BlackBerry UEM

IT Policy Reference Guide

12.23

Contents

BlackBerry UEM IT policy rules

You can use IT policies to manage the security and behavior of devices in your organization's BlackBerry UEM environment. An IT policy is a set of rules that you can use to control device features and functionality. For example, you can use IT policy rules to enforce password requirements, prevent the use of certain device features (for example, the camera), and control the availability of certain apps.

You can configure rules for all device types in the same IT policy. The device OS determines the features that can be controlled using IT policy rules. The device activation type determines which rules apply to a specific device and whether you can use rules to control the entire device or the work space only. Devices ignore IT policy rules that are not applicable.

UEM includes a default IT policy with preconfigured rules for each device type. You can change the default IT policy to meet your organization's needs. If no IT policy is assigned to a user account, a user group that a user belongs to, or a device group that a user's devices belong to, UEM sends the default IT policy to a user's devices. UEM automatically sends an IT policy to a device when a user activates it, when you update an assigned IT policy, or when a different IT policy is assigned to a user account or device.

UEM assigns only one IT policy to a device and uses predefined rules to determine which IT policy to assign. An IT policy assigned directly to a user takes precedence over an IT policy that is assigned through user group membership. If a user is a member of multiple user groups with different IT policies, ranking is used to determined which IT policy to assign. If a user's device belongs to a device group, the IT policy assigned to the device group takes precedence over an IT policy that is assigned directly to the user. If the device belongs to multiple device groups with different IT policies, ranking is used to determined which IT policy to assign.

This guide provides a detailed reference of all IT policy rules that are currently available in UEM.

iOS and iPadOS IT policy rules

The section provides details for the available IT policy rules for iOS and iPadOS devices.

iOS and iPadOS: Password rules

Name	Description	Activation types	Default	Possible values
Password required for device	Specify whether a user must set a device password.	• MDM controls • User privacy (with profile management) • User privacy - User enrollment	Not selected	
Allow simple value	Specify whether the device password can contain sequential or repeated characters, such as DEFG or 3333. Depends on: Password required for device	• MDM controls • User privacy (with profile management)	Selected	
Require alphanumeric value	Specify whether the device password must contain both letters and numbers. Depends on: Password required for device	• MDM controls • User privacy (with profile management)	Not selected	
Minimum passcode length	Specify the minimum number of characters that the device password must contain. Depends on: Password required for device	• MDM controls • User privacy (with profile management)		Minimum value: 1 character Maximum value: 16 characters
Minimum number of complex characters	Specify the minimum number of non-alphanumeric characters that the device password must contain. Depends on: Password required for device	• MDM controls • User privacy (with profile management)	Minimum value: 1 character Maximum value: 4 characters	

Name	Description	Activation types	Default	Possible values
Maximum passcode age	Specify the maximum number of days that the device password can be used. After the specified number of days elapse, the password expires and a user must set a new password. Depends on: Password required for device	• MDM controls • User privacy (with profile management)		Minimum value: 1 day Maximum value: 730 days
Maximum auto-lock	Specify the maximum value that a user can set for the auto-lock time, which is the number of minutes of user inactivity that must elapse before a device locks. If set to "None," all supported values are available on the device. If the selected value is outside of the range supported by the device, the device will use the closest value it supports. Depends on: Password required for device	• MDM controls • User privacy (with profile management)	None	• None • 1 min • 2 mins • 3 mins • 4 mins • 5 mins • 10 mins • 15 mins
Passcode history	Specify the maximum number of previous passwords that a device checks to prevent reuse. Depends on: Password required for device	• MDM controls • User privacy (with profile management)		Minimum value: 1 password Maximum value: 50 passwords

Name	Description	Activation types	Default	Possible values
Maximum grace period for device lock	Specify the maximum value that a user can set for the grace period for device lock, which is the amount of time that a device can be locked before a password is required to unlock it. If set to "None," all values are available on the device. If set to "Immediately," the password is required immediately after the device locks. Depends on: Password required for device	• MDM controls • User privacy (with profile management)	None	• None • Immediately • 1 min • 5 mins • 15 mins • 1 hr • 4 hrs
Maximum failed password attempts	Specify the number of times that a user can enter an incorrect password before a device is wiped. Depends on: Password required for device	• MDM controls • User privacy (with profile management)		Minimum value: 2 times Maximum value: 10 times
Allow password changes (supervised only)	Specify if a user can add, change, or remove the device password. Minimum OS version: 9.0.0	MDM controls	Selected	

iOS and iPadOS: Device functionality rules

Name	Description	Activation types	Default	Possible values
Allow installing apps (supervised only)	Specify whether the App Store is available on an iOS device. If this rule is not selected, the App Store icon is removed from the home screen and users can't install or update apps, including marketplace apps. If the "Allowed content ratings for apps" rule is set to "Don't allow apps", users can't install or update apps, regardless of the setting for this rule. Not supported for unsupervised devices.	MDM controls	Selected	
Allow use of camera (supervised only)	Specify whether the camera is enabled on an iOS device. If this rule is not selected, the Camera icon is removed from the home screen and users can't take photos or videos, or use FaceTime. This rule is deprecated for unsupervised devices.	MDM controls	Selected	
Allow FaceTime (supervised only)	Specify whether FaceTime is available on an iOS device. If this rule is not selected, the FaceTime icon is removed from the home screen and users can't make or receive FaceTime video calls. This rule is deprecated for unsupervised devices. Depends on: Allow use of camera (supervised only)	MDM controls	Selected	

Name	Description	Activation types	Default	Possible values
Allowed exceptions to Camera restriction (supervised only)	If present, the system exempts apps with bundle IDs in the array from the "Allow Camera" restriction. The system doesn't grant these apps access to the camera automatically; they're only exempted from the "Alllow Camera" restriction. This key has no effect when the camera isn't restricted. Minimum OS version: 26.0	MDM controls		
Denied ICCID's for iMessage and FaceTime (supervised only)	An array of strings representing ICCIDs of cellular plans. The device prevents use of any matching cellular networks in iMessage and FaceTime. The array must contain no more than 4 ICCID strings. Minimum OS version: 26.0	MDM controls		
Allow screenshots and screen recording	Specify whether users can save a screenshot of the display. For devices with iOS 9.0 and later, this rule also prevents screen recordings.	• MDM controls • User privacy (with profile management) • User privacy - User enrollment	Selected	
Allow remote screen observation in Classroom	Specify whether remote screen observation is enabled for the Classroom app. To enable this setting, Allow screenshots and screen recording must also be selected. Minimum OS version: 12.0 Depends on: Allow screenshots and screen recording	MDM controls	Selected	
Allow iPhone mirroring (supervised only)	Prevents the iPhone from mirroring to any Mac. Minimum OS version: 18.0	MDM controls	Selected	

Name	Description	Activation types	Default	Possible values
Allow call recording (supervised only)	Specify whether an iOS device can allow call recording. Minimum OS version: 18.1	MDM controls	Not selected	
Allow automatic sync while roaming	Specify whether an iOS device can synchronize data automatically while roaming. If this rule is not selected, a roaming device can synchronize data only when a user accesses an account.	MDM controls	Selected	
Allow voice dialing	Specify whether a user can make phone calls using Voice Control on an iOS device. This rule takes effect only if the "Allow Siri" rule is not selected.	MDM controls	Selected	
Allow Passbook notifications in lock screen	Specify whether an iOS device can display Passbook notifications on the lock screen.	MDM controls	Selected	
Allow in-app purchase	Specify whether users can make in-app purchases.	MDM controls	Selected	
Require iTunes Store password for all purchases	Specify whether users must enter their Apple ID password for each purchase or download. If this rule is not selected, there is a brief grace period after a purchase is made before users must authenticate for subsequent purchases. This rule takes effect only if the "Allow use of iTunes Store" rule, the "Allow installing apps" rule, or the "Allow iBook Store" rule is selected.	MDM controls	Not selected	

Name	Description	Activation types	Default	Possible values
Allow modifying cellular data app settings (supervised only)	Specify whether a user can change cellular data usage for apps on an iOS device.	MDM controls	Selected	
Allow pairing with non-Configurator hosts (supervised only)	Specify whether an iOS device can pair with a computer other than the Apple Configurator host.	MDM controls	Selected	
Autonomous apps in single app mode (supervised only)	Specify the list of apps that can request single app mode on an iOS device. You must specify the bundle ID of each app that you want to include in the list.	MDM controls		
Allow iBooks Store (supervised only)	Specify whether the iBooks Store is available on an iOS device. If this rule is not selected, users can't access the iBooks Store from the iBooks app.	MDM controls	Selected	
Allow installing configuration profiles (supervised only)	Specify whether users can install additional configuration profiles on their device.	MDM controls	Selected	
Show Today view in lock screen	Specify whether users can access the Today view in Notification Center on the lock screen.	• MDM controls • User privacy - User enrollment	Selected	
Show Notification Center in lock screen	Specify whether users can access the Notifications view in Notification Center on the lock screen.	• MDM controls • User privacy - User enrollment	Selected	
Show Control Center in lock screen	Specify whether users can access Control Center on the lock screen.	• MDM controls • User privacy - User enrollment	Selected	

Name	Description	Activation types	Default	Possible values
Allow Touch ID and Face ID to unlock device	Specify whether a user can use Touch ID and Face ID to unlock an iOS device. If this rule is not selected, the user must use a password to unlock the device.	MDM controls	Selected	
Require passcode on first AirPlay pairing	Specify whether a password is required on the first AirPlay pairing. If this rule is selected, all devices receiving AirPlay requests from a device must use a pairing password.	• MDM controls • User privacy - User enrollment	Not selected	
Allow Siri	Specify whether Siri is enabled on an iOS device. If this rule is not selected, users can't use Siri and dictation is disabled.	• MDM controls • User privacy - User enrollment	Selected	
Allow Siri while device is locked	Specify whether a user can use Siri when an iOS device is locked. This rule takes effect only if the user set a password for the device. Depends on: Allow Siri	• MDM controls • User privacy - User enrollment	Selected	
Show user-generated content in Siri (supervised only)	Specify whether Siri can search user-generated content from the Internet. Depends on: Allow Siri	MDM controls	Selected	
Enable Siri profanity filters (supervised only)	Specify if the Siri profanity filter is turned on. Depends on: Allow Siri	MDM controls	Selected	

Name	Description	Activation types	Default	Possible values
Allow dictation to be sent to Siri servers	Specify whether the device can send dictation audio to Siri servers for the purpose of improving dictation results. If this rule is not selected, the device does not send dictation audio to Apple. Minimum OS version: 14.5.0 Depends on: Allow Siri	MDM controls	Selected	
Allow translation to be sent to Siri servers	Specify whether the device can send translation audio to Siri servers for the purpose of improving translation results. If this rule is not selected, the device does not send translation audio to Apple. Minimum OS version: 15.0.0 Depends on: Allow Siri	MDM controls	Selected	
Allow backup of enterprise books	Specify whether a user can back up enterprise books.	• MDM controls • User privacy - User enrollment	Selected	
Allow notes and highlights sync for enterprise books	Specify whether a user can sync enterprise book metadata such as notes and highlights.	• MDM controls • User privacy - User enrollment	Selected	
Allow podcasts (supervised only)	Specify if a user can access podcasts using an iOS device.	MDM controls	Selected	
Allow Apple Music service (supervised only)	Specify if the Apple Music service can be used on the device. If this rule is not selected, the Music app reverts to classic mode.	MDM controls	Selected	
Allow News app (supervised only)	Specify if the user can use the News app on the device.	MDM controls	Selected	
Allow definition lookup (supervised only)	Specify if an iOS device can use the definition lookup functionality.	MDM controls	Selected	

Name	Description	Activation types	Default	Possible values
Allow predictive keyboard (supervised only)	Specify whether an iOS device can use predictive keyboards.	MDM controls	Selected	
Allow auto-correction (supervised only)	Specify whether an iOS device can use keyboard auto-correction.	MDM controls	Selected	
Allow spell check (supervised only)	Specify whether an iOS device can use keyboard spell check.	MDM controls	Selected	
Allow QuickPath keyboard (supervised only)	Specify whether users can use the QuickPath keyboard.	MDM controls	Selected	
Allow iMessage (supervised only)	Specify whether a user can use iMessage on an iOS device.	MDM controls	Selected	
Allow RCS messaging (supervised only)	Specify whether a user can use RCS messaging on an iOS device. Minimum OS version: 18.1	MDM controls	Selected	
Denied ICCID's for RCS	An array of strings representing ICCIDs of cellular plans. The device prevents use of any matching cellular networks with RCS messaging. The array must contain no more than 4 ICCID strings. Minimum OS version: 26.0	MDM controls		
Allow removing apps (supervised only)	Specify whether a user can remove apps (including marketplace apps) from an iOS device. This rule is deprecated for unsupervised devices.	MDM controls	Selected	
Allow modifying Touch ID fingerprints (supervised only)	Specify if the user can update their Touch ID fingerprint.	MDM controls	Selected	

Name	Description	Activation types	Default	Possible values
Force Apple Watch wrist detection	Specify if Apple Watch devices must use wrist detection.	• MDM controls • User privacy - User enrollment	Selected	
Allow pairing with Apple Watch (supervised only)	Specify whether an iOS device can pair with an Apple Watch.	MDM controls	Selected	
Allow Apple Watch to unlock device	Specify whether users can unlock the device from a paired Apple Watch. Minimum OS version: 14.5.0	MDM controls	Selected	
Allow keyboard shortcuts (supervised only)	Specify whether an iOS device can use keyboard shortcuts.	MDM controls	Selected	
Allow wallpaper changes (supervised only)	Specify if a user can change the wallpaper on the device.	MDM controls	Selected	
Allow radio service (supervised only)	Specify if a user can use the iTunes radio service.	MDM controls	Selected	
Allow notification changes (supervised only)	Specify if a user can change the notification settings on the device.	MDM controls	Selected	
Allow Bluetooth changes (supervised only)	Specify whether users can change the Bluetooth settings on the device.	MDM controls	Selected	
Allow Bluetooth (supervised only)	Specify whether users can use Bluetooth on the device. If you don't want to allow Bluetooth, the "Allow Bluetooth changes" rule should also not be selected. If "Allow Bluetooth changes" is selected, users can re-enable Bluetooth on the device.	MDM controls	Selected	
Allow AirPrint (supervised only)	Specify whether users can use AirPrint on the device.	MDM controls	Selected	

Name	Description	Activation types	Default	Possible values
Allow AirPrint credentials storage (supervised only)	Specify whether users can store AirPrint credentials using iCloud Keychain. Depends on: Allow AirPrint (supervised only)	MDM controls	Selected	
Force trusted certificates for TLS (supervised only)	Specify whether the device must use trusted certificates with TLS to connect to printers using AirPrint. Depends on: Allow AirPrint (supervised only)	MDM controls	Not selected	
Allow AirPrint iBeacon discovery (supervised only)	Specify whether the AirPrint app can use iBeacons to discover nearby printers. Depends on: Allow AirPrint (supervised only)	MDM controls	Selected	
Allow users to configure Wi-Fi settings (supervised only)	Specify whether users can configure Wi-Fi connections. Obsolete in OS version: 14.5.0. Use the "Allow Wi-Fi connections only to specified networks" rule instead.	MDM controls	Selected	
Force Wi-Fi to be enabled (supervised only)	Specify whether Wi-Fi is always enabled on the device. If this rule is selected, users can't turn Wi-Fi off using the Device Settings or Control Center and Airplane Mode doesn't disable Wi-Fi.	MDM controls	Not selected	
Allow changing diagnostic submission and app analytics settings (supervised only)	Specify whether users can change diagnostic submission and app analytics settings.	MDM controls	Selected	
Allow dictation (supervised only)	Specify whether users can use dictation on the device.	MDM controls	Selected	

Name	Description	Activation types	Default	Possible values
Allow Wi-Fi connections only to specified networks (supervised only)	Specify whether devices can connect only to Wi-Fi networks specified by a Wi-Fi profile. If this rule is not selected, devices can connect to networks specified by the user. Minimum OS version: 14.5.0	MDM controls	Not selected	
Allow user-configured VPN (supervised only)	Specify whether a user can add a VPN configuration to the device.	MDM controls	Selected	
Allow restart to recovery mode from untrusted host (supervised only)	Specify whether users can restart the device into recovery mode from any host computer. If this rule is not selected, the device can only be restarted into recovery mode from computers that the device has previously trusted. Minimum OS version: 14.5.0	MDM controls	Not selected	
Allow system app removal (supervised only)	Specify whether a user can remove system apps from the device.	MDM controls	Selected	
Allow USB connections when device is locked (supervised only)	Specify whether the user can connect to a USB accessory without unlocking the device. If this rule is not selected, the user must unlock the device to connect to USB accessory and enter device password periodically to maintain a USB connection for an extended time. If this rule is selected, the user never needs to enter a password to connect to a USB accessory.	MDM controls	Not selected	

Name	Description	Activation types	Default	Possible values
Force automatic date and time (supervised only)	Specify whether automatic date and time is enabled on the device. If this rule is selected, users can't disable the automatic date and time setting. If this rule is not selected, users can choose whether to enable the automatic date and time setting.	MDM controls	Not selected	
Allow password autofill (supervised only)	Specify whether the device prompts users to use saved passwords in Safari and other apps. If this rule is not selected, automatic strong passwords are also disabled and won't be suggested to users.	MDM controls	Selected	
Allow password proximity requests (supervised only)	Specify whether a device can request a password from a nearby device.	MDM controls	Selected	
Allow password sharing (supervised only)	Specify whether a user can share passwords using AirDrop.	MDM controls	Selected	
Allow the user to remove or add a cellular plan to the eSIM on the device (supervised only)	Specify whether the user is able to remove or add a cellular plan to the eSIM on the device.	MDM controls	Selected	
Allow eSIM outgoing transfers (supervised only)	Allow transfer of an eSIM from the device on which the restriction is installed to a different device. Minimum OS version: 18.0	MDM controls	Selected	
Preserve eSIM data plan on device wipe (supervised only)	Specify whether to preserve eSIM data plans when the device is wiped. Minimum OS version: 17.2.0	MDM controls	Selected	

Name	Description	Activation types	Default	Possible values
Allow changing cellular plan settings (supervised only)	Specify whether the user can change settings related to their cellular plan.	MDM controls	Selected	
Allow modifying personal hotspot settings (supervised only)	Specify whether the user can to modify the personal hotspot settings.	MDM controls	Selected	
Allow NFC (supervised only)	Specify whether a device can use NFC. Minimum OS version: 14.2.0	MDM controls	Selected	
Allow Apple personalized ads	Specify whether users can receive personalized ads from Apple. Minimum OS version: 14.0.0	MDM controls	Selected	
Allow devices to join classes automatically (supervised only)	Specify whether devices can join classes automatically without prompting the user. This rule is deprecated for unsupervised devices. Minimum OS version: 11.0.0	MDM controls	Not selected	
Allow users to leave Classroom sessions (supervised only)	Specify whether users can leave unmanaged Classroom sessions without requesting permission. This rule is deprecated for unsupervised devices. Minimum OS version: 11.3.0	MDM controls	Not selected	
Allow teachers to lock Classroom app and device (supervised only)	Specify whether teachers can lock the Classroom app and device without prompting the user. This rule is deprecated for unsupervised devices. Minimum OS version: 11.0.0	MDM controls	Not selected	
Allow shared device temporary sessions	Specify whether temporary sessions are allowed on shared devices. Minimum OS version: 13.4.0	MDM controls	Selected	

Name	Description	Activation types	Default	Possible values
Allow Live Voicemail (supervised only)	Specify whether Live Voicemail is allowed on the device. Minimum OS version: 17.2.0	MDM controls	Selected	
Allow auto dim (supervised only)	Allow auto dim on iPads with OLED displays. Minimum OS version: 17.4	MDM controls	Selected	
Allow Genmoji (supervised only)	Allow creating new Genmoji. Minimum OS version: 18.0	MDM controls	Selected	
Allow image playground (supervised only)	Allow use of image generation. Minimum OS version: 18.0	MDM controls	Selected	
Allow image wand (supervised only)	Allow use of image wand. Minimum OS version: 18.0	MDM controls	Selected	
Allow mail summary (supervised only)	Allow the system to create summaries of email messages manually. Minimum OS version: 18.1	MDM controls	Selected	
Allow personalized handwriting results (supervised only)	Allow system to generate text in the user's handwriting. Minimum OS version: 18.0	MDM controls	Selected	

iOS and iPadOS: Software update rules

Name	Description	Activation types	Default	Possible values
Delay software updates (supervised only)	Specify whether the device delays displaying software updates to the user after updates are released. You can specify the length of the delay using the "Software update delay period" rule.	MDM controls	Not selected	

Name	Description	Activation types	Default	Possible values
Software update delay period (supervised only)	Specify the number of days after a device software update is released before the software update prompt is displayed to the user. This rule takes effect only if the "Delay software updates" rule is selected. It may take up to 24 hours for the policy to take effect. For devices with iOS 18 or later, if you enable “Automatically update device OS” and specify an update schedule, the delay period that you specify in this setting is added to the update schedule. For example, if the delay period is 3 days and the update schedule is 2 days after release, the device is automatically updated 5 days after release.	MDM controls	0 days	Minimum value: 0 days Maximum value: 90 days
Recommended software update cadence (supervised only)	This value defines how the system presents software updates to the user. When there is only one update available, the system shows the update to the user. Otherwise, the updates are displayed in the specified order. Minimum OS version: 14.5.0	MDM controls	Both versions	• Both versions • Lower numbered (oldest) version • The highest numbered (most recent) release available
Automatically update device OS (supervised only)	Specify whether the device OS can be updated automatically. Note that it may take more than 24 hours for this rule to take effect.	MDM controls	Not selected	
Automatically update major versions	Specify whether major version of the device OS can be updated automatically. Depends on: Automatically update device OS (supervised only)	MDM controls	Selected	

Name	Description	Activation types	Default	Possible values
Automatically update minor versions	Specify whether minor version of the device OS can be updated automatically. Depends on: Automatically update device OS (supervised only)	MDM controls	Selected	
Automatically update patch versions	Specify whether patch version of the device OS can be updated automatically. Depends on: Automatically update device OS (supervised only)	MDM controls	Selected	
Automatically update rapid security responses	Specify whether rapid security response version of the device OS can be updated automatically. Depends on: Automatically update device OS (supervised only)	MDM controls	Selected	
Update schedule	Specify a schedule for the automatic device OS update. Depends on: Automatically update device OS (supervised only)	MDM controls	Selected	• Scheduled • Immediate
Start days after update available	Specify update schedule. Depends on: Update schedule	MDM controls	4 days	Numerical value
Start time (local device time)	Specify update schedule. Depends on: Update schedule	MDM controls	2:00	Hour: 0 to 23 Minute: 00, 15, 30, 45 Minimum value: 0:00 Maximum value: 23:45

iOS and iPadOS: Apps rules

Name	Description	Activation types	Default	Possible values
Allow use of iTunes Store (supervised only)	Specify whether the iTunes Store is available on an iOS device. If this rule is not selected, the iTunes Store icon is removed from the home screen and users can't preview, purchase, or download content. This rule is deprecated for unsupervised devices.	MDM controls	Selected	
Force limited ad tracking	Specify whether apps on an iOS device can use the Advertising Identifier (a non-permanent device identifier) to provide targeted ads to users.	MDM controls	Not selected	
Allow use of Safari (supervised only)	Specify whether Safari is available on an iOS device. If this rule is not selected, the Safari icon is removed from the home screen and users can't use Safari or open any Web Clips, including BlackBerry Work Apps, on the device. This rule is deprecated for unsupervised devices.	MDM controls	Selected	
Enable autofill (supervised only)	Specify whether Safari remembers information that users enter in web forms. This rule is deprecated for unsupervised devices. Depends on: Allow use of Safari (supervised only)	MDM controls	Selected	
Force fraud warning	Specify whether Safari warns users when they visit websites identified as fraudulent or compromised. Depends on: Allow use of Safari (supervised only)	• MDM controls • User privacy - User enrollment	Not selected	

Name	Description	Activation types	Default	Possible values
Enable JavaScript	Specify whether Safari allows websites to run JavaScript. Depends on: Allow use of Safari (supervised only)	MDM controls	Selected	
Block pop-ups	Specify whether pop-up blocking is enabled in Safari. Depends on: Allow use of Safari (supervised only)	MDM controls	Not selected	
Allow cookies and cross-site tracking	Specify whether Safari can accept cookies and whether users can enable cross-site tracking. You can both prevent cross-site tracking and block all cookies, only prevent cross-site tracking, or only prevent cross-site tracking but allow users to change the Prevent Cross-Site Tracking setting. Depends on: Allow use of Safari (supervised only)	MDM controls	Enable Prevent Cross-Site Tracking	• Enable Prevent Cross-Site Tracking and Block All Cookies • Enable Prevent Cross-Site Tracking • Enable Prevent Cross-Site Tracking and allow users to disable it
Allow Safari private browsing (supervised only)	If "false", the system disables the ability to use private browsing in Safari. Minimum OS version: 26.0	MDM controls	Selected	
Allow Safari history clearing (supervised only)	If "false", the system disables the ability to clear browsing history in Safari. Minimum OS version: 26.0	MDM controls	Selected	
Allow finding devices in the Find My app (supervised only)	Specify whether users can use the Find My app to locate their devices.	MDM controls	Selected	

Name	Description	Activation types	Default	Possible values
Allow finding friends in the Find My app (supervised only)	Specify whether users can use the Find My app to locate their friends.	MDM controls	Selected	
Allow modifying Find My Friends settings (supervised only)	Specify whether users can change settings in the Find My Friends app if it is installed on the device. If this rule is not selected and location services is turned on, users can't turn location services off on the device.	MDM controls	Selected	
Allow use of Game Center (supervised only)	Specify whether Game Center is available on an iOS device. If this rule is not selected, the Game Center icon is removed from the home screen and users can't use Game Center.	MDM controls	Selected	
Allow multiplayer gaming (supervised only)	Specify whether users can play multiplayer games that support Game Center. If this rule is selected and the "Allow adding Game Center friends" rule is not selected, users can play multiplayer games only with existing friends. If this rule is not selected, users can't play multiplayer games or add friends in Game Center. This rule is deprecated for unsupervised devices. Depends on: Allow use of Game Center (supervised only)	MDM controls	Selected	

Name	Description	Activation types	Default	Possible values
Allow adding Game Center friends (supervised only)	Specify whether users can send and receive friend requests in Game Center. The "Allow multiplayer gaming" rule must also be selected to allow users to add friends in Game Center. This rule is deprecated for unsupervised devices. Depends on: Allow use of Game Center (supervised only)	MDM controls	Selected	
Allow AirDrop (supervised only)	Specify whether AirDrop is enabled on an iOS device. If this rule is not selected, users can't use AirDrop with any apps and the AirDrop option is removed from Control Center.	MDM controls	Selected	
Allow Internet results in Spotlight (supervised only)	Specify whether a Spotlight search returns Internet search results when searching for content on a device.	MDM controls	Selected	
Force AirDrop to be unmanaged	Specify whether AirDrop is unmanaged as a drop target.	• MDM controls • User privacy - User enrollment	Not selected	
Allow App Store (supervised only)	Specify whether the App Store is available on an iOS device. Users can still use host apps (iTunes, Configurator) to install or update apps.	MDM controls	Selected	
Allow marketplace apps (supervised only)	Specify whether users are allowed to install alternative marketplace apps. Minimum OS version: 17.4	MDM controls	Selected	
Allow web distribution apps (supervised only)	Specify whether users are allowed to install web distribution apps. Minimum OS version: 17.5	MDM controls	Selected	

Name	Description	Activation types	Default	Possible values
Allow automatic app downloads (supervised only)	Specify whether the device automatically downloads apps purchased on other devices. This does not affect updates to existing apps.	MDM controls	Selected	
Allow enterprise app trust modifications (supervised only)	Specify whether the user can change the enterprise app trust settings on the device.	MDM controls	Selected	
Allow enterprise apps to be trusted	Specify whether the device can trust enterprise apps.	MDM controls	Selected	
Allow Files app to use USB (supervised only)	Specify whether the Files app can access files using a USB connection.	MDM controls	Selected	
Allow Files app to connect to network drives (supervised only)	Specify whether the Files app can access files stored on a network drive.	MDM controls	Selected	
Allow App Clips (supervised only)	Allow users to add some App Clips and remove existing App Clips on the device. Minimum OS version: 14.0.0	MDM controls	Selected	
Allow hiding apps (supervised only)	Allow users to hide apps. It does not affect the user's ability to leave it in the App Library, while removing it from the home screen. Minimum OS version: 18.0	MDM controls	Selected	

Name	Description	Activation types	Default	Possible values
Allow locking apps (supervised only)	Allow users to lock apps. Because hiding apps also requires locking them, disallowing locking also disallows hiding. Minimum OS version: 18.0	MDM controls	Selected	
Allow default browser modification (supervised only)	If false, disables default browser preference modification. The MDM Settings command to set the default browser preference will still work when this is applied. Minimum OS version: 18.2	MDM controls	Selected	

iOS and iPadOS: iCloud rules

Name	Description	Activation types	Default	Possible values
Allow iCloud backup (supervised only)	Specify whether users can back up their device to iCloud. This rule is deprecated for unsupervised devices.	MDM controls	Selected	
Allow iCloud documents and data (supervised only)	Specify whether users can store documents in iCloud. This rule is deprecated for unsupervised devices.	MDM controls	Selected	
Allow My Photo Stream (disallowing can cause data loss)	Specify whether users can turn on My Photo Stream. If this rule is not selected, photos in My Photo Stream are removed from the device and photos in the Camera Roll are no longer added to My Photo Stream. If there are no other copies of these photos, they may be lost.	MDM controls	Selected	

Name	Description	Activation types	Default	Possible values
Allow iCloud photo sharing	Specify whether users can turn on iCloud photo sharing. If this rule is selected, users can create shared streams of photos and videos to share with other people or subscribe to shared streams. If this rule is not selected, photos and videos in shared streams can no longer be viewed on the device. If there are no other copies of these photos and videos, they may be lost.	MDM controls	Selected	
Allow managed apps to store data in iCloud	Specify whether managed apps can use cloud sync.	• MDM controls • User privacy - User enrollment	Selected	
Allow iCloud Keychain (supervised only)	Specify if users can use iCloud Keychain on a device. This rule is deprecated for unsupervised devices.	MDM controls	Selected	
Allow iCloud Photo Library (supervised only)	Specify whether users can upload photos to iCloud Photo Library.	MDM controls	Selected	
Enable activation lock (supervised only)	Specify whether the user must enter their Apple ID and password to reactivate the device. This feature prevents reactivation of lost or stolen devices. Administrators can bypass the activation lock to give the device to a different user.	MDM controls	Not selected	
Allow Cloud Private Relay (supervised only)	If false, the system disables iCloud Private Relay. Requires a supervised device in iOS. Support for this restriction on unsupervised devices is deprecated. Minimum OS version: 15.x	MDM controls	Selected	

iOS and iPadOS: Content ratings rules

Name	Description	Activation types	Default	Possible values
Allow playback of explicit music, podcasts, and iTunes U media (supervised only)	Specify whether explicit music or video content purchased from the iTunes Store or listed in iTunes U is available on an iOS device. Explicit content is flagged by content providers, such as record labels, when sold through the iTunes Store or distributed through iTunes U. If this rule is not selected, explicit music or video content on the device is hidden and users can't preview, purchase, or download explicit music or video content. This rule is deprecated for unsupervised devices.	MDM controls	Selected	
Allow explicit sexual content in iBooks Store	Specify whether explicit sexual content purchased from the iBooks Store is available on an iOS device. Explicit content is flagged by content providers when sold through the iBooks Store. If this rule is not selected, explicit books on the device are hidden and users can't preview, purchase, or download books with explicit sexual content.	MDM controls	Selected	

Name	Description	Activation types	Default	Possible values
Ratings region	Specify the region that an iOS device uses for content ratings.	MDM controls	United States	• Australia • Canada • France • Germany • Ireland • Japan • New Zealand • United Kingdom • United States
Allowed content ratings for movies	Specify the maximum allowed rating for movies that users can download from the iTunes Store. Use this rule to block access to new and existing movies that exceed a maximum rating. If set to "Don't allow movies," all movies purchased from the iTunes Store are hidden and users can't preview, purchase, or download movies. If set to something other than "Don't allow movies," the "Allow use of iTunes Store" rule must also be selected to allow users to download content. The "Ratings region" rule determines which ratings system is used. Depends on: Ratings region	MDM controls	Allow all movies	• Don't allow movies • G • PG • M • MA15+ • R18+ • Allow all movies

Name	Description	Activation types	Default	Possible values
Allowed content ratings for TV shows	Specify the maximum allowed rating for TV shows that users can download from the iTunes Store. Use this rule to block access to new and existing TV shows that exceed a maximum rating. If set to "Don't allow TV shows," all TV shows purchased from the iTunes Store are hidden and users can't preview, purchase, or download TV shows. If set to something other than "Don't allow TV shows," the "Allow use of iTunes Store" rule must also be selected to allow users to download content. The "Ratings region" rule determines which ratings system is used. Depends on: Ratings region	MDM controls	Allow all TV shows	• Don't allow TV shows • P • C • G • PG • M • MA15+ • AV15+ • Allow all TV shows
Allowed content ratings for apps	Specify the maximum allowed rating for apps that users can download from the App Store. Use this rule to block access to new and existing apps that exceed a maximum rating. This rule does not apply to built-in iOS apps. If set to "Don't allow apps," all apps purchased from the App Store are hidden and users can't install or update apps. If set to something other than "Don't allow apps," the "Allow installing apps" rule must also be selected to allow users to install and update apps.	MDM controls	Allow all apps	• Don't allow apps • 4+ • 9+ • 12+ • 17+ • Allow all apps

iOS and iPadOS: Security and privacy rules

Name	Description	Activation types	Default	Possible values
Allow users to accept untrusted TLS certificates	Specify whether users are prompted to trust certificates that can't be verified. This rule applies to Safari and to Mail, Contacts, and Calendar accounts.	MDM controls	Selected	
Force encrypted backups	Specify whether device backups performed in iTunes must be stored in an encrypted format on the computer. Minimum OS version: 8.0.0	• MDM controls • User privacy - User enrollment	Not selected	
Allow modifying account settings (supervised only)	Specify whether a user can change account settings on an iOS device. If this rule is not selected, users can't create new accounts or change their user name, password, or other settings associated with their accounts.	MDM controls	Selected	
Allow automatic updates to certificate trust settings	Specify whether an iOS device allows updates for trusted certificates over a wireless connection.	MDM controls	Selected	
Allow documents from managed sources in unmanaged destinations	Specify whether users can open documents and attachments from managed apps and accounts in personal apps.	• MDM controls • User privacy (with profile management) • User privacy - User enrollment	Selected	
Allow documents from unmanaged sources in managed destinations	Specify whether users can open documents and attachments from personal apps and accounts in managed apps.	• MDM controls • User privacy (with profile management) • User privacy - User enrollment	Selected	

Name	Description	Activation types	Default	Possible values
Allow copy and paste between documents from managed and unmanaged sources	Specify whether copy and paste of content between documents from managed and unmanaged sources respects the settings for the "Allow documents from managed sources in unmanaged destinations" and "Allow documents from unmanaged sources in managed destinations" rules. For example, if this rule is selected, you can copy from an unmanaged source to a managed destination document, only if documents from unmanaged sources are allowed in managed destinations. Minimum OS version: 15.0.0	MDM controls	Selected	
Allow sending diagnostic and usage data to Apple	Specify whether users can choose to send diagnostic and usage data to Apple.	• MDM controls • User privacy - User enrollment	Selected	
Allow Erase All Content and Settings (supervised only)	Specify whether a user can use the "Erase All Content And Settings" option on a device to wipe it.	MDM controls	Selected	
Allow configuring restrictions (supervised only)	Specify whether a user can use the "Enable Restrictions" option to prevent access to apps or features on a device. On iOS 12 and later, this rule also allows the use of Screen Time.	MDM controls	Selected	
Allow Handoff	Specify whether a user can use the activity continuation feature to transfer user activities among multiple devices associated with the user.	MDM controls	Selected	
Allow device name changes (supervised only)	Specify if a user can change the device name.	MDM controls	Selected	

Name	Description	Activation types	Default	Possible values
Require authentication before autofill of sensitive data (supervised only)	Specify whether users must authenticate with the device before Safari and other apps autofill passwords or credit card information. This rule is supported only on devices with Face ID and Touch ID.	MDM controls	Selected	
Allow automatic setup of new devices (supervised only)	Specify whether the device can be used for automatic setup of a new device. If this rule is not selected, the device doesn't display a prompt to set up new devices that are in proximity.	MDM controls	Selected	
Allow Mail Privacy Protection (supervised only)	Specify whether mail protection is enabled. Minimum OS version: 15.2.0	MDM controls	Selected	
Allow Rapid Security Response Installation (supervised only)	Specify whether rapid security response is enabled. Minimum OS version: 16.0.0	MDM controls	Selected	
Allow Rapid Security Response Removal (supervised only)	Specify whether users can disable rapid security response. Minimum OS version: 16.0.0	MDM controls	Selected	
Allow writing tools (supervised only)	Allow Apple Intelligence writing tools. Minimum OS version: 18.0	MDM controls	Selected	
Allow external intelligence integrations (supervised only)	If false, disables the use of external, cloud-based intelligence services with Siri. Minimum OS version: 18.2	MDM controls	Selected	

Name	Description	Activation types	Default	Possible values
Allow external intelligence integrations sign-in (supervised only)	If false, forces external intelligence providers into anonymous mode. If a user is already signed in to an external intelligence provider, applying this restriction will cause them to be signed out. Minimum OS version: 18.2 Depends on: Allow external intelligence integrations (supervised only)	MDM controls	Selected	
Allow use of satellite connectivity (supervised only)	If false, the connection to and use of satellite services is prohibited. Minimum OS version: 18.2	MDM controls	Selected	
Allowed External Intelligence Workspace IDs (supervised only)	If present, Apple Intelligence will only allow the given external integration workspace ID to be used, and will require a sign-in in order to make requests; the user will be required to sign in to integrations that support signing in. Minimum OS version: 18.3	MDM controls		
Notes transcription summary (supervised only)	If false, disables transcription summarization in Notes. Minimum OS version: 18.3	MDM controls	Selected	
Allow Visual Intelligence Summary (supervised only)	When false, disables visual intelligence summarization. Minimum OS version: 18.3	MDM controls	Selected	
Allow Apple Intelligence Report (supervised only)	If false, disables Apple Intelligence report. Minimum OS version: 18.4	MDM controls	Selected	
Allow default calling app modification (supervised only)	If false, disables default calling app modification. Minimum OS version: 18.4	MDM controls	Selected	

Name	Description	Activation types	Default	Possible values
Allow default messaging app modification (supervised only)	If false, disables default messaging app modification. Minimum OS version: 18.4	MDM controls	Selected	
Allow Mail smart replies (supervised only)	If false, disables mail smart replies. Minimum OS version: 18.4	MDM controls	Selected	
Allow Notes transcription (supervised only)	If false, disables notes transcription. Minimum OS version: 18.4	MDM controls	Selected	
Allow Safari summary (supervised only)	If false, disables Safari summarization. Minimum OS version: 18.4	MDM controls	Selected	

macOS IT policy rules

The section provides details for the available IT policy rules for macOS devices.

macOS: Password rules

Name	Description	Activation types	Default	Possible values
IT policy rules target	This rule specifies whether the IT policy rules for the password apply only to the assigned user's account or to the entire device. Minimum OS version: 10.8.0	MDM controls	User	• User • Device
Password required for device	Specify whether a user must set a password.	MDM controls	Not selected	
Allow simple value	Specify whether the password can contain sequential or repeated characters, such as ABCD or 3333. Depends on: Password required for device	MDM controls	Selected	
Require alphanumeric value	Specify whether the password must contain both letters and numbers. Depends on: Password required for device	MDM controls	Not selected	
Minimum password length	Specify the minimum number of characters that the password must contain. Depends on: Password required for device	MDM controls		Minimum value: 1 character Maximum value: 16 characters
Minimum number of complex characters	Specify the minimum number of non-alphanumeric characters that the password must contain. Depends on: Password required for device	MDM controls		Minimum value: 1 character Maximum value: 4 characters

Name	Description	Activation types	Default	Possible values
Maximum password age	Specify the maximum number of days that the password can be used. After the specified number of days elapse, the password expires and the user must set a new password. Depends on: Password required for device	MDM controls		Minimum value: 1 day Maximum value: 730 days
Maximum auto-lock	Specify the maximum value that a user can set for the auto-lock time, which is the number of minutes of user inactivity that must elapse before a device locks. If set to "None," the user can select any value. Depends on: Password required for device	MDM controls	None	• None • 1 min • 2 mins • 3 mins • 4 mins • 5 mins
Password history	Specify the maximum number of previous passwords that a device checks to prevent reuse. Depends on: Password required for device	MDM controls		Minimum value: 1 previous password Maximum value: 50 previous passwords
Maximum grace period for device lock	Specify the maximum value that a user can set for the grace period for device lock, which is the amount of time that a device can be locked before a password is required to unlock it. If set to "None," all values are available on the device. If set to "Immediately," the password is required immediately after the device locks. Depends on: Password required for device	MDM controls	None	• None • Immediately • 1 min • 5 mins • 15 mins • 1 hr • 4 hrs

Name	Description	Activation types	Default	Possible values
Maximum failed password attempts	Specify the number of times that a user can enter an incorrect password before a device is wiped. Depends on: Password required for device	MDM controls	10 attempts	Minimum value: 2 attempts Maximum value: 10 attempts

macOS: Device functionality rules

Name	Description	Activation types	Default	Possible values
Enable Bluetooth	Specify whether Bluetooth is enabled or disabled when the policy is sent to the device. Regardless of the setting of this rule, users can change the Bluetooth setting on their device at any time. Minimum OS version: 10.13.4	MDM controls	Selected	

Android IT policy rules

The section provides details for the available IT policy rules for Android devices.

Android: Password rules

Global (all Android devices)

Name	Description	Activation Types	Default	Possible Values
Password complexity	Specify the minimum complexity level for the device password. Low complexity allows patterns and PINs with repeating or sequential values. Medium complexity requires PINs with no repeating or sequential values and a minimum length of 4 or a password with a minimum length of 4. High complexity requires PINs with no repeating or sequential values and minimum length of 8 or a password with a minimum length of 6. Applies only to devices with Android OS 12 or later with a user privacy activation type (Android Enterprise and Android Management).	• Work and personal - user privacy • Work and personal - user privacy (Premium) • Work and personal - user privacy (Android Management)	Low	• Low • Medium • High • None

Name	Description	Activation Types	Default	Possible Values
Password requirements	Specify the minimum requirements for a device password. If set to "Unspecified," a user does not need to set a password. If set to "Something," the user must set a password but there are no requirements for length or quality. If set to "Numeric," "Alphabetic," or "Alphanumeric," the password must contain at least the specified character types and can also include other character types. If set to "Complex," you can set specific requirements for different character types. Password requirement policy rules are no longer applicable to user privacy activation types (Android Enterprise and Android Management); for user privacy activations, use the Password complexity rule instead.	• Work space only • Work space only (Premium) • Work space only (Android Management) • Work and personal - full control • Work and personal - full control (Premium) • Work and personal - full control (Android Management)	Unspecified	• Unspecified • Something • Numeric • Alphabetic • Alphanumeric • Complex
Minimum password length	Specify the minimum number of characters that the device password must contain. This rule takes effect only if the "Password requirements" rule is set to "Numeric," "Alphabetic," "Alphanumeric," or "Complex." Password requirement policy rules are no longer applicable to user privacy activation types (Android Enterprise and Android Management); for user privacy activations, use the Password complexity rule instead. Depends on: Password requirements	• Work space only • Work space only (Premium) • Work space only (Android Management) • Work and personal - full control • Work and personal - full control (Premium) • Work and personal - full control (Android Management)	4 characters	Minimum: 4 characters Maximum: 16 characters

Name	Description	Activation Types	Default	Possible Values
Maximum failed password attempts	Specify the number of times that a user can enter an incorrect password before a device is wiped or deactivated. Password requirement policy rules are no longer applicable to user privacy activation types (Android Enterprise and Android Management); for user privacy activations, use the Password complexity rule instead. Depends on: Password requirements	• Work space only • Work space only (Premium) • Work space only (Android Management) • Work and personal - full control • Work and personal - full control (Premium) • Work and personal - full control (Android Management)		Minimum: 0 attempts Maximum: 2147483647 attempts
Maximum inactivity time lock	Specify the maximum number of minutes of user inactivity that must elapse before a device locks. On Android devices with a work profile, the work space also locks. Users can set a shorter time period on the device. Password requirement policy rules are no longer applicable to user privacy activation types (Android Enterprise and Android Management); for user privacy activations, use the Password complexity rule instead. Depends on: Password requirements	• Work space only • Work space only (Premium) • Work space only (Android Management) • Work and personal - full control • Work and personal - full control (Premium) • Work and personal - full control (Android Management)		Minimum: 1 minute Maximum: 60 minutes

Name	Description	Activation Types	Default	Possible Values
Secondary authentication timeout	Specify the maximum amount of time, in hours, that the user can use secondary authentication methods, such as a fingerprint, before the user must unlock the device with a strong authentication method such as a password. The maximum is 72 hours. If set to 0, a timeout value is not sent to the device. Password requirement policy rules are no longer applicable to user privacy activation types (Android Enterprise and Android Management); for user privacy activations, use the Password complexity rule instead. Depends on: Password requirements	• Work space only • Work space only (Premium) • Work space only (Android Management) • Work and personal - full control • Work and personal - full control (Premium) • Work and personal - full control (Android Management)		Minimum: 0 hours Maximum: 72 hours
Password expiration timeout	Specify the maximum amount of time that the device password can be used. After the specified amount of time elapses, the password expires and a user must set a new password. If set to 0, the password does not expire. Password requirement policy rules are no longer applicable to user privacy activation types (Android Enterprise and Android Management); for user privacy activations, use the Password complexity rule instead. Depends on: Password requirements	• Work space only • Work space only (Premium) • Work space only (Android Management) • Work and personal - full control • Work and personal - full control (Premium) • Work and personal - full control (Android Management)		Minimum: 0 seconds Max: 9223372036854770 seconds

Name	Description	Activation Types	Default	Possible Values
Password history restriction	Specify the maximum number of previous passwords that a device checks to prevent a user from reusing a device password. If set to 0, the device does not check previous passwords. This rule takes effect only if the "Password requirements" rule is set to "Numeric," "Alphabetic," "Alphanumeric," or "Complex." Password requirement policy rules are no longer applicable to user privacy activation types (Android Enterprise and Android Management); for user privacy activations, use the Password complexity rule instead. Depends on: Password requirements	• Work space only • Work space only (Premium) • Work space only (Android Management) • Work and personal - full control • Work and personal - full control (Premium) • Work and personal - full control (Android Management)		Minimum: 0 passwords Maximum: 2147483647 passwords
Minimum uppercase letters required in password	Specify the minimum number of uppercase letters that the device password must contain. This rule takes effect only if you set the "Password requirements" rule to "Complex." Password requirement policy rules are no longer applicable to user privacy activation types (Android Enterprise and Android Management); for user privacy activations, use the Password complexity rule instead. Depends on: Password requirements	• Work space only • Work space only (Premium) • Work space only (Android Management) • Work and personal - full control • Work and personal - full control (Premium) • Work and personal - full control (Android Management)		Minimum: 0 letters Maximum: 2147483647 letters

Name	Description	Activation Types	Default	Possible Values
Minimum lowercase letters required in password	Specify the minimum number of lowercase letters that the device password must contain. This rule takes effect only if you set the "Password requirements" rule to "Complex." Password requirement policy rules are no longer applicable to user privacy activation types (Android Enterprise and Android Management); for user privacy activations, use the Password complexity rule instead. Depends on: Password requirements	• Work space only • Work space only (Premium) • Work space only (Android Management) • Work and personal - full control • Work and personal - full control (Premium) • Work and personal - full control (Android Management)		Minimum: 0 letters Maximum: 2147483647 letters
Minimum letters required in password	Specify the minimum number of letters that the device password must contain. This rule takes effect only if you set the "Password requirements" rule to "Complex." Password requirement policy rules are no longer applicable to user privacy activation types (Android Enterprise and Android Management); for user privacy activations, use the Password complexity rule instead. Depends on: Password requirements	• Work space only • Work space only (Premium) • Work space only (Android Management) • Work and personal - full control • Work and personal - full control (Premium) • Work and personal - full control (Android Management)		Minimum: 0 letters Maximum: 2147483647 letters

Name	Description	Activation Types	Default	Possible Values
Minimum non-letters in password	Specify the minimum number of non-letter characters (numbers or symbols) required in the password. This rule takes effect only if you set the "Password requirements" rule to "Complex." Password requirement policy rules are no longer applicable to user privacy activation types (Android Enterprise and Android Management); for user privacy activations, use the Password complexity rule instead. Depends on: Password requirements	• Work space only • Work space only (Premium) • Work space only (Android Management) • Work and personal - full control • Work and personal - full control (Premium) • Work and personal - full control (Android Management)	0 characters	Minimum: 0 characters Maximum: 16 characters
Minimum numerical digits required in password	Specify the minimum number of numerals that the device password must contain. This rule takes effect only if you set the "Password requirements" rule to "Complex." Password requirement policy rules are no longer applicable to user privacy activation types (Android Enterprise and Android Management); for user privacy activations, use the Password complexity rule instead. Depends on: Password requirements	• Work space only • Work space only (Premium) • Work space only (Android Management) • Work and personal - full control • Work and personal - full control (Premium) • Work and personal - full control (Android Management)		Minimum: 0 numerals Maximum: 2147483647 numerals

Name	Description	Activation Types	Default	Possible Values
Minimum symbols required in password	Specify the minimum number of non-alphanumeric characters that the device password must contain. For Android devices, a complex password must contain at least one non-alphanumeric character. This rule takes effect only if you set the "Password requirements" rule to "Complex." Password requirement policy rules are no longer applicable to user privacy activation types (Android Enterprise and Android Management); for user privacy activations, use the Password complexity rule instead. Depends on: Password requirements	• Work space only • Work space only (Premium) • Work space only (Android Management) • Work and personal - full control • Work and personal - full control (Premium) • Work and personal - full control (Android Management)		Minimum: 0 characters Maximum: 2147483647 characters

Global (Samsung Knox devices only)

Name	Description	Activation Types	Default	Possible Values
Allow facial authentication	Specify whether a user can authenticate with the device using facial recognition. Applies only to devices that support Samsung Knox API level 3 and later.	• Work and personal - full control (Samsung Knox) • Work space only • Work space only (Premium) • Work and personal - full control • Work and personal - full control (Premium)	Selected	

Name	Description	Activation Types	Default	Possible Values
Allow iris authentication	Specify whether a user can authenticate with the device using an iris scan. Applies only to devices that support Samsung Knox MDM version 5.1.0 and later.	• Work and personal - full control (Samsung Knox) • Work space only • Work space only (Premium)	Selected	
Maximum numeric sequence length	Specify the maximum length of the numeric sequence that is allowed in the device password. Only applies when device password quality is Numeric, Alphanumeric or Complex. Applies only to devices that support Samsung Knox API level 4 and later.	• Work space only • Work space only (Premium) • Work and personal - full control • Work and personal - full control (Premium)		Minimum: 0 characters Maximum: 16 characters
Minimum number of changed characters for new device passwords	Specify the minimum number of changed characters that a new password must include compared to the previous password. Knox calculates the difference between the two passwords using the Levenshtein algorithm. Characters can be numeric, alphabetic, or symbolic. According to the Levenshtein algorithm, strings like "test" and "best" differ from each other by one unit. "Test" and "toad" differ from each other by three units. "Test" and "est" differ from each other by one unit. If set to 0, no restrictions are applied. Applies only to devices that support Samsung Knox API level 6 and later.	• Work space only • Work space only (Premium) • Work and personal - full control • Work and personal - full control (Premium)		Minimum: 0 characters Maximum: 16 characters

Name	Description	Activation Types	Default	Possible Values
Allow device password visibility	Specify whether the Device password is visible when a user is typing it. If this rule is not selected, users and apps cannot change the visibility setting. Applies only to devices that support Samsung Knox API level 6 and later.	• Work and personal - full control • Work and personal - full control (Premium)	Selected	
Require lock screen message	Specify whether you set a message to display when the device is locked. If this rule is not selected, the user can choose a message to display on the lock screen. Applies only to devices that support Samsung Knox API level 2 and later.	• Work space only • Work space only (Premium) • Work and personal - full control • Work and personal - full control (Premium)	Not selected	
Lock screen message	Specify the text to display on the device when the device is locked. Applies only to devices that support Samsung Knox API level 6 and later. Depends on: Require lock screen message	• Work space only • Work space only (Premium) • Work and personal - full control • Work and personal - full control (Premium)		Maximum: 300 characters
Maximum character sequence length	Specify the maximum length of the character sequence that is allowed in the device password. Only applies when device password quality is Alphabetic, Alphanumeric or Complex. Applies only to devices that support Samsung Knox API level 6 and later.	• Work space only • Work space only (Premium) • Work and personal - full control • Work and personal - full control (Premium)		Minimum: 0 characters Maximum: 16 characters

Work profile (all Android devices)

Name	Description	Activation Types	Default	Possible Values
Force device to request password for work profile	Specify whether the device always requests a password to unlock the work profile. When this rule is selected, unlocking the device doesn't unlock the work profile, even if the device and work profile passwords are the same.	• Work and personal - user privacy • Work and personal - user privacy (Premium) • Work and personal - full control • Work and personal - full control (Premium)	Not Selected	

Name	Description	Activation Types	Default	Possible Values
Password requirements	Specify the minimum requirements for a work profile password. If set to "Something," the user must set a password but there are no requirements for length or quality. If set to "Numeric," "Alphabetic," or "Alphanumeric," the password must contain at least the specified character types and can also include other character types. If set to "Complex," the password must contain at least a letter, number and special symbol. If set to "Numeric Complex," the password must contain numeric characters with no repeating sequence (4444) or ordered sequence (1234, 4321, 2468). If set to "Biometric Weak," the password allows for low-security biometric recognition technology.	• Work space only • Work space only (Premium) • Work space only (Android Management) • Work and personal - user privacy • Work and personal - user privacy (Premium) • Work and personal - user privacy (Android Management) • Work and personal - full control • Work and personal - full control (Premium) • Work and personal - full control (Android Management)	Something	• Something • Numeric • Numeric Complex • Alphabetic • Alphanumeric • Biometric Weak • Complex

Name	Description	Activation Types	Default	Possible Values
Maximum failed password attempts	Specify the number of times that a user can enter an incorrect work profile password before the device is deactivated and the work profile is removed. This rule takes effect only if the "Password requirements" rule is set to something other than "Unspecified." Depends on: Password requirements	• Work space only • Work space only (Premium) • Work space only (Android Management) • Work and personal - user privacy • Work and personal - user privacy (Premium) • Work and personal - user privacy (Android Management) • Work and personal - full control • Work and personal - full control (Premium) • Work and personal - full control (Android Management)	0 attempts	Minimum value: 0 attempts Maximum value: 2147483647 attempts

Name	Description	Activation Types	Default	Possible Values
Maximum inactivity time lock	Specify the maximum number of minutes of user inactivity that must elapse before the device and work space lock. If you set a value for both this rule and the global "Maximum inactivity time lock" rule, both the device and work space will lock when either timer expires. Users can set a shorter time period on the device. This rule takes effect only if the "Password requirements" rule is set to something other than "Unspecified." Depends on: Password requirements	• Work space only • Work space only (Premium) • Work space only (Android Management) • Work and personal - user privacy • Work and personal - user privacy (Premium) • Work and personal - user privacy (Android Management) • Work and personal - full control • Work and personal - full control (Premium) • Work and personal - full control (Android Management)		Minimum value: 0 minutes Maximum value: 60 minutes

Name	Description	Activation Types	Default	Possible Values
Secondary authentication timeout	Specify the maximum amount of time, in hours, that the user can use secondary authentication methods, such as a fingerprint, before the user must unlock the device with a strong authentication method such as a password. The maximum is 72 hours. If set to 0, a timeout value is not sent to the device. This rule takes effect only if the "Password requirements" rule is set to something other than "Unspecified." Depends on: Password requirements	• Work space only • Work space only (Premium) • Work space only (Android Management) • Work and personal - user privacy • Work and personal - user privacy (Premium) • Work and personal - user privacy (Android Management) • Work and personal - full control • Work and personal - full control (Premium) • Work and personal - full control (Android Management)		Minimum value: 0 hours Maximum value: 72 hours

Name	Description	Activation Types	Default	Possible Values
Password expiration timeout	Specify the maximum amount of time that the work profile password can be used. After the specified amount of time elapses, the password expires and the user must set a new password. If set to 0, the password does not expire. This rule takes effect only if the "Password requirements" rule is set to something other than "Unspecified." Depends on: Password requirements	• Work space only • Work space only (Premium) • Work space only (Android Management) • Work and personal - user privacy • Work and personal - user privacy (Premium) • Work and personal - user privacy (Android Management) • Work and personal - full control • Work and personal - full control (Premium) • Work and personal - full control (Android Management)	0 seconds	Minimum value: 0 seconds Max: 92233720368547 seconds

Name	Description	Activation Types	Default	Possible Values
Password history restriction	Specify the maximum number of previous passwords that a device checks to prevent a user from reusing a work profile password. If set to 0, the device does not check previous passwords. This rule takes effect only if the "Password requirements" rule is set to "Numeric," "Alphabetic," "Alphanumeric," "Complex," or "Numeric Complex." Depends on: Password requirements	• Work space only • Work space only (Premium) • Work space only (Android Management) • Work and personal - user privacy • Work and personal - user privacy (Premium) • Work and personal - user privacy (Android Management) • Work and personal - full control • Work and personal - full control (Premium) • Work and personal - full control (Android Management)		Minimum value: 0 passwords Maximum value: 2147483647 passwords

Name	Description	Activation Types	Default	Possible Values
Minimum password length	Specify the minimum number of characters that the work profile password must contain. This rule takes effect only if the "Password requirements" rule is set to "Numeric," "Alphabetic," "Alphanumeric," "Complex," or "Numeric Complex." Depends on: Password requirements	• Work space only • Work space only (Premium) • Work space only (Android Management) • Work and personal - user privacy • Work and personal - user privacy (Premium) • Work and personal - user privacy (Android Management) • Work and personal - full control • Work and personal - full control (Premium) • Work and personal - full control (Android Management)		Minimum value: 0 characters Maximum value: 2147483647 characters

Name	Description	Activation Types	Default	Possible Values
Minimum uppercase letters required in password	Specify the minimum number of uppercase letters that the work profile password must contain. This rule takes effect only if you set the "Password requirements" rule to "Complex." Depends on: Password requirements	• Work space only • Work space only (Premium) • Work space only (Android Management) • Work and personal - user privacy • Work and personal - user privacy (Premium) • Work and personal - user privacy (Android Management) • Work and personal - full control • Work and personal - full control (Premium) • Work and personal - full control (Android Management)	0 letters	Minimum value: 0 letters Maximum value: 24 letters

Name	Description	Activation Types	Default	Possible Values
Minimum lowercase letters required in password	Specify the minimum number of lowercase letters that the work profile password must contain. This rule takes effect only if you set the "Password requirements" rule to "Complex." Depends on: Password requirements	• Work space only • Work space only (Premium) • Work space only (Android Management) • Work and personal - user privacy • Work and personal - user privacy (Premium) • Work and personal - user privacy (Android Management) • Work and personal - full control • Work and personal - full control (Premium) • Work and personal - full control (Android Management)	0 letters	Minimum value: 0 letters Maximum value: 24 letters

Name	Description	Activation Types	Default	Possible Values
Minimum non-letters in password	Specify the minimum number of non-letter characters (numbers or symbols) required in the password. This rule takes effect only if you set the "Password requirements" rule to "Complex." Depends on: Password requirements	• Work space only • Work space only (Premium) • Work space only (Android Management) • Work and personal - user privacy • Work and personal - user privacy (Premium) • Work and personal - user privacy (Android Management) • Work and personal - full control • Work and personal - full control (Premium) • Work and personal - full control (Android Management)	0 characters	Minimum value: 0 characters Maximum value: 16 characters

Name	Description	Activation Types	Default	Possible Values
Minimum letters required in password	Specify the minimum number of letters that the work profile password must contain. This rule takes effect only if you set the "Password requirements" rule to "Complex." Depends on: Password requirements	• Work space only • Work space only (Premium) • Work space only (Android Management) • Work and personal - user privacy • Work and personal - user privacy (Premium) • Work and personal - user privacy (Android Management) • Work and personal - full control • Work and personal - full control (Premium) • Work and personal - full control (Android Management)	1 letter	Minimum value: 0 letters Maximum value: 16 letters

Name	Description	Activation Types	Default	Possible Values
Minimum numeric digits required in password	Specify the minimum number of numerals that the work profile password must contain. This rule takes effect only if you set the "Password requirements" rule to "Complex." Depends on: Password requirements	• Work space only • Work space only (Premium) • Work space only (Android Management) • Work and personal - user privacy • Work and personal - user privacy (Premium) • Work and personal - user privacy (Android Management) • Work and personal - full control • Work and personal - full control (Premium) • Work and personal - full control (Android Management)	1 number	Minimum value: 0 numerals Maximum value: 16 numerals

Name	Description	Activation Types	Default	Possible Values
Minimum symbols required in password	Specify the minimum number of non-alphanumeric characters that the work profile password must contain. This rule takes effect only if you set the "Password requirements" rule to "Complex." Depends on: Password requirements	• Work space only • Work space only (Premium) • Work space only (Android Management) • Work and personal - user privacy • Work and personal - user privacy (Premium) • Work and personal - user privacy (Android Management) • Work and personal - full control • Work and personal - full control (Premium) • Work and personal - full control (Android Management)	1 character	Minimum value: 0 characters Maximum value: 16 characters

Work profile (Samsung Knox devices only)

Name	Description	Activation Types	Default	Possible Values
Allow fingerprint authentication	Specify whether the user can use fingerprint authentication in the work profile. Applies only to devices that support Samsung Knox API level 12 and later.	• Work and personal - user privacy (Premium) • Work space only (Premium) • Work space only • Work and personal - full control (Premium)	Selected	
Allow iris authentication	Specify whether a user can authenticate with the work profile using an iris scan. Applies only to devices that support Samsung Knox API level 13 and later.	• Work and personal - user privacy (Premium) • Work space only (Premium) • Work space only • Work and personal - full control (Premium)	Selected	
Allow password visibility	Specify whether the work profile password is visible when a user is typing it. If this rule is not selected, users and apps cannot change the visibility setting. Applies only to devices that support Samsung Knox API level 6 and later.	• Work and personal - user privacy (Premium) • Work space only (Premium) • Work space only • Work and personal - full control (Premium)	Selected	

Name	Description	Activation Types	Default	Possible Values
Enforce two-factor authentication	Specify whether a user must use two-factor authentication to access the work profile. For example, you can use this rule if you want the user to authenticate using a fingerprint and a password. Applies only to devices that support Samsung Knox API level 24 and later.	• Work and personal - user privacy (Premium) • Work space only (Premium) • Work and personal - full control (Premium)	Not Selected	
Maximum character sequence length	Specify the maximum length of the character sequence that is allowed in the work profile password. Only applies when work profile password quality is Alphabetic, Alphanumeric or Complex. Applies only to devices that support Samsung Knox API level 6 and later.	• Work and personal - full control (Premium) • Work and personal - user privacy (Premium)		Minimum value: 0 characters Maximum value: 16 characters
Maximum numeric sequence length	Specify the maximum length of the numeric sequence that is allowed in the work profile password. Only applies when work profile password quality is Numeric, Alphanumeric or Complex. Applies only to devices that support Samsung Knox API level 4 and later.	• Work and personal - full control (Premium) • Work and personal - user privacy (Premium)		Minimum value: 0 numerals Maximum value: 16 numerals

Name	Description	Activation Types	Default	Possible Values
Minimum number of changed characters for new work profile passwords	Specify the minimum number of changed characters that a new password must include compared to the previous password. Device calculates the difference between the two passwords using the Levenshtein algorithm. Characters can be numeric, alphabetic, or symbolic. According to the Levenshtein algorithm, strings like "test" and "best" differ from each other by one unit. "Test" and "toad" differ from each other by three units. "Test" and "est" differ from each other by one unit. If set to 0, no restrictions are applied. Applies only to devices that support Samsung Knox API level 6 and later.	• Work and personal - full control (Premium) • Work and personal - user privacy (Premium)		Minimum value: 0 characters Maximum value: 16 characters

Personal profile (Samsung Knox devices only)

Name	Description	Activation Types	Default	Possible Values
Enforce two-factor authentication	Specify whether a user must use two-factor authentication to access the device. For example, you can use this rule if you want the user to authenticate using a fingerprint and a password. Applies only to devices that support Samsung Knox API level 24 and later.	Work and personal - full control (Premium)	Not Selected	

Knox MDM

Name	Description	Activation Types	Default	Possible Values
Password requirements	Specify the minimum requirements for a device password. If set to "Numeric," "Alphabetic," or "Alphanumeric," the password must contain at least the specified character types and can also include other character types. If set to "Complex," you can set specific requirements for different character types.	Work and personal - full control (Samsung Knox)	Numeric	• Numeric • Alphabetic • Alphanumeric • Complex
Minimum password length	Specify the minimum length of the password on Knox MDM devices. Applies only to devices that support Samsung Knox MDM version 5.0.0 and later. Depends on: Password requirements	Work and personal - full control (Samsung Knox)	4 characters	Minimum: 4 characters Maximum: 16 characters
Minimum lowercase letters required in password	Specify the minimum number of lowercase letters that the password must contain on Knox MDM devices. Applies only to devices that support Samsung Knox MDM version 5.0.0 and later. Depends on: Password requirements	Work and personal - full control (Samsung Knox)	0 letters	Minimum: 0 letters Maximum: 16 letters
Minimum uppercase letters required in password	Specify the minimum number of uppercase letters that the password must contain on Knox MDM devices. Applies only to devices that support Samsung Knox MDM version 5.0.0 and later. Depends on: Password requirements	Work and personal - full control (Samsung Knox)		Minimum: 0 letters Maximum: 16 letters

Name	Description	Activation Types	Default	Possible Values
Minimum complex characters required in password	Specify the minimum number of complex characters (for example, numbers or symbols) that the password must contain on Knox MDM devices. If you set this value to 1, then at least one number is required. If you specify a value greater than 1, then at least one number and at least one symbol are required. Depends on: Password requirements	Work and personal - full control (Samsung Knox)	2 characters	Minimum: 0 characters Maximum: 16 characters
Maximum character sequence length	Specify the maximum length of an alphabetic sequence that is allowed in the device password. For example, if the alphabetic sequence length is set to 5, the alphabetic sequence "abcde" is allowed but the sequence "abcdef" is not allowed. If set to 0, there are no alphabetic sequence restrictions. Depends on: Password requirements	Work and personal - full control (Samsung Knox)		Minimum: 0 letters Maximum: 16 letters
Maximum numeric sequence length	Specify the maximum length of the numeric sequence that is allowed in the device password. Depends on: Password requirements	Work and personal - full control (Samsung Knox)		Minimum: 0 numbers Maximum: 16 numbers

Name	Description	Activation Types	Default	Possible Values
Maximum inactivity time lock	Specify the maximum period of user inactivity before the device locks (key guard lock). If the device is managed by multiple EMM solutions, the device uses the lowest value as the inactivity period. If the device uses a password, the user must provide the password to unlock the device. A value of 0 means no restriction is set. Users can set a shorter time period on the device. Applies only to devices that support Samsung Knox MDM version 5.0.0 and later. Depends on: Password requirements	Work and personal - full control (Samsung Knox)		Minimum: 0 seconds Maximum: 1,000,000 seconds
Maximum failed password attempts	Specify the number of times that a user can enter an incorrect password before a device is wiped. Depends on: Password requirements	Work and personal - full control (Samsung Knox)	0	Minimum: 0 Maximum: 10
Password history restriction	Specify the maximum number of previous passwords that a device checks to prevent a user from reusing a device password. If set to 0, the device does not check previous passwords. Depends on: Password requirements	Work and personal - full control (Samsung Knox)		Minimum: 0 Maximum: 100
Password expiration timeout	Specify the maximum amount of days that the device password can be used. After the specified amount of days elapses, the password expires and a user must set a new password. If set to 0, the password does not expire. Depends on: Password requirements	Work and personal - full control (Samsung Knox)	0	Minimum: 0 Maximum: 365 days

Name	Description	Activation Types	Default	Possible Values
Allow password visibility	Specify if the device password is visible when the user is typing it. If this rule is not selected, users and third-party apps cannot change the visibility setting.	Work and personal - full control (Samsung Knox)	Selected	
Allow fingerprint authentication	Specify whether the user can use fingerprint authentication for a Knox enabled device. Applies only to devices that support Samsung Knox MDM version 5.1.0 and later.	Work and personal - full control (Samsung Knox)	Selected	
Require lock screen message	Specify whether you set a message to display when the device is locked. If this rule is not selected, the user can choose a message to display on the lock screen.	Work and personal - full control (Samsung Knox)	Not selected	
Lock screen message	Specify the text to display on the device when the device is locked. Depends on: Require lock screen message	Work and personal - full control (Samsung Knox)		Maximum: 300 characters

Knox MDM Premium - Workspace

Name	Description	Activation Types	Default	Possible Values
Password requirements	Specify the minimum requirements for the Knox Workspace password. If set to "Numeric," "Alphabetic," or "Alphanumeric," the password must contain at least the specified character types and can also include other character types. If set to "Numeric Complex," the password must contain at least numeric characters with no repeating (4444) or ordered (1234, 4321, 2468) sequences. If set to "Complex," you can set specific requirements for different character types. Applies only to devices that support Samsung Knox MDM version 5.0.0 and later.	• Work space only (Samsung Knox) • Work and personal - full control (Samsung Knox) • Work and personal - user privacy (Samsung Knox)	Numeric	• Numeric • Numeric Complex • Alphabetic • Alphanumeric • Complex
Minimum lowercase letters required in password	Specify the minimum number of lowercase letters that the Knox Workspace password must contain. Applies only to devices that support Samsung Knox MDM version 5.0.0 and later. Depends on: Password requirements	• Work space only (Samsung Knox) • Work and personal - full control (Samsung Knox) • Work and personal - user privacy (Samsung Knox)	0, no restriction	Minimum: 0 Maximum: 16 letters

Name	Description	Activation Types	Default	Possible Values
Minimum uppercase letters required in password	Specify the minimum number of uppercase letters that the Knox Workspace password must contain. Applies only to devices that support Samsung Knox MDM version 5.0.0 and later. Depends on: Password requirements	• Work space only (Samsung Knox) • Work and personal - full control (Samsung Knox) • Work and personal - user privacy (Samsung Knox)	0, no restriction	Minimum: 0 Maximum: 16 letters
Minimum complex characters required in password	Specify the minimum number of complex characters (for example, numbers or symbols) that the Knox Workspace password must contain. At least one number and one symbol are required. Depends on: Password requirements	• Work space only (Samsung Knox) • Work and personal - full control (Samsung Knox) • Work and personal - user privacy (Samsung Knox)	3 characters	Minimum: 3 characters Maximum: 16 characters
Maximum character sequence length	Specify the maximum length of an alphabetic sequence that is allowed in the Knox Workspace password. For example, if the alphabetic sequence length is set to 5, the alphabetic sequence "abcde" is allowed but the sequence "abcdef" is not allowed. If set to 0, there are no alphabetic sequence restrictions. Depends on: Password requirements	• Work space only (Samsung Knox) • Work and personal - full control (Samsung Knox) • Work and personal - user privacy (Samsung Knox)	0, no restriction	Minimum: 0 Maximum: 16 letters

Name	Description	Activation Types	Default	Possible Values
Minimum number of changed characters for new passwords	Specify the minimum number of changed characters that a new password must include compared to the previous password. Knox Workspace calculates the difference between the two passwords using the Levenshtein algorithm. Characters can be numeric, alphabetic, or symbolic. According to the Levenshtein algorithm, strings like "test" and "best" differ from each other by one unit. "Test" and "toad" differ from each other by three units. "Test" and "est" differ from each other by one unit. If set to 0, no restrictions are applied.	• Work space only (Samsung Knox) • Work and personal - full control (Samsung Knox) • Work and personal - user privacy (Samsung Knox)	0, no restriction	Minimum: 0 Maximum: 64 characters
Minimum password length	Specify the minimum length of the password for the Knox Workspace. Applies only to devices that support Samsung Knox MDM version 5.0.0 and later.	• Work space only (Samsung Knox) • Work and personal - full control (Samsung Knox) • Work and personal - user privacy (Samsung Knox)	4 characters	Minimum: 4 characters Maximum: 16 characters
Maximum inactivity time lock	Specify the maximum period of user inactivity in the Knox Workspace before the workspace locks. A value of 0 means no restriction is set. Users can set a shorter time period on the device. Applies only to devices that support Samsung Knox MDM version 5.0.0 and later.	• Work space only (Samsung Knox) • Work and personal - full control (Samsung Knox) • Work and personal - user privacy (Samsung Knox)	0, no restriction	Minimum: 0 Maximum: 10000000 seconds

Name	Description	Activation Types	Default	Possible Values
Maximum failed password attempts	Specify the number of times that a user can enter an incorrect password before the Knox Workspace is wiped. If set to 0, there are no restrictions on the number of times a user can enter an incorrect password. Applies only to devices that support Samsung Knox MDM version 5.0.0 and later. Depends on: Password requirements	• Work space only (Samsung Knox) • Work and personal - full control (Samsung Knox) • Work and personal - user privacy (Samsung Knox)	10	Minimum: 0 Maximum: 10
Password history restriction	Specify the maximum number of previous passwords that a device checks to prevent a user from reusing a Knox Workspace password. If set to 0, the device does not check previous passwords. Depends on: Password requirements	• Work space only (Samsung Knox) • Work and personal - full control (Samsung Knox) • Work and personal - user privacy (Samsung Knox)	0, no restriction	Minimum: 0 Maximum: 100
Password expiration timeout	Specify the maximum number of days that the Knox Workspace password can be used. After the specified number of days elapses, the password expires and a user must set a new password. If set to 0, the password does not expire. Depends on: Password requirements	• Work space only (Samsung Knox) • Work and personal - full control (Samsung Knox) • Work and personal - user privacy (Samsung Knox)	0, password doesn't expire	Minimum: 0 Maximum: 365 days

Name	Description	Activation Types	Default	Possible Values
Allow keyguard customizations	Specify whether the Knox Workspace can use keyguard customizations, such as trust agents. If this rule is not selected, keyguard customizations are turned off as specified in the provided feature list. Applies only to devices that support Samsung Knox MDM version 5.4.0 and later.	• Work and personal - full control (Samsung Knox) • Work and personal - user privacy (Samsung Knox)	Selected	
Allow keyguard trust agents	Specify whether a user can keep the workspace unlocked for 2 hours after the workspace inactivity timeout value. If you do not set an inactivity timeout value, the user can perform this action by default. This rule applies to the Knox Workspace only. Applies only to devices that support Samsung Knox MDM version 5.4.0 and later. Depends on: Allow keyguard customizations	• Work and personal - full control (Samsung Knox) • Work and personal - user privacy (Samsung Knox)	Not selected	
Allow password visibility	Specify whether the Knox Workspace password is visible when a user is typing it. If this rule is not selected, users and apps cannot change the visibility setting.	• Work space only (Samsung Knox) • Work and personal - full control (Samsung Knox) • Work and personal - user privacy (Samsung Knox)	Selected	

Name	Description	Activation Types	Default	Possible Values
Enforce two-factor authentication	Specify whether a user must use two-factor authentication to access the Knox Workspace. For example, you can use this rule if you want the user to authenticate using a fingerprint and a password.	• Work space only (Samsung Knox) • Work and personal - full control (Samsung Knox) • Work and personal - user privacy (Samsung Knox)	Not selected	
Allow fingerprint authentication	Specify whether the user can use fingerprint authentication for the Knox Workspace. Applies only to devices that support Samsung Knox MDM version 5.4.0 and later.	• Work space only (Samsung Knox) • Work and personal - full control (Samsung Knox) • Work and personal - user privacy (Samsung Knox)	Selected	
Allow iris authentication	Specify whether a user can authenticate with the work space using an iris scan. Applies only to devices that support Samsung Knox MDM version 5.4.0 and later.	• Work space only (Samsung Knox) • Work and personal - full control (Samsung Knox) • Work and personal - user privacy (Samsung Knox)	Selected	

Android: Device functionality rules

Name	Description	Activation Types	Default	Possible Values
Disable camera	Specify whether the device camera is disabled.	• Work space only • Work space only (Premium) • Work space only (Android Management) • Work and personal - full control • Work and personal - full control (Premium) • Work and personal - full control (Android Management)	Not selected	

Name	Description	Activation Types	Default	Possible Values
Allow Bluetooth configuration	Specify whether a user can configure Bluetooth settings and use Bluetooth technology in the Knox Workspace. On "Work and personal - full control (Samsung Knox)" devices, this rule takes effect only if the "Allow Bluetooth" rule in the "Knox MDM" category is set to Allow.	• Work space only • Work space only (Premium) • Work space only (Android Management) • Work and personal - full control • Work and personal - full control (Premium) • Work and personal - full control (Android Management) • Work and personal - full control (Samsung Knox) • Work and personal - user privacy (Samsung Knox)	Selected	

Name	Description	Activation Types	Default	Possible Values
Allow Bluetooth	Specify whether the device can use Bluetooth technology.	• Work space only • Work space only (Premium) • Work space only (Android Management) • Work and personal - full control • Work and personal - full control (Premium) • Work and personal - full control (Android Management) • Work and personal - full control (Samsung Knox) • Work and personal - user privacy (Samsung Knox)	Selected	

Name	Description	Activation Types	Default	Possible Values
Allow Bluetooth sharing	Specify whether a user can share content from the work profile over a Bluetooth connection. Depends on: Allow Bluetooth	• Work space only • Work space only (Premium) • Work and personal - user privacy • Work and personal - user privacy (Premium) • Work and personal - full control • Work and personal - full control (Premium)	Not selected	
Allow Bluetooth A2DP	Specify whether a device can use the Bluetooth A2DP. A device can use the Bluetooth A2DP to stream audio files to another Bluetooth enabled device (for example, a headset). Applies only to devices that support Samsung Knox API level 2 and later. Depends on: Allow Bluetooth	• Work space only • Work space only (Premium) • Work and personal - full control • Work and personal - full control (Premium) • Work and personal - full control (Samsung Knox)	Selected	

Name	Description	Activation Types	Default	Possible Values
Allow Bluetooth AVRCP	Specify whether a device can use the Bluetooth AVRCP. A device can use the Bluetooth AVRCP to allow a Bluetooth enabled device (for example, a headset) to control the device's media apps. Applies only to devices that support Samsung Knox API level 2 and later. Depends on: Allow Bluetooth	• Work space only • Work space only (Premium) • Work and personal - full control • Work and personal - full control (Premium) • Work and personal - full control (Samsung Knox)	Selected	
Allow Bluetooth HFP	Specify whether a device can use the Bluetooth HFP. A device can use the Bluetooth HFP to allow a Bluetooth enabled device (for example, a car kit or a headset) to access the Contacts and Phone apps on the device to make phone calls. Applies only to devices that support Samsung Knox API level 2 and later. Depends on: Allow Bluetooth	• Work space only • Work space only (Premium) • Work and personal - full control • Work and personal - full control (Premium) • Work and personal - full control (Samsung Knox)	Selected	

Name	Description	Activation Types	Default	Possible Values
Allow Bluetooth HSP	Specify whether a device can use the Bluetooth HSP. A device can use the Bluetooth HSP to allow a Bluetooth headset to connect to the device. Applies only to devices that support Samsung Knox API level 2 and later. Depends on: Allow Bluetooth	• Work space only • Work space only (Premium) • Work and personal - full control • Work and personal - full control (Premium) • Work and personal - full control (Samsung Knox)	Selected	
Allow Bluetooth PBAP	Specify whether a device can exchange phone book contacts with other Bluetooth enabled devices using the Bluetooth PBAP. Applies only to devices that support Samsung Knox API level 2 and later. Depends on: Allow Bluetooth	• Work space only • Work space only (Premium) • Work and personal - full control • Work and personal - full control (Premium) • Work and personal - full control (Samsung Knox)	Selected	

Name	Description	Activation Types	Default	Possible Values
Allow Bluetooth SPP	Specify whether a device can use the Bluetooth SPP. Applies only to devices that support Samsung Knox API level 2 and later. Depends on: Allow Bluetooth	• Work space only • Work space only (Premium) • Work and personal - full control • Work and personal - full control (Premium) • Work and personal - full control (Samsung Knox)	Selected	
Allow configuring mobile networks	Specify whether a user can configure mobile network settings on the device. This rule does not apply to Work and personal - full control and Work and personal - full control (Premium) activated devices running Android OS version 11 and later.	• Work space only • Work space only (Premium) • Work space only (Android Management) • Work and personal - full control • Work and personal - full control (Premium) • Work and personal - full control (Android Management)	Selected	

Name	Description	Activation Types	Default	Possible Values
Allow changing Wi-Fi settings	Specify whether the user can change the settings in the work Wi-Fi profile. If this rule is not selected, the user can't change any settings in the profile, including their Wi-Fi connection credentials. Applies to Android Enterprise and Android Management devices.	• Work space only • Work space only (Premium) • Work space only (Android Management) • Work and personal - full control • Work and personal - full control (Premium) • Work and personal - full control (Android Management)	Not selected	
Allow changing Wi-Fi networks	Specify whether the user can set up connections to Wi-Fi networks other than the one specified by the Wi-Fi profile. Applies to Android Enterprise and Android Management devices.	• Work space only • Work space only (Premium) • Work space only (Android Management) • Work and personal - full control • Work and personal - full control (Premium) • Work and personal - full control (Android Management)	Selected	

Name	Description	Activation Types	Default	Possible Values
Allow tethering configuration	Specify whether a user can configure tethering and mobile hotspots.	• Work space only • Work space only (Premium) • Work space only (Android Management) • Work and personal - full control • Work and personal - full control (Premium) • Work and personal - full control (Android Management)	Selected	
Allow tethering	Specify if a device can share mobile data with another device using USB, Wi-Fi, or Bluetooth. Applies only to devices that support Samsung Knox API level 2 and later.	• Work space only • Work space only (Premium) • Work and personal - full control • Work and personal - full control (Premium) • Work and personal - full control (Samsung Knox)	Selected	

Name	Description	Activation Types	Default	Possible Values
Allow Bluetooth tethering	Specify if a device can share its mobile network connection with other devices using Bluetooth. If this rule is not selected, the user cannot change this setting on the device. Applies only to devices that support Samsung Knox API level 2 and later. Depends on: Allow tethering	• Work space only • Work space only (Premium) • Work and personal - full control • Work and personal - full control (Premium) • Work and personal - full control (Samsung Knox)	Selected	
Allow USB tethering	Specify if a device can share its mobile network connection with other devices using USB. If this rule is not selected, the user cannot change this setting on the device. Applies only to devices that support Samsung Knox API level 2 and later. Depends on: Allow tethering	• Work space only • Work space only (Premium) • Work and personal - full control • Work and personal - full control (Premium) • Work and personal - full control (Samsung Knox)	Selected	

Name	Description	Activation Types	Default	Possible Values
Allow Wi-Fi tethering	Specify if a device can share its mobile network connection with other devices using Wi-Fi. If this rule is not selected, the user cannot change this setting on the device. Applies only to devices that support Samsung Knox API level 2 and later. Depends on: Allow tethering	• Work space only • Work space only (Premium) • Work and personal - full control • Work and personal - full control (Premium) • Work and personal - full control (Samsung Knox)	Selected	
Allow factory reset	Specify whether the user can reset the device to factory defaults. On BlackBerry Devices powered by Android, this rule also disables the Deactivate button in the BlackBerry UEM Client app.	• Work space only • Work space only (Premium) • Work space only (Android Management)	Selected	
Allow mounting physical media	Specify whether a user can mount physical media, such as SD cards and flash drives that support USB On-The-Go, to the device.	• Work space only • Work space only (Premium) • Work space only (Android Management) • Work and personal - full control • Work and personal - full control (Premium) • Work and personal - full control (Android Management)	Selected	

Name	Description	Activation Types	Default	Possible Values
Allow outgoing calls	Specify if a user can place outgoing calls. If this rule is not selected, the device can only make emergency calls. All other outgoing calls are blocked.	• Work space only • Work space only (Premium) • Work space only (Android Management) • Work and personal - full control • Work and personal - full control (Premium) • Work and personal - full control (Android Management)	Selected	
Allow mobile data usage while roaming	Specify whether a user can use mobile data while roaming. If this rule is not selected, apps can't connect to the Internet over a wireless network when the device is roaming.	• Work space only • Work space only (Premium) • Work space only (Android Management) • Work and personal - full control • Work and personal - full control (Premium) • Work and personal - full control (Android Management) • Work and personal - full control (Samsung Knox)	Selected	

Name	Description	Activation Types	Default	Possible Values
Allow SMS messages	Specify whether a user can send and receive SMS messages.	• Work space only • Work space only (Premium) • Work space only (Android Management) • Work and personal - full control • Work and personal - full control (Premium) • Work and personal - full control (Android Management)	Selected	
Default SMS app	Specify the package ID of the default SMS app. On devices with Work and personal - full control activations, the app must be a pre-installed system app.	• Work space only • Work space only (Premium) • Work and personal - full control • Work and personal - full control (Premium)		

Name	Description	Activation Types	Default	Possible Values
Set time automatically	Specify whether a device must set the date and time automatically. If this rule is selected, the user can't manually set the date and time.	• Work space only • Work space only (Premium) • Work space only (Android Management) • Work and personal - full control • Work and personal - full control (Premium) • Work and personal - full control (Android Management)	Not selected	
Obtain time zone from network	Specify whether the device obtains the time zone from the network. Depends on: Set time automatically	• Work space only • Work space only (Premium) • Work and personal - full control • Work and personal - full control (Premium)	Use network	• Do not use network • Use network
Device time zone	Specify the time zone that the device uses in TZ identifier format. Depends on: Obtain time zone from network (not enabled)	• Work space only • Work space only (Premium) • Work and personal - full control • Work and personal - full control (Premium)	Canada/ Eastern	Time zone specified in standard TZ identifier format

Name	Description	Activation Types	Default	Possible Values
Default launcher	Specify the package ID of the launcher app that must be used on the device. For this rule to apply to the device, you must push the launcher app to the device.	• Work space only • Work space only (Premium) • Work space only (Android Management) • Work and personal - full control • Work and personal - full control (Premium) • Work and personal - full control (Android Management)		
Allow user to boot into safe mode	Specifies if the user is not allowed to reboot the device into safe boot mode. In safe mode, all third-party apps are disabled, while those that are pre-installed continue to work.	• Work space only • Work space only (Premium) • Work and personal - full control • Work and personal - full control (Premium)	Not selected	

Name	Description	Activation Types	Default	Possible Values
Allow microphone	Specify whether the microphone of a device can be turned on and is available to apps on the device. If this rule is not selected, the microphone is disabled for all services. If this rule is not selected, users and third-party apps cannot enable the microphone. This rule applies only to the recording microphone, not the phone app microphone on "Work and personal - full control (Samsung Knox)" devices, this rule takes effect only if the "Allow microphone" rule in the "Knox MDM" category is selected.	• Work space only • Work space only (Premium) • Work space only (Android Management) • Work and personal - full control • Work and personal - full control (Premium) • Work and personal - full control (Android Management) • Work and personal - full control (Samsung Knox) • Work and personal - user privacy (Samsung Knox)	Selected	
Stay awake when plugged in to AC charger	Specify whether the device stays awake when it is plugged in to an to AC charger.	• Work space only • Work space only (Premium) • Work space only (Android Management)	Not selected	
Stay awake when plugged in to a USB charger	Specify whether the device stays awake when it is plugged in to a USB charger.	• Work space only • Work space only (Premium) • Work space only (Android Management)	Not selected	

Name	Description	Activation Types	Default	Possible Values
Stay awake when plugged in to a wireless charger	Specify whether the device stays awake when it is plugged in to a wireless charger.	• Work space only • Work space only (Premium) • Work space only (Android Management)	Not selected	
Allow user to configure screen timeout	Specify whether the user can configure the screen timeout period.	• Work space only • Work space only (Premium)	Allow User	• Disallow User • Allow User
Screen timeout	Specify the period of user inactivity before the screen turns off. Depends on: Allow user to configure screen timeout (not enabled)	• Work space only • Work space only (Premium)		Minimum: 0 seconds Maximum: 86400 seconds
Allow user to configure screen brightness	Specify whether the user can configure the screen brightness.	• Work space only • Work space only (Premium)	Allow User	• Disallow User • Allow User
Force adaptive brightness	Specify whether adaptive brightness is enabled on the device. Depends on: Allow user to configure screen brightness (not enabled)	• Work space only • Work space only (Premium)	Allow User	• Disallow User • Allow User
Screen brightness	Specify the screen brightness level for the device. Depends on: Force adaptive brightness (not enabled)	• Work space only • Work space only (Premium)		Minimum: 0 Maximum: 255

Name	Description	Activation Types	Default	Possible Values
Allowed input methods	Specify whether the user can use any input method (for example, a keyboard), only the input methods provided by the device, or only the input methods provided by the device plus additional input methods you specify. For Android 9 and earlier, this rule applies to the entire device, not just the work profile. For Android 10 and later devices, this rule applies only to the work profile. If the user enables an input method before the rule is set, the rule will not take effect unless the enabled input method is in the allowed list.	• Work space only • Work space only (Premium) • Work space only (Android Management) • Work and personal - user privacy • Work and personal - user privacy (Premium) • Work and personal - user privacy (Android Management) • Work and personal - full control • Work and personal - full control (Premium) • Work and personal - full control (Android Management)	All	• All • System only • Specified

Name	Description	Activation Types	Default	Possible Values
Input method packages	Specify the package ID for input method services (for example, keyboards) that the user can access in addition to those provided with the device by default. Depends on: Allowed input methods	• Work space only • Work space only (Premium) • Work space only (Android Management) • Work and personal - user privacy • Work and personal - user privacy (Premium) • Work and personal - user privacy (Android Management) • Work and personal - full control • Work and personal - full control (Premium) • Work and personal - full control (Android Management)		

Name	Description	Activation Types	Default	Possible Values
Allowed accessibility services	Specify the accessibility services that the user can access. By default the user can use any accessibility service. System accessibility services are always available to the user. This rule applies to the entire device, not just the work profile.	• Work space only • Work space only (Premium) • Work space only (Android Management) • Work and personal - user privacy • Work and personal - user privacy (Premium) • Work and personal - user privacy (Android Management) • Work and personal - full control • Work and personal - full control (Premium) • Work and personal - full control (Android Management)	All	• All • System only • Specified

Name	Description	Activation Types	Default	Possible Values
Accessibility service packages	Specify the package IDs for additional accessibility services that the user can access. If you do not specify a package ID, users can only use the system services. System accessibility services are always available to the user. Depends on: Allowed accessibility services (Specified)	• Work space only • Work space only (Premium) • Work space only (Android Management) • Work and personal - user privacy • Work and personal - user privacy (Premium) • Work and personal - user privacy (Android Management) • Work and personal - full control • Work and personal - full control (Premium) • Work and personal - full control (Android Management)		
Allow system error dialogs	Specify whether system error dialogs for crashed or unresponsive apps display on the device. If this rule is not selected, when an app stops or is unresponsive, the system will force-stop the app as if the user chose the "close app" option in the dialog box. A feedback report isn't collected because users can't provide explicit consent.	• Work space only • Work space only (Premium) • Work space only (Android Management)	Selected	

Name	Description	Activation Types	Default	Possible Values
Force device to use Access Point Name profile settings	Specify whether the device must use the settings from an assigned Access Point Name profile to connect to a wireless network, or whether the user can select any Access Point Names on the device.	• Work space only • Work space only (Premium)	Not selected	
Allow ambient display	Specify whether the user can enable ambient display on the device. Ambient display shows notifications on the lock screen when the device is locked. If Ambient display rule is disallowed, then 'Allow Accessibility services' should be limited to system. For Samsung devices, to disallow ambient display you must also set the "Allow accessibility services" rule to "System" or "Specified".	• Work space only • Work space only (Premium)	Selected	
Allow airplane mode	Specify whether the user can enable airplane mode on the device.	• Work space only • Work space only (Premium) • Work and personal - full control • Work and personal - full control (Premium)	Selected	
Allow user to configure private DNS	Specify whether a user can configure private DNS, which uses TLS for DNS queries.	• Work space only • Work space only (Premium) • Work and personal - full control • Work and personal - full control (Premium)	Allow User	• Disallow User • Allow User

Name	Description	Activation Types	Default	Possible Values
Use opportunistic private DNS	Specify whether the DNS queries will attempt TLS and fallback when not available. Depends on: Allow user to configure private DNS (not enabled)	• Work space only • Work space only (Premium)	Allow User	• Disallow User • Allow User
Private DNS server	Specify the server address to use for private DNS queries. Depends on: Use opportunistic private DNS (not enabled)	• Work space only • Work space only (Premium)		
Allow date and time changes	Specify if a user can manually change the date and time setting on a device. Applies only to devices that support Samsung Knox API level 5 and later.	• Work space only • Work space only (Premium) • Work and personal - full control • Work and personal - full control (Premium) • Work and personal - full control (Samsung Knox)	Selected	
Force automatic time sync	Specify if the device must obtain the date and time automatically using NITZ. If this rule is not selected, the user can choose whether the device automatically syncs the date and time. Applies only to devices that support Samsung Knox API level 2 and later. Depends on: Allow date and time changes	• Work space only • Work space only (Premium) • Work and personal - full control • Work and personal - full control (Premium) • Work and personal - full control (Samsung Knox)	Selected	

Name	Description	Activation Types	Default	Possible Values
Allow Built-in Samsung VPN	Specify if a user can use the build-in VPN functionality. If this rule is not selected, the user cannot open a VPN session, or access the VPN settings in the Settings app. Applies only to devices that support Samsung Knox API level 4 and later.	• Work space only (Premium) • Work space only • Work and personal - full control • Work and personal - full control (Premium)	Selected	
Allow NFC	Specify whether a device can use NFC. Applies only to devices that support Samsung Knox API level 11 and later and Samsung Knox version 2.4.0 and later.	• Work space only • Work space only (Premium) • Work and personal - full control • Work and personal - full control (Premium) • Work and personal - full control (Samsung Knox) • Work and personal - user privacy (Samsung Knox)	Selected	

Name	Description	Activation Types	Default	Possible Values
Allow OTA updates	Specify if a device can update its OS using a Firmware Over-The-Air (FOTA) client (for example, Samsung Knox EMM or WebSync DM). If this rule is not selected, all wireless update requests (user-initiated, server-initiated, and system-initiated) are blocked. The user may see messages related to new OS updates but any attempt to update the OS fails. Applies only to devices that support Samsung Knox API level 5 and later.	• Work space only • Work space only (Premium) • Work and personal - full control • Work and personal - full control (Premium) • Work and personal - full control (Samsung Knox)	Selected	
Allow Wi-Fi	Specify whether a device can make Wi-Fi connections. After you deselect this rule and then reselect it, the device cannot use Wi-Fi until it is restarted.	• Work space only • Work space only (Premium) • Work and personal - full control • Work and personal - full control (Premium) • Work and personal - full control (Samsung Knox)	Selected	

Name	Description	Activation Types	Default	Possible Values
Allow Wi-Fi Direct	Specify if a device can use Wi-Fi Direct. When this rule is selected, the device can make connections using Wi-Fi Direct. This rule also affects the S Beam feature on Samsung devices. Applies only to devices that support Samsung Knox API level 6 and later.	• Work space only • Work space only (Premium) • Work and personal - full control • Work and personal - full control (Premium) • Work and personal - full control (Samsung Knox)	Selected	
Allow WAP push while roaming	Specify if a device can receive WAP push messages when roaming. If this rule is not selected, the device cannot receive MMS messages when roaming and the user cannot change this setting on the device. This rule applies only when the device is roaming.	• Work space only • Work space only (Premium) • Work and personal - full control • Work and personal - full control (Premium) • Work and personal - full control (Samsung Knox)	Selected	

Name	Description	Activation Types	Default	Possible Values
Allow automatic sync while roaming	Specify whether a device can synchronize data automatically while roaming. If this rule is not selected, a roaming device can synchronize data only when a user accesses an account and the user cannot change this setting on the device. This setting applies only when the device is roaming.	• Work space only • Work space only (Premium) • Work and personal - full control • Work and personal - full control (Premium) • Work and personal - full control (Samsung Knox)	Selected	
Allow voice calls while roaming	Specify if a device can make or receive voice calls while roaming. Applies only to devices that support Samsung Knox API level 5 and later.	• Work space only • Work space only (Premium) • Work and personal - full control • Work and personal - full control (Premium) • Work and personal - full control (Samsung Knox)	Selected	

Name	Description	Activation Types	Default	Possible Values
Allow SD card	Specify if a device can access an SD card. If this rule is not selected, read and write access to the SD card is blocked. Applies only to devices that support Samsung Knox API level 2 and later.	• Work space only • Work space only (Premium) • Work and personal - full control • Work and personal - full control (Premium) • Work and personal - full control (Samsung Knox)	Selected	
Allow data on mobile network	Specify if a device can use a mobile network connection. If this rule is not selected, the device cannot use the SIM data connection. Applies only to devices that support Samsung Knox API level 2 and later.	• Work space only • Work space only (Premium) • Work and personal - full control • Work and personal - full control (Premium)	Selected	
Allow users to add new Wi-Fi networks	Specify whether users can add new Wi-Fi profiles to the device. If this rule is not selected, users can only use the work Wi-Fi profiles that you configure. Applies only to devices that support Samsung Knox API level 4 and later.	• Work space only • Work space only (Premium) • Work and personal - full control • Work and personal - full control (Premium)	Selected	

Name	Description	Activation Types	Default	Possible Values
Force Bluetooth discoverable mode	Specify whether Bluetooth discoverable mode is enabled on the device. If this rule is selected the device is always available for incoming Bluetooth connection requests. If this rule is not selected and the user turns on Bluetooth, the device is not visible to other devices. Applies only to devices that support Samsung Knox API level 2 and later.	• Work space only • Work space only (Premium) • Work and personal - full control • Work and personal - full control (Premium)	Selected	
Disallowed Wi-Fi SSIDs	Specify the list of Wi-Fi SSIDs that you want to prevent devices from connecting to. These can be used to block SSIDs added by the carrier, user, etc. Applies only to devices that support Samsung Knox API level 4 and later.	• Work space only • Work space only (Premium) • Work and personal - full control • Work and personal - full control (Premium) • Work and personal - full control (Samsung Knox)		

Name	Description	Activation Types	Default	Possible Values
Allow Android Beam	Specify whether users can use Android Beam or S Beam to send contact information, web bookmarks, and other data to a nearby device. Applies only to devices that support Samsung Knox API level 6 and later.	• Work space only • Work space only (Premium) • Work and personal - full control • Work and personal - full control (Premium) • Work and personal - full control (Samsung Knox)	Selected	
Allow Media Transfer Protocol (MTP)	Specify if a device can use MTP. Because Android supports USB file transfer through MTP only, you can use this rule to block any kind of file transfer through USB. Picture Transfer Protocol (PTP) is a subset of MTP and is also affected by this rule. Applies only to devices that support Samsung Knox API level 2 and later.	• Work space only • Work space only (Premium) • Work and personal - full control • Work and personal - full control (Premium) • Work and personal - full control (Samsung Knox)	Selected	

Name	Description	Activation Types	Default	Possible Values
Allow USB host storage	Specify if a device can use USB host storage using USB OTG. If this rule is selected, a user can connect any pen drive (portable USB storage), external HD, or SD card reader, and it is mounted as a storage drive on the device. If this rule is not selected, a user cannot mount any external storage device. Applies only to devices that support Samsung Knox API level 6 and later.	• Work space only • Work space only (Premium) • Work and personal - full control • Work and personal - full control (Premium) • Work and personal - full control (Samsung Knox)	Selected	

Name	Description	Activation Types	Default	Possible Values
Allow user-configured VPN in workspace	Specify whether the user can configure a VPN profile in the work profile. This rule or the "Force always-on VPN" IT policy rule must be selected to allow the device to use BlackBerry Secure Connect Plus.	• Work space only • Work space only (Premium) • Work space only (Android Management) • Work and personal - user privacy • Work and personal - user privacy (Premium) • Work and personal - user privacy (Android Management) • Work and personal - full control • Work and personal - full control (Premium) • Work and personal - full control (Android Management)	Selected	

Name	Description	Activation Types	Default	Possible Values
Allow USB file transfer	Specify whether a user can transfer files to and from the device over a USB connection. For 'Work and Personal - Full Control' activation types, USB file transfers are allowed only in the personal perimeter.	• Work space only • Work space only (Premium) • Work space only (Android Management) • Work and personal - full control • Work and personal - full control (Premium) • Work and personal - full control (Android Management)	Selected	
Allow cross profile caller ID	Specify whether caller ID information from the managed profile will be shown in the parent profile for incoming calls.	• Work and personal - user privacy • Work and personal - user privacy (Premium) • Work and personal - user privacy (Android Management) • Work and personal - full control • Work and personal - full control (Premium) • Work and personal - full control (Android Management)	Selected	

Name	Description	Activation Types	Default	Possible Values
Allow searching work contacts from personal apps	Specify whether users can search work contacts from apps that are not in the work profile.	• Work and personal - user privacy • Work and personal - user privacy (Premium) • Work and personal - full control • Work and personal - full control (Premium) • Work and personal - user privacy (Android Management) • Work and personal - full control (Android Management)	Selected	

Name	Description	Activation Types	Default	Possible Values
Allowed cross-profile widgets	Specify the package IDs for widget providers that can be available to users in the parent profile. If you do not specify any widgets, no widgets are available. The user can add allowed widgets to a widget host running under the parent profile, for example the home screen. A package may have more than one provider component, where each component provides a different widget type.	• Work and personal - user privacy • Work and personal - user privacy (Premium) • Work and personal - user privacy (Android Management) • Work and personal - full control • Work and personal - full control (Premium) • Work and personal - full control (Android Management)		
Allowed system apps	Specify the package IDs for the system apps that are installed in the work profile. If you remove apps from this list, the apps are deleted from the work profile on users' devices.	• Work space only • Work space only (Premium) • Work and personal - user privacy • Work and personal - user privacy (Premium) • Work and personal - full control • Work and personal - full control (Premium)		

Name	Description	Activation Types	Default	Possible Values
Force always-on VPN	Specify whether a VPN connection is always available for work data.	• Work space only • Work space only (Premium) • Work space only (Android Management) • Work and personal - user privacy • Work and personal - user privacy (Premium) • Work and personal - user privacy (Android Management) • Work and personal - full control • Work and personal - full control (Premium) • Work and personal - full control (Android Management)	Not Selected	
Use BlackBerry Secure Connect Plus for VPN connection	Specify whether BlackBerry Secure Connect Plus provides the VPN connection that is always available. Depends on: Force always-on VPN	• Work space only (Premium) • Work and personal - user privacy (Premium) • Work and personal - full control (Premium)	Use BSCP	• Do not use BSCP • Use BSCP

Name	Description	Activation Types	Default	Possible Values
VPN app package ID	Specify the package ID for the VPN app that is always available. Depends on: Use BlackBerry Secure Connect Plus for VPN connection (not enabled)	• Work space only • Work space only (Premium) • Work and personal - user privacy • Work and personal - user privacy (Premium) • Work and personal - full control • Work and personal - full control (Premium)		
Force work apps to only use VPN	Specify whether all work apps, including the BlackBerry UEM Client and Google Play must use the specified VPN app. In this case you must open ports in the firewall to allow BlackBerry UEM Client to communicate with the BlackBerry Infrastructure through BlackBerry UEM. The VPN app must be correctly configured on the device before this rule is applied. If it is not, the device can't send and receive device management communications from BlackBerry UEM and may not be able to obtain the needed configuration to allow the VPN app to function. For BSCP, UEM Client ensures the configuration is applied before enabling this rule. Depends on: Force always-on VPN	• Work space only • Work space only (Premium) • Work and personal - user privacy • Work and personal - user privacy (Premium) • Work and personal - full control • Work and personal - full control (Premium)	Selected	

Name	Description	Activation Types	Default	Possible Values
Work apps exempt from VPN	Specify the package IDs of work apps that are not required to send data over the VPN connection when "Force work apps to only use VPN" is selected. Depends on: Force always-on VPN	• Work space only • Work space only (Premium) • Work and personal - user privacy • Work and personal - user privacy (Premium) • Work and personal - full control • Work and personal - full control (Premium)		
Allow Android system windows	Specify whether Android devices can display windows other than app windows; for example, windows for toasts, system error messages, and phone calls.	• Work space only • Work space only (Premium)	Selected	
Allow users to modify apps in Android Settings	Specify whether users can modify apps in Settings or launchers. If this rule is not selected, users can't uninstall apps, disable apps, clear app caches, clear app data, force apps to stop, or clear app defaults from the device Settings or launchers.	• Work space only • Work space only (Premium) • Work and personal - user privacy • Work and personal - user privacy (Premium) • Work and personal - full control • Work and personal - full control (Premium)	Selected	

Name	Description	Activation Types	Default	Possible Values
Allow printing	Specify whether the user can print files using the device OS print functionality. This rule does not block sharing files to apps that can send files to a printer.	• Work space only • Work space only (Premium) • Work and personal - user privacy • Work and personal - user privacy (Premium) • Work and personal - full control • Work and personal - full control (Premium)	Selected	

Name	Description	Activation Types	Default	Possible Values
Allow user to configure location	Specify whether the user can turn the location feature on or off.	• Work space only • Work space only (Premium) • Work space only (Android Management) • Work and personal - user privacy • Work and personal - user privacy (Premium) • Work and personal - user privacy (Android Management) • Work and personal - full control • Work and personal - full control (Premium) • Work and personal - full control (Android Management)	Selected	

Name	Description	Activation Types	Default	Possible Values
Allow audio recording	Specify whether a device can record audio in the work profile. If this rule is not selected, the user can still make calls and use audio streaming using the device microphone. This rule applies to phone calls, voice recognition, and VoIP. If an app declares a use type and does something else, then this rule cannot block the app. If you deselect this rule, any ongoing audio recording is interrupted. Video recording is still allowed if no audio recording is attempted. Applies only to devices that support Samsung Knox API level 6 and later.	• Work and personal - user privacy (Premium) • Work space only • Work space only (Premium) • Work and personal - full control • Work and personal - full control (Premium) • Work and personal - full control (Samsung Knox)	Selected	
Allow Google auto-sync	Specify if Google accounts and apps can sync automatically. This rule does not block Google Play from updating installed apps. Users can still manually sync from some apps, including Gmail. Applies only to devices that support Samsung Knox MDM version 5.0.0 and later.	• Work and personal - user privacy (Premium) • Work space only • Work space only (Premium) • Work and personal - full control (Premium) • Work and personal - full control (Samsung Knox) • Work and personal - user privacy (Samsung Knox)	Selected	

Name	Description	Activation Types	Default	Possible Values
Allow video recording	Specify if a device can record video. If this rule is not selected, the camera is still available so that a user can take pictures and use video streaming. If you deselect this rule, any ongoing video recording is interrupted. Applies only to devices that support Samsung Knox API level 6 and later.	• Work and personal - user privacy (Premium) • Work space only • Work space only (Premium) • Work and personal - full control • Work and personal - full control (Premium) • Work and personal - full control (Samsung Knox)	Selected	
Allow sending crash reports to Google	Specify if the user can send crash reports to Google. Applies only to devices that support Samsung Knox API level 5 and later.	• Work and personal - user privacy (Premium) • Work space only • Work space only (Premium) • Work and personal - full control • Work and personal - full control (Premium) • Work and personal - full control (Samsung Knox) • Work and personal - user privacy (Samsung Knox)	Selected	

Name	Description	Activation Types	Default	Possible Values
Allow camera	Specify whether a user can use the camera. Applies only to devices that support Samsung Knox API level 11 and later.	• Work and personal - user privacy (Premium) • Work and personal - full control (Premium) • Work and personal - full control (Samsung Knox) • Work and personal - user privacy (Samsung Knox)	Selected	
Allow data on mobile network	Specify if a device can use a mobile network connection. If this rule is not selected, the device cannot use the SIM data connection.	Work and personal - full control (Samsung Knox)	Selected	
Allow users to modify Wi-Fi profile settings	Specify if a user can modify work Wi-Fi profile settings such as static IP configuration, proxy settings, or security type. When this rule is not selected, the user can modify only the username, anonymous identity, password, and WEP keys of a work Wi-Fi profile. When this rule is not selected, the user cannot remove the work Wi-Fi profile. If this rule is selected, the user can modify all work Wi-Fi profile settings and also delete it.	Work and personal - full control (Samsung Knox)	Selected	
Allow users to add Wi-Fi networks	Specify whether users can add new Wi-Fi profiles to the device. If this rule is not selected, users can only use the work Wi-Fi profiles that you configure.	Work and personal - full control (Samsung Knox)	Selected	

Name	Description	Activation Types	Default	Possible Values
Allow users to modify the Settings app	Specify if a user is allowed to make changes to the Settings app. If this rule is not selected, the user cannot make changes to system preferences.	Work and personal - full control (Samsung Knox)	Selected	
Allow VPN	Specify if a user can use the native VPN functionality. If this rule is not selected, the user cannot open a VPN session, or access the VPN settings in the Settings app.	Work and personal - full control (Samsung Knox)	Selected	
Allow multiple user accounts	Specify if multiple user accounts can be created on the device.	Work and personal - full control (Samsung Knox)	Not selected	
Allow adding email accounts	Specify if the user can add work email accounts to the device.	• Work and personal - full control (Samsung Knox) • Work and personal - user privacy (Samsung Knox)	Selected	

Android: Security and privacy rules

Name	Description	Activation Types	Default	Possible Values
Allow deleting users	Specify if the user can delete users from the device. If this rule is selected, the primary user can delete other users. Secondary users can only delete themselves.	• Work space only • Work space only (Premium) • Work space only (Android Management) • Work and personal - full control • Work and personal - full control (Premium) • Work and personal - full control (Android Management)	Selected	
Allow device backup	Specify whether the device can use the backup service. If the rule is not selected, the user can't backup or restore data on the device.	• Work space only • Work space only (Premium)	Not selected	
Force SD card erase on device unmanage	If the SD card exists in the device it will be erased when the device is factory wiped as a result of being unmanaged.	• Work space only • Work space only (Premium) • Work and personal - full control • Work and personal - full control (Premium)	Not selected	

Name	Description	Activation Types	Default	Possible Values
Allow users to deactivate devices from UEM Client	Specify whether the user can deactivate the device using the BlackBerry UEM client. If this rule is not selected, the Deactivate My Device button in the BlackBerry UEM Client is disabled.	• Work space only • Work space only (Premium) • Work and personal - full control • Work and personal - full control (Premium)	Selected	
Display owner information on lock screen	Specify the information that the device displays when the device is locked.	• Work space only • Work space only (Premium) • Work space only (Android Management) • Work and personal - full control • Work and personal - full control (Premium) • Work and personal - full control (Android Management)		Maximum value: 100 characters

Name	Description	Activation Types	Default	Possible Values
Send security logs to UEM	Specify whether the device synchronizes security logs with UEM. On Android 11 and later devices activated with Work and personal - full control, certain security logs are not visible (for example personal app launch events) or they are redacted (for example, details of physical volume mount events).	• Work space only • Work space only (Premium) • Work space only (Android Management) • Work and personal - full control • Work and personal - full control (Premium) • Work and personal - full control (Android Management)	Not selected	
Allow firmware recovery	Specify if a user can update the operating system of a device using download mode. Cannot be combined with Android update policy APIs.	• Work space only • Work space only (Premium) • Work and personal - full control • Work and personal - full control (Premium) • Work and personal - full control (Samsung Knox)	Selected	

Name	Description	Activation Types	Default	Possible Values
Require SD card encryption	Specify if a device must encrypt all data on the external SD card. This rule requires the value of the "Password requirements" rule to be at least "Alphanumeric."	• Work space only • Work space only (Premium) • Work and personal - full control • Work and personal - full control (Premium) • Work and personal - full control (Samsung Knox)	Not selected	
Audit log outcomes	Specify whether the audit log records failures, successes, or both. Applies only to devices that support Samsung Knox API level 6 and later.	• Work space only (Premium) • Work and personal - full control (Premium)	All	• All • Failures • Successes
Audit log severity level	Specify the minimum severity level of events added to the audit log. Events of the selected severity and higher are added to the log. For example, if you select "Error", Critical and Alert severity events are also logged. Applies only to devices that support Samsung Knox API level 6 and later.	• Work space only (Premium) • Work and personal - full control (Premium)	Critical	• Alert • Critical • Error • Warning

Name	Description	Activation Types	Default	Possible Values
Allow cross profile copy and paste	Specify whether data that is copied to the clipboard can be pasted in a related profile.	• Work and personal - user privacy • Work and personal - user privacy (Premium) • Work and personal - user privacy (Android Management) • Work and personal - full control • Work and personal - full control (Premium) • Work and personal - full control (Android Management)	Not Selected	

Name	Description	Activation Types	Default	Possible Values
Allow adding and removing accounts	Specify whether a user can add or remove user accounts, such as email accounts, on the device. **Note:** If your organization uses BlackBerry Work, this rule must be enabled for BlackBerry Work to access email accounts set up under the work profile.	• Work space only • Work space only (Premium) • Work space only (Android Management) • Work and personal - user privacy • Work and personal - user privacy (Premium) • Work and personal - user privacy (Android Management) • Work and personal - full control • Work and personal - full control (Premium) • Work and personal - full control (Android Management)	Selected	

Name	Description	Activation Types	Default	Possible Values
Allow additional Google accounts	Specify whether the user can add additional Google accounts to the work profile. Depends on: Allow adding and removing accounts	• Work space only • Work space only (Premium) • Work and personal - user privacy • Work and personal - user privacy (Premium) • Work and personal - full control • Work and personal - full control (Premium)	Selected	

Name	Description	Activation Types	Default	Possible Values
Disallowed account types	Specify the types of accounts that cannot be added to the work profile. If no account types are specified, there is no restriction. For more information, see KB 46860. Depends on: Allow adding and removing accounts	• Work space only • Work space only (Premium) • Work space only (Android Management) • Work and personal - user privacy • Work and personal - user privacy (Premium) • Work and personal - user privacy (Android Management) • Work and personal - full control • Work and personal - full control (Premium) • Work and personal - full control (Android Management)		

Name	Description	Activation Types	Default	Possible Values
Allow screen capture	Specify if a user can take screen shots of the device.	• Work space only • Work space only (Premium) • Work space only (Android Management) • Work and personal - user privacy • Work and personal - user privacy (Premium) • Work and personal - user privacy (Android Management) • Work and personal - full control • Work and personal - full control (Premium) • Work and personal - full control (Android Management)	Selected	
Allow personal data in work profile	Specify whether files and data in the personal profile can be sent to the work profile or accessed from work apps.	• Work and personal - user privacy • Work and personal - user privacy (Premium) • Work and personal - full control • Work and personal - full control (Premium)	Selected	

Name	Description	Activation Types	Default	Possible Values
Allow location requests in work profile to access Google Maps in personal profile	Specify whether location requests made in the work profile can use Google Maps in the personal profile to provide the location information.	• Work and personal - user privacy • Work and personal - user privacy (Premium) • Work and personal - user privacy (Android Management) • Work and personal - full control • Work and personal - full control (Premium) • Work and personal - full control (Android Management)	Selected	
Allow user to create work email from the personal profile	Specify whether a user can create an email from their work email account using a personal app.	• Work and personal - user privacy • Work and personal - user privacy (Premium) • Work and personal - full control • Work and personal - full control (Premium)	Not Selected	

Name	Description	Activation Types	Default	Possible Values
Allow work profile to set alarms using the personal clock	Specify whether the user can set alarms from the work profile using the personal clock app.	• Work and personal - user privacy • Work and personal - user privacy (Premium) • Work and personal - full control • Work and personal - full control (Premium)	Selected	
Allow work apps to access images from the personal camera	Specify whether work apps can access images from the personal camera app.	• Work and personal - user privacy • Work and personal - user privacy (Premium) • Work and personal - user privacy (Android Management) • Work and personal - full control • Work and personal - full control (Premium) • Work and personal - full control (Android Management)	Not Selected	

Name	Description	Activation Types	Default	Possible Values
Allow work apps to access video from the personal camera	Specify whether work apps can access video from the personal camera app.	• Work and personal - user privacy • Work and personal - user privacy (Premium) • Work and personal - user privacy (Android Management) • Work and personal - full control • Work and personal - full control (Premium) • Work and personal - full control (Android Management)	Not Selected	
Allow work apps to open the personal camera	Specify whether work apps can open the personal camera app.	• Work and personal - user privacy • Work and personal - user privacy (Premium) • Work and personal - full control • Work and personal - full control (Premium)	Not Selected	

Name	Description	Activation Types	Default	Possible Values
Allow personal apps to play work media	Specify whether personal apps can play media stored in the work profile.	• Work and personal - user privacy • Work and personal - user privacy (Premium) • Work and personal - user privacy (Android management) • Work and personal - full control • Work and personal - full control (Premium) • Work and personal - full control (Android Management)	Not Selected	
Allow sending bug reports	Specify whether the user can send bug reports from the device.	• Work and personal - user privacy • Work and personal - user privacy (Premium) • Work space only (Premium) • Work space only • Work and personal - full control • Work and personal - full control (Premium)	Selected	

Name	Description	Activation Types	Default	Possible Values
Send bug reports using the BlackBerry DDT app	Specify whether Android devices powered by BlackBerry must use the BlackBerry DDT app to send bug reports to BlackBerry. Depends on: Allow sending bug reports	• Work space only • Work space only (Premium) • Work and personal - user privacy • Work and personal - user privacy (Premium) • Work and personal - full control • Work and personal - full control (Premium)	Not Selected	

Name	Description	Activation Types	Default	Possible Values
Allow transfer of work contacts using Bluetooth	Specify whether the device can use Bluetooth to send work contacts to another Bluetooth enabled device.	• Work and personal - user privacy • Work and personal - user privacy (Premium) • Work and personal - user privacy (Android Management) • Work space only • Work space only (Premium) • Work space only (Android Management) • Work and personal - full control • Work and personal - full control (Premium) • Work and personal - full control (Android Management)	Not Selected	

Name	Description	Activation Types	Default	Possible Values
Allow lock screen features	Specify whether special features can be enabled on the device lock screen.	• Work space only • Work space only (Premium) • Work space only (Android Management) • Work and personal - user privacy • Work and personal - user privacy (Premium) • Work and personal - user privacy (Android Management) • Work and personal - full control • Work and personal - full control (Premium) • Work and personal - full control (Android Management)	Selected	
Allow camera on lock screen	Specify whether users can access the device camera on lock screen. Depends on: Allow lock screen features	• Work space only • Work space only (Premium) • Work space only (Android Management)	Selected	

Name	Description	Activation Types	Default	Possible Values
Allow notifications	Specify whether the device can display notifications on the lock screen. Depends on: Allow lock screen features	• Work space only • Work space only (Premium) • Work space only (Android Management)	Selected	
Allow all notification content	Specify whether all notification content can appear on the lock screen or only the notification type. Depends on: Allow lock screen features	• Work space only • Work space only (Premium) • Work space only (Android Management) • Work and personal - user privacy • Work and personal - user privacy (Premium) • Work and personal - user privacy (Android Management) • Work and personal - full control • Work and personal - full control (Premium) • Work and personal - full control (Android Management)	Selected	

Name	Description	Activation Types	Default	Possible Values
Allow fingerprint authentication	Specify whether the user can unlock the device using a fingerprint. Depends on: Allow lock screen features	• Work space only • Work space only (Premium) • Work space only (Android Management) • Work and personal - user privacy • Work and personal - user privacy (Premium) • Work and personal - user privacy (Android Management) • Work and personal - full control • Work and personal - full control (Premium) • Work and personal - full control (Android Management)	Selected	

Name	Description	Activation Types	Default	Possible Values
Allow biometrics	Specify whether the user can use biometric authentication to unlock the device. Depends on: Allow lock screen features	• Work space only • Work space only (Premium) • Work space only (Android Management) • Work and personal - user privacy • Work and personal - user privacy (Premium) • Work and personal - user privacy (Android Management) • Work and personal - full control • Work and personal - full control (Premium) • Work and personal - full control (Android Management)	Selected	

Name	Description	Activation Types	Default	Possible Values
Allow facial recognition	Specify whether the user can unlock the device using face recognition. Depends on: Allow lock screen features	• Work space only • Work space only (Premium) • Work space only (Android Management) • Work and personal - user privacy • Work and personal - user privacy (Premium) • Work and personal - user privacy (Android Management) • Work and personal - full control • Work and personal - full control (Premium) • Work and personal - full control (Android Management)	Selected	

Name	Description	Activation Types	Default	Possible Values
Allow iris authentication	Specify whether the user can unlock the device using an iris scan. Depends on: Allow lock screen features	• Work space only • Work space only (Premium) • Work space only (Android Management) • Work and personal - user privacy • Work and personal - user privacy (Premium) • Work and personal - user privacy (Android Management) • Work and personal - full control • Work and personal - full control (Premium) • Work and personal - full control (Android Management)	Selected	

Name	Description	Activation Types	Default	Possible Values
Allow trust agents for Google Smart Lock	Specify whether trust agents can unlock the device using Google Smart Lock. Depends on: Allow lock screen features	• Work space only • Work space only (Premium) • Work space only (Android Management) • Work and personal - user privacy • Work and personal - user privacy (Premium) • Work and personal - user privacy (Android Management) • Work and personal - full control • Work and personal - full control (Premium) • Work and personal - full control (Android Management)	Selected	

Name	Description	Activation Types	Default	Possible Values
Allow Google NFC trust agent	Specify if NFC can be used to unlock the device using Google Smart Lock. Depends on: Allow trust agents for Google Smart Lock	• Work space only • Work space only (Premium) • Work and personal - user privacy • Work and personal - user privacy (Premium) • Work and personal - full control • Work and personal - full control (Premium)	Selected	
Allow tags with basic authentication to unlock the device	Specify if NFC tags that authenticate using the tag ID can be used to unlock the device using Google Smart Lock. Depends on: Allow Google NFC trust agent	• Work space only • Work space only (Premium) • Work and personal - user privacy • Work and personal - user privacy (Premium) • Work and personal - full control • Work and personal - full control (Premium)	Selected	

Name	Description	Activation Types	Default	Possible Values
Allow secure NFC tags to unlock the device	Specify if NFC tags that use challenge-response authentication can be used to unlock the device using Google Smart Lock. Depends on: Allow Google NFC trust agent	• Work space only • Work space only (Premium) • Work and personal - user privacy • Work and personal - user privacy (Premium) • Work and personal - full control • Work and personal - full control (Premium)	Selected	
Allow Google Bluetooth trust agent	Specify if Bluetooth can be used to unlock the device using Google Smart Lock. Depends on: Allow trust agents for Google Smart Lock	• Work space only • Work space only (Premium) • Work and personal - user privacy • Work and personal - user privacy (Premium) • Work and personal - full control • Work and personal - full control (Premium)	Selected	

Name	Description	Activation Types	Default	Possible Values
Allow Google places trust agent	Specify if places can be used to unlock the device using Google Smart Lock. Depends on: Allow trust agents for Google Smart Lock	• Work space only • Work space only (Premium) • Work and personal - user privacy • Work and personal - user privacy (Premium) • Work and personal - full control • Work and personal - full control (Premium)	Selected	
Allow custom places	Specify if a user can trust places other than Home. Depends on: Allow Google places trust agent	• Work space only • Work space only (Premium) • Work and personal - user privacy • Work and personal - user privacy (Premium) • Work and personal - full control • Work and personal - full control (Premium)	Selected	

Name	Description	Activation Types	Default	Possible Values
Allow Google Face trust agent	Specify if face image can be used to unlock the device using Google Smart Lock. Depends on: Allow trust agents for Google Smart Lock	• Work space only • Work space only (Premium) • Work and personal - user privacy • Work and personal - user privacy (Premium) • Work and personal - full control • Work and personal - full control (Premium)	Not Selected	
Allow Google Voice trust agent	Specify if voice can be used to unlock the device using Google Smart Lock. Depends on: Allow trust agents for Google Smart Lock	• Work space only • Work space only (Premium) • Work and personal - user privacy • Work and personal - user privacy (Premium) • Work and personal - full control • Work and personal - full control (Premium)	Selected	

Name	Description	Activation Types	Default	Possible Values
Allow Google On-body trust agent	Specify if On-body can be used to unlock the device. Depends on: Allow trust agents for Google Smart Lock	• Work space only • Work space only (Premium) • Work and personal - user privacy • Work and personal - user privacy (Premium) • Work and personal - full control • Work and personal - full control (Premium)	Selected	
Trust agent inactivity timeout	Specify Device inactivity timeout in minutes. When a device is in an idle state for a certain period of time, Google Smart Lock trust agents will be revoked. Depends on: Allow trust agents for Google Smart Lock	• Work space only • Work space only (Premium) • Work and personal - user privacy • Work and personal - user privacy (Premium) • Work and personal - full control • Work and personal - full control (Premium)	240 minutes	Minimum value: 1 minute Maximum value: 525600 minutes (1 year)

Name	Description	Activation Types	Default	Possible Values
Allow obtaining device location	Specify if work apps can obtain location of device. This policy will supersede any location profile assigned to the user.	• Work space only • Work space only (Premium) • Work space only (Android Management) • Work and personal - user privacy • Work and personal - user privacy (Premium) • Work and personal - user privacy (Android Management) • Work and personal - full control • Work and personal - full control (Premium) • Work and personal - full control (Android Management)	Selected	

Name	Description	Activation Types	Default	Possible Values
Allow transfer of work data using NFC	Specify whether the device can send work data to another device using NFC.	• Work space only • Work space only (Premium) • Work space only (Android Management) • Work and personal - user privacy • Work and personal - user privacy (Premium) • Work and personal - user privacy (Android Management) • Work and personal - full control • Work and personal - full control (Premium) • Work and personal - full control (Android Management)	Selected	
Allowed notification listeners	Specify which personal apps can intercept notifications from other apps.	• Work and personal - user privacy • Work and personal - user privacy (Premium) • Work and personal - full control • Work and personal - full control (Premium)	System only	• All • System only • Specified

Name	Description	Activation Types	Default	Possible Values
Allow autofill	Specify whether the device can save user-entered form data to automatically fill future forms.	• Work space only • Work space only (Premium) • Work and personal - user privacy • Work and personal - user privacy (Premium) • Work and personal - full control • Work and personal - full control (Premium)	Selected	

Name	Description	Activation Types	Default	Possible Values
Allow user to add certificates to the work profile certificate store	Specify whether the user can add trusted certificate authorities and client certificates to the work profile certificate store.	• Work space only • Work space only (Premium) • Work space only (Android Management) • Work and personal - user privacy • Work and personal - user privacy (Premium) • Work and personal - user privacy (Android Management) • Work and personal - full control • Work and personal - full control (Premium) • Work and personal - full control (Android Management)	Not Selected	

Name	Description	Activation Types	Default	Possible Values
Allow AI assistant to use screen content	Specify if the AI assistant on the device can use capture screen content.	• Work space only • Work space only (Premium) • Work and personal - user privacy • Work and personal - user privacy (Premium) • Work and personal - full control • Work and personal - full control (Premium)	Selected	
Allow AI to offer suggestions based on screen content	Specify if the AI assistant will provide selection suggestions based on screen content. Depends on: Allow AI assistant to use screen content	• Work space only • Work space only (Premium) • Work and personal - user privacy • Work and personal - user privacy (Premium) • Work and personal - full control • Work and personal - full control (Premium)	Selected	

Name	Description	Activation Types	Default	Possible Values
Allow Circle to Search	Specify if Circle to Search functionality is enabled in the work profile. Minimum OS version: 15.0	• Work space only • Work space only (Premium) • Work and personal - user privacy • Work and personal - user privacy (Premium) • Work and personal - full control • Work and personal - full control (Premium)	Selected	
Limit length of time work profile can be turned off	Specify whether users must turn on the work profile after a specified time limit to continue using the device. If the work profile is turned off longer than the specified time period, personal apps are disabled and the device displays a notification.	• Work and personal - full control • Work and personal - full control (Premium) • Work and personal - full control (Android Management)	Not Selected	
Maximum off-time	Specify the maximum number of hours that the user can keep the work profile turned off. Depends on: Limit length of time work profile can be turned off	• Work and personal - full control • Work and personal - full control (Premium) • Work and personal - full control (Android Management)	259200 seconds (3 days)	Minimum: 259200 seconds (3 days) Maximum: 31622400 seconds (366 days)

Name	Description	Activation Types	Default	Possible Values
Require certificate revocation (CRL) check for apps	Specify if apps must check for revoked certificates in the server certificate chain when opening SSL connections in the work profile. This rule applies only to apps that use the standard Java SSL sockets and TrustManager implementation (including most native apps), but does not apply to third-party browsers. The certificate revocation check uses CRLs from the CRL distribution point listed in the certificates. If the "Require OCSP check" rule is selected, apps first check for certificate revocation using OCSP. If OCSP fails, then apps check the CRLs. This rule applies only to Samsung devices	• Work and personal - user privacy (Premium) • Work and personal - user privacy (Samsung Knox) • Work space only (Premium) • Work and personal - full control (Premium) • Work and personal - full control (Samsung Knox)	Not Selected	
Require OCSP check for apps	Specify if apps must use OCSP before using CRLs to check for revoked certificates when opening SSL connections in the work profile. The OCSP check uses the OCSP response server in the "Authority Information Access" extension in the certificate. This rule applies only to Samsung devices. Depends on: Require certificate revocation (CRL) check for apps	• Work and personal - user privacy (Premium) • Work and personal - user privacy (Samsung Knox) • Work space only (Premium) • Work and personal - full control (Premium) • Work and personal - full control (Samsung Knox)	Not Selected	

Name	Description	Activation Types	Default	Possible Values
Validate end-user installed certificates	Specify whether the device validates certificates installed by end users. If one of the validation checks (for example, certification path, expiration date, or revocation status) fails, the device blocks the installation of the certificate. This rule applies only to Samsung devices.	• Work and personal - user privacy (Premium) • Work space only (Premium) • Work and personal - full control (Premium) • Work and personal - full control (Samsung Knox)	Not Selected	
Allow "Share via" list	Specify whether a work app can display the "Share via" list to allow a user to share content across work apps in the work profile.	• Work and personal - user privacy (Premium) • Work and personal - user privacy (Samsung Knox) • Work space only • Work space only (Premium) • Work and personal - full control (Premium) • Work and personal - full control (Samsung Knox)	Selected	

Name	Description	Activation Types	Default	Possible Values
Allow screenshots in the work profile to be stored in the personal profile	Specify whether screenshots taken in the work profile can be saved in the personal profile. This rule applies only to devices running Android OS 13.0.0 and later, but does not apply to devices running Android OS 15.0.0 and later. Applies only to devices that support Samsung Knox API level 36 and later. Minimum OS version: 13.0.0	• Work and personal - user privacy (Premium) • Work and personal - full control (Premium)	Not Selected	
Allow work files in the personal profile	Specify whether a user can move files from the work profile to the personal profile on a device. This rule does not apply to devices running Android OS 13 and later. Applies only to devices that support Samsung Knox API level 11 and later. Minimum OS version: 13.0.0	• Work and personal - user privacy (Premium) • Work and personal - full control (Premium)	Not Selected	
Allow personal files in the work profile	Specify whether a user can move files from the personal profile to the work profile on a device. This rule does not apply to devices running Android OS 13 and later. Applies only to devices that support Samsung Knox API level 11 and later. Minimum OS version: 13.0.0	• Work and personal - user privacy (Premium) • Work and personal - full control (Premium)	Not Selected	

Name	Description	Activation Types	Default	Possible Values
Enable work and personal data synchronization	Specify if apps can synchronize data between the work profile and the personal profile. This rule does not apply to devices running Android OS 13 and later.	• Work and personal - user privacy (Premium) • Work and Personal - user privacy (Samsung Knox) • Work and personal - full control (Premium) • Work and personal - full control (Samsung Knox)	Not Selected	
Allow personal calendar data in the work profile	Specify whether the calendar app can import personal calendar data into the work profile. This rule does not apply to devices running Android OS 13 and later. Applies only to devices that support Samsung Knox API level 11 and later. Depends on: Enable work and personal data synchronization	• Work and personal - user privacy (Premium) • Work and personal - full control (Premium)	Not Selected	
Allow work calendar data in the personal profile	Specify whether the calendar app can export work calendar from the work profile into the personal profile. This rule does not apply to devices running Android OS 13 and later. Applies only to devices that support Samsung Knox API level 11 and later. Depends on: Enable work and personal data synchronization	• Work and personal - user privacy (Premium) • Work and personal - full control (Premium)	Not Selected	

Name	Description	Activation Types	Default	Possible Values
Allow contact synchronization	Specify whether the contacts app can synchronize contact data between the Knox Workspace and the personal space. Depends on: Enable work and personal data synchronization	• Work and personal - full control (Samsung Knox) • Work and personal - user privacy (Samsung Knox)	Not Selected	
Allow calendar synchronization	Specify whether the calendar app can synchronize calendar data between the Knox Workspace and the personal space. Depends on: Enable work and personal data synchronization	• Work and personal - full control (Samsung Knox) • Work and personal - user privacy (Samsung Knox)	Not Selected	
Allow user modification of "Show notification content" setting	Specify whether a user can change the "Show notification content" setting on a device. This setting determines whether the device displays reduced information about work notifications in the personal profile. This rule does not apply to devices running Android OS 13 and later. Applies only to devices that support Samsung Knox API level 11 and later. Depends on: Enable work and personal data synchronization	• Work and personal - user privacy (Premium) • Work and personal - full control (Premium)	Not Selected	
Require fast encryption	Specify if a device must use fast encryption mode only.	Work and personal - full control (Samsung Knox)	Not Selected	

Name	Description	Activation Types	Default	Possible Values
Allow screen capture (DDMS)	Specify if a user can take screenshots. If this rule is not selected, users also cannot take screenshots using the Dalvik Debug Monitor Server (DDMS).	Work and personal - full control (Samsung Knox)	Selected	
Allow factory reset	Specify if a user can perform a factory reset on a device.	Work and personal - full control (Samsung Knox)	Selected	
Allow users to deactivate devices	Specify whether the user can deactivate the device and wipe all work data.	Work and personal - full control (Samsung Knox)	Selected	
Data wipe on deactivation	Specify what data is deleted from the device when it is deactivated.	Work and personal - full control (Samsung Knox)	Delete work space	• Delete work space • Delete all device data
Allow screen capture in Knox Workspace	Specify whether a user can take screenshots in the Knox Workspace.	• Work and personal - full control (Samsung Knox) • Work and personal - user privacy (Samsung Knox)	Selected	
Allow work files into the personal space	Specify whether a user can move work files from the Knox Workspace to the personal space on a device.	• Work and personal - full control (Samsung Knox) • Work and personal - user privacy (Samsung Knox)	Selected	

Name	Description	Activation Types	Default	Possible Values
Allow non-secure keypad	Specify whether a user can use a non-secure keypad in the Knox Workspace.	• Work and personal - full control (Samsung Knox) • Work and personal - user privacy (Samsung Knox)	Selected	
Allow personal files in the Knox Workspace	Specify whether a user can move files from the personal space to the Knox Workspace on a device.	• Work and personal - full control (Samsung Knox) • Work and personal - user privacy (Samsung Knox)	Not Selected	
Enable Trusted Boot verification	Specify whether Trusted Boot verifies the OS and kernel before decrypting the Knox Workspace. If this rule is selected and the device OS or kernel is compromised, the Knox warranty bit is fused and the user can no longer access or create a Knox Workspace. If this rule is selected, the device restarts for the rule to take effect.	Work and personal - full control (Samsung Knox)	Not Selected	
Allow USB access for apps in Knox Workspace	Specify whether apps in Knox Workspace can read and write data to a USB storage device.	• Work and personal - full control (Samsung Knox) • Work and personal - user privacy (Samsung Knox)	Not Selected	

Android: Apps rules

Name	Description	Activation Types	Default	Possible Values
Send SMS/MMS logs to UEM	Specify whether the device synchronizes logs for SMS text messages and MMS messages with your EMM server.	Work space only (Premium)	Not selected	
Send phone logs to UEM	Specify whether the device synchronizes the call log for the Phone app with your EMM server. This rule applies only to the following activation types: Work space only (Premium)	Work space only (Premium)	Not selected	
Require app verification	Specify whether the device must verify apps. If this rule is not selected, the user can disable app verification. This rule affects both work and personal apps.	• Work space only • Work space only (Premium) • Work space only (Android Management) • Work and personal - user privacy • Work and personal - user privacy (Premium) • Work and personal - user privacy (Android Management) • Work and personal - full control • Work and personal - full control (Premium) • Work and personal - full control (Android Management)	Selected	

Name	Description	Activation Types	Default	Possible Values
Allow installation of non Google Play apps override	Specify whether users can install apps from sources other than Google Play (unknown sources) globally on the device for all users, install apps using the app installer (the ACTION_INSTALL_PACKAGE mechanism), or install non Google Play apps. If this rule is not selected, the user cannot change this setting on the device. If the rule is selected, users can access the UI that allows them to install non Google Play apps. If you disallow installation of non-Google play apps using this rule, the settings for the same rule in personal and work profiles are ignored. If this rule is selected, you can disallow installation of non-Google play apps in just the work profile or just the personal profile.	• Work space only • Work space only (Premium) • Work and personal - full control • Work and personal - full control (Premium) • Work and personal - full control (Samsung Knox) • Work and personal - user privacy • Work and personal - user privacy (Premium)	Selected	
Allow installation of non Google Play apps	Specify whether users can install apps using the app installer (the ACTION_INSTALL_PACKAGE mechanism).	• Work space only • Work space only (Premium) • Work and personal - user privacy • Work and personal - user privacy (Premium) • Work and personal - full control • Work and personal - full control (Premium)	Not selected	

Name	Description	Activation Types	Default	Possible Values
Installation policy of non Google Play apps	Specify whether users can install apps from sources other than Google Play (unknown sources)	• Work space only (Android Management) • Work and personal - user privacy (Android Management) • Work and personal - full control (Android Management)		• Disallow untrusted app install on entire device • Allow untrusted app installs in the device's personal profile only • Allow untrusted app installs on entire device
Allow phone	Specify if a user can use the phone. If this rule is not selected, the device can only make emergency calls. All other calls and messages are blocked. Applies only to devices that support Samsung Knox API level 2 and later.	• Work space only • Work space only (Premium) • Work and personal - full control • Work and personal - full control (Premium) • Work and personal - full control (Samsung Knox)	Selected	
Allow outgoing MMS	Specify if a device can send MMS messages.	• Work and personal - full control (Samsung Knox) • Work space only • Work space only (Premium)	Selected	

Name	Description	Activation Types	Default	Possible Values
Allow incoming MMS	Specify if a device can receive MMS messages.	• Work space only • Work space only (Premium) • Work and personal - full control (Samsung Knox)	Selected	
Allow RCS features	Specify whether Rich Communication Services can be used on the device.	• Work space only • Work space only (Premium) • Work and personal - full control • Work and personal - full control (Premium) • Work and personal - full control (Samsung Knox)	Selected	
Set SMS/MMS Signature	Specify the signature that is appended to outgoing SMS or MMS messages sent by the user. The signature can contain a maximum of 30 characters.	• Work and personal - full control (Samsung Knox) • Work space only • Work space only (Premium)		Maximum value: 30 characters

Name	Description	Activation Types	Default	Possible Values
Allow outgoing SMS	Specify if a device can send SMS messages.	• Work space only • Work space only (Premium) • Work and personal - full control • Work and personal - full control (Premium) • Work and personal - full control (Samsung Knox)	Selected	
Allow incoming SMS	Specify if a device can receive SMS messages.	• Work space only • Work space only (Premium) • Work and personal - full control • Work and personal - full control (Premium) • Work and personal - full control (Samsung Knox)	Selected	

Name	Description	Activation Types	Default	Possible Values
Default app permissions	Specify whether app permission requests are granted or denied by default. If you select "Prompt user" the user is asked to grant or deny permissions. If you select "Always grant" the user is not prompted and permission requests are always granted. If you select "Always deny" the user is not prompted and permissions requests are always denied. "Always grant" is supported by some sensor-related permissions only with Workspace only activations.	• Work space only • Work space only (Premium) • Work space only (Android Management) • Work and personal - user privacy • Work and personal - user privacy (Premium) • Work and personal - user privacy (Android Management) • Work and personal - full control • Work and personal - full control (Premium) • Work and personal - full control (Android Management)	Prompt user	• Prompt user • Always grant • Always deny

Name	Description	Activation Types	Default	Possible Values
Skip first use hints	Specify whether work apps should to skip showing any introductory hints that display the first time the app is launched.	• Work space only • Work space only (Premium) • Work space only (Android Management) • Work and personal - user privacy • Work and personal - user privacy (Premium) • Work and personal - user privacy (Android Management) • Work and personal - full control • Work and personal - full control (Premium) • Work and personal - full control (Android Management)	Not Selected	

Name	Description	Activation Types	Default	Possible Values
Apps restricted from metered networks	Specify the apps that are restricted from using metered data networks. You may want to restrict app network usage due to data costs and limits or battery and performance issues.	• Work space only • Work space only (Premium) • Work and personal - user privacy • Work and personal - user privacy (Premium) • Work and personal - full control • Work and personal - full control (Premium)		
Apps allowed to access work calendar	Specify the personal app package IDs that are allowed to access the work calendar.	• Work and personal - user privacy • Work and personal - user privacy (Premium) • Work and personal - full control • Work and personal - full control (Premium)		

Name	Description	Activation Types	Default	Possible Values
Apps allowed to manage certificates	Specify the list of app package IDs that can manage certificate.	• Work space only • Work space only (Premium) • Work and personal - user privacy • Work and personal - user privacy (Premium) • Work and personal - full control • Work and personal - full control (Premium)		
Apps allowed to request cross-profile access	Specify the package IDs of apps that can request permission from the user to access data in both the work and personal profiles.	• Work and personal - user privacy • Work and personal - user privacy (Premium) • Work and personal - full control • Work and personal - full control (Premium)		

Name	Description	Activation Types	Default	Possible Values
Allow S Voice	Specify whether a device can use the S Voice app. This rule does not apply to devices running Android OS 13 and later. Applies only to devices that support Samsung Knox API level 6 and later.	• Work space only • Work space only (Premium) • Work and personal - full control • Work and personal - full control (Premium) • Work and personal - full control (Samsung Knox)	Selected	
Enable JavaScript	Specify whether the native Android browser prevents the browser from running JavaScript code for a website. If this rule is not selected, a website that requires JavaScript to be active to execute a function (for example, an animation) cannot execute the function. If this rule is not selected, a user cannot change the setting on the device. Applies only to devices that support Samsung Knox API level 2 and later.	• Work and personal - user privacy (Premium) • Work and personal - user privacy (Samsung Knox) • Work space only • Work space only (Premium) • Work and personal - full control (Premium) • Work and personal - full control (Samsung Knox)	Selected	
Allow Google Play	Specify whether a user can use Google Play to install apps. This rule applies when a device is not connected to your organization's network.	Work and personal - full control (Samsung Knox)	Selected	

Name	Description	Activation Types	Default	Possible Values
Allow Android Backup Service	Specify if the user can back up device data to Google servers.	Work and personal - full control (Samsung KNOX)	Selected	
Allow browser cookies	Specify if the built-in Android browser prevents websites from storing cookies on a device. If this rule is not selected, websites that use cookies to preload user authentication information cannot do so. If this rule is not selected, the user cannot change this setting on the device.	• Work and personal - full control (Samsung Knox) • Work and personal - user privacy (Samsung Knox)	Selected	
Allow autofill setting	Specify if the built-in Android browser prevents websites from providing autofill suggestions when a user is filling in form data on a webpage, even if the user has previously filled in the form. If this rule is not selected, the user cannot change this setting on the device.	• Work and personal - full control (Samsung Knox) • Work and personal - user privacy (Samsung Knox)	Selected	
Enable pop-up browser setting	Specify if the built-in Android browser overrides the default pop-up browser setting to prevent websites from popping up new browser windows when the user navigates to a website that invokes this action. If this rule is not selected, the user cannot change this setting on the device.	• Work and personal - full control (Samsung Knox) • Work and personal - user privacy (Samsung Knox)	Selected	
Allow Google services	Specify whether a user can use Google services such as Gmail, Google Settings, and Google Play. This rule applies to the Knox Workspace only.	• Work and personal - full control (Samsung Knox) • Work and personal - user privacy (Samsung Knox)	Selected	

Name	Description	Activation Types	Default	Possible Values
Allow unified account view in BlackBerry Hub	Specify whether BlackBerry Hub can display both work and personal accounts and messages together in a single view. If this rule is not selected, the device must display work accounts and messages in a separate view from personal accounts and messages in BlackBerry Hub. If this rule is selected, the app must also be configured to allow a unified view for this rule to have an effect.	• Work and personal - user privacy • Work and personal - user privacy (Premium) • Work and personal - full control • Work and personal - full control (Premium)	Selected	

Android: Personal rules

Name	Description	Activation types	Default	Possible values
Allow audio recording	Specify whether a device can record audio. If this rule is not selected, the user can still make calls and use audio streaming using the device microphone. This rule applies to phone calls, voice recognition, and VoIP. If an app declares a use type and does something else, then this rule cannot block the app. If you deselect this rule, any ongoing audio recording is interrupted. Video recording is still allowed if no audio recording is attempted. This rule applies to the Personal space only. Applies only to devices that support Samsung Knox API level 6 and later.	• Work and personal - full control • Work and personal - full control (Premium)	Selected	

Name	Description	Activation types	Default	Possible values
Allow video recording	Specify whether a device can record video. If this rule is not selected, the camera is still available so that the user can take pictures and the user can use video streaming. When this rule is not selected, any ongoing video recording is interrupted. Applies only to devices that support Samsung Knox API level 6 and later.	• Work and personal - full control • Work and personal - full control (Premium)	Selected	
Allow sending crash reports to Google	Specify if the user can send crash reports to Google. Applies only to devices that support Samsung Knox API level 5 and later.	• Work and personal - full control • Work and personal - full control (Premium)	Selected	
Allow screen capture	Specify if a user can take screen shots of the device.	• Work and personal - full control • Work and personal - full control (Premium) • Work and personal - full control (Android Management)	Selected	
Allow lock screen features	Specify whether special features can be enabled on the device lock screen.	• Work and personal - full control • Work and personal - full control (Premium)	Selected	
Allow camera on lock screen	Specify whether users can access the device camera on lock screen. Depends on: Allow lock screen features	• Work and personal - full control • Work and personal - full control (Premium)	Selected	

Name	Description	Activation types	Default	Possible values
Allow notifications	Specify whether the device can display notifications on the lock screen. Depends on: Allow lock screen features	• Work and personal - full control • Work and personal - full control (Premium)	Selected	
Allow all notification content	Specify whether all notification content can appear on the lock screen or only the notification type. Depends on: Allow lock screen features	• Work and personal - full control • Work and personal - full control (Premium)	Selected	
Allow fingerprint authentication	Specify whether the user can unlock the device using a fingerprint. Depends on: Allow lock screen features	• Work and personal - full control • Work and personal - full control (Premium)	Selected	
Allow biometrics	Specify whether the user can use biometric authentication to unlock the device. Depends on: Allow lock screen features	• Work and personal - full control • Work and personal - full control (Premium)	Selected	
Allow facial recognition	Specify whether the user can unlock the device using face recognition. Depends on: Allow lock screen features	• Work and personal - full control • Work and personal - full control (Premium)	Selected	
Allow iris authentication	Specify whether the user can unlock the device using an iris scan. Depends on: Allow lock screen features	• Work and personal - full control • Work and personal - full control (Premium)	Selected	

Name	Description	Activation types	Default	Possible values
Allow trust agents for Google Smart Lock	Specify whether trust agents can unlock the device using Google Smart Lock. Depends on: Allow lock screen features	• Work and personal - full control • Work and personal - full control (Premium)	Selected	
Allow Google NFC trust agent	Specify if NFC can be used to unlock the device using Google Smart Lock. Depends on: Allow trust agents for Google Smart Lock	• Work and personal - full control • Work and personal - full control (Premium)	Selected	
Allow tags with basic authentication to unlock the device	Specify if NFC tags that authenticate using the tag ID can be used to unlock the device using Google Smart Lock. Depends on: Allow Google NFC trust agent	• Work and personal - full control • Work and personal - full control (Premium)	Selected	
Allow secure NFC tags to unlock the device	Specify if NFC tags that use challenge-response authentication can be used to unlock the device using Google Smart Lock. Depends on: Allow Google NFC trust agent	• Work and personal - full control • Work and personal - full control (Premium)	Selected	
Allow Google Bluetooth trust agent	Specify if Bluetooth can be used to unlock the device using Google Smart Lock. Depends on: Allow trust agents for Google Smart Lock	• Work and personal - full control • Work and personal - full control (Premium)	Selected	
Allow places trust agent	Specify if places can be used to unlock the device using Google Smart Lock. Depends on: Allow trust agents for Google Smart Lock	• Work and personal - full control • Work and personal - full control (Premium)	Selected	

Name	Description	Activation types	Default	Possible values
Allow custom places	Specify if a user can trust places other than Home. Depends on: Allow places trust agent	• Work and personal - full control • Work and personal - full control (Premium)	Selected	
Allow Google Face trust agent	Specify if face image can be used to unlock the device using Google Smart Lock. Depends on: Allow trust agents for Google Smart Lock	• Work and personal - full control • Work and personal - full control (Premium)	Not selected	
Allow Google Voice trust agent	Specify if voice can be used to unlock the device using Google Smart Lock. Depends on: Allow trust agents for Google Smart Lock	• Work and personal - full control • Work and personal - full control (Premium)	Selected	
Allow Google On-body trust agent	Specify if On-body can be used to unlock the device using Google Smart Lock. Depends on: Allow trust agents for Google Smart Lock	• Work and personal - full control • Work and personal - full control (Premium)	Selected	
Trust agent inactivity timeout	Specify Device inactivity timeout in minutes. When a device is in an idle state for a certain period of time, Google Smart Lock trust agents will be revoked. Depends on: Allow trust agents for Google Smart Lock	• Work and personal - full control • Work and personal - full control (Premium)	240 minutes	Minimum value: 1 minute Maximum value: 525600 minutes (365 days)
Allow AI assistant to use screen content	Specify if the AI assistant on the device can use capture screen content.	• Work and personal - full control • Work and personal - full control (Premium)	Selected	

Name	Description	Activation types	Default	Possible values
Allow AI to offer suggestions based on screen content	Specify if the AI assistant will provide selection suggestions based on screen content. Depends on: Allow AI assistant to use screen content	• Work and personal - full control • Work and personal - full control (Premium)	Selected	
Allow developer options	Specify whether users can enable developer options on the device.	• Work and personal - full control • Work and personal - full control (Premium)	Not selected	
Allowed personal apps from Google Play	Specify the apps that users can install from Google Play in the personal space. You can allow all apps from Google Play, block users from installing specified apps, or allow only specified apps to be installed. This rule does not block users from installing apps in the personal space using a method other than Google Play.	• Work and personal - full control • Work and personal - full control (Premium) • Work and personal - full control (Android Management)	Allow all apps	• Allow all apps • Block specified apps • Allow only specified apps
Personal apps	Specify the package IDs for the apps that you want to block or allow in the personal space. If you chose to block specified apps, users can't install the specified apps from Google Play. If you chose to allow only specified apps, users can install only the specified apps. Depends on: Allowed personal apps from Google Play	• Work and personal - full control • Work and personal - full control (Premium) • Work and personal - full control (Android Management)		

Name	Description	Activation types	Default	Possible values
Allow S Voice	Specify whether a device can use the S Voice app. This rule does not apply to devices with Android OS 13 and later. Applies only to devices that support Samsung Knox API level 6 and later.	• Work and personal - full control • Work and personal - full control (Premium)	Selected	

Windows IT policy rules

The section provides details for the available IT policy rules for Windows devices.

Windows: Password rules

Name	Description	Activation types	Default	Possible values
Password required for device	Specify whether a user must set a device password. Minimum OS version: 10.0	MDM controls	No	• No • Yes
Allow simple password	Specify whether the device password can contain repeated or sequential characters, such as 1111 or 1234. Depends on: Password required for device Minimum OS version: 10.0	MDM controls	Allow	• Disallow • Allow
Minimum password length	Specify the minimum number of characters that the device password must contain. Depends on: Password required for device Minimum OS version: 10.0	MDM controls	4 characters	Minimum value: 4 characters Maximum value: 16 characters
Password complexity	Specify the complexity of the device password. If set to "Alphanumeric," the password must contain both letters and numbers. If set to "Numeric," the password must contain only numbers. Depends on: Password required for device Minimum OS version: 10.0	MDM controls	Numeric	• Alphanumeric • Numeric

Name	Description	Activation types	Default	Possible values
Minimum number of character types	Specify the minimum number of character types that the device password must contain. If you select "1," the password requires numbers. If you select "2," the password also requires lowercase letters. If you select "3," the password also requires uppercase letters. If you select "4," the password also requires special characters. This rule does not apply to Windows 10 computers and tablets. Depends on: Password complexity Minimum OS version: 10.0	MDM controls	numbers required	• numbers required • numbers and lowercase letters required • numbers, lowercase letters, and uppercase letters required • numbers, lowercase letters, uppercase letters, and special characters required Minimum value: 1 character type Maximum value: 4 character types
Password expiration	Specify the maximum number of days that the device password can be used. After the specified number of days elapse, the password expires and a user must set a new password. If set to 0, the password does not expire. Depends on: Password required for device Minimum OS version: 10.0	MDM controls	0 days	Minimum value: 0 days Maximum value: 730 days
Password history	Specify the maximum number of previous passwords that a device checks to prevent a user from reusing a device password. If set to 0, the device does not check previous passwords. Depends on: Password required for device Minimum OS version: 10.0	MDM controls	0 passwords	Minimum value: 0 passwords Maximum value: 50 passwords

Name	Description	Activation types	Default	Possible values
Maximum failed password attempts	Specify the number of times that a user can enter an incorrect password before a device is wiped. If set to 0, the device is not wiped regardless of how many times the user enters an incorrect password. This rule does not apply to devices that allow multiple user accounts, including Windows 10 computers and tablets and Windows Mobile devices with Microsoft Passport. Depends on: Password required for device Minimum OS version: 10.0	MDM controls	0 attempts	Minimum value: 0 attempts Maximum value: 999 attempts
Maximum inactivity time lock	Specify the period of user inactivity that must elapse before a device locks. If set to 0, the device does not lock automatically. Depends on: Password required for device Minimum OS version: 10.0	MDM controls	0 minutes	Minimum value: 0 minutes Maximum value: 999 minutes
Allow idle return without password	Specify whether a user must type the password when the idle grace period ends. If this rule is selected, the user can set the password grace period timer. This rule does not apply to Windows 10 computers and tablets. Depends on: Password required for device Minimum OS version: 10.0	MDM controls	Allow	• Disallow • Allow

Name	Description	Activation types	Default	Possible values
Allow use of biometric gestures	Enable or disable the use of biometric gestures, such as face and fingerprint, as an alternative to the PIN gesture for Windows Hello for Business. Depends on: Password required for device Minimum OS version: 10.0.14393	MDM controls	Selected	
Enable enhanced anti-spoofing for facial feature recognition	Enable or disable enhanced anti-spoofing for facial feature recognition on Windows Hello face authentication. Depends on: Password required for device Minimum OS version: 10.0.14393	MDM controls	Not selected	

Windows: Device functionality rules

Name	Description	Activation types	Default	Possible values
Allow storage card	Specify whether the storage card is enabled.	MDM controls	Allow	• Disallow • Allow
Allow Windows license reactivation	Specify whether users can reactivate their Windows license if required, for example, after a significant hardware change. This rule does not apply to Windows 10 smartphones. Minimum OS version: 10.0.14393	MDM controls	Allow	• Disallow • Allow
Allow Wi-Fi	Specify whether a device can make Wi-Fi connections. This rule does not apply to Windows 10 computers and tablets. Minimum OS version: 10.0	MDM controls	Allow	• Disallow • Allow

Name	Description	Activation types	Default	Possible values
Allow Internet Sharing	Specify whether a user can use Internet Sharing. Depends on: Allow Wi-Fi Minimum OS version: 10.0	MDM controls	Allow	• Disallow • Allow
Allow auto-connect to Wi-Fi hotspots	Specify whether a device can automatically connect to Wi-Fi hotspots and Wi-Fi networks that are shared with contacts. Depends on: Allow Wi-Fi Minimum OS version: 10.0	MDM controls	Allow	• Disallow • Allow
Allow manual Wi-Fi configuration	Specify whether a user can configure a device to connect to Wi-Fi networks that are outside your installed networks. This rule does not apply to Windows 10 computers and tablets. Depends on: Allow Wi-Fi Minimum OS version: 10.0	MDM controls	Allow	• Disallow • Allow
Allow offline maps automatic updates	Specify whether the device automatically downloads updates for offline maps when the device is online. Minimum OS version: 10.0.14393	MDM controls	Allow	• Allow • Disallow • Required
Allow offline maps updates over metered connection	Specify whether the device automatically downloads updates for offline maps when the device is using a metered connection. Depends on: Allow offline maps automatic updates Minimum OS version: 10.0.14393	MDM controls	Allow	• Allow • Disallow • Required

Name	Description	Activation types	Default	Possible values
Allow SMS and MMS sync	Specify whether users can back up and restore SMS and MMS messages and use and Messaging Everywhere. This rule does not apply to Windows 10 computers and tablets. Minimum OS version: 10.0.14393	MDM controls	Disallow	• Disallow • Allow
Allow notification mirroring	Specify whether app and system notifications can be mirrored to other Windows devices that the user is logged in to. Minimum OS version: 10.0.14393	MDM controls	Allow	• Disallow • Allow
Allow NFC	Specify whether a device can use NFC. This rule does not apply to Windows 10 computers and tablets. Minimum OS version: 10.0	MDM controls	Allow	• Disallow • Allow
Allow Bluetooth	Specify whether a device can use Bluetooth. Minimum OS version: 10.0	MDM controls	Allow	• Disallow • Allow
Allow VPN	Specify whether a device can use VPN. Minimum OS version: 10.0	MDM controls	Allow	• Disallow • Allow
Allow VPN over mobile networks	Specify whether a device can use VPN over mobile networks. Minimum OS version: 10.0	MDM controls	Allow	• Disallow • Allow
Allow VPN roaming over mobile networks	Specify whether a device can connect to VPN when the device roams over mobile networks. Depends on: Allow VPN over mobile networks Minimum OS version: 10.0	MDM controls	Allow	• Disallow • Allow

Name	Description	Activation types	Default	Possible values
Allow telemetry	Specify whether a device can send telemetry information (such as SQM or Watson) to Microsoft. Minimum OS version: 10.0 Obsolete in OS version: 10.0.19045	MDM controls	Allow	• Disallow • Allow except for secondary data requests • Allow
Allow copy and paste	Specify whether a user can copy and paste. This rule does not apply to Windows 10 computers and tablets. This rule applies only to Windows 10 Mobile devices. Minimum OS version: 10.0	MDM controls	Allow	• Disallow • Allow
Allow adding email accounts	Specify whether a user can add email accounts to the device. Minimum OS version: 10.0	MDM controls	Allow	• Disallow • Allow
Allow manual root certificate installation	Specify whether a user can manually install root and intermediate CAP certificates. This rule does not apply to Windows 10 computers and tablets. This rule applies only to Windows 10 Mobile devices. Minimum OS version: 10.0	MDM controls	Allow	• Disallow • Allow
Require device encryption	Specify whether a device must use internal storage encryption. Once you turn device encryption on, you cannot turn it off using this rule. This rule does not apply to Windows 10 computers and tablets. Minimum OS version: 10.0	MDM controls	Off	• Off • On

Name	Description	Activation types	Default	Possible values
Allow app store	Specify whether the app store is allowed. This rule does not apply to Windows 10 computers and tablets. This rule applies only to Windows 10 Mobile devices. Minimum OS version: 10.0	MDM controls	Allow	• Disallow • Allow
Allow apps from Windows Store	Specify whether the device can open apps from the Windows Store. This rule disables apps downloaded by a user and apps preloaded on the device. This rule does not apply to Windows 10 smartphones. Minimum OS version: 10.0.14393	MDM controls	Allow	• Disallow • Allow
Allow developer unlock	Specify whether a developer can unlock a device. Minimum OS version: 10.0	MDM controls	Allow	• Disallow • Allow
Allow browser	Specify whether Internet Explorer or Microsoft Edge are allowed on the device. This rule does not apply to Windows 10 computers and tablets. This rule applies only to Windows 10 Mobile devices. Minimum OS version: 10.0	MDM controls	Allow	• Disallow • Allow
Allow cookies	Specify whether cookies are allowed in the browser. This rule is supported only by Microsoft Edge version 45 and earlier. Minimum OS version: 10.0	MDM controls	Allow	• Disallow • Allow

Name	Description	Activation types	Default	Possible values
Allow Do Not Track headers	Specify whether the browser can send Do Not Track headers. This rule is supported only by Microsoft Edge version 45 and earlier. Minimum OS version: 10.0 Obsolete in OS version: 10.0.19045	MDM controls	Disallow	• Disallow • Allow
Allow InPrivate browsing on the work network	Specify whether users can use InPrivate browsing while connected to your work network. This rule is supported only by Microsoft Edge version 45 and earlier. Minimum OS version: 10.0 Obsolete in OS version: 10.0.19045	MDM controls	Allow	• Disallow • Allow
Allow pop-up blocker	Specify whether the pop-up blocker is allowed. This rule is supported only by Microsoft Edge version 45 and earlier. Minimum OS version: 10.0 Obsolete in OS version: 10.0.19045	MDM controls	Disallow	• Disallow • Allow
Allow SmartScreen Filter	Specify whether the SmartScreen Filter can be used in the browser. This rule is supported only by Microsoft Edge version 45 and earlier. Minimum OS version: 10.0 Obsolete in OS version: 10.0.19045	MDM controls	Allow	• Disallow • Allow

Name	Description	Activation types	Default	Possible values
Allow ignoring SmartScreen Filter site warnings	Specify whether users can ignore SmartScreen Filter warnings about potentially malicious websites and continue on to the site. This rule is supported only by Microsoft Edge version 45 and earlier. Depends on: Allow SmartScreen Filter Minimum OS version: 10.0 Obsolete in OS version: 10.0.19045	MDM controls	Allow	• Disallow • Allow
Allow ignoring SmartScreen Filter download warnings	Specify whether users can ignore SmartScreen Filter warnings about downloading unverified files and continue the download process. This rule is supported only by Microsoft Edge version 45 and earlier. Depends on: Allow SmartScreen Filter Minimum OS version: 10.0 Obsolete in OS version: 10.0.19045	MDM controls	Allow	• Disallow • Allow
Display IP address during WebRTC phone calls	Specify whether the localhost IP address is displayed while making phone calls using the WebRTC protocol. This rule does not apply to Windows 10 smartphones. This rule is supported only by Microsoft Edge version 45 and earlier. Minimum OS version: 10.0 Obsolete in OS version: 10.0.19045	MDM controls	Allow	• Disallow • Allow

Name	Description	Activation types	Default	Possible values
Allow autofill	Specify whether the browser remembers text entered in web forms. This rule is supported only by Microsoft Edge version 45 and earlier. Minimum OS version: 10.0 Obsolete in OS version: 10.0.19045	MDM controls	Allow	• Disallow • Allow
Allow saving and managing passwords	Specify whether the user can save and manage passwords in the browser. This rule is supported only by Microsoft Edge version 45 and earlier. Minimum OS version: 10.0 Obsolete in OS version: 10.0.19045	MDM controls	Allow	• Disallow • Allow
Allow search suggestions in address bar	Specify whether search suggestions are allowed in the address bar. This rule is supported only by Microsoft Edge version 45 and earlier. Minimum OS version: 10.0 Obsolete in OS version: 10.0.19045	MDM controls	Allow	• Disallow • Allow
Allow extensions in Edge browser	Specifies whether Microsoft Edge extensions are allowed. This rule is supported only by Microsoft Edge version 45 and earlier. Minimum OS version: 10.0.14393 Obsolete in OS version: 10.0.19045	MDM controls	Allow	• Disallow • Allow

Name	Description	Activation types	Default	Possible values
Mobile browser first run URL	Specify the URL that opens in Microsoft Edge when the browser is opened for the first time. This rule does not apply to Windows 10 computers and tablets. This rule applies only to Windows 10 Mobile devices. Minimum OS version: 10.0 Obsolete in OS version: 10.0.19045	MDM controls		
Browser start pages	Specify start pages for the browser. Separate multiple pages using the XML-escaped characters < and >. This rule does not apply to Windows 10 smartphones. This rule is supported only by Microsoft Edge version 45 and earlier. Minimum OS version: 10.0 Obsolete in OS version: 10.0.19045	MDM controls		
Send Intranet traffic to Internet Explorer	Specify whether the device opens Intranet sites in Internet Explorer. If this rule is not selected, Intranet sites open in Microsoft Edge. This rule does not apply to Windows 10 smartphones. This rule is supported only by Microsoft Edge version 45 and earlier. Minimum OS version: 10.0 Obsolete in OS version: 10.0.19045	MDM controls	Allow	• Disallow • Allow

Name	Description	Activation types	Default	Possible values
Enterprise site list URL	If your organization has enabled Enterprise Mode for Internet Explorer, specify the URL for your organization's enterprise site list. This rule is supported only by Microsoft Edge version 45 and earlier. Minimum OS version: 10.0 Obsolete in OS version: 10.0.19045	MDM controls		
Display message when opening enterprise site list pages in Microsoft Edge	Specify whether Microsoft Edge displays an interstitial page when opening sites that are configured to open in Internet Explorer using the enterprise site list. This rule does not apply to Windows 10 smartphones. This rule is supported only by Microsoft Edge version 45 and earlier. Minimum OS version: 10.0.14393 Obsolete in OS version: 10.0.19045	MDM controls	Disallow	• Disallow • Allow
Allow edge swipe	Specify whether the user can use edge swipe actions, for example, swiping from the right edge to open the Action Center or swiping from the left edge to view all open apps. This rule does not apply to Windows 10 smartphones. Minimum OS version: 10.0.14393	MDM controls	Allow	• Disallow • Allow

Name	Description	Activation types	Default	Possible values
Allow access to developer tools	Specify whether the user can display Developer Tools in Microsoft Edge by pressing F12. This rule does not apply to Windows 10 smartphones. This rule is supported only by Microsoft Edge version 45 and earlier. This rule applies only to devices running Windows 10.0 to, but not including, version 10.0.19045. Minimum OS version: 10.0	MDM controls	Allow	• Disallow • Allow
Allow access to the about:flags page	Specify whether users can access the about:flags page, which can be used to change developer settings and to enable experimental features. This rule is supported only by Microsoft Edge version 45 and earlier. This rule applies only to devices running Windows 10.0.14393 to, but not including, version 10.0.19045. Minimum OS version: 10.0.14393	MDM controls	Allow	• Disallow • Allow
Allow screen capture	Specify whether a user can use the screen capture feature. This rule does not apply to Windows 10 computers and tablets. This rule applies only to Windows 10 Mobile devices. Minimum OS version: 10.0	MDM controls	Allow	• Disallow • Allow
Allow location services	Specify if a user can turn on the location service. This rule applies only to devices running Windows 10.0 to, but not including, version 10.0.19045. Minimum OS version: 10.0	MDM controls	Allow	• Disallow • Allow

Name	Description	Activation types	Default	Possible values
Allow USB connection	Specify whether a computer can access a device's memory using a USB connection. Both MTP and IP over USB are turned off when this rule is enforced. This rule does not apply to Windows 10 computers and tablets. This rule applies only to Windows 10 Mobile devices. Minimum OS version: 10.0	MDM controls	Allow	• Disallow • Allow
Allow mobile data roaming	Specify whether a device can use data services over the wireless network when the device is roaming. Minimum OS version: 10.0	MDM controls	Allow	• Disallow • Allow
Allow camera	Specify whether a device can use the camera. Minimum OS version: 10.0	MDM controls	Allow	• Disallow • Allow
Allow search to use location	Specify whether the search can use location information. Minimum OS version: 10.0	MDM controls	Allow	• Disallow • Allow
Enable safe search permissions	Specify whether you want to configure safe search permissions so that you can filter adult content. This rule does not apply to Windows 10 computers and tablets. This rule applies only to Windows 10 Mobile devices. Minimum OS version: 10.0	MDM controls	Not selected	

Name	Description	Activation types	Default	Possible values
Safe search permissions	Specify what level of safe search (filtering adult content) is required. If you set the value to Moderate, valid search results are not filtered. This rule does not apply to Windows 10 computers and tablets. This rule applies only to Windows 10 Mobile devices. Depends on: Enable safe search permissions Minimum OS version: 10.0	MDM controls	Moderate	• Strict • Moderate
Allow voice recording	Specify whether voice recording is allowed. This rule does not apply to Windows 10 computers and tablets. This rule applies only to Windows 10 Mobile devices. Minimum OS version: 10.0	MDM controls	Allow	• Disallow • Allow
Allow action center notifications	Specify whether a device can display action center notifications above the device lock screen. This rule does not apply to Windows 10 computers and tablets. This rule applies only to Windows 10 Mobile devices. Minimum OS version: 10.0	MDM controls	Allow	• Disallow • Allow
Allow Cortana	Specify whether Cortana is allowed on a device. Minimum OS version: 10.0	MDM controls	Allow	• Disallow • Allow
Allow Cortana above lock	Specify whether the user can interact with Cortana using voice commands while the device is locked. Depends on: Allow Cortana Minimum OS version: 10.0.14393	MDM controls	Allow	• Disallow • Allow

Name	Description	Activation types	Default	Possible values
Allow speech model updates	Specify whether the device can receive Microsoft updates to the speech recognition and speech synthesis models. Minimum OS version: 10.0.14393	MDM controls	Allow	• Disallow • Allow
Allow sync my settings	Specify whether a user can share their device settings with other devices using the "Sync My Settings" option. Minimum OS version: 10.0	MDM controls	Allow	• Disallow • Allow
Lock screen image provider	Specify the package ID of the lock screen image provider. If you don't set this rule, the user can set the lock screen image. This rule does not apply to Windows 10 computers and tablets. This rule applies only to Windows 10 Mobile devices. Minimum OS version: 10.0.14393	MDM controls		
Update installation day	Specify the day that updates are installed. This rule takes effect only if the "Automatic updates" rule is set to "Install updates and restart at specified time." This rule does not apply to Windows 10 smartphones. Minimum OS version: 10.0.14393 Obsolete in OS version: 10.0.19045	MDM controls	Every day	• Every day • Sunday • Monday • Tuesday • Wednesday • Thursday • Friday • Saturday

Name	Description	Activation types	Default	Possible values
Update installation hour	Specify the hour of the day that updates are installed. The value corresponds to a 24-hour clock where 0 represents 12 AM. This rule takes effect only if the "Automatic updates" rule is set to "Install updates and restart at specified time." This rule does not apply to Windows 10 smartphones. Minimum OS version: 10.0.14393 Obsolete in OS version: 10.0.19045	MDM controls	3 (3:00 am)	Minimum value: 0 (midnight) Maximum value: 23 (11:00 pm)
Active hours start	Specify the start of the range of hours when the user is usually active and Windows update reboots are not scheduled. The value corresponds to a 24-hour clock where 0 represents 12 AM. If the "Automatic Updates" rule is set to "Turn off automatic updates," this rule does not apply. This rule does not apply to Windows 10 smartphones. Minimum OS version: 10.0.14393 Obsolete in OS version: 10.0.19045	MDM controls	8 (8:00 am)	Minimum value: 0 (midnight) Maximum value: 23 (11:00 pm)

Name	Description	Activation types	Default	Possible values
Active hours end	Specify the end of the range of hours when the user is usually active and Windows update reboots are not scheduled. The value corresponds to a 24-hour clock where 0 represents 12 AM. If the "Automatic Updates" rule is set to "Turn off automatic updates," this rule does not apply. This rule does not apply to Windows 10 smartphones. Minimum OS version: 10.0.14393 Obsolete in OS version: 10.0.19045	MDM controls	17 (5:00 pm)	Minimum value: 0 (midnight) Maximum value: 23 (11:00 pm)
Delivery Optimization mode	Specify the methods that Delivery Optimization can use to download Windows updates, apps, and app updates to the device. This rule does not apply to Windows 10 smartphones. Minimum OS version: 10.0.14393 Obsolete in OS version: 10.0.19045	MDM controls	HTTP and peering on same NAT	• HTTP only • HTTP and peering on same NAT • HTTP and peering across private group • HTTP and Internet peering • HTTP only - no contact with Delivery Optimization cloud service • BITS only

Name	Description	Activation types	Default	Possible values
Allow Delivery Optimization peer caching over VPN	Specify whether the device can participate in peer caching when connected to the work network using VPN. This rule takes effect only if the "Delivery Optimization mode" rule is set to an option that allows peering. This rule does not apply to Windows 10 smartphones. Minimum OS version: 10.0.15063 Obsolete in OS version: 10.0.19045	MDM controls	Allow	• Disallow • Allow
Group identifier	Specify an arbitrary group ID that the device belongs to for local network peering between devices that are on different domains or are not on the same LAN. This rule takes effect only if the "Delivery Optimization mode" rule is set to "HTTP and peering across private group". This rule does not apply to Windows 10 smartphones. Minimum OS version: 10.0.14393 Obsolete in OS version: 10.0.19045	MDM controls		

Name	Description	Activation types	Default	Possible values
Minimum RAM for peer caching	Specify the minimum amount of RAM in GB that the device must have to use peer caching. Devices with less than the specified amount of RAM can't use peer caching. If set to 0, the Delivery Optimization cloud service default is used. This rule takes effect only if the "Delivery Optimization mode" rule is set to an option that allows peering. This rule does not apply to Windows 10 smartphones. Minimum OS version: 10.0.15063 Obsolete in OS version: 10.0.19045	MDM controls	4 GB	Minimum value: 0 GB Maximum value: 2147483647 GB
Cache drive	Specify the drive that Delivery Optimization uses for the cache on the device. The drive location can be specified using environment variables, drive letter, or a full path. If no drive is specified, %SystemDrive% is used to store the cache. This rule takes effect only if the "Delivery Optimization mode" rule is set to an option that allows peering. This rule does not apply to Windows 10 smartphones. Minimum OS version: 10.0.14393 Obsolete in OS version: 10.0.19045	MDM controls		

Name	Description	Activation types	Default	Possible values
Minimum disk size allowed to peer	Specify the minimum disk size capacity in GB for the device to use peer caching. If set to 0, the Delivery Optimization cloud service default is used. This rule takes effect only if the "Delivery Optimization mode" rule is set to an option that allows peering. Recommended values: 64 GB to 256 GB. This rule does not apply to Windows 10 smartphones. Minimum OS version: 10.0.15063 Obsolete in OS version: 10.0.19045	MDM controls	64 GB	Minimum value: 0 GB Maximum value: 2147483647 GB
Maximum cache size percentage	Specify the maximum percentage of the disk size that Delivery Optimization can use for the cache. The "Absolute maximum cache size" rule takes precedence over this rule. This rule takes effect only if the "Delivery Optimization mode" rule is set to an option that allows peering. This rule applies to Windows 10 computers and tablets. Minimum OS version: 10.0.14393 Obsolete in OS version: 10.0.19045	MDM controls	20 percent	Minimum value: 1 percent Maximum value: 100 percent

Name	Description	Activation types	Default	Possible values
Absolute maximum cache size	Specify the maximum size in GB of the Delivery Optimization cache. Delivery Optimization clears the cache when the device is low on disk space. This rule takes precedence over the "Maximum cache size percentage" rule. If set to 0, the Delivery Optimization cloud service default is used. This rule takes effect only if the "Delivery Optimization mode" rule is set to an option that allows peering. This rule does not apply to Windows 10 smartphones. Minimum OS version: 10.0.14393 Obsolete in OS version: 10.0.19045	MDM controls	10 GB	Minimum value: 0 GB Maximum value: 2147483647 GB
Minimum file size to cache	Specify the minimum file size in MB that can be downloaded using peering. If set to 0, the Delivery Optimization cloud service default is used. This rule takes effect only if the "Delivery Optimization mode" rule is set to an option that allows peering. This rule does not apply to Windows 10 smartphones. Minimum OS version: 10.0.15063 Obsolete in OS version: 10.0.19045	MDM controls	100 MB	Minimum value: 0 GB Maximum value: 2147483647 GB

Name	Description	Activation types	Default	Possible values
Maximum cache age	Specify the maximum time in seconds that each file remains in the Delivery Optimization cache after downloading successfully. If set to 0, Delivery Optimization holds the files in the cache and makes them available for upload to other devices as long as the cache size is not exceeded. This rule takes effect only if the "Delivery Optimization mode" rule is set to an option that allows peering. This rule does not apply to Windows 10 smartphones. Minimum OS version: 10.0.14393 Obsolete in OS version: 10.0.19045	MDM controls	259200 seconds (72 hours)	Minimum value: 0 GB Maximum value: 2147483647 GB
Maximum download bandwidth percentage	Specify the maximum percentage of available download bandwidth that Delivery Optimization uses across all concurrent download activities. If set to 0, Delivery Optimization dynamically adjusts to use the available bandwidth for downloads. This rule does not apply to Windows 10 smartphones. Minimum OS version: 10.0.14393	MDM controls	0	Minimum value: 0 percent Maximum value: 100 percent

Name	Description	Activation types	Default	Possible values
Maximum download bandwidth	Specify the maximum download bandwidth in KB/second that Delivery Optimization can use across all concurrent download activities. If set to 0, Delivery Optimization dynamically adjusts to use the available bandwidth for downloads. This rule does not apply to Windows 10 smartphones. Minimum OS version: 10.0.14393	MDM controls	0	Minimum value: 0 GB Maximum value: 2147483647 GB
Minimum download quality	Specify the minimum download speed in KB/second for background downloads. This rule affects the blending of peer and HTTP sources. Delivery Optimization complements the download from the HTTP source to achieve the minimum value set. This rule takes effect only if the "Delivery Optimization mode" rule is set to an option that allows peering. This rule does not apply to Windows 10 smartphones. Minimum OS version: 10.0.14393 Obsolete in OS version: 10.0.19045	MDM controls	500 KB/ second	Minimum value: 0 GB Maximum value: 2147483647 GB

Name	Description	Activation types	Default	Possible values
Minimum battery percentage for upload	Specify the minimum battery percentage remaining for devices to upload cached data to LAN and group peers while on battery power. Uploads will pause if the battery level drops below the minimum percentage. If set to 0, the Delivery Optimization cloud service default is used. This rule does not apply to Windows 10 smartphones. Minimum OS version: 10.0.15063 Obsolete in OS version: 10.0.19045	MDM controls	0, use the Delivery Optimization cloud service default	Minimum value: 0 percent Maximum value: 100 percent
Maximum upload bandwidth	Specify the maximum upload bandwidth in KB/second that Delivery Optimization can use across all concurrent upload activities. If set to 0, unlimited possible bandwidth is permitted, optimized for minimal usage. This rule takes effect only if the "Delivery Optimization mode" rule is set to an option that allows peering. This rule does not apply to Windows 10 smartphones. Minimum OS version: 10.0.14393 Obsolete in OS version: 10.0.14393	MDM controls	0	Minimum value: 0 GB Maximum value: 2147483647 GB

Name	Description	Activation types	Default	Possible values
Monthly upload data cap	Specify the maximum total data in GB that Delivery Optimization can upload to Internet peers in each calendar month. If set to 0, no monthly upload limit is applied. This rule takes effect only if the "Delivery Optimization mode" rule is set to an option that allows peering. This rule does not apply to Windows 10 smartphones. Minimum OS version: 10.0.14393 Obsolete in OS version: 10.0.19045	MDM controls	20 GB	Minimum value: 0 GB Maximum value: 2147483647 GB
Allow Windows Ink Workspace	Specify whether users can access the Windows Ink Workspace. This rule does not apply to Windows 10 smartphones. Minimum OS version: 10.0.14393	MDM controls	Allow	• Disallow • Allow only when device unlocked • Allow
Allow Windows Ink Workspace app suggestions	Specify whether Windows Ink Workspace is allowed to suggest apps. This rule does not apply to Windows 10 smartphones. Depends on: Allow Windows Ink Workspace Minimum OS version: 10.0.14393	MDM controls	Disabled	• Disallow • Allow

Windows: Security and privacy rules

Name	Description	Activation types	Default	Possible values
Send activation data to Microsoft	Specify whether the device can send data about its activation state to Microsoft. This rule applies to Windows 10 computers and tablets and to smartphones with Windows 10 Mobile Enterprise. Minimum OS version: 10.0.14393	MDM controls	Disabled	• Disabled • Enabled
Allow device to accept pairing and privacy consent prompts	Specify whether the device can automatically accept pairing and privacy user consent prompts when launching apps. If this rule is not selected, the user must manually accept the prompts. Minimum OS version: 10.0.14393	MDM controls	Disabled	• Disabled • Enabled
Allow projection to device	Specify whether the device is discoverable for other devices to project to it. This rule does not apply to Windows 10 smartphones. Minimum OS version: 10.0.14393	MDM controls	Allow	• Disallow • Allow
Require PIN for pairing	Specify whether a PIN is required for pairing with other devices. This rule does not apply to Windows 10 smartphones. Minimum OS version: 10.0.14393	MDM controls	Not required	• Not Required • Required
Enable Microsoft advertising ID	Specify whether the Microsoft advertising ID is enabled on the device. Minimum OS version: 10.0.14393	MDM controls	65535	• Disabled • Enabled • Not configured

Name	Description	Activation types	Default	Possible values
Default app access to account information	Specify whether apps can access account information by default. If you select "User controlled," the user can choose whether to allow access. If you select "Allow," apps can access account information. If you select "Disallow," apps can't access account information. Minimum OS version: 10.0.14393	MDM controls	User controlled	• User controlled • Allow • Disallow
Apps allowed access to account information	Specify the list of apps that are always allowed to access account information. Specify apps using package family names, separated by semi-colons (;). Apps specified in this rule ignore the setting in the "Default app access to account information" rule. Minimum OS version: 10.0.14393	MDM controls		
Apps denied access to account information	Specify the list of apps that are never allowed to access account information. Specify apps using package family names, separated by semi-colons (;). Apps specified in this rule ignore the setting in the "Default app access to account information" rule. Minimum OS version: 10.0.14393	MDM controls		

Name	Description	Activation types	Default	Possible values
App access to account information controlled by user	Specify the list of apps that users can choose to allow or disallow access to account information. Specify apps using package family names, separated by semi-colons (;). Apps specified in this rule ignore the setting in the "Default app access to account information" rule. Minimum OS version: 10.0.14393	MDM controls		
Default app access to calendar	Specify whether apps can access the calendar by default. If you select "User controlled," the user can choose whether to allow access. If you select "Allow," apps can access the calendar. If you select "Disallow," apps can't access the calendar. Minimum OS version: 10.0.14393	MDM controls	User controlled	• User controlled • Allow • Disallow
Apps allowed access to calendar	Specify the list of apps that are always allowed to access the calendar. Specify apps using package family names, separated by semi-colons (;). Apps specified in this rule ignore the setting in the "Default app access to calendar" rule. Minimum OS version: 10.0.14393	MDM controls		
Apps denied access to calendar	Specify the list of apps that are never allowed to access the calendar. Specify apps using package family names, separated by semi-colons (;). Apps specified in this rule ignore the setting in the "Default app access to calendar" rule. Minimum OS version: 10.0.14393	MDM controls		

Name	Description	Activation types	Default	Possible values
App access to calendar controlled by user	Specify the list of apps that users can choose to allow or disallow access to the calendar. Specify apps using package family names, separated by semi-colons (;). Apps specified in this rule ignore the setting in the "Default app access to calendar" rule. Minimum OS version: 10.0.14393	MDM controls		
Default app access to call history	Specify whether apps can access the call history by default. If you select "User controlled," the user can choose whether to allow access. If you select "Allow," apps can access the call history. If you select "Disallow," apps can't access the call history. Minimum OS version: 10.0.14393	MDM controls	User controlled	• User controlled • Allow • Disallow
Apps allowed access to call history	Specify the list of apps that are always allowed to access the call history. Specify apps using package family names, separated by semi-colons (;). Apps specified in this rule ignore the setting in the "Default app access to call history" rule. Minimum OS version: 10.0.14393	MDM controls		
Apps denied access to call history	Specify the list of apps that are never allowed to access the call history. Specify apps using package family names, separated by semi-colons (;). Apps specified in this rule ignore the setting in the "Default app access to call history" rule. Minimum OS version: 10.0.14393	MDM controls		

Name	Description	Activation types	Default	Possible values
App access to call history controlled by user	Specify the list of apps that users can choose to allow or disallow access to the call history. Specify apps using package family names, separated by semi-colons (;). Apps specified in this rule ignore the setting in the "Default app access to call history" rule. Minimum OS version: 10.0.14393	MDM controls		
Default app access to camera	Specify whether apps can access the camera by default. If you select "User controlled," the user can choose whether to allow access. If you select "Allow," apps can access the camera. If you select "Disallow," apps can't access the camera. Minimum OS version: 10.0.14393	MDM controls	User controlled	• User controlled • Allow • Disallow
Apps allowed access to camera	Specify the list of apps that are always allowed to access the camera. Specify apps using package family names, separated by semi-colons (;). Apps specified in this rule ignore the setting in the "Default app access to camera" rule. Minimum OS version: 10.0.14393	MDM controls		
Apps denied access to camera	Specify the list of apps that are never allowed to access the camera. Specify apps using package family names, separated by semi-colons (;). Apps specified in this rule ignore the setting in the "Default app access to camera" rule. Minimum OS version: 10.0.14393	MDM controls		

Name	Description	Activation types	Default	Possible values
App access to camera controlled by user	Specify the list of apps that users can choose to allow or disallow access to the camera. Specify apps using package family names, separated by semi-colons (;). Apps specified in this rule ignore the setting in the "Default app access to camera" rule. Minimum OS version: 10.0.14393	MDM controls		
Default app access to contacts	Specify whether apps can access the contacts by default. If you select "User controlled," the user can choose whether to allow access. If you select "Allow," apps can access the contacts. If you select "Disallow," apps can't access the contacts. Minimum OS version: 10.0.14393	MDM controls	User controlled	• User controlled • Allow • Disallow
Apps allowed access to contacts	Specify the list of apps that are always allowed to access the contacts. Specify apps using package family names, separated by semi-colons (;). Apps specified in this rule ignore the setting in the "Default app access to contacts" rule. Minimum OS version: 10.0.14393	MDM controls		
Apps denied access to contacts	Specify the list of apps that are never allowed to access the contacts. Specify apps using package family names, separated by semi-colons (;). Apps specified in this rule ignore the setting in the "Default app access to contacts" rule. Minimum OS version: 10.0.14393	MDM controls		

Name	Description	Activation types	Default	Possible values
App access to contacts controlled by user	Specify the list of apps that users can choose to allow or disallow access to the contacts. Specify apps using package family names, separated by semi-colons (;). Apps specified in this rule ignore the setting in the "Default app access to contacts" rule. Minimum OS version: 10.0.14393	MDM controls		
Default app access to email	Specify whether apps can access email on the device by default. If you select "User controlled," the user can choose whether to allow access. If you select "Allow," apps can access email. If you select "Disallow," apps can't access email. Minimum OS version: 10.0.14393	MDM controls	User controlled	• User controlled • Allow • Disallow
Apps allowed access to email	Specify the list of apps that are always allowed to access email. Specify apps using package family names, separated by semi-colons (;). Apps specified in this rule ignore the setting in the "Default app access to email" rule. Minimum OS version: 10.0.14393	MDM controls		
Apps denied access to email	Specify the list of apps that are never allowed to access email. Specify apps using package family names, separated by semi-colons (;). Apps specified in this rule ignore the setting in the "Default app access to email" rule. Minimum OS version: 10.0.14393	MDM controls		

Name	Description	Activation types	Default	Possible values
App access to email controlled by user	Specify the list of apps that users can choose to allow or disallow access to email. Specify apps using package family names, separated by semi-colons (;). Apps specified in this rule ignore the setting in the "Default app access to email" rule. Minimum OS version: 10.0.14393	MDM controls		
Default app access to location services	Specify whether apps can access location services by default. If you select "User controlled," the user can choose whether to allow access. If you select "Allow," apps can access location services. If you select "Disallow," apps can't access location services. Minimum OS version: 10.0.14393	MDM controls	User controlled	• User controlled • Allow • Disallow
Apps allowed access to location services	Specify the list of apps that are always allowed to access location services. Specify apps using package family names, separated by semi-colons (;). Apps specified in this rule ignore the setting in the "Default app access to location services" rule. Minimum OS version: 10.0.14393	MDM controls		
Apps denied access to location services	Specify the list of apps that are never allowed to access location services. Specify apps using package family names, separated by semi-colons (;). Apps specified in this rule ignore the setting in the "Default app access to location services" rule. Minimum OS version: 10.0.14393	MDM controls		

Name	Description	Activation types	Default	Possible values
App access to location services controlled by user	Specify the list of apps that users can choose to allow or disallow access to location services. Specify apps using package family names, separated by semi-colons (;). Apps specified in this rule ignore the setting in the "Default app access to location services" rule. Minimum OS version: 10.0.14393	MDM controls		
Default app access to messaging	Specify whether apps can access SMS and MMS messaging by default. If you select "User controlled," the user can choose whether to allow access. If you select "Allow," apps can access messaging. If you select "Disallow," apps can't access messaging. Minimum OS version: 10.0.14393	MDM controls	User controlled	• User controlled • Allow • Disallow
Apps allowed access to messaging	Specify the list of apps that are always allowed to access SMS and MMS messaging. Specify apps using package family names, separated by semi-colons (;). Apps specified in this rule ignore the setting in the "Default app access to messaging" rule. Minimum OS version: 10.0.14393	MDM controls		

Name	Description	Activation types	Default	Possible values
Apps denied access to messaging	Specify the list of apps that are never allowed to access SMS and MMS messaging. Specify apps using package family names, separated by semi-colons (;). Apps specified in this rule ignore the setting in the "Default app access to messaging" rule. Minimum OS version: 10.0.14393	MDM controls		
App access to messaging controlled by user	Specify the list of apps that users can choose to allow or disallow access to SMS and MMS messaging. Specify apps using package family names, separated by semi-colons (;). Apps specified in this rule ignore the setting in the "Default app access to messaging" rule. Minimum OS version: 10.0.14393	MDM controls		
Default app access to microphone	Specify whether apps can access the microphone by default. If you select "User controlled," the user can choose whether to allow access. If you select "Allow," apps can access the microphone. If you select "Disallow," apps can't access the microphone. Minimum OS version: 10.0.14393	MDM controls	User controlled	• User controlled • Allow • Disallow
Apps allowed access to microphone	Specify the list of apps that are always allowed to access the microphone. Specify apps using package family names, separated by semi-colons (;). Apps specified in this rule ignore the setting in the "Default app access to microphone" rule. Minimum OS version: 10.0.14393	MDM controls		

Name	Description	Activation types	Default	Possible values
Apps denied access to microphone	Specify the list of apps that are never allowed to access the microphone. Specify apps using package family names, separated by semi-colons (;). Apps specified in this rule ignore the setting in the "Default app access to microphone" rule. Minimum OS version: 10.0.14393	MDM controls		
App access to microphone controlled by user	Specify the list of apps that users can choose to allow or disallow access to the microphone. Specify apps using package family names, separated by semi-colons (;). Apps specified in this rule ignore the setting in the "Default app access to microphone" rule. Minimum OS version: 10.0.14393	MDM controls		
Default app access to motion data	Specify whether apps can access motion data by default. If you select "User controlled," the user can choose whether to allow access. If you select "Allow," apps can access motion data. If you select "Disallow," apps can't access motion data. Minimum OS version: 10.0.14393	MDM controls	User controlled	• User controlled • Allow • Disallow
Apps allowed access to motion data	Specify the list of apps that are always allowed to access motion data. Specify apps using package family names, separated by semi-colons (;). Apps specified in this rule ignore the setting in the "Default app access to motion data" rule. Minimum OS version: 10.0.14393	MDM controls		

Name	Description	Activation types	Default	Possible values
Apps denied access to motion data	Specify the list of apps that are never allowed to access motion data. Specify apps using package family names, separated by semi-colons (;). Apps specified in this rule ignore the setting in the "Default app access to motion data" rule. Minimum OS version: 10.0.14393	MDM controls		
App access to motion data controlled by user	Specify the list of apps that users can choose to allow or disallow access to motion data. Specify apps using package family names, separated by semi-colons (;). Apps specified in this rule ignore the setting in the "Default app access to motion data" rule. Minimum OS version: 10.0.14393	MDM controls		
Default app access to phone	Specify whether apps can access the phone by default. If you select "User controlled," the user can choose whether to allow access. If you select "Allow," apps can access the phone. If you select "Disallow," apps can't access the phone. Minimum OS version: 10.0.14393	MDM controls	User controlled	• User controlled • Allow • Disallow
Apps allowed access to phone	Specify the list of apps that are always allowed to access the phone. Specify apps using package family names, separated by semi-colons (;). Apps specified in this rule ignore the setting in the "Default app access to phone" rule. Minimum OS version: 10.0.14393	MDM controls		

Name	Description	Activation types	Default	Possible values
Apps denied access to phone	Specify the list of apps that are never allowed to access the phone. Specify apps using package family names, separated by semi-colons (;). Apps specified in this rule ignore the setting in the "Default app access to phone" rule. Minimum OS version: 10.0.14393	MDM controls		
App access to phone controlled by user	Specify the list of apps that users can choose to allow or disallow access to the phone. Specify apps using package family names, separated by semi-colons (;). Apps specified in this rule ignore the setting in the "Default app access to phone" rule. Minimum OS version: 10.0.14393	MDM controls		
Default app access to radios	Specify whether apps can access device radios by default. If you select "User controlled," the user can choose whether to allow access. If you select "Allow," apps can access the radios. If you select "Disallow," apps can't access the radios. Minimum OS version: 10.0.14393	MDM controls	User controlled	• User controlled • Allow • Disallow
Apps allowed access to radios	Specify the list of apps that are always allowed to access device radios. Specify apps using package family names, separated by semi-colons (;). Apps specified in this rule ignore the setting in the "Default app access to radios" rule. Minimum OS version: 10.0.14393	MDM controls		

Name	Description	Activation types	Default	Possible values
Apps denied access to radios	Specify the list of apps that are never allowed to access device radios. Specify apps using package family names, separated by semi-colons (;). Apps specified in this rule ignore the setting in the "Default app access to radios" rule. Minimum OS version: 10.0.14393	MDM controls		
App access to radios controlled by user	Specify the list of apps that users can choose to allow or disallow access to device radios. Specify apps using package family names, separated by semi-colons (;). Apps specified in this rule ignore the setting in the "Default app access to radios" rule. Minimum OS version: 10.0.14393	MDM controls		
Default app access to trusted devices	Specify whether apps can access the list of trusted devices by default. If you select "User controlled," the user can choose whether to allow access. If you select "Allow," apps can access the trusted devices. If you select "Disallow," apps can't access trusted devices. Minimum OS version: 10.0.14393	MDM controls	User controlled	• User controlled • Allow • Disallow
Apps allowed access to trusted devices	Specify the list of apps that are always allowed to access the list of trusted devices. Specify apps using package family names, separated by semi-colons (;). Apps specified in this rule ignore the setting in the "Default app access to trusted devices" rule. Minimum OS version: 10.0.14393	MDM controls		

Name	Description	Activation types	Default	Possible values
Apps denied access to trusted devices	Specify the list of apps that are never allowed to access the list of trusted devices. Specify apps using package family names, separated by semi-colons (;). Apps specified in this rule ignore the setting in the "Default app access to trusted devices" rule. Minimum OS version: 10.0.14393	MDM controls		
App access to trusted devices controlled by user	Specify the list of apps that users can choose to allow or disallow access to the list of trusted devices. Specify apps using package family names, separated by semi-colons (;). Apps specified in this rule ignore the setting in the "Default app access to trusted devices" rule. Minimum OS version: 10.0.14393	MDM controls		
Default app synchronization	Specify whether apps can synchronize with the device by default. If you select "User controlled," the user can choose whether to allow synchronization. If you select "Allow," apps can synchronize with the device. If you select "Disallow," apps can't synchronize with the device. Minimum OS version: 10.0.14393	MDM controls	User controlled	• User controlled • Allow • Disallow
Apps allowed to synchronize with the device	Specify the list of apps that are always allowed to synchronize with the device. Specify apps using package family names, separated by semi-colons (;). Apps specified in this rule ignore the setting in the "Default app synchronization" rule. Minimum OS version: 10.0.14393	MDM controls		

Name	Description	Activation types	Default	Possible values
Apps not allowed to synchronize with the device	Specify the list of apps that are never allowed to synchronize with the device. Specify apps using package family names, separated by semi-colons (;). Apps specified in this rule ignore the setting in the "Default app synchronization" rule. Minimum OS version: 10.0.14393	MDM controls		
App synchronization controlled by user	Specify the list of apps that users can choose to allow to synchronize with the device. Specify apps using package family names, separated by semi-colons (;). Apps specified in this rule ignore the setting in the "Default app synchronization" rule. Minimum OS version: 10.0.14393	MDM controls		
Default app access to notifications	Specify whether apps can access device notifications by default. If you select "User controlled," the user can choose whether to allow access. If you select "Allow," apps can access notifications. If you select "Disallow," apps can't access notifications. Minimum OS version: 10.0.14393	MDM controls	User controlled	• User controlled • Allow • Disallow
Apps allowed access to notifications	Specify the list of apps that are always allowed to access notifications. Specify apps using package family names, separated by semi-colons (;). Apps specified in this rule ignore the setting in the "Default app access to notifications" rule. Minimum OS version: 10.0.14393	MDM controls		

Name	Description	Activation types	Default	Possible values
Apps not allowed access to notifications	Specify the list of apps that are never allowed to access notifications. Specify apps using package family names, separated by semi-colons (;). Apps specified in this rule ignore the setting in the "Default app access to notifications" rule. Minimum OS version: 10.0.14393	MDM controls		
App notification access controlled by user	Specify the list of apps that users can choose to allow to access notifications. Specify apps using package family names, separated by semi-colons (;). Apps specified in this rule ignore the setting in the "Default app access to notifications" rule. Minimum OS version: 10.0.14393	MDM controls		
Default app access to diagnostic information	Specify whether apps can access device diagnostic information about other apps by default. If you select "User controlled," the user can choose whether to allow access. If you select "Allow," apps can access diagnostic information. If you select "Disallow," apps can't access diagnostic information. Minimum OS version: 10.0.15063	MDM controls	User controlled	• User controlled • Allow • Disallow

Name	Description	Activation types	Default	Possible values
Apps allowed access to diagnostic information	Specify the list of apps that are always allowed to access device diagnostic information. Specify apps using package family names, separated by semi-colons (;). Apps specified in this rule ignore the setting in the "Default app access to diagnostic information" rule. Minimum OS version: 10.0.15063	MDM controls		
Apps not allowed access to diagnostic information	Specify the list of apps that are never allowed to access device diagnostic information. Specify apps using package family names, separated by semi-colons (;). Apps specified in this rule ignore the setting in the "Default app access to diagnostic information" rule. Minimum OS version: 10.0.15063	MDM controls		
App access to diagnostic information controlled by user	Specify the list of apps that users can choose to allow to access device diagnostic information. Specify apps using package family names, separated by semi-colons (;). Apps specified in this rule ignore the setting in the "Default app access to diagnostic information" rule. Minimum OS version: 10.0.15063	MDM controls		
Default apps can run in background	Specify whether apps can run in background by default. If you select "User controlled," the user can choose whether to allow access. If you select "Allow," apps can run in background. If you select "Disallow," apps can't run in background. Minimum OS version: 10.0.15063	MDM controls	User controlled	• User controlled • Allow • Disallow

Name	Description	Activation types	Default	Possible values
Apps allowed to run in background	Specify the list of apps that are always allowed to run in background. Specify apps using package family names, separated by semi-colons (;). Apps specified in this rule ignore the setting in the "Default apps can run in background" rule. Minimum OS version: 10.0.15063	MDM controls		
Apps not allowed to run in background	Specify the list of apps that are never allowed to run in background. Specify apps using package family names, separated by semi-colons (;). Apps specified in this rule ignore the setting in the "Default apps can run in background" rule. Minimum OS version: 10.0.15063	MDM controls		
App ability to run in background controlled by user	Specify the list of apps that users can choose to allow to run in background. Specify apps using package family names, separated by semi-colons (;). Apps specified in this rule ignore the setting in the "Default apps can run in background" rule. Minimum OS version: 10.0.15063	MDM controls		
MDM wins over group policies	When enabled MDM policy will be used whenever both the MDM policy and its equivalent group policy are set on the device. Minimum OS version: 10.0.17763	MDM controls	No	• No • Yes

Name	Description	Activation types	Default	Possible values
BitLocker encryption method for desktop	Specify the BitLocker Drive Encryption method and cipher strength for desktop. Minimum OS version: 10.0.17763	MDM controls	AES-CBC 128-bit	• AES-CBC 128-bit • AES-CBC 256-bit • XTS-AES 128-bit • XTS-AES 256-bit
Allow storage card encryption prompts on the device	Specify whether the device prompts the user to encrypt the storage card. If this rule is not selected, encryption is not disabled. Minimum OS version: 10.0.17763	MDM controls	No	• No • Yes
Allow BitLocker Device Encryption to enable encryption on the device	Specify whether BitLocker Device Encryption can enable encryption on the device. If this rule is not selected, encryption is not disabled but the user is not prompted to enable it. Minimum OS version: 10.0.17763	MDM controls	No	• No • Yes
Set default encryption methods for each drive type	Specify whether the default algorithm and cipher strength used by BitLocker Drive Encryption can be configured separately for different drive types. Minimum OS version: 10.0.17763	MDM controls	Not selected	
Encryption method for operating system drives	Specify the encryption method for operating system drives. Depends on: Set default encryption methods for each drive type Minimum OS version: 10.0.17763	MDM controls	AES-CBC 128-bit	• AES-CBC 128-bit • AES-CBC 256-bit • XTS-AES 128-bit • XTS-AES 256-bit

Name	Description	Activation types	Default	Possible values
Encryption method for fixed data drives	Specify the encryption method for fixed data drives. Depends on: Set default encryption methods for each drive type Minimum OS version: 10.0.17763	MDM controls	AES-CBC 128-bit	• AES-CBC 128-bit • AES-CBC 256-bit • XTS-AES 128-bit • XTS-AES 256-bit
Encryption method for removable data drives	Specify the encryption method for removable data drives. Depends on: Set default encryption methods for each drive type Minimum OS version: 10.0.17763	MDM controls	AES-CBC 128-bit	• AES-CBC 128-bit • AES-CBC 256-bit • XTS-AES 128-bit • XTS-AES 256-bit
Require additional authentication at startup	Specify whether BitLocker requires additional authentication each time the device starts. This setting is applied when BitLocker is turned on. Minimum OS version: 10.0.17763	MDM controls	Not selected	
Allow BitLocker without a compatible TPM	Specify whether BitLocker can be started without a TPM chip. If this rule is selected, BitLocker can be started with a password or a startup key on a USB flash drive. Depends on: Require additional authentication at startup Minimum OS version: 10.0.17763	MDM controls	Not selected	
Require TPM startup key	Specify whether a TPM startup key is optional, required, or disallowed. Depends on: Require additional authentication at startup Minimum OS version: 10.0.17763	MDM controls	Optional	• Optional • Required • Disallowed

Name	Description	Activation types	Default	Possible values
Require TPM startup PIN	Specify whether a TPM startup PIN is optional, required, or disallowed. Depends on: Require additional authentication at startup Minimum OS version: 10.0.17763	MDM controls	Optional	• Optional • Required • Disallowed
Require TPM startup key and PIN	Specify whether both a TPM startup key and PIN are optional, required, or disallowed. Depends on: Require additional authentication at startup Minimum OS version: 10.0.17763	MDM controls	Optional	• Optional • Required • Disallowed
Require TPM startup	Specify whether TPM startup is optional, required, or disallowed. Depends on: Require additional authentication at startup Minimum OS version: 10.0.17763	MDM controls	Optional	• Optional • Required • Disallowed
Require minimum PIN length for startup	Specify whether BitLocker has a minimum startup PIN length. Minimum OS version: 10.0.17763	MDM controls	Not selected	
Minimum PIN length	Specify the minimum number of digits for the startup PIN. Depends on: Require minimum PIN length for startup Minimum OS version: 10.0.17763	MDM controls	6 digits	Minimum value: 6 digits Maximum value: 20 digits
Pre-boot recovery message and URL	Specify whether you can customize the BitLocker pre-boot recovery message and URL that are displayed on the pre-boot key recovery screen when the OS drive is locked. Minimum OS version: 10.0.17763	MDM controls	Not selected	

Name	Description	Activation types	Default	Possible values
Pre-boot recovery screen	Specify whether the BitLocker pre-boot recover screen is empty, displays a default message and URL, displays a custom message, or displays a custom URL. Depends on: Pre-boot recovery message and URL Minimum OS version: 10.0.17763	MDM controls	Empty	• Empty • Use default recovery message and URL • Custom recovery message • Custom recovery URL
Custom recovery message	If you selected "Custom recovery message" in the "Pre-boot recovery screen" rule, specify the custom message. Depends on: Pre-boot recovery message and URL Minimum OS version: 10.0.17763	MDM controls		Minimum value: 1 character Maximum value: 900 characters
Custom recovery URL	If you selected "Custom recovery URL" in the "Pre-boot recovery screen" rule, specify the custom URL. Depends on: Pre-boot recovery message and URL Minimum OS version: 10.0.17763	MDM controls		Minimum value: 1 character Maximum value: 500 characters
BitLocker OS drive recovery options	Specify whether you can customize how BitLocker-protected operating system drives are recovered in the absence of the required startup key information. This setting is applied when you turn on BitLocker. Minimum OS version: 10.0.17763	MDM controls	Not selected	

Name	Description	Activation types	Default	Possible values
Allow certificate-based data recovery agent for OS drives	Specify whether a data recovery agent can be used with BitLocker-protected operating system drives. Depends on: BitLocker OS drive recovery options Minimum OS version: 10.0.17763	MDM controls	Not selected	
Allow recovery password generation for OS drives	Specify whether the user can create and store a BitLocker recovery password for OS drives. Depends on: BitLocker OS drive recovery options Minimum OS version: 10.0.17763	MDM controls	Allowed	• Allowed • Required • Disallowed
Allow recovery key generation for OS drives	Specify whether the user can create and store a BitLocker recovery key for OS drives. Depends on: BitLocker OS drive recovery options Minimum OS version: 10.0.17763	MDM controls	Allowed	• Allowed • Required • Disallowed
Exclude recovery options from the BitLocker setup wizard for OS drives	Specify whether recovery options are hidden from the user when they turn on BitLocker on an OS drive. Depends on: BitLocker OS drive recovery options Minimum OS version: 10.0.17763	MDM controls	Not selected	
Allow saving BitLocker recovery information for OS drives to Active Directory Domain Services	Specify whether BitLocker recovery information for OS drives can be saved to Active Directory Domain Services. Depends on: BitLocker OS drive recovery options Minimum OS version: 10.0.17763	MDM controls	Not selected	

Name	Description	Activation types	Default	Possible values
Stored BitLocker recovery information for OS drives	Specify whether Active Directory Domain Services stores only recovery passwords, or both recovery passwords and key packages for OS drives. Depends on: BitLocker OS drive recovery options Minimum OS version: 10.0.17763	MDM controls	Store recovery passwords only	• Store recovery passwords only • Store recovery passwords and key packages
Require Active Directory backup for recovery information for OS drives	Specify whether BitLocker recovery information saved to Active Directory Domain Services for OS drives must be backed up. Depends on: BitLocker OS drive recovery options Minimum OS version: 10.0.17763	MDM controls	Not selected	
BitLocker fixed drive recovery options	Specify whether you can customize how BitLocker-protected fixed drives are recovered in the absence of the required startup key information. This setting is applied when you turn on BitLocker. Minimum OS version: 10.0.17763	MDM controls	Not selected	
Allow certificate-based data recovery agent for fixed drives	Specify whether a data recovery agent can be used with BitLocker-protected fixed drives. Depends on: BitLocker fixed drive recovery options Minimum OS version: 10.0.17763	MDM controls	Not selected	

Name	Description	Activation types	Default	Possible values
Allow recovery password generation for fixed drives	Specify whether the user can create and store a BitLocker recovery password for fixed drives. Depends on: BitLocker fixed drive recovery options Minimum OS version: 10.0.17763	MDM controls	Allowed	• Allowed • Required • Disallowed
Allow recovery key generation for fixed drives	Specify whether the user can create and store a BitLocker recovery key for fixed drives. Depends on: BitLocker fixed drive recovery options Minimum OS version: 10.0.17763	MDM controls	Allowed	• Allowed • Required • Disallowed
Exclude recovery options from the BitLocker setup wizard for fixed drives	Specify whether recovery options are hidden from the user when they turn on BitLocker on a fixed drive. Depends on: BitLocker fixed drive recovery options Minimum OS version: 10.0.17763	MDM controls	Not selected	
Allow saving BitLocker recovery information for fixed drives to Active Directory Domain Services	Allow BitLocker recovery information for fixed drives to be saved to Active Directory Domain Services. Depends on: BitLocker fixed drive recovery options Minimum OS version: 10.0.17763	MDM controls	Not selected	
Stored BitLocker recovery information for fixed drives	Specify whether Active Directory Domain Services stores only recovery passwords, or both recovery passwords and key packages for fixed drives. Depends on: BitLocker fixed drive recovery options Minimum OS version: 10.0.17763	MDM controls	Store recovery passwords only	• Store recovery passwords only • Store recovery passwords and key packages

Name	Description	Activation types	Default	Possible values
Require Active Directory backup for recovery information for fixed drives	Specify whether BitLocker recovery information saved to Active Directory Domain Services for fixed drives must be backed up. Depends on: BitLocker fixed drive recovery options Minimum OS version: 10.0.17763	MDM controls	Not selected	
Require BitLocker protection for fixed data drives	Specify whether BitLocker protection is required to allow write access to fixed data drives. If this rule is selected, all fixed data drives that are not BitLocker-protected will be mounted as read-only. Minimum OS version: 10.0.17763	MDM controls	Not selected	
Require BitLocker protection for removable data drives	Specify whether BitLocker protection is required to allow write access to removeable data drives. If this rule is selected, all removeable data drives that are not BitLocker-protected will be mounted as read-only. Minimum OS version: 10.0.17763	MDM controls	Not selected	
Allow write access to devices configured in another organization	Specify whether removable drives that don't match the device's identification fields can have write access. If this rule is selected, only drives with identification fields matching the computer's identification fields will be given write access. Depends on: Require BitLocker protection for removable data drives Minimum OS version: 10.0.17763	MDM controls	Not selected	

Name	Description	Activation types	Default	Possible values
Allow recovery key location prompt	Specify whether the user is prompted to choose where to back up the OS drive's recovery key. When this rule is not selected, the OS drive's recovery key backs up to the user's Microsoft Entra ID account. Minimum OS version: 10.0.17763	MDM controls	Yes	• No • Yes
Enable encryption for standard users	Specify whether encryption is enabled on all fixed drives, even if a current logged in user is a standard user. This setting is only supported in Microsoft Entra ID accounts. Minimum OS version: 10.0.17763	MDM controls	No	• No • Yes

Windows: Company owned devices only rules

Name	Description	Activation types	Default	Possible values
Allow user to reset device	Specify whether a user can reset a device to factory settings using the control panel and hardware key combination. This feature may cause the device to fail or lose connectivity and require that the device be serviced at a Nokia-authorized repair center to reset to factory settings. Microsoft is not liable for any damage to the device or any loss of productivity that results from use of this feature. Microsoft requires that software vendors provide disclaimers to users when their products expose this feature and capabilities. This rule does not apply to Windows 10 computers and tablets. This rule applies only to Windows 10 Mobile devices. Minimum OS version: 10.0	MDM controls	Allow	• Disallow • Allow
Allow manual MDM unenrollment	Specify whether a user can delete the workplace account using the workplace control panel. The MDM server can always remotely delete the account. This feature may cause the device to fail or lose connectivity and require that the device be serviced at a Nokia-authorized repair center to reset to factory settings. Microsoft is not liable for any damage to the device or any loss of productivity that results from use of this feature. Microsoft requires that software vendors provide disclaimers to users when their products expose this feature and capabilities. Minimum OS version: 10.0	MDM controls	Allow	• Disallow • Allow

Legal notice

© 2025 BlackBerry Limited. Trademarks, including but not limited to BLACKBERRY, EMBLEM Design, ATHOC, and SECUSMART are the trademarks or registered trademarks of BlackBerry Limited, its subsidiaries and/or affiliates, used under license, and the exclusive rights to such trademarks are expressly reserved. All other trademarks are the property of their respective owners.

Patents, as applicable, identified at: www.blackberry.com/patents.

This documentation including all documentation incorporated by reference herein such as documentation provided or made available on the BlackBerry website provided or made accessible "AS IS" and "AS AVAILABLE" and without condition, endorsement, guarantee, representation, or warranty of any kind by BlackBerry Limited and its affiliated companies ("BlackBerry") and BlackBerry assumes no responsibility for any typographical, technical, or other inaccuracies, errors, or omissions in this documentation. In order to protect BlackBerry proprietary and confidential information and/or trade secrets, this documentation may describe some aspects of BlackBerry technology in generalized terms. BlackBerry reserves the right to periodically change information that is contained in this documentation; however, BlackBerry makes no commitment to provide any such changes, updates, enhancements, or other additions to this documentation to you in a timely manner or at all.

This documentation might contain references to third-party sources of information, hardware or software, products or services including components and content such as content protected by copyright and/or third-party websites (collectively the "Third Party Products and Services"). BlackBerry does not control, and is not responsible for, any Third Party Products and Services including, without limitation the content, accuracy, copyright compliance, compatibility, performance, trustworthiness, legality, decency, links, or any other aspect of Third Party Products and Services. The inclusion of a reference to Third Party Products and Services in this documentation does not imply endorsement by BlackBerry of the Third Party Products and Services or the third party in any way.

EXCEPT TO THE EXTENT SPECIFICALLY PROHIBITED BY APPLICABLE LAW IN YOUR JURISDICTION, ALL CONDITIONS, ENDORSEMENTS, GUARANTEES, REPRESENTATIONS, OR WARRANTIES OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, ANY CONDITIONS, ENDORSEMENTS, GUARANTEES, REPRESENTATIONS OR WARRANTIES OF DURABILITY, FITNESS FOR A PARTICULAR PURPOSE OR USE, MERCHANTABILITY, MERCHANTABLE QUALITY, NON-INFRINGEMENT, SATISFACTORY QUALITY, OR TITLE, OR ARISING FROM A STATUTE OR CUSTOM OR A COURSE OF DEALING OR USAGE OF TRADE, OR RELATED TO THE DOCUMENTATION OR ITS USE, OR PERFORMANCE OR NON-PERFORMANCE OF ANY SOFTWARE, HARDWARE, SERVICE, OR ANY THIRD PARTY PRODUCTS AND SERVICES REFERENCED HEREIN, ARE HEREBY EXCLUDED. YOU MAY ALSO HAVE OTHER RIGHTS THAT VARY BY STATE OR PROVINCE. SOME JURISDICTIONS MAY NOT ALLOW THE EXCLUSION OR LIMITATION OF IMPLIED WARRANTIES AND CONDITIONS. TO THE EXTENT PERMITTED BY LAW, ANY IMPLIED WARRANTIES OR CONDITIONS RELATING TO THE DOCUMENTATION TO THE EXTENT THEY CANNOT BE EXCLUDED AS SET OUT ABOVE, BUT CAN BE LIMITED, ARE HEREBY LIMITED TO NINETY (90) DAYS FROM THE DATE YOU FIRST ACQUIRED THE DOCUMENTATION OR THE ITEM THAT IS THE SUBJECT OF THE CLAIM.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW IN YOUR JURISDICTION, IN NO EVENT SHALL BLACKBERRY BE LIABLE FOR ANY TYPE OF DAMAGES RELATED TO THIS DOCUMENTATION OR ITS USE, OR PERFORMANCE OR NON-PERFORMANCE OF ANY SOFTWARE, HARDWARE, SERVICE, OR ANY THIRD PARTY PRODUCTS AND SERVICES REFERENCED HEREIN INCLUDING WITHOUT LIMITATION ANY OF THE FOLLOWING DAMAGES: DIRECT, CONSEQUENTIAL, EXEMPLARY, INCIDENTAL, INDIRECT, SPECIAL, PUNITIVE, OR AGGRAVATED DAMAGES, DAMAGES FOR LOSS OF PROFITS OR REVENUES, FAILURE TO REALIZE ANY EXPECTED SAVINGS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION, LOSS OF BUSINESS OPPORTUNITY, OR CORRUPTION OR LOSS OF DATA, FAILURES TO TRANSMIT OR RECEIVE ANY DATA, PROBLEMS ASSOCIATED WITH ANY APPLICATIONS USED IN CONJUNCTION WITH BLACKBERRY PRODUCTS OR SERVICES, DOWNTIME COSTS, LOSS OF THE USE OF BLACKBERRY PRODUCTS OR SERVICES OR ANY PORTION THEREOF OR OF ANY AIRTIME SERVICES, COST OF SUBSTITUTE GOODS, COSTS OF COVER, FACILITIES OR SERVICES, COST OF CAPITAL, OR OTHER SIMILAR PECUNIARY LOSSES, WHETHER OR NOT SUCH DAMAGES

WERE FORESEEN OR UNFORESEEN, AND EVEN IF BLACKBERRY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW IN YOUR JURISDICTION, BLACKBERRY SHALL HAVE NO OTHER OBLIGATION, DUTY, OR LIABILITY WHATSOEVER IN CONTRACT, TORT, OR OTHERWISE TO YOU INCLUDING ANY LIABILITY FOR NEGLIGENCE OR STRICT LIABILITY.

THE LIMITATIONS, EXCLUSIONS, AND DISCLAIMERS HEREIN SHALL APPLY: (A) IRRESPECTIVE OF THE NATURE OF THE CAUSE OF ACTION, DEMAND, OR ACTION BY YOU INCLUDING BUT NOT LIMITED TO BREACH OF CONTRACT, NEGLIGENCE, TORT, STRICT LIABILITY OR ANY OTHER LEGAL THEORY AND SHALL SURVIVE A FUNDAMENTAL BREACH OR BREACHES OR THE FAILURE OF THE ESSENTIAL PURPOSE OF THIS AGREEMENT OR OF ANY REMEDY CONTAINED HEREIN; AND (B) TO BLACKBERRY AND ITS AFFILIATED COMPANIES, THEIR SUCCESSORS, ASSIGNS, AGENTS, SUPPLIERS (INCLUDING AIRTIME SERVICE PROVIDERS), AUTHORIZED BLACKBERRY DISTRIBUTORS (ALSO INCLUDING AIRTIME SERVICE PROVIDERS) AND THEIR RESPECTIVE DIRECTORS, EMPLOYEES, AND INDEPENDENT CONTRACTORS.

IN ADDITION TO THE LIMITATIONS AND EXCLUSIONS SET OUT ABOVE, IN NO EVENT SHALL ANY DIRECTOR, EMPLOYEE, AGENT, DISTRIBUTOR, SUPPLIER, INDEPENDENT CONTRACTOR OF BLACKBERRY OR ANY AFFILIATES OF BLACKBERRY HAVE ANY LIABILITY ARISING FROM OR RELATED TO THE DOCUMENTATION.

Prior to subscribing for, installing, or using any Third Party Products and Services, it is your responsibility to ensure that your airtime service provider has agreed to support all of their features. Some airtime service providers might not offer Internet browsing functionality with a subscription to the BlackBerry® Internet Service. Check with your service provider for availability, roaming arrangements, service plans and features. Installation or use of Third Party Products and Services with BlackBerry's products and services may require one or more patent, trademark, copyright, or other licenses in order to avoid infringement or violation of third party rights. You are solely responsible for determining whether to use Third Party Products and Services and if any third party licenses are required to do so. If required you are responsible for acquiring them. You should not install or use Third Party Products and Services until all necessary licenses have been acquired. Any Third Party Products and Services that are provided with BlackBerry's products and services are provided as a convenience to you and are provided "AS IS" with no express or implied conditions, endorsements, guarantees, representations, or warranties of any kind by BlackBerry and BlackBerry assumes no liability whatsoever, in relation thereto. Your use of Third Party Products and Services shall be governed by and subject to you agreeing to the terms of separate licenses and other agreements applicable thereto with third parties, except to the extent expressly covered by a license or other agreement with BlackBerry.

The terms of use of any BlackBerry product or service are set out in a separate license or other agreement with BlackBerry applicable thereto. NOTHING IN THIS DOCUMENTATION IS INTENDED TO SUPERSEDE ANY EXPRESS WRITTEN AGREEMENTS OR WARRANTIES PROVIDED BY BLACKBERRY FOR PORTIONS OF ANY BLACKBERRY PRODUCT OR SERVICE OTHER THAN THIS DOCUMENTATION.

BlackBerry Enterprise Software incorporates certain third-party software. The license and copyright information associated with this software is available at http://worldwide.blackberry.com/legal/thirdpartysoftware.jsp.

BlackBerry Limited
2200 University Avenue East
Waterloo, Ontario
Canada N2K 0A7

BlackBerry UK Limited
Ground Floor, The Pearce Building, West Street,
Maidenhead, Berkshire SL6 1RL
United Kingdom

Published in Canada