# Table of Contents

About this guide ............................................................................................... 4  
About Qualys ....................................................................................................... 4  
Qualys Support .................................................................................................... 4  

Get Started ........................................................................................................ 5  

Configurations .................................................................................................. 6  
EULA Management .............................................................................................. 6  
APNs Certificates ............................................................................................... 7  
    What is an APNs Certificate? ............................................................................. 7  
    Pre-requisites to Generate the Certificate ......................................................... 7  
    Steps to Generate APNs Certificate ................................................................. 7  
Organization Info ............................................................................................... 13  
    Organization Information .................................................................................. 13  
    Settings ............................................................................................................ 13  

SEM User Management ..................................................................................... 15  
Creating a New SEM User .................................................................................. 15  

Mobile Device Inventory .................................................................................. 18  

Vulnerability Management ................................................................................. 21  
    Vulnerability Management in SEM ................................................................. 21  

Patch Management ........................................................................................... 26  

Dashboards and Reports ................................................................................... 31  
    Dashboards ...................................................................................................... 31  
    Reports ............................................................................................................ 33  

Appendix ............................................................................................................ 35  
Renew APNs Certificate .................................................................................... 35
About this guide

This user guide helps to get started with and use Secure Enterprise Mobility (SEM) 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 Secure Enterprise Mobility (SEM) User Guide. Qualys SEM offers you a cloud-based solution, to help you secure, monitor, and manage mobile devices (including smart phones and tablets) across your enterprise.

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 SEM users, and monitor various dashboards and reports.

**SEM User** - SEM Users are the holders of the mobile devices.

With SEM, you can:
- Manage enrolled mobile devices centrally
- Manage vulnerabilities and configuration assessment on enrolled mobile devices
- Fix the detected vulnerabilities
- Secure data on enrolled mobile devices

We’ll help you get started quickly!

**What are the steps?**

1) Setup End User License Agreement (EULA). For information on setting up EULA, refer [EULA Management](#). (This step is optional)

2) Configure APNs certificates, if your SEM users have iOS devices to enroll. For more information, refer [APNs Certificates](#).

3) Create SEM users. For detailed steps, refer [Creating a New SEM User](#). If you add an email address while creating SEM user, the user will receive an email that contains the credentials and enrollment details.

4) Now, SEM users can start enrolling their mobile devices. For more information, refer [Device Enrollment](#).

5) Monitor mobile devices inventory and its security posture using Dashboards and Reports once SEM 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 SEM user, the user must accept the EULA at the time of device enrollment.

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 SEM server with the Apple devices. Qualys SEM helps you generate and renew APNs certificates.

**What is an APNs Certificate?**

SEM 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 Certificate Signing Request file (CSR) 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.
10) Upload the certificate file (.pem) that you downloaded from the Apple portal.

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 SEM user device including ownership of the device, asset communication mode, option to provide mobile number and device enrollment without SEM EMM.

For 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 SEM EMM, select appropriate check-box. You can enroll all iOS devices or Android devices without SEM EMM.
Application Settings
This setting allows you to set a default value for Maximum Enrollable Assets field while creating SEM 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.
SEM User Management

SEM 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.

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

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

Creating a New SEM User

You’ll be able to create a new SEM user with the following steps:
1) Navigate to Users tab and click Add User from the New drop-down.
2) On the Add User page, enter the user information in the Personal Information section and then click Next.

3) On the Add 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 SEM user, and the SEM 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 SEM user. The default value for maximum enrollable assets is configured in Application Settings.
- Status: You can create a user 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.
Mobile Device Inventory

Once SEM 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
- 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
- Logs: Displays various audit logs, sent messages and diagnostic logs
Vulnerability Management

Qualys VM 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 Management in SEM

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 Management in SEM 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 **Inventory** and then click **Vulnerability** 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.

<table>
<thead>
<tr>
<th>Severity</th>
<th>Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Minimal</td>
<td>Basic information disclosure might enable intruders to discover other vulnerabilities, but lack of this information does not make the vulnerability harder to find.</td>
</tr>
<tr>
<td></td>
<td>Medium</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Serious</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Critical</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Urgent</td>
<td>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.</td>
</tr>
</tbody>
</table>
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></td>
<td>Minimal</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></td>
<td>Medium</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></td>
<td>Serious</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></td>
<td>Critical</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></td>
<td>Urgent</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></td>
<td>Minimal</td>
<td>Intruders may be able to retrieve sensitive information related to the mobile device.</td>
</tr>
<tr>
<td></td>
<td>Medium</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></td>
<td>Serious</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 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 Management

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. This opens 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 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.
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.

Dashboards

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.

Get Started with SEM Dashboard

Go to Dashboard to see a complete and continuously updated view of all your mobile assets, in one place within the SEM app.

You can create new dashboard, edit or delete existing dashboards. You can include various widgets to your dashboard.
Select **SEM Mobile Vulnerability Management** template.

VM dashboard template provides complete visibility of mobile vulnerabilities.
Reports

This section helps you to view Audit Log reports. Audit log report is the logs of the actions performed on the SEM portal.

Go to Reports.

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 SEM 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.