Apple's Rapid Security Response Software Updates

What

Apple is known for its high standards of security and privacy for its users. However, no system is perfect and vulnerabilities can still be found and exploited by malicious actors. That's why Apple has developed a Rapid Security Response (RSR) process that allows it to quickly identify, fix and deploy security updates to its devices.

What is RSR?

Rapid Security Response (RSR) is a method for deploying security fixes to users more frequently. RSR is a process that Apple follows when it becomes aware of a security issue that affects its products or platforms. It involves four main steps:

- Investigation: Apple's security team analyzes the issue and determines its severity, impact and scope.
- Mitigation: Apple's engineers work on developing a patch or workaround to address the issue and prevent further exploitation.
- Testing: Apple's quality assurance team tests the patch or workaround to ensure it works as intended and does not introduce new problems.
- Deployment: Apple's release team distributes the patch or workaround to its users via software updates, security bulletins or other channels.

When/Why

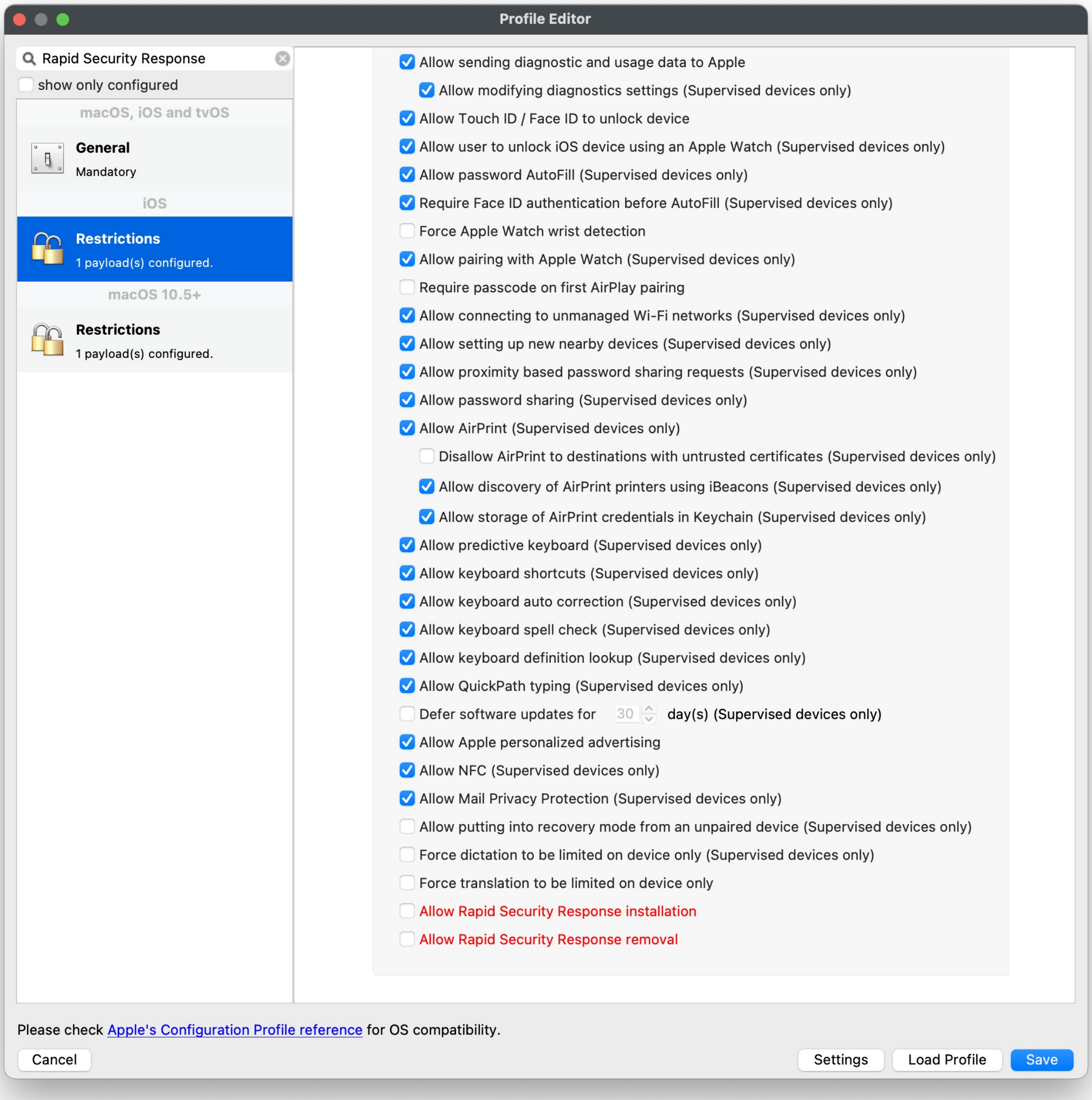
RSR is important because it helps Apple protect its users from potential harm caused by security breaches.

Rapid Security Responses don’t adhere to the managed software update delay; however, because they apply only to the latest minor operating system version, if that minor operating system update is delayed, the response is also effectively delayed. If necessary, the user can also remove the responses.

If a device is using the latest operating system and there is a Rapid Security Response available, AvailableOSUpdates returns the response. The MDM sends a command to install the response. Note that an MDM can only install the response on devices using the latest minor version.

How

RSR works by leveraging Apple's resources, such as configuration profiles. There are options within macOS and iOS/iPadOS Restrictions payload to allow the installation and removal of these Rapid Security Response updates. Screen shots below for reference:



☑ Allow sending diagnostic and usage data to Apple

- ☑ Allow modifying diagnostics settings (Supervised devices only)

☑ Allow Touch ID / Face ID to unlock device

☑ Allow user to unlock iOS device using an Apple Watch (Supervised devices only)

☑ Allow password AutoFill (Supervised devices only)

☑ Require Face ID authentication before AutoFill (Supervised devices only)

☐ Force Apple Watch wrist detection

☑ Allow pairing with Apple Watch (Supervised devices only)

☐ Require passcode on first AirPlay pairing

☑ Allow connecting to unmanaged Wi-Fi networks (Supervised devices only)

☑ Allow setting up new nearby devices (Supervised devices only)

☑ Allow proximity based password sharing requests (Supervised devices only)

☑ Allow password sharing (Supervised devices only)

☑ Allow AirPrint (Supervised devices only)

- ☐ Disallow AirPrint to destinations with untrusted certificates (Supervised devices only)
- ☑ Allow discovery of AirPrint printers using iBeacons (Supervised devices only)
- ☑ Allow storage of AirPrint credentials in Keychain (Supervised devices only)

☑ Allow predictive keyboard (Supervised devices only)

☑ Allow keyboard shortcuts (Supervised devices only)

☑ Allow keyboard auto correction (Supervised devices only)

☑ Allow keyboard spell check (Supervised devices only)

☑ Allow keyboard definition lookup (Supervised devices only)

☑ Allow QuickPath typing (Supervised devices only)

☐ Defer software updates for 30 day(s) (Supervised devices only)

☑ Allow Apple personalized advertising

☑ Allow NFC (Supervised devices only)

☑ Allow Mail Privacy Protection (Supervised devices only)

☐ Allow putting into recovery mode from an unpaired device (Supervised devices only)

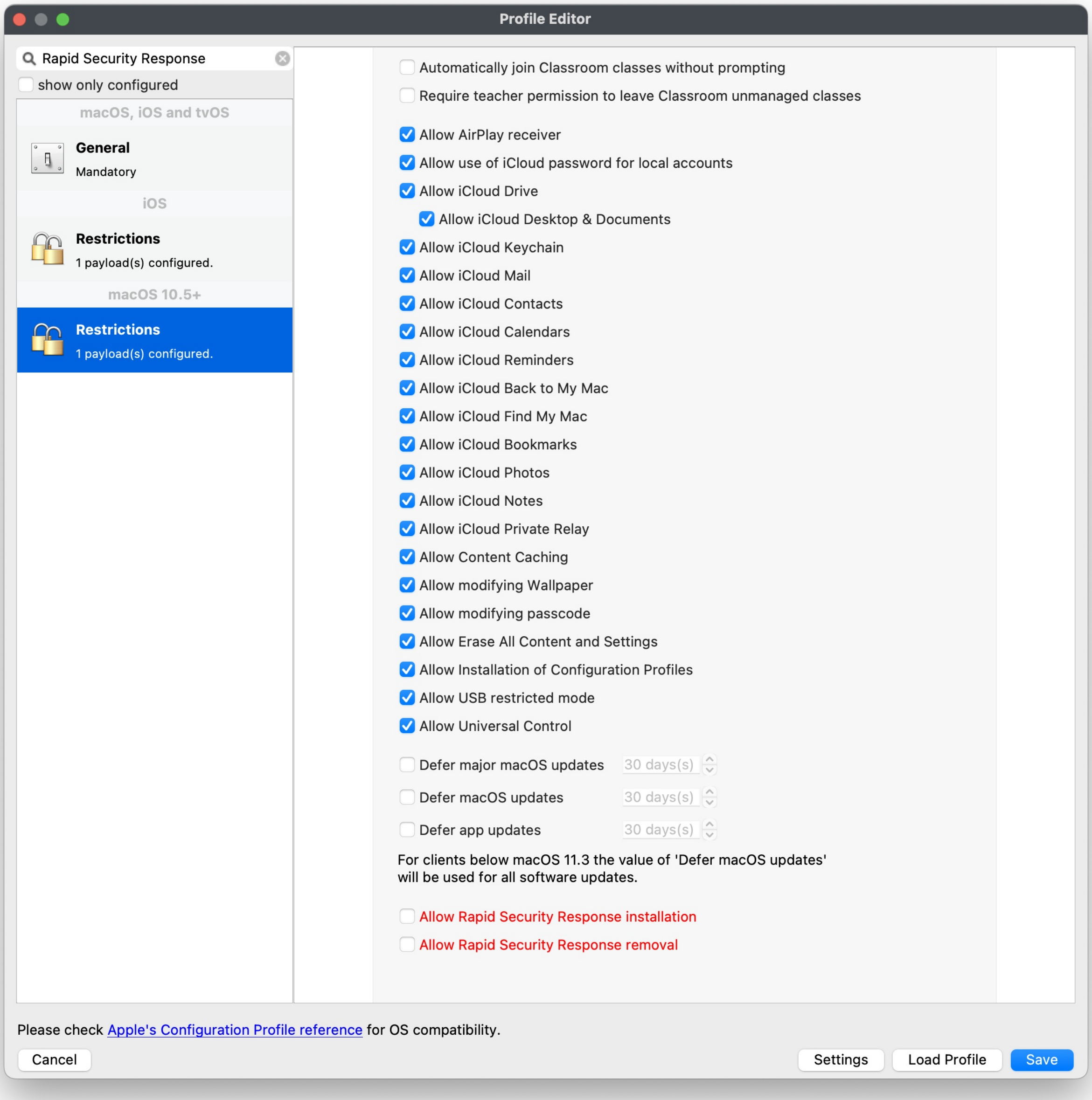
☐ Force dictation to be limited on device only (Supervised devices only)

☐ Force translation to be limited on device only

☐ Allow Rapid Security Response installation

☐ Allow Rapid Security Response removal

Please check Apple's Configuration Profile reference for OS compatibility.



□ Automatically join Classroom classes without prompting
□ Require teacher permission to leave Classroom unmanaged classes

☑ Allow AirPlay receiver
☑ Allow use of iCloud password for local accounts
☑ Allow iCloud Drive
 ☑ Allow iCloud Desktop & Documents
☑ Allow iCloud Keychain
☑ Allow iCloud Mail
☑ Allow iCloud Contacts
☑ Allow iCloud Calendars
☑ Allow iCloud Reminders
☑ Allow iCloud Back to My Mac
☑ Allow iCloud Find My Mac
☑ Allow iCloud Bookmarks
☑ Allow iCloud Photos
☑ Allow iCloud Notes
☑ Allow iCloud Private Relay
☑ Allow Content Caching
☑ Allow modifying Wallpaper
☑ Allow modifying passcode
☑ Allow Erase All Content and Settings
☑ Allow Installation of Configuration Profiles
☑ Allow USB restricted mode
☑ Allow Universal Control

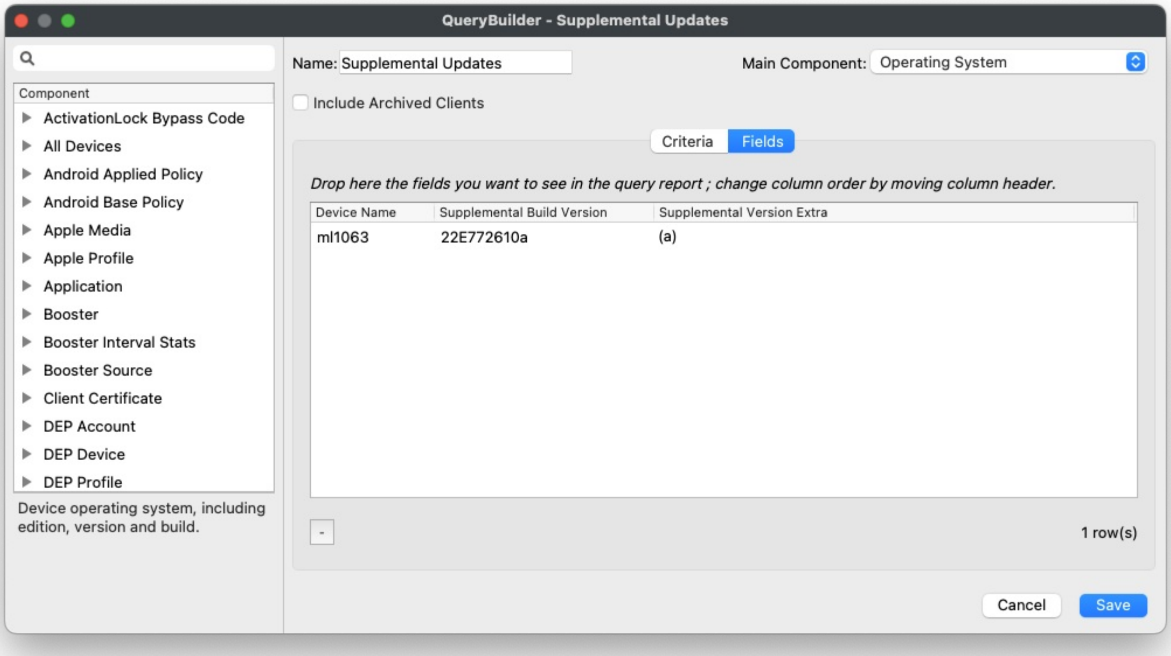
□ Defer major macOS updates 30 days(s)
□ Defer macOS updates 30 days(s)
□ Defer app updates 30 days(s)

For clients below macOS 11.3 the value of 'Defer macOS updates' will be used for all software updates.

□ Allow Rapid Security Response installation
□ Allow Rapid Security Response removal

Please check Apple's Configuration Profile reference for OS compatibility.

As of FileWave 15, there are two additional Inventory Items relating to Rapid Security Response; both labelled as Supplemental:



Name: Supplemental Updates

Main Component: Operating System

□ Include Archived Clients

Device operating system, including edition, version and build.

Drop here the fields you want to see in the query report ; change column order by moving column header.

Device Name	Supplemental Build Version	Supplemental Version Extra
ml1063	22E772610a	(a)

1 row(s)

Note, Supplemental Build Version will only show a value if there is a current RSR installed on a device. Once a device updates to the next macOS version, that has no RSR installed, these two inventory items will become blank again.

Related Content

For Apple documentation regarding Rapid Security Response Updates:

- Manage Rapid Security Responses on Apple devices
- Use MDM to deploy software updates to Apple devices

Revision #5
★Created 8 June 2023 16:04:17 by Andrew Kloosterhuis
Updated 11 April 2024 17:04:14 by Josh Levitsky