Secure Enterprise Mobility

User Guide

Version 1.4.0

April 28, 2022

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

Table of Contents

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 smartphones and tablets) across your enterprise.

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

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

SEM User - Users added to the SEM module/application are considered as SEM Users. SEM Users are holders/owners of the mobile devices.

With SEM, you can:

- Compressive visibility into mobile devices details, installed apps, and configurations, even if they are not on VPN or network,

- Real-time visibility into vulnerabilities and critical device settings along with monitoring for potentially harmful applications,

- Automatic correlation of vulnerabilities with apps and Android patches, and

- Orchestration of appropriate response actions such as deploying patches from Google Play Store or uninstalling vulnerable apps.

We'll help you get started quickly!

Supported Platforms

- Android (Version 4.4.2 and higher)

- iOS (Version 9.0 and higher)

- iPadOS (Version 13.1 and higher)

What are the steps?

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

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

3) Create SEM users. For detailed steps, refer to Creating a New SEM User. If you add an email address while creating an SEM user, the user will receive an email that contains the credentials and enrollment details. SEM users have the **Bulk User Upload** option to add multiple users in one go!

4) Now, SEM users can start enrolling their mobile devices. For more information, refer to Device Enrollment. If devices are already enrolled in any EMM, configure the 'Enroll device without SEM EMM' for iOS and Android, i.e., select the 'All iOS devices' and 'All Android devices' check-boxes. For more details, refer to Enrollment Settings. You can auto-enroll the devices through an automated enrollment process.

5) Monitor mobile devices inventory and its security posture using Dashboards and Reports once SEM users enroll their devices.

6) If the devices are enrolled in Intune, then configure Intune Connector to sync the enrolled devices in SEM agentless.

Configurations

This section helps you to create and manage EULA. It also helps you to configure APNs certificates. This section also helps you 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, and so on.

Typically, the organization’s legal team provides EULA.

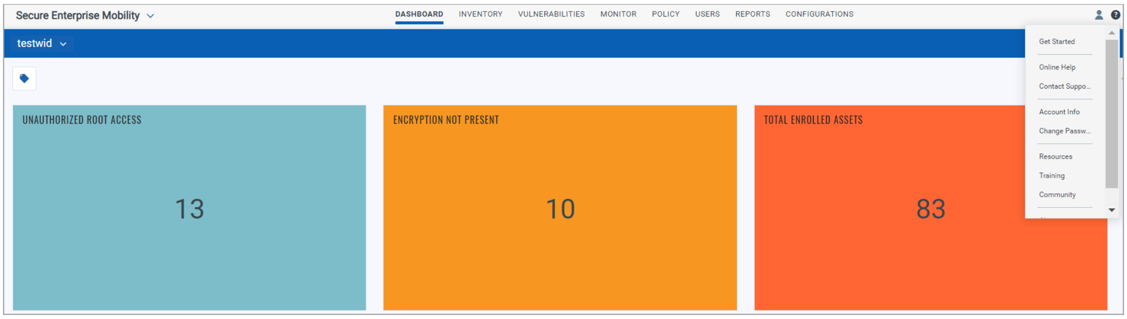
Customer's use of the Cloud Services will result in Personal Identifiable Information being processed by Qualys. Customer acts as a data controller, and Qualys acts as a Data Processor. It is the customers’ obligation, and Qualys shall not have any obligation, to gather the appropriate consent from every data subject from whom the customer is gathering Personally Identifiable Information through the Cloud Services. The customer is required to enter into an end-user agreement with each data subject that informs the subject of the data 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 provide you with a provision to add the End User License Agreement text. This step is optional. If EULA is configured, the asset user must accept the EULA before enrolling assets.

Qualys allows you to configure your own EULA text based on your organization's needs 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 the help icon (question mark icon) and then click **Get Started**.



UNAUTHORIZED ROOT ACCESS 13

ENCRYPTION NOT PRESENT 10

TOTAL ENROLLED ASSETS 83

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

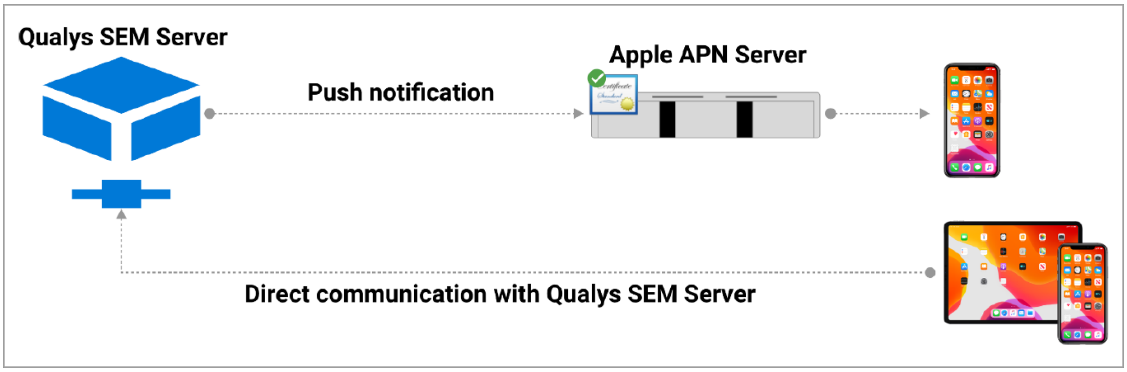
You can also access the EULA from **Configurations** > **EULA**. You can edit the EULA text using the **Edit** action from the quick action menu.

APNs Certificates

This section applies only to the 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 an APNs certificate to send notifications to the Apple devices when communication is initiated by the administrator or 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 using the Apple ID, which belongs to the organization.

- Mac OS X or Windows workstation with Administrative permissions

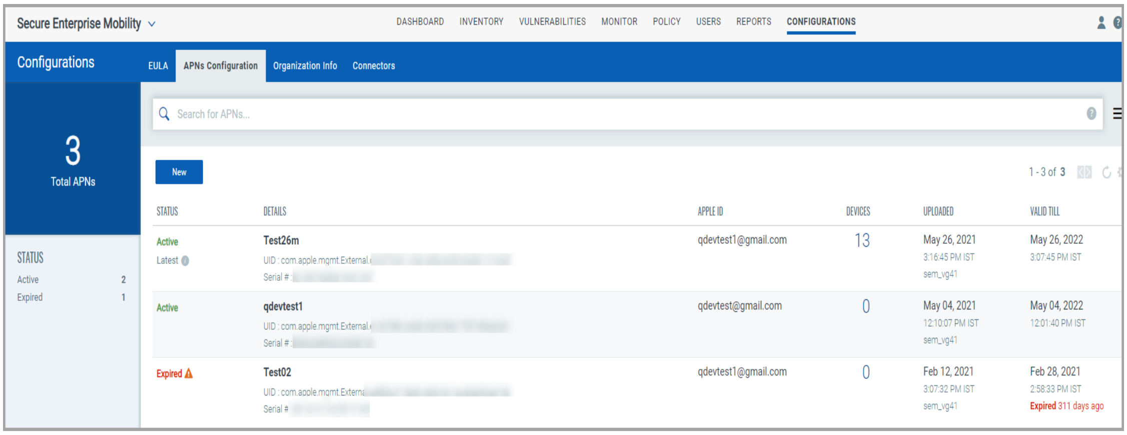
- Web browser (Safari, Mozilla Firefox, or Chrome are required to work with Apple's

website)

Steps to Generate APNs Certificate

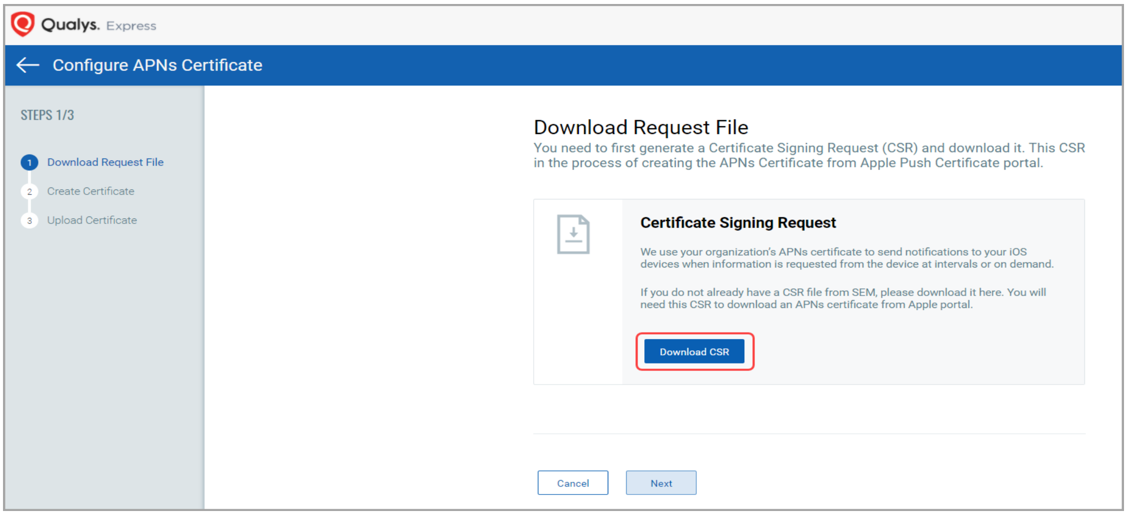
1) Login to the SEM Portal at https://xxxx.apps.qualys.com.

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



STATUS	DETAILS	APPLE ID	DEVICES	UPLOADED	VALID TILL
Active Latest	Test26m UID : com.apple.mgmt.External.[redacted] Serial # : [redacted]	qdevtest1@gmail.com	13	May 26, 2021 3:16:45 PM IST sem_vg41	May 26, 2022 3:07:45 PM IST
Active	qdevtest1 UID : com.apple.mgmt.External.[redacted] Serial # : [redacted]	qdevtest@gmail.com	0	May 04, 2021 12:10:07 PM IST sem_vg41	May 04, 2022 12:01:40 PM IST
Expired ⚠	Test02 UID : com.apple.mgmt.Externa[redacted] Serial # [redacted]	qdevtest1@gmail.com	0	Feb 12, 2021 3:07:32 PM IST sem_vg41	Feb 28, 2021 2:58:33 PM IST Expired 311 days ago

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



Download Request File

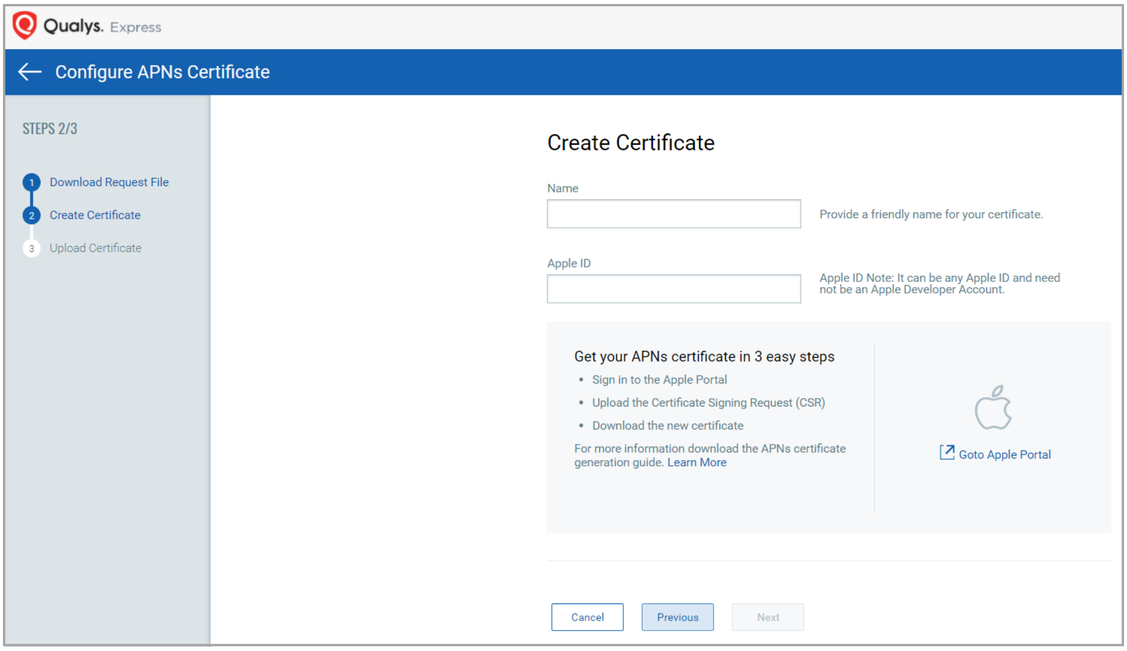
You need to first generate a Certificate Signing Request (CSR) and download it. This CSR in the process of creating the APNs Certificate from Apple Push Certificate portal.

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 SEM, please download it here. You will need this CSR to download an APNs certificate from Apple portal.

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



Create Certificate

Name

Provide a friendly name for your certificate.

Apple ID

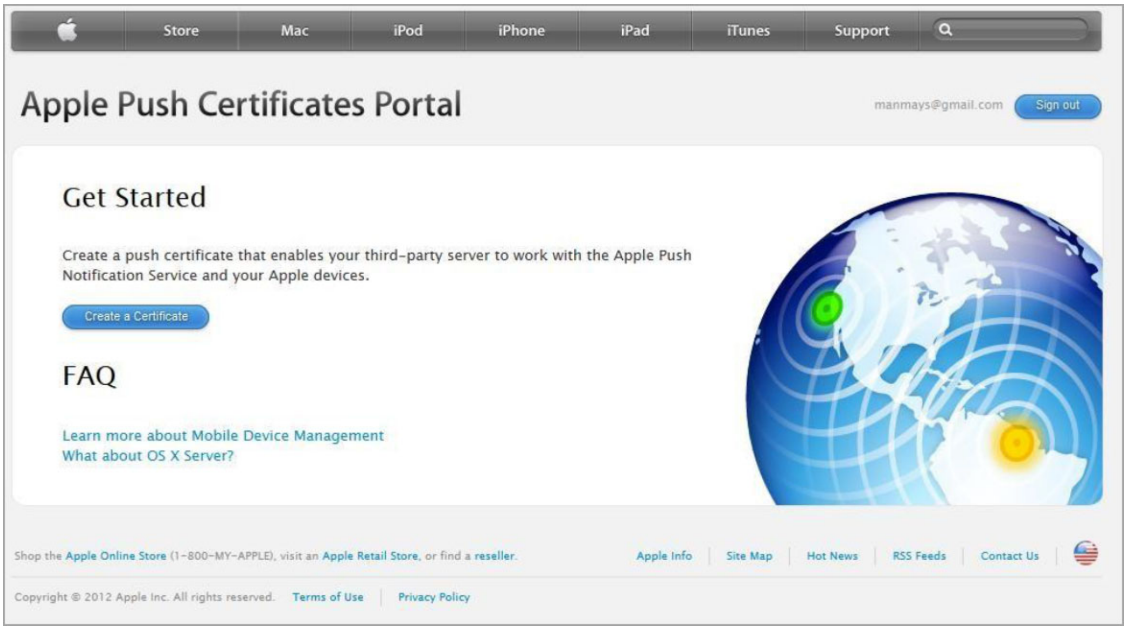
Apple ID Note: It can be any Apple ID and need not be an Apple Developer Account.

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

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



Apple Push Certificates Portal

manmays@gmail.com

Get Started

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

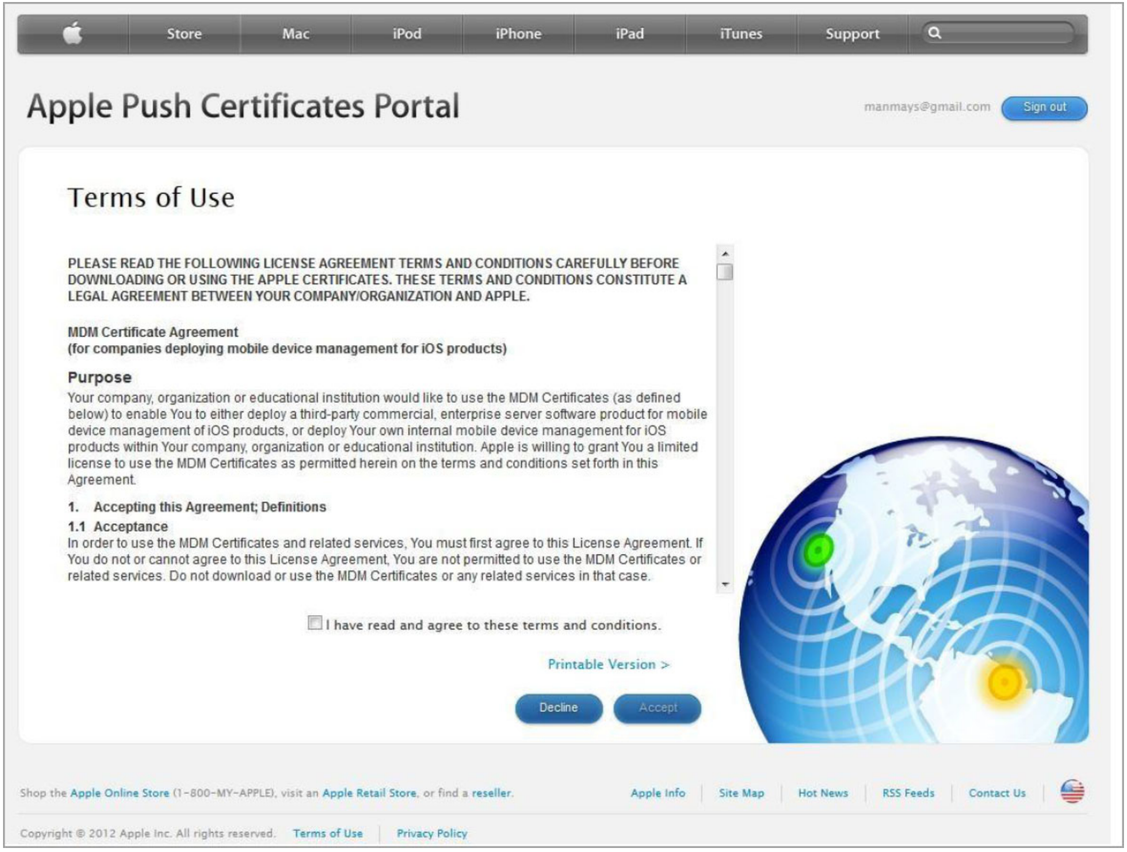
FAQ

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.

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**.



Apple Push Certificates Portal

manmays@gmail.com Sign out

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 >

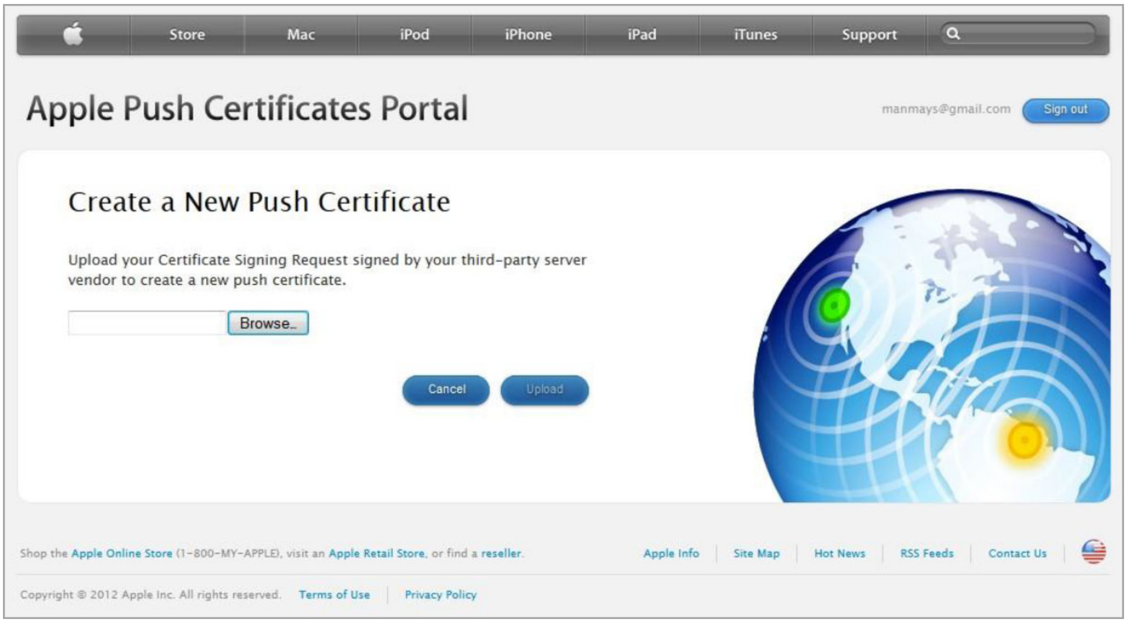
Decline Accept

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.



Apple Push Certificates Portal

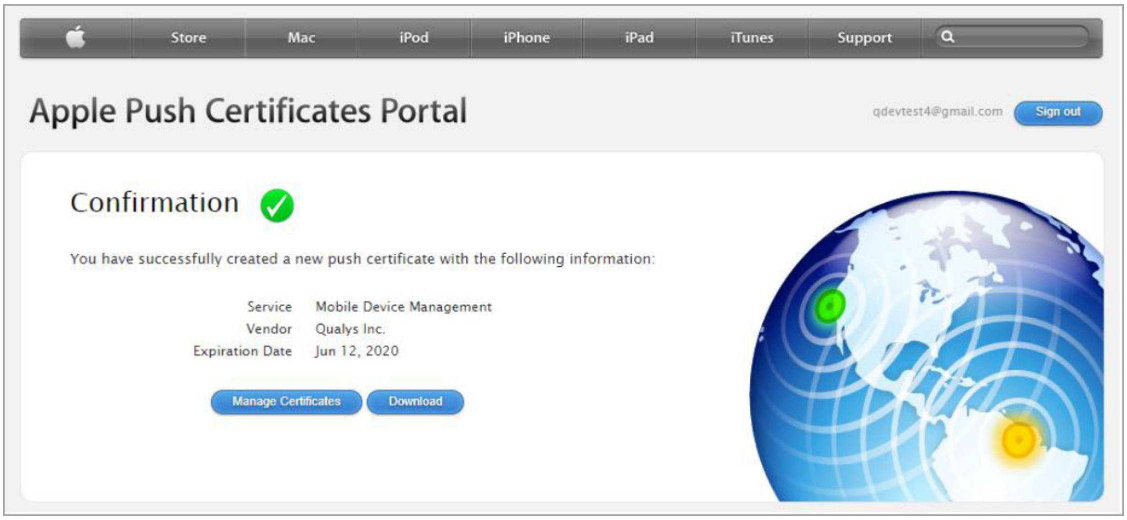
Create a New Push Certificate

Upload your Certificate Signing Request signed by your third-party server vendor to create a new push certificate.

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

Copyright © 2012 Apple Inc. All rights reserved.

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



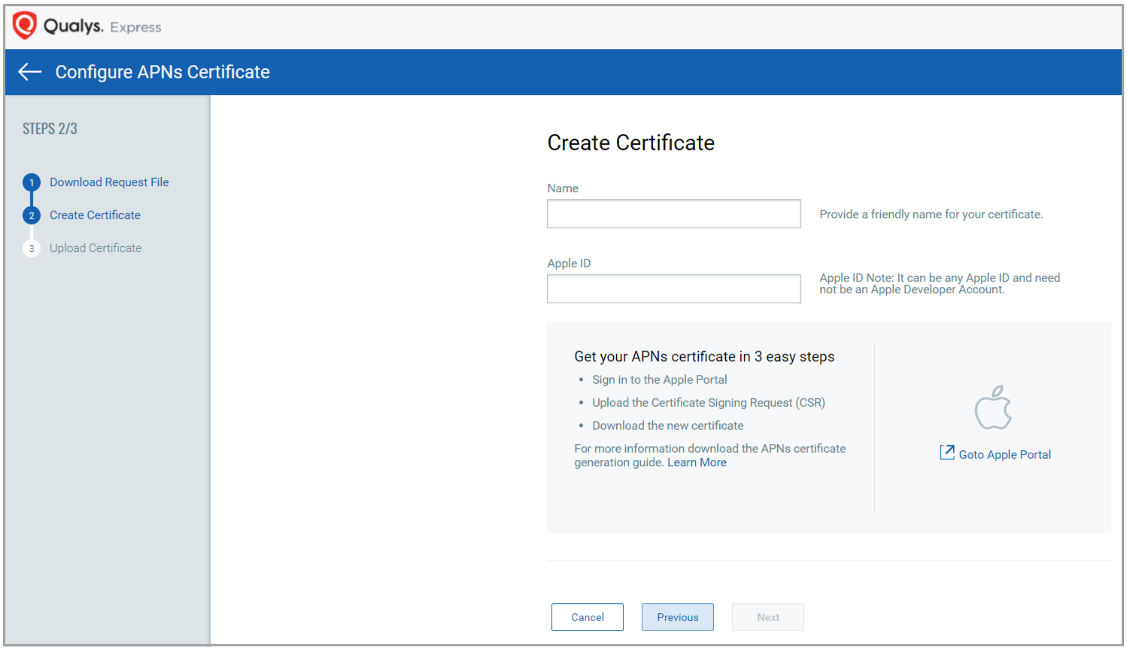
Apple Push Certificates Portal

Confirmation ✓

You have successfully created a new push certificate with the following information:

Service	Mobile Device Management
Vendor	Qualys Inc.
Expiration Date	Jun 12, 2020

9) 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**.



Provide a friendly name for your certificate.

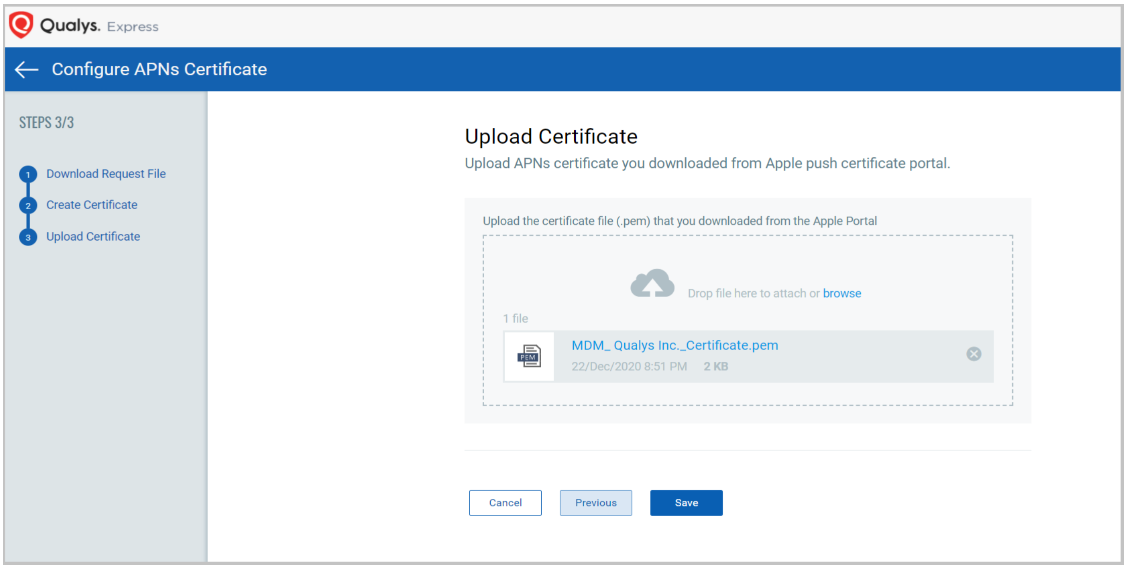
Apple ID Note: It can be any Apple ID and need not be an Apple Developer Account.

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

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



Upload APNs certificate you downloaded from Apple push certificate portal.

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

Drop file here to attach or browse

1 file

MDM_ Qualys Inc._Certificate.pem
22/Dec/2020 8:51 PM 2 KB

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

The APNs Configuration tab lists the APNs certificate, and you can start using it to manage your Apple devices. The validity of the APNs certificate is 365 days, so you must renew the APNs Certificate before expiring the certificate. To know more, refer to Renew APNs Certificate.

Organization Information

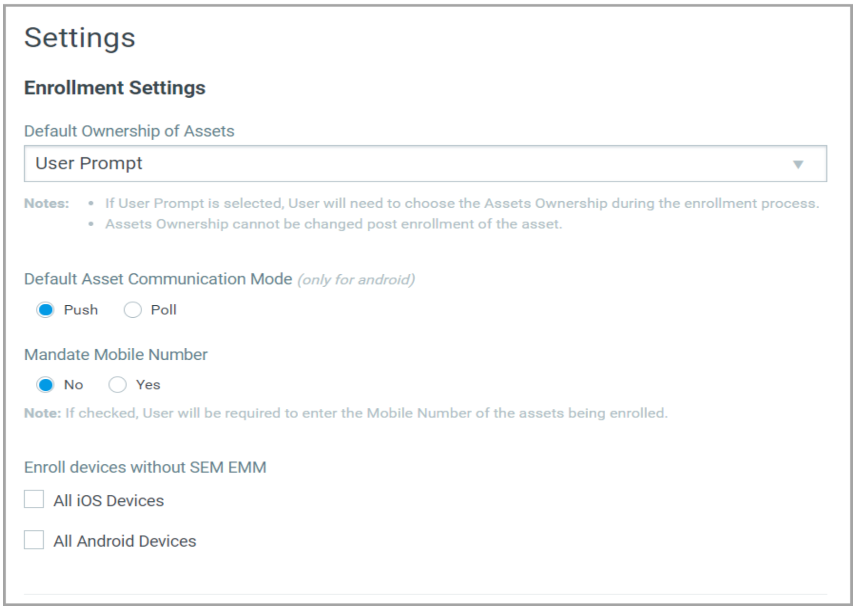
This section helps you configure the organization-level information. The sender's address helps to send out any communication or notification from the organization.

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 a mobile number, and device enrollment without SEM EMM.



Settings

Enrollment Settings

Default Ownership of Assets

User Prompt ▾

Notes:
- If User Prompt is selected, User will need to choose the Assets Ownership during the enrollment process.
- Assets Ownership cannot be changed post enrollment of the asset.

Default Asset Communication Mode *(only for android)*

● Push ○ Poll

Mandate Mobile Number

● No ○ Yes

Note: If checked, User will be required to enter the Mobile Number of the assets being enrolled.

Enroll devices without SEM EMM

□ All iOS Devices

□ All Android Devices

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

- Push: Qualys server initiates communication with the device when required.

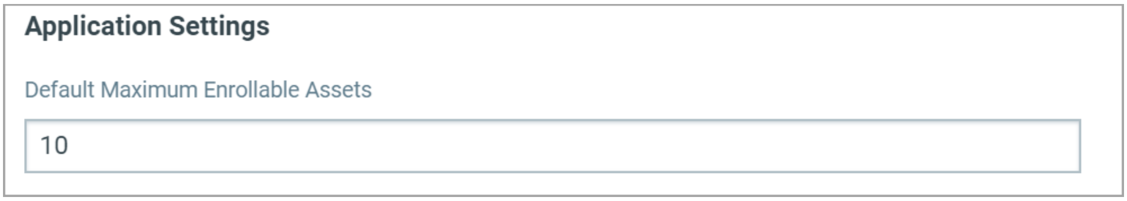
- Poll: Device will communicate to the Qualys server after the specified regular interval. You can set the polling intervals in Sync Settings.

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

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

Application Settings

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



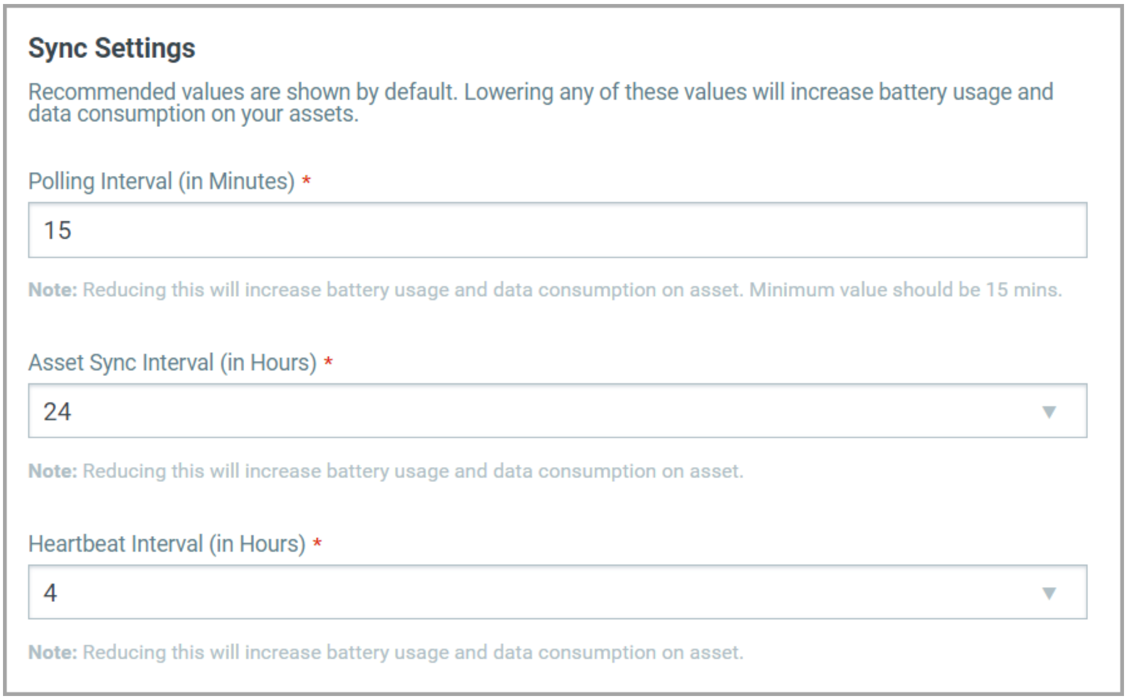
Application Settings

Default Maximum Enrollable Assets

10

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) *

15

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

Asset Sync Interval (in Hours) *

24 ▼

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

Heartbeat Interval (in Hours) *

4 ▼

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 such as newly installed apps, changes in settings, and so on, to the Qualys server as per the intervals set here.

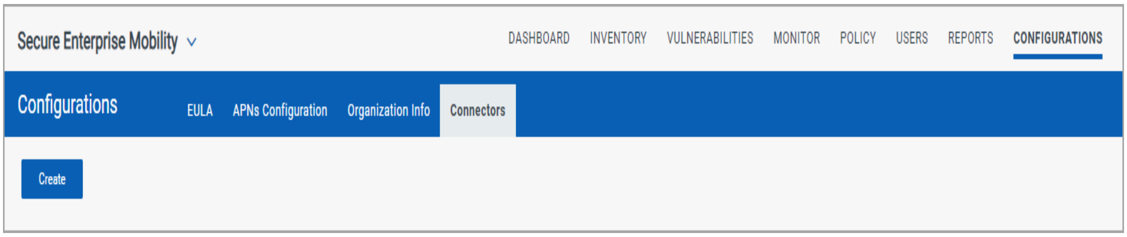
- Heartbeat Interval (in Hours): Device regularly communicates to the Qualys server notifying its status as per interval set here.

Connector

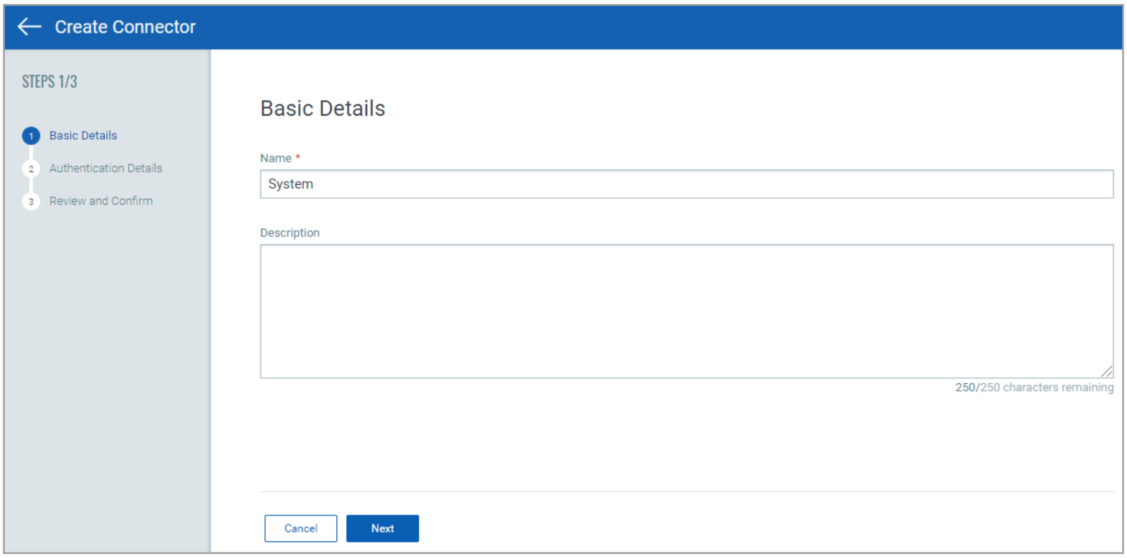
Configure the connector to sync the devices enrolled in EMM/MDM solution in SEM. For now, you can sync only those devices that are enrolled in Intune EMM using a connector.

Following are the steps to configure a new connector:

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



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



Basic Details

Name *

System

Description

250/250 characters remaining

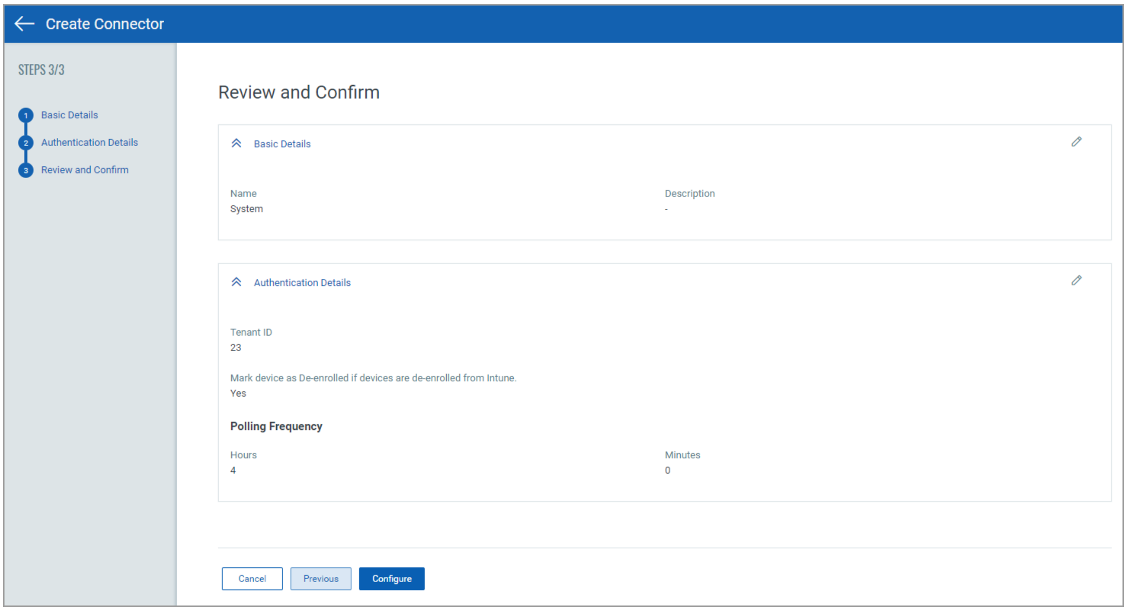
3) Enter Authentication Details.

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

Note: Polling frequency can be set to a minimum of 1 hour, which 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) Once the entered details are reviewed and confirmed, click **Configure**.



Create Connector

STEPS 3/3

1 Basic Details
2 Authentication Details
3 Review and Confirm

Review and Confirm

Basic Details

Name
System

Description
-

Authentication Details

Tenant ID
23

Mark device as De-enrolled if devices are de-enrolled from Intune.
Yes

Polling Frequency

Hours
4

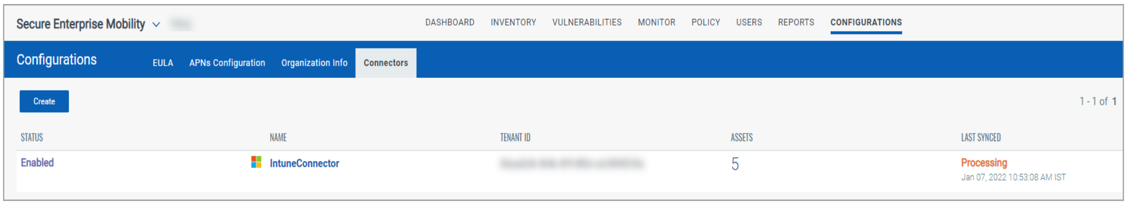
Minutes
0

Cancel | Previous | 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 the **Configurations** > **Connectors** sub-tab.



Secure Enterprise Mobility [redacted]

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

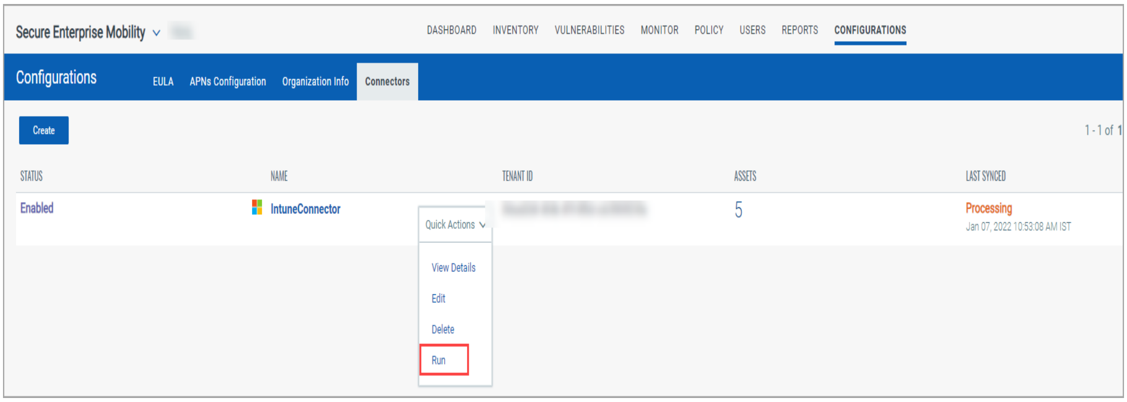
Configurations: EULA | APNs Configuration | Organization Info | Connectors

Create

1 - 1 of 1

STATUS	NAME	TENANT ID	ASSETS	LAST SYNCED
Enabled	IntuneConnector	[redacted]	5	Processing Jan 07, 2022 10:53:08 AM 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 clicking **Run**.



STATUS	NAME	TENANT ID	ASSETS	LAST SYNCED
Enabled	IntuneConnector	[redacted]	5	Processing Jan 07, 2022 10:53:08 AM IST

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

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

Note: These devices are enrolled without SEM EMM.

Auto-merging of Cloud Agent Assets with Intune Synced Assets

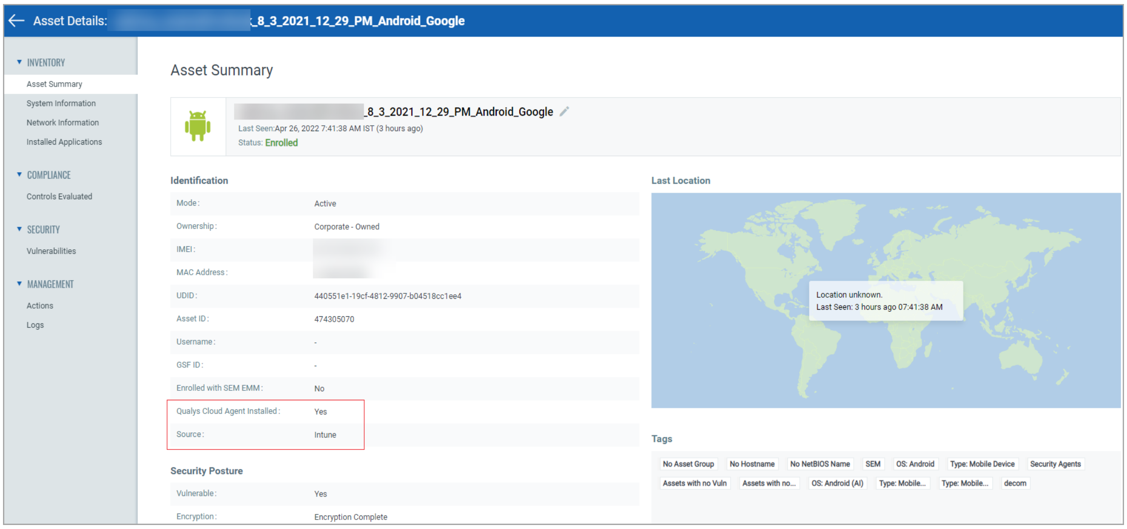
Once a connector is configured, the assets enrolled in EMM/MDM solution are automatically synced with Intune assets. It is optional if you want to install the Cloud Agent on the synced assets. Installing the Cloud Agent lets you leverage the benefits for both the Cloud Agent and Intune.

Once the agent is enrolled, the Cloud Agent asset gets automatically merged into the respective Intune synced asset. Once it is merged, only one asset entity appears on the UI.

In the **Asset Details** window, you can confirm the following:

- If the agent is installed on the asset or not, by referring to the **Qualys Cloud Agent Installed** field. If the agent is installed on the asset then the **Qualys Cloud Agent Installed** field displays **Yes**.

- If the asset is enrolled with Intune or not, by referring to the **Source** field. If the asset is synced through Intune then the **Source** field displays **Intune**.



Asset Details: [redacted]_8_3_2021_12_29_PM_Android_Google

Asset Summary

[redacted]_8_3_2021_12_29_PM_Android_Google
Last Seen:Apr 26, 2022 7:41:38 AM IST (3 hours ago)
Status: Enrolled

Identification

Mode: Active
Ownership: Corporate - Owned
IMEI: [redacted]
MAC Address: [redacted]
UDID: 440551e1-19cf-4812-9907-b04518cc1ee4
Asset ID: 474305070
Username: -
GSF ID: -
Enrolled with SEM EMM: No
Qualys Cloud Agent Installed: Yes
Source: Intune

Security Posture

Vulnerable: Yes
Encryption: Encryption Complete

Last Location

Location unknown.
Last Seen: 3 hours ago 07:41:38 AM

Tags

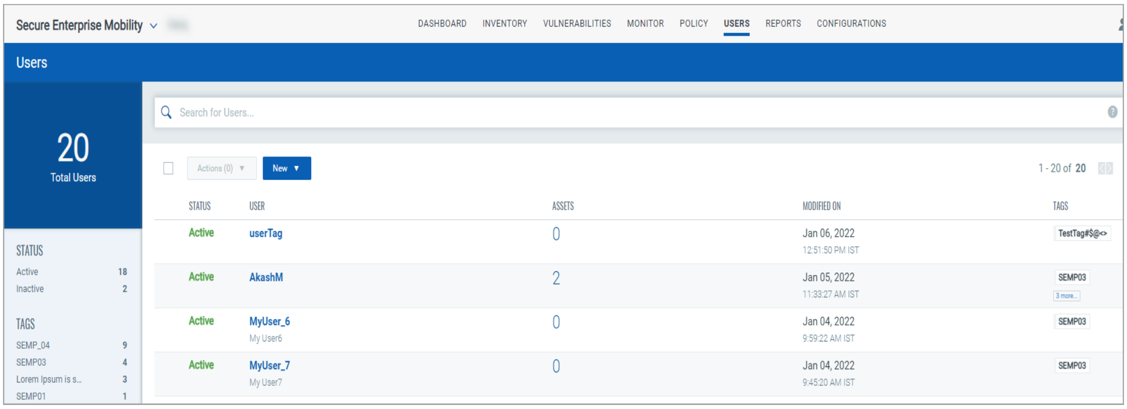
No Asset Group | No Hostname | No NetBIOS Name | SEM | OS: Android | Type: Mobile Device | Security Agents
Assets with no Vuln | Assets with no... | OS: Android (AI) | Type: Mobile... | Type: Mobile... | decom

SEM User Management

SEM users are the users who enroll their devices as per email received from the Admin User. The email contains detailed steps to enroll the mobile device. To enroll the device, refer to Device Enrollment.

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

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



STATUS	
Active	18
Inactive	2

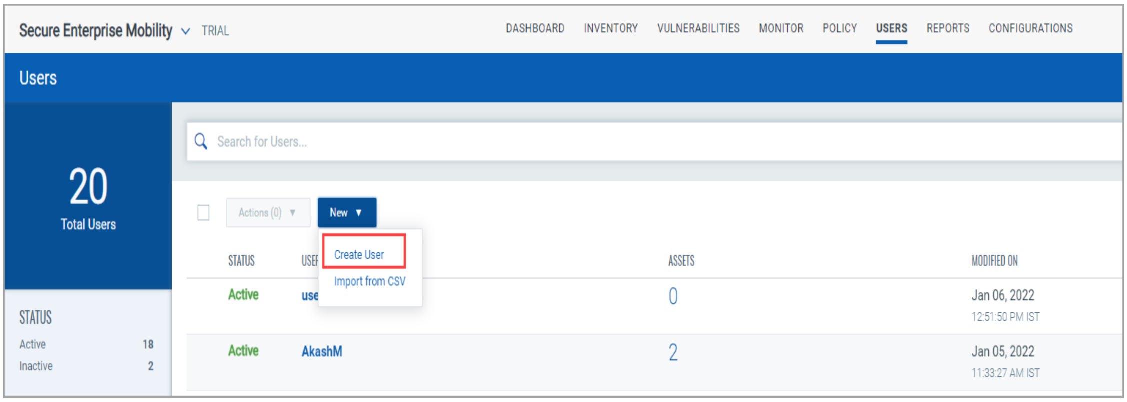
TAGS	
SEMP_04	9
SEMP03	4
Lorem Ipsum is s...	3
SEMP01	1

STATUS	USER	ASSETS	MODIFIED ON	TAGS
Active	userTag	0	Jan 06, 2022 12:51:50 PM IST	TestTag#$@<>
Active	AkashM	2	Jan 05, 2022 11:33:27 AM IST	SEMP03 3 more...
Active	MyUser_6 My User6	0	Jan 04, 2022 9:59:22 AM IST	SEMP03
Active	MyUser_7 My User7	0	Jan 04, 2022 9:45:20 AM IST	SEMP03

Creating a New SEM User

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

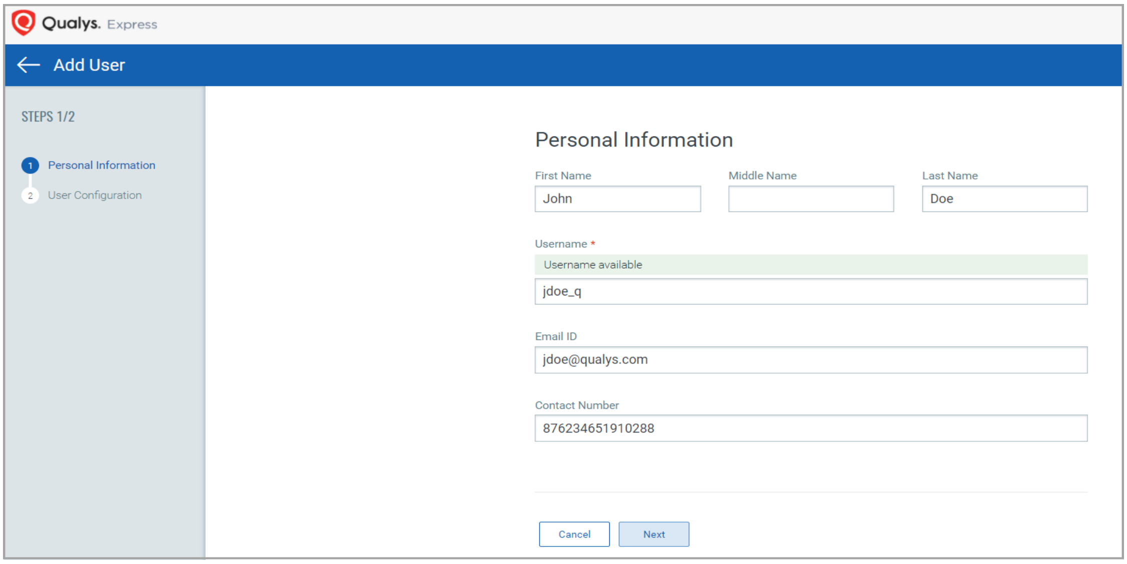
1) Navigate to the **Users** tab and click **Create User** from the **New** drop-down menu.



STATUS	
Active	18
Inactive	2

STATUS	USER	ASSETS	MODIFIED ON
Active	use	0	Jan 06, 2022 12:51:50 PM IST
Active	AkashM	2	Jan 05, 2022 11:33:27 AM IST

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



Personal Information

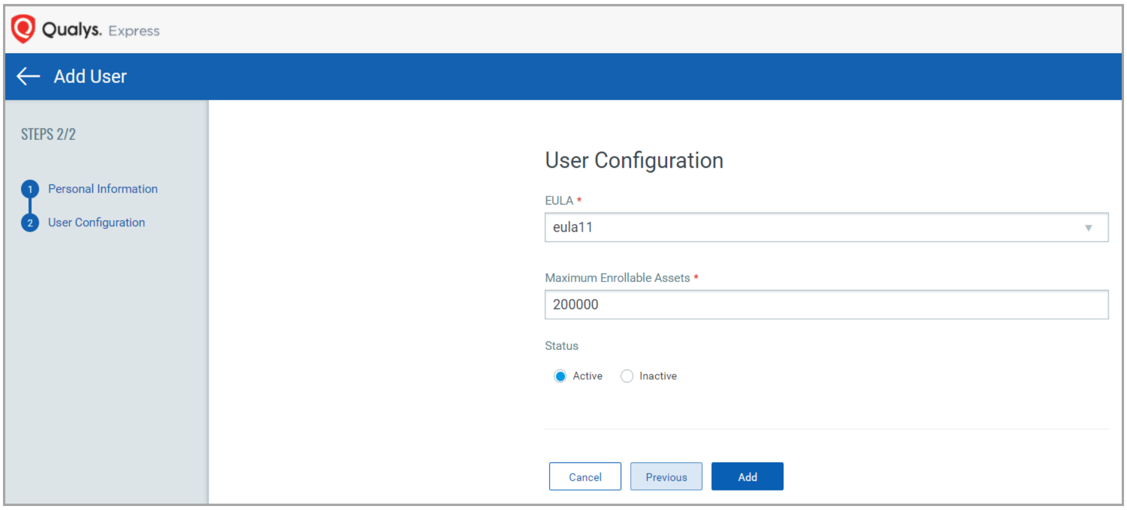
First Name: John
Middle Name:
Last Name: Doe
Username *
Username available
jdoe_q
Email ID: jdoe@qualys.com
Contact Number: 876234651910288

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

- **EULA**: Configure the EULA message you want users to read and accept. For more information, refer to 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.



User Configuration

EULA *: eula11

Maximum Enrollable Assets *: 200000

Status: ● Active ○ Inactive

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

Once you add a user with a valid email address, an email is sent to the user to enroll the device.

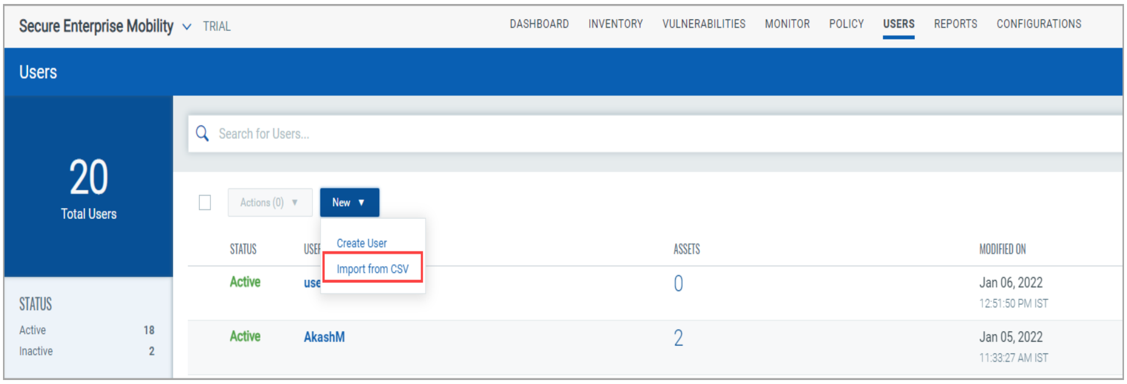
Bulk User Upload

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

Importing Users

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

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



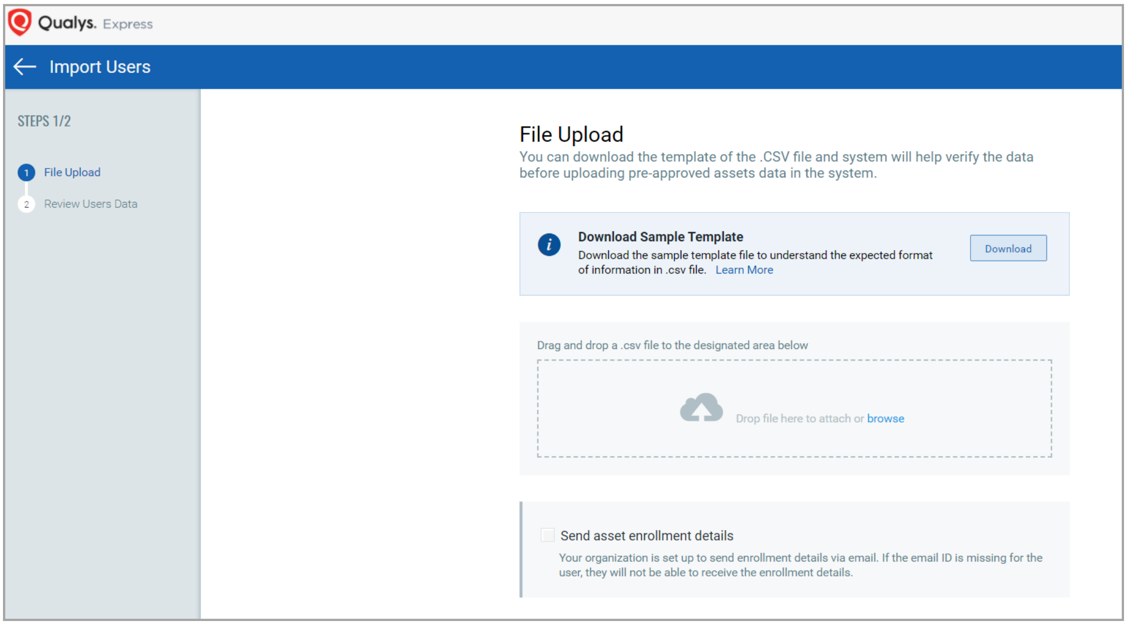
20 Total Users

STATUS

Active	18
Inactive	2

STATUS	USER	ASSETS	MODIFIED ON
Active	use	0	Jan 06, 2022 12:51:50 PM IST
Active	AkashM	2	Jan 05, 2022 11:33:27 AM IST

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



File Upload

You can download the template of the .CSV file and system will help verify the data before uploading pre-approved assets data in the system.

Download Sample Template

Download the sample template file to understand the expected format of information in .csv file. Learn More

Drag and drop a .csv file to the designated area below

□ Send asset enrollment details

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 the users in SEM, make sure you have met the following conditions:

- 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

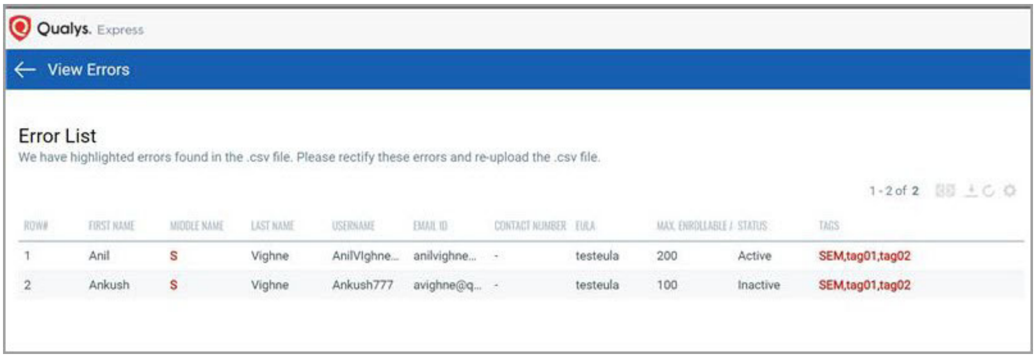
- If mandatory fields are left blank or file contains duplicate data; you will be informed of the line numbers and data that needs to be fixed. Data will be saved only when all the errors are cleared

- Make sure you have the latest CSV file format. Refer to the following table to fill the correct information in the 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 the 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), click the **View Errors** link to see the Error List page with a list of errors in the CSV file. Following is the screen for sample errors:



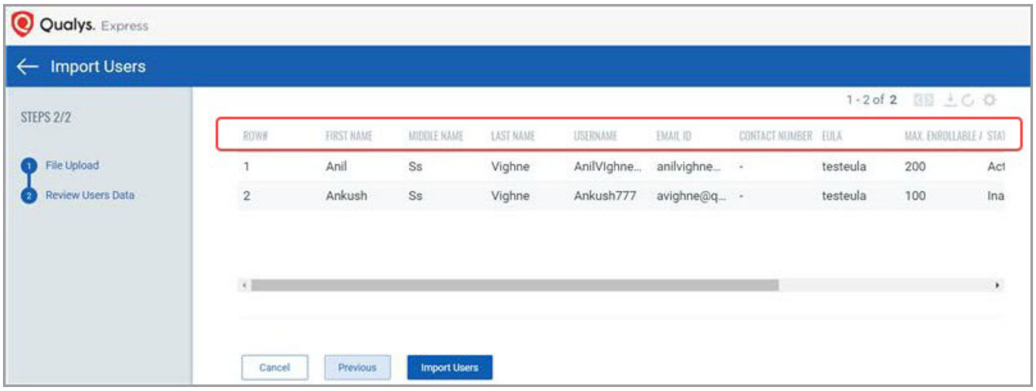
Error List

We have highlighted errors found in the .csv file. Please rectify these errors and re-upload the .csv file.

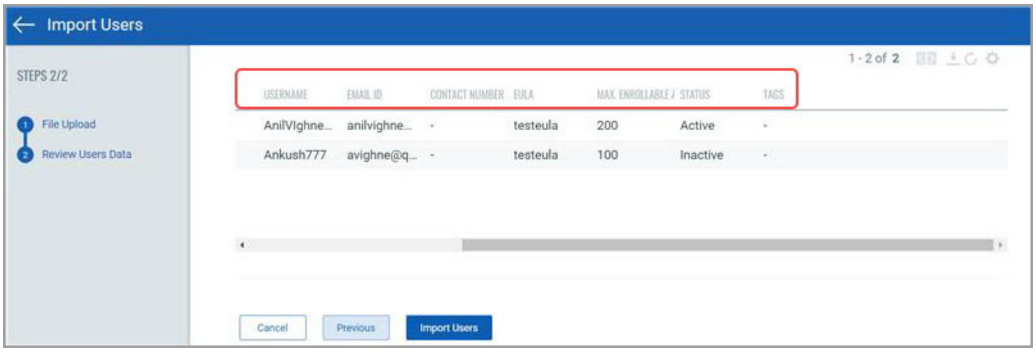
1 - 2 of 2

ROW#	FIRST NAME	MIDDLE NAME	LAST NAME	USERNAME	EMAIL ID	CONTACT NUMBER	EULA	MAX. ENROLLABLE /	STATUS	TAGS
1	Anil	S	Vighne	AnilVIghne...	anilvighne...	-	testeula	200	Active	SEM,tag01,tag02
2	Ankush	S	Vighne	Ankush777	avighne@q...	-	testeula	100	Inactive	SEM,tag01,tag02

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



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



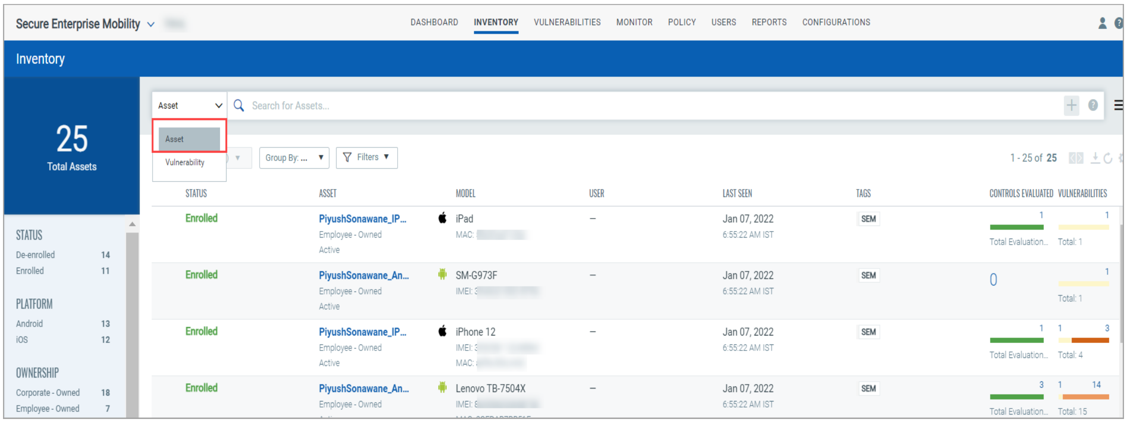
USERNAME	EMAIL ID	CONTACT NUMBER	EULA	MAX. ENROLLABLE /	STATUS	TAGS
AnilVighne...	anilvighne...	-	testeula	200	Active	-
Ankush777	avighne@q...	-	testeula	100	Inactive	-

Mobile Device Inventory

Once the SEM users enroll their mobile devices, you can view the list under the **Inventory** tab.

Refer to 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 applications.

Select the **Asset** option 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.



STATUS	
De-enrolled	14
Enrolled	11
PLATFORM	
Android	13
iOS	12
OWNERSHIP	
Corporate - Owned	18
Employee - Owned	7

STATUS	ASSET	MODEL	USER	LAST SEEN	TAGS	CONTROLS EVALUATED	VULNERABILITIES
Enrolled	PiyushSonawane_IP... Employee - Owned Active	iPad MAC: [redacted]	–	Jan 07, 2022 6:55:22 AM IST	SEM	1 Total Evaluation...	1 Total: 1
Enrolled	PiyushSonawane_An... Employee - Owned Active	SM-G973F IMEI: [redacted]	–	Jan 07, 2022 6:55:22 AM IST	SEM	0	1 Total: 1
Enrolled	PiyushSonawane_IP... Employee - Owned Active	iPhone 12 IMEI: [redacted] MAC: [redacted]	–	Jan 07, 2022 6:55:22 AM IST	SEM	1 Total Evaluation...	1 3 Total: 4
Enrolled	PiyushSonawane_An... Employee - Owned	Lenovo TB-7504X IMEI: [redacted]	–	Jan 07, 2022 6:55:22 AM IST	SEM	3 Total Evaluation...	1 14 Total: 15

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

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

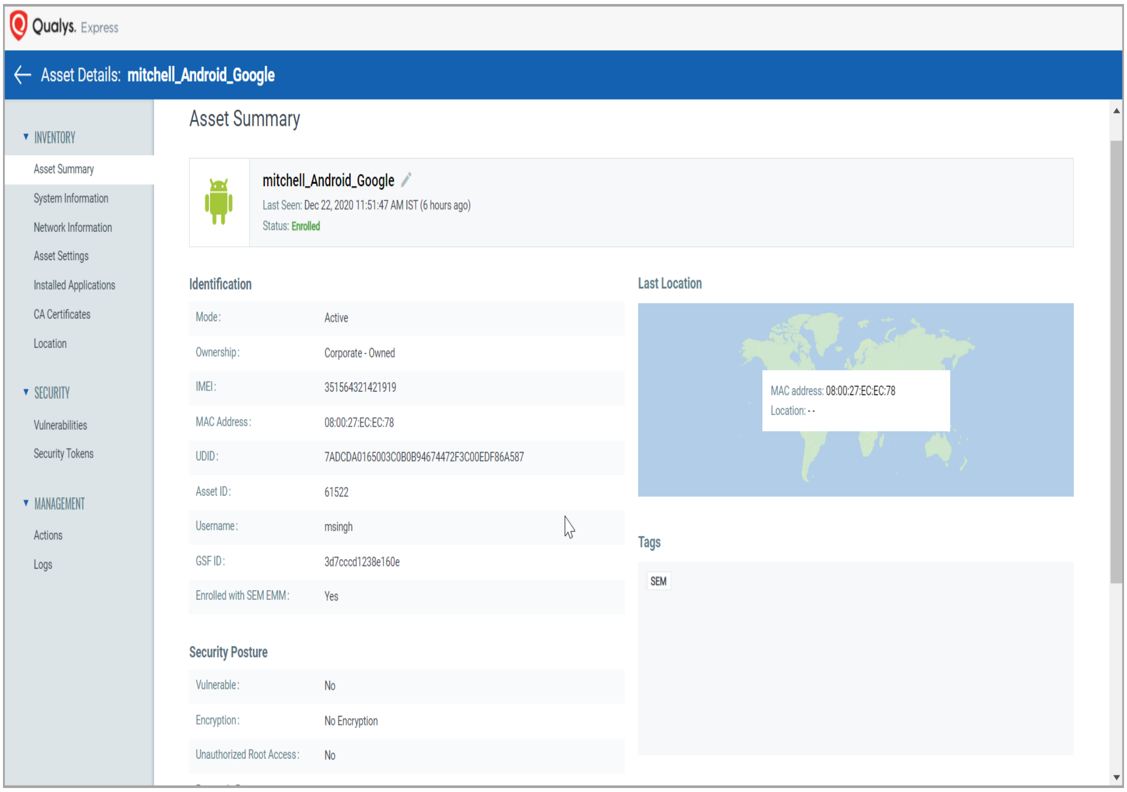
- Enrolled: Device is ready for management

- De-enrolled: Corporate data is deleted, and the 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 Summary

mitchell_Android_Google

Last Seen: Dec 22, 2020 11:51:47 AM IST (6 hours ago)

Status: Enrolled

Identification

Mode:	Active
Ownership:	Corporate - Owned
IMEI:	351564321421919
MAC Address:	08:00:27:EC:EC:78
UDID:	7ADCDA0165003C0B0B94674472F3C00EDF86A587
Asset ID:	61522
Username:	msingh
GSF ID:	3d7cccd1238e160e
Enrolled with SEM EMM:	Yes

Security Posture

Vulnerable:	No
Encryption:	No Encryption
Unauthorized Root Access:	No

Last Location

MAC address: 08:00:27:EC:EC:78
Location: - -

Tags

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

- 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 Assessment

Qualys Vulnerability Assessment 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 the unexpected changes in your network before they turn into breaches.

Vulnerability Assessment in SEM

Vulnerability Assessment in SEM gives you visibility into mobile devices vulnerable to threats due to outdated OS.

On enrollment, 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 the best coverage of vulnerabilities of Android and iOS, it includes:

Device vulnerabilities including 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. It also detects the OS vulnerabilities exploits too.

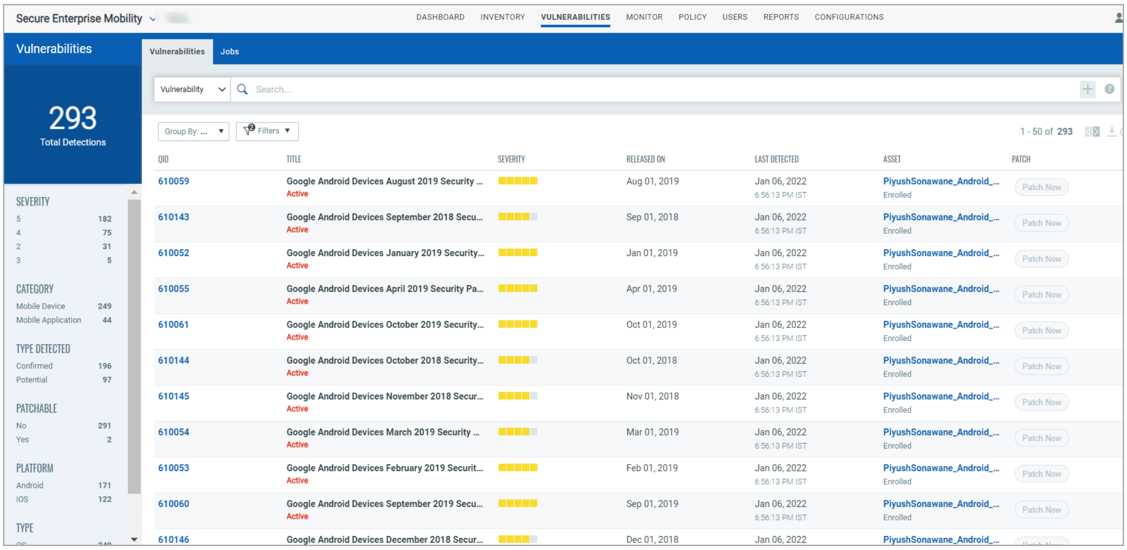
Detection of Jailbreak/Rooted devices, Encryption disabled, Password removed/disabled.

For App vulnerabilities, we detect the CVE of the vulnerable apps, such as the Google Chrome application vulnerabilities shown in the above example and detect the potentially harmful applications. We cover the application's vulnerabilities from 2016 till the latest.

We detect the devices connected to an open Wi-Fi network for network vulnerabilities.

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

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



293
Total Detections

SEVERITY	
5	182
4	75
2	31
3	5

CATEGORY	
Mobile Device	249
Mobile Application	44

TYPE DETECTED	
Confirmed	196
Potential	97

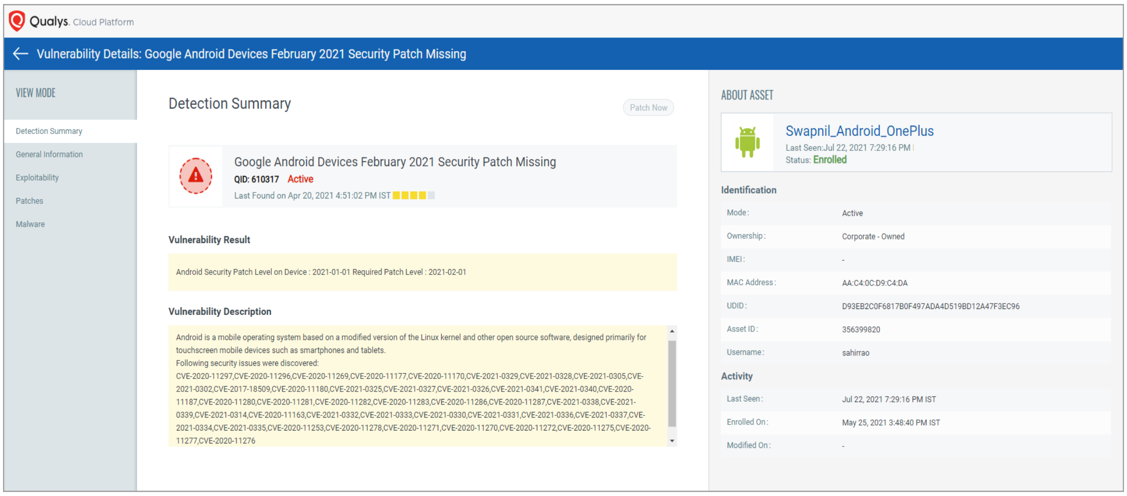
PATCHABLE	
No	291
Yes	2

PLATFORM	
Android	171
iOS	122

TYPE

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... Active	▮▮▮▮▮	Oct 01, 2019	Jan 06, 2022 6:56:13 PM IST	PiyushSonawane_Android_... Enrolled	Patch Now
610144	Google Android Devices October 2018 Security... Active	▮▮▮▮▯	Oct 01, 2018	Jan 06, 2022 6:56:13 PM IST	PiyushSonawane_Android_... Enrolled	Patch Now
610145	Google Android Devices November 2018 Secur... Active	▮▮▮▮▯	Nov 01, 2018	Jan 06, 2022 6:56:13 PM IST	PiyushSonawane_Android_... Enrolled	Patch Now
610054	Google Android Devices March 2019 Security ... Active	▮▮▮▮▯	Mar 01, 2019	Jan 06, 2022 6:56:13 PM IST	PiyushSonawane_Android_... Enrolled	Patch Now
610053	Google Android Devices February 2019 Securit... Active	▮▮▮▮▮	Feb 01, 2019	Jan 06, 2022 6:56:13 PM IST	PiyushSonawane_Android_... Enrolled	Patch Now
610060	Google Android Devices September 2019 Secu... Active	▮▮▮▮▮	Sep 01, 2019	Jan 06, 2022 6:56:13 PM IST	PiyushSonawane_Android_... Enrolled	Patch Now
610146	Google Android Devices December 2018 Secur...	▮▮▮▮▯	Dec 01, 2018	Jan 06, 2022	PiyushSonawane_Android_...	

Click a particular QID to view the vulnerability details.



Vulnerability Details: Google Android Devices February 2021 Security Patch Missing

Detection Summary

Google Android Devices February 2021 Security Patch Missing
QID: 610317 Active
Last Found on Apr 20, 2021 4:51:02 PM IST ▮▮▮▮▯

Vulnerability Result

Android Security Patch Level on Device : 2021-01-01 Required Patch Level : 2021-02-01

Vulnerability Description

Android is a mobile operating system based on a modified version of the Linux kernel and other open source software, designed primarily for touchscreen mobile devices such as smartphones and tablets.
Following security issues were discovered:
CVE-2020-11297,CVE-2020-11296,CVE-2020-11269,CVE-2020-11177,CVE-2020-11170,CVE-2021-0329,CVE-2021-0328,CVE-2021-0305,CVE-2021-0302,CVE-2017-18509,CVE-2020-11180,CVE-2021-0325,CVE-2021-0327,CVE-2021-0326,CVE-2021-0341,CVE-2021-0340,CVE-2020-11187,CVE-2020-11280,CVE-2020-11281,CVE-2020-11282,CVE-2020-11283,CVE-2020-11286,CVE-2020-11287,CVE-2021-0338,CVE-2021-0339,CVE-2021-0314,CVE-2020-11163,CVE-2021-0332,CVE-2021-0333,CVE-2021-0330,CVE-2021-0331,CVE-2021-0336,CVE-2021-0337,CVE-2021-0334,CVE-2021-0335,CVE-2020-11253,CVE-2020-11278,CVE-2020-11271,CVE-2020-11270,CVE-2020-11272,CVE-2020-11275,CVE-2020-11277,CVE-2020-11276

ABOUT ASSET

Swapnil_Android_OnePlus
Last Seen:Jul 22, 2021 7:29:16 PM I
Status: Enrolled

Identification

Mode :	Active
Ownership :	Corporate - Owned
IMEI :	-
MAC Address :	AA:C4:0C:D9:C4:DA
UDID :	D93EB2C0F6817B0F497ADA4D519BD12A47F3EC96
Asset ID :	356399820
Username :	sahirrao

Activity

Last Seen :	Jul 22, 2021 7:29:16 PM IST
Enrolled On :	May 25, 2021 3:48:40 PM IST
Modified On :	-

Vulnerability details include the following:

- 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

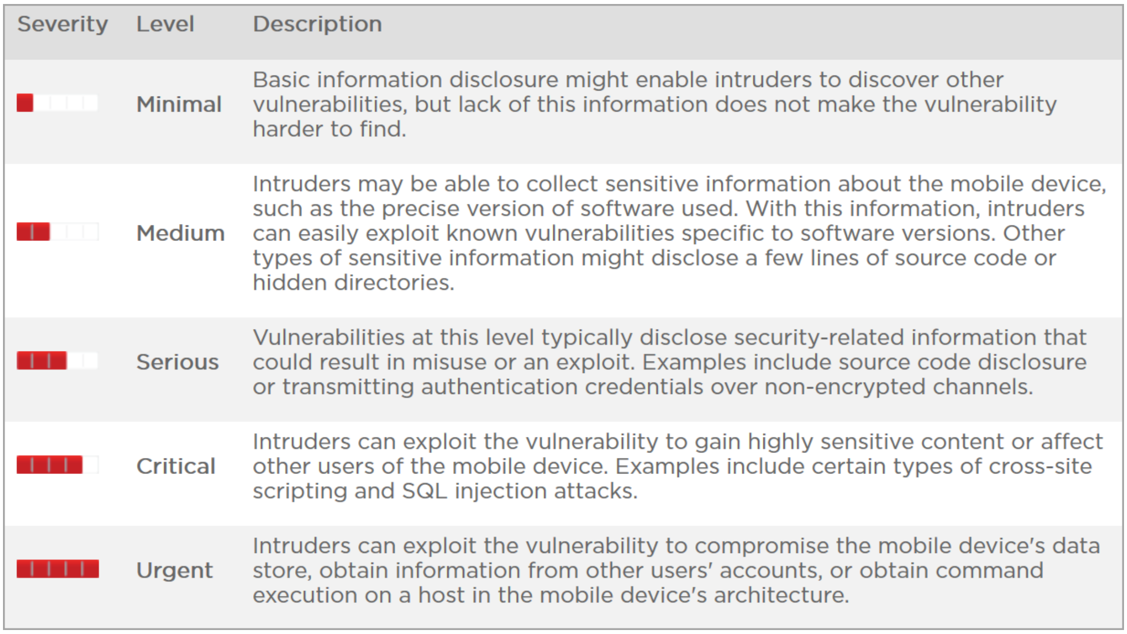
- Malware: Displays any published malware, where you can assess its malware family and risk

Tell me about Severity Levels

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

Confirmed Vulnerabilities

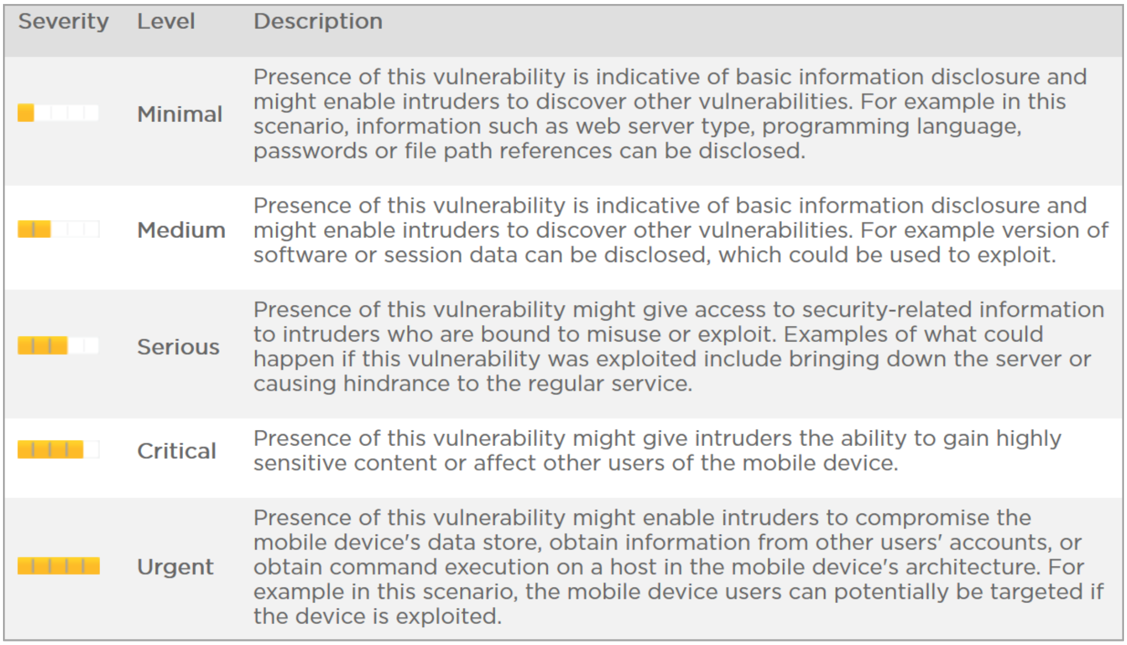
Confirmed vulnerabilities (QIDs) are the design flaws, programming errors, or misconfigurations that make your mobile device susceptible to malicious attacks. Depending on the level of the security risk, the successful exploitation of a confirmed vulnerability can vary from the disclosure of information to a complete compromise of the mobile device. Even if the device isn't fully compromised, an exploited confirmed vulnerability could still lead to the mobile devices 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

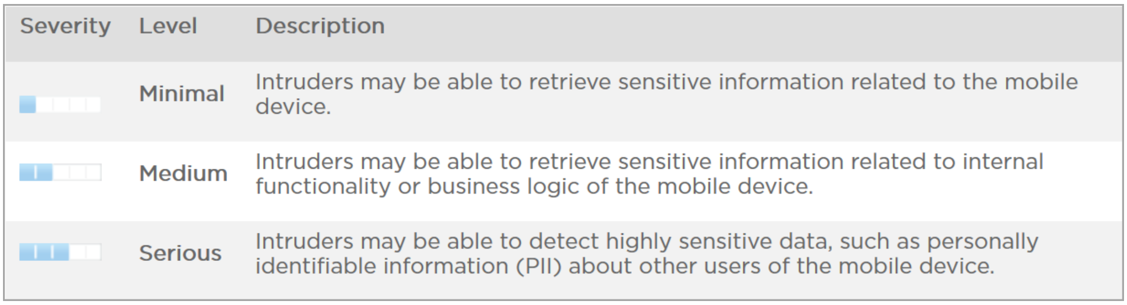
Potential Vulnerabilities indicate the observation of a weakness or error commonly used to attack a mobile device are unable to confirm if the weakness or error could be exploited. Where possible, the QID's description and results section include information and hints for following up with manual analysis.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

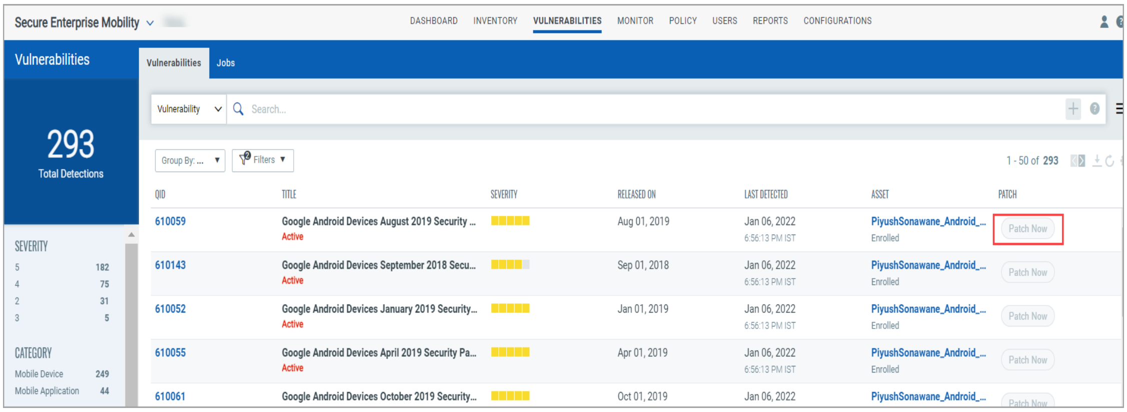
Active - A vulnerability detected by two or more scans is set to Active.

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

Reopened - The most recent scan reopened a vulnerability, 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 the **Patch Now** option. The **Patch Now** button will be enabled only for the patchable vulnerabilities. This option updates the application to the latest version.



293
Total Detections

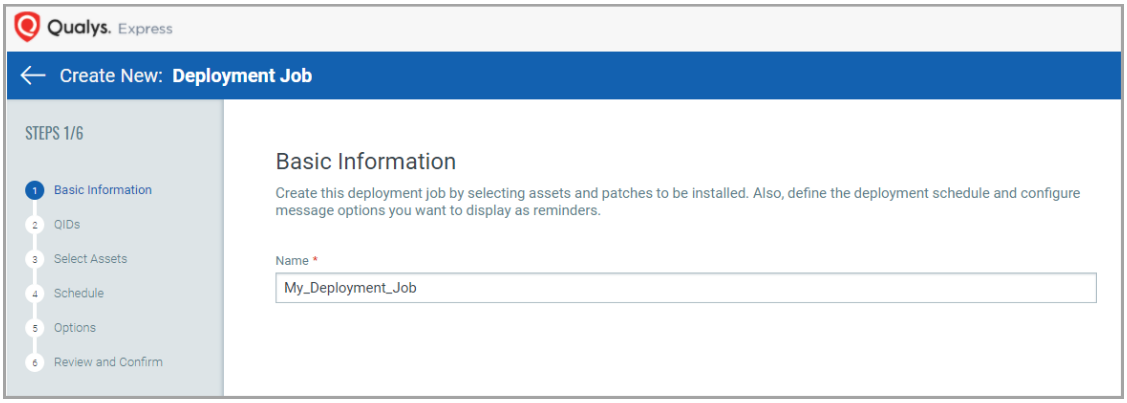
SEVERITY	
5	182
4	75
2	31
3	5

CATEGORY	
Mobile Device	249
Mobile Application	44

1 - 50 of 293

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

Click **Patch Now** to update the particular application. This opens the **Deployment Job** wizard.



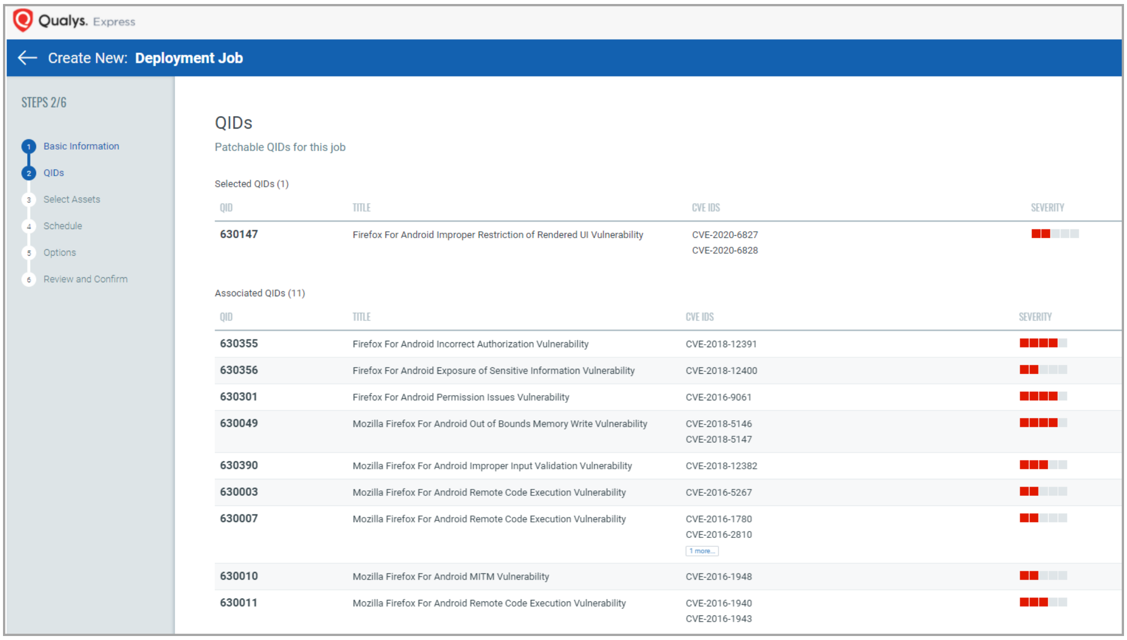
Basic Information

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 *

My_Deployment_Job

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



QIDs

Patchable QIDs for this job

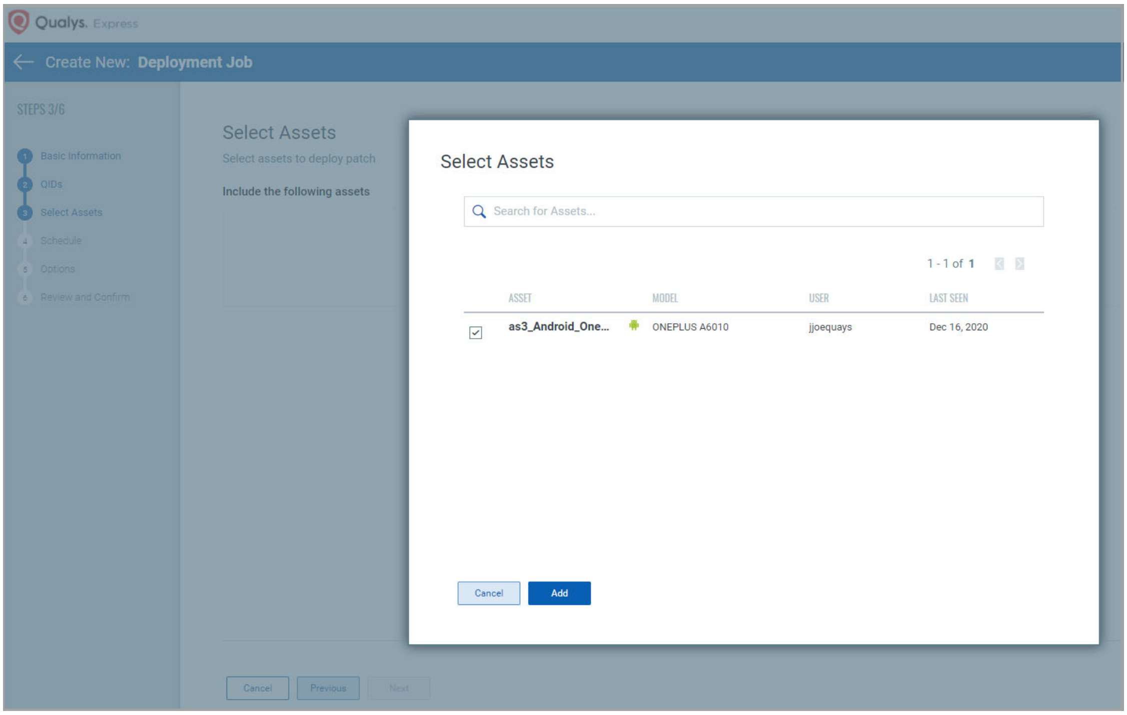
Selected QIDs (1)

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 the selected QIDs and the associated QIDs. Click **Next**.



Select Assets

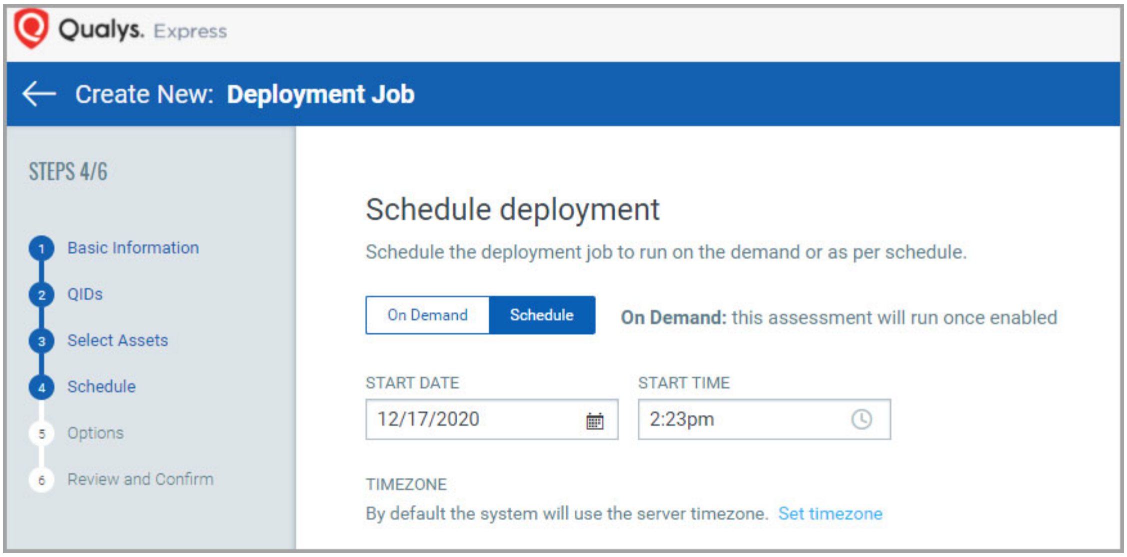
Search for Assets...

1 - 1 of 1

	ASSET	MODEL	USER	LAST SEEN
☑	as3_Android_One...	ONEPLUS A6010	jjoequays	Dec 16, 2020

Cancel Add

Click **Select Assets** and select the assets you need to apply patches. Click **Add** to add the selected assets, and then click **Next**.



Schedule deployment

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

On Demand: this assessment will run once enabled

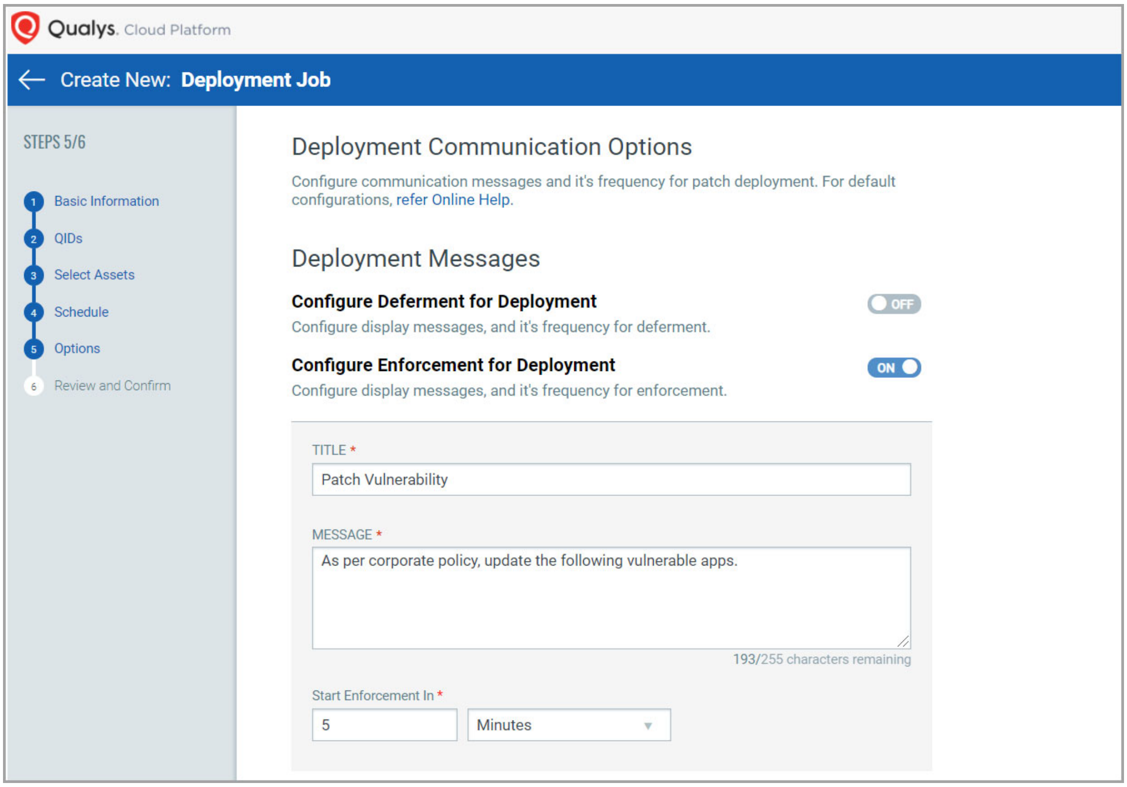
START DATE: 12/17/2020

START TIME: 2:23pm

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 the future. Click **Next**.



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 OFF

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

Configure Enforcement for Deployment ON

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

TITLE *: Patch Vulnerability

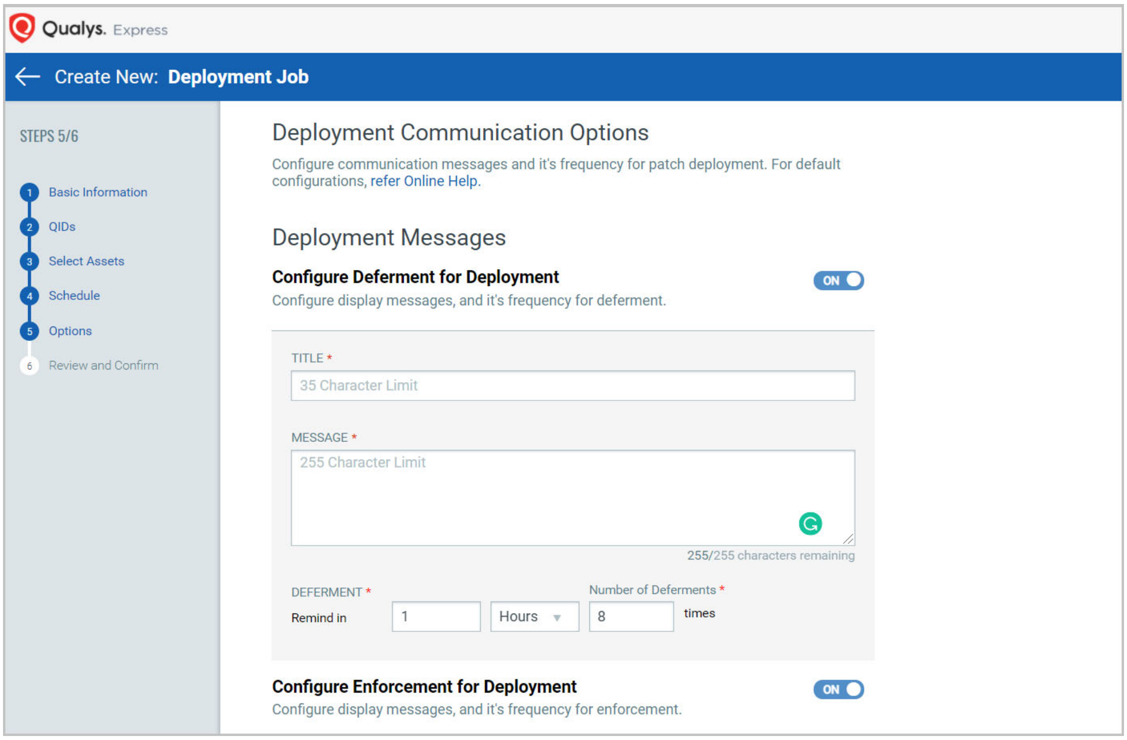
MESSAGE *: As per corporate policy, update the following vulnerable apps.

193/255 characters remaining

Start Enforcement In *: 5 Minutes

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

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



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 1 Hours

Number of Deferments * 8 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 the **Configure Deferment for Deployment** option, you need to configure the title, message, deferment, and the number of deferments.

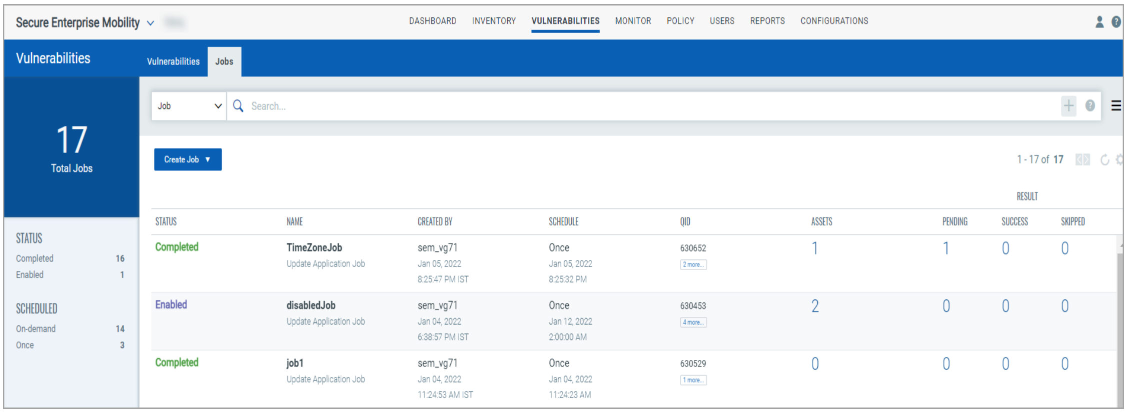
If you don't configure the deferment, the default title and message will be displayed. The default deferment is reminded after every 1 hour and for a maximum of 8 times before enforcement.

If you don't configure both deferment and enforcement, the 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 the deployment job.

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



17
Total Jobs

STATUS

Completed	16
Enabled	1

SCHEDULED

On-demand	14
Once	3

1 - 17 of 17

						RESULT		
STATUS	NAME	CREATED BY	SCHEDULE	QID	ASSETS	PENDING	SUCCESS	SKIPPED
Completed	TimeZoneJob Update Application Job	sem_vg71 Jan 05, 2022 8:25:47 PM IST	Once Jan 05, 2022 8:25:32 PM	630652 2 more...	1	1	0	0
Enabled	disabledJob Update Application Job	sem_vg71 Jan 04, 2022 6:38:57 PM IST	Once Jan 12, 2022 2:00:00 AM	630453 4 more...	2	0	0	0
Completed	job1 Update Application Job	sem_vg71 Jan 04, 2022 11:24:53 AM IST	Once Jan 04, 2022 11:24:23 AM	630529 1 more...	0	0	0	0

Job status shows various statuses for deployment jobs.

Configuration Assessment for Mobile Devices

You can perform the configuration evaluation against best practices for the Android and iOS platforms. Currently, most of the configuration details are collected in SEM. 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 help you take necessary 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.

Policy Actions

Qualys SEM provides some default out-of-the-box policies for Android and iOS platforms.

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 is displayed.

These policies are associated with every asset that is enrolled in SEM. 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 SEM.

You can perform the following actions on a Policy:

- Create a policy: create customized policies for Android and iOS platforms for required controls and associate them with assets to evaluate them later.

- View a policy: view details of a policy anytime.

- Edit a policy: edit a policy to update any details, assets, or controls information.

- Deactivate a policy: deactivate an active policy.

- Delete a policy: delete an existing policy.

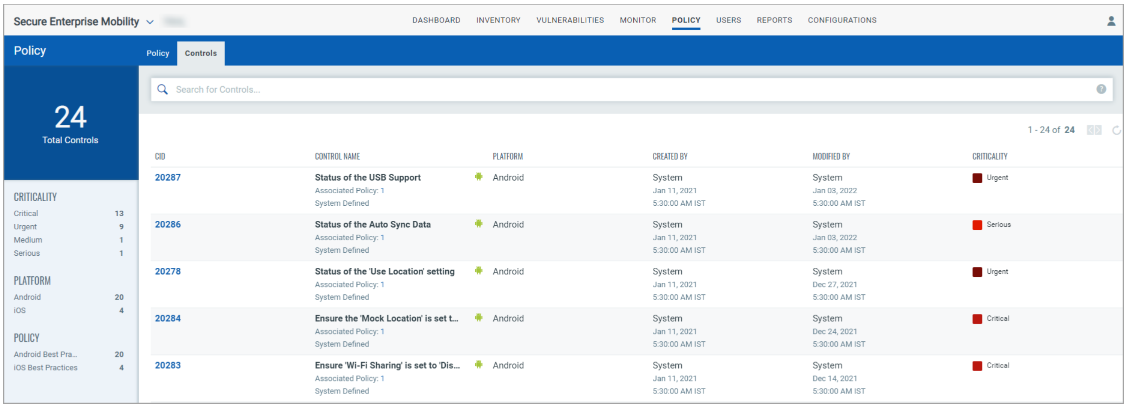
- Evaluate a policy: evaluate an existing active policy.

- Activate a policy: activate an inactive policy.

For more information and detailed steps, refer to the **Policy Actions** section in the Online Help.

Monitor Controls

Every policy has one or more controls assigned to it. The 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 is displayed. SEM supports system-defined controls. The **Policy** > **Controls** sub-tab lists all controls and their details, such as control name, platform, the criticality of the control and so on.



24
Total Controls

CRITICALITY

Critical	13
Urgent	9
Medium	1
Serious	1

PLATFORM

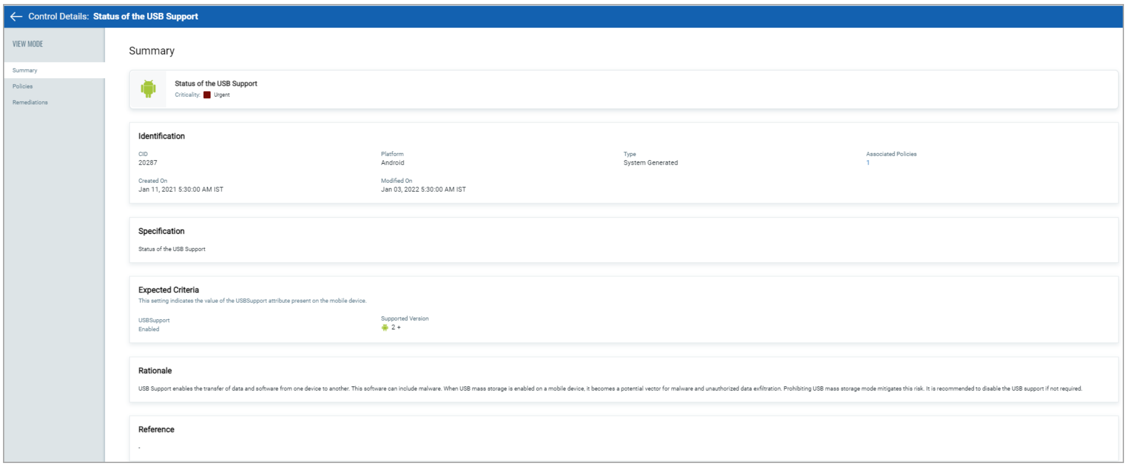
Android	20
iOS	4

POLICY

Android Best Pra...	20
iOS Best Practices	4

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 t... 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 'Dis... 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.



Summary

Status of the USB Support
Criticality: ■ Urgent

Identification

CID: 20287
Platform: Android
Type: System Generated
Associated Policies: 1
Created On: Jan 11, 2021 5:30:00 AM IST
Modified On: Jan 03, 2022 5:30:00 AM IST

Specification

Status of the USB Support

Expected Criteria

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

USBSupport: Enabled
Supported Version: 2 +

Rationale

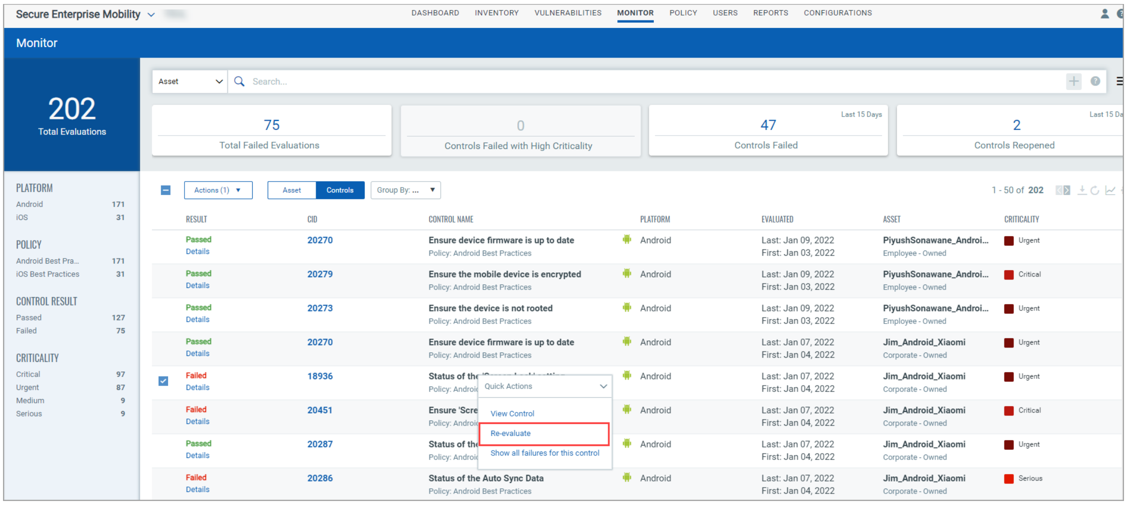
USB Support enables the transfer of data and software from one device to another. This software can include malware. When USB mass storage is enabled on a mobile device, it becomes a potential vector for malware and unauthorized data exfiltration. Prohibiting USB mass storage mode mitigates this risk.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

Reference

-

Re-evaluate Controls

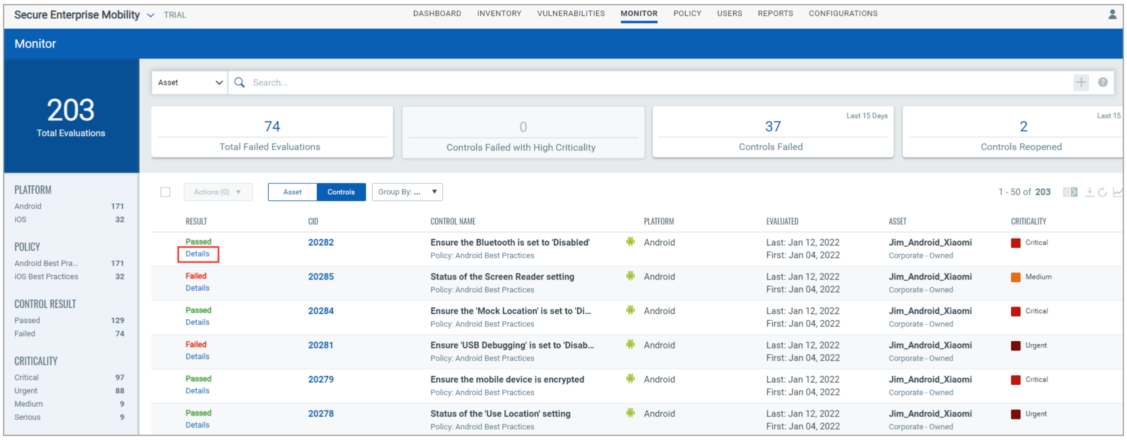
You can re-evaluate a control by selecting the **Quick Actions** menu next to the control name and clicking **Re-evaluate**.



	RESULT	CID	CONTROL NAME	PLATFORM	EVALUATED	ASSET	CRITICALITY
	Passed Details	20270	Ensure device firmware is up to date Policy: Android Best Practices	Android	Last: Jan 09, 2022 First: Jan 03, 2022	PiyushSonawane_Androi... Employee - Owned	Urgent
	Passed Details	20279	Ensure the mobile device is encrypted Policy: Android Best Practices	Android	Last: Jan 09, 2022 First: Jan 03, 2022	PiyushSonawane_Androi... Employee - Owned	Critical
	Passed Details	20273	Ensure the device is not rooted Policy: Android Best Practices	Android	Last: Jan 09, 2022 First: Jan 03, 2022	PiyushSonawane_Androi... Employee - Owned	Urgent
	Passed Details	20270	Ensure device firmware is up to date Policy: Android Best Practices	Android	Last: Jan 07, 2022 First: Jan 04, 2022	Jim_Android_Xiaomi Corporate - Owned	Urgent
☑	Failed Details	18936	Status of the Policy: Androi	Android	Last: Jan 07, 2022 First: Jan 04, 2022	Jim_Android_Xiaomi Corporate - Owned	Urgent
	Failed Details	20451	Ensure 'Scre Policy: Androi	Android	Last: Jan 07, 2022 First: Jan 04, 2022	Jim_Android_Xiaomi Corporate - Owned	Critical
	Passed Details	20287	Status of the Policy: Androi	Android	Last: Jan 07, 2022 First: Jan 04, 2022	Jim_Android_Xiaomi Corporate - Owned	Urgent
	Failed Details	20286	Status of the Auto Sync Data Policy: Android Best Practices	Android	Last: Jan 07, 2022 First: Jan 04, 2022	Jim_Android_Xiaomi Corporate - Owned	Serious

After the re-evaluation, 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.



203
Total Evaluations

74
Total Failed Evaluations

0
Controls Failed with High Criticality

Last 15 Days
37
Controls Failed

Last 15
2
Controls Reopened

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

1 - 50 of 203

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

Monitor Assets

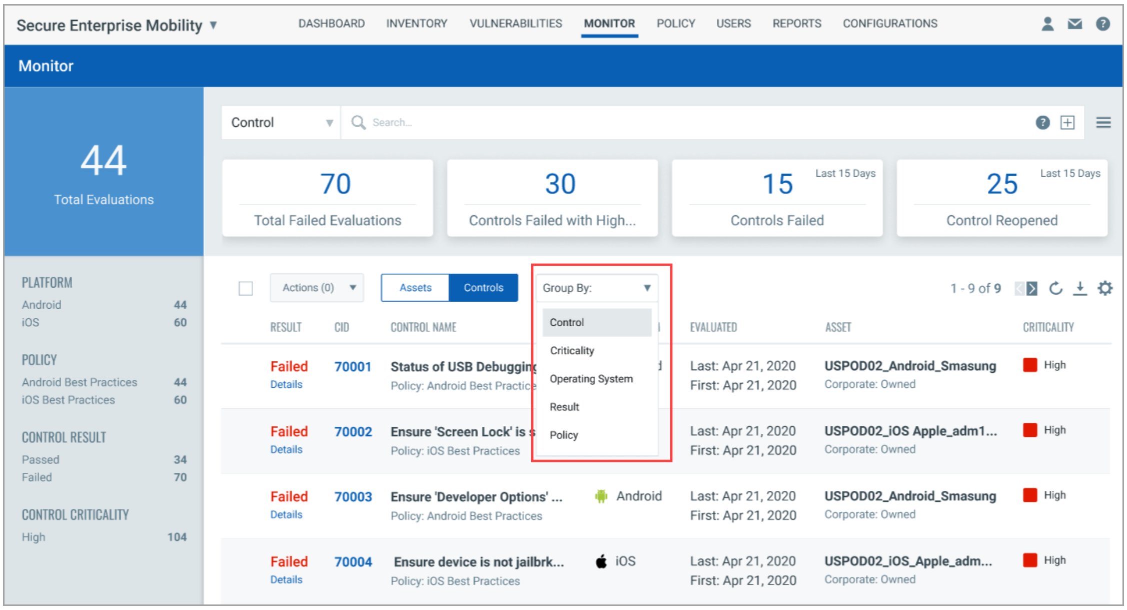
In the **Monitor** tab, you can monitor your compliance posture in real-time for each asset. Go to the **Monitor** > **Assets** sub-tab to view details such as asset, model, and evaluation status at a quick glance.

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

The controls are validated, and the **Controls** sub-tab displays the pass or fail status.

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 a specific selection.



44 Total Evaluations

70	30	15 (Last 15 Days)	25 (Last 15 Days)
Total Failed Evaluations	Controls Failed with High...	Controls Failed	Control Reopened

PLATFORM	
Android	44
iOS	60
POLICY	
Android Best Practices	44
iOS Best Practices	60
CONTROL RESULT	
Passed	34
Failed	70
CONTROL CRITICALITY	
High	104

1 - 9 of 9

RESULT	CID	CONTROL NAME		EVALUATED	ASSET	CRITICALITY
Failed Details	70001	Status of USB Debuggin Policy: Android Best Practice		Last: Apr 21, 2020 First: Apr 21, 2020	USPOD02_Android_Smasung Corporate: Owned	🟥 High
Failed Details	70002	Ensure 'Screen Lock' is s Policy: iOS Best Practices		Last: Apr 21, 2020 First: Apr 21, 2020	USPOD02_iOS Apple_adm1... Corporate: Owned	🟥 High
Failed Details	70003	Ensure 'Developer Options' ... Policy: Android Best Practices	Android	Last: Apr 21, 2020 First: Apr 21, 2020	USPOD02_Android_Smasung Corporate: Owned	🟥 High
Failed Details	70004	Ensure device is not jailbrk... Policy: iOS Best Practices	iOS	Last: Apr 21, 2020 First: Apr 21, 2020	USPOD02_iOS_Apple_adm... Corporate: Owned	🟥 High

Dashboards and Reports

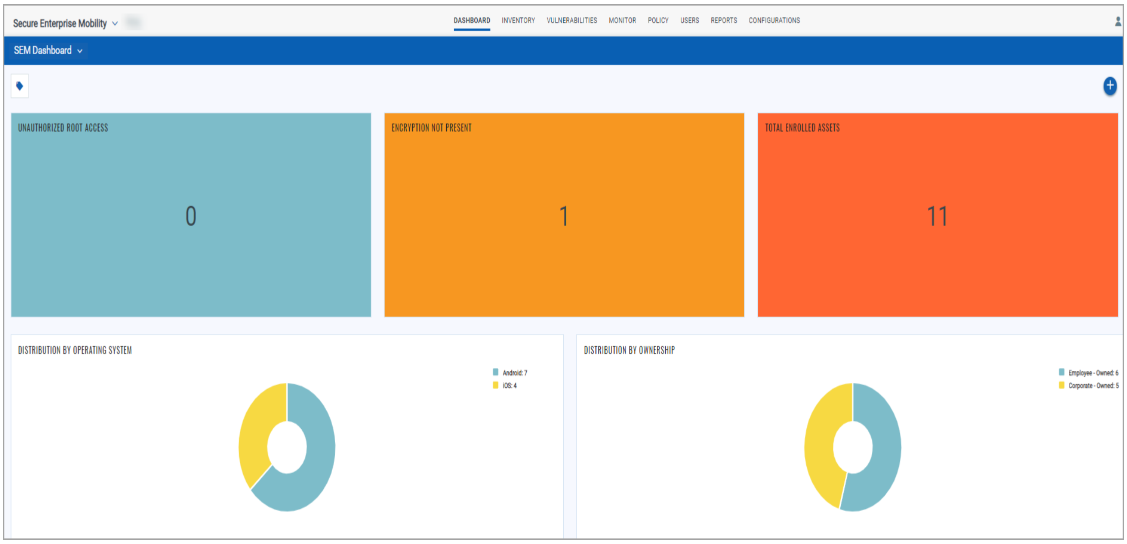
This section helps you monitor and analyze various dashboards and reports for the mobile assets. Once device enrollment is complete, you can configure various dashboards to view mobile asset's data and their details.

Dashboards

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

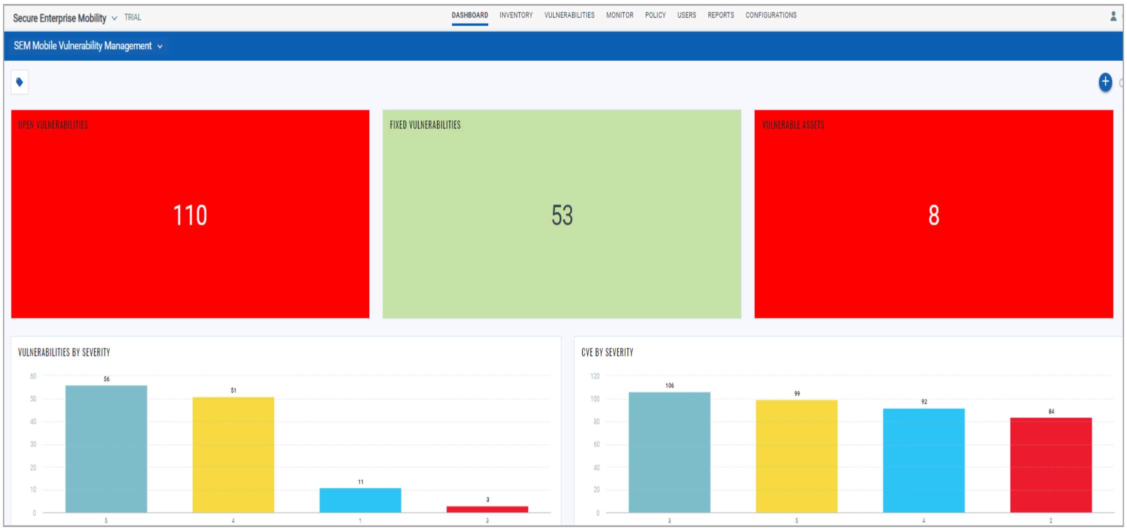
Get Started with SEM Dashboard

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



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

Select the **SEM Mobile Vulnerability Management** template.

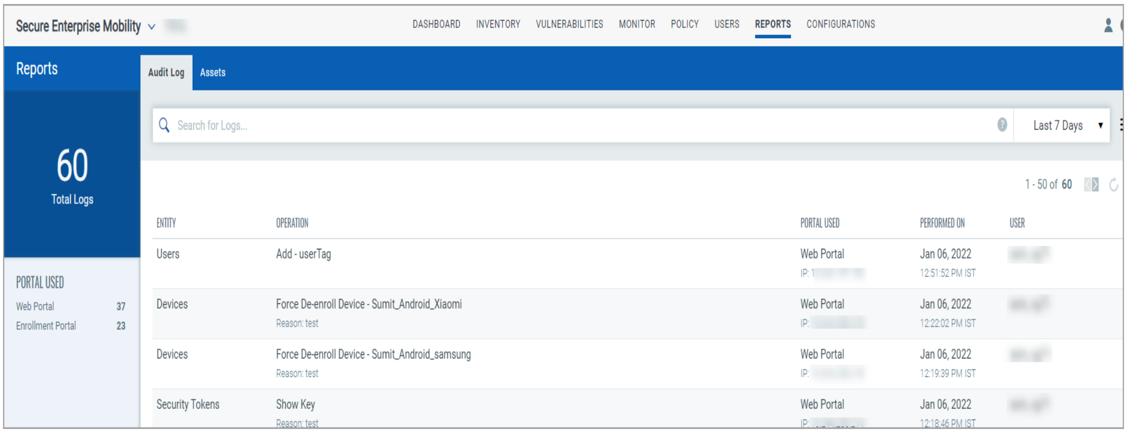


VM dashboard template provides complete visibility of mobile vulnerabilities.

Reports

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

Go to the **Reports** tab to analyze various audit logs in audit log reports related to device enrollment and user configurations.



60
Total Logs

PORTAL USED

Web Portal	37
Enrollment Portal	23

ENTITY	OPERATION	PORTAL USED	PERFORMED ON	USER
Users	Add - userTag	Web Portal IP: 1[redacted]	Jan 06, 2022 12:51:52 PM IST	[redacted]
Devices	Force De-enroll Device - Sumit_Android_Xiaomi Reason: test	Web Portal IP: [redacted]	Jan 06, 2022 12:22:02 PM IST	[redacted]
Devices	Force De-enroll Device - Sumit_Android_samsung Reason: test	Web Portal IP: [redacted]	Jan 06, 2022 12:19:39 PM IST	[redacted]
Security Tokens	Show Key Reason: test	Web Portal IP: [redacted]	Jan 06, 2022 12:18:46 PM IST	[redacted]

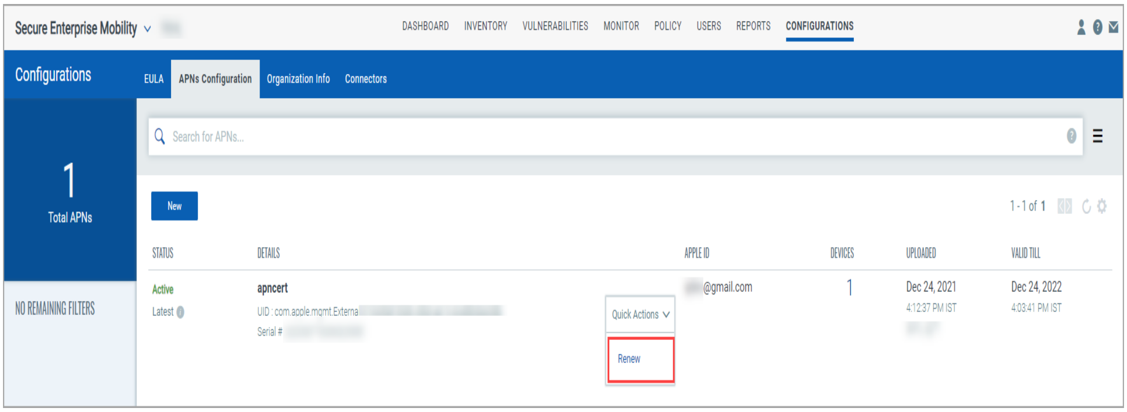
Appendix

Renew APNs Certificate

The validity of the APNs certificate is 365 days, so the administrator must renew the certificate after every 365 days. The Qualys SEM Portal notifies the administrator when the certificate expires 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, resulting in the administrator having to manually de-enroll and then re-enroll all Apple devices in the system again.

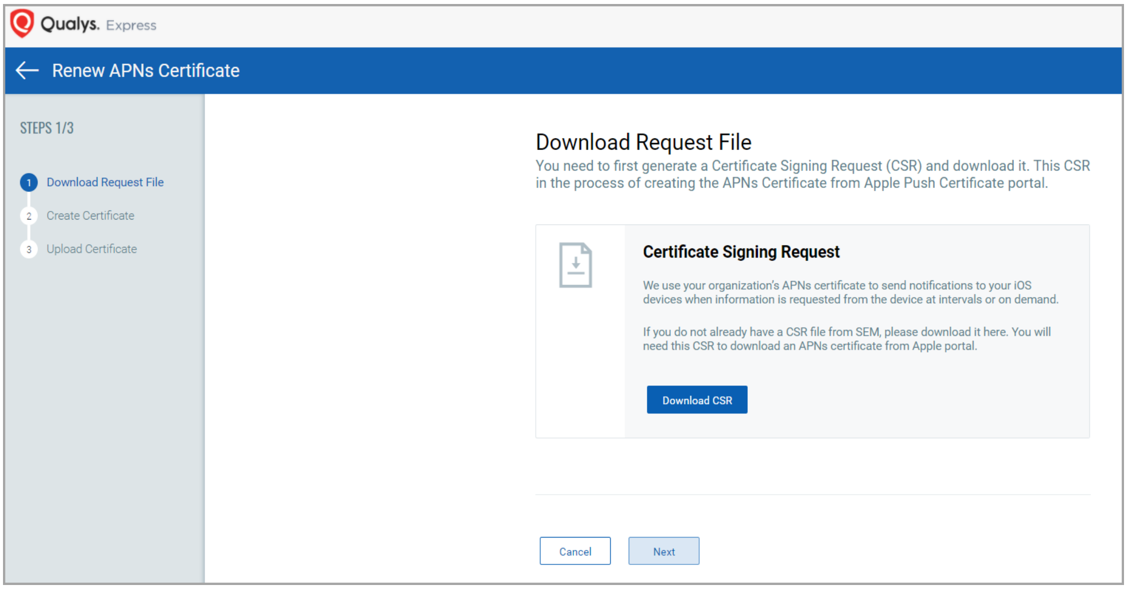
Steps to renew APNs certificate:

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



STATUS	DETAILS	APPLE ID	DEVICES	UPLOADED	VALID TILL
Active Latest	apncert UID : com.apple.mgmt.Externa[redacted] Serial # [redacted]	[redacted]@gmail.com	1	Dec 24, 2021 4:12:37 PM IST [redacted]	Dec 24, 2022 4:03:41 PM IST

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



Qualys. Express

Renew APNs Certificate

STEPS 1/3

1 Download Request File
2 Create Certificate
3 Upload Certificate

Download Request File

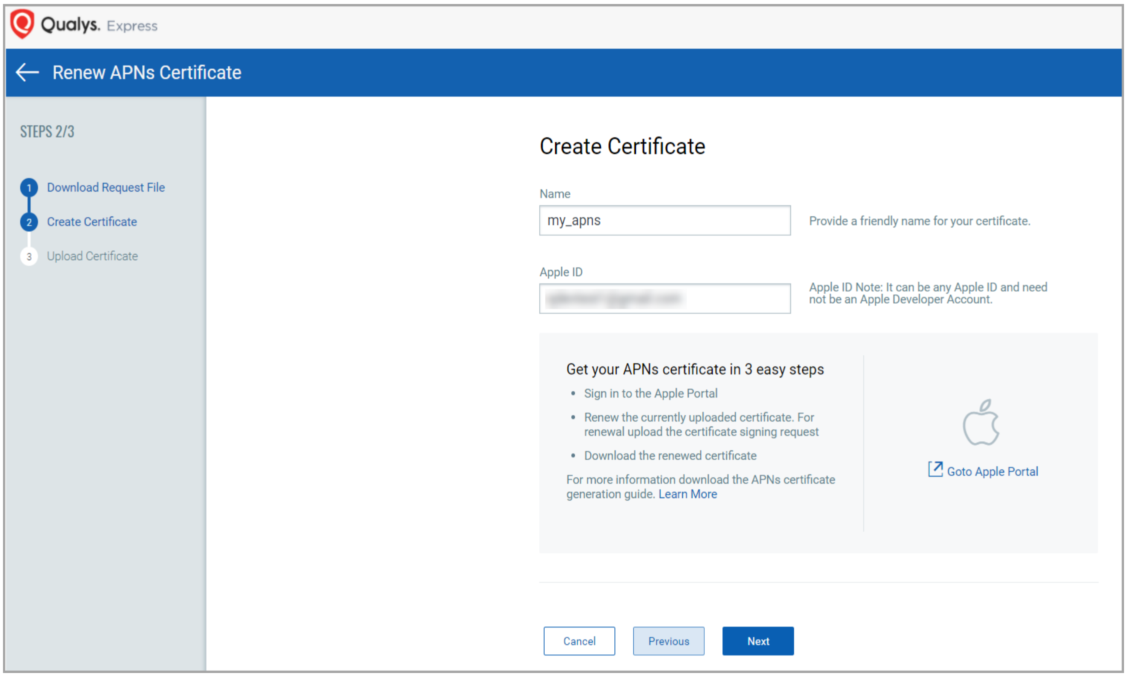
You need to first generate a Certificate Signing Request (CSR) and download it. This CSR in the process of creating the APNs Certificate from Apple Push Certificate portal.

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 SEM, please download it here. You will need this CSR to download an APNs certificate from Apple portal.

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



Qualys. Express

Renew APNs Certificate

STEPS 2/3

1 Download Request File
2 Create Certificate
3 Upload Certificate

Create Certificate

Name: my_apns

Provide a friendly name for your certificate.

Apple ID: [redacted]

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

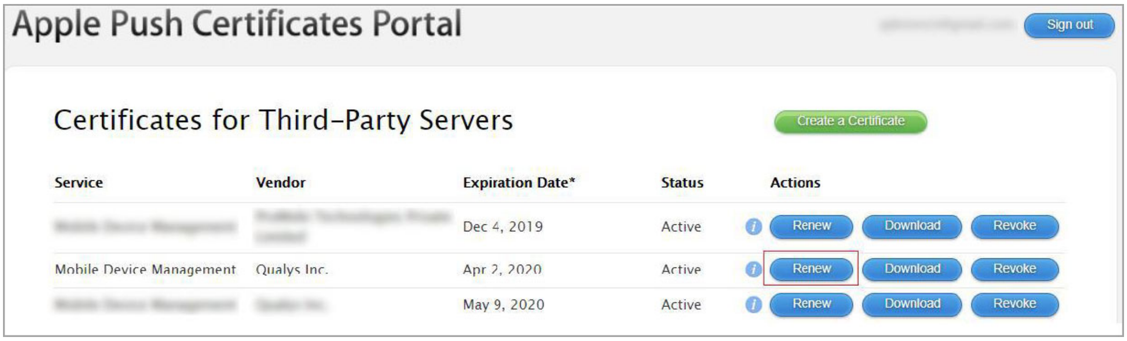
- Sign in to the Apple Portal
- Renew the currently uploaded certificate. For renewal upload the certificate signing request
- Download the renewed certificate

For more information download the APNs certificate generation guide. Learn More

4) Login to Apple Push Certificate Portal using the same Apple ID and password that you used to create the APNs certificate. Locate the APNs certificate 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.



Apple Push Certificates Portal

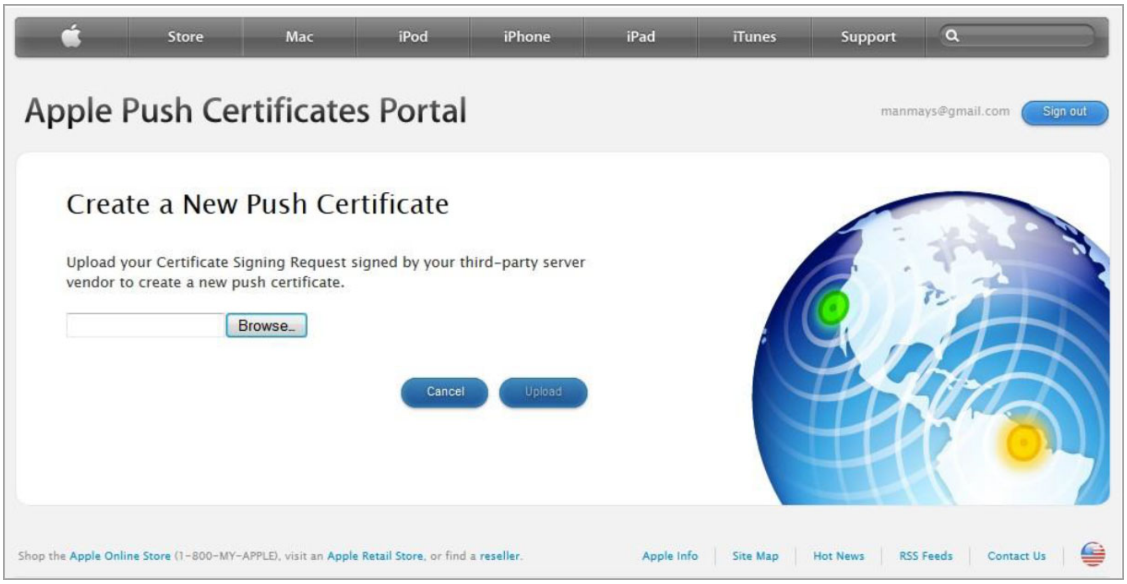
[redacted] Sign out

Certificates for Third-Party Servers

Create a Certificate

Service	Vendor	Expiration Date*	Status	Actions
[redacted]	[redacted]	Dec 4, 2019	Active	Renew Download Revoke
Mobile Device Management	Qualys Inc.	Apr 2, 2020	Active	Renew Download Revoke
[redacted]	[redacted]	May 9, 2020	Active	Renew Download Revoke

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



Apple Push Certificates Portal

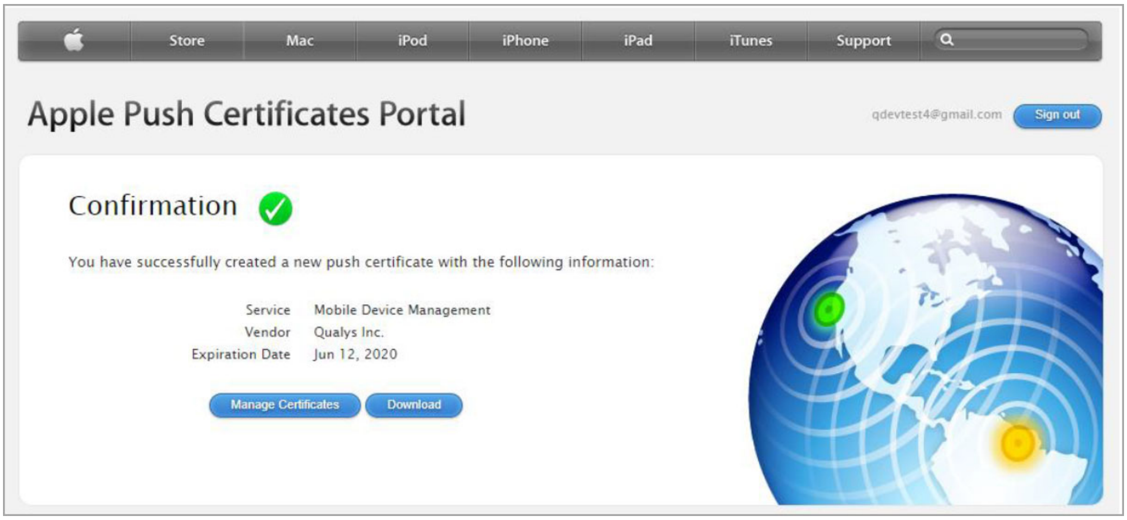
manmays@gmail.com Sign out

Create a New Push Certificate

Upload your Certificate Signing Request signed by your third-party server vendor to create a new push certificate.

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

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



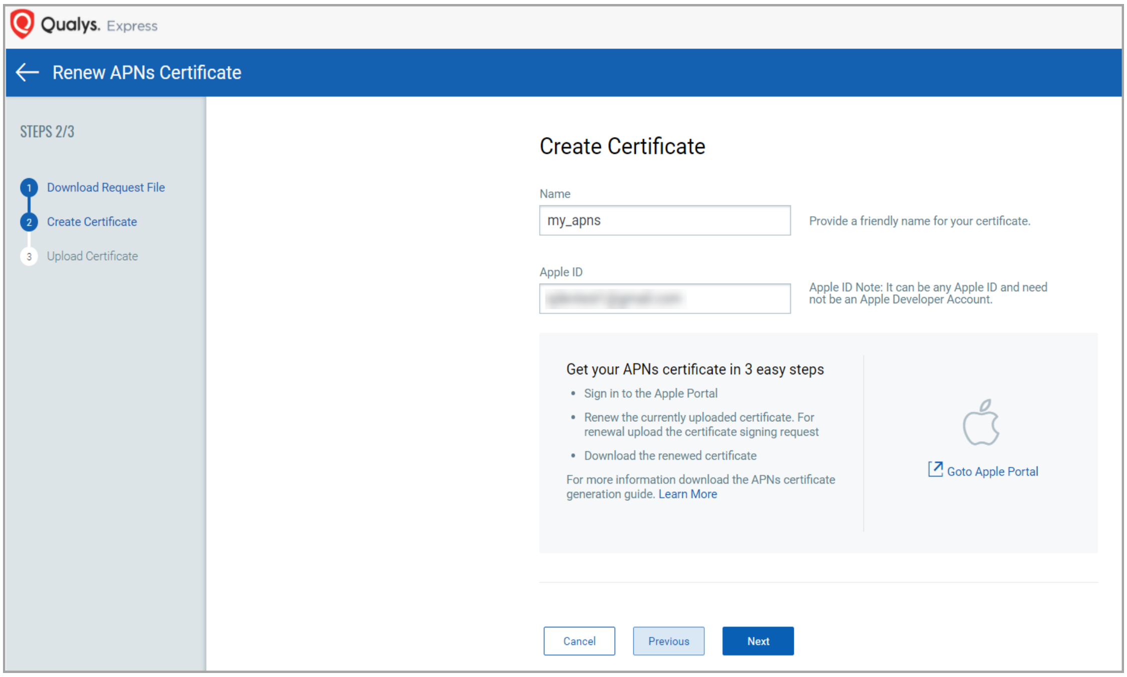
Apple Push Certificates Portal

Confirmation ✓

You have successfully created a new push certificate with the following information:

Service	Mobile Device Management
Vendor	Qualys Inc.
Expiration Date	Jun 12, 2020

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



Create Certificate

Name

my_apns

Provide a friendly name for your certificate.

Apple ID

[redacted]

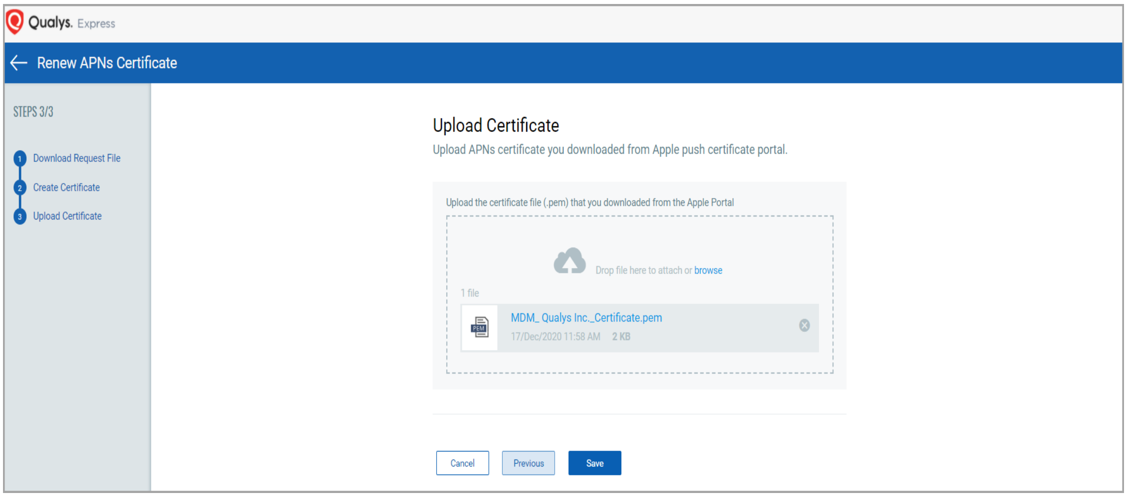
Apple ID Note: It can be any Apple ID and need not be an Apple Developer Account.

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

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



Upload Certificate

Upload APNs certificate you downloaded from Apple push certificate portal.

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

MDM_ Qualys Inc._Certificate.pem
17/Dec/2020 11:58 AM 2 KB

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.