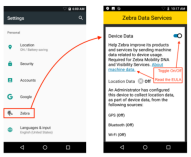
ZEBRA Data Services ZDS Agent Software

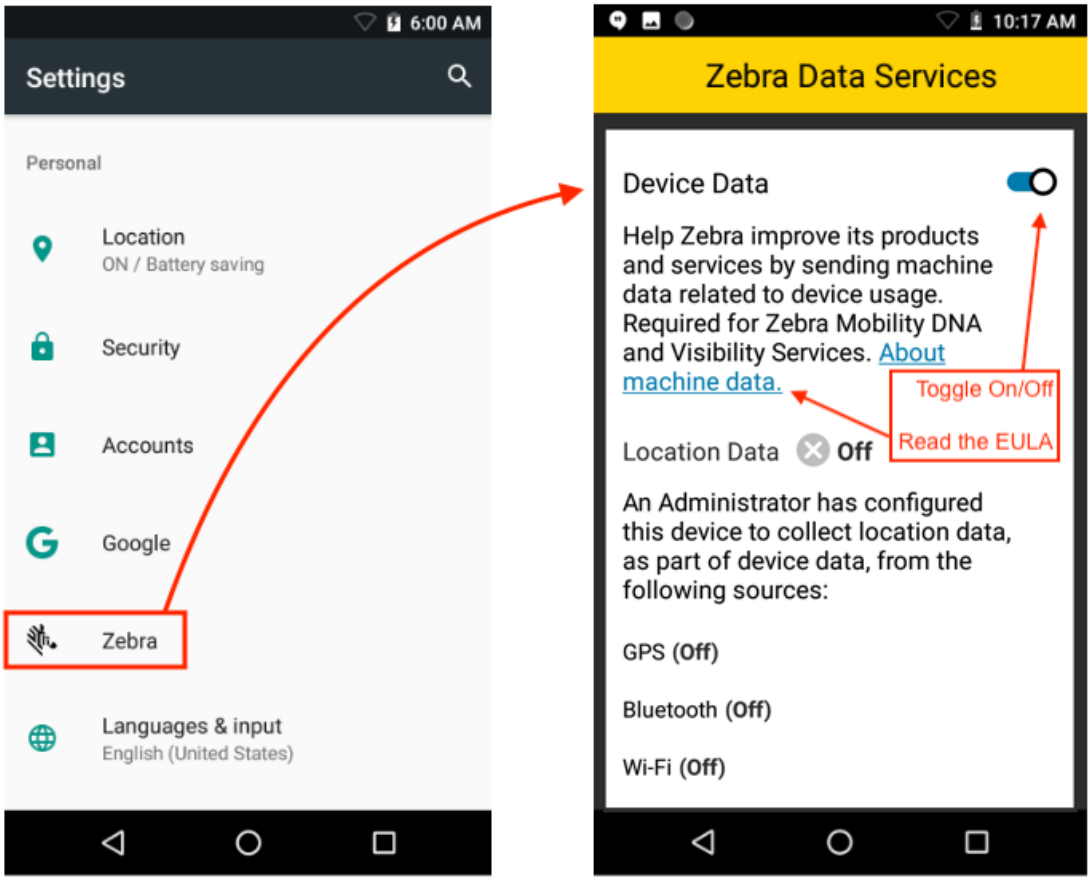


ZEBRA Data Services ZDS Agent Software User Guide

Contents

1 ZEBRA Data Services ZDS Agent Software
2 Specifications
3 Overview
4 Usage Instructions
5 OVERVIEW
6 ZDS RESOURCE REQUIREMENTS
7 PREREQUISITE
8 VERIFY ZDS IS ENABLED ON DEVICES
9 MODIFY ZDS CONFIGURATION
10 HOW TO CHANGE THE CONFIGURATION
11 FAQ
12 Documents / Resources
12.1 References

ZEBRA Data Services ZDS Agent Software



Specifications

- **Product Name**: VisibilityIQTM
- **Software:** Zebra Data Services (ZDS) Agent
- **Release Date**: October 2023
- **Data Upload Frequency:** Default every 24 hours
- **Transport Security:** HTTPS

Overview

Zebra Data Service (ZDS) agent software is a continuous background service running on all supported Zebra devices. It collects and uploads analytics data from ZDS plug-ins and Zebra-authorized third-party apps. Data is transmitted securely via HTTPS and updated automatically.

ZDS data is essential for Zebra's VisibilityIQ (VIQ) service, providing actionable insights for Zebra Android mobile computers. Increasing the data upload frequency to at least 4 times every 24 hours is recommended for improved data availability and accuracy in analytics insights.

Usage Instructions

Types of Configuration

Refer to the user manual for specific instructions on different configurations available for the ZDS agent.

Changing Configuration

To change the configuration of the ZDS agent, follow these steps:

1. Access the ZDS agent settings on your Zebra device.

2. Modify the desired configuration parameters.
3. Save the changes to apply the new configuration settings.

Configuration Files
The ZDS agent uses configuration files to store settings. These files can be accessed and modified to tailor the agent's behaviour according to specific requirements. Refer to the user manual for detailed information on managing configuration files.

OVERVIEW

Zebra Data Service (ZDS) agent software is a continuous background service running on all supported Zebra devices and is responsible for collecting and uploading analytics data coming from ZDS plug-ins and Zebra-authorized third-party apps. ZDS starts collecting and transmitting data from the first time the device is turned on and updates itself and the ZDS Plug-ins automatically. Data is uploaded to the Zebra analytics database every 24 hours by default with transport secured with HTTPS.

Zebra's VisibilityIQ (VIQ) service leverages the data from ZDS agent to provide actionable insight for Zebra Android mobile computers for customers. It's recommended customer should increase the ZDS data upload frequency to at least 4 times every 24 hours to improve data availability and accuracy in analytics insight provided by VIQF and Proactive Battery Replacement (PBR).

ZDS data is required in all VIQF and PBR offerings to ensure users will have the same level of visibility insight no matter whether customer has an MDM in place or not. The table below demonstrates the availability of the VIQF and PBR reports based on different data sources with VIQ offers:

Note:

1. An "x" in a cell indicates the data source in that column can be used to build the report in that row.

2. Color coding:

- Green: indicates the report is available
- white: indicates the report is not available

3. A cell in green color but w/o an "x" means the report can be available by combining other data source.

	VIQ OneCare Data Sources	VIQ Foresight and PBR Data Sources		
	Zebra backend systems	ZDS	42 Gears or SOTI	AirWatch or Mobile Iron
VIQ OneCare Reports				
Contracts	x			
Repair	x			
Repair Lifecycle	x			
Ontime Delivery	x			
Repair Repeat Rate	x			
Repair Return Rate	x			
Top Repair Metrics	x			
Case Lifecycle	x			
LifeGuard Analytics		x		
PBR Reports				
PBR Battery Replacement		x		
VIQ Operational Reports				
Devices				
Total Devices		x	x	x
Devices in Operation*		x	x	x
Newly Activated Devices		x	x	x
Out of Contact Devices		x	x	x
Predictive states		x	x	x
Battery				
Critical Battery Events		x	x	
Battery Swap Activity		x		
Smart Battery Health		x		
Battery Level		x	x	
Battery Discharge Rate		x	x	
Utilization				
Applications Analytics		x		
Device Disruptions		x		
Utilization Rightsizing		x	x	
WLAN Signal Strength		x	x	
Physical Memory		x	x	
Storage Memory		x	x	
Scan Metrics		x		
Geo Locations		x	x	

Note: Devices in Operation require ZDS for full utilization options. SOTI and 42 Gears can provide information only for battery-related utilization. AirWatch and MobileIron require ZDS to compute utilization.
Note: Reports highlighted in yellow require ZDS.
Note: VIQF with MDM uses MDM to provide site information. VIQF using IOT gets site information passed through ZDS. PRB gets site information either via MDM or via ZDS depending on deployment.

ZDS RESOURCE REQUIREMENTS

The following are estimated resource requirements for ZDS:

- ZDS requires approximately 35 MB RAM – 30 MB for code execution and up to 5 MB for data collection buffer.
- The impact of ZDS on battery discharge is normally less than 2% over 24 24-hour period, i.e., is less than .08% discharge rate per hour.
- ZDS transmission/uploads are compressed, and the amount of data transmitted/uploaded per device is on average approximately 70KB or less per day for 24-hour transmission rates, increasing to normally around 80KB per day for 6-hour transmission rates. Measurements have been made for some customers with 4, hours, 2 hours, 1 hour and 30 minute
  transmission/upload rates to have averages of around 85 KB, 225 KB, 250 KB and 400 KB respectively.

PREREQUISITE

For ZDS agent to be able to transmit data to VisibilityIQ, the following prerequisites need to be met:

1. ZDS agent is enabled on all devices
2. Enable network connectivity on devices (WWAN or WLAN-based)
3. Ensure the device can reach the Internet
4. If devices are behind a corporate firewall, ensure the ZDS cloud server can be reached from the devices. The server info and port used by ZDS are listed as below:
    1. **Server 1 address:** **https://analytics.zebra.com**; using IP address 104.198.59.61 on Port: 443
    2. **Server 2 address**: **https://device-https.savannacore.zebra.com**; using IP address: 34.68.84.87 on Port: 443
5. Zebra recommends using ping or a similar network tool to confirm communication between the device network and the ZDS server(s). Once such a connection is verified, all devices on that network should be able to connect to and send collected data to the server(s).

The Zebra Data Service itself uses **connectivitycheck.gstatic.com**, which also must be visible on the network for ZDS operation.

Note: Zebra recommends using DNS server names (instead of IP addresses) when whitelisting (aka “allowlisting”) to avoid service interruptions and required router changes if IP addresses change in the future.

VERIFY ZDS IS ENABLED ON DEVICES

There are two ways that customer can check if ZDS is running on their devices.

1. If the Customer has an MDM with the devices enrolled, they can check if the following package names show up for their devices on the MDM console:

- **com.symbol.dataanalytics.apk** | Main analytics engine for ZDS
- **com.symbol.dataanalytics.dca.apk** | Data collection plug-in for ZDS

2. Customer can also check the ZDS status on the device if they have access to their devices.
   For the detailed procedure to verify that ZDS is running on the device, please refer to the ZDS Verification Guide via the link below:
   https://www.zebra.com/content/dam/zebra_new_ia/en-us/support-and-downloads/visibilityiq/visibilityiq-foresight/VIQ-ZDS-Agent-Verification-Guide.pdf

MODIFY ZDS CONFIGURATION

TYPES OF CONFIGURATION

The following configurations for the ZDS agent can be modified by loading a configuration file (Barcode or XML file) to devices:

1. Enable ZDS applications if disabled Some customers may disable the ZDS agent during device staging. These customers will need to enable the ZDS agent after they purchase the VisibilityIQ Foresight service, so they can view the insight based on ZDS data on the VisibilityIQ portal
2. Change ZDS data upload frequency
   ZDS uploads data every 24 hours by default. If the 24-hour upload default setting is used rather than a more frequent upload setting, it is more likely that a device will miss the data upload window if the device is in “sleep” mode or internet access is not available, hence the analytics insight from VisibilityIQ will be impacted due to lack of data.
   ZDS agent can accept configuration changes such as to the upload interval and data-collection events when needed. It is recommended customers increase the ZDS data upload frequency to at least 4 times every 24 hours.
3. Enable WLAN and/or GPS data collection
   Certain ZDS data used by VIQF/IOT reports are not collected by default. This data includes GPS and WLAN data collection which are not collected by default to protect customer privacy. If a customer has GPS-enabled devices and wishes to view data within the GPS Location report, then GPS data collection must be enabled. Similarly, if the customer wishes to see the last known BSSID in the Out of Contact Report and/or have a fully functional WLAN Signal Strength report, WLAN data collection must be enabled.
   Also, the customer needs to make sure Wi-Fi and/or GPS functionality shall be enabled on devices for related data to be collected.

HOW TO CHANGE THE CONFIGURATION

There are 2 options the customer can change the configuration of the ZDS agent:

Option 1- Using configuration barcodes

Customers can use the barcode file obtained from the Zebra team to change the configuration. This option requires access to the devices and manual procedures. Therefore, it’s suitable for scenarios with a small number of devices to be configured.
Procedure:

1. Open StageNow on the device, and scan in the appropriate barcodes
2. Verify success message in StageNow

3. The device should now be collecting and sending data per the new configuration.

Option 2 – Using XML file

- To configure ZDS agent on large number of devices, a configuration XML file can be deployed via a tool authorized with Zebra MX framework. Typically, these tools are MDMs, test tools, or StageNow.
- Customer can deploy the XML file via MDM or other tools per their existing procedure.

CONFIGURATION FILES
The configuration files (barcodes and XML) can be obtained from the following link:

1. **Enable ZDS agent:**
   https://www.zebra.com/content/dam/zebra_new_ia/en-us/support-and-downloads/visibilityiq/visibilityiq-foresight/VIQ-ZDS-Enable-Configurations.zip
2. **Upload Frequency**
   https://www.zebra.com/content/dam/zebra_new_ia/en-us/support-and-downloads/visibilityiq/visibilityiq-foresight/VIQ-ZDS-Upload-Configurations.zip
3. **Enable WLAN data collection:**
   https://www.zebra.com/content/dam/zebra_new_ia/en-us/support-and-downloads/visibilityiq/visibilityiq-foresight/VIQ-ZDS-WLAN-Enable-Configurations.zip
4. **Enable GPS data collectio**n:
   https://www.zebra.com/content/dam/zebra_new_ia/en-us/support-and-downloads/visibilityiq/visibilityiq-foresight/VIQ-ZDS-GPS-Enable-Configurations.zip

For more detailed information regarding ZDS agent, please follow the link below:
https://techdocs.zebra.com/zds/about/

FAQ

- **What is the purpose of ZDS agent software?**
  - The ZDS agent software collects and uploads analytics data from ZDS plug-ins and authorized third-party apps on supported Zebra devices to provide actionable insights through Zebra's VisibilityIQ service.
- **How often is data uploaded by default?**
  - Data is uploaded to the Zebra analytics database every 24 hours by default.
- **Why is it recommended to increase the data upload frequency?**
  - Increasing the data upload frequency to at least 4 times every 24 hours improves data availability and accuracy in analytics insight provided by VIQF and Proactive Battery Replacement (PBR).

Documents / Resources

ZEBRA Data Services ZDS Agent Software [pdf] User Guide
Data Services ZDS Agent Software, ZDS Agent Software, Agent Software, Software

References

- Document
- Document
- About Zebra Data Service - TechDocs
- User Manual

Manuals+, Privacy Policy

This website is an independent publication and is neither affiliated with nor endorsed by any of the trademark owners. The "Bluetooth®" word mark and logos are registered trademarks owned by Bluetooth SIG, Inc. The "Wi-Fi®" word mark and logos are registered trademarks owned by the Wi-Fi Alliance. Any use of these marks on this website does not imply any affiliation with or endorsement.