PTT Pro, Voice, and Profile Client

Workcloud Communication



Deployment Guide Mobile Device Management

MN-005042-01EN Rev A

2025/03/10

ZEBRA and the stylized Zebra head are trademarks of Zebra Technologies Corporation, registered in many jurisdictions worldwide. All other trademarks are the property of their respective owners. ©2025 Zebra Technologies Corporation and/or its affiliates. All rights reserved.

Information in this document is subject to change without notice. The software described in this document is furnished under a license agreement or nondisclosure agreement. The software may be used or copied only in accordance with the terms of those agreements.

For further information regarding legal and proprietary statements, please go to:

SOFTWARE: zebra.com/informationpolicy. COPYRIGHTS: zebra.com/copyright. PATENTS: ip.zebra.com. WARRANTY: zebra.com/warranty. END USER LICENSE AGREEMENT: zebra.com/eula.

Terms of Use

Proprietary Statement

This manual contains proprietary information of Zebra Technologies Corporation and its subsidiaries ("Zebra Technologies"). It is intended solely for the information and use of parties operating and maintaining the equipment described herein. Such proprietary information may not be used, reproduced, or disclosed to any other parties for any other purpose without the express, written permission of Zebra Technologies.

Product Improvements

Continuous improvement of products is a policy of Zebra Technologies. All specifications and designs are subject to change without notice.

Liability Disclaimer

Zebra Technologies takes steps to ensure that its published Engineering specifications and manuals are correct; however, errors do occur. Zebra Technologies reserves the right to correct any such errors and disclaims liability resulting therefrom.

Limitation of Liability

In no event shall Zebra Technologies or anyone else involved in the creation, production, or delivery of the accompanying product (including hardware and software) be liable for any damages whatsoever (including, without limitation, consequential damages including loss of business profits, business interruption, or loss of business information) arising out of the use of, the results of use of, or inability to use such product, even if Zebra Technologies has been advised of the possibility of such damages. Some jurisdictions do not allow the exclusion or limitation of incidental or consequential damages, so the above limitation or exclusion may not apply to you.

Introduction

This guide describes the procedures for using a Mobile Device Manager (MDM) to configure the Workcloud Communication apps. This guide is intended for readers who are familiar with the desired MDM and ensure that the target devices are pre-configured with the necessary MDM agent.

When you first deploy a Zebra client using a MDM application, you must install the client and apply the appropriate permissions for each app. You can deploy Zebra PTT Pro, Zebra Voice, and the Zebra Profile Client using an MDM.

Workcloud Communication apps support the following MDMs:

- VMware Workspace ONE (formerly AirWatch)
- SOTI
- StageNow



NOTE: These instructions are for devices running Android 10 or Android 11. For the most recent versions of these apps, see <u>zebra.com/support</u>.

App Deployment Files

Each app requires a set of files to configure the permissions on the device OS and to configure how the app functions. Additional configuration options are available through the XML or JSON files for each app. The JSON and XML configuration files can also be managed through the MDM.

The following guides provide additional configuration information for each client app:

- PTT Pro for Android
 - Workcloud Communication PTT Pro for Android Configuration Guide
 - Workcloud Communication PTT Pro for Android Programmer Guide
- Zebra Voice
 - Workcloud Communication Voice Programmer Guide
 - Voice administrator guide applicable to your PBX.
- Profile Client
 - Workcloud Communication Profile Client Android Configuration and Programmer Guide

MDM Deployment Files for PTT Pro

PTT Pro requires five files to be deployed when installing the PTT Pro app through an MDM:

- PTTPro_bypass_data_consent.xml bypasses the OS permission data consent screen.
- PTTPro_Battery_Optimization.xml optimizes battery performance when using PTT Pro.
- PTT_display_over.xml permits PTT Pro to display over other apps.
- PTTPro_Config.xml passes a token to the Provisioning Manager and receives configuration information.
- WFCPTTPerms.txt provides the necessary permissions for Android.

On Android 10, files can be loaded to the SD card. On Android 11, use the /enterprise/device/ settings/pttpro.

PTT_Pro_Bypass_Data_Consent.xml

```
<wap-provisioningdoc>
  <characteristic version="10.2" type="Intent">
    <parm name="Action" value="StartActivity" />
    <parm name="ActionName" value="android.intent.action.VIEW" />
```

PTT_Pro_Battery_Optimization

```
<wap-provisioningdoc>
  <characteristic version="9.3" type="AppMgr">
     <parm name="Action" value="BatteryOptimization" />
     <parm name="RemovePackageNames" value="com.symbol.wfc.pttpro" />
  </characteristic>
  </wap-provisioningdoc>
```

PTT_display_over.xml

```
<wap-provisioningdoc>
  <characteristic version="10.0" type="AccessMgr">
    <parm name="PermissionAccessAction" value="1" />
    <parm name="PermissionAccessPermissionName"</pre>
 value="android.permission.SYSTEM ALERT WINDOW" />
    <parm name="PermissionAccessPackageName" value="com.symbol.wfc.pttpro" />
    <parm name="PermissionAccessSignature" value="MIIDhzCCAm</pre>
+qAwIBAqIEQ8wDKDANBqkqhkiG9w0BAQsFADB0MQswCQYDVQQGEwJVUzELMAkGA1UECBMCSUwxEz
ARBgNVBAcTClNjaGF1bWJ1cmcxHDAaBgNVBAoTE1N5bWJvbCBUZWNobm9sb2dpZXMxCzAJB
gNVBAsTAk1DMRgwFgYDVQQDEw9Jb3VyaSBUYXJzb3Vub3YwHhcNMTQwNjEzMTcyNzQ3WhcNNDEx
MDI5MTcyNzQ3WjB0MQswCQYDVQQGEwJVUzELMAkGA1UECBMCSUwxEzARBgNVBAcTClNjaGF1bWJ1
cmcxHDAaBgNVBAoTE1N5bWJvbCBUZWNobm9sb2dpZXMxCzAJBgNVBAsTAk1DMRgwFgYDVQQDEw9J
b3VyaSBUYXJzb3Vub3YwqqEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwqqEKAoIBAQCRkeWNk97aFom
UXuSc/RddMzGO31b0rHG1pd0KbPmq522AoqUGV6+Mp3E2U2GN9CVq421rOKmQqm+vsPJDd/
nkjhXshz+3cDFrFHGY2ZxX93L
+XtXBq7XY809ktNXM9Cz6f7026r1c5Ue1QTeZBzH0jfNcU4YJKvVCsc8cDQHs6P96JubYpCvlsi
SqDXg6Ck20AqlhdOz189AQF9Qndm74oJy1FAS/6ZKh5xdSU17OnN6C
+Oidwmkz8X134V7pN0fSQnp1kaMz+z0xMQIxQXnmK795geiBV1sysnIWfKEB4ip9GxDRj0SLq5n/
qj6QP3UX9Im55ba0D5dxEEJNFsxdAqMBAAGjITAfMB0GA1UdDqQWBBQaxvuYVjlGl4sOVLpbqQo9
q1WltjANBqkqhkiG9w0BAQsFAAOCAQEAP123iSmemDDFH1BBSoBK7KFi490Nj9BOKotzVByJGcc
LV2277TkvogUlnPFgk+ARfZu8FYeVeNJbp0K
+iznFiv51NfcS5YpxUB01c0zcxHSXUt6BsC/3Z8NKaOYoKyrfmHaW9OVGDhY2JPGirBAIQp
+y7a71pTh1mVyPSESHgXcKitTrNtNua2yh98CuNmIeZ9fThbxn0VWJ9ChqF1d8Lo1Bx1xyq1m/
JVZYFVP9T8rGR3sp2U2+391Yr/Xx2j09cIIDrnTAZX1EOhNrFqe3tObaQrbPVR5/WqVXjmGmXus
+Y3ZKVY2t1Ip8q8q0IOCrj0wm531pe+qfQ3CXSXMIIw==" />
  </characteristic>
</wap-provisioningdoc>
```

PTTPro_Config.xml

 $\mathbf{Z}\mathbf{A}$

NOTE: Replace TOKEN NAME with the value of your token.

```
<wap-provisioningdoc>
  <characteristic version="8.3" type="Intent">
    <parm name="Action" value="StartActivity" />
    <parm name="ActionName" value="android.intent.action.VIEW" />
    <parm name="Package" value="com.symbol.wfc.pttpro" />
    <parm name="Uri" value="wfctp://TOKEN NAME" />
    </characteristic>
</wap-provisioningdoc>
```

WFCPTTPerms.txt

```
<characteristic uuid="e135b2b0-e9ac-4dd2-8b92-65eb259dc42d"</pre>
 type="com.airwatch.android.androidwork.permissions"
target="1"><parm name="AppLevelRuntimePermissions"</pre>
value="W3sicGFja2FnZU5hbWUiOiJjb20uc3ltYm9sLndmYy5wdHRwcm8iLCJwZXJtaXNzaW9
ucy16W3sibmFtZSI6ImFuZHJvaWQucGVybWlzc2lvbi5XUklURV9DT05UQUNUUyIsInZhbHVlIjoi
MSJ9LHsibmFtZSI6ImFuZHJvaWQucGVybWlzc2lvbi5DQUxMX1BIT05FIiwidmFsdWUi0iIxIn0sey
JuYW111joiYW5kcm9pZC5wZXJtaXNzaW9uLlJFQ09SRF9BVURJTyIsInZhbHVl1joiMSJ9LHsibmFt
ZSI6ImFuZHJvaWQucGVybWlzc2lvbi5SRUFEX0NPTlRBQ1RTIiwidmFsdWUi0iIxIn0seyJuYW11I
joiYW5kcm9pZC5wZXJtaXNzaW9uLklOVEVSTkVUIiwidmFsdWUiOiIxIn0seyJuYW1lIjoiYW5kcm
9pZC5wZXJtaXNzaW9uLlJFQURfU0VUVE10R1MiLCJ2YWx1ZSI6IjEifSx7Im5hbWUi0iJhbmRyb21
kLnBlcmlpc3Npb24uUkVBRF9QSE9ORV9TVEFURSIsInZhbHVlIjoiMSJ9LHsibmFtZSI6ImFuZHJ
vaWQucGVybWlzc21vbi5SRUFEX0VYVEVSTkFMX1NUT1JBR0UiLCJ2YWx1ZSI6IjEifSx7Im5hbWUi
OiJhbmRyb2lkLnBlcm1pc3Npb24uV1JJVEVfRVhURVJOQUxfU1RPUkFHRSIsInZhbHVlIjoiMSJ9L
HsibmFtZSI6ImFuZHJvaWQucGVybWlzc2lvbi5SRUFEX1BST0ZJTEUiLCJ2YWx1ZSI6IjEifSx7Im
5hbWUiOiJhbmRyb2lkLnBlcm1pc3Npb24uVVNFX0NSRURFT1RJQUxTIiwidmFsdWUiOiIxIn0seyJu
W111joiYW5kcm9pZC5wZXJtaXNzaW9uLk1BTkFHRV9BQ0NPVU5UUyIsInZhbHVl1joiMSJ9LHsibm
FtZSI6ImFuZHJvaWQucGVybWlzc2lvbi5SRUFEX1NZTkNfU1RBVFMiLCJ2YWx1ZSI6IjEifSx7Im5
hbWUiOiJhbmRyb21kLnB1cm1pc3Npb24uUkVBRF9TWU5DX1NFVFRJTkdTIiwidmFsdWUiOiIxIn0s
eyJuYW111joiYW5kcm9pZC5wZXJtaXNzaW9uLldSSVRFX1NZTkNfU0VUVE1OR1MiLCJ2YWx1ZSI6I
EifSx7Im5hbWUiOiJhbmRyb2lkLnBlcm1pc3Npb24uUkFJU0VEX1RIUkVBRF9QUk1PUk1UWSIs
InZhbHVlIjoiMSJ9XXld" type="string" /></characteristic>
```

MDM Deployment Files for Zebra Voice

Zebra Voice requires three files to be deployed when installing the Voice app through an MDM:

- BatteryOptimizationWFCVoice.xml optimizes battery performance when using Zebra Voice.
- SystemAlertPermission.xml enables Zebra Voice to display over other apps.
- GrantWFCVoicePermissions.txt provides the necessary Android OS permissions.

BatteryOptimizationWFCVoice

SystemAlertPermission.xml

```
<wap-provisioningdoc>
  <characteristic type="AccessMgr" version="10.1">
    <parm name="PermissionAccessAction" value="1"/>
    <parm name="PermissionAccessPermissionName"</p>
 value="android.permission.SYSTEM_ALERT_WINDOW"/>
    <parm name="PermissionAccessPackageName" value="com.symbol.wfc.voice"/>
    <parm name="PermissionAccessSignature" value="MIIDhzCCAm</pre>
+gAwIBAgIEQ8wDKDANBgkqhkiG9w0BAQsFADB0MQswCQYDVQQGEwJVUzELMAkGA1UECBMCSUwx
EzARBgNVBAcTClNjaGF1bWJ1cmcxHDAaBgNVBAoTE1N5bWJvbCBUZWNobm9sb2dpZXMxCzAJB
gNVBAsTAk1DMRgwFgYDVQQDEw9Jb3VyaSBUYXJzb3Vub3YwHhcNMTQwNjEzMTcyNzQ3WhcNND
ExMDI5MTcyNzQ3WjB0MQswCQYDVQQGEwJVUzELMAkGA1UECBMCSUwxEzARBgNVBAcTC1NjaGF1
bWJ1cmcxHDAaBgNVBAoTE1N5bWJvbCBUZWNobm9sb2dpZXMxCzAJBgNVBAsTAk1DMRgwFgYDVQ
QDEw9Jb3VyaSBUYXJzb3Vub3YwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCRkeWN
k97aFomUXuSc/RddMzGO31b0rHG1pd0KbPmq522AoqUGV6+Mp3E2U2GN9CVq421rOKmQqm+vsPJ
Dd/nkjhXshz+3cDFrFHGY2ZxX93L+XtXBq7XY809ktNXM9Cz6f7026r1c5Ue1QTeZBzH0jfNcU
4YJKvVCsc8cDQHs6P96JubYpCvlsiSqDXg6Ck20AqlhdOz189AQF9Qndm74oJy1FAS/6ZKh5xd
SU17OnN6C+Oidwmkz8X134V7pN0fSQnp1kaMz+z0xMQIxQXnmK795geiBV1sysnIWfKEB4ip9Gx
DRj0SLq5n/qj6QP3UX9Im55ba0D5dxEEJNFsxdAgMBAAGjITAfMB0GA1UdDgQWBBQaxvuYVjlG
14sOVLpbqQo9q1WltjANBgkqhkiG9w0BAQsFAAOCAQEAP123iSmemDDFH1BBSoBK7KFi490Nj9BO
KotzVByJGccLV2277TkvogUlnPFgk+ARfZu8FYeVeNJbp0K
+iznFIv51NfcS5YpxUB01c0zcxHSXUt6BsC/3Z8NKaOYoKyrfmHaW9OVGDhY2JPGirBAIQp
+y7a71pTh1mVyPSESHgXcKitTrNtNua2yh98CuNmIeZ9fThbxn0VWJ9ChqF1d8Lo1Bx1xyq1m/
JVZYFVP9T8rGR3sp2U2+391Yr/Xx2j09cIIDrnTAZX1EOhNrFqe3tObaQrbPVR5/WgVXjmGmXus
+Y3ZKVY2t11p8q8q0IOCrj0wm531pe+qfQ3CXSXMIIw=="/>
  </characteristic>
</wap-provisioningdoc>
```

GrantWFCVoicePermissions.txt

The value for the AppLevelRuntimePermissions can encoded or decoded in Base64 format. Go to <u>https://www.base64encode.org/</u> to encode or decode the value.

```
<characteristic uuid="e135b2b0-e9ac-4dd2-8b92-65eb259dc41d"
type="com.airwatch.android.androidwork.permissions"
target="1"><parm name="AppLevelRuntimePermissions"
value="W3sicGFja2FnZU5hbWUiOiJjb20uc3ltYm9sLndmYy52b2ljZSIsInBlcm1pc3Npb25
zIjpbeyJuYW1lIjoiYW5kcm9pZC5wZXJtaXNzaW9uLkJJTkRfQUNDRVNTSUJJTElUWV9TRVJWS
UNFIiwidmFsdWUiOiIxIn0seyJuYW1lIjoiYW5kcm9pZC5wZ</pre>
```

App Deployment Files

XJtaXNzaW9uLkFDQ0VTU19DT0FSU0VfTE9DQVRJT04iLCJ2YWx1ZSI6IjEifSx7Im5hbWUiOiJh bmRyb2lkLnBlcm1pc3Npb24uQUNDRVNTX0ZJTkVfTE9DQVR JT04iLCJ2YWx1ZSI6IjEifSx7Im5hbWUiOiJhbmRyb2lkLnBlcm1pc3Npb24uUkVRVUVTVF9JR0 5PUkVfQkFUVEVSWV9PUFRJTUlaQVRJT05TIiwidmFsdWUi0 ilxIn0seyJuYW1l1joiYW5kcm9pZC5wZXJtaXNzaW9uL1NZU1RFTV9BTEVSVF9XSU5ET1ciLCJ2Y Wx1ZSI6IjEifSx7Im5hbWUi0iJhbmRyb2lkLnBlcm1pc3 Npb24uRVhQQU5EX1NUQVRVU19CQVIiLCJ2YWx1ZSI6IjEifSx7Im5hbWUiOiJhbmRyb21kLnBlcm1 pc3Npb24uR0VUX1RBU0tTIiwidmFsdWUi0iIxIn0seyJ uYW111joiYW5kcm9pZC5wZXJtaXNzaW9uLldSSVRFX0NPT1RBQ1RTIiwidmFsdWUiOiIxIn0seyJu YW111joiYW5kcm9pZC5wZXJtaXNzaW9uLkdFVF9BQ0NP VU5UUyIsInZhbHVlIjoiMSJ9LHsibmFtZSI6ImFuZHJvaWQucGVybWl zc2lvbi5DQUxMX1BIT05FIiwidmFsdWUi0iIxIn0seyJuYW1lIjoiYW5kcm9pZC5wZ XJtaXNzaW9uLlJFQ09SRF9BVURJTyIsInZhbHVlljoiMSJ9LHsibmFt ZSI6ImFuZHJvaWQucGVybWlzc2lvbi5SRUFEX0NPTlRBQ1RTIiwidmFsdWUi0iIxIn 0seyJuYW1l1joiYW5kcm9pZC5wZXJtaXNzaW9uLkZPUkVHUk9VTkRfU 0VSVklDRSIsInZhbHVlIjoiMSJ9LHsibmFtZSI6ImFuZHJvaWQucGVybWlzc2lvbi5 JT1RFUk5FVCIsInZhbHVlIjoiMSJ9LHsibmFtZSI6ImFuZHJvaWQucGV ybWlzc2lvbi5NT0RJR1lfQVVESU9fU0VUVElOR1MiLCJ2YWx1ZSI6IjEifSx7Im5h bWUiOiJhbmRyb21kLnBlcm1pc3Npb24uUkVBRF9TRVRUSU5HUyIsInZh bHVl1joiMSJ9LHsibmFtZSI6ImFuZHJvaWQucGVybWlzc2lvbi5SRUFEX1BIT05FX1N UQVRFIiwidmFsdWUiOiIxIn0seyJuYW111joiYW5kcm9pZC5wZXJtaXN zaW9uLkFDQ0VTU19XSUZJX1NUQVRFIiwidmFsdWUiOiIxIn0seyJuYW11IjoiYW5kcm 9pZC5wZXJtaXNzaW9uLkFDQ0VTU19ORVRXT1JLX1NUQVRFIiwidmFsdW UiOiIxIn0seyJuYW11IjoiYW5kcm9pZC5wZXJtaXNzaW9uLlJFQ0VJVkVfQk9PVF9DT 01QTEVURUQiLCJ2YWx1ZSI6IjEifSx7Im5hbWUiOiJhbmRyb2lkLnBlc mlpc3Npb24uV0FLRV9MT0NLIiwidmFsdWUiOiIxIn0seyJuYW11IjoiYW5kcm9pZC5wZ XJtaXNzaW9uLkRJU0FCTEVfS0VZR1VBUkQiLCJ2YWx1ZSI6IjEifSx7I m5hbWUiOiJhbmRyb2lkLnBlcm1pc3Npb24uVklCUkFURSIsInZhbHVlIjoiMSJ9LHsibm FtZSI6ImFuZHJvaWQucGVybWlzc2lvbi5CTFVFVE9PVEhfQURNSU4iLCJ 2YWx1ZSI6IjEifSx7Im5hbWUi0iJhbmRyb2lkLnBlcm1pc3Npb24uQkxVRVRPT1RIIi widmFsdWUiOiIxIn0seyJuYW11IjoiYW5kcm9pZC5wZXJtaXNzaW9uLlV TRV9TSVAiLCJ2YWx1ZSI6IjEifSx7Im5hbWUiOiJhbmRyb21kLnBlcm1pc3Npb24u00 9ORklHVVJFX1NJUCIsInZhbHVlIjoiMSJ9LHsibmFtZSI6ImFuZHJvaWQu cGVybWlzc2lvbi5SRUFEX0VYVEVSTkFMX1NUT1JBR0UiLCJ2YWx1ZSI6IjEifSx7Im 5hbWUiOiJhbmRyb2lkLnBlcm1pc3Npb24uV1JJVEVfRVhURVJOQUxfU1RP UkFHRSIsInZhbHVlIjoiMSJ9LHsibmFtZSI6ImFuZHJvaWQucGVybWlzc2lvbi5CUk 9BRENBU1RfU1RJQ0tZIiwidmFsdWUi0iIxIn0seyJuYW11IjoiYW5kcm9p ZC5wZXJtaXNzaW9uLlJFQURfUFJPRklMRSIsInZhbHVlIjoiMSJ9LHsibmFtZSI6ImF uZHJvaWQucGVybWlzc2lvbi5DSEFOR0VfV0lGSV9NVUxUSUNBU1RfU1RBVE UiLCJ2YWx1ZSI6IjEifSx7Im5hbWUiOiJhbmRyb21kLnBlcm1pc3Npb24uR0VUX0F DQ09VT1RTIiwidmFsdWUiOiIxIn0seyJuYW111joiYW5kcm9pZC5wZXJtaX NzaW9uLlVTRV9DUkVERU5USUFMUyIsInZhbHVlIjoiMSJ9LHsibmFtZSI6ImFuZHJ vaWQucGVybWlzc2lvbi5NQU5BR0VfQUNDT1VOVFMiLCJ2YWx1ZSI6IjEifSx 7Im5hbWUiOiJhbmRyb2lkLnBlcm1pc3Npb24uQVVUSEVOVE1DQVRFX0FDQ09VT1RT IiwidmFsdWUiOiIxIn0seyJuYW1l1joiYW5kcm9pZC5wZXJtaXNzaW9uLlJ FQURfU110Q19TVEFUUyIsInZhbHVl1joiMSJ9LHsibmFtZSI6ImFuZHJvaWQucGVy bWlzc2lvbi5SRUFEX1NZTkNfU0VUVElOR1MiLCJ2YWx1ZSI6IjEifSx7Im5h bWUiOiJhbmRyb2lkLnBlcm1pc3Npb24uV1JJVEVfU110Q19TRVRUSU5HUyIsInZ hbHVlljoiMSJ9LHsibmFtZSI6ImFuZHJvaWQucGVybWlzc2lvbi5SQUlTRU RfVEhSRUFEX1BSSU9SSVRZIiwidmFsdWUiOiIxInldfV0=" type="string" /></ characteristic>

PFM_Config.xml

RA

NOTE: Replace Zebra PROFILE CLIENT TOKEN with your customer token.

```
<wap-provisioningdoc>
<characteristic version="8.3" type="Intent">
<parm name="Action" value="StartActivity" />
<parm name="ActionName" value="android.intent.action.VIEW" />
<parm name="Package" value="com.zebra.dfs" />
<parm name="Uri" value="wfcpp://Zebra PROFILE CLIENT TOKEN" />
</characteristic>
</wap-provisioningdoc>
```

MDM Deployment Files for the Profile Client

The Profile Client requires three files to be deployed when installing the app through an MDM:

- Profile_client_display_over.xml enables the Profile Client to display over other apps.
- PFM_Config.xml provides a connection to the Profile Manager and requires the customer's API token.
- ProfileClient_PERMS.txt provides the necessary OS permissions that enables the app to function properly.

Profile_client_display_over.xml

```
<wap-provisioningdoc>
  <characteristic version="10.0" type="AccessMgr">
    <parm name="PermissionAccessAction" value="1" />
    <parm name="PermissionAccessPermissionName"</pre>
 value="android.permission.SYSTEM_ALERT_WINDOW" />
    <parm name="PermissionAccessPackageName" value="com.zebra.dfs" />
    <parm name="PermissionAccessSignature" value="MIIDlzCCAn</pre>
+gAwIBAgIEJIXuHTANBgkqhkiG9w0BAQsFADB8MQswCQYDVQQGEwJVUzELMAkGA1UEC
BMCSUwxFTATBgNVBAcTDExpbmNvbG5zaGlyZTEbMBkGA1UEChMSWmVicmEgVGVjaG5vbG9naWVz
MRIwEAYDVQQLEw1XRkNvbm51Y3QxGDAWBqNVBAMTD01vdXJpIFRhcnNvdW5vdjAeFw0xNzExMTA
yMTAwMTdaFw00NTAzMjgyMTAwMTdaMHwxCzAJBgNVBAYTA1VTMQswCQYDVQQIEwJJTDEVMBMGA1
UEBxMMTGluY29sbnNoaXJlMRswGQYDVQQKExJaZWJyYSBUZWNobm9sb2dpZXMxEjAQBgNVBAsTCV
dGQ29ubmVjdDEYMBYGA1UEAxMPSW91cmkgVGFyc291bm92MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ
8AMIIBCgKCAQEAn7KwSizkIUz8Dd33rkt6YRSRFJKbhhN/9QDsI+BWquMo0so/ZellQwLVsI0LP0
QnNHRzeQSG4TLYZUo1DyQzjdeMtkeliWjr5WYfwR9PIn7QX+J8r9DEtLsYfeUcfxpuEuJxc/q86FE
6S6fx6QX7BVc4gZjjjqVsJogjYbhy8jUR1qOyuJIVE10nqCXOzC01WdXDNxQ81UJpKzyTsLfnHhOI
4SvwauDCef2PorhgfeSD1id66Q6QZ9qq+J7Woae8IAmKhgvGpSzaRdOXtCzSoin3vHu9OTcjjcFWf
EvznWRdTecAth8/JgIcrTaZNIh09+lGuqa4DTQ2ozUP8qvtGQIDAQABoyEwHzAdBgNVHQ4EFgQU
Zo3uLIjn0S4cKjsilgrBt9xo2jIwDQYJKoZIhvcNAQELBQADggEBAEzPNHOHuSkxbHUFS57mtN+df
/cd4xUU7N76h2dZglfd7/mgVep7LGEgfmrRHXUI9zvPOJP5E0S2pZTZtQ/i4FRlagnLA8gJo0dpr6
nnYYasMaNmBRcaqoNva5PBLd5WuWCJqLfhnKAW1rSxO1MFkchXvbnNLAm4cjNurIC2dTZXNUmscONn
+sX
+TO6XLKfwvMIcG5S0ofC8HbAmsP1N5RLuarR6sP54f9mb4I3jBeLO46d4D0yqVlfE1cESmW27xF
```

```
xfQgO3mvWBG6Q004e6CBVMk4gWfMbBjtWTHDWfKV8tTEgLM4dFgUJ+uq6JqCHki4b5/
KsQcLrqi9pODNbNs1Y=" />
    </characteristic>
</wap-provisioningdoc>
```

ProfileClient_PERMS.txt

```
<characteristic uuid="e135b2b0-e9ac-4dd2-8b92-65eb259dc43d"</pre>
 type="com.airwatch.android.androidwork.permissions"
 target="1"><parm name="AppLevelRuntimePermissions"</pre>
value="W3sicGFja2FnZU5hbWUiOiJjb20uemVicmEuZGZzIiwicGVybWlzc2lvbnMiOlt7
Im5hbWUiOiJhbmRyb2lkLnBlcm1pc3Npb24uRk9SRUdST1VORF9TRVJWSUNFIiwidmFsdWUiOiI
xIn0seyJuYW1l1joiYW5kcm9pZC5wZXJtaXNzaW9uLklOVEVSTkVUIiwidmFsdWUiOiIxIn0sey
JuYW111joiYW5kcm9pZC5wZXJtaXNzaW9uLlJFQURfU0VUVElOR1MiLCJ2YWx1ZSI6IjEifSx7I
m5hbWUiOiJhbmRyb2lkLnBlcm1pc3Npb24uUkVBRF9QSE9ORV9TVEFURSIsInZhbHVlIjoiMSJ9
LHsibmFtZSI6ImFuZHJvaWQucGVybWlzc2lvbi5BQ0NFU1NfV01GSV9TVEFURSIsInZhbHVlIjoi
MSJ9LHsibmFtZSI6ImFuZHJvaWQucGVybWlzc2lvbi5BQ0NFU1NfTkVUV09SS19TVEFURSIsInZ
hbHVl1joiMSJ9LHsibmFtZSI6ImFuZHJvaWQucGVybWlzc2lvbi5SRUNFSVZFX0JPT1RfQ09NUEx
FVEVEIiwidmFsdWUiOiIxIn0seyJuYW11IjoiYW5kcm9pZC5wZXJtaXNzaW9uLldBS0VfTE9DSyIs
InZhbHVl1joiMSJ9LHsibmFtZSI6ImFuZHJvaWQucGVybWlzc2lvbi5SRUFEX0VYVEVSTkFMX1N
UT1JBR0UiLCJ2YWx1ZSI6IjEifSx7Im5hbWUiOiJhbmRyb2lkLnBlcm1pc3Npb24uV1JJVEVfRVh
URVJOQUxfU1RPUkFHRSIsInZhbHVl1joiMSJ9LHsibmFtZSI6ImFuZHJvaWQucGVybWlzc2lvbi5
TWVNURU1fQUxFUlRfV0lORE9XIiwidmFsdWUiOiIxIn1dfV0=" type="string" /></
characteristic>
```

Installing the Apps

You can install and manage Workcloud Communication using Workspace ONE, SOTI MobiControl, or Zebra StageNow. The steps for installing each app are provided below. When using the Profile Client with Zebra PTT Pro or Zebra Voice, install the Profile Client first.

This guide provides the procedures for each app but does not provide the detailed user interfaces for each MDM. Specific MDM details are beyond the scope of this document. The administrator deploying the apps is expected to understand the details of the MDM.



NOTE: Zebra StageNow is only applicable to Zebra Android devices.

The location of the configuration files differs between Android 10 and Android 11.

Android 10 and earlier:

Files can be copied to the external SD card (/sdcard).

Android 11 and later:

Files can be copied to /enterprise/device/settings/<app>.

Installing the Profile Client

Create the deployment files for the Profile Client as described previously, create an optional configuration file, and download the latest APK from the Zebra support site.

- 1. Upload the APK and the deployment files to the MDM.
- 2. Install the Zebra Profile Client.
- 3. Apply the Profile_client_display_over.xml file.
- 4. Apply the ProfileClient_PERMS.txt file.
- 5. Apply additional configuration parameters using the WFCDFSConfig.json file.

Installing the Voice Client

Create the deployment files for Zebra Voice as described previously, create an optional configuration file, and download the latest APK from the Zebra support site.

- 1. Upload the Zebra Voice APK and the deployment files to the MDM.
- 2. Install Zebra Voice.
- 3. Apply the BatteryOptimizationWFCVoice.xml file.
- 4. Apply the GrantWFCVoicePermissions.txt file.

- **5.** Apply the SystemAlertPermission.xml file.
- 6. Apply the PFM_Config.xml file.



NOTE: Enter your token to the PFM_Config.xml file.

7. Apply additional configuration parameters using the WFConnect.xml file.

Installing PTT Pro

Create the deployment files for PTT Pro for Android as described previously, create an optional configuration file, and download the latest APK from the Zebra support site.

- 1. Upload the PTT Pro for Android APK and deployment files to the MDM.
- 2. Install the PTT Pro for Android client.
- 3. Apply the PTT_Pro_Bypass_Data_Consent.xml file.
- 4. Apply the PTT_Pro_Battery_Optimization.xml file.
- 5. Apply the PTT_display_over.xml file.
- 6. Apply the WFCPTTPerms.txt file.
- 7. Apply the PTTPro_config.xml file.



NOTE: Enter your token in the PTTPro_config.xml file.

8. Apply additional configuration parameters using the WFCPTTProDefault.json file.

Updating an App

You can use an MDM to update the configuration of installed apps. Update the configuration file for each app and deploy the new configuration using the MDM. It is not necessary to reinstall the apps or reapply the permissions.

SOTI MobiControl

SOTI MobiControl is a comprehensive Mobile Device Management (MDM) solution that empowers organizations to efficiently manage, secure, and support mobile devices and endpoints.

SOTI Enrollment Methods

The following enrollment methods are described in detailed:

UUT Enrollment to SOTI via afw# Method

- 1. Perform a Factory Reset on UUT.
- 2. From the welcome page, click Lets' Go.
- 3. Click Set up as new.
- 4. Connect to any WLAN with internet connection (e.g.,-ZEWireless).
- 5. Enter afw#mobicontrol in email text field.
- 6. Click Install Android for work.
- 7. Click Install.
- 8. Click Next on the set up work device screen.
- 9. Select I consent and click OK.
- 10. From the Location Consent page, click Next .
- 11. Launch the MobiControl application and enter the Enrollment ID WEWUXV79.

Whitelist Package Name

- enable_system_app com.symbol.tool.stagenow
- enable_system_app com.zebra.licenseuiapp
- enable_system_app com.symbol.pttexpress

Whitelisting the above apps:

For example:

- Select the enrolled device in the console > Send script > choose legacy & send enable_system_app com.symbol.tool.stagenow.
- 2. Select Script Type as Legacy.

Enrolling SOTI via StageNow Method

For single barcode staging, select StageNow tool version MX 9.1

for Device Owner (DO) mode.

←

1. Download the latest SOTI Google Mobicontrol apk <u>https://pulse.soti.net/support/soti-mobicontrol/agent-downloads/</u>.

SOTI PULSE News Marketplace	Product Support Community	(Lit Google Lens X) 21 Z
Home > SOTI MobiControl > Agent Downloads		
SOTI MobiControl Device Agent Downlo	pads	
()	0	۵
Android	Apple	Linux
Android Enterprise Agents and Plugins		
Android Classic - OEM Specific Agents and Plugins	macOS Agent	Linux - Generic Agent
Android Management API- Companion	iOS Agent	Linux - OEM Specific Agent

2. Click Android Enterprise Agents and Plugin .

\leftarrow \rightarrow C \simeq pulse.soti.net/support/soti-mobicontrol/agent-downloads/android/android-enterprise/	☆ 章	₹
SOTI PULSE News Marketplace Product Support	Community Q	
Home > SOTI MobiControl > Agent Downloads > Android > Android Enterprise Android Enterprise Agents and Plugins		
Agent This is the Agent (App) to install in your Android Enterprise Device to work with SOTI MobiControl. Click the Download button to get it from our Servers.	Plugin The Plugin allows you to leverage components of our Android+ technology in Android Enterprise. Click here to learn more. Manufacturer -Please Select-	
From the Play Store You can also download the agent from the Google Play store.		

 $\widehat{}$

- 3. Click the **DOWNLOAD** button to download the apk.
- 4. Launch **StageNow** on the host PC and log in as an administrator.
- 5. Click **Create New Profile** and select the appropriate MX version.

- 6. Select **Xpertmode** and click **Create**. The selected MX version must be equal to or earlier than the MX version present in the device.
- 7. Add WIFI, FileMgr, AppMgr, and Intent CSP's, and click Continue.
- 8. From WIFI CSP, select the Network Action as Add a New Network and provide SSID (WLAES_CSST) and Passphrase (validation) and click Continue.

		2 Finiter	3 Annhlor	4		
Network Action	n: 0	riemy	мрранун	IRCIR		
Add a New Netw	work v					
SSID:						
WLAES_CSST		0				
Security Mode:	:0	-				
Personal	v					
WPA-Personal	Mode: 🕡					
WPA/WPA2	¥					
Encryption Type	pet 🔞					
Do not change	¥					
Key Type: 💮						
Hex Key	Passphrase					
Protect Key?						
Passphrase: 🕞	9					
validation		0				
Use DHCP? 🕑	0					
Use Proxy?						
	Harris Down Law Control					
None	Manual Proxy Auto-Comp					
Specify Hotspo	ot Options?					
Specify OmniTr	frail Options?					
Specify FTM Op	Options?					
Global Proxy St	itate: 💮					
00	Off Do Not Change					
	and the change					

- 9. From FileMgr CSP, select the following:
 - File Action as Transfer/copy File.
 - Target path and File name as /data/tmp/public/Latest MobiControl APK Name.
 - Source Access Method as File on a remote server.
 - From the Source archive URI, select the latest MobiControl app and click **Continue**.

1 - 2 - 3 - 4 Wi-Fi FileMgr AppMgr Intent
Save Setting for Re-use
Transfer/Copy File Delete File Download and Expand Archive File
Target Access Method: (?) File in the device file system
 Target Path and File Name: //data/tmp/public/GoogleMobiControl1520_1025.apk

	Staging Server URI Selector
Wi-Fi FileMgr	Staging Server: Built In ~
File in the device file system Target Path and File Name:	Select a File GoogleMobiControl1520_1025.apk
/data/tmp/public/GoogleMobiControl1520_1025.apk 💿 Source Access Method: 💿	OK Cancel
File on a remote server File in the device file system File embedded in XML	
Source File URI:	C

- **10.** From AppMgr CSP, select **Install** from the **Action** drop down list.
- 11. From the **APK Path and Name** drop down list, enter /data/tmp/public/<latest mobicontrolapk name>.

12. Click Continue.

	1 _ (2	- 3 -	4
	Wi-Fi	FileMgr	AppMgr	Intent
Action: 🕜				
Install	~			
APK Path and Name: 💿				
/data/tmp/public/GoogleMob	Control1520_1025.apk			
Protected List Action: 💿				
Do nothing	~			
Access to App Info Action	. 0			
Do nothing Do nothing App Info fr application	ess to or all ons Disable Access to App Info for all applications			

- 13. From the Intent CSP, select Enroll a Device Owner from the Action list box.
- 14. Enternet.soti.mobicontrol.androidwork from the Package Name list box.
- 15. Enter net.soti.mobicontrol.admin.DeviceAdminAdapter from Class Name list box.
- 16. From Json Values, click JSON File to select the JSON file from the Local folder.
- 17. Click Continue.

1) - (2	3	4	
Wi-Fi		FileMgr	AppMgr	Intent	
Action: 🕜					
Enroll a Device Owner	~				
Package Name: 🕜					
net.soti.mobicontrol.androidwork	8				
Class Name: 🛞					
net.soti.mobicontrol.admin.DeviceAdminA	dapter 😗				
Json Values: 🔞					
Do Nothing Json File J	son String				
ISON File:					

18. Click Complete Profiles , select PDF417 barcode type, and click Test.

- + Export for JS + Export for MDM NFC/SD/USB Barcode Last Tested Published Latest Staged Type Staging Client **送告**業 PDF417 StageNow Recomment for 2D Scar Engines Linear for 1D Lase JS PDF417 腦膜 Recommended for 2D Scan JS Linear for 1D Las Stage Test Test Select Publish 🖉 XpertConfig: Soti_new 🗹 Profile Id: 18 Profile Status: Complete StageNow Config Review Publish Barcode NFC/SD/USB Туре Staging Client Last Tested Published Latest Staged PDF417 StageNow 於結果 Recommended for 2D Scan Engines Linear StageNow Recommended for 1D Laser 🌄 Publish Stage Test Action Select Publish
- **19.** From the A13 device, select the **JSbarcode** option while generating the barcode.

Deploying XML Files and Passing Intents via SOTI

1. Open your browser and navigate to the provided link to launch the latest SOTI MDM console:<u>https://zebratech12.mobicontrolcloud.com/MobiControl/</u>.

2. Enter the Username and Password as sttester

SOTIONE ONE PLATFORM - CONNECTING EVERYTHING	
	Log In Please enter your credentials.
PROVEN MOBILITY MANAGEMENT	stester
	LOGIN

- 3. Click LOG IN.
- 4. Click the **Hamburger** icon in the top left corner.

5. Go to Configurations > **Policies** and click **File Sync**.

ſ

OTI MOBICONTROL Poli	licies			@ 4	sttester 🗸
0	Family: All 4† Filters: None V		Search Pol	licies ,0	NEW APP POLICY
~	APP POLICIES (1 - 50 of 452) 50 \checkmark Per Page \leftarrow 1 of 10 \rightarrow \bigcirc				
	POLICY NAME	FAMILY	APPS	CREATED DATE	ASSIGNED DATE
	✓	ndroid Plus	1	2024-11-07 6:31:31 PM	2024-11-07 6:31:44 PN
	✓ ⊘ 4562451	ndroid Plus	1	2024-11-07 6:47:11 PM	2024-11-07 6:47:48 PM
	♥ 🕢 4562452	ndroid Plus	1	2024-11-07 6:49:43 PM	2024-11-07 6:49:54 PN
NS	✔ 🔗 4562453	ndroid Plus	1	2024-11-07 7:55:27 PM	2024-11-07 7:55:45 PN
	✔	ndroid Plus	1	2025-01-08 8:26:51 AM	N/A
	✔ @ 4562455	🛱 Android Plus	1	2025-01-08 9:49:13 AM	N/A
	✓ Ø 49517	ntroid Plus	1	2024-12-27 2:40:57 PM	N/A
ings	✓ Ø 495171	🛱 Android Plus	1	2024-12-27 3:18:40 PM	N/A
rary	✓ Ø 495172	ntroid Plus	1	2024-12-27 3:24:14 PM	N/A
Permissions	✓ Ø 495173	🛱 Android Plus	1	2024-12-27 3:30:36 PM	N/A
ilth	✓ Ø 49518	🛱 Android Plus	1	2025-01-04 9:19:53 AM	N/A
NS es ings vary termissions lth hewces into a new group Dased on the	✓ <	Android Plus Android Plus	1 1 1 1 1 1 1 1 1 1 1 1 1 1	2024-11-07 6:31:31 PM 2024-11-07 6:49:43 PM 2024-11-07 6:49:43 PM 2024-11-07 7:55:27 PM 2025-01-08 8:26:51 AM 2025-01-08 9:49:13 AM 2024-12-27 2:40:57 PM 2024-12-27 3:18:40 PM 2024-12-27 3:24:14 PM 2024-12-27 3:30:36 PM 2025-01-04 9:19:53 AM	2024-11-07 6: 2024-11-07 6: 2024-11-07 6: 2024-11-07 7: N/A N/A N/A N/A N/A N/A N/A N/A

SOTI MOBICONTROL Poli	cies				() 🗘 🛛	sttester 🗸
Policies (Family:	All 🕴 Status: All 🗸		Search Poli	cies 🔎 🕂 NEW F	ILE SYNC POLICY
Apps	FILE SYN	IC POLICIES (1 - 250 of 517) 250 ∨ Per Page ← 1 of	3 → C		FILE MANAGE	R () ()
accessible on your devices		NAME	STATUS	FAMILY	DEVICE FILE / FOLDER NAME	DIR
Compliance		WI_Agent_permission	🕢 Assign	🛱 Android	%sdcard%	ц с
Customize criteria that define whether or not your devices are compliant		O Delegation_Scope_WI	⊘ Assign	n Android	%sdcard%	ط C
Enrollment		Combined_xml	⊘ Assign	🛱 Android	/sdcard/	th C
Create enrollment policies for devices that will be managed through MobiControl		⊘ wi_agent_combined	⊘ Assign	🛱 Android	/sdcard/	t∳ C
File Sync		⊘ A7_filesync	⊘ Assign	🛱 Android	%sdcard%	ψc
Firmware Management		⊘ combine	⊘ Assign	🛱 Android	/sdcard/	t∳ C
Create policies to manage updates for your devices		FW_upgrade_recovery_sdcard_CradleFW_5_1.zip	Ø Draft	🛱 Android	%sdcard%	ط C
Circul		O nim_filesync	O Assign	n Android	%sdcard%	th C
Signal Trigger automated actions based on configured		⊘ A14-A13_4490	⊘ Assign	🛱 Android	%sdcard%	ф С
		⊘ cope_sdcard	Assign	🛱 Android	%sdcard%	ц с
Device Relocation Relocate devices into a new group based on the		🔗 ps-xml download install apk	Assign	🛱 Android	%sdcard%	<i>(</i> ↓ ₁ E

6. Choose Android Plus, right-click the File Sync and select Create File Sync Rule.



7. Enter the policy Name and Description.

SOTI MOBICONTROL Polic	cies				0 4	sttester 🗸
Policies	Famil	『라 FILE SYNC POLICY Android		0	vlicies 🔎 🕂 NEW FIL	LE SYNC POLICY
Apps	FILE	1 SET UP POLICY (2) CONFIGURE	3 script 4 schedule		FILE MANAGER	
accessible on your devices		Start by giving a name and description to this	s File Sync Policy for Android devices.		DEVICE FILE / FOLDER NAME	DIF
Compliance		Details			%sdcard%	山
your devices are compliant		Name *	e.g. File Sync Corporate Devices		%sdcard%	山
Enrollment Create enrollment policies for devices that will		Description	e.g. Canada HQ Office		/sdcard/	山
be managed through MobiControl					/sdcard/	сĿ
File Sync					%sdcard%	сĿ
Firmware Management					/sdcard/	山
Create policies to manage updates for your devices					%sdcard%	പ
Signal					%sdcard%	പ്പ
Trigger automated actions based on configured conditions					%sdcard%	പ
Device Relocation			CANCEL	NEXT	%sdcard%	പ
Relocate devices into a new group based on the			OTTOLL		%sdcard%	rth

8. Click Next.

- 9. Download the file(s) from the Server to Devices as shown in the device path and file name below:
 - A8/A10 device: /sdcard/WFConnect/
 - A11/A13 Device: /enterprise/device/settings/WFConnect/

	es				② ⁴	8 sttester 🗸
Policies	Famil	FILE SYNC POLICY Android	0	Dicies		W FILE SYNC POLICY
Apps	FILE	SET UP POLICY - 2 CONFIGURE			FILE MAN	
Configure and Manage Apps that will be accessible on your devices		Configure this policy's storage and sync setti	ngs.		DEVICE FILE / FOLDER NAME	DIR
Compliance Customize criteria that define whether or not		File Settings			%sdcard%	th C
your devices are compliant		File Sync Type	Upload from Device Download from Server		%sdcard%	۵ لغ
Enrollment Create enrollment policies for devices that will		Server File / Folder Name *	%ROOT%\		/sdcard/	ىلەر ت
be managed through MobiControl		Device File / Folder Name *	%sdcard%		/sdcard/	(↓) [
File Sync		Use Subfolders for Files			%sdcard%	<u>(</u> ↓) [
Firmware Management		Curra Cattinara			/sdcard/	(J) €
Create policies to manage updates for your devices		Sync Settings			%sdcard%	<u>ل</u> ه ٦
Cinnel		Transfer Files When	Files are Different 🗸		%sdcard%	<u>ب</u> ۲
Signal Trigger automated actions based on configured		Sync Sub-Folders			%sdcard%	ت ل
		Sync Online Devices Now			%sdcard%	du C
Device Relocation Relocate devices into a new group based on the		BACK	CANCEL NEXT		%sdcard%	r∳n E

- **10.** Click the **Browse** icon and select the XML file to upload.
- **11.** Click **OK.**

≡ SOTI MOBICONTROL	Policies			⑦ ♫ R sttester ∨
Policies		/ Android	⑦ dicies	NEW FILE SYNC POLICY
Apps	FILE MANAGER		0	FILE MANAGER
Configure and Manage Apps that will be accessible on your devices	,O Search folders	Please avoid closing the browser while Upload or Do	ownload is in process.	/ FOLDER NAME DIR
Compliance	> Folders	FILES (1 - 3 of 3)	,0 wfc × 🖬	े ए।
Customize criteria that define whether or i your devices are compliant		NAM Import File		ं त्या
Enrollment Create enrollment policies for devices that		WFC File *	Browse File BROWSE	स् ।
be managed through MobiControl		WFC		ය් [
File Sync		WFC	CANCEL	्र (म ह
Firmware Management				ጥ ር
Create policies to manage updates for you devices				· ጥ ር
Signal				ං
Trigger automated actions based on confi conditions				ن بل ال
Device Relocation			CANCEL	, <u>с</u> , с

12. Navigate to the Rule Target tab and select your device.

- 13. Go to the Advanced Tab, and scroll down and click script.
 - a) Sending intent for A8/A10 device

```
sendintent -a
"intent:#Intent;action=wfc.voice.ACTION_NEW_CONFIG;S.profile_uri=/
sdcard/WFConnect/WFConnect.xml;end"
```

b) Sending intent for A11/A13 device

__chmod 777 /enterprise/device/settings/WFConnect/WFConnect.xml

```
sendintent -a
```

```
"intent:#Intent;action=wfc.voice.ACTION_NEW_CONFIG;S.profile_uri=/
enterprise/device/settings/WFConnect/WFConnect.xml;end"
```

Policies	Famil	FILE SYNC POLICY Android		0	olicies 👂 🕂 NE	W FILE SYNC POLICY
Apps Configure and Manage Apps that will be	FILE	SET UP POLICY - CONFIGURE	3 SCRIPT — 4 SCHEDULE		FILE MAN	AGER III (F5)
accessible on your devices		Enable Post-Sync Scrint		D	DEVICE FILE / FOLDER NAME	DIR
Compliance Customize criteria that define whether or not		endole i ose ogne ocnipe			%sdcard%	ت له
your devices are compliant		Script Type	Device Script Custom		%sdcard%	ىلە ت
Enrollment		Script Editor			/sdcard/	t C
create enrollment policies for devices that will be managed through MobiControl		<pre>1 sendintent -a "intent:#Intent</pre>	;action=wfc.voice.ACTION_NEW_CONFIG;S.profil	e_u	/sdcard/	ٿ ل
File Sync				-	%sdcard%	ୟ ୮
Firmware Management					/sdcard/	ت له
Create policies to manage updates for your devices					%sdcard%	ڪ (
Signal					%sdcard%	<u>ل</u> ه د
Trigger automated actions based on configured conditions		Execute Script Only if Files Transmitted	Q		%sdcard%	ط c
Device Relocation		PACK	CANCEL	NEVT	%sdcard%	ى ئ
Relocate devices into a new group based on the		DACK	CANCEL	NEXT	%sdcard%	r↓n ⊂

M

NOTE: The process of uploading XML files and specifying the intent in the script section varies depending on the XML files and the operating system. Proceed to the next page for detailed instructions on which XML files to add and the actions to perform for different Zebra applications and OS platforms.

14. After providing the script, click **OK**.



E SOTI MOBICONTROL Policies 2 4 R strester -						
Policies	Famil	FILE SYNC POLICY Android		0	licies P New Fil	E SYNC POLICY
Apps	FILE		script — 4 schedule		FILE MANAGER	
		Schedule this policy as per Device Updates or set a	a Custom Schedule.		DEVICE FILE / FOLDER NAME	DIR
Compliance		Details			%sdcard%	<u>ل</u> ا د
		Schedule Type *	Device Update Custom		%sdcard%	<u>ب</u> د
Enrollment Create enrollment policies for devices that will					/sdcard/	de c
be managed through MobiControl					/sdcard/	بل C
File Sync					%sdcard%	ت ل
Firmware Management					/sdcard/	ڪ ٿ
					%sdcard%	<u>ب</u> ۲
Signal					%sdcard%	de C
					%sdcard%	<u>ل</u> ه د
Device Relocation		BACK	CANCEL SAVE AND ASSIGN SAV	E	%sdcard%	<u>ب</u> د
					0/edeard0/	

Deploying XMLs and Intents for Workcloud Communication Applications Using StageNow

Zebra PTTPro

- XML File Name: activate_key.xml
- A8/A10 device: /sdcard/
 - script to be passed: mxconfig /sdcard/activate_Key.xml
- A11/A13 device: /enterprise/device/settings/pttpro/
 - script to be passed:
 - chmod 777 /enterprise/device/settings/pttpro/activate_Key.xml
 - mxconfig /enterprise/device/settings/pttpro/activate_Key.xml

SOTI MobiControl

E SOTI MOBICONTROL Policies 🕐 🗘 🗷 attester 🗸							
Policies	Famil	FILE SYNC POLICY Android			? dic	ies 🔎 🕈	NEW FILE SYNC POLICY
Apps Configure and Manage Apps that will be	FILE	SET UP POLICY	— 3 SCRIPT — 4 SC	CHEDULE	Ц	FILEN	JANAGER 🔟 🎼
Compliance		Enable Post-Sync Script				DEVICE FILE / FOLDER NAME	DIR 산 C
your devices are compliant		Script Type	Device Script	Custom		%sdcard%	را ب
Enrollment		Script Editor				/sdcard/	ط C
be managed through MobiControl		1 sendintent -a "intent:#intent	;action=wfc.voice.ACTION_NEW_)	CONFIG;S.profile_u		/sdcard/	جې (
File Sync						%sdcard%	جې (
Firmware Management						/sdcard/	ې ۲
Create policies to manage updates for your devices						%sdcard%	ج (
Signal						%sdcard%	جې (۲
Trigger automated actions based on configured conditions		Execute Script Only if Files Transmitted				%sdcard%	جې (۲
Device Pelocation		DACI			- 1	%sdcard%	ط C
Relocate devices into a new group based on the		BAUN		CANCEL NEXT		%sdcard%	r↓n E

- XML File Name: Config-reset.xml
- A8/A10 device: /sdcard/
 - script to be passed: mxconfig /sdcard/Config-reset.xml
- A11/A13 device:/enterprise/device/settings/pttpro/
 - script to be passed:
 - chmod 777 /enterprise/device/settings/pttpro/Config-reset.xml
 - mxconfig /enterprise/device/settings/pttpro/Config-reset.xml

≡ SOTI MOBICONTROL Policies			
Policies	Famil 🛱 FILE SYNC POLICY Android	🕐 ticies 🔎 🕈	NEW FILE SYNC POLICY
Apps Configure and Manage Apps that will be accessible on your devices	FILE SET UP POLICY - CONFIGURE - 3 SCRIPT - 4 SCHEDULE		
Compliance Customize criteria that define whether or not	Enable Post-Sync Script	%sdcard%	عالم المراجع (المراجع المراجع ا مراجع المراجع ال
your devices are compliant Enrollment Create enrollment policies for devices that will	ScriptEditor 1 sendintent -a "intent:#Intent;action=wfc.voice.ACTION_NEW_CONFIG;S.profile_u	%sdcard% /sdcard/	بة 10 بالا 10 بالا 10
be managed through MobiControl		/sdcard/ %sdcard%	بط C بط C
Firmware Management Create policies to manage updates for your devices		/sdcard/ %sdcard%	ب در بن د
Signal Trigger automated actions based on configured conditions	Execute Script Only if Files Transmitted	%sdcard% %sdcard%	ں لیے 1 لیے
Device Relocation Relocate devices into a new group based on the	BACK CANCEL NEXT	%sdcard% %sdcard%	بل C بل C

Zebra Voice Client

• XML File Name: WFConnect.xml

A8/A10 device

sendintent -a

```
"intent:#Intent;action=wfc.voice.ACTION_NEW_CONFIG;S.profile_uri=/sdcard/
WFConnect/WFConnect.xml;end"
```

- A11/A13 device
 - script to be passed:
 - chmod 777 /enterprise/device/settings/WFConnect/WFConnect.xml

```
sendintent -a
intent:#Intent;action=wfc.voice.ACTION_NEW_CONFIG;S.profile_uri=/
enterprise/device/settings/WFConnect/WFConnect.xml;end
```

Profile Manager

For A8/A10/A11 device

json file: key.json

- To push key.json to device
 - json file: key.json
- Script
 - chmod 777 /enterprise/device/settings/key.json

E SOTI MOBICONTROL Policies ② L, 🔊 sttester 🗸				
Policies	amit I FILE SYNC POLICY Android	⑦ vicies	P + NEW FI	LE SYNC POLICY
Apps Configure and Manage Apps that will be	ILE SET UP POLICY - CONFIGURE - 3 SCRIPT -	(4) SCHEDULE	FILE MANAGE	
accessible on your devices			DEVICE FILE / FOLDER NAME	DIR
Compliance	Enable Post-Sync Script		%sdcard%	بل ۵
Customize criteria that define whether or not your devices are compliant	Script Type Device Script	Custom	%sdcard%	ला (
Enrollment	Script Editor		/sdcard/	ط C
Create enrollment policies for devices that will be managed through MobiControl	<pre>1 sendintent -a "intent:#Intent;action=wfc.voice.</pre>	ACTION_NEW_CONFIG;S.profile_u	/sdcard/	ىلەر ت
File Sync			%sdcard%	ط C
Firmware Management			/sdcard/	<u>را</u> د
Create policies to manage updates for your devices			%sdcard%	<u>ل</u> ان (
Simul			%sdcard%	<u>را</u> ب (1
Trigger automated actions based on configured conditions	Execute Script Only if Files Transmitted		%sdcard%	<u>را</u> ب (
Durin Delevation		_	%sdcard%	ය් ස
Relocate devices into a new group based on the	ВАСК	CANCEL NEXT	%sdcard%	r4n D

Intent to enroll device to PTTPro server and PFM server

sendintent -a "intent:#Intent;action=com.zebra.dfs.ACTION_ENROLL_DEVICE;S.
store=<store_name>;end"

sendintent -a "intent:#Intent;action=com.zebra.dfs.ACTION_ENROLL_DEVICE;end"

sendintent -a "intent:#Intent;action=com.zebra.dfs.ACTION_ENROLL_DEVICE;S.
store=<store_name>;end"

Deployment Intent for PVM Token Parameters via SOTI

```
sendintent -a "intent: wfctp-uat://
PTT_Pro_All#Intent;action=android.intent.action.VIEW;component=
com.symbol.wfc.pttpro;end"
```

STAGENOW

Install, Upgrade, and Uninstall Zebra Apks from StageNow to DUT

- **1.** Launch the Stage Now Application.
- 2. Click Create a New Profile.
- 3. Select MX version **MX > 9.0** or according to the device's MX Version.
- 4. Click Xpert Mode.
- 5. Click the Create button.
- 6. Enter the Profile Name and click Start.
- 7. From the Settings list, select **FileMgr & AppMgr** and click + icon.
- 8. Click Add.
- 9. FileMgr:
 - a. File Action: Transfer/Copy File
 - b. Target Access Method: File in the device file system
 - c. Target Path and File Name:
 - d. Source Access Method: File on a remote server
 - e. Source File URI: Click on and select the APK file on your system

Figure 1 Staging Server

Staging Se	wer:
Built In	×
Select a Fil	e
C:\Users\PN	6664\OneDrive - Zebra Technologies\Desi

10. Click **Continue** to move to the next section, **AppMgr**.

- 11. Application Action: Install/Upgrade
- 12. To Install/Upgrade:
 - a. APK Path and Name

A8/A10/A11 device: /sdcard/<file_name.apk> or /data/tmp/public/ <file_name.apk>

- a. Access to App Info Action: Do nothing
- b. App Feature Action: Do nothing



NOTE:

13. Click **Continue** > **Complete Profile**.

Install, Upgrade, and Uninstall Zebra Apks from StageNow to DUT without FileMgr

- 1. Click Create a New Profile.
- 2. Select MX version MX > 9.0 or according to the device's MX Version.
- 3. Click the Create button.
- 4. Click Xpert Mode.
- 5. Enter the Profile Name and click Start.
- 6. From the Settings list, select **AppMgr** (Perform application (APK) management), and click the + Icon to add.
- 7. Enter the required data and click Add.
- 8. To install/upgrade, copy and paste the following path:

```
A8/A10/A11 device: /sdcard/<file_name.apk>
```

or

/data/tmp/public/<file_name.apk>



NOTE: You must copy the APK to either the /sdcard/ or /data/tmp/public/ location on the DUT.

- **9.** To uninstall, provide the Application Package Name only.
- **10.** Click **Continue** and then click **Complete Profile**.
- 11. Select the barcode type **PDF417 StageNow** checkbox, and then click **Test** button to generate the StageNow barcode.
- 12. Launch the StageNow App from the DUT and scan the generated barcode.

Deploying XML File into Specified Path

- 1. Click Create a New Profile.
- 2. Select MX version MX > 9.0 or, according to the device's MX Version.
- 3. Select Xpert Mode and click Create . Enter the Profile Name.
- 4. Click the Start button, select the FileMgr, and click Add (+).
- 5. Enter target path and file name.

/sdcard/WFConnect/WFConnect.xml

- 6. Select the source file and click Continue, then Complete Profile.
- 7. Select the barcode and click TEST.
- 8. Scan the generated barcode using the StageNow application on the device.

Deploying XML Files and Configuring Intents to Designated Paths

The following steps are for configuring intent from the StageNow server considering Workcloud Communication Voice.

- 1. Click Create a New Profile.
- 2. Select MX version MX > 9.0 or according to the device's MX Version.
- 3. Select Xpertmode and click Create.
- 4. Enter a Profile Name and click Start.
- 5. Select FileMgr and click Add (+).
- 6. Select the Intent and click Add (+).
- 7. Click Add FileMgr.
- 8. Enter the target path and file name as

/sdcard/WFConnect/WFConnect.xml

Table 1 Intent Definition

Name	Description
Action	wfc.voice.ACTION_NEW_CONFIG
Intent Type	startActivity
Extra 0	This extra parameter defines the URI of the configuration file.
Туре	String
Name	profile_uri
Value	/sdcard/WFConnect/WFConnect.xml

9. Click Continue , then Complete Profile.

- 10. Select the barcode type PDF417 StageNow checkbox, then click the Test button to generate the StageNow barcode.
- **11.** Launch the **StageNow** app from the DUT and scan the generated barcode.

Deploying XMLs and Intents for Workcloud Communication Applications Using StageNow

Zebra PTTPro (PVM Token)

- XML File Name: activate_key.xml or Config-reset.xml or activate_ESN.XML.
- Target Path and File Name
- A8/A10 device: /sdcard/pttpro/<file_name.xml>
- A11/A13 device: /enterprise/device/settings/pttpro/<file_name.xml>

Table 2Intent Definition

Name	Description
Android Action	android.intent.action.VIEW
Intent Type	startActivity
Package Name	com.symbol.wfc.pttpro
URI	wfctp-uat://Dyna_latest_pro
Extra 0	None
Туре	None
Name	None
Value	None

Zebra PTTPro (Deploying JSON)

- **1.** Create a Profile and Add File Manager and intent, as shown in the following table.
- 2. Click Continue.

Table 3Intent Definition

Name	Description	
File Action	Transfer/Copy File	
Target access method	File in the device file system	
Target path and file name	<pre>/enterprise/device/settings/pttpro/ WFCPTTProDefault.json (Change the location based on android OS version)</pre>	
Android Action Name	com.symbol.wfc.pttpro.ACTION_DEFAULT_CONFIG	
URI	Upload the json file	
Intent Type	Broadcast	
Extra 0	0	

Table 3 Intent Definition (Continued)

Name	Description
Туре	0
Name	configpath
Value	<pre>/enterprise/device/settings/pttpro/ WFCPTTProDefault.json (Change the location based on android OS version)</pre>

Zebra Voice Client

- XML File Name: WFConnect.xml.
- Target Path and File Name
 - A8/A10 device: /sdcard/WFConnect/<file_name.xml>
 - A11/A13 device: /enterprise/device/settings/WFConnect/<file_name.xml>

Table 4Intent Definition

Name	Description
Android Action	wfc.pttpro.ACTION_NEW_CONFIG
Intent Type	startActivity
URI	wfctp-uat://Dyna_latest_pro
Extra 0	None
Туре	String
Name	profile_ur
Value	0

Assigning or registering a Device to a Site via StageNow

to assign/register:

- 1. Click Create New Profile, select MX version , thenXpert Mode, and click Create.
- 2. Provide the Profile Name and click Start.
- **3.** Select Intent, click **Add** and provide the intent details as described in the following table:

Table 5 Intent Details

Name	Description
Action	StartActivity
Android Action Name	android.intent.action.VIEW
Package Name	com.symbol.wfc.pttpro
Token Name	Uri (example: wfctp-uat: //3rdParty)

4. Click Continue , then Complete profile.

5. Generate the barcode.



www.zebra.com