Oracle® MICROS Tablet 700 Series

Security Guide

E86335-04

June 2020

ORACLE

E86335-04

Contents

Tables

Preface

Audience

This document is intended for those who set up, install, and operate Oracle MICROS Tablet 700 Series tablets. It is not specific to a particular software application.

Customer Support

To contact Oracle Customer Support, access My Oracle Support at the following URL:
https://support.oracle.com

When contacting Customer Support, please provide the following:

- Product version and program/module name
- Functional and technical description of the problem (include business impact)
- Detailed step-by-step instructions to recreate
- Exact error message received and any associated log files
- Screenshots of each step you take

Documentation

Oracle Hospitality product documentation is available on the Oracle Help Center at
http://docs.oracle.com/en/industries/food-beverage/

Revision History

Date	Description of Change
December 2017	• Updated to include Tablet 721
March 2019	• Added TPM information
April 2020	• Updated to include Tablet 721P

1 Oracle MICROS Tablet 700 Series Security Overview

This chapter provides an overview of Oracle MICROS Tablet 700 Series security features and explains general device security principles.

Basic Security Considerations

The following principles are fundamental to using any hardware or software securely:

- Keep software up to date. This includes software specific to the product as well as the latest patches available from third party vendors.
- Limit account privileges as much as possible. Users should only be given the access necessary to perform their work. User privileges should be reviewed periodically to determine relevance to current work requirements.
- Install software securely. For example, use firewalls, secure protocols using TLS (SSL), and secure passwords. See Performing a Secure Tablet 700 Series Installation for more information.
- Monitor system activity. Establish who should access which system components, and how often, and monitor those components.
- Learn about and use the Tablet 700 Series security features. See Implementing Tablet 700 Series Security for more information.
- Use secure development practices. For example, take advantage of existing database security functionality instead of creating your own application security.
- Keep up to date on security information. Oracle regularly issues security-related patch updates and security alerts. You must install all security patches as soon as possible. See the Oracle Critical Patch Updates and Security Alerts web site: http://www.oracle.com/technetwork/topics/security/alerts-086861.html

Overview of Tablet 700 Series Security

The 700 Series tablets are ruggedized mobile devices that incorporate a mixture of hardware and software components commonly found in Microsoft Windows-based devices. For peripherals connectivity, industry standard ports have been integrated on-board.

Table 1 – Tablet 700 Series Hardware Component Overview

Feature	Tablet 720	Tablet 721/721P
Processor	Intel Atom Quad Core, 1.33GHz	Intel Atom Quad Core, 1.44GHz
RAM	2GB	4GB
Storage	64GB Flash	64GB Flash
TPM	Intel Bay Trail fTPM 2.0 (Disabled by default)	Intel Cherry Trail fTPM 2.0 TCG 2.0 compliant (Disabled by default)

Feature	Tablet 720	Tablet 721/721P
Operating System	Microsoft Windows Embedded 8.1 Industry Pro - or - Microsoft Windows 10 IoT Enterprise 2016 LTSB	Microsoft Windows 10 IoT Enterprise 2016 LTSB Microsoft Windows 10 IoT Enterprise 2019 LTSC
Display	7-inch LED-Backlight Screen with Capacitive Touch	7-inch LED-Backlight Screen with Capacitive Touch
Display Resolution	1280 x 800	1280 x 800
WLAN	Wi-Fi 802.11a/b/g/n	Wi-Fi 802.11a/b/g/n/ac
Bluetooth	Bluetooth 4.0 LE	Dual Mode Bluetooth 4.2, BLE
USB Port	USB 2.0 x 1	USB 3.0 x 1
Headset Jack	1	1
DC In	1	1
AC/DC Adaptor	Input: 100 – 240V AC; Output: 5V DC, 3A	Input: 100 – 240V AC; Output: 12V DC, 5A
Battery Pack	Replaceable rechargeable Li-ion battery, 3.7V, 4000mAh Backup/Bridge Battery: 240mAh	Replaceable rechargeable Li-polymer battery, 3.6V, 8800mAh Backup/Bridge Battery: 240mAh
Enclosure	ABS + PC plastics	ABS + PC plastics
Dimensions (H x W x D)	5.24 in x 8.26 in x 0.93 in 133 mm x 210 mm x 23.5 mm	Tablet 721: 5.24in x 8.75in x 0.7in 133mm x 210mm x 18mm Tablet 721P: 7in x 10in x 2in 177.8mm x 254mm x 50.8mm
Temperature	Operation: 0 °C (32 °F) to 40 °C (104 °F) Storage: -20 °C (-4 °F) to 60 °C (140 °F)	Operation: 0 °C (32 °F) to 40 °C (104 °F) Storage: -20 °C (-4 °F) to 60 °C (140 °F)
Humidity	0% to 90% Non-Condensing	0% to 90% Non-Condensing
Weight	1.31 lbs (0.59 kg)	Tablet 721: 1.31 lbs (0.59 kg) Tablet 721P: Up to 2 lbs (0.91 kg)
Magnetic Stripe Reader	Triple Track Readers (ISO TK1, 2 & 3), JIS & AAMVA Compliant	Triple Track Readers (ISO TK1, 2 & 3), JIS & AAMVA Compliant
Barcode Scanner	Optional; 1D/2D Barcode Scanner	Optional; 1D/2D Barcode Scanner
NFC/RFID	Optional; Supports ISO/IEC 14443 A Reader/Writer Mode @ 13.56MHz	Optional; Supports ISO 14443A/B, ISO 15693, MIFARE Ultralight, and FeliCa Reader/Writer Mode @ 13.56MHz

Table 2 – Tablet 700 Series Software Architecture Overview

Feature	Tablet 720	Tablet 721/721P
Operating System	Microsoft Windows Embedded 8.1 Industry Pro - or - Microsoft Windows 10 IoT Enterprise 2016 LTSB	Microsoft Windows 10 IoT Enterprise 2016 LTSB Microsoft Windows 10 IoT Enterprise 2019 LTSC
Boot Firmware	UEFI – Insyde H20 based	UEFI – Insyde H20 based

Understanding the Tablet 700 Series Environment

When planning your Tablet 700 Series implementation, consider the following:

- Which resources need to be protected?
- You need to restrict access to external ports, such as the USB port.
- You need to protect customer data, such as credit card numbers.
- You need to protect internal data, such as proprietary source code.
- You need to protect system components from being disabled by external attacks or intentional system overloads.
- Who are you protecting data from? For example, you need to protect your subscribers' data from other subscribers, but someone in your organization might need to access that data to manage it. You can analyze your workflows to determine who needs access to the data; for example, it is possible that a system administrator can manage your system components without needing to access the system data.
- What will happen if protections on a strategic resource fail? In some cases, a fault in your security scheme is nothing more than an inconvenience. In other cases, a fault might cause great damage to you or your customers. Understanding the security ramifications of each resource will help you protect it properly.

Physical Security

Point-of-Sale mobile tablets are implemented in environments where physical access to the devices can be difficult or impossible to control. The devices are typically used in publicly accessible areas based on optimal usage for employees rather than secured computer rooms. When not in use, tablets should be secured in a locked cabinet or room to ensure their physical security.

Factory UEFI Firmware Settings

The UEFI Firmware provides several security settings that are not enabled or configured securely by default. In order to be configured securely, installation environment specific settings, such as passwords, will need to be created. The following settings are available in the firmware and should be enabled/configured during the installation:

- Secure Boot
- Supervisor Password

Factory Windows Installation Settings

The factory operating system installation includes several changes to settings, policies, and services that are installed by default in Windows. The following items have been modified from the defaults in order to improve operating system performance and security out of the box:

- Local Security Policy modifications
    - Enabled clear pagefile at shutdown
    - Disabled Internet Explorer legacy TLS and SSL protocols
    - Enabled Windows Update auto-install daily at 3:00AM
    - Default Administrative shares removed
    - Disabled the default lock screen (Tablet 721/721P)
    - Disabled password entry on Wake (Tablet 721/721P)
- Windows Applications/Services modifications
    - Windows store uninstalled
    - Internet Information Services uninstalled
    - Homegroup Provider disabled (not available in Microsoft Windows 10 IoT Enterprise 2019, Build 1809)
    - Windows Media Services disabled
    - UPnP disabled
    - Autoplay disabled
    - WifiSense disabled (Microsoft Windows 10 only)
    - OneDrive disabled (Tablet 721/721P)
    - Auto Defragment drives disabled
- Network Shares

User Accounts in Factory Installations

The preinstalled factory operating system should not contain any default user accounts or passwords. During the first boot, the user will be required to create an administrative user account and provide a password. Administrative users should not be used for day to day operation of the device.

Windows Defender and Windows Firewall in the Factory Installations

Windows Defender and Windows Firewall are provided in the factory operating system installation for all configurations of the Tablet 700 Series. The definitions are updated with the current version available at the time the factory operating system was created.

Factory Recovery

The Tablet 700 Series can be restored to its original factory shipped state by performing a USB system recovery. In situations where the device or its operating system is believed to be compromised, this feature can be used to quickly restore the operating system to the factory settings. This feature wipes the contents of the entire disk.

The *Oracle MICROS Tablet 700 Series Setup Guide* contains instructions for performing a system recovery.

2 Secure Tablet 700 Series Installation

This chapter presents planning information and basic guidance for your Tablet 700 Series installation. Please consult your IT Security Officer for any security decisions or requirements that pertain to your operating environment.

Pre-Installation Security

- Review the *Oracle Hospitality MICROS Hardware Wireless Networking Best Practices Guide* for help with Wi-Fi connections.
- Review a network diagram for the installation environment. Verify the device will only be installed on secured networks behind a hardware firewall.
- Determine out-of-box operating system security settings. Some information is needed for Windows out of box setup. The first boot will require configuring an administrative account, network connection settings, and the computer name.
- Determine a safe and secure location to leave devices unattended if charging or docking stations will be utilized.

Secure Tablet 700 Series Implementation

Physically Securing the Device

Point-of-Sale mobile tablets are implemented in environments where physical access to the devices can be difficult or impossible to control. The devices are typically used in publicly accessible areas based on optimal usage for employees rather than secured computer rooms. When not in use, tablets should be secured in a locked cabinet or room to ensure their physical security.

- Consider storing the devices in a controlled environment, such as an office or locked cabinetry, when not actively being used.
- Install any multi-bay chargers in a locked room if applicable.
- Set up a designated area for charging devices that is inaccessible to the general public.

Windows Out-of-Box Setup

All configurations of the Tablet 700 Series come with a preinstalled version of Microsoft Windows. The first time the device is booted, the Windows Out-of-Box Experience will launch in order to capture operating system configuration information including user accounts, computer name, and network connection settings.

General guidance for out-of-box setup:

- Picking a network connection.
  Only connect to secure wireless networks. Networks using older key-exchange protocols, such as WEP, are not secure.
- Choose to Customize Settings.
  The Windows Express installation settings are convenient, but may enable unnecessary operating system features for the use case of the device. Features such as WifiSense or Location Services are examples of settings that are configurable using these setup screens.
- Creating an account for the PC.
  The initial user created by Windows setup will have administrative privileges in the system. Avoid choosing user names that leak information, such as the privilege level. Use complex passwords for all Administrative and Standard user accounts.

- Computer Name.

  Windows 8.1: When entering the computer name of the device, avoid choosing a computer name that leaks information about device. For example, entering Windows81POSTerminal1 allows an attacker with network access to immediately determine the operating system version and the purpose of the device.

  Windows 10: The setup process automatically sets a random computer name during installation.

3 Implementing Tablet 700 Series Security

Physical Security

- Regularly inspect physical security, such as covers and screws, are present.
- Regularly inspect the device and its peripherals for signs of tampering.
- Regularly inspect the device for any unusual devices that have been attached to the device.

UEFI Firmware Security

- Set a Supervisor Password.
  A supervisor password will prevent unauthorized access to the UEFI firmware setup and configuration user interface. This ensures that only authorized users can modify any settings configured after the installation. Users will have three attempts at keying the correct password. After three failed attempts to enter the supervisor password, entry to the UEFI setup will become locked.

  If the supervisor password is forgotten or lost, it cannot be recovered or cleared. If further UEFI setup changes need to be made, the device will need to be repaired by a qualified Oracle repair facility.

  See the *Configuring Tablet 721/721P System Security Settings* section of the *Oracle MICROS Tablet 700 Series Setup Guide* for information on enabling this setting.

- Enable secure boot.
  Secure boot is an effective defense against low level malware that attacks the boot code used to start the operating system. Malware at this level can remain completely undetected by some security software installed at the operating system level, and cannot be removed easily.

  See the *Configuring Tablet 721/721P System Security Settings* section of the *Oracle MICROS Tablet 700 Series Setup Guide* for information on enabling this setting.

  A firmware supervisor password is required to enable secure boot. If enabling a supervisor password is undesired, set the password temporarily to enable secure boot. Once secure boot has been enabled, the password can be cleared (not recommended) as long as the current password is known.

Operating System Security

- Drive Encryption.
  Drive encryption can protect data stored on the hard drive when physical security controls have failed. All models of the Tablet 700 Series come with versions of Microsoft Windows that support Bitlocker drive encryption.
- Application Whitelisting.?
  Application whitelisting allows administrators to define the applications permitted to run on the device. All models of the Tablet 700 Series come with versions of Microsoft Windows that support the AppLocker feature.

Refer to the vendor's documentation for operating system security information and features.

- Windows 10 IoT Enterprise Edition Security Features
  https://technet.microsoft.com/en-us/library/mt589972(v=vs.85).aspx

Additional Reference Documents

The following documents provide standards and additional guidance for operating system hardening and maintaining a secure operating system environment:

- PCI DSS
  https://www.pcisecuritystandards.org/security_standards/index.php
- Center for Internet Security (CIS) Benchmarks (used for OS Hardening)
  https://benchmarks.cisecurity.org/downloads/multiform/

Appendix A: Secure Deployment Checklist

The following security checklist includes guidelines that help secure your device:

- Ensure all covers and security screws are installed.
- Monitor system access.
- Use Secure Boot.
- Enforce access controls effectively.
    - Lock and expire default or temporary user accounts used during installation.
    - Enforce password management.
    - Practice the principle of least privilege.
    - Grant necessary privileges only.
    - Do not use administrator accounts for daily operations.
    - Ensure unnecessary network shares have been removed.
- Only install system components required for the use case.
- Ensure remote access software has been disabled.
- Use a firewall to restrict network access.
- Use malware protection software.
- Use drive encryption to protect data at rest.
- Ensure the system is able to receive operating system updates automatically.
- Ensure the system is able to receive virus definition updates automatically.