Workspace One SDK Events

The Workspace ONE® SDK utilizes a callback mechanism to notify applications about various occurrences and results of asynchronous operations. When the SDK triggers a callback, it often includes an event that signals the specific nature of the notification. Applications integrating the Workspace ONE® SDK can listen for these events and implement custom logic to handle them appropriately.

Table of Contents

Workspace One Anchor Events

The `WS1AnchorEvents` interface provides a set of events that can be used to handle various scenarios in the Workspace ONE SDK. This needs to be implemented by the Application and its reference passed via SDKClientConfig. More information present in BaseIntegrationGuide The events include:

Event	Description	Callback Context/Data	Actionable Response
onClearAppDataCommandReceived	Method to handle application data wipe command from console.	Application context, Reason for which app wipe is requested. See Clear Reason Codes.	App should use this callback to clear all the application data.
onAnchorAppCheckIn	Method to handle device checked in (signed out) broadcast from AnchorApp.	Application context	App should use this callback to remove information of old logged in user.
onAnchorAppCheckOut	Method to handle device checked out (signed in) broadcast from AnchorApp.	Application context	App should use this callback to update information of new logged in user.

Event	Description	Callback Context/Data	Actionable Response
onApplicationConfigurationChange	Method to handle application configuration change broadcast from console.	New application configuration defined in console, Application context	App should use this callback to update application configuration.
onApplicationProfileReceived	Method to handle application profile received from console.	Application context, Unique id assigned to each profile, ApplicationProfile	App should use this callback to update application profile.
onOGChangeStatusReceived	Method to handle Organization Group Change broadcast from console.	Application context	App should use this callback to receive OG change command status.
onAnchorAppStatusReceived	Method to handle anchor application status received from console.	Application context, Anchor app status	App should use this callback to update anchor application status.

Event	Description	Callback Context/Data	Actionable Response
onAnchorAppUpgrade	Method to handle broadcast for Anchor App Upgrade.	Application context, Boolean flag indicating if it is an upgrade or removal of anchor app	App should use this callback to take action on anchor application upgrade.
handleProfileReady	Method to handle profile ready broadcast from console.	Application context, profile type, UUID, Boolean flag indicating if profile group is installed or not	App should use this callback to update application profile.
handleAutoEnrollmentStatus	Method to handle auto enrollment completion broadcast from console.	Status integer to indicate the status of auto enrollment. When complete, AirWatchSDKConstants.AUTO_ENROLLMENT_STATUS_COMPLETE will be used as an input	App should use this callback to handle auto enrollment status.

Event	Description	Callback Context/Data	Actionable Response
onEnrollmentComplete	Method to handle enrollment completion broadcast from console.	Application context, Enrollment From the app ({@link AirWatchSDKConstants#ANCHOR_APP_PACKAGES}) which handled the enrollment	App should use this callback to perform actions on enrollment completion.

Clear Reason Codes

The `ClearReasonCode` is an Enum representing various reasons for initiating a data wipe action. This enum is used to categorize and identify the specific reason for a wipe action, such as app uninstallation, compliance violations, or user-triggered actions. Each reason is associated with a unique integer code for easy identification and processing. The defined codes are as follows:

- ANCHOR_APP - Anchor app triggered data wipe.
- ANCHOR_APP_UN_INSTALLED - Triggered when the anchor app is uninstalled and a broadcast message is sent to the app in case of WS1 and Container.
- MAX_ATTEMPT_VIOLATION - Triggered when the maximum number of authentication attempts is violated.
- USER_DELETE_ACCOUNT_AND_SERVICE - Triggered when the user deletes the account and service from the app settings.
- APP_STATUS_ENDPOINT - Triggered by the app status endpoint.
- BREAK_MDM_COMMAND - Triggered by an enterprise wipe command from the command processor.
- COMPROMISE_DETECTED_AW - Triggered when compromise protection is enabled and AirWatch detects the device is compromised.
- COMPROMISE_DETECTED_ENSURE_IT - Triggered when Ensure IT detects the device is compromised.
- COMPROMISE_DETECTED_GUARD_IT - Triggered when Guard IT detects the device is compromised.
- REQUESTED_BY_APP - Triggered by the app without user interaction, e.g., when the anchor is removed and the remove package is not received.
- CTS_INCOMPATIBLE - Triggered when SafetyNet detects the device failed to pass Android compatibility testing, indicating the device might be tampered or modified.
- UNKNOWN - Triggered by an unknown code.
- NON_COMPLIANT - Triggered when the device fails one or more compliance policies.
- APP_NOT_SUPPORTED - Triggered when the app is not supported.
- APP_INACTIVITY - Triggered when the app is inactive beyond the configured time on the console.
- APP_INITIALIZATION_FAILED - Triggered when app initialization fails.

Document Information

Revision History

07Apr2025 Initial Publication.

License