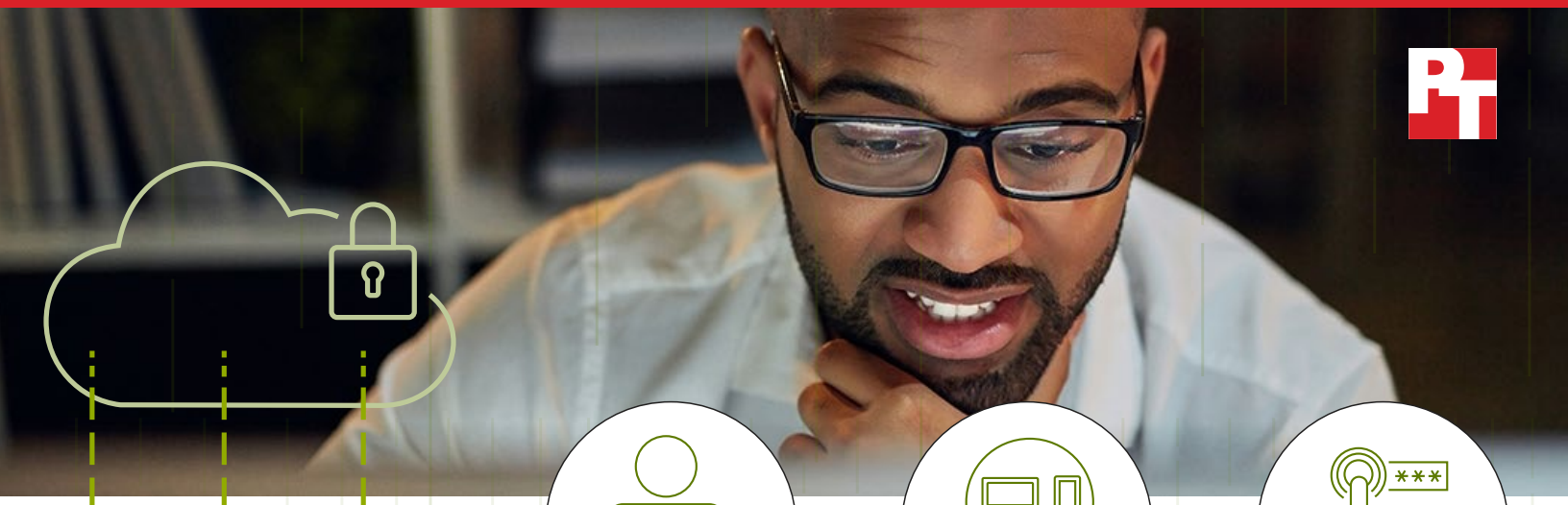


Up to
60%
faster when enrolling a macOS device

Offer more endpoint choices - laptops, smartphones, tablets, smartwatches, and more

Securely sign into multiple apps with a single touch

Support a broader set of devices and onboard end users more easily with VMware Workspace ONE

Compared to Microsoft Intune, VMware Workspace ONE offered a broader set of use cases with support for Android Enterprise, Chromebooks, Apple macOS and iOS, and Microsoft Windows 10

The proliferation of computers is good for the everyday user—they have plenty of endpoint options (laptops, smartphones, tablets, and smartwatches, among others) to fit their lifestyles. But that presents a pressing challenge for your organization: Can you leverage employee or customer familiarity and preference while following the numerous policies and procedures of your IT department? The answer is yes, by choosing a unified endpoint management (UEM) solution that supports numerous platforms and gives IT granular control over endpoints.

We tested and researched two popular UEM solutions, VMware Workspace ONE® and Microsoft Intune, to see if Workspace ONE could offer advantages for existing Intune users. What did we find? Workspace ONE supported more device types than Intune while saving time on most of our tested management tasks. With Workspace ONE, your organization can offer greater platform flexibility to employees and customers, shorten endpoint management time, and reduce user downtime.

The increasing number of endpoints available to your organization can help it succeed. Workspace ONE allows you better balance multiple platform management demands while adhering to your digital policies and procedures.

What is unified endpoint management?

Unified endpoint management (UEM) is centralized management and security of numerous devices and applications using a single software tool. Manageable devices include laptops, desktops, smartphones, tablets, and others, while the list of manageable apps includes those aimed at internet browsers and productivity, among others.

UEM helps organizations deliver a consistent and enjoyable user experience. Whether users are opening their smartphone or laptop, UEM solutions deliver the same interface and settings that they're used to across endpoints.

VMware Workspace ONE

Between email, word processing, and chat software, much of today's work takes place in the digital workspace. VMware Workspace ONE, powered by VMware AirWatch®, is a unified, integrated platform for the digital workspace. The solution lets you centrally manage and monitor users' endpoints (laptops, workstations, and mobile devices), cloud-hosted virtual desktops, and applications from the cloud or from an on-premises deployment.

Reduce user downtime while performing select management tasks

Choosing Workspace ONE to manage the endpoints in your organization can save time for your IT staff as well as reduce the potential downtime that users might experience during management. Based on our hands-on testing for example, if an admin needs to adjust the settings of an Apple® iPad® in a retail store kiosk after a critical app update, changing the settings would be faster using Workspace ONE than with Intune, and customers would be able to use the kiosk sooner.

For Android and Android for Enterprise, Apple iOS and macOS®, and Microsoft Windows 10 platforms, we performed three common management tasks: enrolling a device in UEM management, deploying an app to a device, and changing settings on a device. Using Workspace ONE was faster in three-quarters of the tasks (8 of 12). The sections below provide details by platform. After you've read this report, continue to page 8 and see the science behind it.

What are profiles?

Profiles dictate what options users have on their devices. Profiles can define settings for a device, restrict users from completing certain actions, set requirements for password length, or restrict a user from using power controls on their computer. Defining and restricting profiles helps protect your organization from unwanted behaviors.

Android and Android for Enterprise

Change settings up to **25% faster** on Android platforms

Most smartphones in the world use some version of the Android operating system.[1] As it's highly likely that a user in your organization has an Android phone or wants to use one, performing any kind of management task quickly on the endpoints, in this case Android devices, would be ideal. In our hands-on testing, changing settings on an Android device using Workspace ONE took 20 percent less time than with Intune. This could reduce downtime for your users and shorten the amount of time admins need to finish the task. Given the popularity of the Android and Android Enterprise platforms (and the amount of times your admins would have to repeat this task), these savings could add up.

Changing settings on an Android device

Less time is better

Change more Android settings

We found that Workspace ONE offers these Android device management features that Intune doesn't offer:

- Allows changes to system update settings
- Configures Launcher, an app launcher to help customize and secure Android devices
- Configures Chrome Browser Settings

Microsoft Windows 10

Change settings up to **33% faster** on Windows 10 platforms

In a recent article, Mashable listed what they considered to be eight of the best laptops for enterprises. Seven of those laptops ran Microsoft Windows 10, and they came from four different vendors.[2] Regardless of what preferences or features make a laptop good for an enterprise, there's no denying the prevalence of Windows 10 endpoints today for large organizations. Compared to Intune, using Workspace ONE to change settings on a Windows 10 device was 33 percent faster and deploying an app to a Windows 10 device was 14 percent faster.

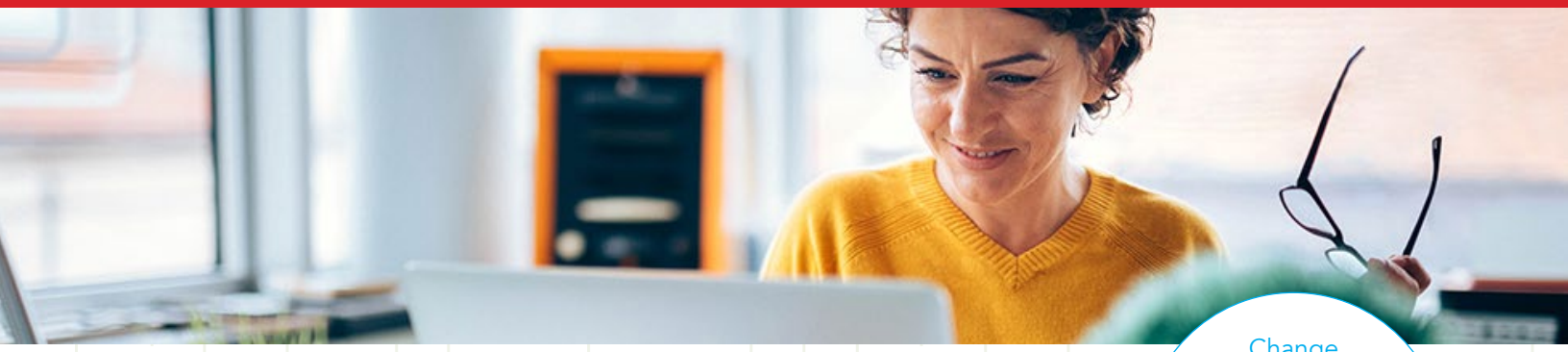
Changing settings on a Windows 10 device

Less time is better

Integrate Dell Command for more security

We found that by integrating Windows 10 with Dell Command, Workspace ONE offers these management features:

- Enables BIOS-level changes on Dell devices
- Allows toggling of TPM Chip status (useful for Bitlocker)
- Allows changes to Secure boot settings
- Allows changes to Virtualization settings
- Disables Bluetooth at BIOS level



Manage iOS with ease

We found that Workspace ONE offers these iOS device management features:

- Supports CalDav and CardDav protocols to give access and share contacts and calendars (Intune does not out of box)
- Restricts AirPlay® Mirroring to only white-listed destinations

Apple iOS

Change settings up to **44% faster** on iOS platforms

Apple iOS is the second most popular smartphone operating system on the planet.[3] Being able to manage both Android and iOS endpoints should meet your mobile management needs. It's worth noting that the Apple iPhone® and iPad run iOS, and the iPad holds the largest single-vendor market share of the tablet global market.[4] Companies often deploy them for single-application usage and interfaces, such as kiosks and digital signage, and many retailers and restaurants use them as point-of-sale terminals. In our hands-on testing, changing settings on an iOS device with Workspace ONE was 44 percent faster than Intune, and it was 31 percent faster to enroll an iOS device in Workspace ONE UEM management.

Changing settings on an iOS device

Less time is better

Enroll macOS devices up to **60% faster**

Apple macOS

The Apple MacBook Pro® is consistently a popular choice for enterprise users.[5] Whether your IT staff are preparing one for a new app developer or pushing out device changes for your marketing team, you can rest assured that IT staff using Workspace ONE can quickly do the tasks and let users be on their way. It was 60 percent faster to enroll a macOS device in UEM management and 20 percent faster to deploy device changes to a macOS device using Workspace ONE than Intune.

Enrolling a macOS device in UEM management

Less time is better

Better manage macOS resources

We found that Workspace ONE offers these macOS device management features that Intune doesn't offer:

- Supports .dmg files, which are more commonplace than .pkg files; Intune supports only .pkg files for MAM
- Supports an Enterprise Wipe of devices
- Allows changes to several settings (see p. 6 for details)

Supported platform	VMware Workspace ONE	Microsoft Intune
Windows 10	✓	✓
iOS	✓	✓
macOS	✓	✓
Android and Android Enterprise	✓	✓
Chrome OS	✓	
Tizen	✓	
QNX	✓	
Apple Watch	✓	
Apple TV	✓	
Windows IoT	✓	✓
Windows 7	✓	✓
Windows 8.1	✓	✓
Surface Hub	✓	✓
Windows 10 mobile	✓	✓
Windows Holographic for Business	✓	✓
Total supported platforms	**15**	**10**

Offer more platforms to users

If you're an existing Intune user, we found the same functions and features for Workspace ONE that you likely leverage with Intune. A significant difference we found in hands-on testing, however, is that Workspace ONE allows your organization to use more platforms than Intune, including ChromeOS for Chromebooks. That's a significant advantage for organizations that appreciate the cost efficiency of Chromebooks as well as for education systems throughout the US, where these devices are popular.[6]

Workspace ONE also supports many internet of things (IoT) and ruggedized endpoints, which have made their way into the digital workspace. According to a 2018 IDC report, Workspace ONE is currently a leader in support for IoT and ruggedized endpoints. The paper also notes that Intune has limited support for IoT devices outside of Windows IoT, but that "VMware has many wearable and smart glasses partners, with live deployments in customer sites, including Google Glass, Upskill, Atheer, ODG, Vuzix, and RealWear, as well as Microsoft HoloLens. Workspace ONE is deployed in ruggedized devices from Samsung, Zebra, Honeywell, LG, HTC, Sony, Kyocera, Lenovo, Panasonic, and Zebra, as well as mobile printer/peripherals from Zebra and others."[7]

The more platforms and devices your organization can support, the better equipped your users will be to stay productive. In terms of customer experience, they'll have more ways to engage with your products and services.

Improve employee satisfaction by becoming a digital leader

More than three quarters of respondents to an MIT Sloan Management Review survey claimed "they want to work for a digitally enabled company or digital leader."[8] Digital leaders must change with digital and cultural trends. One way to do this is to support numerous platforms and endpoints that satisfy employees' lifestyles and roles as well as drive productivity. Choosing Workspace ONE for your organization can help you be better poised to serve your employees' changing digital needs.

Manage and secure devices with helpful features

Workspace ONE can make managing and securing endpoints in your organization simple for IT admins and users with adaptive management, single sign-on (SSO), and per-app VPN.

Adaptive management is a user-focused management approach for Android and iOS mobile devices that lets users run pre-approved, open-access applications without direct IT involvement.[9] If users want access to native apps that require management, adaptive management offers additional security through the use of profiles. This approach allows users to decide which apps are right for their roles while maintaining operational consistency throughout an organization.

When a user logs in with a single ID and password to VMware Identity Manager, they get access to the growing number of independent apps and services. Workspace ONE offers SSO for Android, iOS, Windows 10, and ChromeOS platforms.[10,11] This is convenient for users, particularly those using multiple endpoints, and can reduce redundant sign-on processes. IT can appreciate the minimized risk of users creating easy-to-hack passwords, among other things.

Per-app VPN is a key security feature for Android, iOS, Windows 10, and macOS platforms that lets select applications (not the device) securely connect to your private networks even when the device is connected via a public network (e.g. working remotely).[12] Minimizing an endpoint's potential attack vectors is a clear benefit for the security of your organization.

Support users that need helpful macOS resources

Workspace ONE better integrates with macOS features than Intune. In our testing, we found that Workspace ONE integrates with more macOS features than Intune, including Time Machine, AirPlay, and Network file locations. For organizations with many macOS users, configuring these settings with Workspace ONE can alleviate some burden for users and admins, saving time for both. We found Workspace ONE offers the following features for macOS devices that Intune does not:

- Supports CalDav accounts to access and share calendars (Intune does not out of the box)
- Supports CardDav accounts to access and share contacts (Intune does not out of the box)
- Customize Docks for desktops
- Adjust Parental Controls, such as hiding profanity in Dictionary and Dictation and limiting access to websites
- Configure items that automatically start on login, such as Applications, Files and Folders, and Authenticated Network Mounts
- Block user commands such as Connect to server, Eject, Burn Disc, Go to Folder, Restart, and Shutdown
- Restrict AirPlay Mirroring to only white-listed destinations
- Restrict only specific Kernel Extensions, which can be toggled to allow a user override
- Configure Energy Saver Options
- Configure Time Machine settings

Conclusion

Having different platforms and endpoints in your organization's IT infrastructure is a good thing. It allows users to work with what they know and meet productivity challenges with many options. Additionally, it allows your organization to offer the endpoint and platform flexibility that can attract and keep employees by meeting their digital needs.

For companies using or considering the UEM solution Intune, your users and IT staff can manage and control a broader array of devices, including those running the platform ChromeOS, with the UEM solution Workspace ONE. Additionally, Workspace ONE saves time on certain management tasks compared to Intune and has more macOS features than Intune. If you use Intune, or have considered it, but want to offer greater platform flexibility to your employees and customers, shorten endpoint management time, and reduce user downtime, consider moving to Workspace ONE.

---

1 "Smartphone Market Share," accessed April 10, 2019, https://www.idc.com/promo/smartphone-market-share/os

2 Obias, Rudie, "8 of the best laptops for business: See why the MacBook Pro and Lenovo ThinkPad top our list," accessed April 17, 2019, https://mashable.com/roundup/best-laptops-for-business/

3 "Smartphone Market Share," accessed April 10, 2019

4 "Global tablet market share held by tablet vendors from 2nd quarter 2011 to 3rd quarter 2018," accessed April 11, 2019, https://www.statista.com/statistics/276635/market-share-held-by-tablet-vendors/

5 Athow, Desire, "Best business laptops 2019: top laptops for work," accessed April 23, 2019, https://www.techradar.com/news/best-business-laptops

6 Molla, Rani, "Apple wants to sell more iPads to schools, but Google already owns the education market," accessed April 11, 2019, https://www.recode.net/2018/3/27/17169624/apple-ipad-google-education-event-chromebooks-market

7 Hochmuth, Phil, "IDC MarketScape: Worldwide Enterprise Mobility Management Software for Ruggedized/IoT Device Deployments 2018 Vendor Assessment," accessed April 9, 2019, https://www.idc.com/getdoc.jsp?containerId=US44246518

8 Kane, Gerald C., Doug Palmer, Anh Nguyen Phillips, David Kiron, and Natasha Buckley, "Strategy, not technology, drives digital transformation," accessed April 26, 2019, https://sloanreview.mit.edu/projects/strategy-drives-digital-transformation/

9 "Managing Access to Applications," accessed April 10, 2019, https://docs.vmware.com/en/VMware-Workspace-ONE/services/WS1-IDM-deploymentguide/GUID-E3A63D80-4259-4C13-8FA3-713F7E0BF5BB.html

10 "VMware AirWatch SAML Integration Guide," accessed April 9, 2019, https://resources.workspaceone.com/view/j87fqmyx6b-jzwbvjvvtq/en

11 "VMware AirWatch Chrome OS Platform Guide," accessed April 10, 2019, https://docs.vmware.com/en/VMware-Workspace-ONE-UEM/9.6/chromeos.pdf

12 "Deploying Per-App Tunnel to devices," accessed April 8, 2019, https://docs.vmware.com/en/VMware-Workspace-ONE-UEM/9.6/vmware-airwatch-guides-96/GUID-AW96-Configure_Per-App-Tun_Over.html

This document describes what we tested, how we tested, and what we found. To learn how these facts translate into real-world benefits, read the report Support a broader set of devices and onboard end users more easily with VMware Workspace ONE.

We concluded our hands-on testing on April 11, 2019. During testing, we determined the appropriate hardware and software configurations and applied updates as they became available. The results in this report reflect configurations that we finalized on February 21, 2019 or earlier. Unavoidably, these configurations may not represent the latest versions available when this report appears.

Our results

The table below presents our findings in detail.

Platform	Task	VMware Workspace ONE® (mm:ss)	Microsoft Intune (mm:ss)	Time difference	Time percentage
Android	Enrolling an Android device in UEM management	01:18	01:16	-00:02	-3%
	Deploying an app to Android device	01:05	01:15	00:10	15%
	Changing settings on an Android device	00:43	00:54	00:11	25%
	Android scenario total	03:06	03:25	00:19	10%
Microsoft Windows 10	Enrolling a Windows 10 device in UEM management	00:57	00:51	-00:06	-11%
	Deploying an app to Windows 10 device	01:43	01:57	00:14	14%
	Changing settings on a Windows 10 device	00:49	01:05	00:16	33%
	Window 10 scenario total	03:29	03:53	00:24	12%
Apple® iOS	Enrolling an iOS device in UEM management	01:28	01:55	00:27	31%
	Deploying an app to iOS device	01:09	01:05	-00:04	-6%
	Changing settings on an iOS device	00:48	01:09	00:21	44%
	iOS scenario total	03:25	04:09	00:44	21%

Platform	Task	VMware Workspace ONE® (mm:ss)	Microsoft Intune (mm:ss)	Time difference	Time percentage
Apple macOS®	Enrolling a macOS device in UEM management	01:38	02:37	00:59	60%
	Deploying an app to macOS device	03:18	03:10	-00:08	-4%
	Changing settings on a macOS device	00:48	00:58	00:10	20%
	macOS scenario total	05:44	06:45	01:01	18%

System configuration information

The table below presents detailed information on the systems we tested.

Server configuration information	Dell® Latitude® 5491	Apple Mac mini®	HP Chromebook™ x360 Model 14-da0011dx	Apple iPhone® XS	Google Pixel™ 3
Processor					
Vendor	Intel®	Intel	Intel	Apple	Qualcomm®
Model number	Core i5-8400H	Core i3-8100	Core i3-8130U	A12 Bionic	Snapdragon 845
Core frequency (GHz)	2.5	3.6	2.20	2.49	2.5
Number of cores	4	4	2	6	8
Cache	8MB SmartCache	6MB SmartCache	4MB SmartCache	N/A	N/A
Memory					
Amount	8GB	8GB	8GB	4GB	4GB
Type	DDR4	DDR4	DDR4	N/A	N/A
Speed (MHz)	2,666	2,667	2,400	N/A	N/A
Integrated graphics					
Vendor	Intel	Intel	Intel	Apple	Adreno
Model number	UHD Graphics 630	UHD Graphics 630	UHD Graphics 620	A12 Bionic	630
Storage					
Amount (GB)	256	128	64	64	64
Connectivity/expansion					
Wired internet	Ethernet	Ethernet	N/A	N/A	N/A
Wireless internet	802.11ac Dual Band	802.11ac (a/b/g/n compatible)	802.11ac	802.11ac	802.11a/b/g/n/ac
Bluetooth	4.2	5.0	4.2	5.0	5.0
USB	3 x USB 3.1, 1 x USB Type-C	2 x USB 3.0	2 x USB 3.1 Type C, 1x USB 3.1	N/A	N/A
Thunderbolt	N/A	4 x Thunderbolt 3	N/A	N/A	N/A
Video	1 x HDMI	1 x HDMI	N/A	N/A	N/A
Cellular	N/A	N/A	N/A	LTE	LTE
Battery					
Type	Lithium-polymer	N/A	Lithium-polymer	Lithium-ion	Lithium-polymer
Size	Integrated	N/A	Integrated	Integrated	Integrated
Rated capacity	68Wh	N/A	60Wh	2,658mAh	2,915mAh
Display					
Size	14”	N/A	14”	5.8”	5.5”
Type	LED-backlit	N/A	LED-backlit	Super Retina HD (OLED)	OLED

Server configuration information	Dell® Latitude® 5491	Apple Mac mini®	HP Chromebook™ x360 Model 14-da0011dx	Apple iPhone® XS	Google Pixel™ 3
Resolution	1920 x 1080	N/A	1920 x 1080	2436x1125	2160x1080
Touchscreen	No	No	Yes	Yes	Yes
Operating system					
Vendor	Microsoft	Apple	Google	Apple	Android
Name	Windows 10 Pro	macOS	ChromeOS	iOS	Pie
Build number or version	Version: 10.0.17134, Build: 17134	Mojave 10.14.3	71.0.3578.127, Nami.10775.47.0	12.1.4	9 with 2/5/19 security patch
BIOS					
BIOS name and version	Dell Inc. 1.1.6	N/A	N/A	N/A	N/A
Dimensions					
Height (in)	0.8"	1.4"	0.6"	5.65"	5.7"
Width (in)	13.1"	7.7"	12.8"	2.79"	2.7"
Depth (in)	9.0"	7.7"	8.9"	0.30"	0.30"
Weight	3.63 lbs.	2.9 lbs.	3.7 lbs.	6.24 oz.	5.22 oz.

How we tested

To test Intune, we used Microsoft Azure with Enterprise Mobility + Security E5 and Azure Active Directory Premium P2 licenses. For Workspace ONE, we used the Workspace ONE UEM SaaS environment connected to Workspace ONE Identity Manager.

For Windows enrollment in Workspace ONE, we used Windows Auto-Discovery Service to automatically detect our cloud enrollment server. For your own setup, follow the instructions in Chapter 2 of the VMware AirWatch Windows Autodiscovery Service Installation Guide.

Enrolling devices in Workspace ONE

Enrolling a Windows 10 device

1. On the target device, click Start, and open Settings.
2. Click Accounts.
3. Click Access work or school.
4. Click Connect.
5. Enter the user's email address, and click Next.
6. With the user email address and password, sign into Workspace ONE.
7. When prompted, set up a PIN.
8. On the Setting up your device screen, click Got it.

Enrolling a macOS device

1. On the target device, open the User Activation email.
2. In the Activation email, click awagent.com.
3. On the Download page, click Download.
4. Open, and run the AirwatchAgent download.
5. Click VMware AirWatch Agent.pkg.
6. On the Welcome to the VMware AirWatch Agent Installer screen, click Continue.
7. On the License screen, click Continue.
8. On the pop-up, click Agree.
9. On the Installation Type screen, click Install. If prompted, enter your password.
10. Once completed, click close.
11. Open the VMware AirWatch Agent.
12. On the Status screen, click Enroll Now.
13. When the VMware AirWatch Agent authentication screen appears, select Server Details.
14. On the Authenticate screen, enter the Server Name and Group ID.
15. On the Welcome to AirWatch! screen, click Continue.
16. On the Enter your credentials screen, enter your credentials, and click Continue.
17. On the Enable Device Management screen, click Enable.
18. When prompted, enter your computer password.

Enrolling an iOS device

1. On the target device, open the User Activation email.
2. In the Activation email, click the link for awagent.com.
3. On the Download page, click Go to Apple AppStore.
4. In the Apple AppStore AirWatch Agent page, tap Get, and tap Install. Once the installation completes, open the application.
5. On the Authenticate screen, select QR Code.
6. To get the Server Name and Group ID, scan the QR code.
7. On the User Credential page, enter your username and password, and tap Next.
8. On the Enable Device Management screen, tap Redirect and Enable.
9. On the Install Profile screen, tap Install.
10. Tap Install.
11. On the Warning screen, tap Install.
12. On the Remote Management pop-up, tap Trust.
13. On the App Installation pop-up, tap Install.

Enrolling an Android device

1. On the target device, click Start, and open Settings.
2. Click on Accounts.
3. Click on Access work or school.
4. Click on Connect.
5. Enter the user email address.
6. Click Next.
7. Sign into Workspace ONE with the user email address and password.
8. On the You're all set! screen, click Done.

Enrolling devices in Intune

Enrolling a Windows 10 device

1. On the target device, click Start, and open Settings.
2. Click on Accounts.
3. Click on Access work or school.
4. Click on Connect.
5. Enter the user email address.
6. Click Next.
7. Sign into Intune with the user email address and password.
8. When prompted, set up a PIN.
9. On the You're all set! screen, click Done.

Enrolling a macOS device

1. On the target device, open Safari, and navigate to portal.manage.microsoft.com.
2. On the Microsoft Intune login page, log in with your user credentials.
3. In the portal, click the hamburger button, and select My Devices.
4. On the My Devices screen, click the notification link to enroll your device.
5. On the Which device is this? screen, click Enroll.
6. On the Enroll this Device screen, click Install.
7. On the Install "Management Profile"? pop-up, click Install. If prompted, enter your password.
8. Click Continue.
9. Click Install.

Enrolling an iOS device

1. On the iPhone, open the App Store.
2. Search Intune Company Portal.
3. Tap Get, and tap Install Microsoft Intune Company Portal. If requested, enter your password.
4. Once the installation has completed, launch the Microsoft Intune Company Portal app.
5. Sign in using your user credentials.
6. On the Company Access Setup screen, tap Begin.
7. On the What can the company see? screen, tap Continue.
8. On the What's next? screen, tap Continue.
9. Tap Allow.
10. When the settings screen pops up, tap Install. Enter passcode if prompted.
11. On the pop-up, tap Install.
12. On the Warning screen, tap Install.
13. On the Remote Management pop-up, tap Trust.
14. After installation finishes, tap Done.
15. In the Safari web browser, tap Open.
16. On the Company Access Setup screen, tap Done.

Enrolling an Android device

1. On the Android device, open the Google Play store.
2. Search Intune Company Portal.
3. Tap Install.
4. Once the installation has completed, launch the Microsoft Intune Company Portal app.
5. Sign in using your user credentials.
6. On the Company Access Setup screen, tap Continue
7. On the Who cares about your privacy? screen, tap Continue.
8. On the What's next? screen, tap Next.
9. On the Activate device admin app? screen, tap Activate this device admin app.
10. On the Company Access Setup screen, tap Done.

Deploying an application from Workspace One

Deploying an application to a Windows 10 device (internal)

1. In the AirWatch Console, select the Apps & Books workspace.
2. On the Native page, on the Internal tab, click Add Application.
3. Select Upload.
4. On the Add screen, click Choose File.
5. Select the target file, and click OK.
6. Click Continue.
7. On the Application screen, click Save & Assign.
8. On the Assignment screen, click the field for Select Assignment Groups, and select WindowsTest. Click Save & Publish.
9. On the View Device Assignment screen, click Publish.

Deploying an application to a macOS device (internal)

1. Download the VMware Admin Assistant Tool for Mac.
2. Launch Admin Assistant Tool installer.
3. On the introduction tab in the Install VMware AirWatch Admin Assistant wizard, click Continue.
4. Click Continue, and click Agree.
5. Click Install.
6. Enter credentials as needed.
7. Once Installation has completed, close the installer and move it to trash.
8. Open VMware AirWatch Admin Assistant.
9. Search for target file (.dmg), and open it in the assistant.
10. Once parsing has completed, click Reveal in Finder.
11. Locate the .plist metadata file created for the Mac application.
12. In the AirWatch Console, select the Apps & Books workspace.
13. On the Native page, on the internal tab, click Add Application.
14. Select Upload.
15. On the Add screen, click Choose File.
16. Select the target file, and click OK.
17. Click Continue.
18. Click Upload.
19. Select the .plist metadata file that you previously created.
20. Click Save.
21. Click Continue.
22. On the Application screen, click Save & Assign.
23. On the Assignment screen, click the field for Select Assignment Groups, and select MacOSTest.
24. Click Save & Publish.
25. On the View Device Assignment Screen, click Publish.

Deploying an application to an iOS device (public)

1. In the AirWatch console, select the Apps & Books workspace.
2. On the list view page, on the Public tab, click Add Application.
3. On the Add Application screen, for Platform, select Apple iOS.
4. Select Search App Store.
5. Under Name, type `Slack`, and press Enter.
6. Next to Slack – Business Communication for Teams on the Search screen, click Select.
7. On the Add Application screen, click the Assignment tab.
8. Click the field for Select Assignment Groups, and select iOSTest.
9. Click Save & Publish.
10. On the View Device Assignment screen, click Publish.

Deploying an application to an Android device (public)

1. In the AirWatch console, select the Apps & Books workspace.
2. On the list view page, on the Public tab, click Add Application.
3. On the Add Application screen, for Platform, select Android.
4. Select Search App Store.
5. Under Name, type `Slack`, and press Search.
6. On the Google Play screen, select Slack.
7. On the Slack screen, click Approve.
8. Click Approve.
9. On the Approval Settings, click Save.
10. Click the field for Select Assignment Groups, and select AndroidTest.
11. Click Save & Publish.
12. On the View Device Assignment screen, click Publish.

Deploying an application from Intune

Deploying an application to a Windows 10 device (internal)

1. On the Azure Portal, select All services, and select Intune.
2. Select Client Apps, and select Apps.
3. Click Add.
4. On the Add app panel, select Line-of-business App.
5. Select the App package file. To add the app, click the blue folder icon.
6. In the File Explorer, select the desired file, and click OK.
7. Click OK.
8. Under App information, enter a description and publisher. Click OK.
9. Click Add.
10. Once the file has finished uploading, select the app from the app list.
11. In the app panel, select Assignments.
12. In the Assignments panel, click Add group.
13. In the Add group panel under Assignment type, select Required.
14. Select Included Groups.
15. Select groups to include, and select Windows 10 Test.
16. Click Select.
17. Click OK.
18. Click Save.

Deploying an application to a macOS device (internal)

1. On the target macOS device, navigate to https://github.com/msintuneappsdk/intune-app-wrapping-tool-mac, and download the Intune App Wrapping Tool for Mac.
2. Open the terminal.
3. Navigate to the intune-app-wrapping-tool folder, and run the following command:
   a. `IntuneAppUtil -c <source_file> -o <output_file> [-v]`
4. In the Azure portal, select All services, and select Intune.

5. Select Client Apps, and select Apps.
6. Click Add.
7. In the Add app panel, select Line-of-business, and click the app package file.
8. In the App package file panel, click Select a File.
9. Using the previous command, select the .intunemac file output.
10. Click OK.
11. Select App information.
12. Enter a description and publisher name, and click OK. We used `test` for both.
13. Click Add.

Deploying an application to an iOS device (public)

1. On the Azure Portal, select All services, and select Intune.
2. Select Client Apps, and select Apps.
3. Click Add.
4. In the Add app panel, click iOS store app.
5. Click Search the App Store.
6. In the search bar, type `Slack`.
7. Select Slack.
8. Click OK.
9. In the App information panel, click OK.
10. Click Add.
11. In the Slack panel, click Assignments.
12. In the Assignments panel, click Add group.
13. In the Add group panel under Assignment type, select Required.
14. Select Included Groups.
15. Select groups to include, and select iOSTest.
16. Click Select.
17. Click OK.
18. Click Save.

Deploying an application to an Android device (public)

1. On the Azure Portal, select All services, and select Intune.
2. Select Client Apps, and select Apps.
3. Click Add.
4. In the Add app panel, for app type, click Android store app.
5. In the App Information panel, enter a name, a description, and a publisher.
6. Navigate to the Google Play web store, and search for Slack.
7. Copy the URL for the Slack App.
8. Navigate back to the Azure Portal, and paste the Appstore URL in the designated area in the App information panel.
9. Select the minimum operating system.
10. Click OK.
11. In the App information panel, click OK.
12. Click Add.
13. In the Slack panel, click Assignments.
14. In the Assignments panel, click Add group.
15. Under Assignment type in the Add group panel, select Required.
16. Select Included Groups.
17. Select groups to include, and select AndroidTest.
18. Click Select.
19. Click OK.

Deploying profiles with Workspace One

Deploying a profile to Android

1. In the Workspace One console, click Devices.
2. In the Devices workspace, under Profiles & Resources, select Profiles.
3. Click Add, and click Add Profile.
4. On the Add Profile screen, select Android.
5. On the General screen, for name, type `Android Passcode`. Under Smart Groups, select All Devices. Click Passcode.
6. Click Configure.
7. For Minimum Passcode Length on the Passcode screen, select 4. Click Save and Publish.
8. On the View Device Assignment screen, click Publish.

Deploying a profile to iOS

1. In the Workspace One console, click Devices.
2. In the Devices workspace, under Profiles & Resources, select Profiles.
3. Click Add, then Add Profile.
4. On the Add Profile screen select iOS.
5. On the General screen, for name, type `iOS Passcode`. Under Smart Groups, select All Devices. Click Passcode.
6. Click Configure.
7. Check Require passcode on device.
8. On the Passcode screen, for Minimum Passcode Length, select 4. Click Save and Publish.
9. On the View Device Assignment screen, click Publish.

Deploying a profile to macOS

1. In the Workspace One console, click Devices.
2. In the Devices workspace, under Profiles & Resources, select Profiles.
3. Click Add, then Add Profile.
4. On the Add Profile screen, select macOS.
5. On the Select Context screen, select Device Profile.
6. On the General screen, for name, type `macOS Passcode`. Under Smart Groups, select All Devices. Click Passcode.
7. Click Configure.
8. Check Require passcode on device.
9. On the Passcode screen, for Minimum Passcode Length, select 6. Click Save and Publish.
10. On the View Device Assignment screen, click Publish.

Deploying a profile to Windows 10

1. In the Workspace One console, click Devices.
2. In the Devices workspace, under Profiles & Resources, select Profiles.
3. Click Add, and click Add Profile.
4. On the Add Profile screen, select Windows.
5. On the Select Device Type screen, select Windows Desktop.
6. On the Select Context screen, select Device Profile.
7. On the General screen, for name, type `Windows Password`. Under Smart Groups, select All Devices. Click Password.
8. Click Configure.
9. On the Password screen, for Minimum Password Length, type `6`. Click Save and Publish.
10. On the View Device Assignment screen, click Publish.

Deploying profiles with Intune

Deploying a profile to Android

1. In the Intune workspace, click Intune.
2. Click Device configuration.
3. On the Device configuration panel, click Profiles.
4. In the Profiles panel, click Create Profile.
5. On the Create Profile panel, enter the following:
   - Name: Android Password
   - Platform: Android
   - Profile Type: Device Restrictions
   - Settings: Configure, Password
6. On the Password panel, select Require for Password
7. On the Android for Work compliance policy panel, select System Security.
8. Select Minimum password length, and type 6.
9. On the Device restrictions panel, click OK.
10. On the Create Profile panel, select Create.
11. On the Android Password panel, click Assignments.
12. On the Assignments Panel, click Assign to groups to include.
13. On the Assign to Include panel, select All Users & All Devices, and click Save.

Deploying a profile to iOS

1. In the Intune workspace, click Intune.
2. Click Device configuration.
3. On the Device configuration panel, click Profiles.
4. In the Profiles panel, click Create Profile.
5. On the Create Profile panel, enter the following:
   - Name: iOS Password
   - Platform: iOS
   - Profile type: Device restrictions
6. On the Device restrictions panel, click Password.
7. On the Password panel, select Password Required. For Required password type, choose Numeric. For Minimum password length, type 6. Click OK.
8. Click OK, and click Create.
9. On the iOS Password-Assignments panel, click Assignments.
10. On the Assignments Panel, click Select groups to include.
11. Select All Users & All Devices.
12. Click Save.

Deploying a profile to macOS

1. In the Intune workspace, click Intune.
2. Click Device configuration.
3. On the Device configuration panel, click Profiles.
4. In the Profiles panel, click Create Profile.
5. On the Create Profile panel, enter the following:
   - Name: macOS Password
   - Platform: macOS
   - Profile type: Device restrictions
6. Click Configure.
7. On the Device restrictions panel, select Password.
8. On the Password panel, select Require. For Minimum password length, enter 6.
9. Click OK

10. Click OK on Device restrictions panel
11. Click Create.
12. On the macOS Password panel, click Assignments.
13. On the Assignments Panel, click Select groups to include.
14. On the Select groups to Include panel, select All Users & All Devices.
15. Click Save.

Deploying a profile to Windows 10

1. In the Intune workspace, click Intune.
2. Click Device configuration.
3. On the Device configuration panel, click Profiles.
4. In the Profiles panel, click Create Profile.
5. On the Create Profile panel, enter the following:
   - Name: Windows Password
   - Platform: Windows 10 and later
   - Profile type: Device restrictions
6. On the Device restrictions panel, select Password.
7. On the Password panel, select Require. For Minimum password length, type 6.
8. Click OK.
9. On Device restrictions, Click OK.
10. Click Create.
11. On the Windows Password panel, click Assignments.
12. On the Assignments Panel, click Select groups to include.
13. Select All Users & All Devices.
14. Click Save.

Chromebook management with Workspace ONE

We set up a Google account with G Suite™ Business and Chrome Enterprise to manage Chromebooks at admin.google.com. We completed the following actions from the Workspace ONE UEM console.

Registering Chrome OS EMM

1. Navigate to Groups & Settings → All Settings → Chrome OS → Chrome OS EMM Registration.
2. Enter the domain and Google admin email address.
3. Click Test Connection.
4. Click Device Sync.

Enrolling a Chromebook in EMM

1. Starting with a new Chromebook, enter the information to connect to the wireless network, and click Next.
2. At the login screen, enter your email using the managed domain, and log in using your domain credentials.
3. At the You're signed in! screen, click Accept and Continue.

Deploying an app to ChromeOS (public)

1. Navigate to Devices → Profiles & Resources → Profiles.
2. On the Profiles page, click Add, and click add Profile.
3. Select Chrome OS, and click User.
4. Name your profile, select Assigned Groups, and click Application Control.
5. Enter the App ID and Name, and click Save and Publish.

Deploying a profile to ChromeOS

1. Navigate to Devices → Profiles & Resources → Profiles.
2. On the Profiles page click Add, and add profile.
3. Select Chrome OS, and click Device.
4. Name your profile, select Assigned Groups, and click Network.
5. Enter network settings for your network, and click Save and Publish.

This project was commissioned by VMware.