Apple OS Updates Process

This document provides an overview of the Apple OS update process. Last updated: 02/2023.

Contents

Apple OS Native OS Process and Documentation

Apple provides documentation on how users can manually and automatically install operating systems updates on their device. Also provides information about the updates.

- About software updates for Apple devices - Apple Support
    - Although Apple limits it's documentation about when they push updates, they have commented in the past about staggering updates to provide additional layer of protection to update servers but also a safeguard if early adopters report serious issues. There has been several occasions Apple has needed to pull back an update and quickly release a new update.
- Update your iPhone or iPad - Apple Support
- Apple security updates - Apple Support
- About iOS 16 Updates - Apple Support

Intune OS Update and Delay Capabilities

Intune can delay and push up Apple updates due to capabilities made available to MDMs by Apple.

- Use MDM to deploy software updates to Apple devices - Apple Support
- Learn about managed software updates - Apple Support (CA)
- Use Microsoft Intune policies to manage iOS/iPadOS software updates | Microsoft Learn

Baseline Configurations

Baseline configurations listed were derived from the Statewide Security Standards, the Security

Benchmarks from the Center for Internet Security (CIS Controls v8 IG 3), the CIS Apple iOS and iPadOS Benchmarks, and the enterprise security recommendations from Apple and Microsoft. Many of the baseline configurations are required due to dependencies that exist in the solution.

Category	Description	Basis for Control
iOS Software Updates	Newly released iOS/iPadOS software updates will be delayed to devices to allow for appropriate analysis and regression testing.	Recommended by Apple and Microsoft; Approach ensures balance between testing and security risk
	Agencies may provide a group of individuals to receive updates in advance of enterprise deployment to participate in analysis and regression testing.	Best practice, Recommended by Apple and Microsoft; Approach ensures balance between testing and security risk
	Intune will attempt to update devices that have fallen behind on major iOS updates during scheduled check-ins.	CIS Controls V8 4.1 “Establish and Maintain a Secure Configuration Process” CIS Controls V8 4.6 “Securely Manage Enterprise Assets and Software”.
	Zero-day updates will be pushed when deemed necessary to negate a security risk or a non-working critical capability.	CIS Controls V8 4.1 “Establish and Maintain a Secure Configuration Process” CIS Controls V8 4.6 “Securely Manage Enterprise Assets and Software”.

Additional Information

- Users and Technical staff are provided guides on the differences between User initiated updates, Apple automatic updates and Intune pushed updates. They also provide tips and troubleshooting information.
- Currently Intune is configured to delay iOS/iPadOS updates to 14 days. This provides a balance between mitigating security risk and impact to the business or device management.
- EIS has implemented an Intune testing group within each organization (agency, board, or committee) to receive the latest updates. This will allow them to test for business impacts (similar to windows update rings).
- It is not uncommon to have a few OS releases (or even revokes) in a short amount of time before it stabilizes. There is no rolling back which means we need to be following the recommendation as a default and we can choose to move faster when we need.
- EIS has dynamic Azure Active Directory groups looking for Apple devices on specified operating systems and has Intune attempt to update them. Agencies may need to

assist the user/device if the device is not updating. There are many factors why a device might not update such as power, network, storage space, last connectivity, operating system is unable to complete the request, password requirements etc.

Zero-Day Updates

Zero-days are vulnerabilities that are discovered and either actively leaked or exploited before the responsible vendor has had a chance to release a patch fixing the flaw.

- Enterprise managed devices may not be susceptible to zero-day vulnerabilities due to configured security settings and application review and deployment procedures. Every zero-day update should be reviewed and have a risk assessment completed by the organization unless otherwise instructed or communicated to by EIS.
- Organization accepts all risk when electing to update their devices ahead of the enterprise update schedule.
- If requested, an organization will be provided additional Azure AD Security Groups they can utilize to deploy updates ahead of the enterprise update schedule.
- EIS will leverage partnerships with Microsoft and Apple to review potential risk and impacts of zero-day updates based upon industry feedback and will provide recommendations and guidance as appropriate. Organization should not expect expedited turnaround due to delays with vendors.
- EIS will utilize standard change management processes and procedures if they determine that a zero day or other update should be deployed ahead of the enterprise update schedule for all enterprise managed mobile devices.
- Potential risks of early update deployment
    - Device may “brick” and become unusable until the operating system has been reinstalled using an Apple tool resulting in total data loss on the device.
    - Device may experience unexpected issues like loss of connectivity, loss of functionality, significant battery, or application issues.
    - Device may experience configuration and compliance issues with Enterprise mobile device management tool.
- Users will not be able to update their devices manually unless the update has been made available after the software delay or otherwise made available by enterprise mobile device management.