Contents

Surface Duo management overview

11/2/2020 • 3 minutes to read • Edit Online

Commercial customers can manage Surface Duo using any of various Enterprise mobility management (EMM) solutions that each provide a consistent set of cloud-based, device management capabilities whether managing employee- or company-owned devices.

You can manage Duo manage Duo via the Microsoft EMM that uses a unified console -- Microsoft Endpoint Manager – and extensible components like Microsoft Intune. Alternatively, you can use any EMM provider in Google's Android ecosystem. In some cases, third-party EMM solutions provide additional support to meet specific scenarios that may be useful depending on your environment.

To compare EMM solutions, refer to the Android Enterprise Solutions Directory. Endpoint Manager with Intune lets you manage Duo with the latest mobile device management policies as well as earlier technologies such as Exchange ActiveSync. If you already use Exchange ActiveSync settings to manage mobile devices, you can apply those settings to Duo devices with Intune using an Email device-configuration profile. For more information, see Add email settings to devices using Intune.

The primary means of managing devices in Intune, profiles provide default settings that you can customize to meet the needs of your organization.

Managing personally owned Surface Duo devices

SOLUTION	FEATURES	LEARN MORE
App Protection Policies without device enrollment	Allows you to manage and protect your organization's data within an application. Deploy app protection policies, a lightweight management solution without requiring device enrollment. A growing number of apps can now be managed with app protection policies including Microsoft Office and third-party apps like Adobe Acrobat, Service Now, and Zoom. For a complete list, refer to Microsoft Intune protected apps.	- App protection policies overview - Android app protection policy settings in Microsoft Intune. - Prepare Android apps for app protection policies with the Intune App Wrapping Tool.
Android Enterprise work profile	Targeted at BYOD deployments, work profiles provide a separate space on Duo for work apps and data, giving organizations full control of their data, apps, and security policies without restricting users from using their device for personal apps and data.	- Configure Android Enterprise Work Profile for Surface Duo.

Managing corporate-owned Surface Duo devices

SOLUTION	DESCRIPTION	LEARN MORE
Corporate-owned devices with work profile	Targeted at organizations that wish to enable personal use on corporate-owned single-user devices that they have provided for work. It's designed to give organizations more granular control than managing with a work profile but don't wish to completely lock down devices using Full device management or dedicated device management. Work and personal profile app data isolated by Android OS but differs from Android Enterprise work profile by providing admins more device-level control. IT admins can see, control, and configure the work accounts, applications, and data in the work profile, while end users are guaranteed that admins will have no visibility into the data and applications in the personal profile.	- Intune announcing public preview for Android Enterprise corporate-owned devices with a work profile
Android Enterprise Fully Managed	Provides comprehensive device and app management capabilities for company-owned devices associated with a single user and leveraged exclusively for work and not personal use. Full device management provides IT with full control over device data and security, as well as access to Android's full suite of app management features. For example: - You can set the minimum password requirements on a device - Remotely wipe and lock a device - Set default responses to app permission requests. - Customize end user experience with Microsoft Launcher You also have full control over the apps on a device, including the ability to remotely install and remove apps.	- Set up Intune enrollment of Android Enterprise fully managed devices.
Dedicated device management	This enterprise deployment scenario is targeted for devices deployed into specific use cases like logistics, transportation and factory floors. Use it for locked down experiences where you need to restrict usage to one or two apps and prohibit users from altering any settings.	- Set up Intune enrollment of Android Enterprise dedicated devices

Learn more

- Ignite Session: Deploy, Manage, and Enable Productivity with Surface Duo in the Enterprise

- Manage devices with Microsoft Intune
- Intune deployment planning, design, and implementation guide
- Enroll Android devices with Intune

Surface Duo security overview

11/2/2020 • 5 minutes to read • Edit Online

Surface Duo has protection built in at every layer with deeply integrated hardware, firmware, and software to keep your devices, identities, and data secure. As an Android 10 device, Surface Duo utilizes Android security features at the OS level and at the Google services layer. The Android OS leverages traditional OS security controls to protect user data and system resources, protects device integrity against malware, and provides application isolation. Additionally, Google provides a number of services layered on top of the OS that, when combined with Android OS security, help to continuously protect the Android user.

- **Custom engineered UEFI.** Unique to Surface Duo, among Android devices, is Microsoft's custom engineered Unified Extensible Firmware Interface (UEFI) which enables full control over firmware components. Microsoft delivers Enterprise-grade security to Surface Duo by writing or reviewing every line of firmware code in house, enabling Microsoft to respond directly and agilely, to potential firmware threats and to mitigate supply chain security risks.
- **Verified Boot.** Starting at the hardware level upon sign-in, Verified Boot strives to ensure executed code only comes from a trusted source. It establishes a full chain of trust -- from hardware-protected root of trust to the bootloader, boot partition and other verified partitions. When Surface Duo boots up, each stage verifies the integrity and authenticity of the next stage before handing over execution.
- **App separation.** Application sandboxing isolates and guards Android apps, preventing malicious apps from accessing private information. Mandatory, always-on encryption and key handling help protect data in transit and at rest -- even if devices fall into the wrong hands. Encryption is protected with Keystore keys, which store cryptographic keys in a container, making it more difficult to extract from a device.
- **Google Play Protect.** At the software layer, Surface Duo uses Google Play Protect threat detection, which scans all applications including public apps from Google Play, system apps updated by Microsoft and carriers, and sideloaded apps.
- **Microsoft Defender ATP.** The enterprise grade antivirus and malware protection software for Window 10 is now available for Android devices managed from Intune. To learn more, see Microsoft defender ATP for Android.

Mobile device management security

Surface Duo is secured in a corporate environment using an Enterprise Mobility Management (EMM) solution that provides a consistent set of protection tools, technologies, and best practices that you can tailor to meet your organizational and compliance requirements. A broad range of management APIs gives IT departments the tools to help prevent data leakage and enforce compliance in a variety of scenarios. Multi-profile support and device-management options enable separation of work and personal data, helping keep company data secure.

MDM security is built on an expanding set of configuration technologies to enable users to be productive on the go while also protecting critical corporate intellectual property. This includes app protection policies, device restriction policies, and related technologies designed to enable you to meet specific goals depending on your environment -- whether your business consists of delivering restaurant takeout orders, managing IT services for dental offices, or handling sensitive national security information.

For example, you may wish to strengthen device authentication by requiring users to enter a 6-digit alphanumeric pin along with 2-factor authentication. you may want to restrict the devices that users can enroll to help ensure you stay compliant with licensing limits or avoid granting access to "jailbroken" phones or other unsupported device types. Intune and other EMMs provide organizations with the flexibility to manage devices according to their needs.

App protection policies

App protection policies (APP) are rules that ensure an organization's data remains safe or contained in a managed app. A policy can be a rule that is enforced when the user attempts to access or move "corporate" data, or a set of actions that are prohibited or monitored when the user is inside the app. A managed app is an app that has app protection policies applied to it and can be managed by Intune.

App protection policies allow you to manage and protect your organization's data within an application. Many productivity apps, such as the Microsoft Office apps, can be managed by Intune MAM. See the official list of Microsoft Intune protected apps available for public use.

Security considerations for managing Surface Duo

The growing number of policy settings available in mobile device management solutions enable organizations to adjust protection levels to meet their specific needs. To help organizations prioritize security settings for Surface Duo (or any other Android device), Intune has introduced its Android Enterprise security configuration framework organized into several distinct configuration scenarios, providing guidance for work profile and fully managed scenarios.

SECURITY LEVEL	TARGETED TO	SUMMARY	SETTINGS INFO
Work profile basic security - Level 1	Personal devices with access to work or school data.	Introduces password requirements, separates work and personal data, and validates Android device attestation.	Work profile level 1 settings
Work profile high security - Level 3 (Due to framework conventions, this is the next level above Level 1.) **	Devices used by users or groups who are uniquely high risk. For example, users who handle highly sensitive data where unauthorized disclosure causes considerable material loss.	Introduces mobile threat defense or Microsoft Defender ATP, sets the minimum Android version to 8.0, enacts stronger password policies, and further restricts work and personal separation.	Work profile level 3 settings
Fully managed basic security -Level 1	Minimum-security configuration for an enterprise device, applicable to most mobile users accessing work or school data.	Introduces password requirements, sets the minimum Android version to 8.0, and enacts certain device restrictions.	Fully managed Level 1 settings
Fully managed enhanced security Level 2	Devices where users access sensitive or confidential information.	Enacts stronger password policies and disables user/account capabilities.	Fully managed Level 2 settngs
Fully managed high security Level 3	Devices used by users or groups who are uniquely high risk. For example, users who handle highly sensitive data where unauthorized disclosure causes considerable material loss.	Increases the minimum Android version to 10.0, introduces mobile threat defense or Microsoft Defender ATP, and enforces additional device restrictions.	Fully managed Level 3 settings

As with any framework, settings within a corresponding level may need to be adjusted based on the needs of the organization as security must evaluate the threat environment, risk appetite, and impact to usability.

Learn more

- Android Enterprise security configuration framework

- App protection policies overview
- Android app protection policy settings in Microsoft Intune
- Set enrollment restrictions
- Android Enterprise Security white paper

Configure Android Enterprise Work Profile for Surface Duo

11/2/2020 • 2 minutes to read • Edit Online

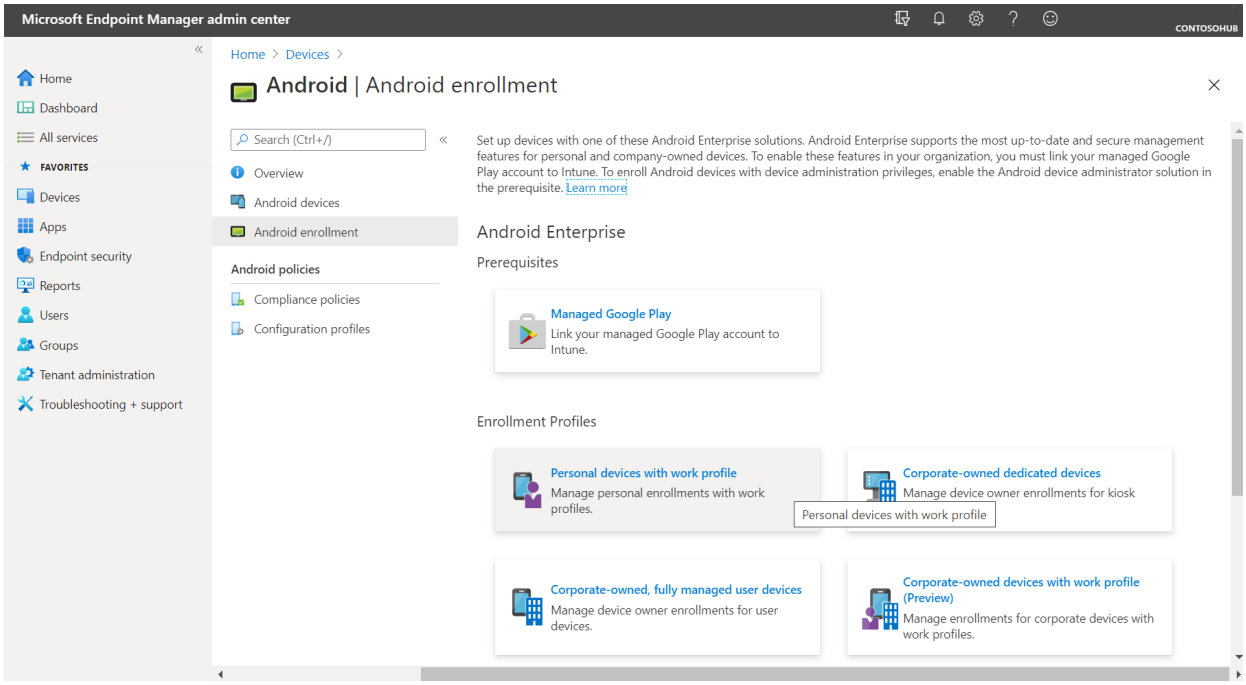
Targeted at BYOD deployments, work profiles provide a separate space on Duo for work apps and data, giving organizations full control of their data, apps, and security policies without preventing employees from using their device for personal apps and data.

Set up Android Enterprise Work Profile

Use work profiles to manage corporate data and apps on user-owned Android devices. By default, enrollment of personally owned work profile devices is enabled and requires no further admin configuration.

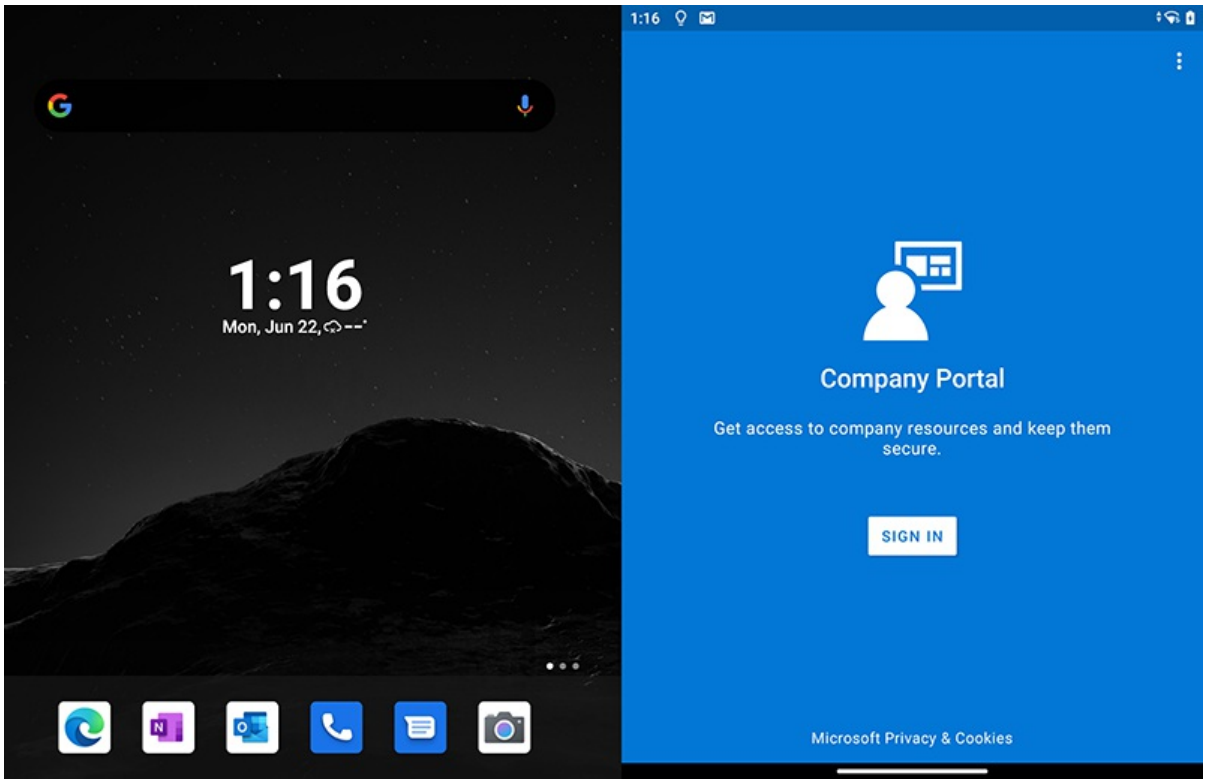
To enable Enterprise Work Profile:

- In Endpoint Manager, select **Devices** > **Android** > **Android enrollment** and then select **Personal devices with work profile**.

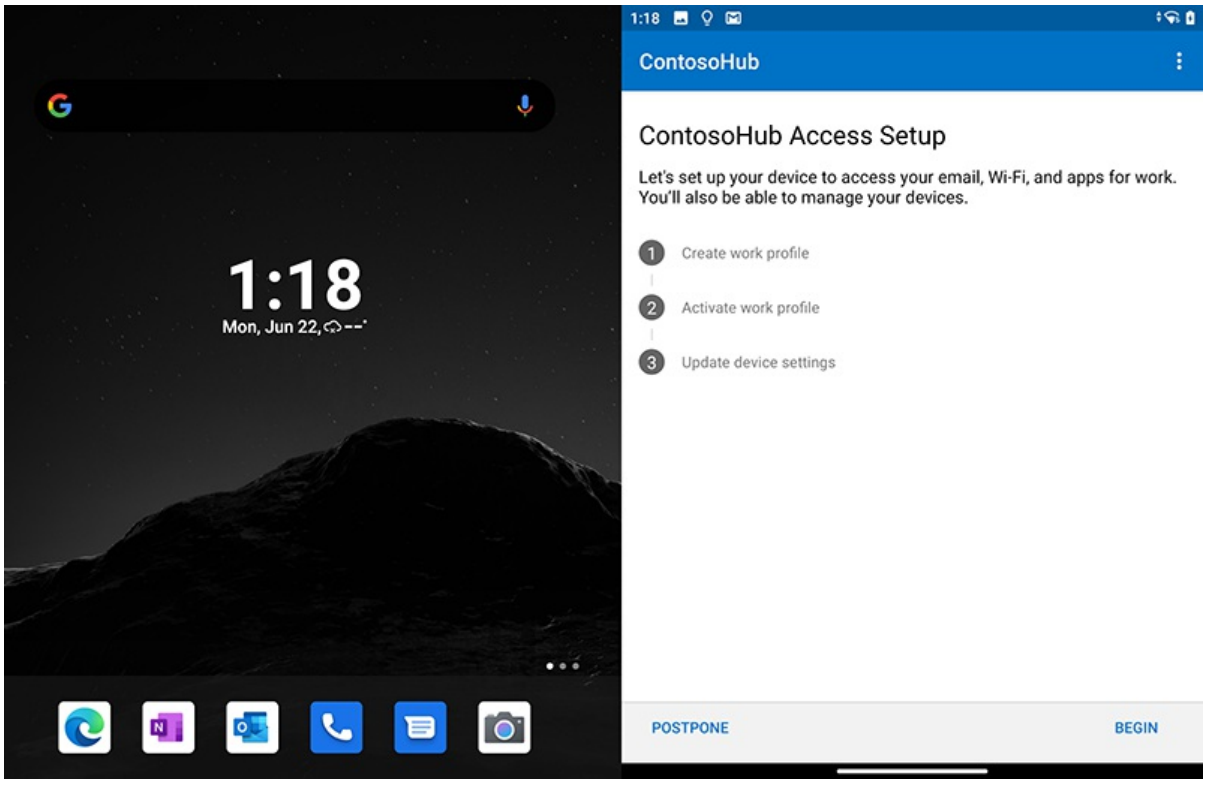


Sign into Surface Duo with Android Enterprise Work Profile

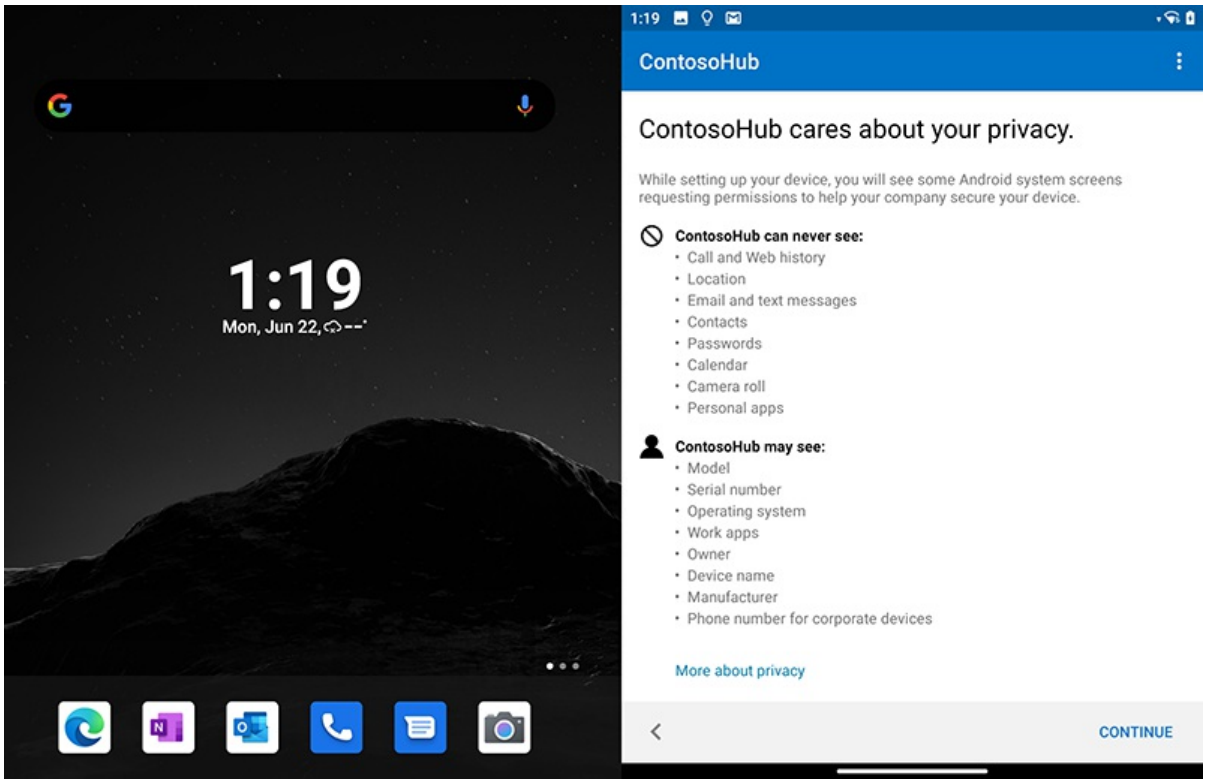
1. Install the Company Portal app from Google Play Store and sign in with your Microsoft work or school account.

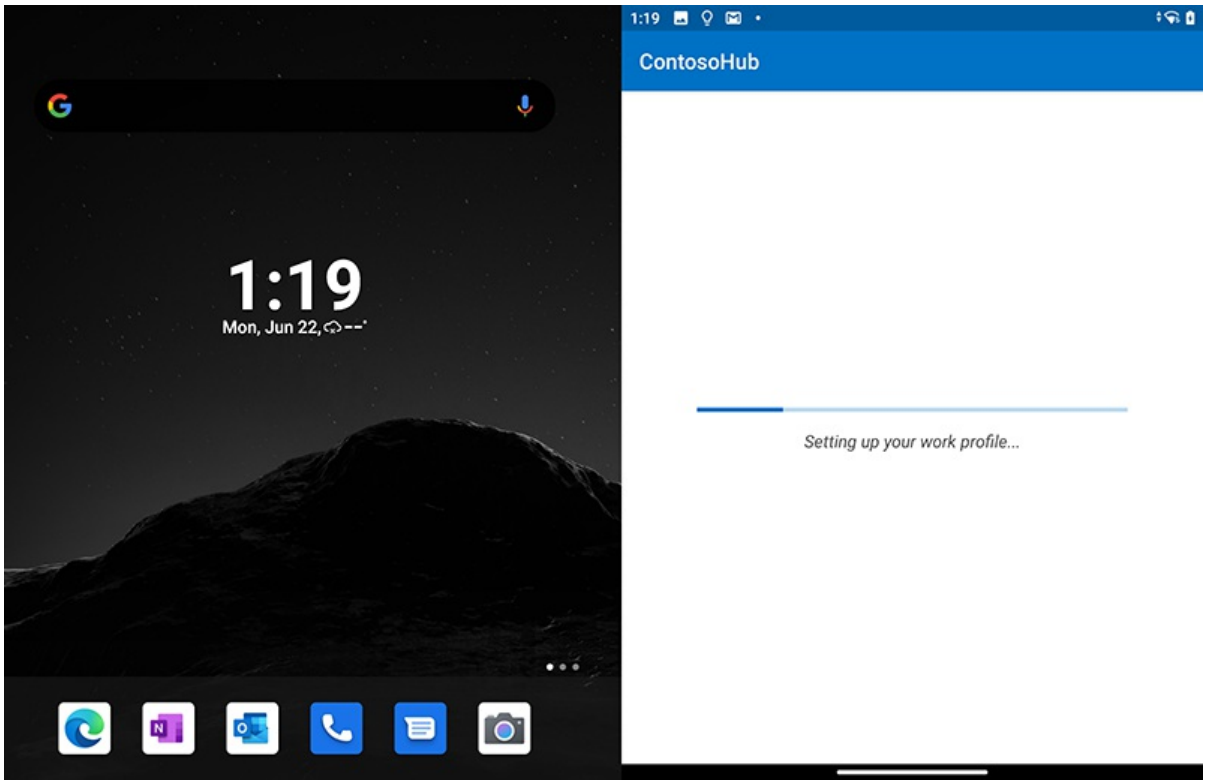


2. On the Access Setup page, select **Begin**.

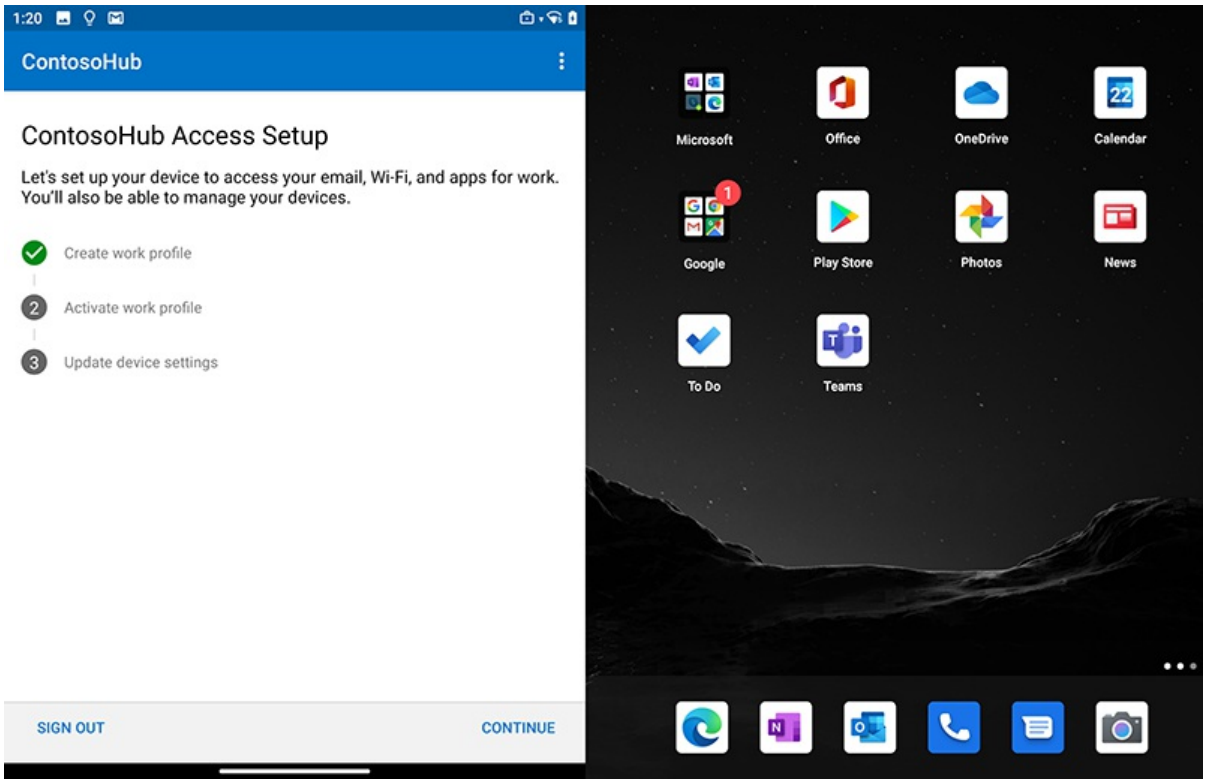


3. Review the information on the privacy page and select **Continue**.

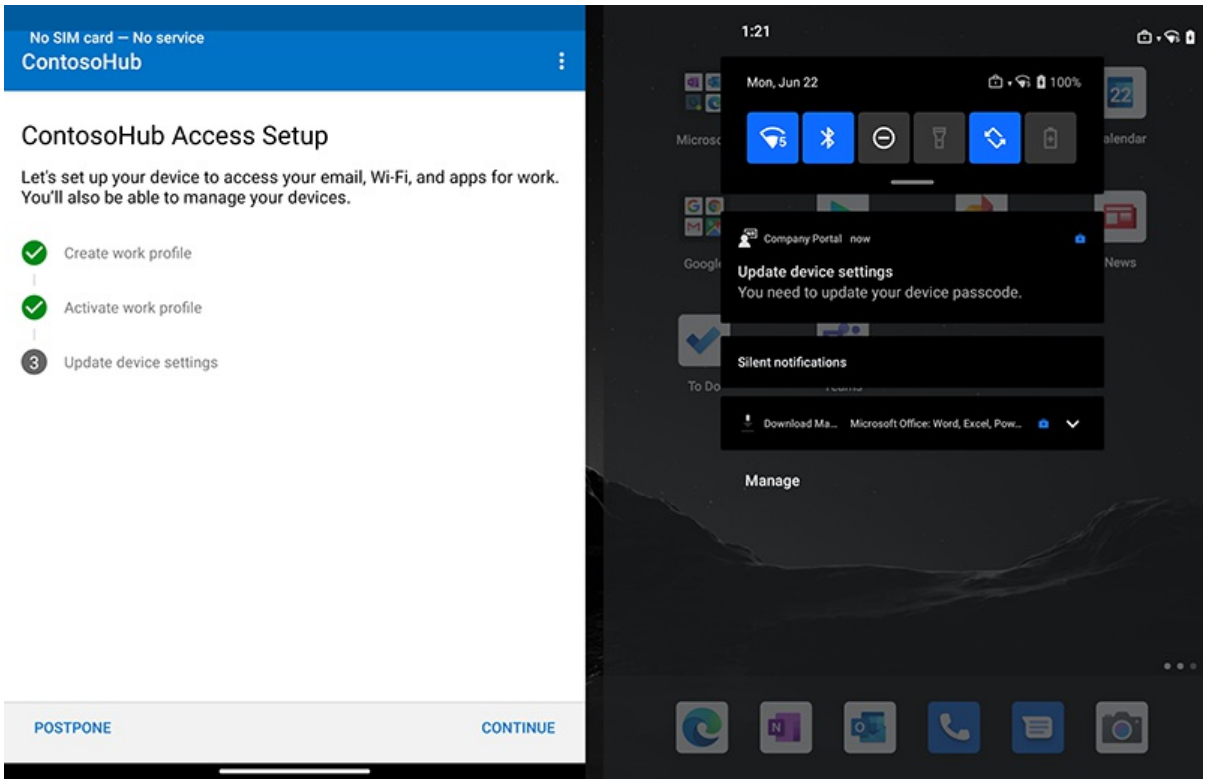




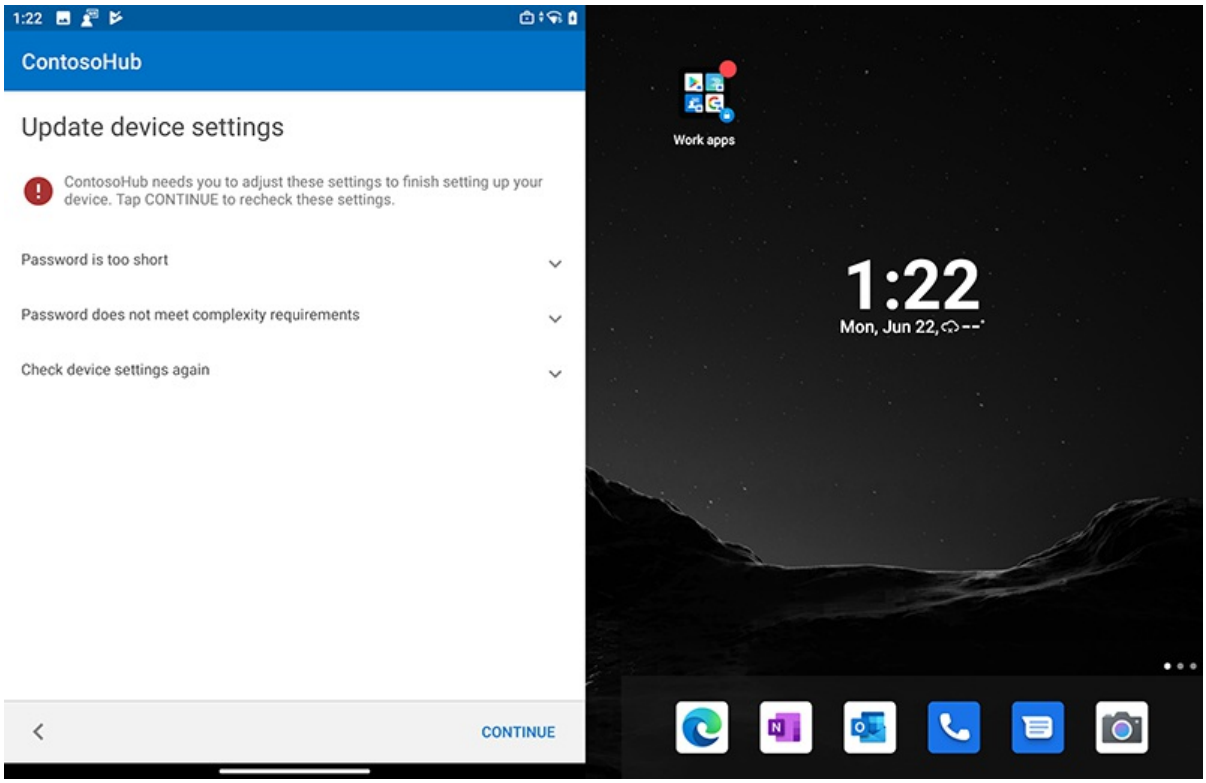
4. When the work profile setup completes, select **Continue** to activate and register the device.



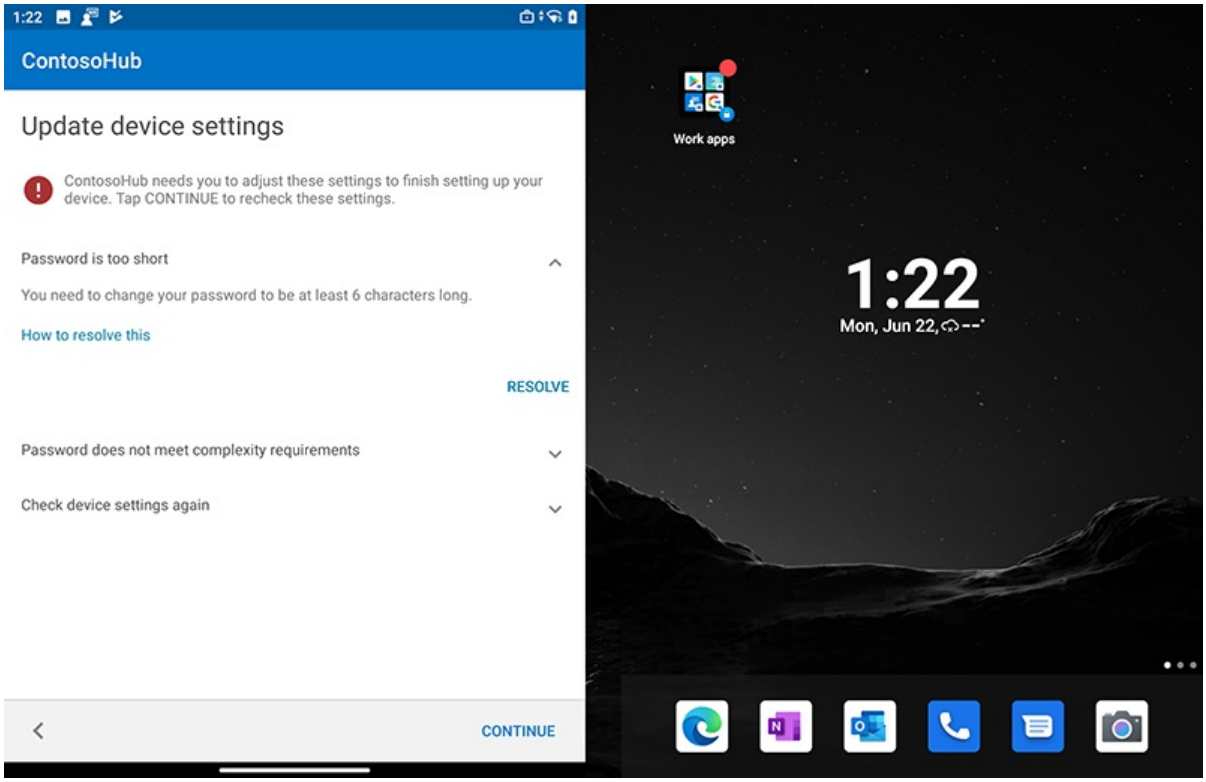
5. Select **Continue**.

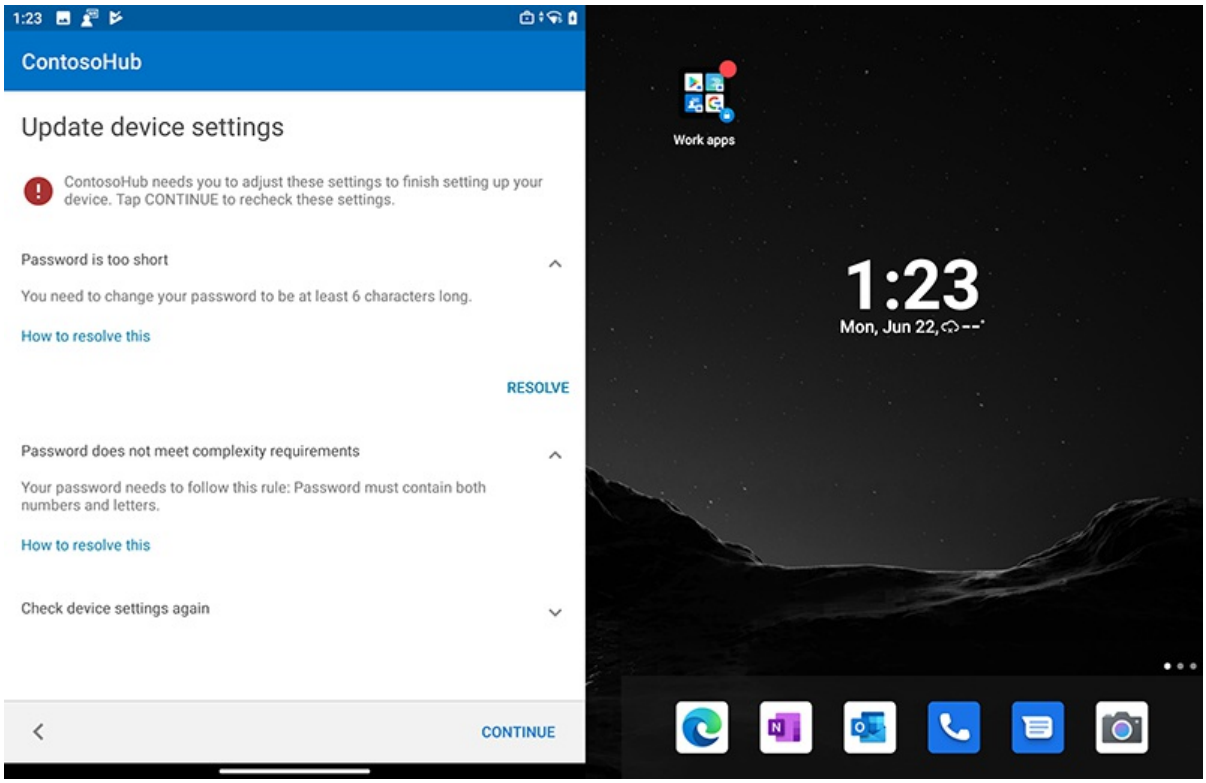


6. When you have activated the work profile, select **Continue** to update device settings. In this example, the work profile applies an MDM setting to require a stronger 6-digit alphanumeric password.



7. Select **Resolve** to enter the required authentication and then select **Continue** to complete Work Profile setup.





Learn more

- Set up enrollment of Android Enterprise work profile devices

Configure Microsoft Launcher for Surface Duo

11/2/2020 • 2 minutes to read • Edit Online

Surface Duo supports Microsoft Launcher for enterprise, an Android application that lets users personalize their phone, stay organized on the go, and seamlessly sync their Calendar, Task, Notes and more between mobile devices and their PCs. In fact, the Surface Duo launcher is a two-screen customized version of Microsoft Launcher that you can adjust to define the preferred experiences on the fully managed devices for your organization as well as allow users some options to personalize their experiences on these corporate devices. For example, you can select which apps you want pinned to the home screen, deploy a branded wallpaper, or hide a search bar while allowing users to enable the Search bar if desired.

Microsoft Launcher settings

Microsoft Launcher includes the following settings to customize the end user experience:

- Home Screen App Order User Change Allowed
- Set Grid Size
- Set Device Wallpaper
- Set Device Wallpaper User Change Allowed
- Feed Enable
- Feed Enable User Change Allowed
- Search Bar Placement
- Search Bar Placement User Change Allowed
- Dock Mode
- Dock Mode User Change Allowed

For full details of each setting, refer to Configure Microsoft Launcher for Android Enterprise with Intune.

For step by step deployment instructions, refer to How to Setup Microsoft Launcher on Android Enterprise Fully Managed Devices with Intune.

Support for Surface Duo

11/2/2020 • 2 minutes to read • Edit Online

- Online support
- Phone support

> **NOTE**
> You will be required to log into the online submission portal using your Microsoft Account or Azure Active Directory Account.

For business customers: Submit your service request.

For Microsoft Premier customers: Submit your service request on Services Hub.

Still need help? Go to Microsoft Community.

Surface Lifecycle for Android-based devices

11/2/2020 • 2 minutes to read • Edit Online

The Surface Lifecycle for Android-based devices covers Android version and security updates for Surface Duo. The lifecycle begins when a device is first released and concludes when Surface ceases publication of updates.

Surface Android device support

Surface Android devices will receive Android version and security updates for at least 3 years from its release date (September 10, 2020). In cases where the support duration is longer than 3 years, an updated end of servicing date will be published 18 months before expiration of the last planned servicing date.

The following table outlines support information for Surface Duo:

DEVICE	SUPPORTED OS AT DEVICE RELEASE	RELEASE DATE	LAST PLANNED ANDROID VERSION UPDATE	LAST PLANNED SECURITY UPDATE
Surface Duo	Android 10	September 10, 2020	September 10, 2023	September 10, 2023