Oracle® Hospitality Workstation 6 Series

Security Guide

Release 1.0
E73830-06
February 2026

Oracle Hospitality Workstation 6 Series Security Guide Release 1.0

E73830-06

Contents

Preface

Audience

This document is intended for those who set up, install, and operate the Oracle MICROS Workstation 6 Series, which includes the 610, 620, 625E, 625X, 650, and 655X configurations. 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
- 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/

Table 1-1 Revision History

Date	Description
April 2016	Initial publication.
July 2016	Updated to include details for the Workstation 610 with Microsoft Windows 10.
November 2016	Added information for the Workstation 610 configuration with Microsoft Windows 8.1 and a 64GB SSD.
March 2017	Added information for the Workstation 620 and Workstation 650 configurations without MSR.
October 2018	Added Merchant Link compatibility information.
March 2020	Added Oracle Linux security information and new Workstation 6 Series models.

1

Workstation 6 Series Security Overview

This chapter provides an overview of Workstation 6 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 and drivers specific to the product as well as the latest patches available from 3rd 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 Workstation 6 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 Workstation 6 Series security features. See Implementing Workstation 6 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 Workstation 6 Series Security

The Workstation 6 Series point of sale terminals are ruggedized devices that incorporate a mixture of hardware and software components commonly found in PC-based devices. For peripherals connectivity, both industry standard and Oracle MICROS proprietary ports have been integrated on-board.

There are six hardware configurations available: 610, 620, 625E, 625X, 650, and 655X

Table 1-1 Workstation 610/620/650 Hardware Component Overview

Feature	610	620	650
Processor	Intel Atom E3827 Dual-Core processor with 1.75GHz clock speed	Intel Celeron 3765U Dual-Core Processor with 1.9GHz clock speed	Intel i5-5350U Dual-Core Processor with 1.8GHz base and 2.9GHz Turbo maximum clock speed
TPM	Atmel AT97SC3204 (TCG 1.2 Compliant)	Intel Broadwell fTPM (TCG 2.0 compliant)	
Storage	32 GB or 64 GB MO-297 Slim SATA 2.0 Solid State Drive standard SD Card Socket	128 GB M.2 SATA 3.0 Solid State Drive standard	256 GB M.2 SATA 3.0 Solid State Drive standard
Magnetic Stripe Reader (MSR)	▪ Modular Integrated 3-Track Magnetic Stripe Reader; Capable of Hardware Encryption at the Swipe. ▪ Triple Data Encryption (TDES/3DES or AES algorithm ▪ Derived Unique Key per Transaction (DUKPT) key rotation algorithm ▪ Merchant Link encryption key pre-injected.	Two configurations available: • With Modular Integrated 3-Track Magnetic Stripe Reader; Capable of Hardware Encryption at the Swipe • Triple Data Encryption (TDES/3DES or AES algorithm • Derived Unique Key per Transaction (DUKPT) key rotation algorithm • Merchant Link encryption key pre-injected • Without Modular Integrated 3-Track Magnetic Stripe Reader	
Network	10/100/1G RJ45 Ethernet 802.11 a/b/g/n Dual Band Radio w/Bluetooth 4.0 (Optional)		
USB	9 Total: • 2 High Speed USB on I/O Panel • 1 High Speed USB in Stand • 2 USB 2.0 on I/O Panel • 1 USB 2.0 12V Powered Header on I/O Panel • 3 USB 2.0 Internal	10 Total: • 2 High Speed USB on I/O Panel • 1 High Speed USB in Stand • 2 USB 2.0 on I/O Panel • 1 USB 2.0 12V/1A Powered Header on I/O Panel • 3 USB 2.0 Internal • 1 Industry Standard 24V/2A Powered USB on I/O Panel	
Serial Ports	4 Total Standard: • 2 - RJ45 RS232 Powered (0/5/9/12V Selectable) • 1 - RJ45 RS232 • 1 - RJ45 RS422/RS232 IDN	3 Total Standard: • 1 - RJ45 RS232 Powered (0/5/9/12V Powered) • 1 - RJ45 RS232 • 1 - RJ45 RS422/RS232 IDN	
Adjustable Stand Expansion Modules (Optional)	Powered USB Expansion Module: • 1 24V Powered USB • 3 12V Powered USB • 2 High Speed USB		
Cash Drawer Ports	2 - MICROS Series 2 Cash Drawer Ports 12/24V Selectable		

Feature	610	620	650
Customer Display Port	1 - Customer Display Port		
Expansion Ports	1 - MICROS Expansion Port 1 - Mini PCI Express Port (internal)	1 - MICROS Expansion Port	

Table 1-2 Workstation 6 Software Architecture Overview

Feature	610	620	650
Operating System	Two configurations available: • Microsoft Windows Embedded 8.1 Industry Pro (32-bit only) • Microsoft Windows 10 IoT Enterprise (64-bit only) • Oracle Linux for MICROS (via optional migration product)	• Microsoft Windows 10 IoT Enterprise (64-bit only) • Oracle Linux for MICROS (via optional migration product)	
Boot Firmware	UEFI - Phoenix SecureCore 3.1 based (UEFI 2.3.1 compliant)		

Table 1-3 Workstation 625/655 Hardware Component Overview

Feature	655X (other models may not include all features listed below)
Processor	Intel Core i5-8265U Quad Core 1.6GHz
TPM	Intel, TCG 2.0 Compliant
Storage	256 GB M.2 NVMe SATA 3.0 SSD standard
Removable Recovery Media	128/256 GB SSD. Allows rapid restore to the original factory condition.
Magnetic Stripe Reader (MSR)	▪ Modular Integrated 3-Track Magnetic Stripe Reader; Capable of Hardware Encryption at the Swipe. ▪ Triple Data Encryption (TDES/3DES or AES algorithm ▪ Derived Unique Key per Transaction (DUKPT) key rotation algorithm ▪ Merchant Link encryption key pre-injected.
Network	2 - GbE RJ45 Ethernet ports (2nd RJ45 port can be used as dual-NIC for workstation or as a hub for network-connected peripherals.) 802.11 a/b/g/n/ac, 2x2 MIMO with dual band radio and Bluetooth 5.0. Supports VPro on Intel i5.

Feature	655X (other models may not include all features listed below)
USB	9 Total: • 4 - High Speed USB on I/O panel 1 High Speed USB in stand • 1 - Ultra High Speed USB on I/O panel, DisplayPort capable 1 USB 2.0 12V powered Header on I/O Panel • 1 - USB 12V powered header on I/O panel • 1 - USB 24V powered header on I/O panel • 2 - Internal Micro USB 2.0 ports
Serial Ports	3 Total Standard: • 1 - RJ45 RS232 Powered (0/5/9/12V 1A selectable) • 1 - RJ45 RS232 • 1 - RJ45 RS422/RS232 IDN
Adjustable Stand Expansion Modules (Optional)	Powered USB Expansion Module: • 1 24V Powered USB • 3 12V Powered USB • 2 High Speed USB
Cash Drawer Ports	2 - MICROS Series 2 cash drawer ports (12/24V selectable)
Customer Display Port	1 – MICROS DIN customer display port
Power Output	1 - 12V power out (2.5A)
Expansion Ports	1 - MICROS expansion port 1 - Mini PCI Express port (internal)
Integrated Camera (Optional)	• Operator-facing; supports facial recognition. • Active array size: 2592x1944

Table 1-4 Workstation 625/655 Software Architecture Overview

Feature	625E, 625X, 655X
Operating System	Two configurations available: • Microsoft Windows 10 IoT Enterprise (64-bit only) • Oracle Linux for MICROS
Boot Firmware	UEFI - Phoenix SecureCore 4.1.0.404 based

Understanding the Workstation 6 Series Environment

When planning your Workstation 6 implementation, consider the following:

- Which resources must be protected?
- You must restrict access to external ports, such as USB ports or serial ports.
- You must protect customer data, such as credit card numbers.
- You must protect internal data, such as proprietary source code.
- You must 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 terminals are installed in environments where physical access to the devices can be difficult or impossible to control. The devices are typically installed in publicly accessible areas based on optimal usage for employees rather than secured computer rooms.

All Workstation 6 Series configurations incorporate mechanical design features that can mitigate physical security risks. Security screws have been provided for each removable cover and for all available mounting options. These features cannot prevent all physical intrusions, but they can increase the time and complexity involved in gaining access to the device.

Factory UEFI Firmware Settings

The UEFI Firmware provides several security settings that are not enabled or configured securely by default. For a secure configuration, you must create installation environment-specific settings, such as passwords. The following settings are available in the firmware and should be enabled/configured during the installation:

- Secure Boot
- Supervisor Password
- Hard Drive Password

The UEFI firmware will enable the following hardware devices by default:

- Trusted Platform Module (TPM)
- Intel Management Engine (ME) / Active Management Technology (AMT)
- USB Ports 1 – 6

Factory Microsoft 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 modified from the defaults in order to improve operating system security out of the box:

- Local Security Policy modifications
    - Enabled clear pagefile at shutdown
    - Disabled Internet Explorer legacy TLS and SSL protocols
- Windows Applications/Services modifications
    - Windows store uninstalled
    - Internet Information Services uninstalled
    - Homegroup Provider disabled
    - Windows Media Services disabled
    - UPnP disabled
    - Autoplay disabled
    - WifiSense disabled
- Network Shares
    - Default Administrative shares removed

User Accounts in Factory Installations

The preinstalled factory operating system should not contain any default user accounts or passwords. During the first boot, you must 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 Workstation 6 Series. The definitions are updated with the current version available at the time the factory operating system was created.

Factory Recovery

All Workstation 6 configurations include a built-in factory recovery feature. The recovery operating system resides on a primary disk, so no additional installation media is required. 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. **Note that the factory recovery feature will wipe the contents of the operating system partition.**

Factory Intel ME/AMT Configuration (650 Configuration Only)

The 650 utilizes the Intel i5-5350U CPU, which includes the Intel® Management Engine coprocessor. The Intel ME is a dedicated hardware and software solution that provides out of band support features completely independent of the CPU.

The Intel ME is enabled by the default Workstation 6 UEFI firmware; however, the firmware's factory default state is unconfigured. This ensures that unauthorized access to the features of the management engine remain inaccessible until it has been provisioned.

2

Performing a Secure Workstation 6 Series Installation

This chapter presents planning information and basic guidance for your Workstation 6 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 if the wireless add-on card will be installed.
- Review a network diagram for the installation environment. Verify the device will only be installed on secured networks behind a hardware firewall.
- Determine how the device will be physically secured. Wall or cabinetry mounts may need to be installed in order to physically secure the device.
- **Microsoft Windows**: Determine out of box operating system security settings. Some information is required for Windows out-of-box setup. The first boot requires configuring an administrative account, network connection settings, and the computer name.
- **Oracle Linux for MICROS**: When migrating from Microsoft Windows to Oracle Linux for MICROS, information is required to complete the operating system setup. Oracle Linux for MICROS setup requires configuring a super user account with a user-configurable password, network connection settings, and the computer name.

Installing Workstation 6 Series Securely

Physically Securing the Device

The *Oracle MICROS Workstation 6 Series Setup Guide* provides detailed instructions for securely assembling the device. To maximize the time and complexity involved for an attacker to physically access the device, install the security screws on all removable covers and mounting configurations. The following sections in the *Workstation Setup* chapter offer detailed instructions for securely assembling and installing the device:

- Securing the I/O Panel Cover
- Securing the Workstation to the Adjustable Stand
- Securing the Adjustable Stand Cover
- Securing the Workstation Display to the Wall Mount

- Securing the Adjustable Stand to the Counter

Microsoft Windows Out-of-Box Setup

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 Microsoft Windows out-of-box setup:

- **Selecting 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.**
  The default computer name supplied by Windows Setup is randomly generated. In some cases, this naming scheme will be undesirable. When changing the computer name of the device, avoid choosing a computer name that leaks information about device. For example, Windows10POSTerminal1 allows an attacker with network access to immediately determine the operating system version and the purpose of the device.

Oracle Linux for MICROS Setup

The first time the device is booted, the Oracle Linux for MICROS setup process begins. This setup requires configuration information including Support user account name and network connection settings.

General guidance for Oracle Linux for MICROS:

- **Creating a Support user account name and password.**
  The Oracle Linux for MICROS installation process provides instructions for naming Support user accounts. For the Support user account password, use complex passwords.
- **Selecting a network connection.**
  Only connect to secure networks.
- **Configure Network Settings.**
  Oracle Linux for MICROS setup does not automatically name the device. Avoid choosing a computer name that leaks information about device. For example, Linux10POSTerminal2 allows an attacker with network access to immediately determine the operating system version and the purpose of the device.

Oracle Linux provides firewall protection for both inbound and outbound traffic. Only select ports for transmitting data in/out are open; all other ports are closed.

3

Implementing Workstation 6 Series Security

Physical Security

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

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 must be repaired by a qualified Oracle repair facility.

  See the *Configuring System Security Settings* sections of the *Oracle MICROS Workstation 6 Series Setup Guide* and the *Oracle MICROS Workstation 6 Series Setup Guide for the 625 and 655* 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 easily removed. All models of the Workstation 6 Series utilize UEFI 2.3.1 Errata C compliant firmware and include support for the secure boot feature.

  See the *Configuring System Security Settings* sections of the *Oracle MICROS Workstation 6 Series Setup Guide* and the *Oracle MICROS Workstation 6 Series Setup Guide for the 625 and 655* 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.
- **Set a HDD Password.**
  A hard drive password will prevent unauthorized access to a bootable hard drive. This ensures that only authorized users can boot the password protected drive after

the installation. Users will have three attempts at keying the correct password. After three failed attempts to enter the HDD password, the HDD will become permanently locked.

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

See the *Configuring System Security Settings* section of the *Oracle MICROS Workstation 6 Series Setup Guide* and the *Oracle MICROS Workstation 6 Series Setup Guide for the 625 and 655* for information on enabling this setting.

- **Disable unused USB Ports.** Disabling the USB ports on the device can be an effective defense against attempts to install malware or hardware components used to gain access to the device. When USB ports are disabled through UEFI firmware on the Workstation 6 Series devices, the respective port will not supply power to attached USB peripherals.

  See the *Other Advanced BIOS Configurations* section of the *Oracle MICROS Workstation 6 Series Setup Guide* and the *Configuring Workstation Settings* section of the *Oracle MICROS Workstation 6 Series Setup Guide for the 625 and 655* for information on enabling these settings.

Operating System Security

- **Drive Encryption.**
  Drive encryption can protect data stored on the hard drive when physical security controls have failed. Microsoft Windows-based Workstation 6 Series models support Bitlocker drive encryption.
- **Application Whitelisting.**
  Application whitelisting allows administrators to define the applications permitted to run on the device. All models of the Workstation 6 Series come with versions of Microsoft Windows that support the AppLocker feature.

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

- Windows 8.1 Security
  https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-8.1-and-8/hh832031(v=ws.11)
- Windows 8.1 Industry Pro Additional Security Features
  https://msdn.microsoft.com/en-us/library/dn449278(v=winembedded.82).aspx
- Windows 10 IoT Enterprise Edition Security Features
  https://docs.microsoft.com/en-us/windows/security/
- Oracle Linux 7.x Security Guide:
  https://docs.oracle.com/en/operating-systems/oracle-linux/7/security/
- Oracle Linux Security page:
  https://linux.oracle.com/security/

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/

Intel Active Management Technology (Model 650 only)

Refer to the Intel Setup and Configuration Software deployment guide for instructions about securely enabling and configuring Intel AMT:

https://www.intel.com/content/www/us/en/support/articles/000020917/software/manageability-products.html?productId=39104&localeCode=us_en

4 Secure Deployment Checklist

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

- Ensure the workstation is physically and securely mounted to a stationary object.
- Ensure all covers and security screws are installed.
- Monitor system access.
- Use Secure Boot.
- Disable unused external I/O ports.
- 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 receives operating system updates automatically.
- Ensure the system receives virus definition updates automatically.