

# RUGGED DEVICE MANAGEMENT CHECKLIST FOR IT ADMINS

“ This checklist covers the key areas an IT admin must focus on to secure, deploy and manage rugged devices in the enterprise. “

## CHOOSING RUGGED DEVICES

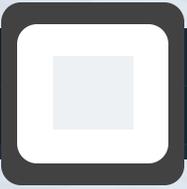
### 1. DETERMINE HOW AND WHERE THE DEVICE WILL BE USED

#### FACTORS TO CONSIDER

- Will the device be used outdoors?
- Will the device be exposed to harsh environments?
- What kind of task will the device be required to perform?
- Does the device need a high-capacity battery to perform extended on-the-field operations?
- Will you need to read the screen in direct sunlight?
- What additional features and integrations will the device require (GPS, RFID, Camera)?

#### WHY THIS IS SIGNIFICANT

With the demand for rugged devices growing, the need for smartphones, tablets, and mobile computers that can perform operations while withstanding harsh environments are jumping up. Look for devices that are certified to withstand rain, sand, and humidity, while also delivering long battery life.



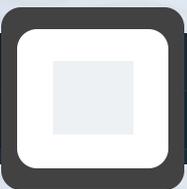
## 2. IDENTIFY WHO WILL USE THE DEVICE

### FACTORS TO CONSIDER

- Will the devices be deployed on a per-user basis, or will the devices be shared?
- Will the device be consumer-oriented or be fully rugged?
- Will the device be used by office personnel or frontline workers?

### WHY THIS IS SIGNIFICANT

To make the right choice when purchasing rugged devices for your organization, you must determine who will end up using the device. If multiple people use the device, look for a less expensive device with the durability to handle frequent drops, bumps, spills and other accidents.



## 3. DETERMINE THE HARDWARE AND OS REQUIRED

### FACTORS TO CONSIDER

- Will your users require mobile computers or tablets for handling industrial operations?
- Will your industrial operations require devices with intense customization features?
- Do your business operations require handling large amounts of data?
- Is battery life and durability a crucial requirement for your devices?

### WHY THIS IS SIGNIFICANT

Android and Windows are the two popular operating systems for rugged devices. When it comes to memory and overall computing power, Windows devices are preferred with their higher memory and advanced operating systems. However, when battery life, durability, and intense customization options are of the essence, Android devices are the better option.

## 4. DETERMINE THE LEVEL OF RUGGEDNESS REQUIRED

### FACTORS TO CONSIDER

- What level of tolerance must your rugged devices uphold?
- Will the device be used in mission-critical assignments?
- Have you determined the minimum IP ratings and MIL-STD-810 tests your rugged devices must meet?

### WHY THIS IS SIGNIFICANT

You can determine the level of ruggedness of a device by employing a couple of tests. These include the US military standard (MIL-STD-810) tests, which determine whether commercial devices can efficiently operate under different environmental conditions, and the Ingress Protection (IP) scale ratings, which define the sealing effectiveness of the devices against intrusion from solid or liquid particles. In the simplest terms, rugged devices may be classified as semi-rugged, fully-rugged, or ultra-rugged, depending on their overall rugged characteristics.

## DEPLOYING AND MANAGING RUGGED DEVICES

## 1. EVALUATE YOUR WORKFORCE AND DETERMINE THE DEVICE DEPLOYMENT METHOD

### FACTORS TO CONSIDER

- Will the device be used for personal services, or is it a corporate-only device?
- Have you identified the operating systems for your rugged devices and determined their supported deployment methods?
- Do you require the devices to be deployed out-of-the-box to end-users?

### WHY THIS IS SIGNIFICANT

To choose a suitable deployment method, you must first evaluate your corporate requirements. Look for a Unified Endpoint Management (UEM) solution that supports zero-touch deployment options. If you plan to deploy Android devices, make sure to enroll your organization in the Android Enterprise Recommended program, and confirm the UEM supports Android Enterprise enrollment.

## 2. IDENTIFY POLICIES AND CONFIGURATIONS TO MANAGE RUGGED DEVICES

### FACTORS TO CONSIDER

- Will you need to lock down rugged devices to just a required set of applications and services?
- Will you need to enforce restrictions and security configurations on rugged devices?
- For Android devices, does your organization require OEMConfig support from popular rugged device vendors?
- Have you implemented mechanisms to encrypt and secure the data stored on rugged devices?
- Do you require setting up network security and access management policies on rugged devices?
- Have you enforced a mechanism that deploys and manages the necessary work apps on rugged devices?
- Do you have a mechanism in place that manages OS updates and patches on rugged devices?

### WHY THIS IS SIGNIFICANT

To enforce a strong rugged device management strategy, identify the policies and configurations your business requires and look for a UEM solution that supports these functionalities. In addition, popular vendors like Google have their own offerings for managing rugged devices (such as Android Enterprise Recommended and OEMConfig). Again, look for a UEM solution that provides ample support for such offerings.

## 3. MONITOR RUGGED DEVICE USAGE, TRACK COMPLIANCE, AND GENERATE REPORTS

### FACTORS TO CONSIDER

- Will you need to regularly monitor the health and status of your rugged devices?
- Will you need to monitor the location of rugged devices and lock them down when outside work zones?
- Will you need to maintain a record of the online history, network usage, and apps installed on rugged devices?
- How will you ensure your policies and configurations maintain compliance with regulatory guidelines?

### WHY THIS IS SIGNIFICANT

A remote monitoring strategy helps maintain compliance and reduce device downtime by providing real-time troubleshooting capabilities that help monitor device usage and proactively resolve potential issues. Look for a UEM solution that provides effective monitoring capabilities, including remote view and control, location tracking, remote commands, and more, and is capable of maintaining compliance with the necessary regulatory guidelines.