Windows Desktop Device Enrollment

Overview

This section discusses enrolling Windows Desktop devices into AirWatch. Device enrollment establishes the initial communication with AirWatch to enable Mobile Device Management (MDM).

Windows Desktop devices enroll using MDM-functionality built into the Windows OS. Devices can be enrolled by end users using native MDM Workplace/Work Account settings, through Azure Active Directory integration, or using bulk provisioning to configure devices before sending them to end users.

Enrollment can also require the downloading of the AirWatch Protection Agent. This agent adds endpoint security to your Windows Desktop devices to ensure your data and devices remain secure wherever the device may go. The AirWatch Protection Agent for Windows Desktop co-opts the native Windows Desktop functionality such as BitLocker encryption, Windows Firewall, and Windows Automatic Updates to keep devices secure and up-to-date.

Windows Desktop vs Windows 7 devices

Devices running Windows 8.1 or Windows 10 use the native MDM enrollment method. The native MDM enrollment (Workplace/Work Account) method maximizes the functionality available to you to manage your Windows 8 and Windows 10 devices.

AirWatch combines Windows 8.1 and Windows 10 devices under the unified Windows Desktop platform. All of your desktops, laptops, and tablets running Windows 8.1 and Windows 10 and enrolled using the native MDM enrollment are Windows Desktop devices.

Devices managed with Microsoft SCCM cannot be enrolled using the native MDM enrollment. You can enroll your SCCM-managed Windows 8 and Windows 10 devices as Windows 7 devices. AirWatch recommends foregoing SCCM and using the native MDM enrollment method for its increased functionality.

While both Windows Desktop and Windows 7 use the AirWatch Agent, only the Windows 7 enrollment method uses the AirWatch Agent to enroll. A device enrolled with the AirWatch Agent will receive Windows 7 policies and profiles and not Windows Desktop ones.