# 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

*Verity Confidential*
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 smartphones 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**

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

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

5) Log in using corporate Apple ID and password. Click **Create a Certificate**.
6) Select I have read and agree to these terms and conditions check box, and then click Accept.
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**.

![Configure APNs Certificate](image)

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

![Configure APNs Certificate](image)

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](image) 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.

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.

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

- 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.

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.

![Configure Connector](image1.png)

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.

![Connectors Sub-tab](image2.png)

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**.

![Run Option](image3.png)
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.

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

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.

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

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

<table>
<thead>
<tr>
<th>Fields</th>
<th>Mandatory / Optional</th>
<th>Validations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>Mandatory</td>
<td>Should be alphanumeric and ‘+’, ‘@’, ‘.’, ‘_’, ‘-’ these five characters are allowed. Must be at least 6 characters in length and maximum 250 characters are allowed.</td>
</tr>
<tr>
<td>First_Name</td>
<td>Optional</td>
<td>Should be alphanumeric. Must be at least 2 characters in length and maximum 250 characters are allowed.</td>
</tr>
<tr>
<td>Middle_Name</td>
<td>Optional</td>
<td>Should be alphanumeric. Must be at least 2 characters in length and maximum 250 characters are allowed.</td>
</tr>
<tr>
<td>Last_Name</td>
<td>Optional</td>
<td>Should be alphanumeric. Must be at least 2 characters in length and maximum 250 characters are allowed.</td>
</tr>
</tbody>
</table>
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:

<table>
<thead>
<tr>
<th>Fields</th>
<th>Mandatory / Optional</th>
<th>Validations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email_ID</td>
<td>Optional</td>
<td>Must be in standard email format. For example: <a href="mailto:yourname@yourdomain.com">yourname@yourdomain.com</a></td>
</tr>
<tr>
<td>Contact_Number</td>
<td>Optional</td>
<td>Should be numeric. Must be at least 4 digits in length.</td>
</tr>
<tr>
<td>EULA</td>
<td>Optional</td>
<td>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.</td>
</tr>
<tr>
<td>Maximum Enrollable Assets</td>
<td>Mandatory</td>
<td>Should be numeric. Must be greater than zero.</td>
</tr>
<tr>
<td>Status</td>
<td>Mandatory</td>
<td>Copy and paste the status as mentioned. This field is case sensitive. Status can be Active or Inactive.</td>
</tr>
<tr>
<td>Tag</td>
<td>Optional</td>
<td>Should be alphanumeric and Tag name is case sensitive.</td>
</tr>
</tbody>
</table>
3) Click **Next** after uploading a valid CSV file. Review the user list and click **Import Users** to upload users.

**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.

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.

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 apps 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.
Click a particular QID to view the vulnerability details.

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 misconfigurations 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.

### 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.

<table>
<thead>
<tr>
<th>Severity</th>
<th>Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minimal</td>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>Medium</td>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>Serious</td>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>Critical</td>
<td></td>
<td>Presence of this vulnerability might give intruders the ability to gain highly sensitive content or affect other users of the mobile device.</td>
</tr>
<tr>
<td>Urgent</td>
<td></td>
<td>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.</td>
</tr>
</tbody>
</table>

Information Gathered

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

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

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. The '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.

This opens the Deployment Job wizard.
Provide the name for the deployment job and click **Next**.

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

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

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.

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.

Job status shows various status for deployment jobs.
Patch Orchestration
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.

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

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.

**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**.

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.
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.

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


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.

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.