WINCOR NIXDORF

BEETLE /moPOS Device Hub

Mobile POS solution

Security Advice

(July 2015)

We would like to know
your opinion on this publication.

Please send us a copy of this page
if you have any constructive criticism on:
- the contents
- the layout
- the product.

We would like to thank you in advance
for your comments.
With kind regards,

Wincor Nixdorf International GmbH
R&D, SAT11
Wohlrabedamm 31

D-13629 Berlin

E-Mail: retail.documentation@wincor-nixdorf.com

Your opinion

Contents

1 Introduction

THIS SECURITY ADVICE FOR BEETLE /moPOS DEVICE HUB (“ADVICE”) ONLY INFORMS ABOUT SOME POSSIBLE PREVENTIVE MEASURES TO ENABLE USERS OF THE BEETLE /moPOS TABLETS, BEETLE /moPOS DEVICE HUBS AND WIFI ROUTERS TO BETTER SECURE SUCH AGAINST FRAUD ATTACKS. EVEN WHEN FOLLOWING THE COMPLETE ADVICE, THIS MAY NOT SECURE AGAINST BREACHES, SECURITY ISSUES AND POSSIBLE DATA LOSSES. THE RESPONSIBILITY TO SECURE THE USE AND OPERATION OF BEETLE /moPOS TABLETS, DEVICE HUBS AND WIFI ROUTERS NEEDS TO BE CAREFULLY AND INDIVIDUALLY CONSIDERED BY THE USER.

This document provides a baseline guide to secure the BEETLE /moPOS Device Hub as recommended by WINCOR NIXDORF International GmbH (hereinafter “Wincor Nixdorf”).

The following recommendations in this baseline guide are intended for use on the tablets, POS Device Hubs and WiFi routers of a BEETLE /moPOS System, but most are product-independent.

Following chapters describe different aspects of security and their recommended configuration.

2 Abbreviations

IP	IP stands for Internet Protocol. An IP address is a network address which is a prerequisite for identifying and accessing network enabled devices. Typically IP addresses are either static or dynamically assigned via a DHCP server.
LAN	Local area network: wired network infra-structure
SSID	SSID stands for Service Set Identifier ; this is the name of a wireless network to be entered when connecting from mobile devices to a router
POS	Point of Sale
WEP	Wired Equivalent Privacy a type of weak encryption used for WiFi communication
WPA	Wi-Fi Protected Access
WiFi	Wireless local area network. Also known as WLAN

3 BEETLE /moPOS Device Hub

3.1 Passwords

Make sure that each password used on the BEETLE /moPOS Devices Hub follows the general rules as defined below.

3.2 Network host name

After first initial login make sure the network host name will be set to an appropriate unique name for customer network environment.

4 WiFi router

For connecting mobile devices and BEETLE /moPOS Device Hubs a market-usual WiFi router needs to be used. Some recommendations and prerequisites need to be fulfilled to have a working configuration.

The WiFi router does not have to be a Wincor Nixdorf product. Usual WiFi routers from the market can be used as long as they meet the requirements and recommendation for communication with mobile tablets.

Detailed recommendations regarding wireless security can also be found under the following link https://www.pcisecuritystandards.org/security_standards/documents.php with the tab “Fact Sheets & Info Supps” and the document “PCI DSS 2.0 Wireless Guidelines”. The document describes different requirements and can be used in addition to this document.

4.1 WiFi encryption

The WiFi router shall use a strong encryption such as WPA2. If possible, IEEE 802.1X/EAP should be the preferred authentication method. Otherwise a true random pre-shared key (PSK) with at least 13 characters can be used. The PSK should be changed on regular basis.

Typically WEP must not be used as a security control for wireless networks since meanwhile estimated as too weak for encryption.

If the data of card reader are transferred over the wireless connection, you should consider using strong cryptography such as TLS 1.2 within the software stack.

4.2 Change default settings

Change default PSK if not using IEEE 802.1X/EAP.

Change the default SSID name in order not to provide information about the hardware used.

Close down management interfaces of the access point and disable unnecessary applications, ports and protocols.

4.3 Strong Passwords

Make sure that each password usable on the BEETLE /moPOS Device Hub follows the general rules as defined below.

Set up a firewall with proper configuration. For security reasons it is recommended to forbid routing ALL ports from the WiFi network to the LAN network. However, for usage of BEETLE /moPOS some of the open ports and protocols should be restricted to the minimum. For required ports see “getting started”.
In general, allow only ports which are necessary. Disallow ports which are not required.

The wireless network should be segmented from the corporate network.

5 Usage of Password

5.1 Default Passwords WebGUI

The POS Device Hub can be configured with an HTTP-based web administration Graphical User Interface (in the following text referred as WebGUI). After first initial login into WebGUI please change the password of the WebGUI to an individual password. Do not continue using the default password as delivered from factory. The password of the WebGUI need be set in appropriate length and complexness to avoid easy investigation by non-authorized users.

5.1.1 Default System Passwords

After first initial login into WebGUI please make sure that all passwords will be exchanged with your desired passwords. The passwords of all users (such as upload-fw, upload-media, upload-config, upload-plugins,…) need to be set in appropriate length and complexness to avoid easy investigation by non-authorized users. In the WebGUI you will find a dialog under Configuration /passwords.

5.2 Length and complexness of passwords

For security it is important that used passwords are long enough and have a certain complexity. A password just containing a usual word or passwords containing just "hello" "1234" etc. do definitely not follow state of the art security.

It is recommended to use passwords with

- at least 10 characters,
- containing at least four letters (recommended to use at least one upper and lower case),
- containing at least one number,
- containing at least one special character,
- not containing the user ID,
- being different from the last passwords.

5.3 Live time of Passwords

For security it is important to change in an appropriate regular time interval used passwords. Appropriate means in that context that it fits to customer's security guide lines. Especially in case there is a suspicion that a password might become public or compromised it needs to be changed at the system so that old password is not usable any more.

Therefore, it is a strong recommendation to change passwords in regular time interval.

5.4 Entering wrong passwords

In general, the BEETLE /moPOS Device Hub handles cases of wrong input of passwords as following:

In case end user enters three times a wrong password the assigned user is blocked and you cannot continue trying to login.

To unblock the user you need to reboot the POS Device Hub. For this, local physical access to the POS Device Hub is required. Alternatively - without rebooting -after 10 minutes you may re-login.

These settings for the POS Device Hub affect either the Web administration password or the passwords for the user's upload-fw, upload-media, upload-config, upload-plugins.

For tablets, integrators shall provide similar mechanisms. When entering wrong passwords for the usual POS user three times the system should block concerning this user. Since a tablet is mobile, it should not be sufficient to just reboot for making the user unblocked.

Please follow industry best practices for mobile devices when using in an industrial environment.

6 Avoiding usage of compromised tablets

Since a table is a mobile device the risk of theft is even higher than a traditional POS system. In case a tablet should be considered as compromised due to this or other reasons it is recommended to handle this also by the BEETLE /moPOS due to some actions to avoid the possibility of continue using the tablet:

- In the BEETLE /moPOS WebGUI make sure that the tablet will be removed from the list of available tablets.
- Usually if the login account handling on the tablet is done in the way that a login will be locked after a while of inactivity the tablet should be locked when taken away from the store.
- In case the mass storage encryption tool has been used on the tablet. The mass storage on the tablet should not be readable without knowledge of the valid encryption key.
- If using a PSK on the WiFi, this should be changed if a tablet is considered to be compromised.

7 EFFECT; ENFORCEABILITY; DISCLAIMER

THIS ADVICE DOES NOT CONSTITUTE AN OFFER TO PURCHASE OR LICENSE, NOR AN AGREEMENT OF ANY KIND, AND BY THIS ADVICE NO SUCH AGREEMENT SHALL BE DEEMED TO EXIST. THIS ADVICE IS NOT INTENDED TO NAME, AND DOES NOT CONSTITUTE BINDING NOR COMPLETE NOR INDIVIDUALISED RECOMMENDATIONS BY WINCOR NIXDORF, BUT IS MERELY INTENDED TO NAME SOME BASIC AND ABSTRACT PROPOSALS; THEREFORE NO CLAIM NOR ANY LEGAL RIGHTS AGAINST WINCOR NIXDORF MAY BE BASED ON THIS DOCUMENT. FOR THE NAMED PROPOSALS AND RECOMMENDATIONS ANY WARRANTY IS EXCLUDED. WINCOR NIXDORF SHALL HAVE NEITHER LEGAL NOR FINANCIAL OBLIGATIONS WITH RESPECT TO THE ADVICE, UNLESS SUCH HAVE BEEN MUTUALLY AGREED IN A WRITTEN AND BINDING CONTRACT, WHICH HAS BEEN PROPERLY EXECUTED AND AT LEAST SIGNED BY WINCOR NIXDORF.

Wincor Nixdorf International GmbH
D-33094 Paderborn
Order No.: ***01750280321A***