techstep

Techstep Essentials MDM

Getting started

Date: 25/08/2023

Contents

1 Introduction 4
2 The first step – how to log in 5
3 Integrate with Apple and Android 6
4 Creating users and groups 7
5 Handling policies 7
6 Adding devices 7
7 Sending operations to devices 8
8 Monitoring devices and system 8

PUBLISHED BY:

Techstep Poland S.A.
Ul. Wajdeloty 12A
80-437 Gdańsk
Copyright© 2008-2023 by Techstep Poland S.A.

All rights reserved. The entire content of the document is the exclusive property of Famoc S.A. and may not be reproduced or distributed without the written consent of the publisher. The publication may contain brands and product names that are trademarks or registered trademarks of their respective owners.

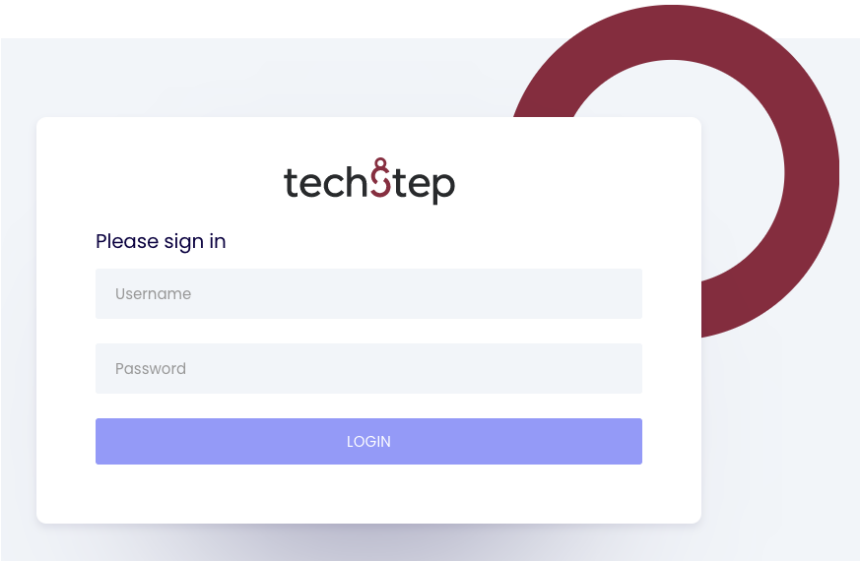
SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS AND SERVICES INTRODUCED IN THIS MANUAL ARE SUBJECT TO CHANGES. ANY INFORMATION AND RECOMMENDATIONS PROVIDED IN THIS DOCUMENT IS RELEVANT, HOWEVER, ALL RESPONSIBILITY FOR THE IMPLEMENTATION AND USE OF THE PRODUCTS AND SERVICES IS WITH THE USERS

1 Introduction

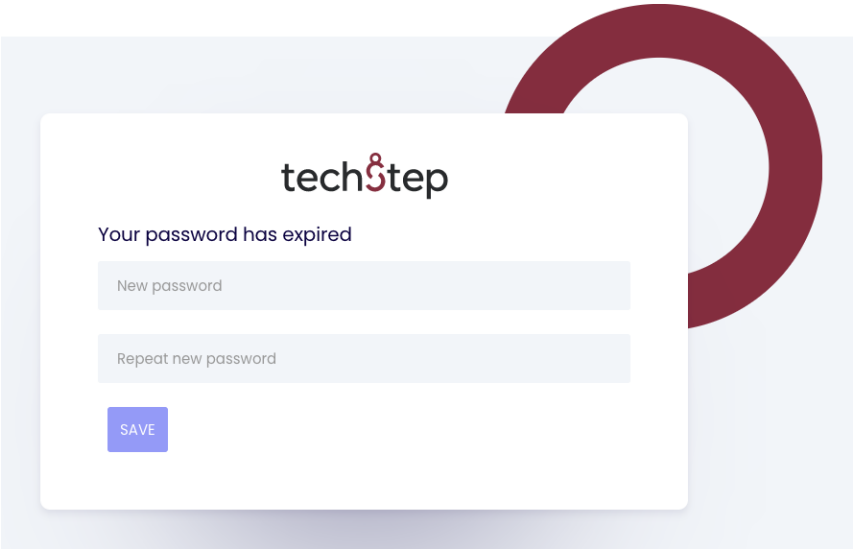
Hi! The fact that you are reading this documentation means that you have decided to use our system, for which we thank you very much. Now we'll walk you through the basics of setting up Essentials MDM and setting up your environment to efficiently manage your devices. We start with... logging in.

2 The first step – how to log in

The credentials are provided by Techstep. You will enter the credentials here:



Normally you will have to change the password at first login:



3 Integrate with Apple and Android

There are two critical integrations for Android and Apple.

- Apple Push Notification service is the MDM protocol created by Apple to manage their devices. It requires the MDM provider to have a valid APNs certificate configured. For more information, see Apple push notification integration guide.
- Managed Google Play allows you to publish, manage and distribute applications in your enterprise's Google Play Store. These applications will be available for users in the Google Play app on Android devices with a managed work profile. Android Enterprise allows you to create managed work profiles on Android devices. The same Google account is used for both services. You can find out more here: Android Enterprise & Managed Google Play guide

If you want to easily enroll and manage Apple and Android devices, then consider:

Apple

- Apple Business Manager is a simple, web-based portal for IT administrators that works with Techstep Essentials MDM solution for buying apps, automated enrolment for iPhone, iPad and Mac. For more information, visit Integration with Apple Business Manager and VPP (Volume Purchase Program).
- Synchronization with Apple Device Enrolment Program provides a fast and easy way to enrol iOS devices into Techstep Essentials MDM. For more information, visit Apple DEP integration guide.
- Apple VPP is a simple, easy to use solution to bulk purchase, distribute and manage apps and books on Apple devices. You can find more information here

Android

- Knox Mobile Enrollment is the quickest and most automated way to enroll a large number of Samsung devices to your Essentials console for corporate use. For more information, visit Samsung KNOX Mobile Enrollment .
- Android Enterprise zero-touch allows enterprises to enrol corporate devices to Essentials without a necessity of going through the manual enrolment procedure. For more information, visit Android zero-touch integration.

If you have both systems, please do all.

4 Creating users and groups

Before you start to enrol devices, you will have to create users, and eventually user and/or device groups. The user is necessary because someone must be assigned to the device and these can be real users/employees added manually or imported from the users directory.

Each user can be assigned to a specific group. This feature is useful when managing a large number of devices and users as it allows users to be grouped by similar requirements and group actions to be carried out.

- Creating users in Techstep Essentials MDM.
- Creating groups in Techstep Essentials MDM.

5 Handling policies

This is the most important part of the settings / restrictions that are applied on the devices. It covers components (apps and configurations) automatically applied on the device, security restrictions, and any other basic settings. Based on the device mode (fully managed, BYOD, WPC, COSU) and user / device groups assignment, device is attached to the proper policy. You can find more information by visiting overview over policies .

6 Adding devices

Adding devices, both Android and Apple in Essentials, can be done in several ways depending on the device mode. Below you will find some examples:

- Fully managed – in this mode we fully control corporate devices
  - Adding Android device in fully managed mode.
  - Adding iOS device in fully managed mode.
- BYOD mode is the typical use of private owned devices in a company.
  - Adding Android device in BYOD mode
  - Adding iOS device in BYOD mode.
- WPC mode – it is container for business data on a company device and at the same time the possibility of private use.
  - Adding Android device in WPC (work profile on company owned devices)
- COSU mode - dedicated device for specific purpose (single app / launcher with limited apps)
  - Adding Android dedicated device (COSU).

7 Sending operations to devices

To manage devices on a day-to-day basis, you can perform various operations like adding new devices, installing agents or applications, configure some functionalities, apply policies etc. You can find more information here

8 Monitoring devices and system

Here you will find more information on how to view the status of devices and applications managed by Essentials and monitor system alerts. You can find more information here: Monitoring the system .