Restrictions Payload

A restrictions payload disables specific applications or functionality on Android or iOS devices. Each device can only use one restrictions payload. If there are multiple restrictions payloads applied to the folder the device is in, only the payload with the highest priority will be sent to the device. You can view the payloads that have been sent to the device by viewing device details.

When you are using a restrictions payload, ensure you are not locking down functionality that is required for other operations. For example, watch for the following scenarios:

- Do not block the Settings application if you are using a passcode payload, since the user needs to access Settings in order to set or change a passcode.
- Ensure software payloads have been distributed and the desired apps have been installed on the device before you disallow installing apps.
- Ensure your white listed apps are installed on the device before you apply a payload to enable white listing.

Android

Simple Restrictions

Encrypt device	Encrypts the personal information saved on the device. This includes accounts, settings, apps, media, and other data saved to the internal phone storage media. This does not encrypt removable storage media such as an SD card. Enabling this option prompts the user to encrypt the device, but does not force encryption. The user is required to set a passcode before encrypting the device, because the passcode is used to decrypt the information each time the device is unlocked. Depending on the device, encryption may not be a reversible action.
Allow Settings Application	Allows the user to access and change the Android device settings.
Allow installing apps	Allows the user to install apps. Removing the check for this option does not prevent users from deleting apps on the device. Avalanche cannot prevent the removal of apps at the device level.
Allow use of camera	Allows the user to launch the camera application.
Allow Web applications	Allows the user to launch a web browser.
Allow Default Web browser	Allows the user to launch the default web browser.

Allow Mail applications	Allows the user to launch email applications.
Allow Google Search bar	Allows the user to use the Google Search application.
Allow use of YouTube	Allows the user to use a YouTube application.

Samsung SAFE Restrictions

Enable SAFE Restrictions	Allows you to restrict specific actions on a Samsung SAFE device. When the payload is sent to devices, these options are applied only on Samsung SAFE devices.
Allow uninstalling apps	Allows the user to uninstall apps.
Allow voice dialer	Allows the user to dial using voice commands.
Allow Play Store	Allows the user to access the Google Play Store.
Encrypt external SD card	Allows the user to encrypt external SD cards on Samsung SAFE devices. The encryption process must be performed by users at the device level. To encrypt an external SD card on a device after deploying a restrictions payload with this option selected, launch the Settings app and navigate to **Security > Encrypt external SD card**. Tap **Set screen lock type >Password** and then set and confirm a password. This password is used to access data on the SD card, as well as decrypt the card. After setting the password, you are returned to the Encrypt external SD card screen and you must tap **Continue** and then enter the password to start the encryption process. When fully encrypted, a notification appears at the top of the screen. To decrypt an external SD card, this option must be deactivated in Avalanche and synced to the device. Once synced, launch the Settings app and navigate to the Encrypt external SD card screen. Tap **Turn off** and enter the password you set previously. Tap **Apply** and then wait for the SD card to be decrypted. A notification appears at the top of the screen when complete.

App restrictions	Allows you to create a list of specific applications and assign restrictions or allowances to each individual app. To add a specific app for management, type the name and package details in the text boxes and click **Add App**. For example, in order to add restrictions to the Gmail app, type: `Gmail com.google.android.gm` Set restrictions on an app by selecting the app in the list and clicking the **Set Restrictions** icon. You can only set restrictions for a single app at a time. Options selected here will only apply to the app you selected. If an app requires use of an option you've restricted, the app will automatically close when launched and display an error message. If an open app asks for permission to access a restricted setting and the device user gives permission, this will also force the app to close.
Device restrictions	Globally restrict how all apps interact with each other and your Samsung SAFE device. Selecting a restriction prevents any apps on the device from performing the specified action. For example, if you select Read SMS, devices that receive this payload cannot open and view SMS messages. If an app requires use of an option you've restricted, the app will automatically close when launched and display an error message. If an app asks for permission to access a restricted setting and the device user gives permission, this will also force the app to close.

Black List

A Black List indicates apps not approved for use and redirects users to the home screen when an unapproved app is launched.

To block a specific app, search for apps in the Google Play Store by clicking the **Browse** icon, or enter the name and package details and click **Add App**. Type the friendly name for the app in the **App Name** text box, and the Android package name in the **App Package** text box. For example, in order to block a Gmail app, type: `Gmail com.google.android.gm`

To delete an app from the list, enable the check box next to the name of the app and click the **Delete** icon.

In order for the device user to override app restrictions on the device, you must set a **Smart Device Client Administrator Password** from **Tools > System Settings** in Avalanche. After setting the password and syncing the device, you can input the password on a device to disable app restrictions.

To deactivate app restrictions, edit the original payload, redeploy the payload, and sync the desired devices.

White List

A **White List** indicates the approved apps and prevents all other apps from launching.

If you create a White List, you must select a **Default App** from the list of approved apps. Generally, the default app is an app launcher that lists the available apps. After deploying the payload, tap the **Home** button on a device to launch the default app. Holding down the home button or navigating to a blocked app displays a dialog box that lists the available apps.

To add a specific app to the white list, search for apps in the Google Play Store by clicking the **Browse** icon. You can also add apps manually by typing the friendly name for the app in the **App Name** text box and the Android package name in the **App Package** text box. For example, in order to add a Gmail app, type: `Gmail com.google.android.gm`

To delete an app from the list, enable the check box next to the name of the app and click the **Delete** icon.

In order for the device user to override app restrictions on the device, you must set a **Smart Device Client Administrator Password** from **Tools > System Settings** in Avalanche. After setting the password and syncing the device, you can input the password on a device to disable app restrictions.

To deactivate app restrictions, edit the original payload, redeploy the payload, and sync the desired devices.

Deploying white list restrictions on a Samsung SAFE device will disable both hard and soft home keys and create a button that allows the user to navigate back to the home app.

Android Enterprise

Admin password

Devices that receive a restrictions payload can be set to require an admin password to perform certain actions from the device, such as unenrolling. To set an admin password, create or edit an Android Enterprise Restrictions payload, select **Enable Admin Override**, then enter a password. When attempting to perform a restricted action, the device user will be prompted for the admin password. The admin password is also required to temporarily disable dedicated device mode on a device.

Dedicated device mode

For more information about dedicated device mode, see Dedicated Device (Lock Task) Mode.

Disable factory reset protection	Factory reset protection requires an authorized account to sign in on the device after a factory reset. The authorized account is an account that was on the device before the factory reset. Using a corporate account on a device with factory reset protection provides another layer of device security by ensuring the company will retain control over the device, even after a factory reset. Factory reset protection is enabled by default. Select this option to disable it.
Disable factory resetting from the settings app	Prevents the user from factory resetting the device from the settings app.

Disable smart lock	Disable Google Smart Lock options, including staying unlocked when in a trusted location or when paired to a trusted device.
Block uninstallation of managed apps	Prevents the user from uninstalling managed apps that have been pushed to the device.
Disable keyguard camera	Disables opening the camera from the lock screen.
Allow USB debugging	Allow access to developer options to enable USB debugging.
Disable adding Google user accounts	Prevent the user from adding a personal Google account to the device. This restriction must be set during provisioning to ensure the user does not add personal accounts before the restriction is in place. Setting this restriction will not remove accounts already on the device.
Enable dedicated device mode (lock task mode)	Puts fully managed devices into lock task mode. This mode locks the device to the launchpad included in the Android Enterprise enabler. Only apps whitelisted in this payload will be accessible through the launchpad. **Enable System Info in the Status Bar.** Shows time, battery, and Wi-Fi information in the status bar.
Whitelisted apps	Create a whitelist to lock the device to approved apps. Apps in the list will appear in the enabler launchpad. To add a specific app to the white list, search for apps in the Google Play Store by clicking the **Browse** icon. You can also add apps manually by typing the friendly name for the app in the **App Name** field and the Android package name in the **App package** field. For example, in order to add a Gmail app, type: `Gmail` `com.google.android.gm`
Allow USB debugging	Allow a user to enable developer options and use USB debugging.

Fully managed device mode

Factory reset protection	Factory reset protection requires an authorized account to sign in on the device after a factory reset. The authorized account is an account that was on the device before the factory reset. Using a corporate account on a device with factory reset protection provides another layer of device security by ensuring the company will retain control over the device, even after a factory reset. Factory reset protection is enabled by default. Select this option to disable it.

Factory resetting from the settings app	Prevents the user from factory resetting the device from the settings app.
Disable smart lock	Disable Google smart lock options, including staying unlocked when in a trusted location or when paired to a trusted device.
Block uninstallation of managed apps	Prevents the user from uninstalling apps installed from the managed enterprise Play Store.
Disable keyguard camera	Disables opening the camera from the lock screen.
Disable adding Google user accounts	Prevent the user from logging into enterprise apps with personal accounts. This restriction must be set during provisioning to ensure the user does not add personal accounts. Setting this restriction will not remove accounts already on the device.
Allow USB debugging	Allow a user to enable developer options and use USB debugging.

iOS

Device Functionality

Allow installing apps	Allows the user to install apps. Removing the check for this option does not prevent users from deleting apps on the device. Avalanche cannot prevent the removal of apps at the device level.
Allow use of camera	Allows the user to launch the camera application.
Allow FaceTime	Allows the user to place or receive FaceTime calls.
Allow screen capture	Allows the user to save a screenshot of the display.
Allow automatic sync while roaming	Allows the device to sync accounts automatically, even when the device is roaming.
Allow Siri	Allows the user to use Siri voice commands or dictation.
Allow Siri while locked	Allows the user to use Siri without entering a passcode when the device is locked.

Allow Siri querying user-generated content (Supervised only)	Allows the user access to content in Siri added by other users.
Allow voice dialing	Allows the user to dial using a voice command.
Allow Passbook while device locked	Allows the device to display Passbook notifications while the device is locked.
Allow In-App Purchase	Allows the user to make purchases through installed apps.
Force user to enter password for all purchases	Forces the user to type in their iTunes Store account password each time they make a purchase.
Allow multiplayer gaming	Allows the user to play multiplayer games in the Game Center.
Allow adding Game Center friends	Allows the user to add friends in the Game Center.
Allow Control Center while locked	Allows the user to swipe up to view the Control Center even when the device is locked.
Allow Notification View while locked	Allows the user to view notifications even when the device is locked.
Allow Today view while locked	Allows the user to swipe down to see the Today view even when the device is locked.
Allow iBooks Store	Allows the user to access the iBooks Store.
Allow use of AirDrop	Allows the user to access AirDrop.
Allow account change	Allows the user to change account settings.
Allow cellular data usage for apps	Allows apps on the device to use a cellular data connection.

Applications

Allow use of iTunes Store	Allows the user to access the iTunes Store.

Allow use of YouTube	Allows the user to open the YouTube app.
Allow use of Google Search	Allows the user to use Google Search.
Allow Web browser	Allows the user to launch Safari. When this option is disabled, the user will not be able to launch Safari, but will still be able to launch other web browsers, such as Chrome.
Enable autofill	Allows the user to turn on Safari's auto-fill feature.
Limit ad tracking	Prevents the device's ID from being used for advertisement tracking.
Force fraud warning	When the user visits a fraudulent or compromised website, Safari displays a warning.
Allow JavaScript	Allows web pages that the user accesses using Safari to run JavaScript.
Block pop-ups	Sets Safari to block pop-up messages.
Accept cookies	Allows Safari to accept all cookies, reject all cookies, or accept cookies only from sites that are directly accessed.
Allow change to Find My Friends (Supervised only)	Allows applications to access Find My Friends.

Content Ratings

Allow explicit content	Allows the user to see explicit music or video content in the iTunes Store. Explicit content is flagged by content providers.
Ratings region	The media region with the rating system the device should use in allowing content.
Allowed content ratings	**Movies.** The level of allowed content for movies. **TV Shows.** The level of allowed content for TV shows. **Apps.** The level of allowed content for apps.

Kiosk Mode (Supervised device only)

Enable kiosk mode	When kiosk mode is enabled, the device will only launch the app specified and will block other apps. To specify the app for kiosk mode, use the app's Apple ID. To exit kiosk mode, an administrator must modify the payload to turn off kiosk mode and update the device. Kiosk mode is only available for devices that are in Supervised mode. For more information, see your Apple documentation.
Disable Autolock	Prevents the device from locking automatically.
Disable device rotation	Disables the display from changing orientation when the device is rotated.
Disable ringer switch	Disables any functionality associated with the ringer switch.
Disable sleep/wake button	Disables any functionality associated with the sleep/wake button.
Disable touch	Disables the touch functionality of the screen.
Disable volume button	Disables any functionality of the volume button.
Allow Assistive Touch	Allows the user to use Assistive Touch features to make the device more accessible. This option is for users who have problems touching the screen or pressing buttons.
Allow Assistive Touch adjustment	Allows the user to configure Assistive Touch options.
Allow invert colors	Allows the user to invert the colors on the screen.
Allow user to adjust color inverting	Allows the user to configure color inversion options.
Allow mono audio	Allows the user to switch the audio output to mono.
Allow Speak Selection	Allows the user to select text and use the Speak Selection feature for text-to-speech.
Allow VoiceOver	Allows the user to use VoiceOver features to make the device more accessible. This option is for users who need audible presentation of screen materials or menus.
Allow user to adjust VoiceOver	Allows the user to configure VoiceOver options.
Allow zoom	Allows the user to use zoom features.

Allow user to change zoom	Allows the user to change the zoom settings.
Autonomous permitted App IDs to run	Allows apps, identified by their bundle IDs, to enter Single App Mode. This option only applies if you have apps that have the ability to enter Single App Mode. Avalanche does not make apps enter Single App Mode, it only allows the app to do so.

iCloud

Allow backup	Allows the user to back up the device using iCloud.
Allow document Sync	Allows the user to store documents in iCloud.
Allow Photo Stream	Allows the user to use Photo Stream. If Photo Stream is disabled after the device user has shared photos using Photo Stream, photos already shared will be removed.
Allow shared photo streams	Allows the user to share his photo stream and view others' photo streams.

Security and Privacy

Allow unlocking by Touch ID	Allows the user to use Touch ID to unlock the device.
Allow Host Pairing	Allows the device to pair with computers other than the computer used to put the device in Supervised mode.
Allow diagnostic data to be sent to Apple	Allows the device to send diagnostic data to Apple.
Allow user to accept untrusted certificates	Allows the user to accept TLS certificates that can't be verified. This setting is enforced for Safari, Mail, Contacts, and Calendar.
Allow open from managed to unmanaged Apps/Accounts	Allows the user to switch to unmanaged applications or accounts from a managed app or account. For example, if the email app is managed but the browser app is not, the user would be allowed to click on a link in an email that launches the browser.

Allow open from unmanaged to managed Apps/Accounts	Allows the user to switch to managed applications or accounts from an unmanaged app or account. For example, if the email app is managed but the browser app is not, the user would be allowed to click on a link on a web page that launches the email app.
Allow Over-The-Air PKI Updates	Allows public key infrastructure updates. If this option is not enabled, you may experience issues with any application that depends on certificates, including internet browsers.
Allow interaction while install config profile (Supervised only)	Allows the administrator to send down configuration profiles silently, without user interaction.
Force encrypted backups	Forces the user to encrypt any backups using iTunes.

For some of the options in a restrictions payload for iOS, the device must be manually configured to be in Supervised mode using Apple Configurator. For information on Supervised mode, see your Apple documentation.