, as explained above. Also detects the OS vulnerabilities exploits too.

Detection of Jailbreak/Rooted devices, Encryption disabled, Password removed/disabled.

For App vulnerabilities, we detect the CVE of the vulnerable apps like the Google Chrome app vulnerabilities shown in the above example and detects the potential harmful apps. We cover the app vulnerabilities from 2016 to the latest.

For Network vulnerabilities, we detect the devices connected to an open Wi-Fi network.

Vulnerability Assessment in VMDR Mobile gives you visibility into mobile devices that are vulnerable to threats due to outdated OS.

For Android, if the device manufacturers like Samsung, Google, LG, and Huawei has published the advisory of security updates for such devices, the QIDs are marked as Confirmed and for rest of the devices, the QIDs are marked as Potential.

Navigate to **Vulnerabilities** tab to see the list of vulnerability detections for the mobile devices.

STATUS	ASSET	MODEL	USER	LAST SEEN	TAGS	CONTROLS EVALUATED	VULNERABILITIES
Enrolled	vg33_Android_lgt_70	LS-S201		Mar 23, 20...	tag1	6 / 13	0
Enrolled	vg33_Android_motorola_182	Moto G (5S)		Mar 23, 20...		6 / 13	0
Enrolled	vg33_Android_samsung_307	SM-N920G		Mar 23, 20...		7 / 12	0
Enrolled	vg33_Android_samsung_298	SM-J730GM		Mar 23, 20...	tag1	7 / 12	0
Enrolled	vg33_Android_samsung_553	SM-T355Y		Mar 23, 20...		8 / 11	0
Enrolled	vg33_Android_lenovo_26	Lenovo K8		Mar 23, 20...		6 / 13	0
Enrolled	vg33_Android_tecno_43	TECNO 7C		Mar 23, 20...	tag1	6 / 14	0
Enrolled	vg33_Android_samsung_120	SM-A710F		Mar 23, 20...	tag1	10 / 11	0

Click a particular QID to view the vulnerability details.

The screenshot shows a web interface for vulnerability details. The title bar reads 'Vulnerability Details: Shazam For Android Code Injection Vulnerability'. On the left is a sidebar with 'VIEW MODE' and a list of tabs: 'Detection Summary' (selected), 'General Information', 'Exploitability', 'Patches', and 'Malware'. The main content area is titled 'Detection Summary' and features a red warning icon, the title 'Shazam For Android Code Injection Vulnerability', a QID of '630067' in red, and a status of 'Active'. It also shows 'Last Found on Dec 16, 2020 10:24:40 PM IST' and a 'Patch Now' button. Below this is a 'Vulnerability Result' section with a yellow background stating: 'Vulnerable app version detected. com.shazam.android 9.23.0-190311 Required Version : com.shazam.android 9.26'. On the right is an 'ABOUT ASSET' section for 'as3_Android_OnePlus', showing 'Last Seen: Dec 16, 2020 11:59:43 ...' and 'Status: Enrolled'. Below this is an 'Identification' table with fields: Mode (Active), Ownership (Corporate - Owned), IMEI (-), MAC Address (0E:C8:1C:A1:7A:2D), UDID (AA72C5A4B342D777EFDE9F877EF6F8CBF6BE6A60), Asset ID (61516), and Username (redacted). At the bottom is an 'Activity' section with fields: Last Seen (Dec 16, 2020 11:59:43 PM IST), Enrolled On (Dec 16, 2020 8:13:46 PM IST), and Modified On (-).

Vulnerability details includes:

- Detection Summary: Displays vulnerability detected
- General Information: Displays vulnerability summary with possible threats and solution
- Exploitability: Lists known exploits for this vulnerability available from third-party vendors and/or publicly available sources
- Patches: Displays available patches for this vulnerability
- Malware: Displays any published malware, where you can assess its malware family and risk






Tell me about Severity Levels

The severity level assigned to a vulnerability tells you the security risk associated with its exploitation.

Confirmed Vulnerabilities

Confirmed vulnerabilities (QIDs) are design flaws, programming errors, or mis-configurations that make your mobile device susceptible to malicious attacks. Depending on the level of the security risk, the successful exploitation of a confirmed vulnerability can vary from the disclosure of information to a complete compromise of the mobile






device. Even if the device isn't fully compromised, an exploited confirmed vulnerability could still lead to mobile device being used to launch attacks against users of the mobile device.

Severity	Level	Description
	Minimal	Basic information disclosure might enable intruders to discover other vulnerabilities, but lack of this information does not make the vulnerability harder to find.
	Medium	Intruders may be able to collect sensitive information about the mobile device, such as the precise version of software used. With this information, intruders can easily exploit known vulnerabilities specific to software versions. Other types of sensitive information might disclose a few lines of source code or hidden directories.
	Serious	Vulnerabilities at this level typically disclose security-related information that could result in misuse or an exploit. Examples include source code disclosure or transmitting authentication credentials over non-encrypted channels.
	Critical	Intruders can exploit the vulnerability to gain highly sensitive content or affect other users of the mobile device. Examples include certain types of cross-site scripting and SQL injection attacks.
	Urgent	Intruders can exploit the vulnerability to compromise the mobile device's data store, obtain information from other users' accounts, or obtain command execution on a host in the mobile device's architecture.

Potential Vulnerabilities




Potential Vulnerabilities indicate the observation of weakness or error that is commonly used to attack a mobile device, and unable to confirm if the weakness or error could be exploited. Where possible, the QID's description and results section include information and hints for following-up with manual analysis. For example, the exploitability of a QID

may be influenced by characteristics that cannot be confirmed, such as the native Android vulnerabilities which might be present on the Android manufacturer's devices for which advisory is not published.

Severity	Level	Description
	Minimal	Presence of this vulnerability is indicative of basic information disclosure and might enable intruders to discover other vulnerabilities. For example in this scenario, information such as web server type, programming language, passwords or file path references can be disclosed.
	Medium	Presence of this vulnerability is indicative of basic information disclosure and might enable intruders to discover other vulnerabilities. For example version of software or session data can be disclosed, which could be used to exploit.
	Serious	Presence of this vulnerability might give access to security-related information to intruders who are bound to misuse or exploit. Examples of what could happen if this vulnerability was exploited include bringing down the server or causing hindrance to the regular service.
	Critical	Presence of this vulnerability might give intruders the ability to gain highly sensitive content or affect other users of the mobile device.
	Urgent	Presence of this vulnerability might enable intruders to compromise the mobile device's data store, obtain information from other users' accounts, or obtain command execution on a host in the mobile device's architecture. For example in this scenario, the mobile device users can potentially be targeted if the device is exploited.

Information Gathered

Information Gathered issues (QIDs) include visible information about the mobile device's platform, OS version, model and installed security patch level.

Severity	Level	Description
	Minimal	Intruders may be able to retrieve sensitive information related to the mobile device.
	Medium	Intruders may be able to retrieve sensitive information related to internal functionality or business logic of the mobile device.
	Serious	Intruders may be able to detect highly sensitive data, such as personally identifiable information (PII) about other users of the mobile device.

Tell me about vulnerability status

You'll see the status of the detected vulnerabilities under the **Inventory > Vulnerabilities** tab. We continuously update the status of detected vulnerabilities based on the mobile asset data synced as per the asset sync interval.

Each vulnerability instance is assigned a status - New, Active, Fixed or Reopened.

New - The first time a vulnerability is detected by a scan the status is set to New.

Active - A vulnerability detected by two or more scans is set to Active.

Fixed - A vulnerability was verified by the most recent scan as fixed, and this vulnerability was detected by the previous scan.

Reopened - A vulnerability was reopened by the most recent scan, and this vulnerability was verified as fixed by the previous scan. The next time the vulnerability is detected by a scan, the status is set to Active.

Patch Orchestration

For the Android public app (Google Play Store) vulnerabilities, you can patch them using Patch Now option. '**Patch Now**' button will be enabled for the patchable vulnerabilities. This option updates the app to the latest version.

Click **Patch Now** to update the particular app.

QID	TITLE	SEVERITY	RELEASED ON	LAST DETECTED	ASSET	PATCH
610059	Google Android Devices August 2019 Security ... Active	■■■■■	Aug 01, 2019	Jan 06, 2022 6:56:13 PM IST	PiyushSonawane_Android... Enrolled	Patch Now
610143	Google Android Devices September 2018 Secu... Active	■■■■■	Sep 01, 2018	Jan 06, 2022 6:56:13 PM IST	PiyushSonawane_Android... Enrolled	Patch Now
610052	Google Android Devices January 2019 Security... Active	■■■■■	Jan 01, 2019	Jan 06, 2022 6:56:13 PM IST	PiyushSonawane_Android... Enrolled	Patch Now
610055	Google Android Devices April 2019 Security Pa... Active	■■■■■	Apr 01, 2019	Jan 06, 2022 6:56:13 PM IST	PiyushSonawane_Android... Enrolled	Patch Now
610061	Google Android Devices October 2019 Security...	■■■■■	Oct 01, 2019	Jan 06, 2022	PiyushSonawane_Android...	Patch Now

This opens the **Deployment Job** wizard.

← Create New: **Deployment Job**

STEPS 1/6

- 1 Basic Information
- 2 QIDs
- 3 Select Assets
- 4 Schedule
- 5 Options
- 6 Review and Confirm

Basic Information

Create this deployment job by selecting assets and patches to be installed. Also, define the deployment schedule and configure message options you want to display as reminders.

Name *

Provide the name for the deployment job and click **Next**.

← Create New: Deployment Job

STEPS 2/6

- 1 Basic Information
- 2 QIDs
- 3 Select Assets
- 4 Schedule
- 5 Options
- 6 Review and Confirm

QIDs

Patchable QIDs for this job

Selected QIDs (1)

QID	TITLE	CVE IDS	SEVERITY
630147	Firefox For Android Improper Restriction of Rendered UI Vulnerability	CVE-2020-6827 CVE-2020-6828	■■■■■

Associated QIDs (11)

QID	TITLE	CVE IDS	SEVERITY
630355	Firefox For Android Incorrect Authorization Vulnerability	CVE-2018-12391	■■■■■
630356	Firefox For Android Exposure of Sensitive Information Vulnerability	CVE-2018-12400	■■■■■
630301	Firefox For Android Permission Issues Vulnerability	CVE-2016-9061	■■■■■
630049	Mozilla Firefox For Android Out of Bounds Memory Write Vulnerability	CVE-2018-5146 CVE-2018-5147	■■■■■
630390	Mozilla Firefox For Android Improper Input Validation Vulnerability	CVE-2018-12382	■■■■■
630003	Mozilla Firefox For Android Remote Code Execution Vulnerability	CVE-2016-5267	■■■■■
630007	Mozilla Firefox For Android Remote Code Execution Vulnerability	CVE-2016-1780 CVE-2016-2810 1 more...	■■■■■
630010	Mozilla Firefox For Android MITM Vulnerability	CVE-2016-1948	■■■■■
630011	Mozilla Firefox For Android Remote Code Execution Vulnerability	CVE-2016-1940 CVE-2016-1943	■■■■■

This shows selected QIDs and associated QIDs. Click **Next**.

Qualys Express

← Create New: Deployment Job


STEPS 3/6

- 1 Basic Information
- 2 QIDs
- 3 Select Assets
- 4 Schedule
- 5 Options
- 6 Review and Confirm

Select Assets

Select assets to deploy patch

Include the following assets

☒ **as3_Android_One...**  ONEPLUS A6010 **jjoequays** Dec 16, 2020

1 - 1 of 1

Cancel Add

Cancel Previous Next

Click **Select Assets** and select the assets on which you need to apply patches.

Click **Add** to add the selected assets and then click **Next**.

Create New: Deployment Job

STEPS 4/6

- 1 Basic Information
- 2 QIDs
- 3 Select Assets
- 4 **Schedule**
- 5 Options
- 6 Review and Confirm

Schedule deployment

Schedule the deployment job to run on the demand or as per schedule.

On Demand: this assessment will run once enabled

START DATE

START TIME

TIMEZONE
 By default the system will use the server timezone. [Set timezone](#)

Click **On Demand** to run the job and click **Schedule** to schedule the deployment job in future. Click **Next**.

Create New: Deployment Job

STEPS 5/6

- 1 Basic Information
- 2 QIDs
- 3 Select Assets
- 4 Schedule
- 5 **Options**
- 6 Review and Confirm

Deployment Communication Options

Configure communication messages and it's frequency for patch deployment. For default configurations, refer [Online Help](#).

Deployment Messages

Configure Deferment for Deployment

Configure display messages, and it's frequency for deferment.

Configure Enforcement for Deployment

Configure display messages, and it's frequency for enforcement.

TITLE *

MESSAGE *

193/255 characters remaining

Start Enforcement In *

If you enable the **Configure Enforcement for Deployment** option, you need to configure title, message, and time to enforce deployment.

If you don't configure enforcement, default title and message will be displayed. The default enforcement starts in 5 minutes.

← Create New: **Deployment Job**

STEPS 5/6

- 1 Basic Information
- 2 QIDs
- 3 Select Assets
- 4 Schedule
- 5 **Options**
- 6 Review and Confirm

Deployment Communication Options

Configure communication messages and it's frequency for patch deployment. For default configurations, [refer Online Help](#).

Deployment Messages

Configure Deferment for Deployment ON

Configure display messages, and it's frequency for deferment.

TITLE *

35 Character Limit

MESSAGE *

255 Character Limit

255/255 characters remaining

DEFERMENT *

Remind in Hours **Number of Deferments *** times

Configure Enforcement for Deployment ON

Configure display messages, and it's frequency for enforcement.

Deployment communication options are optional to configure. If you enable Configure Deferment for Deployment option, you need to configure title, message, deferment and number of deferment.

If you don't configure deferment, default title and message will be displayed. The default deferment will be reminded after every 1 hour and for maximum 8 times before enforcement.

If you don't configure both deferment and enforcement, default deferment with the default title and message is displayed. The default deferment is reminded after every 1 hour and for maximum of 8 times before enforcement.

After default deferment, default enforcement will be applied.

Click **Next** to review your selection. Click **Save** to complete deployment job.

You can check the status of the deployment job on **Jobs** tab.

Vulnerabilities

Vulnerabilities

Jobs

39

Total Jobs

Job

Search...

Create Job

1 - 39 of 39

									RESULT		
STATUS		NAME	CREATED BY	SCHEDULE	QID	ASSETS	PENDING	SUCCESS	SKIPPED		
Completed	35	Completed	pixel_Job	Update Application Job	Dec 09, 2021 9:24:20 PM IST	On-demand	630451	0	0	0	0
Enabled	2										
Disabled	2										
SCHEDULED											
On-demand	29	Completed	test1234	Update Application Job	Aug 19, 2021 3:29:57 PM IST	On-demand	630067	1	0	1	0
Once	10										
		Disabled	test1111	Update Application Job	Jul 07, 2021	On-demand	630053	5	0	0	0

Job status shows various status for deployment jobs.

Policy Compliance

You can perform configuration evaluation against best practices for the Android and iOS platforms. Currently, most of the configuration details are collected in VMDR Mobile. However, you have to go to individual assets and verify the status of that particular configuration.

The configuration assessment shows the assets and their misconfigurations which helps you to take action on such devices. It also ensures that the assets do not undergo any attack or vulnerability due to misconfigurations.

This feature is available in the VMDR Mobile Device bundle.

Creating Policies

You can create customized policies for Android and iOS platform for required controls and associate them with assets to evaluate them later.

To know more on how to create a policy, click [here](#).

Viewing Policies

Qualys VMDR Mobile provides some default out-of-the-box policies for Android and iOS platform. Every policy has one or more controls assigned to it. Controls define what evaluation should be performed on an asset. Based on the evaluations performed on the assets, the pass or fail status for the assets are displayed.

These policies are associated with every asset that is enrolled in VMDR Mobile. Based on the platform selected (iOS or Android), these policies are automatically evaluated with every asset enrollment. Once a policy is enabled for an asset, you can view the compliance posture in the **Monitor** tab.

Supported policies are:

- iOS Best Practices
- Android Best Practices

Navigate to the **Policy** tab to view all the policies supported by Qualys VMDR Mobile.

Click on the policy to open it in the view mode.

← Policy Details: iOS Best Practices

VIEW MODE

Policy Information

Controls

Assets

Policy Information

iOS Best Practices

Created By: System

Basic Details

Policy Name

iOS Best Practices

Platform

iOS

Status

Active

Description

The controls within the policy are configured on the basis of values provided by CIS benchmark.

Modified By

Username

System

Modified On

Oct 28, 2021 1:11:23 PM IST

Created By

Username

System

Created On

May 07, 2021 11:08:00 AM IST

Monitoring Controls

Every policy has one or more controls assigned to it. Controls define what evaluation should be performed on an asset. The controls are validated by evaluating the assets and then the pass or fail status of the assets are displayed. VMDR Mobile supports system-defined controls. The **Controls** tab lists all controls and their details such as control name, platform, criticality of the control and so on.

Policy					
Policy		Controls			
24 Total Controls		Search for Controls...			
1 - 24 of 24					
CID	CONTROL NAME	PLATFORM	CREATED BY	MODIFIED BY	CRITICALITY
20287	Status of the USB Support Associated Policy: 1 System Defined	Android	System Jan 11, 2021 5:30:00 AM IST	System Jan 03, 2022 5:30:00 AM IST	Urgent
20286	Status of the Auto Sync Data Associated Policy: 1 System Defined	Android	System Jan 11, 2021 5:30:00 AM IST	System Jan 03, 2022 5:30:00 AM IST	Serious
20278	Status of the 'Use Location' setting Associated Policy: 1 System Defined	Android	System Jan 11, 2021 5:30:00 AM IST	System Dec 27, 2021 5:30:00 AM IST	Urgent
20284	Ensure the 'Mock Location' is set to 'Off' Associated Policy: 1 System Defined	Android	System Jan 11, 2021 5:30:00 AM IST	System Dec 24, 2021 5:30:00 AM IST	Critical
20283	Ensure 'Wi-Fi Sharing' is set to 'Disabled' Associated Policy: 1 System Defined	Android	System Jan 11, 2021 5:30:00 AM IST	System Dec 14, 2021 5:30:00 AM IST	Critical

Click on any control to view details specific to that control.

Control Details: Status of the USB Support

Summary

Status of the USB Support
Criticality: ■ Urgent

Identification	Platform	Type	Associated Policies
ID 20287 Created On Jan 11, 2021 9:30:00 AM IST	Android	System Generated	1

Specification
Status of the USB Support

Expected Criteria
This setting indicates the value of the USBSupport attribute present on the mobile device.

USB Support	Supported Version
Enabled	2+

Rationale
USB Support enables the transfer of data and software from one device to another. This software can include malware. When USB mass storage is enabled on a mobile device, it becomes a potential vector for malware and unauthorized data exfiltration. Prohibiting USB mass storage mode mitigates this risk. It is recommended to disable the USB support if not required.

Reference
-

Monitor the Assets

In the **Monitor** tab, you can monitor your compliance posture in real time for each asset. View details such as asset, model, evaluation status at a quick glance.

Once the asset is on-boarded, then based on the platform the best practices policies are assigned automatically to the assets and the assets are evaluated. After the evaluation, you can view the overall evaluation result in the **Monitor** tab.

The controls are validated and the pass or fail status is displayed in the **Controls** sub-tab.

From the **Controls** sub-tab, you can drill down to view details of each control and their pass or fail status. Click on the **CID** to view further specifications of the control. A CID is a unique ID assigned by Qualys to each control.

Use **Group By** drop-down menu to view results for specific selection.

VMDR Mobile | DASHBOARD | INVENTORY | VULNERABILITIES | **MONITOR** | POLICY | USERS | REPORTS | CONFIGURATIONS

Monitor

Asset | Search...

40.5K Total Evaluations

21.9K Total Failed Evaluations | 0 Controls Failed with High ... | 6 Controls Failed (Last 15 Days) | 0 Controls Reopened (Last 15 Days)

PLATFORM: Android 40.5K, iOS 11

POLICY: Android Best Pra... 19.9K, IncludeT1andExc... 4.12K, IncludeT1Exclud... 4.12K, IncludeT1T2Excl... 2.07K, IncludeT1Exclud... 2.07K, 8 more

CONTROL RESULT: Failed 21.9K, Passed 18.6K

Actions (0) | Asset | Controls | **Group By** | 1 - 50 of 40541

RESULT	CID	CONTROL NAME	ASSET	FORM	EVALUATED	ASSET	CRITICALITY
Passed	20278	Status of the U...	Control	Android	Last: Mar 17, 2022 First: Mar 17, 2022	vg33_Android_xiaomi_13	Urgent
Passed	20284	Ensure the Moc...	Operating System	Android	Last: Mar 17, 2022 First: Mar 17, 2022	vg33_Android_xiaomi_33	Critical
Failed	20278	Status of the U...	Result	Android	Last: Mar 17, 2022 First: Mar 17, 2022	vg33_Android_xiaomi_33	Urgent
Passed	20282	Ensure the Blueoo...	Policy: Android Best Pr...	Android	Last: Mar 17, 2022 First: Mar 17, 2022	vg33_Android_huawei_12	Critical
Failed	20281	Ensure USB Debug...	Policy: Android Best Pr...	Android	Last: Mar 17, 2022 First: Mar 17, 2022	vg33_Android_huawei_12	Urgent

Re-evaluation of Controls

You can re-evaluate a control by selecting the **Quick Actions** menu next to the control name and click **Re-evaluate**.

Monitor

Asset | Search...

202 Total Evaluations

75 Total Failed Evaluations | 0 Controls Failed with High Criticality | 47 Controls Failed (Last 15 Days) | 2 Controls Reopened (Last 15 Days)

Actions (1) | Asset | Controls | Group By | 1 - 50 of 202

RESULT	CID	CONTROL NAME	PLATFORM	EVALUATED	ASSET	CRITICALITY
Passed	20270	Ensure device firmware is up to date	Android	Last: Jan 09, 2022 First: Jan 03, 2022	PiyushSonawane_Androi...	Urgent
Passed	20279	Ensure the mobile device is encrypted	Android	Last: Jan 09, 2022 First: Jan 03, 2022	PiyushSonawane_Androi...	Critical
Passed	20273	Ensure the device is not rooted	Android	Last: Jan 09, 2022 First: Jan 03, 2022	PiyushSonawane_Androi...	Urgent
Passed	20270	Ensure device firmware is up to date	Android	Last: Jan 07, 2022 First: Jan 04, 2022	Jim_Android_Xiaomi	Urgent
Failed	18936	Status of the	Android	Last: Jan 07, 2022 First: Jan 04, 2022	Jim_Android_Xiaomi	Urgent
Failed	20451	Ensure 'Scre...	Android	Last: Jan 07, 2022 First: Jan 04, 2022	Jim_Android_Xiaomi	Critical
Passed	20287	Status of the	Android	Last: Jan 07, 2022 First: Jan 04, 2022	Jim_Android_Xiaomi	Urgent

After the re-evaluation is done, the control's status is updated across the application.

Click the **Details** link (below the Result status) to view the control evaluation details for an asset.

Monitor

203

Total Evaluations

PLATFORM

Android 171

iOS 32

POLICY

Android Best Pra... 171

iOS Best Practices 32

CONTROL RESULT

Passed 129

Failed 74

CRITICALITY

Critical 97

Urgent 88

Medium 9

Serious 9

Asset

Search...

74

Total Failed Evaluations

0

Controls Failed with High Criticality

37

Controls Failed

Last 15 Days

2

Controls Reopened

Last 15 Days

Actions (0)

Asset

Controls

Group By:

1 - 50 of 203

RESULT	CID	CONTROL NAME	PLATFORM	EVALUATED	ASSET	CRITICALITY
<div>Passed</div> <div>Details</div>	20282	Ensure the Bluetooth is set to 'Disabled' Policy: Android Best Practices	<div></div> Android	Last: Jan 12, 2022 First: Jan 04, 2022	Jim_Android_Xiaomi Corporate - Owned	<div></div> Critical
<div>Failed</div> <div>Details</div>	20285	Status of the Screen Reader setting Policy: Android Best Practices	<div></div> Android	Last: Jan 12, 2022 First: Jan 04, 2022	Jim_Android_Xiaomi Corporate - Owned	<div></div> Medium
<div>Passed</div> <div>Details</div>	20284	Ensure the 'Mock Location' is set to 'Di... Policy: Android Best Practices	<div></div> Android	Last: Jan 12, 2022 First: Jan 04, 2022	Jim_Android_Xiaomi Corporate - Owned	<div></div> Critical
<div>Failed</div> <div>Details</div>	20281	Ensure 'USB Debugging' is set to 'Disab... Policy: Android Best Practices	<div></div> Android	Last: Jan 12, 2022 First: Jan 04, 2022	Jim_Android_Xiaomi Corporate - Owned	<div></div> Urgent
<div>Passed</div> <div>Details</div>	20279	Ensure the mobile device is encrypted Policy: Android Best Practices	<div></div> Android	Last: Jan 12, 2022 First: Jan 04, 2022	Jim_Android_Xiaomi Corporate - Owned	<div></div> Critical
<div>Passed</div> <div>Details</div>	20278	Status of the 'Use Location' setting Policy: Android Best Practices	<div></div> Android	Last: Jan 12, 2022 First: Jan 04, 2022	Jim_Android_Xiaomi Corporate - Owned	<div></div> Urgent

Dashboards and Reports

This section helps you to monitor and analyze various dashboards and reports for the mobile assets. Once device enrollment is complete, you can configure various dashboards to view mobile assets data and their details.

Customizable Dynamic Dashboard

Dashboard gives you a quick one-page summary of your overall security posture, based on the most recent vulnerability scan results for your mobile assets.

This section helps you monitor and analyze various dashboards and reports for the mobile assets. Once device enrollment is complete, you can configure various dashboards to view mobile assets data and their details.

Qualys VMDR Mobile integrates with Unified Dashboard (UD) to bring information from all Qualys applications into a single place for visualization. UD provides a powerful, new dashboarding framework along with platform service that will be consumed and used by all other products to enhance the existing dashboard capabilities.

Qualys VMDR Mobile offers several dashboards out-of-the-box. Each dashboard displays a short description of the information it offers. You can also easily configure widgets to pull information from other modules/applications and add them to your dashboard. You can also add as many dashboards as you like to customize your view.

See the [Unified Dashboard help](#) for more information.

Global Dashboard Permissions

Your access to Unified Dashboard depends on the global permissions granted to you from the Admin utility. Refer to the [Online Help](#) in the Admin utility for information on Global Dashboard Permissions.

Note: When you assign the Global Dashboard permissions to a role, the Global Dashboard permissions override the module-specific dashboard permissions. As a result, the module-specific dashboard permissions are ignored.

You can create new dashboard, edit or delete existing dashboards. You can include various widgets to your dashboard.

Reports

This section helps you to view Audit Log reports. Audit log report is the logs of the actions performed on the VMDR Mobile portal. Go to the **Reports** tab.

VMDR Mobile

DASHBOARDINVENTORYVULNERABILITIESMONITORPOLICYUSERSREPORTSCONFIGURATIONS

Reports

Audit Log

4
Total Logs

PORTAL USED
Enrollment Portal3
Web Portal1

Search for Logs...

Last 7 Days

1 - 4 of 4

ENTITY	OPERATION	PORTAL USED	PERFORMED ON	USER
Devices	Enrollment - [redacted]_Android_samsung	Enrollment Portal IP: [redacted]	Apr 28, 2022 10:35:56 AM IST	[redacted]
Devices	Add - [redacted]_Android_samsung	Enrollment Portal IP: [redacted]	Apr 28, 2022 10:35:29 AM IST	[redacted]
Devices	Add - [redacted]_Android_samsung	Enrollment Portal IP: [redacted]	Apr 28, 2022 10:30:29 AM IST	[redacted]
Devices	Delete - [redacted]_Android_OPPO	Web Portal IP: [redacted]	Apr 28, 2022 10:25:39 AM IST	[redacted]

You can analyze various audit logs in audit log reports related to device enrollment and user configurations.

Appendix

Renew APNs Certificate

The validity of APNs certificate is of 365 days, so the administrator must renew the certificate after every 365 days. The Qualys VMDR Mobile Portal notifies the administrator when the certificate is expiring via email. The administrator must renew this certificate before the certificate expires. If the certificate expires, the administrator might be unable to manage the Apple devices in their organization, which might result in the administrator having to manually de-enroll and then re-enroll all Apple devices in the system again.

Steps to renew APNs certificate:

- 1) Navigate to **Configurations > APNs Configuration** and click **Renew**.

The screenshot shows the 'Configurations' section of the Qualys VMDR Mobile Portal, specifically the 'APNs Configuration' tab. The page displays a table of APNs with columns for Status, Details, Apple ID, Devices, Uploaded, and Valid Till. A 'Renew' button is highlighted in the 'Quick Actions' dropdown for the 'Expired' APN.

STATUS	DETAILS	APPLE ID	DEVICES	UPLOADED	VALID TILL
Active	Test26m UID: [redacted] Serial #: [redacted]	[redacted]@gmail.com	14	May 26, 2021 3:16:45 PM IST	May 26, 2023 3:07:45 PM IST
Expiring	qdevtest1 UID: [redacted] Serial #: [redacted]	[redacted]t@gmail.com	0	May 04, 2021 12:10:07 PM IST	May 04, 2022 12:01:40 PM IST Expiring in 4 days
Expired	Test02 UID: [redacted] Serial #: [redacted]	[redacted]@gmail.com	0	Feb 12, 2021 3:07:32 PM IST	Feb 28, 2021 2:58:33 PM IST Expired 425 days ago

The 'Expired' row shows a 'Quick Actions' dropdown menu with 'Renew' and 'Delete' options. The 'Renew' option is highlighted with a red box.

2) Download Certificate Signing Request file (CSR) and click **Next**. You may skip this step if you have already downloaded the CSR.

The screenshot shows the 'Renew APNs Certificate' wizard in the Qualys Cloud Platform. The left sidebar indicates 'STEPS 1/3' with '1 Download Request File' selected. The main content area is titled 'Download Request File' and explains that a Certificate Signing Request (CSR) is needed. It includes a 'Certificate Signing Request' section with a download icon and a 'Download CSR' button. At the bottom, there are 'Cancel' and 'Next' buttons.

← Renew APNs Certificate

STEPS 1/3


1 Download Request File

2 Create Certificate

3 Upload Certificate

Download Request File

You need to first generate a Certificate Signing Request (CSR) and download it. This CSR is in the process of creating the APNs Certificate from Apple Push Certificate portal.



Certificate Signing Request

We use your organization's APNs certificate to send notifications to your iOS devices when information is requested from the device at intervals or on demand.

If you do not already have a CSR file from VMDR Mobile, please download it here. You will need this CSR to download an APNs certificate from Apple portal.

[Download CSR](#)

[Cancel](#) [Next](#)

3) Click **Goto Apple Portal** link to go to Apple Push Certificate Portal (<https://identity.apple.com/pushcert/>)

The screenshot shows the 'Renew APNs Certificate' wizard in the Qualys Cloud Platform. The left sidebar indicates 'STEPS 2/3' with '2 Create Certificate' selected. The main content area is titled 'Create Certificate' and contains form fields for 'Name' (with value 'Test26m') and 'Apple ID'. A note states that the Apple ID can be any Apple ID, not necessarily a Developer Account. At the bottom, there is a section 'Get your APNs certificate in 3 easy steps' with a list of steps and a 'Goto Apple Portal' link.

Qualys Cloud Platform

← Renew APNs Certificate

STEPS 2/3

1 Download Request File

2 Create Certificate

3 Upload Certificate

Create Certificate

Name

Test26m

Provide a friendly name for your certificate.


Apple ID

Apple ID Note: It can be any Apple ID and need not be an Apple Developer Account.

Get your APNs certificate in 3 easy steps

- Sign in to the Apple Portal
- Renew the currently uploaded certificate. For renewal upload the certificate signing request
- Download the renewed certificate

For more information download the APNs certificate generation guide. [Learn More](#)

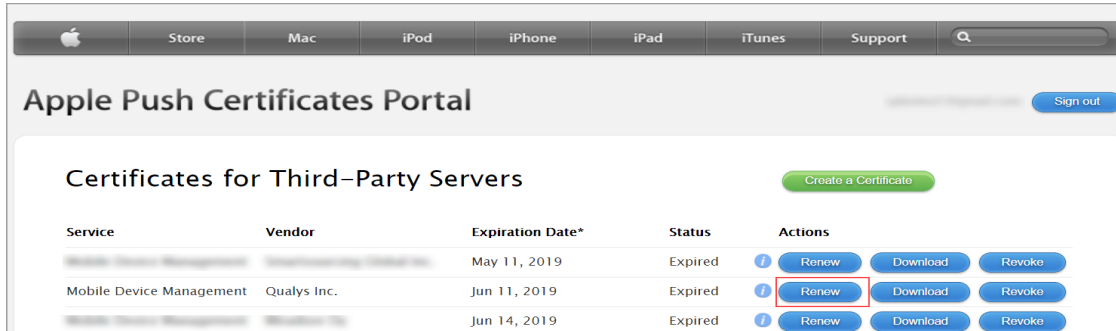


[Goto Apple Portal](#)

4) Login to Apple Push Certificate Portal using the same Apple ID and password that you used to originally create the APNs certificate. Locate the APNs certificate that you want to use, and then click **Renew**.

Note: If multiple certificates are listed, please ensure that you have selected the correct APNs certificate that you would like to renew.

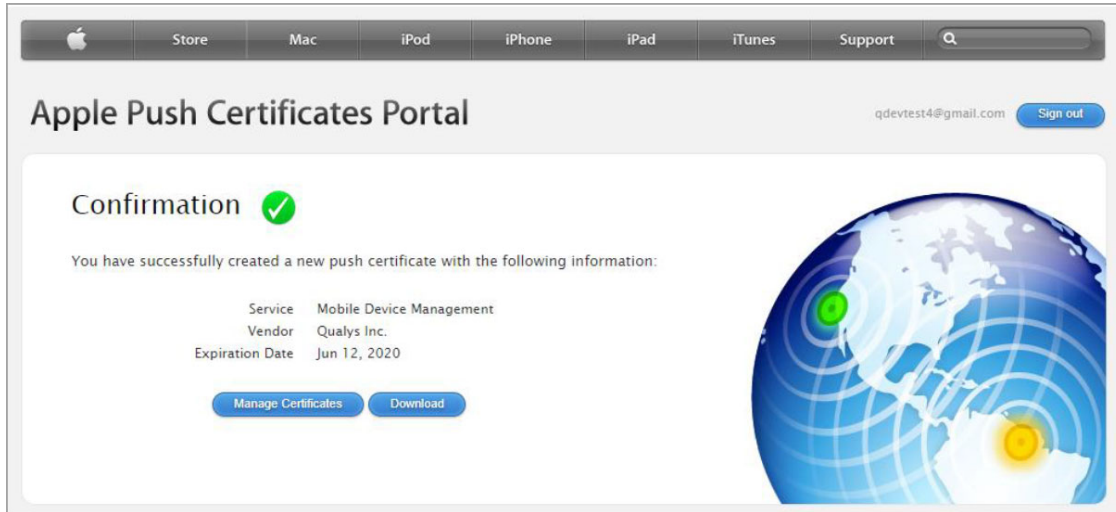
You may compare the Serial # or expiration date for the APNs certificate that you selected to confirm that you are using the right certificate or compare the UID of the certificate.



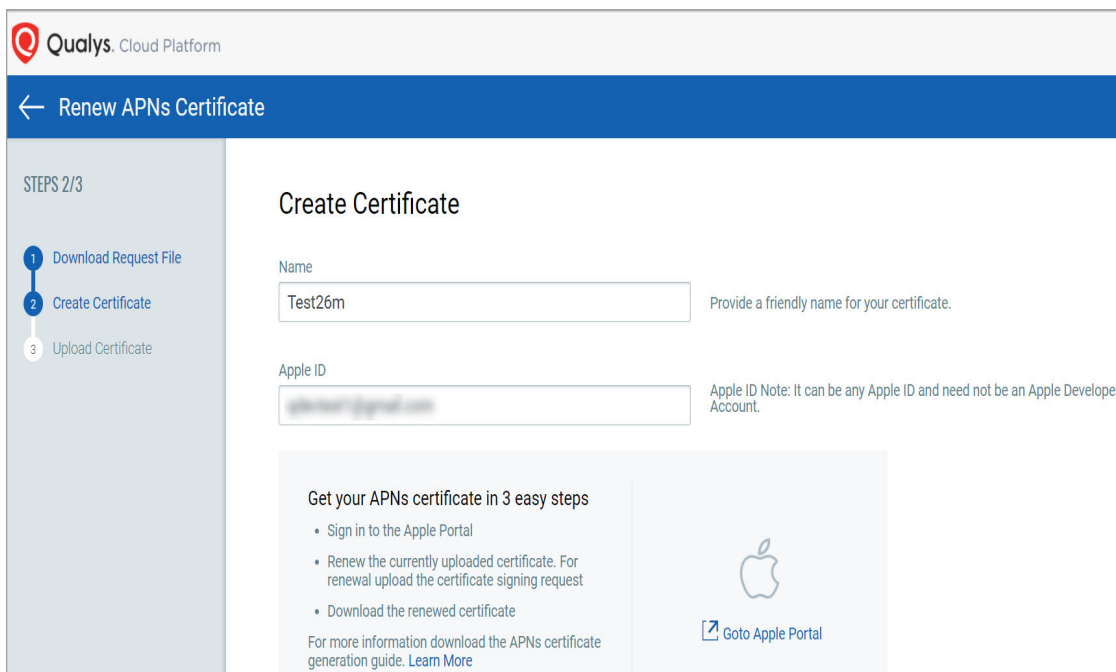
5) Browse to locate the certificate file and then click **Upload**.



6) In the confirmation window, download the PEM file to a known location.



7) Now, go back to your Renew APNs Certificate wizard in the Qualys portal. In the Create Certificate tab, existing APNs Name and the Apple ID will be shown.



8) Upload the certificate file (.pem) that you downloaded from the Apple portal.

The screenshot shows the Qualys Cloud Platform interface for renewing an APNs certificate. The page title is 'Renew APNs Certificate'. On the left, a sidebar indicates the current step is '3/3' and lists the steps: '1 Download Request File', '2 Create Certificate', and '3 Upload Certificate'. The main content area is titled 'Upload Certificate' and includes the instruction: 'Upload APNs certificate you downloaded from Apple push certificate portal.' Below this, a dashed box contains the text 'Upload the certificate file (.pem) that you downloaded from the Apple Portal' and a cloud icon with the text 'Drop file here to attach or browse'. A file named 'MDM_Qualys Inc._Certificate.pem' is shown as uploaded, with a timestamp of '16/Jun/2021 4:42 PM' and a size of '2 KB'. At the bottom, there are three buttons: 'Cancel', 'Previous', and 'Save'.

9) Enter the Qualys Portal password and Click **Save**. This APNs certificate is now listed in the APNs Configuration tab and you can continue managing your Apple devices using this certificate.