Visibility IQ Foresight Technical Best Practicses

Zebra Managed & Integration Services Team (EMEA)
Date: June 2023

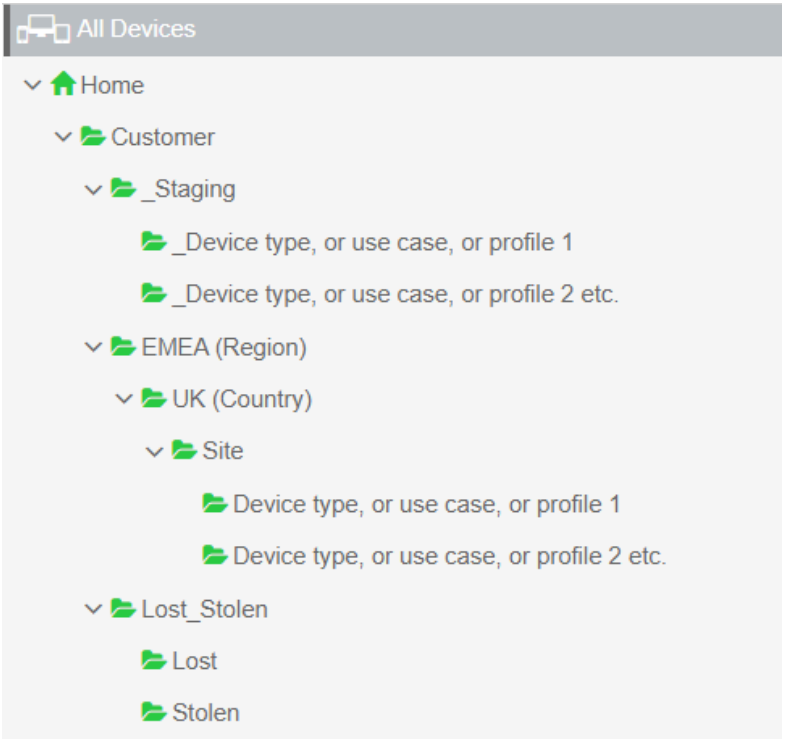
Table of Content

Common Information

Compliant Device Group Structure (site hierarchy)

Visibility IQ Foresight Reporting VIQ dashboard relies on customer site names as a data field to properly display certain reports (Case Backlog, Case Archive, Repair Depot, Active Devices, etc.). Site names are held in several different back-end systems. The Visibility IQ Foresight reporting dashboard gathers site names from each of those systems. When those site names do not match from system to system the VIQ dashboard treats them as different sites.
Note:
Best practice is to use the below Device Group structure information. This does not impact customers using VIQF Connect.
Below are some examples showing the different levels of the VIQ complaint / default site hierarchy.

Level 1	*Level 2*	*Level 3*	*Level 4*	*Level 5*
Customer				
	_Staging			
		_Device type, or use case, or profile 1		
		_Device type, or use case, or profile 2 etc.		
	EMEA (Region)			
		UK (Country)		
			Site (Reported as Site Name in the VIQ portal)	
				Device type, or use case, or profile 1
				Device type, or use case, or profile 2 etc.
	Lost_Stolen			
		Lost		
		Stolen		



_Staging

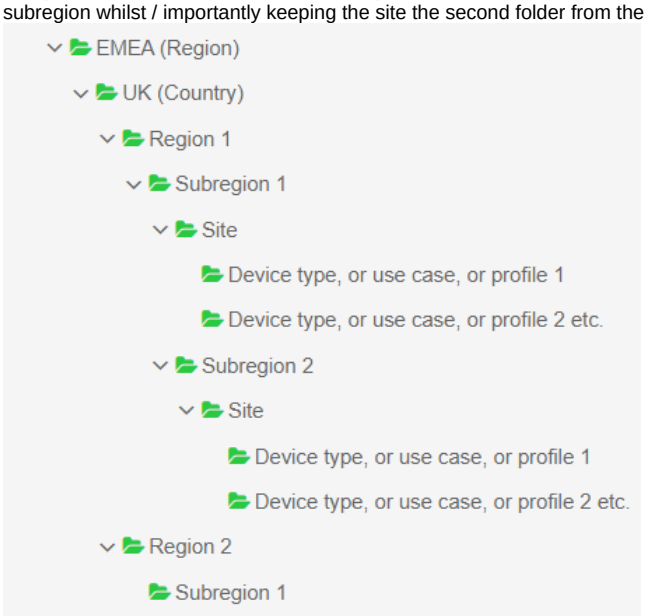
The _Staging folder is used to stage devices and separate newly staged devices from those being utilized on site to keep reports in VIQ accurate**.**
Relocation rules can be setup to target staging folder(s), and automatically relocate devices to site folders using a specified IP range.
_ is used as a prefix to hide folder(s) from the VIQ portal, all subsequent folders need to begin with an _ as seen in the examples.
_Staging can also be used as a testing area.

Region / Country

For the reports to be shown correctly in the VIQ portal these folders are needed. For multi-region / multi-country customers expand the site hierarchy as required. For single region / single country customers leave these folders as setup.
Regions being NA (North America), LATAM (Latin America), EMEA (Europe, the Middle East and Africa) and APAC (Asia and the Pacific Region countries).

Site

The VIQ portal is getting the site name from the second folder from the bottom of the structure.
To manage multiple device types, or use cases, or profiles, create multiple folders directly under the site level as seen in the examples.
If required, the hierarchy can be further expanded between the country and site levels. The example below shows the addition of multiple region and subregion whilst / importantly keeping the site the second folder from the bottom of the structure.



Lost_Stolen

To ensure the reports in VIQ are accurate, devices known to be either lost or stolen should be relocated to the applicable folder.
Further configuration can be applied to these folders to wipe, lock, or display a return address / contact number in the event that they later come online.

ZDS (Zebra Data Services)

Zebra Data Service (ZDS) is a service running in the background continuously and is responsible for collecting and uploading the data coming from ZDS Plugins or any third-party apps (Zebra authorized apps). ZDS uses HTTPS as secure transport protocol. ZDS is also responsible of updating the ZDS plugin apps and itself. Users can scan a barcode to configure certain settings of ZDS and its plugins like upload intervals and events.
ZDS stores all the data into the database and uploads everything every 24hr (or whatever is the upload frequency is defined in the system configuration, but it cannot be less than 5 mins). Few Limitations for Data upload and storage which is configurable:

- Only ~ 70 KB of data will be collected per day.
- Only ~ 2 MB of compressed data will be uploaded per day. This higher limit will allow ZDS to upload cached data in case ZDS was not able to upload data on previous days.
- Only 5MB of data can be stored into the ZDS database. In case this limitation occurs, the old data will be deleted and replaced by new data.

> ZDS is enabled out of Box, if the device has access to internet, data will be uploaded to the server. Information on how ZDS can be disabled is mentioned in further sections. It is recommended to explicitly configure ZDS to be enabled in cases of prior staging in case ZDS was disabled. On later versions of Android there is a UI in which a user could disable ZDS data collection. Zebra suggests locking this out as well. Both enabling and locking out the UI can be done via MX (StageNow) AnalyticsMgr CSP.

VIQF requires at least ZDS agent version: 3.5 or newer.
If ZDS is older you need to update ZDS on device manually. Download the ZDS agents from below url's:

- https://analytics.zebra.com/da-binaries/latest/apk/com.symbol.dataanalytics.apk
- https://analytics.zebra.com/da-binaries/latest/apk/com.symbol.dataanalytics.dca.apk

If ZDS agent is on v3.5 or newer the ZDS agent will be updated from time to time using LifeGuard Service. It is recommended to always use the latest LifeGuard patch available for the Zebra Android Device in use.
All collected data will be uploaded to below server:

ZDS Server #1:

- **URL**: https://analytics.zebra.com
- **IP Address**: 104.198.59.61
- **Port**: 443

ZDS Server #2:

- **URL**: https://device-https.savannacore.zebra.com
- **IP Address**: 34.68.84.87
- **Port**: 443 *This server uses Certificate-based Mutual Authentication.*

> Devices must be able to connect to above URL, which requires internet connection or proxy configured on device to route the traffic to the analytics server.

If additional information such as GPS and WLAN data should be visible on VIQ portal, use below StageNow barcodes to enable the additional data collection.
On older devices e.g., MC18 with Lollipop (5.1.1 and latest LifeGuard Patch) does not have ZDS agent v3.5. It comes with ZDS agent v1.0. However, it should be possible to install v3.5 from above mentioned URL's to be used with VIQ.

> ZDS is used by VIQF for Lifeguard Analytics Report, and advanced reporting such as Smart Battery, Application Analytics, Barcode Scan Analytics, Device Disruption Analytics, etc.

Below machine data will be collected:

- About Machine Data see https://www.zebra.com/content/dam/zebra_new_ia/en-us/channel/terms-conditions/na/zebra-restricted-eula-170515.pdf

Standard Data

- Device Info & Device Utilization
- BSP, LG patch & Security patch levels
- RAM available
- Flash info & health
- Battery info & health
- Data Traffic statistics: Wi-Fi / Cellular / Bluetooth / Ethernet
- WLAN Connectivity Info
- WWAN Connectivity Info
- Apps Info and usage
- Additional Apps Info (Value-adds): MX STATS, SimulScan, EMDK, Data Wedge, EHS, StageNow
- Scanner Info and statistics
- Reboots – system and app caused

- ANR
- CPU, Memory usage (Planned)

Optional - based on specific services

- Location: Cellular, GPS
- Location: WLAN, Bluetooth (Planned)

Optional - Available since 2023

- CPU stats in Zagent_CPU_Stats table for A10 and above.
- Memory per app collection
- storage per app.
- doze_mode events
- Low Mem alerts
- Scan to Application (Identifies the app that is calling the Scanner)
    - Dependent on Datawedge version (8.2.211 and above)
- Fall detection

Reference Material:

- About Zebra Data Service - TechDocs
- Available Product Documentation - Zebra Technologies TechDocs
- Full MX Feature Matrix - TechDocs (zebra.com)
- Analytics Manager - TechDocs (zebra.com)
- Power Manager - TechDocs (zebra.com)
- Getting Started - Zebra Technologies TechDocs

Security

Common overview

Once a device is successfully enrolled into an EMM it should be secured from threads, unauthorized access to sensitive information, etc.
It is important to further protect the devices by applying policies to protect device hardware, networks which will be used to communicate, applications, websites, etc.
To secure the different layers see below checklist:

- Hardware/OS – Layer
  - Enforce complex password policies
  - Enforce encryption of internal/external SD Cards
  - Disable USB Access
  - Apply the latest Zebra LifeGuard patches for your Zebra Android Device

- Application – Layer
  - Use a lockdown screen
  - Update/Patch your applications
  - Disable sideloading applications. Always use an EMM to provisioning applications or use the Google Play Store.
  - Blacklist all unapproved applications on BYOD (Bring Your Own Device) or COPE (Company-owned personally enabled) devices.

- Content – Layer
  - Use an EMM email gateway for Exchange email, if any.
  - Enforce application sharing restrictions to prevent data leakage from business applications and email accounts.
  - Use of an EMM secure document manager and secure web browser to grant secure access to corporate files and websites.

- Communication – Layer
  - Disable Bluetooth pairing if not required on the device.
  - Configure and enforce VPN per application if available.
  - Whitelist Wi-Fi access points.

- Thread – Layer
  - Use an EMM secure web browser and block access to unapproved categories of websites (e.g., gambling, websites) or websites with invalid certificates.
  - Enable/Configure antivirus protection.

Maximizing Device Security for Android Enterprise device

Having the best EMM and Device OS in place does not make sense if certain security options are not turned on and provides device users to break out of lock screens or turn off management capabilities, etc.
To maximize device security below device settings should be considered and activated/deactivated. On any EMM supporting Android Enterprise a profile must/can be created to configure below settings/payloads:

- Ability to Safe Boot (Power Menu): Should be deactivated, unless required for troubleshooting.
- Ability to Factory Reset option (Settings app): Should be deactivated.
- Factory Reset Protection: Should be activated. Once device is factory reset, valid Google account credentials needs to be entered to re-use the device. Note: Not required if device is registered with GZT (Google Zero Touch).
- Ability to turn on Debug Mode: Should be deactivated, unless required for troubleshooting.
- Ability to use USB File Sync: Should be deactivated, unless required for troubleshooting.
- Ability to turn on Tethering: Should be deactivated.
- Adding an EMM lock screen or using at least Zebra EHS (Enterprise Home Screen).

OS / Firmware Updates for devices (LG OTA [FOTA {Firmware Over The Air}]

Zebra recommends updating the device OS / LifeGuard level regular. This helps ensuring the device has the latest fixes/patches, features available. If supported by EMM / MDM the best option is to use Zebra FOTA service by connecting the EMM / MDM to the Zebra FOTA or LifeGuard Service. This requires a Zebra User Account with a valid Z1C (Zebra One Care) contract.
Details, if FOTA (LG Updates) are available, can be obtained from the EMM / MDM provider. Below EMM / MDM vendor supports FOTA:

- 42gears / Sure MDM, v6 or newer
- Soti / MobiControl, v15.3 or newer

Additional information:

- Soti MobiControl
  - Using LifeGuard OTA for Upgrading Firmware on Zebra Devices (soti.net)
- 42gears SureMDM
  - Zebra LifeGuard OTA Updates (42gears.com)
- Zebra Techdocs
  - About Zebra LifeGuard for Android - TechDocs

GPS for location report on VIQ dashboard

Using the location report on the VIQ dashboard requires location data collected from devices either by location data collected by EMM or ZDS agent. If the device is not equipped with an GPS radio, location data cannot be collected at all. If a GPS radio is available on some EMM's the device needs to be configured to allow GPS data collection. Please refer to the EMM documentation to learn more.
If devices used inside a building it might be possible a geo location cannot be calculated and therefore locating is not available.

EMM / MDM specific

Device agents (42gears)

Device agents for different OS types can be downloaded from below link:
42Gears Products - Instant Download Page
Please use at least Android agent version 27.15.05 or newer.

Device agents (Soti MobiControl)

Device agent for different OS types can be downloaded from below link:
Soti Download Page

Network / Firewall

This chapter describes the required network ports and firewall settings for different MDM tool providers
If EMM/MDM is hosted on premise see below link to ensure Google Android Enterprise Management works as expected: Android Enterprise Network Requirements - Android Enterprise Help (google.com)

42gears SureMDM (GCP cloud)

If your devices are behind an enterprise firewall, the following ports and URLs must be allowed to enable smooth communication while using SureMDM. Below is the list of services along with ports used by mentioned services,

- **SureMDM Services -** These services are used for secured and encrypted communication between SureMDM enrolled devices and SureMDM Web Console.
- **SureMDM Remote Support -** SureMDM offers a secure way to remotely view and control enrolled devices using SureMDM Web Console.
- **Firebase cloud messaging -** Google Cloud Messaging (Firebase Cloud Messaging) by Google helps SureMDM server to send secure notifications to enrolled devices. Google uses any of these mentioned ports.
- **Zero Touch Enrollment**: Zero-touch enrollment allows enterprises to provision Android devices by assigning enterprise configuration and security policies right out of the box.
- **Play Services and Android Management -** Google Play services are used to securely update Google apps and apps from Google Play. It is also used for the communication and management of Android Enterprise (Work Managed Device) devices.
- **Samsung KNOX Enrollment -** Samsung KNOX Enrollment is used for Samsung Account authentication for Knox service and for access of enterprise devices to the Knox servers.
- **iOS APNS -** iOS APNS enables secure communication of iOS and/or macOS devices through the SureMDM servers. This also enables third-party apps to send push notifications to iOS devices.
- **Apple services -** Apple services are used for Apple's Mobile Asset Software Update service to provide an XML file with information about available iOS updates.
- **Microsoft services for Windows -** This service is used for Windows notification service by Microsoft which allows secure communication between SureMDM and Windows devices.
- **Office 365 services -** This service is used for managing Windows devices and services behind firewalls and enables secure communication.

The following table explains the communication data pointers for SureMDM:

Server	Domain Name	IP Address	Ports
Zebra MDM Server (NA)	zebramdm.42gears.com	34.102.188.231	80, 443
Zebra MDM Server (EMEA)	zebrams003.eu.suremdm.io	34.111.123.140	
Firebase Cloud Messaging	All traffic or Google's ASN of 15169	List is present here: https://ipinfo.io/AS15169	443, 5228, 5229, 5230
Play Services and Android Management	*.ggpht.com		443
	*.googleusercontent.com		443
	*.gvt1.com		443
	*play.googleapis.com		443
	android.clients.google.com		443
Zero Touch Enrollment	www.googleapis.com		443
Samsung KNOX Enrollment	*.samsung.com		443
	*.samsungknox.com		
	*.secb2b.com		
iOS APNS	17.0.0.0/8		5223, 2195 - 2197
Apple services	mesu.apple.com		443
Microsoft services for Windows	*.notify.live.net		443
	*.notify.windows.com		
	*.wns.windows.com		
Office 365 services	*.manage.microsoft.com		443
	*api.office.com		
	*go.microsoft.com		
	*login.windows-ppe.net		
	*secure.aadcdn. microsoftonline-p.com		
	*vortex.data.microsoft. com		

42gears SureMDM (AWS cloud)

42gears hosts SureMDM instances on it's own SaaS environment. This environment outside of the Zebra VIQF scope.

If your devices are behind an enterprise firewall, the following ports and URLs must be allowed to enable smooth communication while using SureMDM. Below is the list of services along with ports used by mentioned services,

- **SureMDM Services -** These services are used for secured and encrypted communication between SureMDM enrolled devices and SureMDM Web Console.
- **SureMDM Remote Support -** SureMDM offers a secure way to remotely view and control enrolled devices using SureMDM Web Console.
- **Firebase cloud messaging -** Google Cloud Messaging (Firebase Cloud Messaging) by Google helps SureMDM server to send secure notifications to enrolled devices. Google uses any of these mentioned ports.
- **Zero Touch Enrollment**: Zero-touch enrollment allows enterprises to provision Android devices by assigning enterprise configuration and security policies right out of the box.
- **Play Services and Android Management -** Google Play services are used to securely update Google apps and apps from Google Play. It is also used for the communication and management of Android Enterprise (Work Managed Device) devices.
- **Samsung KNOX Enrollment -** Samsung KNOX Enrollment is used for Samsung Account authentication for Knox service and for access of enterprise devices to the Knox servers.
- **iOS APNS -** iOS APNS enables secure communication of iOS and/or macOS devices through the SureMDM servers. This also enables third-party apps to send push notifications to iOS devices.
- **Apple services -** Apple services are used for Apple's Mobile Asset Software Update service to provide an XML file with information about available iOS updates.
- **Microsoft services for Windows -** This service is used for Windows notification service by Microsoft which allows secure communication between SureMDM and Windows devices.
- **Office 365 services -** This service is used for managing Windows devices and services behind firewalls and enables secure communication.

The following table explains the communication data pointers for SureMDM:

Port	Destination	Type	Protocol	Description
443	**SAAS:** suremdm.42gears.com or yourdomain.suremdm.io **On Premise:** your on-premises server URL	Outbound	HTTPS	SureMDM Services
80 (optional)	Same	Outbound	HTTP	SureMDM Services
443	Same	Outbound	TLS or WSS	SureMDM Remote Support
80 (optional)	Same	Outbound	TCP or WS	SureMDM Remote Support
443	s3.amazonaws.com	Outbound	HTTPS	Jobs, Reports, File store and <ac:structured-macro ac:name="unmigrated-wiki-markup" ac:schema-version="1" ac:macro-id="9254fc7f-27ef-43f0-894e-d0ff2f1f60fb"><ac:plain-text-body><![CDATA[Application store. [For 3 Url, select]]></ac:plain-text-body></ac:structured-macro> one, based on your SAAS region or On-Premise S3 bucket]
	suremdm-usstorage.s3.amazonaws.com			
	suremdm-eustorage.s3-eu-west-1.amazonaws.com			
	suremdm-instorage.s3.ap-south-1.amazonaws.com			
	<your-s3-bucket>.<aws-region>.amazonaws.com			
	mars.42gears.com			
443, 5228, 5229, 5230	All traffic or Google's ASN of 15169	Outbound	TLS /HTTPS	Firebase cloud messaging
443	www.googleapis.com	Outbound	HTTPS	Zero Touch Enrollment
443	*.ggpht.com	Outbound	HTTPS	Play Services and Android Management
	*.googleusercontent.com	Outbound		

	*.gvt1.com	Outbound		
	*play.googleapis.com	Outbound		
	android.clients.google.com	Outbound		
443	*.samsung.com	Outbound	HTTPS	Samsung KNOX Enrollment
	*.samsungknox.com	Outbound		
	*.secb2b.com	Outbound		
5223, 2195 - 2197	17.0.0.0/8	Outbound	TLS /HTTPS	iOS APNS
443	mesu.apple.com	Outbound	HTTPS	Apple services
443	*.notify.live.net	Outbound	HTTPS	Microsoft services for Windows
	*.notify.windows.com	Outbound		
	*.wns.windows.com	Outbound		
443	*.manage.microsoft.com	Outbound	HTTPS	Office 365 services
	*api.office.com	Outbound		
	*go.microsoft.com	Outbound		
	*login.windows-ppe.net	Outbound		
	*secure.aadcdn. microsoftonline-p.com	Outbound		
	*vortex.data.microsoft. com	Outbound		

Most recent table can be found at: https://docs.42gears.com/suremdm/docs/SureMDM/CommunicationDataPoints.html

Soti MobiControl (cloud & on-premises)

To allow devices to communicate with the cloud based MobiControl deployment server and in case you want to locate a device, build an MDM device agent (MS WinMob/CE only) or want to enroll devices using the Soti Enrollment Service (Enrollment ID from Add Device rule) you might need to add rules to your local firewall.

SOTI Services

The SOTI Services include the Activation Service, the Agent Builder Service, the Enrollment Service, and the Location Service. These services help to ensure that your MobiControl deployment is provided with:

- the latest certified version of device agents
- fast and easy enrollment of devices
- updates for licenses

All SOTI services are accessed using HTTPS on port 443. It is important to ensure that the following fully qualified domain names and/or IP addresses are whitelisted with your firewall, allowing unrestricted communication between your MobiControl deployment and the SOTI data center.

Service Name	Service URL
Activation Service	activate2.soti.net
Agent Builder Service (MS WinMob/CE only)	activate2.soti.net
Enrollment Service	mc-enroll.soti.net
Location Service	location2.soti.net

The SOTI Services are load-balanced across the following IP addresses:

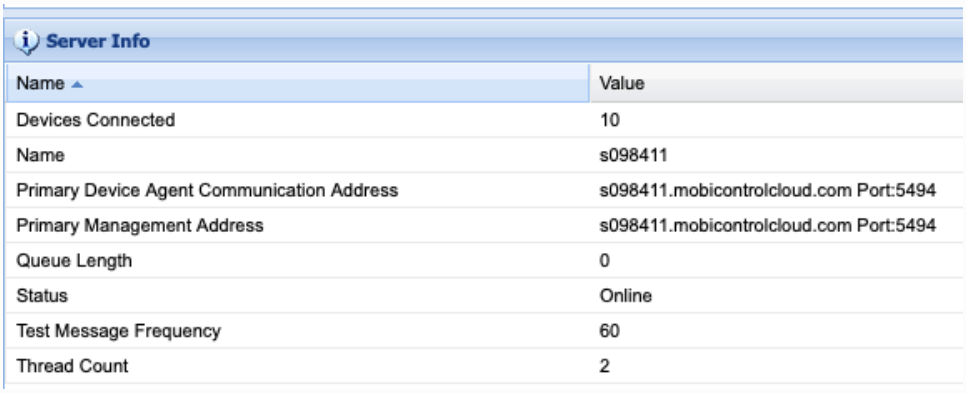
Public IP Addresses
54.208.149.103
54.208.194.169
54.209.62.205
54.209.186.178
54.209.186.251
54.209.207.237

https://www.soti.net/mc/help/v14.4/en/index.html#setup/installing/soti_services.html

Network Ports

MobiControl uses the following ports to communicate between the various system components. See in red color the Device to Deployment Server ports.

Deployment Server IP is accessible from the MobiControl Web Console. See sample below:



Server Info

Name	Value
Devices Connected	10
Name	s098411
Primary Device Agent Communication Address	s098411.mobicontrolcloud.com Port:5494
Primary Management Address	s098411.mobicontrolcloud.com Port:5494
Queue Length	0
Status	Online
Test Message Frequency	60
Thread Count	2

For an interactive guide to MobiControl network connections, see the MobiControl network configuration diagram.

Deployment Server Connections

Below table shows all ports used by Soti MobiControl MDM. The ports mentioned in green color reflects the ports used in a cloud-based environment.

Component Name	Protocol	Port(s)
MobiControl Deployment Server For deployments with multiple deployment servers, for caching purposes.	Binary	5495
MobiControl Management Server	Binary	5494/5495
Amazon App Store	HTTPS	443
Apple Push Notification Service (APNS)	Binary	2195/2196
Apple DEP	HTTPS	443
Apple VPP	HTTPS	443
Certification Authority - DCOM Must be on the same domain	Binary	Dynamic
Certification Authority - HTTP	HTTPS	443
Google Play	HTTPS	443
iTunes	HTTPS	443
LDAP	LDAP/S	389/636
Microsoft SQL Server (MobiControl Database)	Binary	1433
MobiControl Cloud Link Agent	HTTPS	443
MobiControl Device Agents	**Binary/HTTPS**	**5494, 443**
MobiControl Search	HTTPS	9200, 9300
Native MDM	HTTPS	443
SOTI Services	HTTP/S	80, 443
Remote Control	Binary	5494
Windows Notification Service (WNS)	HTTP/S	80, 443

Management Server Connections

Component Name	Protocol	Port(s)
MobiControl Deployment Server	Binary	5494/5495
Amazon App Store	HTTPS	443
Apple Push Notification Service (APNS)	Binary	2195/2196
Apple DEP	HTTPS	443
Apple VPP	HTTPS	443

Certification Authority - DCOM Must be on the same domain	Binary	Dynamic
Certification Authority - HTTP	HTTPS	443
Enterprise Resource Gateway (ERG)	HTTPS	443
Google Play	HTTPS	443
iTunes	HTTPS	443
LDAP	LDAP/S	389/636
Microsoft SQL Server (MobiControl Database)	Binary	1433
MobiControl Cloud Link Agent	HTTPS	443
SOTI Services	HTTP/S	80, 443
MobiControl Search	HTTPS	9200, 9300
MobiControl Console	HTTPS	443
SOTI Assist Server	HTTPS	443

Miscellaneous Connections

Component A	Component B	Protocol	Port(s)
Enterprise Resource Gateway (ERG)	Exchange	Binary	443
Enterprise Resource Gateway (ERG)	SharePoint/WebDAV	HTTPS/WebDAV	443
MobiControl Cloud Link Agent	Certification Authority - DCOM Must be on the same domain	Binary	Dynamic
MobiControl Cloud Link Agent	Certification Authority - HTTP	HTTPS	443
SOTI Assist Server	Microsoft SQL Server (SOTI Assist Database)	Binary	1433
SOTI Assist Server	SOTI Assist UI	HTTPS	443
SOTI Assist UI	Remote Control	HTTPS (web sockets)	443
SOTI Hub	Enterprise Resource Gateway (ERG)	HTTPS	443
SOTI Surf	Enterprise Resource Gateway (ERG)	HTTPS	443
MobiControl Console	Remote Control	HTTPS (web sockets)	443

Most recent information can be found at https://www.soti.net/mc/help/v15.3/en/setup/installing/system_requirements.html?hl=network%2Cports#installing_network_ports

Google services overview

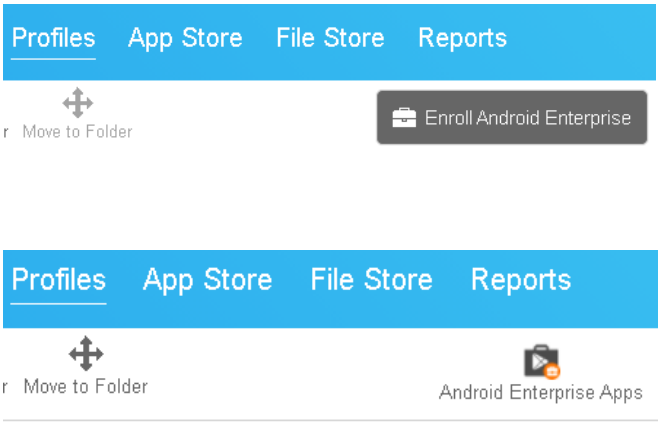
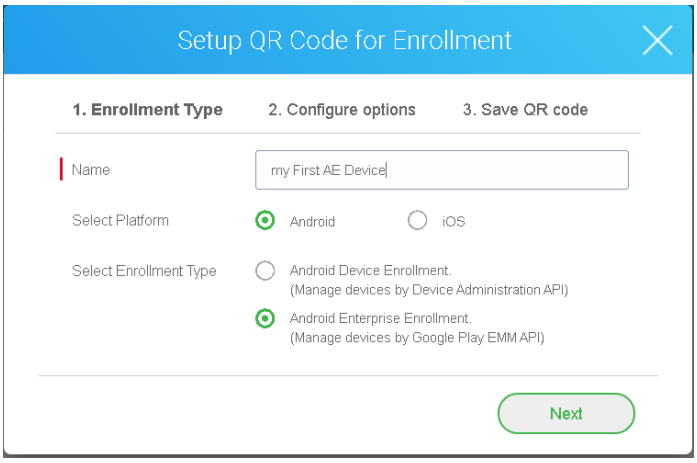
Android Enterprise Network Requirements - Android Enterprise Help (google.com)

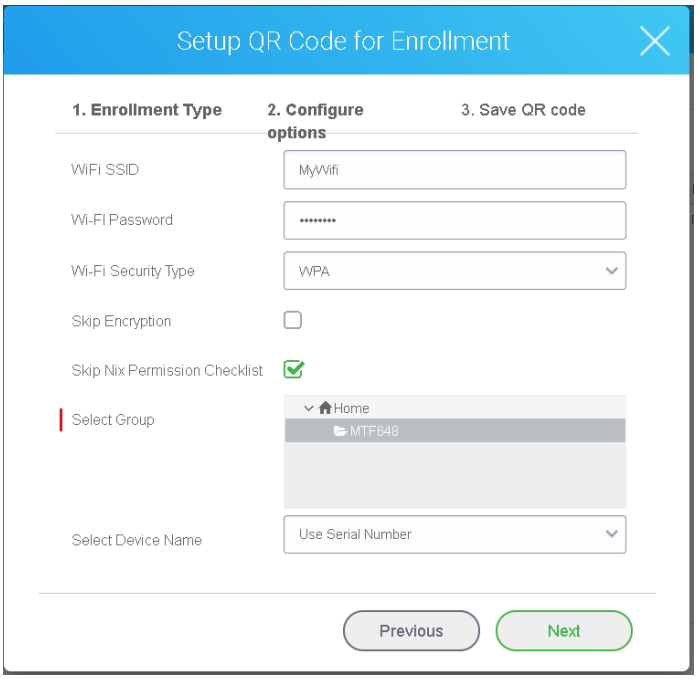
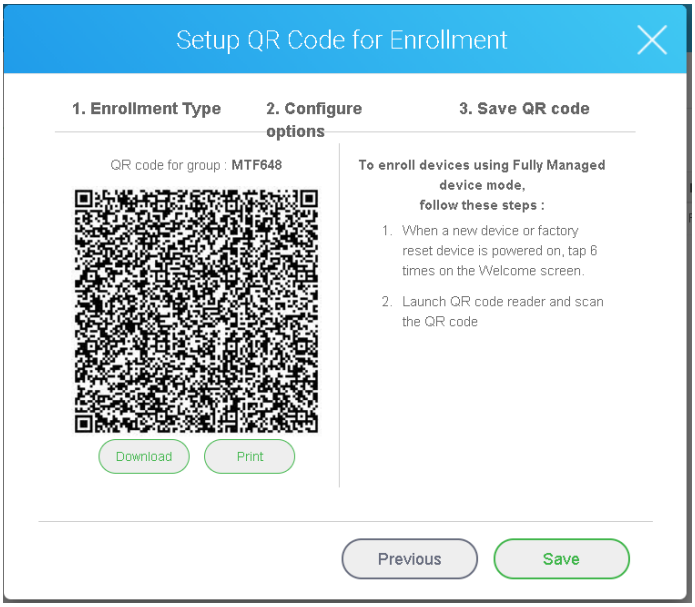
Configuration (MDM)

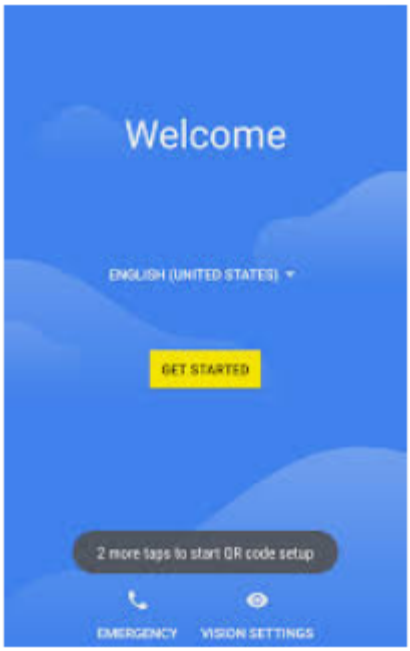
42gears SureMDM (Cloud)

Device Enrollment (you need to setup a link between a Google Account and SureMDM on SureMDM EMM)

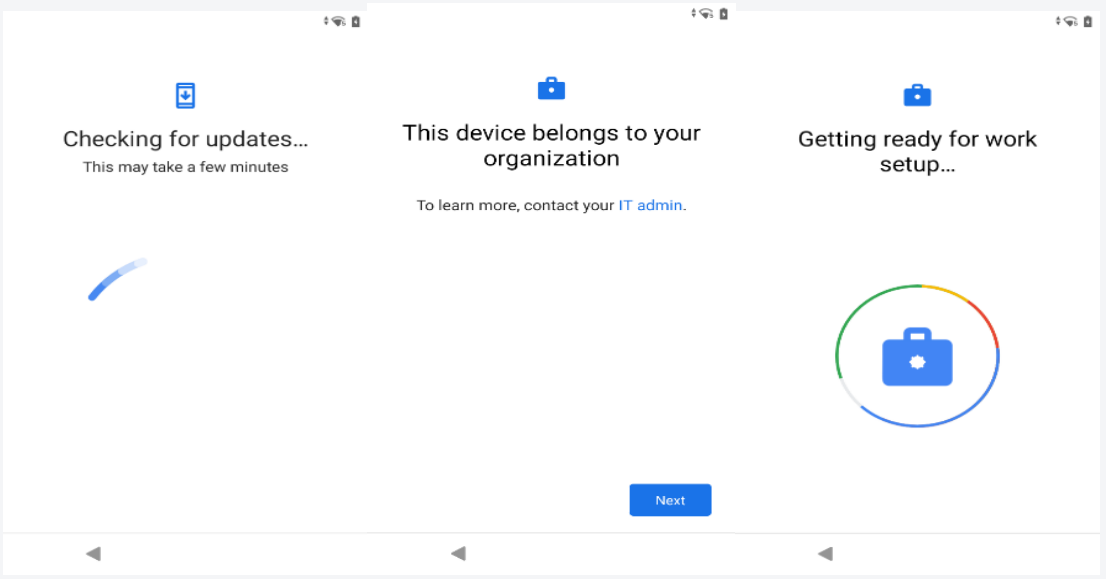
Below chapter provides additional information how to enroll Zebra Mobile Devices (Android Enterprise) into 42gears SureMDM tool. Non-Zebra Device enrollment might be different, and it is strongly recommended to read the Instructions from the device vendor for the non-Zebra devices.
If devices should be used prior Android Enterprise (pre-Android Oreo) or Windows Mobile / Windows CE devices consult with Zebra Managed Services team for further assistance.
SureMDM supports multiple options to enroll a Zebra Android device. The best option is the QR code enrollment.
Additional information at: https://knowledgebase.42gears.com/article/support-dedicated-devices-with-android-enterprise-using-suremdm/
Follow below steps:

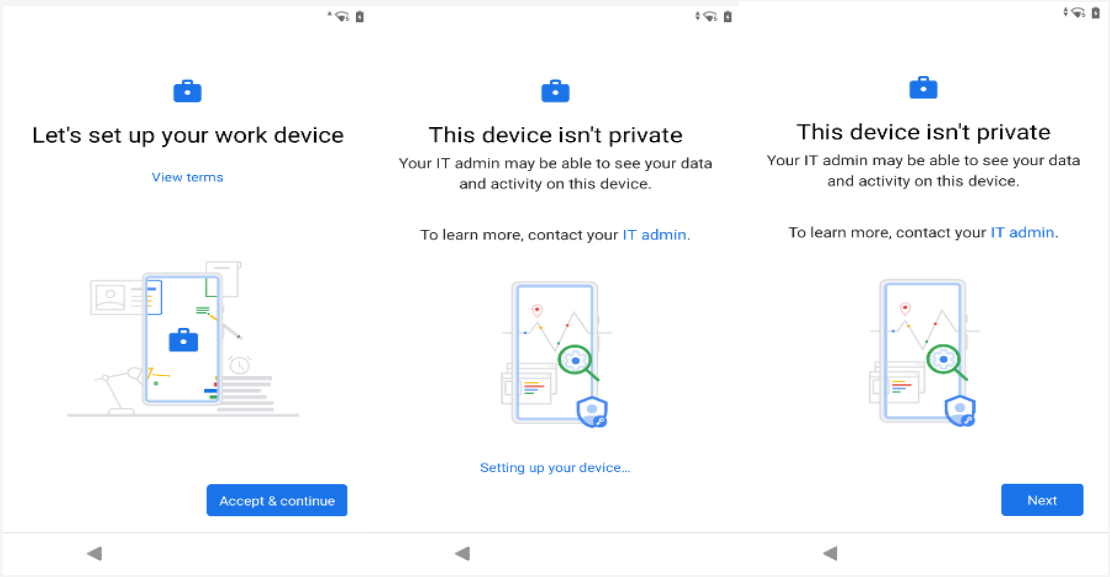
	Screenshot	Description
1		In the profile section, click on Android Enterprise Apps and establish a connection to the Managed Play Store using i.e. your GMail or G-Suite account. Once the connection is established you get the screen to select your Android Enterprise Apps. More information at: **Profile binding to a Google Account (MGPA) to use the Managed Play** Store
2		Click on Enrollment
3		Click on Get Started
4		Give the QR profile a name. Select Android Enterprise Enrollment (Manage devices by Google Play EMM API) Select Next

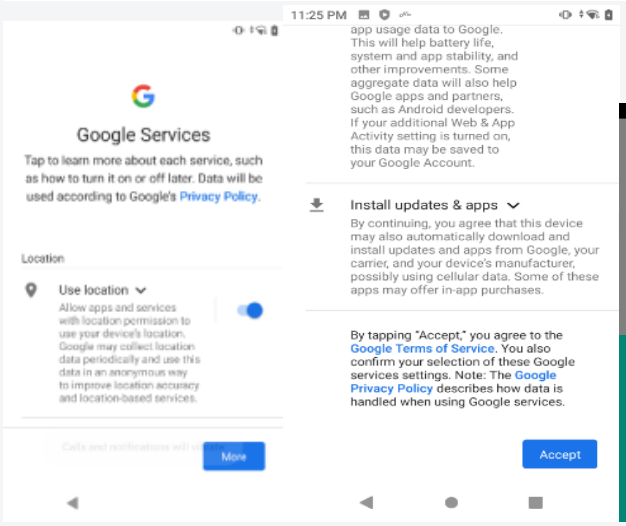
5		Enter additional information and click Next
6		Barcode is created. Click Save. Change the QR code to avoid enrolling to our test instance
7		Factory Reset your device. To achieve a Factory Reset use the Zebra StageNow tool.

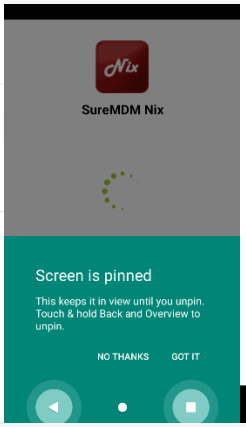
8		If you see the Google Welcome Screen you need either to tap several times on the screen to activate the QR code reader to allow you to scan the previously created QR, or if supported just scan the QR code.

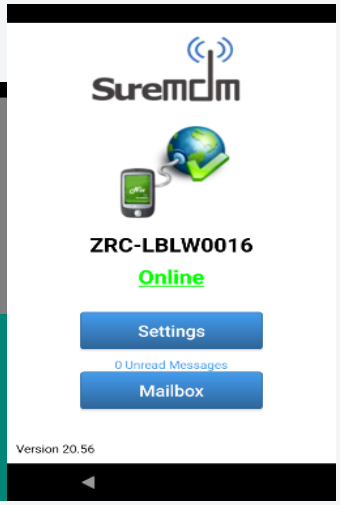
9







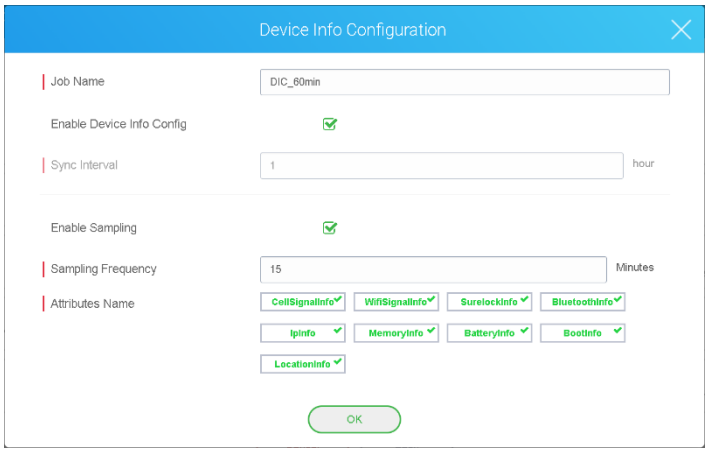




Various screens pop up.
Just follow the screens.
Depending on the Android OS the screens might change.

VIQF required job to collect MDM device data

To allow VIQF having more data available from MDM a certain job needs to be deployed to all Android devices.
Zebra configures the required job already if the instance will be setup and assigns the job to device groups. See below details of the job for Android devices.

	Job type
	Default configuration.

To ensure consistent VIQF experience, make sure the job is deployed to all devices.

Profile binding to a Google Account (MGPA) to use the Managed Play Store

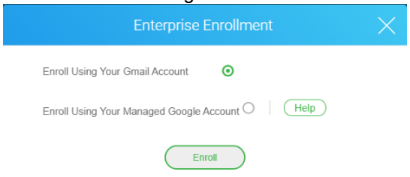
If you want to use the MGPA (Google Managed Play Account) to deploy applications from Google Play Store or if you want to simplify the enrollment to 42gears by scanning a QR code on the device Google Welcome Screen, you need to create an EMM binding.
To do this you require a Google Gmail or G-Suite account.

Gmail Account

In SureMDM click on Profiles

Click on "Enroll Android Enterprise"

Click on "Enroll Using Gmail Account" and then on "Enroll".

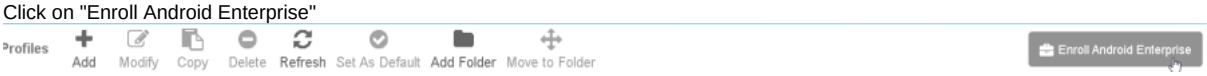


Follow the instructions from the Google Web Site.

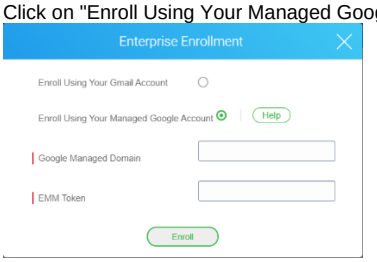
G Suite Account

In SureMDM click on Profiles

Click on "Enroll Android Enterprise"



Click on "Enroll Using Your Managed Google Account" and type in your Google Managed Domain and EMM token then on "Enroll".



How to generate the EMM token click either the Help Button or below link: https://knowledgebase.42gears.com/article/enroll-and-manage-android-mobile-devices-with-g-suite-in-suremdm/

Soti MobiControl (Zebra/Soti Cloud)

Device Enrollment

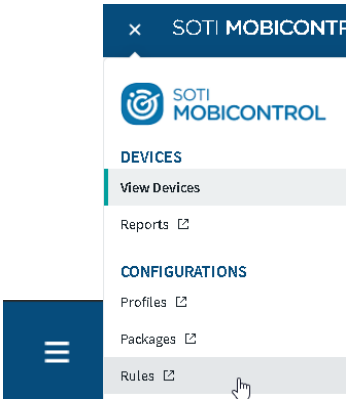
Below chapters provides additional information how to enroll Zebra Mobile Devices (Android) into Soti MobiControl MDM. Non-Zebra Device enrollment might be different and it is strongly recommended to read the Instructions from the device vendor for the non-Zebra devices.

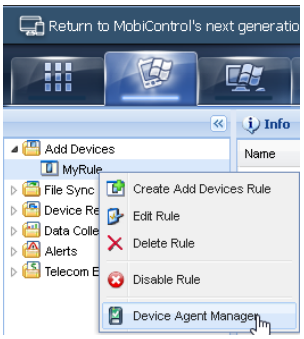
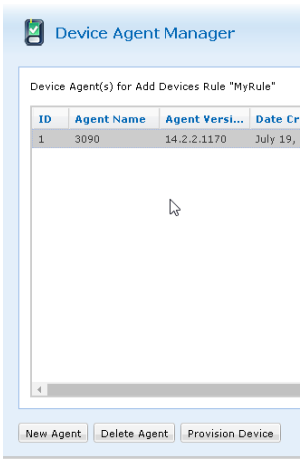
MS Windows Mobile/CE Device

Windows Mobile/CE devices that are running one of the following operating systems can be enrolled on MobiControl:

- CE .NET 4.2 or later
- Windows Mobile 5.0 or later
- Pocket PC 2002 or 2003

Once you have created an add device rule, you must install a device agent on your devices to enroll them in MobiControl. Device agents for the Windows Mobile/CE platform are custom built for each add devices rule. Zebra creates add device rule on request while onboarded into VIQF service.

	Description	Screenshot
1	Login to your Soti MobiControl server	
2	Select option in top left Burger Menu for Configuration >> Rules	
3	If you have an 'Add device' rule already you can proceed with step #8	
4	If you need to create an Add Device Rule, Select Windows Mobile/CE tab **Note: On newer Soti MobiControl versions Add Device rules replaced by Enrolment policy.**	
5	Right click on Add Devices select option 'Create add device rule' and step through wizard.	

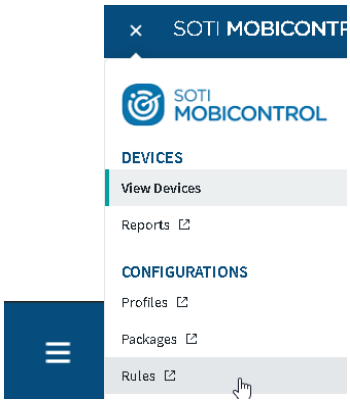
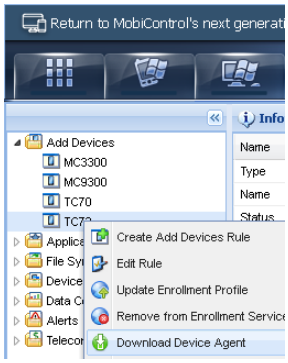
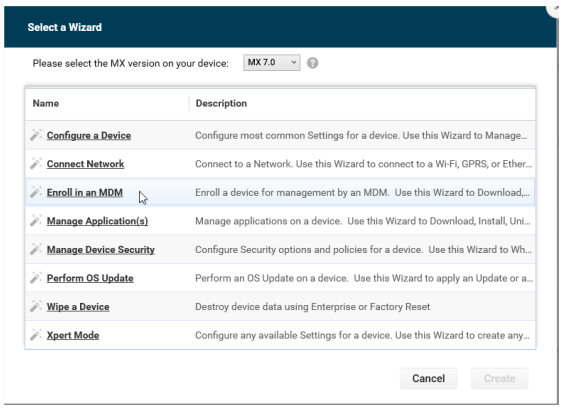
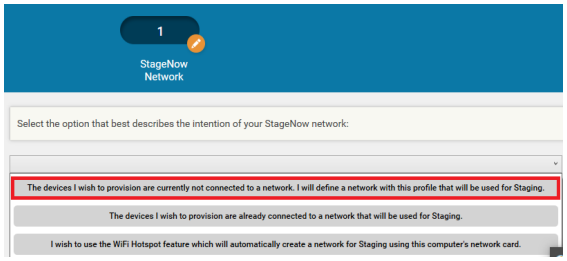
6	After rule is created right click the rule and select the option to 'Device Agent Manager', click on 'New Agent' and step through wizard.	
7	On 'Device Agent Manager', select 'Provision Device' then 'Self-Extracting Executable'.	
8	Connect the device to a network, or connect the device to a PC using USB	
9	Copy Soti MDM agent onto the device and install it. Best is to use MS ActiveSync / Windows Mobile Device Center	

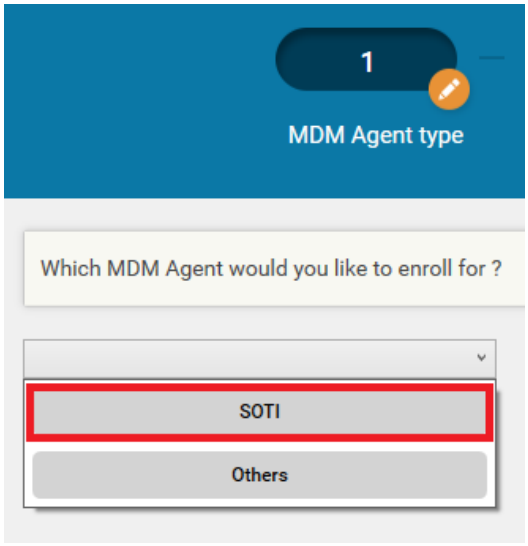
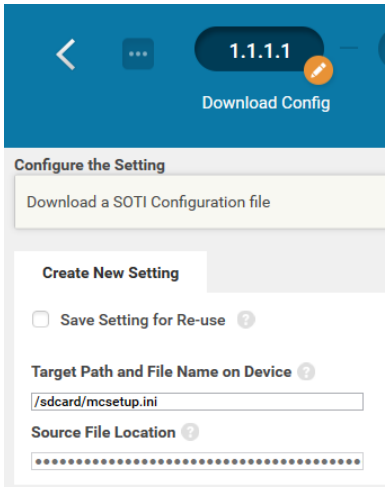
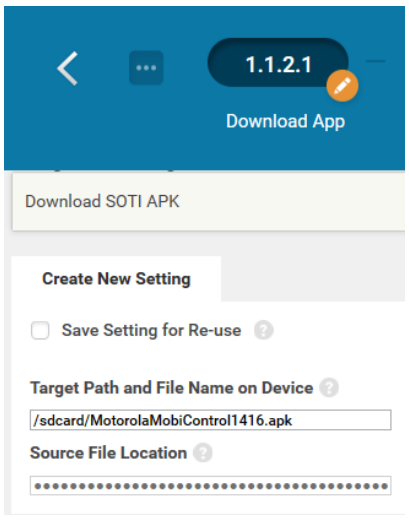
Android Devices DA (Device Administrator, legacy)

Android devices that are running one of the following operating systems can be enrolled into Soti MobiControl: Android v4.0 (KitKat) and above.

Devices with Android operating systems Oreo (8) or above cannot be enrolled as DA (Device Administrator), only as DO (Device Owner [Android Enterprise] / see next chapter). Once you have created an add devices rule, device agent needs to be installed on your devices to enroll them in MobiControl. Best practice is to use Zebra StageNow tool to enroll Zebra Android devices.

	Description	Screenshot
1	Create a directory on your PC where you will store all files needed to deploy through StageNow.	
2	Download the Soti MDM agent (scroll to the bottom and select Android Enterprise) from https://docs.soti.net/oem and save it in the directory you just created.	
3	Login to your Soti MobiControl server.	

4	Select option in top left (Burger Menu) for Configuration >> Rules.	
5	If you have an 'Add device' rule already you can proceed to step #9.	
6	If you need to create an Add Device Rule, Select Android+.	
7	Right click on Add Devices select option 'Create add device rule' and step through wizard.	
8	After rule is created right click the rule and select the option to 'Download Device Agent', in the drop-down box select Zebra.	
9	Select the option to download ini file (mcsetup.ini) and save it to the directory you created for all your StageNow files. Do not download the Soti agent. Use the agent you downloaded above (see step #2).	
10	Open StageNow tool and create a new profile using MX version supported by the device and the 'Enroll in an MDM' template.	
11	In the first template option (StageNow Network) select the first option in the dropdown (I will define a network with this profile).	

12	Step through wizard to connect to your staging wifi network.	
13	Continue through wizard and select Soti as your MDM provider.	
14	Select option yes to download Configuration File. Specify path and name on device of '/sdcard/mcsetup.ini' and then select the mcsetup.ini file you downloaded from the Soti server and in final option to 'Download a Soti Configuration file' select 'No'.	
15	Next select option to download the soti MDM Android app (apk) to the device. Select target path (e.g., /sdcard/MotorolaMobiControl1416.apk) and then select apk you downloaded from the Soti MobiControl web site. Apk file name could be different to reflect the various versions issued by Soti.	
16	Select option to launch Soti apk and enter package name "net.soti.mobicontrol.motorola" and class name "net.soti.mobicontrol.startup.SplashActivity".	
17	Complete the StageNow profile and create the barcode.	

Android Devices DO (Device Owner)

Android Enterprise debuted with 5.0 Lollipop in 2014 as an optional* solution, manufacturers could integrate to provide a common set of device management APIs. From 6.0 Marshmallow it was no longer optional and has since been a mandatory component for all GMS-certified manufacturers. There are still some optional components for Android Enterprise today and the occasional feature released only for newer versions of Android, however these have little impact on core management.
Android Enterprise (AE) offers a few things:
A reliable EMM experience, knowing when a configuration is pushed, all AE devices will support and execute the relevant requests.
A containerized work/life separation primarily aimed at BYOD, referred to as a work profile.
A fully locked-down, managed mode for complete corporate ownership with no personal space, referred to as fully managed (previously work-managed).
A single-use mode (Android Kiosk, but within a work-managed device) for Kiosk-like applications, referred to as dedicated (previously COSU – Corporately Owned, Single Use).
A combined, COPE mode bringing together fully managed and work profile in order to provide a fully managed device with a personal space (fully managed devices with work profiles).
Out of the box, zero-touch enrolment for Android 8.0 and above (or 7.0 for Pixel).
A managed Google Play portal offering an application store for work devices containing only explicitly approved applications.
Silent application installation without the need for a user-provided Google account on the device.
Managed configs, a way of deploying corporate settings to managed applications (think Exchange profiles, but configurable in Gmail directly. See below).
Mandatory device encryption.
Here's a breakdown of the management scenarios Android Enterprise supports:

With fully managed devices there is normally no user space. As the intended use is for wholly company-owned devices, the process of provisioning a fully managed device removes any typically BYOD or COPE (Corporately Owned, Personally Enabled) scenarios and locks the device down strictly to the environment set by the EMM administrator. As of Android 8.0 however, the COPE scenario has been introduced with fully managed devices with work profiles support.
Provisioning a fully managed device by default strips out almost all non-critical system applications unless white-listed, and instead provides access only to authorized apps via managed Google Play. Nothing more. This means should an app require the Camera to function, for example, a Camera app would need to also be authorized or white-listed for use by the business. There is support for enabling system applications, however this will include all of the OEM/carrier bloat most would want to see removed and will therefore require particular apps be disabled, rather than enabled as described above.
Fully managed provisioning is currently initiated on first boot of a new device – or one that's been freshly factory-reset – using:

- A provisioning app on a dedicated provisioning device (configured with EMM server details) and an NFC bump. You need Soti Stage Programmer available from Google Play Store.
- A DPC (Device Policy Controller) identifier on the Google account setup screen. The **DPC identifier** for Soti MobiControl is **afw#mobicontrol**.
- A QR code (ideal for devices without NFC)
- Zero-touch enrolment
- Zebra **StageNow Tool**

Best practice depends on customer requirements. Zebra recommends using Google Zero Touch (GZT) to keep enrollment simple, but DPC identifier, QR code or StageNow are valid alternative options.

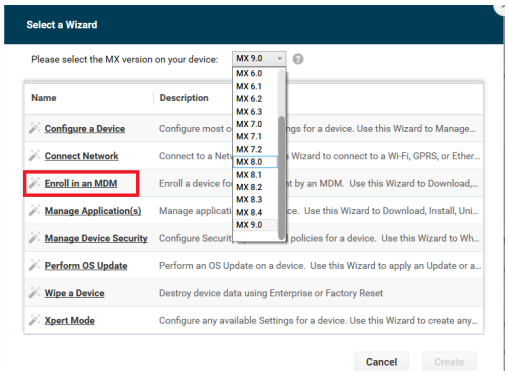
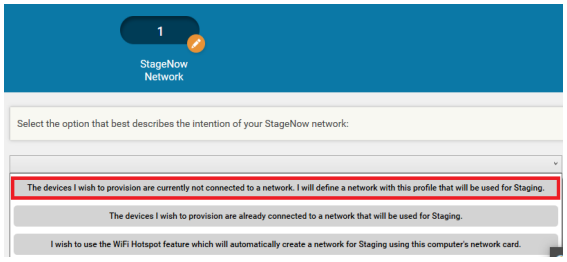
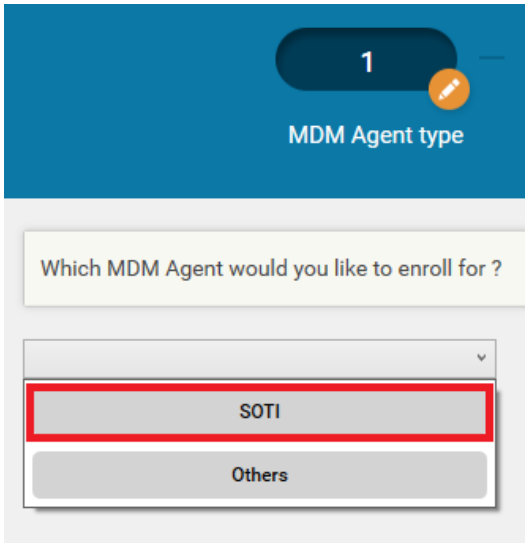
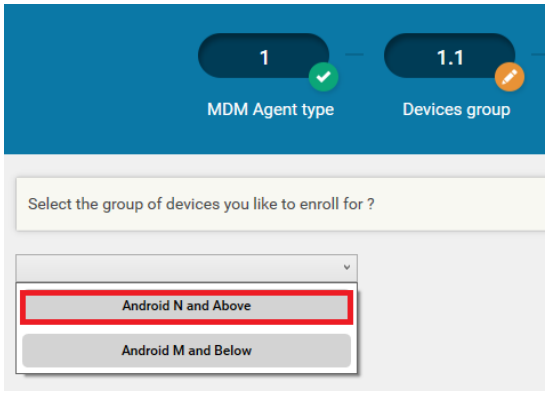
StageNow Profile Creation (Example steps)

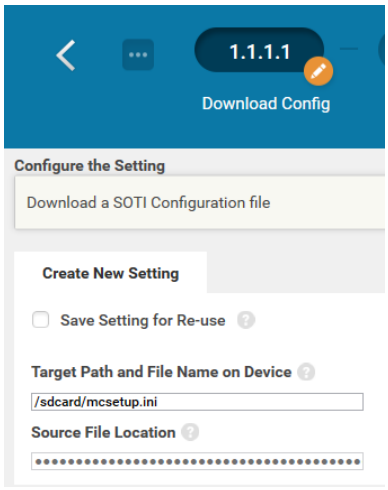
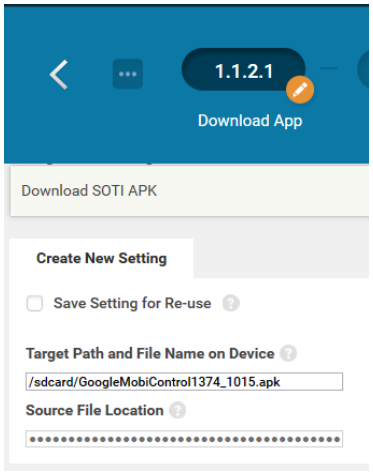
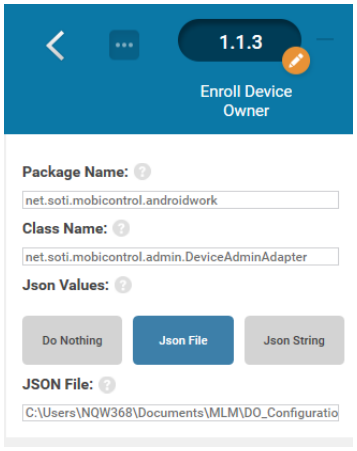
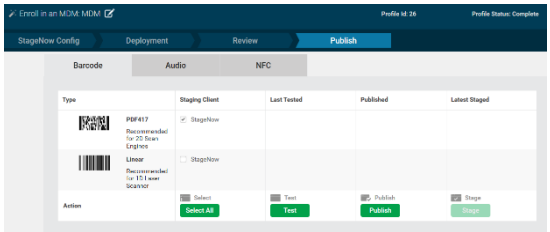
Using StageNow as an enrollment option might be deprecated/limited on Zebra Android Enterprise devices running Android 10 or newer. In such situation Google Zero Touch or QR (Quick Response) code enrollment option should be used.

	Description	Screenshot
1	Create a directory on your PC where you will store all files needed to deploy through StageNow.	
2	Download the Soti agent (scroll to the bottom and select Android Enterprise) from Soti Agent download and save it in the directory you just created	
3	Create a JSON file named 'DO_Configuration.JSON' with content described in Appendix 1	

4	Edit the 'enrollmentId' in the file 'DO_Configuration.JSON' with the Enrollment ID from MobiControl 'Add Device Rule' you want to connect to.If you don't have an Add Device rule already, follow the next few steps.	Example:
		<pre>{
		"android.app.extra.
		PROVISIONING_DEVICE_ADMIN_COMPONENT_NAME":
		"net.soti.mobicontrol.androidwork/net.
		soti.mobicontrol.admin.DeviceAdminAdapter",
		"android.app.extra.
		PROVISIONING_DEVICE_ADMIN_SIGNATURE_CHECKS
		UM":
		"hn8mSNJMPcovWbnnWrb-uMpWZjNlNp-jyV_2A-
		Whumc=\n",
		"android.app.extra.
		PROVISIONING_SKIP_ENCRYPTION":"false",
		"android.app.extra.
		PROVISIONING_LEAVE_ALL_SYSTEM_APPS_ENABLED"
		:true,
		"android.app.extra.
		PROVISIONING_ADMIN_EXTRAS_BUNDLE":
		{
		"enrollmentId":"HRU5AE96"
		}
		}</pre>

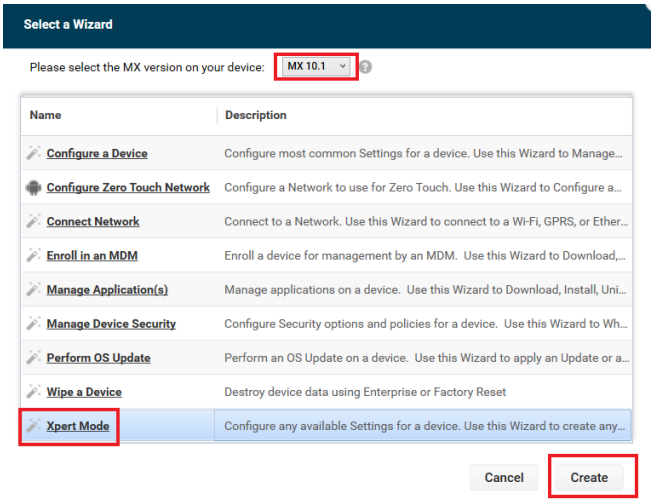
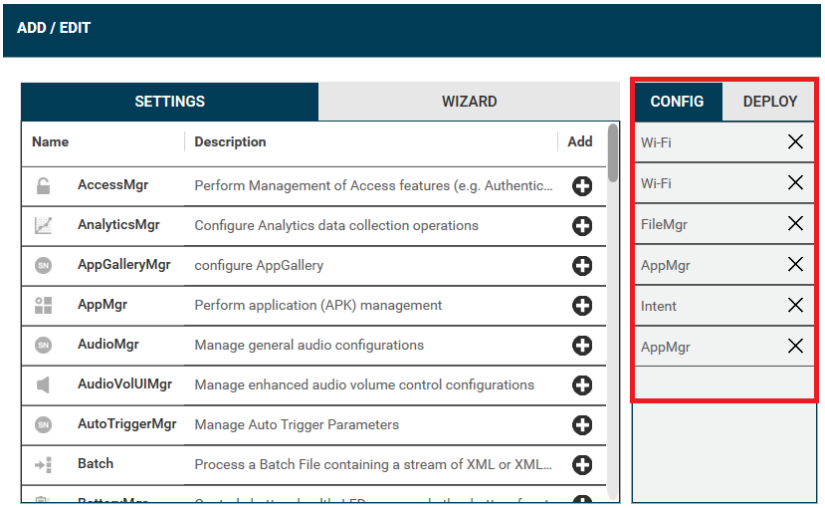
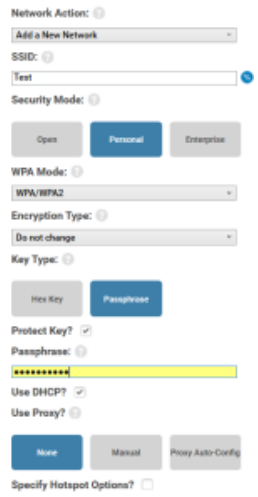
5	Login to your Soti MobiControl server	
6	Select option in top left (Burger Menu) for Configuration >> Rules	
7	If you have an 'Add device' rule already, you can proceed with step #9	
8	If you need to create an Add Device Rule, Select Android+	
9	Right click on Add Devices select option 'Create add device rule' and step through wizard. For "Android Enterprise Setup", select "Managed Google Play Accounts" with your Enterprise Binding account. If you do not have setup your Enterprise Binding, create one. Enterprise Binding is optional, but without the Binding you do not have access to the Managed Google Play Account (MGPA).	
10	After rule is created right click the rule and select the option to 'Download Device Agent', in the drop-down box select Zebra	
11	Select the option to download mcsetup.ini file and save it to the directory you created for all your StageNow files. **Do not download the Soti agent. Use the agent you downloaded (step #2).**	

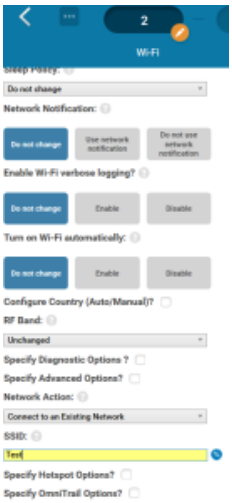
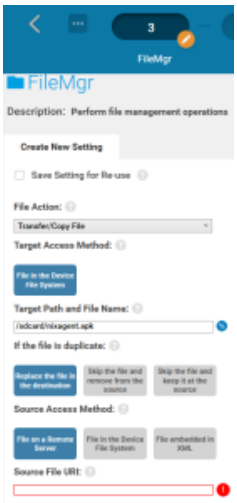
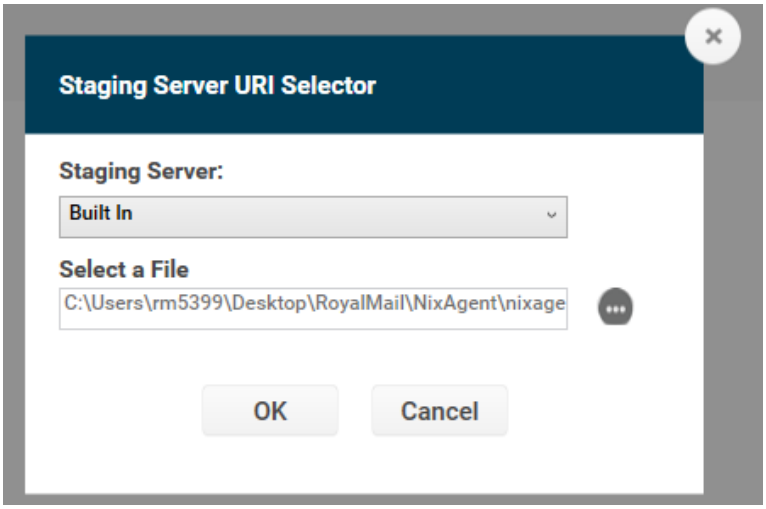
12	Open StageNow tool and create a new profile using MX 8.0 or newer if supported by your device and the 'Enroll in MDM' template. It might be possible to update the Android OS and LifeGuard patch before.	
13	In the first template option (StageNow Network) select the first option in the dropdown (I will define a network with this profile)	
14	Step through wizard to connect to your staging wifi network	
15	Continue through wizard and select Soti as your MDM provider and then select 'Android N' and above	 

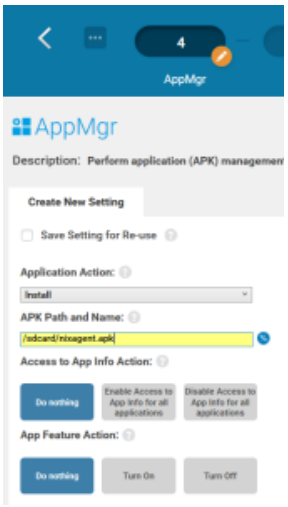
16	Select option yes to download Configuration File. Specify path and name on device of '/sdcard/mcsetup.ini' and then select the mcsetup.ini file you downloaded from the Soti MobiControl server and in final option to 'Download a Soti Configuration file' select 'No'.	
17	Next select option to download the soti apk to the device. select target path (e. g., /sdcard/GoogleMobiControl1374_1015.apk) and then select apk you downloaded from the Soti web server (step #2).	
18	At step 1.1.3 'Enroll Device Owner' select the file 'DO_Configuration.JSON' from your StageNow download folder This setting configures an intent to the device agent to define Soti MobiControl Android Enterprise agent as a Device Owner which results in an fully managed device.	
19	Complete the StageNow profile and create a barcode.	
20	The device must be reset to deploy as DO. Factory Reset is the best option. Boot to Recovery mode and install Factory Reset package.	

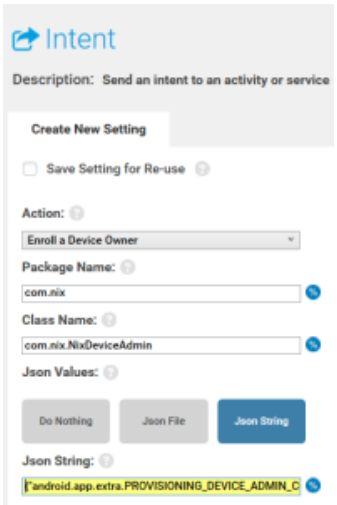
21	At Setup Wizard screen scan StageNow barcode to bypass SUW (Setup Wizard) and start StageNow application on device (client).	 **Note:** **Above barcode only works with Zebra Android devices, but may fail on older Android versions.**
22	Scan the StageNow barcode created above for the Device Enrollment	

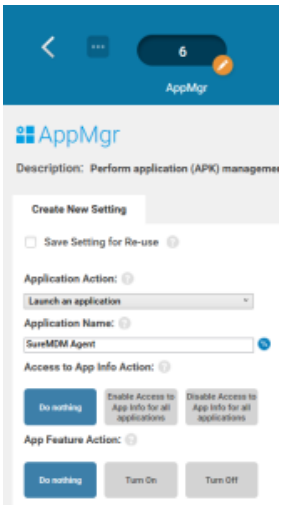
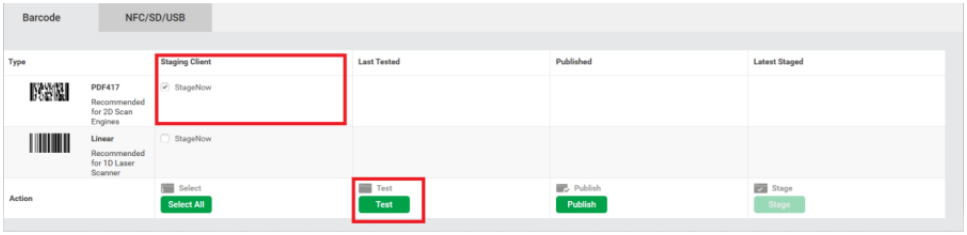
Enroll device into SureMDM (42Gears)

	Description	Screenshot
1	Create a new profile in StageNow	
2	Include the following CSPs	
3	WifiMgr - add a network profile	

4	WifiMgr – connect to network	
5	FileMgr – transfer the NixAgent.apk to the device // NixAgent versions can be downloaded from here.	 

6	AppMgr – install Nix Agent	

7	Intent – make NixAgent device owner, JSON string for SureMDM enrollment should look as follows (adjust the "GroupPath", "AccountId" accordingly):	{
		"android.app.extra.PROVISIONING_DEVICE_ADMIN_COMPONENT_NAME":"com.nix/com.nix.NixDeviceAdmin",
		"android.app.extra.PROVISIONING_DEVICE_ADMIN_SIGNATURE_CHECKSUM":
		"CbIXJyiLvnV9PBgBs7zmKGkyIkf31dJA_DtODzQYiug=",
		"android.app.extra.PROVISIONING_ADMIN_EXTRAS_BUNDLE":
		{
		"AccountId":"*****YOUR ACCOINT ID******",
		"ServerPath":"zebramdm.42gears.com",
		"HttpHeader":"https://",
		"EnrollmentType":"1",
		"GroupPath":"Home/MC33",
		"DeviceNameType":"UseSerialNumber",
		"ShowCheckListScreen":"False"
		}
		}
		 

8	AppMgr – launch NixAgent	
9	Go to *Completed profiles*, click on the following options:	
10	Scan the generated barcodes.	

SOTI Mobicontrol

VIQF required rule to collect MDM device data (Data Collection)

The below data collection metrics needs to be collected for the VIQF dashboard every 60 minutes.
In SOTI MobiControl, server-side truncation of collected data is set by the data collection rule with the shortest server-side truncation setting. It does not matter what rule the data comes from.
Keep in mind that with Zebra Android Devices, the ZDS (Zebra Data Service) agent collects a lot more device machine data compared to Soti MobiControl which will be included into the VIQF dashboard soon. The ZDS agent can be configured via Zebra StageNow Tool (Data Analytics Manager CSP).
ENSURE that every rule has set the default truncation limit.
Below list of minimum required data metrics:

- Available External Storage Shows the amount of external storage available on the device
- Available Internal Storage Shows the amount of internal storage available on the device
- Available Memory Shows the amount of RAM the device has available
- Available System Storage Shows the total amount of system storage available on the device
- Battery Status Shows what percent the battery was at the time the data collection rule ran
- Cellular Carrier Shows what carrier the device is connected to at the time the data collection rule ran
- Cellular Signal Strength Shows what the signal strength is of the device at the time the data collection rule ran
- IP Address Shows the IP address of the device at the time the data collection rule ran
- Location Collects the location of the device
- WiFi Signal Strength (RSSI) Shows the signal strength of a wireless connection. A value of 0 is collected when there is no Signal listed in Manager
- Wifi BSSID (Basic Set Service Identifier)Shows the last connected AP (Access Point)

Best practice for Visibility IQ Foresight is to collect all available standard metrics and then decide which of these metrics does not make sense and need to be removed. Above mentioned metrics are the minimum required.

Printer (Zebra LinkOS only)

Note: Zebra LinkOS enabled printer can be connected to VIQF. Just ensure the latest printer FW (Firmware) is installed and you have a valid contract. To manage printer with Soti MobiControl the new approach is described in more detail at: Printer Management with SOTI Connect
SOTI Connect - Business Mobility & IoT Solutions
SOTI Connect
Legacy approach is described below:
Prerequisites is to have the PAS (Printer Administration Server) set and showing as online in SOTI MobiControl (this part will be done by SOTI or Zebra but requires to be ordered separately).
Ensure that you have an Add Device rule created for printers.
Then, a script command needs to be sent down to printer (using Zebra Setup Utilities and USB connection to your computer):
! U1 setvar "weblink.ip.conn1.location" "https://<FQDN_of_the_server>:<tcp:port>/zebra/weblink/"

VIQF 4.0 or newer supports printer reports (no printer management), connected to ZPC (Zebra Printer Cloud/Connector). VIQF Printer reports requires below SKU's.

SKU	Description	Discount Category
VIQF-PRT-3Y	**36 months Contract**	**Z3**
VIQF-PRT-5Y	**60 months contract**	**Z3**
VIQF- PRT-1R	**12 months renewal contact**	**Z3**
VIQF-PRT-2R	**24 months renewal**	**Z3**
VIQF-PRT-PILOT	**VIQF Printer pilot, 90 days, up to 100 devices**	**X1**

Required Soti MobiControl rules to manage printers

To configure SOTI to capture printer data properly follow these steps:

1. Create Folder Structure in SOTI
2. Create an Add Device Rule for Printers

The details for each of these steps are listed below.

Create SOTI Folder Structure

This is the same for Printers as it is for Mobile Computers.

Add Device Rule for Printers

This is similar process as being used for Mobile Computers as well.

Setup printer management

Zebra Printer Management requires the installation of a PAS (Printer Administration Server), aka Soti Connector.
The PAS will be installed by Zebra or Soti, depending if Soti MobiControl is hosted on Soti MobiControl or Zebra cloud instance.
The PAS installation requires a setup fee to be ordered.
In case the PAS needs to be installed on-premises, Zebra Professional Services or the Zebra Printer team needs to be engaged.

Package Creation and Deployment

Detailed description can be found at: https://www.soti.net/mc/help/v14.4/en/index.html#packagestudio/packagestudioindex.html

> ***For Android Enterprise Devices you could use the MGPA (Managed Google Play Account) to download apps to your device. This requires a so called Enterprise Binding to be setup to connect Soti MobiControl with Google Managed Play Store. https://www.soti.net/mc/help/v14.4/en/index.html#console/reference/dialogs/globalsettings/afweb_configure.html***

Your added device rule for Android Enterprise devices must have the available Enterprise Binding selected.
You need to add apps from the Managed Google Play Store to an Soti MobiControl Application catalogue. See: Android Enterprise - Enterprise Binding (optional) *and* Deploying Android Application Using Application Catalog.

Package Studio Tool

Package Studio is a supplemental program bundled with MobiControl that allows you to create and manage 'packages'- containers for deploying applications, scripts, and other files to devices managed by MobiControl.
To download Package Studio:

1. In the MobiControl console, select the All-Platforms tab and then the Packages tab.
2. On the bar under the platform tabs, click Download Package Studio to download the Package Studio program file (MCStudio.exe) to your computer.

After you have downloaded the Package Studio program file (MCStudio.exe) to your computer, it is ready to run – there are no further installation steps. You are now ready to build packages for use in MobiControl.

Package Project

Packages are the final form of the file and software container that is usable by MobiControl. In Package Studio, you are generally working with "Package Projects", the development phase of a package.
A package project gathers the files, scripts, and applications together and allows you to specify installation instructions. Once you are satisfied with the contents, you 'build' the project to create the final package. Projects can be modified after they have been built. Add or remove files and then simply rebuild the project.
Package projects are saved as *.mcp files.

Building a Package

To turn a package project into a package:

1. Click to select the package project that you want to build into a package. It should be highlighted blue.
2. Open the Project menu and select Build Package.

The Output Window displays the progress of the package building.

Editing a Package Projects

To edit the contents of a package project:

1. Open the File menu and select Open Existing Package Project.
2. Navigate to the file location of the saved project that you want to modify and open the *.mcp file.

The default location for project files is: C:\Users\Username\Documents\MobiControl Packages\.
Two panels will appear: Project and Project Properties.

1. Under Project Properties, edit the properties of the package. Ensure that the changes do not cause compatibility conflicts with the files, folders or scripts in the project.

To add additional files, folders, or scripts to the project:

1. Right-click on the project name and select one of:
    - Add Files
    - Add Folder
    - Add Android *.apk
    - Add Script
2. Follow the instructions for each item type.

To remove files, folders, or scripts from the project:

1. Right-click on the file, folder, or script and select Delete.

Changes are saved automatically.

Using Script in Packages

Package Studio supports the inclusion of custom scripts to your packages. See Using Script Commands for help building custom scripts.
You can set a script to activate at one of four times:

Name	Activation Period
Pre-Install Script	Script is executed before the installation of the other package contents.
Post-Install Script	Script is executed after the installation of the other package contents.
Pre-Uninstall Script	Script is executed before the uninstallation of the other package contents.
Post-Uninstall Script	Script is executed after the uninstallation of the other package contents.

Adding a Package

To add a package to MobiControl:

1. On the Packages tab, click the Add button.
2. Click Browse and navigate to the file location of the package file (.pcg) you created in Package Studio. Click OK.
3. Repeat steps for any additional package files (.pcg) you want to upload to MobiControl.

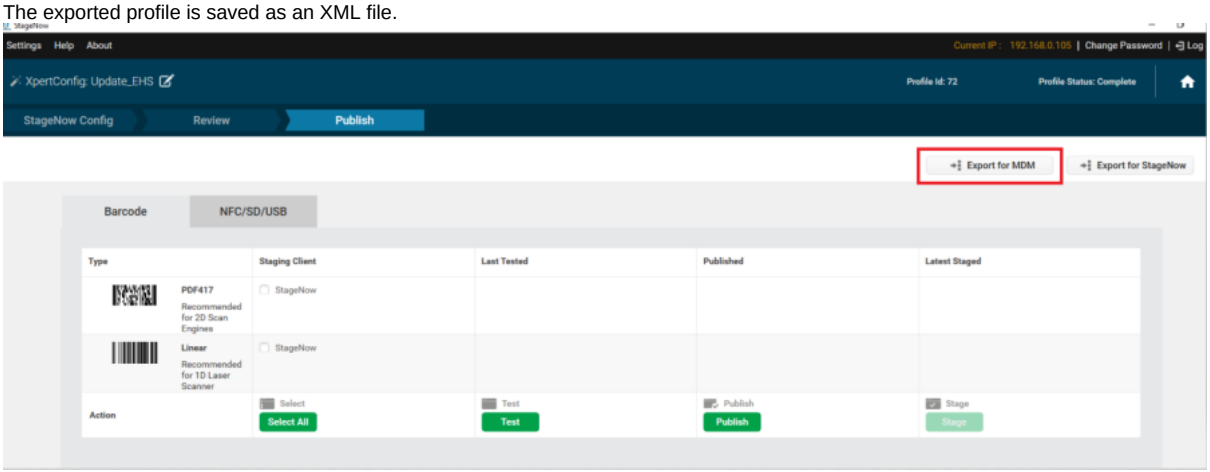
You can add multiple versions of the same package to MobiControl. They are grouped together under their package name and sorted by version number. After uploading packages to MobiControl, deploy them to your devices using a profile.

Example: Deploying a StageNow-generated XML file as a file sync rule or a package

Once you have created a staging profile in StageNow, you can export the profile as an XML file. You can then send the XML profile down to Zebra devices that are enrolled in MobiControl via a file sync rule or a package.
Process:

1. In StageNow, create a configuration profile for Zebra devices.
2. In StageNow, export the profile. When prompted, select **Export for MDM**.

The exported profile is saved as an XML file.

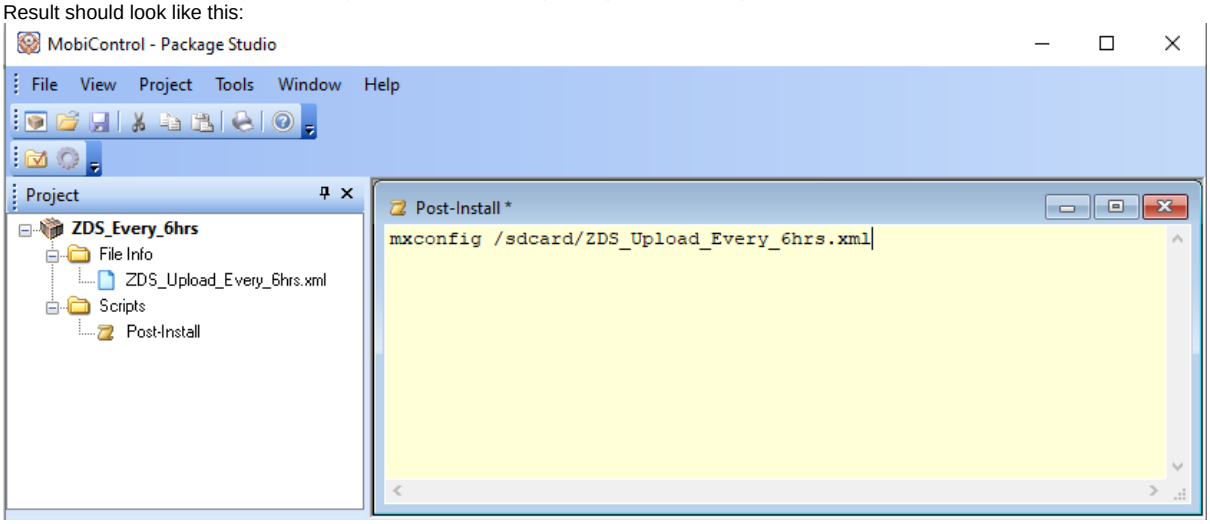


1. Create either a file sync rule (in the MobiControl web console) or a package (using Package Studio), depending on the deployment method you want to use.

When creating the file sync rule or package, include the following:

- The exported profile XML file.
- A script that uses the *mxconfig* command to install the profile on the device.

If you are creating a package in Package Studio, add the script as a *post-install* script.
Result should look like this:



1. If you are deploying via a package, add the package to a MobiControl profile.

When the file sync rule or MobiControl profile is pushed down to the Zebra devices, the *mxconfig* script command executes and installs the Zebra profile on the device.

Android Enterprise - Enterprise Binding (optional)

The Android operating system has several built-in features designed to facilitate easier device management within enterprise deployments. The flexibility of Android continues with these 'work' features; whether your mobility strategy is bring your own device or purpose built device or a mix of both, Android has a solution for you.
In MobiControl, Android devices with work features enabled are managed under the Android Plus banner as Android Enterprise. Enrollment, remote-control, and device configuration are all performed under Android Plus. Unless noted, Android devices with work features enabled can generally accomplish anything a regular Android device can.
Work features are available on devices running Android 4.0 or later. However, in Android 4.0 to 4.4, the functionality is provided using the Android Enterprise client, which must be installed separately on the device. Beginning with Android 5.0, work features are native to the Android operating system.

Device Management Type

There are two types of device management for Android devices with work features enabled: work managed devices and devices with work profiles.
Work managed devices are Android devices where the entire device is managed and under enterprise control. It grants administrators an extensive level of control over devices. Devices must be configured as work managed devices during the initial setup of the device.
Devices with work profiles are devices where only a portion of the device is dedicated to enterprise apps and data. The rest of the device is devoted to personal apps and data and the two sections remain separated. As the device user has ultimate control, there are some limitations to device management in this scenario compared to work managed devices.
This can be easily achieved by just install the Soti MobiControl Android Enterprise agent with the mcsetup.ini file.

Account Type

When enrolling devices in MobiControl, you can choose between two types of accounts for Android devices with work features enabled: Google managed accounts and managed Google Play accounts. You can also choose to skip the Google account creation entirely. Only choose the Skip option if the devices will not require access to the managed Google Play Store.
Google managed accounts are user-based and are best for situations where the device will be associated with a single user for its lifetime.
Managed Google Play accounts are device based and are best for situations where the device will be used by multiple users, such as kiosk environments.

Linking a Google Domain

To link your Google domain to MobiControl:
Perform these steps in the Google Admin Console.

1. In the Users section, enter the users whose devices you want to manage in MobiControl.

Alternatively, you can sync users from Active Directory credentials.

1. In the Domains section, enter the primary domain and, if applicable, any secondary domains that you want to manage through MobiControl.
2. You must verify that you have ownership over the domain. Click Continue and verify domain ownership. Google provides several methods to verify domain ownership.
3. Once you have successfully verified your ownership of the domain, return to the home page of the Google Admin Console.
4. In the Security section, select Manage EMM provider for Android page and request a management token (also called an MDM token).

This MDM token proves to Google that MobiControl is authorized to managed Android devices under this domain.
Perform these steps in the MobiControl console:

1. On the All-Platforms tab, go to the Servers tab.
2. Under Global Settings, select Android Enterprise Bindings to open the Configure Android Enterprise Bindings dialog box.
3. Click the New button and select Google Domain.

The Add Android Enterprise Binding dialog box opens.

1. In the Add Android Enterprise Binding dialog box, enter the primary domain and the MDM token string in the appropriate fields.

An MDM token can be used only by a single instance of MobiControl to manage a single primary domain. However, the same MDM token can be used to bind the same MobiControl instance to multiple secondary domains.

1. If applicable, specify any secondary domains.
2. Click Save to save the new enterprise binding and close the Add Android Enterprise Binding dialog box.

The new enterprise binding is added to the Configure Android Enterprise Bindings dialog box.

1. Click Close to save your enterprise bindings and close the Configure Android Enterprise Bindings dialog box.

MobiControl is now authorized to manage Android devices on the specified domain. You can now enroll your Android devices with work features in MobiControl.

Add Device Rule – with Managed Google Play Account

Rule Name

Enter the name you want to assign to this add devices rule.

Name	Enter the name you want to assign to this add devices rule.

Enrollment Options

Choose the method you want to use to select the device group that devices will be placed in when they are added using this rule.

Manual	Manually select the device group that devices will be placed in when they are added using this rule.
Based on LDAP Group Membership	Map LDAP groups to device groups. Devices whose user is a member of a specified LDAP group will be placed in the corresponding device group.

Rule Target

Select the device groups this add devices rule will target.
The device groups are presented in a hierarchical tree view. Expand a device group to see the subgroups that are under it.
When you select a device group, all the subgroups under it are also selected.

LDAP Mappings

Map LDAP groups to MobiControl device groups. LDAP groups will be evaluated by the order in which they appear in the mapping table, and devices added to the corresponding device group.
Select LDAP Directory Service to select an LDAP connection from the list, and search for an LDAP group using that connection. If no LDAP connection has yet been configured, select Manage Directory Services to open the LDAP Connections Manager which you can use to configure a new connection.
Select Identity Provider (with LDAP) to select an identity provider connection that is backed by LDAP from the list, and search for an LDAP group using that connection. If no identity provider connection has yet been configured, select Manage IdP Connections to open the Identity Provider Manager which you can use to configure a new connection.
Click Add to add an LDAP group to the mapping table or delete to delete an LDAP group from the mapping table. Use the up and down arrow buttons to move an LDAP group up or down in the mapping table.

Authentication

Select a user authentication method for enrolling devices.
User Authentication Options
Note:
This section appears only if you selected Manual as the device group selection method.

Utilize directory services to authenticate users during device enrollment	Use an LDAP directory service or an identity provider (with LDAP groups) for user authentication. Select **LDAP Directory Service** to select an LDAP connection from the list, and search for an LDAP group using that connection. If no LDAP connection has yet been configured, select **Manage Directory Services** to open the LDAP Connections Manager which you can use to configure a new connection. Select **Identity Provider (with LDAP)** to select an identity provider connection that is backed by LDAP from the list, and search for an LDAP group using that connection. If no identity provider connection has yet been configured, select **Manage IdP Connections** to open the Identity Provider Manager which you can use to configure a new connection.
Password required to verify device enrollment	Specify a single password for enrollment across all devices that enroll using this add devices rule.
No password required to verify device enrollment	Allow devices to enroll without verification.

Certificate Authentication Authority

Issue device identity using	Select the certificate authority that will be used to identify devices.

Terms and Conditions

Select a terms and conditions document that will be sent to devices during enrollment. Users must accept the terms and conditions before they can enroll their devices in MobiControl.

Enable Terms and Conditions to apply at Enrollment	Select this option to send terms and conditions to the device. The user must accept the terms and conditions to enroll the device in MobiControl.
Select the Terms and Conditions	Select the document containing the terms and conditions from the list. **Note:** **The document must be either text or HTML, with Unicode character encoding.**
Manage	Opens the Terms and Conditions Manager in which you can add, edit, or delete terms and conditions documents.
Preview	Shows a preview of the selected terms and conditions document.

Android Management

For access to the Managed Google Play Store, choose which method to use to manage the Android devices enrolling using this add devices rule.

Managed Google Accounts	Manage the devices using Google Accounts created in the Google Admin Console.
Managed Google Play Accounts	Manage the devices using a managed Google Play account. Select the enterprise you want to use from the list.
Skip Google Account Addition During Enrollment on Managed Android Devices	Bypass extraneous device setup steps on Android Enterprise devices.

In this section, you could select "Managed Google Play Accounts" if you have an Enterprise Binding.

Agent Download

Device Agent Download Location
Select the location from which the device agent is downloaded to the device during enrollment.

Download from Google Play	Download the device agent from the Google Play Store.
Download directly from the server	Download the device agent from the MobiControl deployment server.

MobiControl Agent Selection
Select the manufacturers to be displayed on the device enrollment instructions page.

Device Name

Specify a combination of text and macros that are used by MobiControl to create a customized name for each device on enrollment.

Device Name	Enter the combination of text and macros you want MobiControl to use to create a customized name for each device. Click the button to the right of the **Device Name** field to see a menu of available macros. Select a macro to have it appear in the **Device Name** field.

Advanced

Specify advanced options for this add devices rule.
Rule Activation/Deactivation Schedule

Activate Date	Select a date and time on which the rule will be activated.
Specify Deactivation Time	Select this option if you want to select a date and time on which the rule will be deactivated.
Deactivation Date	Select a date and time on which the rule will be deactivated.

Rule Filters
Use one or more add devices rule filters to specify which devices are to be targeted by this rule. Only devices that satisfy all of the listed rule filters will be added by the MobiControl deployment server. See Using Add Devices Rule Filters for more information.

New	Opens a menu from which you can select the type of rule filter you want to add to the list.
Edit	Enables you to edit the selected rule filter.
Delete	Deletes the selected rule filter.

Other Options

Enable Rule	Enables this add devices rule.
Preserve Device Location on Re-enrollment	Preserves the device's membership in its device group when the device is re-enrolled. **Best practices is to uncheck this option.**
Cache Password	Caches the LDAP password entered by the device user during enrollment for 10 minutes. During this time profiles that target the device with configurations that require account credentials (Email, VPN, WiFi, etc.) will include the cached password in the configuration to avoid prompting the user for the same credentials repeatedly.
Publish to Enrollment Service	Generates an enrollment ID for the device agent. In cases where the agent is downloaded from the Google Play Store, the agent can use the enrollment ID to determine which deployment server it should connect to.
Force SHA-1 Client Certificate Distribution	Forces the distribution of SHA-1 client certificates to devices.

Device Enrollment Details

Users can enroll their devices by entering the enrollment ID of the enrollment URL in the device agent.

Enrollment ID	Displays the enrollment ID.
Enrollment URL	Displays the enrollment URL.

Deploying Android Application Using Application Catalog

An application catalog provides a simple method for the controlled distribution of applications to your devices. You choose applications pertinent to your device users and push them to a single location on the device. Once the application catalog is enabled, device users can install the applications directly from the catalog, without worrying about retrieving the correct application or version.
Application catalogs are available on the Android Plus, iOS, and Windows Modern platforms. Each platform contains multiple types of applications. Make sure you choose the one best suited for your needs.
Application catalogs are deployed using application catalog rules, which determine the included applications, targeted devices, and other settings.
Application catalog rules are platform specific - you cannot create a single rule that targets both Android Plus and iOS devices.

Application Types

Application Type	Description
Enterprise	Use for applications that are owned or managed by your organization. You will need to upload the .apk to MobiControl or provide a link to the download location of the file. **Note:** **Enterprise applications are unrelated to the Android Enterprise solution. To install Android Enterprise managed applications on your Android Enterprise devices, use Managed Google Play Applications.**
Google Play Store	Use for applications available through the Google Play Store.
Amazon App Store	Use for applications available through the Amazon App Store.
Managed Google Play	Use for applications available through the managed Google Play store. **Note:** **Only available for Android work managed devices or Android devices with a work profile enabled. Enterprise bindings must be active before you can deploy managed Google Play store apps. Furthermore, you must approve apps within the managed Google Play store for them to appear in the MobiControl list of applications.**

Add Application Catalog (Managed Google Play Applications)

In the **Add Application Catalog** Entry dialog box you can select a managed Google Play application to add to this application catalog a managed Google Play application that has already been added to the catalog.

Binding	Select a primary domain or managed enterprise from the **Binding** list. If the list contains more than one primary domain or managed enterprise, the domain or enterprise that was added first will be initially selected. To update the list of applications that have been approved for the selected primary domain or managed enterprise in the managed Google Play Store, click the **Sync Apps** button.
Search	Enter the name of the application you want to add or click the **Search** button to open the **Search Store for Applications** dialog box.
Enter URL	Enter the URL of the application you want to add.

Application Information
In this section you can enter or review application information such as the display name, version, price, seller, and description.
To select an icon for the application, click on the graphic and select the icon file.
To specify additional settings for the application, click the Advanced button to open the Advanced dialog box.

Device Relocation Rules

A device relocation rule enables you to automatically move devices from one group to another based on a change to the IP address or a custom data configuration. To create a device relocation rule, use the Create Device Relocation Rule wizard.

Rule Name

Enter the name you want to assign to this device relocation rule.

Name	Enter the name you want to assign to this device relocation rule.

Rule Target

Select the device groups this device relocation rule will target.
The device groups are presented in a hierarchical tree view. Expand a device group to see the subgroups that are under it.
When you select a device group, all the subgroups under it are also selected.

Mapping

Specify the device relocation mappings that will be used by MobiControl to move devices from one group to another. Mappings are evaluated in the order in which they appear in the mappings list.
Note:
These mappings are evaluated only when the device connects to the deployment server. If the device is already online when its IP address changes, the device must disconnect and reconnect for the relocation to take place.

Add	Opens the **Add/Edit Device Relocation Mapping** dialog box in which you can create a new device relocation mapping.
Edit	Opens the **Add/Edit Device Relocation Mapping** dialog box in which you can edit the selected device relocation mapping.
Delete	Deletes the selected mapping from the list.
Move Up	Moves the selected mapping up one position in the list.
Move Down	Moves the selected mapping down one position in the list.

Add/Edit Device Relocation Mapping

Add or edit a device relocation mapping based on IP address ranges or a custom data identifier or both.
From the device group list, select the group that devices will be moved to when both the IP address range and the custom data identifier parameters are met. Enter the parameters on the IP Address Range and Custom Data Identifier tabs.

All parameters defined in the mapping must be met for the device to be relocated.

IP Address Range

The IP address of the device is determined at the time the device connects to the deployment server.

IP Address Range	Select this option to enable adding, editing or deleting IP address range parameters.
Add	Adds a new IP address range to the list. Enter the range in the **From** and **To** fields.
Edit	Enables you to edit the selected IP address range.
Delete	Deletes the selected IP address range from the list.

Custom Data Identifier

Custom Data Identifier	Select this option to enable adding or editing custom data identifier parameters.
Name	Select the name of the custom data configuration you want to use. Only custom data configurations that have previously been defined for this rule's target device group appear in the list.

Value	Enter the custom data configuration value you want to specify for this parameter.

Advanced

Specify the date and time you want this device relocation rule to be activated and, optionally, deactivated. You can also choose to enable or disable the rule.
Rule Activation/Deactivation Schedule

Activate Date	Select a date and time on which the rule will be activated.
Specify Deactivation Time	Select this option if you want to select a date and time on which the rule will be deactivated.
Deactivation Date	Select a date and time on which the rule will be deactivated.

Android OS Update and LifeGuard Deployments

With Zebra Android 8 (OREO) based on Mobile Device Platform SD660 (e.g., TC77, TC75x, etc.) and newer only GMS (Google Mobile Services) enabled OS are available (no AOSP). This caused the OS update file to be very huge. To make deployments easier Zebra has started to release delta updates of the OS. Please refer to the OS Update release notes to understand if a delta update is available.

How to deploy OS Updates & LifeGuard updates using Soti MobiControl?

> Below steps are a proposal to achieve the task. Needs to be evaluated for each customer if those steps make sense or not. You should also check on the MDM vendor tool release notes if Zebra FOTA (Firmware Over the Air) is supported/available. If yes, you can connect the MDM tool to the Zebra FOTA (Firmware Over the Air) services but requires a valid Z1C (Zebra 1 Care) contract.

Two-step approach:

First deploy the files to the device and with a second step execute OS Update. The first step is a simple file sync rule which deploys all OS Update files and a supporting file to the /sdcard folder of the device. The second step is either using a Soti script command to send down to device or group of devices to start the OS Update process or creating a Soti MobiControl package which starts the OS Update process. In case of the Soti MobiControl package it could contain an XML file, exported from StageNow, or a Soti Post-Install script.

Example: LifeGuard Update: Using File Sync to copy two files (lifeguard.zip and lifeguard.version.txt) from deployment server to the device to /sdcard. The file lifeguard.version.txt is an INI file with below content/structure:

[LG.Version]

LG.Version=11

The File Sync rule contains a post-sync script to copy the file /sdcard/lifeguard.version.txt to /sdcard/lifeguard.version.ini. The post-sync script will be executed if all files has been synced to the devices. The ini file is used by Soti MobiControl custom data to detect if the File Sync is completed. To read the content from the /sdcard/lifeguard.version.ini file you need to create a custom data on device group level. *Note:* *Do not define custom data on root level because Soti MobiControl writes to device log a huge number of error messages if the custom data cannot be found on the device.* If supported by Soti MobiControl version in use, you should point your rule to a virtual device group. You can drop devices into the virtual device group or create a virtual device group filter to automatically add devices to virtual device group. You can use Custom Attributes as well to easily define devices for the virtual device group. You can find more information regarding virtual device groups, virtual device group filter and custom attributes on the Soti MobiControl Online Help page. Once the files (e.g., lifeguard.zip) is available on the device and confirmed by reading successfully the ini file the update process can start. It is recommended to do this manual to better control the update and monitor the results. Therefore, a Soti Script command e.g., install_system_update /sdcard /lifeguard.zip might be enough to invoke the update process. Soti MobiControl script commands can be issued on device group level. If supported by Soti MobiControl version in use, you can create a filtered virtual device group to easily identify devices ready for upgrade. Filter could contain:

- Current OS / LifeGuard version
- Content of the ini file,
- Etc.

You can find more information regarding virtual device groups and virtual device group on the Soti MobiControl Online Help page.

SureMDM (42Gears)

Deployment of StageNow XML files

Once you have created a staging profile in StageNow, you can export the profile as an XML file. You can then send the XML configuration down to Zebra devices that are enrolled in SureMDM via a run script job.
Process:

1. In StageNow, create a configuration profile for Zebra devices.
2. In StageNow, export the profile. When prompted, select **Export for MDM**.

The exported profile is saved as an XML file.

1. On SureMDM Home, click Jobs -> New Job -> Android -> Run Script

All MX-compatible run scripts for the 42Gears platform should have the following format:

```
!#suremdm
zebra(<StageNow-generated-XML-on-one-line>)
```

Example:

```
!#suremdm
zebra(<wap-provisioningdoc><characteristic type="CameraMgr" version="4.3><parm name="UseAllCameras" value="1/><
/characteristic></wap-provisioningdoc>)
```

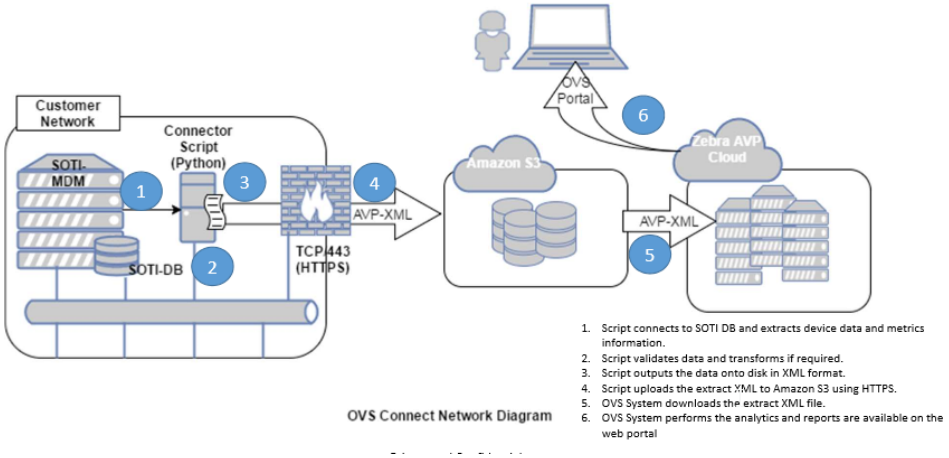
IMPORTANT NOTE: The content of the run script in the parentheses must be a one-liner – use Notepad++ or any other non-formatted text editor to get rid of all \n, LFs, CRs, etc. in the StageNow-generated XML file. More on SureMDM run scripts here.

1. Once run script is ready, push to the device as a job.

VIQ – Connect (on-premises)

If customers host its own EMM/MDM to manage devices, the EMM/MDM needs to be connected to the VIQF portal. There are several options, depending on the EMM/MDM tool and version of the tool used.

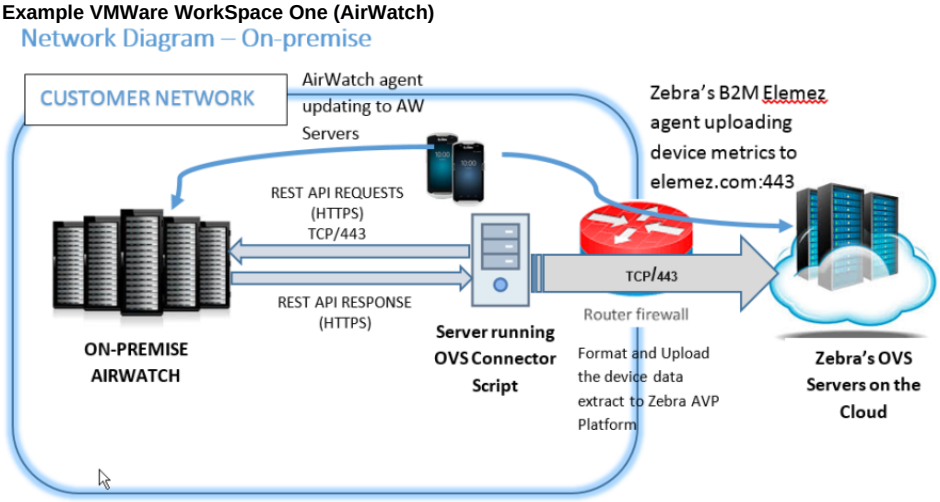
- Python Script and/or REST api to connect to the EMM/MDM database to read the required information, to convert/normalize the data for VIQ and to upload the EMM/MDM information to the Zebra Data Warehouse.
  Example Soti MobiControl



1. Script connects to SOTI DB and extracts device data and metrics information.
2. Script validates data and transforms if required.
3. Script outputs the data onto disk in XML format.
4. Script uploads the extract XML to Amazon S3 using HTTPS.
5. OVS System downloads the extract XML file.
6. OVS System performs the analytics and reports are available on the web portal

OVS Connect Network Diagram

Example VMWare WorkSpace One (AirWatch)



- REST api only (if supported by the EMM/MDM) to read the required information and to upload the EMM/MDM information to the Zebra Data Warehouse. In this scenario, the VIQ-Connect script resides on the Zebra network which does not need to install additional scripts at customer site.

In case of VMWare WorkSpace One (aka AirWatch) and MobileIron EMM/MDM tool the ZDS (Zebra Data Services) agent needs to be activated on Zebra Android Devices. See chapter ZDS.

Soti MobiControl

If the version of Soti MobiControl is v13 or lower the Python Connector script is required. The Connector Script will be installed/configured remotely by Zebra. If Soti MobiControl is on v14 or newer the data will be extracted using REST api calls. It is up to the customer to ensure the Rest api access is granted with the correct read permissions.
The Zebra onboarding PM's takes care of the coordination and drive the implementation.

VMWare WorkSpace One (aka AirWatch)

For VMWare WorkSpace One data will be extracted using REST api.
It is up to the customer to ensure the Rest api access is granted with the correct read permissions.
Below read access is required:

- /api/system
  - /api/system/info

    - /api/system/groups/search/
    - /api/system/groups/{group-id}/children
    - /api/system/users/enrolleddevices/search
- /api/mdm
    - /api/mdm/devices/id

The Zebra onboarding PM's takes care of the coordination and drive the implementation.
Below Device Data will be collected

#	Parameter Name	Comments
1	Id	Numeric Id
2	UDID	Unique ID of the device in the system
3	DeviceFriendlyName	
	LocationGroupId	The 'LocationGroupId' is mapped to the name string from Organization Group Hierarchy
4	Model	Device Model Name
5	MacAddress	Device MAC Address
6	OperatingSystem	Operating System Version
7	LastEnrolledOn	Enrollment Date andn Time
8	Platform	Platform information (Windows/Android etc)
9	SerialNumber	Serial Number of the device
10	LastSeen	Date and Time when device last connected to Airwatch system
11	PhoneNumber	Phone number (for a cellular device)
12	OEMInfo	OEM Information
13	Imei	IMEI (Hardware Identification Number)
14	AcLineStatus	If the device is charging or not

The VIQ Portal organizes the devices under sites. The site information is derived from the organization group hierarchy under which the device is enrolled.
The following information about Organization Group will be read.

- Hierarchy of the group
- Name
- GroupID
- Country

Appendix

Zebra StageNow

Soti MobiControl

Example JSON File Content (Android DO enrollment with StageNow)

Copy below content on Notepad and save with json extension.

```
{
"android.app.extra.PROVISIONING_DEVICE_ADMIN_COMPONENT_NAME":
"net.soti.mobicontrol.androidwork/net.soti.mobicontrol.admin.DeviceAdminAdapter",
"android.app.extra.PROVISIONING_DEVICE_ADMIN_SIGNATURE_CHECKSUM":
"hn8mSNJMPcovWbnnWrb-uMpWZjNlNp-jyV_2A-Whumc=\n",
"android.app.extra.PROVISIONING_SKIP_ENCRYPTION":"false",
"android.app.extra.PROVISIONING_LEAVE_ALL_SYSTEM_APPS_ENABLED":true,
"android.app.extra.PROVISIONING_ADMIN_EXTRAS_BUNDLE":
{
"enrollmentId":"enrollmentId"
}
}
```

Some more information can be found at the Google Android Developers page to be able to implement additional settings during device enrollment into the JSON file:
https://developer.android.com/reference/android/app/admin/DevicePolicyManager
https://developers.google.com/android/management/provision-device

Abbreviations

Abbreviation	Description
DA	Device Administrator
DO	Device Owner
DPC	Device Policy Controller
MDM	Mobile Device Management
MGPA	Managed Google Play Account
OVS	Operational Visibility Service (aka VIQF)
PAS	Printer Administration Server
VIQF	Visibility IQ Foresight (aka OVS)
VIQF-C	Visibility IQ Foresight - Connect
ZDS	Zebra Data Service

Troubleshooting / FAQ

Soti MobiControl

Issue/FAQ	Resolution	Comments
Mobile Device cannot connect to cloud based MDM (Soti MobiControl)	• Check, if FW/Proxy allows outbound connection to MDM Server on port 5494. • Check, if FW/Proxy allows untrusted ssl certificates. By default MobiControl is the issuer of the certificate for the ssl connection. If security policy does allow only certificates that is signed by a recognized Certificate Authority raise a case with Zebra or Soti.	Example of an Soti MobiControl Root Certificate: Common name: MobiControl Server SANs: s00xxxx.mobicontrolcloud.com Valid from December 31, 1999 to June 4, 2030 Serial Number: 77088766621585520 22 (0x6afb6e7b19426bd 6) Signature Algorithm: sha1WithRSAEncrypt ion Issuer: MobiControl Root CA
Printer cannot connect to cloud-based MDM (Soti MobiControl)	• Check, if PAS (Printer Administration Server) is available / ONLINE / configured. • Ensure the PAS communication port is not blocked on FW/Proxy. Port will be provided once the PAS Server is onboarded by Zebra/Soti • Check, if the printer configuration is correct.	
Android Enterprise device does not get apps deployed from managed Google Play Store.	• Check, if Enterprise Binding is configured. • Check, if Enterprise Binding is added to the Add Device rule. • Check, if an Application Catalogue is created and assigned to device or device group.	

ZDS (Zebra Data Service)

Issue/FAQ	Resolution	Comments
What is the package name of the current agent?	There would be two apks • **com.symbol.dataanalytics.apk**This is the main Analytics Engine • **com.symbol.dataanalytics.dca.apk** These are the ious plugins that collect data	
What is the port and IP address that the agent will attempt to communicate to?	Server address: http://analytics.zebra.com Server Port: 443	
How can the customer block the installation of the new agent if they choose to do so? (For example, if a package does not reside on the device, customers can not disable it via MX.)	can be disabled vis AnalyticsManager CSP	
How frequently will the agent report back?	Once in 24 hours	
How much data is sent back during each sync?	~70 KB	
What is the size of the agent?	~2.2 MB	