

For Users in Europe, the Middle East and Africa

European Radio Equipment Directive

Cybersecurity Enhancement Supplementary Guide

POS Products Edition

Changes to Specifications to Ensure Compliance with RED

This section describes changes that have been made to specifications to ensure compliance with cybersecurity requirements.

System Development Information for RED compliant products

This section describes the information necessary to develop systems using products that are compliant with RED.

Cautions

- No part of this document may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior written permission of Seiko Epson Corporation.
- The contents of this document are subject to change without notice. Please contact us for the latest information.
- While every precaution has been taken in the preparation of this document, Seiko Epson Corporation assumes no responsibility for errors or omissions.
- Neither is any liability assumed for damages resulting from the use of the information contained herein.
- Neither Seiko Epson Corporation nor its affiliates shall be liable to the purchaser of this product or third parties for damages, losses, costs, or expenses incurred by the purchaser or third parties as a result of: accident, misuse, or abuse of this product or unauthorized modifications, repairs, or alterations to this product, or (excluding the U.S.) failure to strictly comply with Seiko Epson Corporation's operating and maintenance instructions.
- Seiko Epson Corporation shall not be liable for any damages or problems arising from the use of any options or any consumable products other than those designated as Genuine Epson Products or Epson Approved Products by Seiko Epson Corporation.

Trademarks

Microsoft and Windows are registered trademarks of Microsoft Corporation in the United States and/or other countries.

Wi-Fi® is a registered trademark of Wi-Fi Alliance®.

The Bluetooth® word mark and logos are registered trademarks owned by Bluetooth SIG, Inc. and any use of such marks by Seiko Epson Corporation is under license.

Apple and macOS are trademarks of Apple Inc., registered in the U.S. and other countries.

IOS is a trademark or registered trademark of Cisco in the U.S. and other countries and is used under license.

Android™ is a trademark of Google LLC.

All other trademarks are the property of their respective owners and used for identification purpose only.

ESC/POS Command System

Epson ESC/POS is a proprietary POS printer command system that includes patented or patent-pending commands. ESC/POS is compatible with most Epson POS printers and displays.

ESC/POS is designed to reduce the processing load on the host computer in POS environments. It comprises a set of highly functional and efficient commands and also offers the flexibility to easily make future upgrades.

Contents

- Contents.....3
- Purpose of This Document4
- About the European Radio Equipment Directive4
- Epson Product Security Policy4

Changes to Specifications to Ensure Compliance with RED 5

- Products that are in scope of RED6
 - Printers that are in scope of RED 6
 - How to Determine if a Printer is Compliant with RED..... 7
 - How to Print a Network Status Sheet..... 7
- Software.....9
 - Operating Systems that are supported by RED compliant products 9
 - Software Supporting Devices Compliant with RED10
 - Software Not Supporting Devices Compliant with RED11
 - Firmware Update Notification11

System Development Information for RED compliant products 12

- Business System Development Using only Products that are Compliant with RED 12
- Adding a Printer that is Compliant with RED to an Existing Business System 13
 - Secure Printing Setting13
- Troubleshooting..... 15
- Supplementary Information 16

Purpose of This Document

This supplementary document explains the specifications of products that are in compliance with the cybersecurity requirements of the European Radio Equipment Directive and provides important points to note when using said products. It includes changes to specifications that affect customers whose systems are already in operation and secure. Please refer to this document for information about these changes and how to respond to them.

In addition to the information in this document, please also refer to the Technical Reference Guide for your printer.

About the European Radio Equipment Directive

The European Radio Equipment Directive is the key legal framework for radio equipment sold in the EU. Products sold on the EU market meet these standards.

For more information about this law, please see the following URL:

 <http://data.europa.eu/eli/dir/2014/53/oj/>

Epson Product Security Policy

For more information about Epson's security efforts, see the following website. The Security Guidebook posted on the website provides information about the security features built into the product.

 <https://support.epson.net/security/>

Changes to Specifications to Ensure Compliance with RED

To comply with the cybersecurity requirements of the European Radio Equipment Directive (hereinafter referred to as RED), Epson is making the following changes to the specifications of products sold in Europe from 2025.

- Factory default passwords are unique for each device. (Passwords will be printed on a label attached to the product.)
- Security will be ensured from factory shipment
- Authentication will be required for online communication.
- Online communication will be encrypted and kept confidential.
- Wireless communication will be encrypted and kept confidential.
- Customers will be notified of any changes related to security.
- Authentication will be required when updating firmware and sensitive settings.

Conventional functions might not be possible on printers that are compliant with RED, because the default values for the communication protocol have been changed to a more secure method or a newer version. In addition, the use of encrypted communication might appear to cause reduced performance in some cases. Care should be taken when installing new printers that are compliant with RED in existing business systems already in operation.

Products that are in scope of RED

Printers that are in scope of RED

The printers shown in the following table, bound for countries requiring the CE mark are compliant in scope of RED.

Compliant Printer	Remarks
TM-H6000VI	All models
TM-L100	All models except Serial/USB Model
TM-m30II-S	All models
TM-m30II-SL	All models
TM-m30III	All models
TM-m30III-H	All models
TM-m50	All models
TM-m50II	All models
TM-P20II	All models
TM-P80II	All models
TM-P80II Auto Cutter model	All models
TM-T20IV	All models except Serial/USB Model
TM-T88VII	All models

When using any of the following interfaces on a RED compliant device, the Business System has to be compatible to the RED specifications.

- Ethernet Interface
- Wireless LAN Interface
OT-WL06 (Wireless LAN Unit) is required except for models with built-in wireless LAN.
- Bluetooth Interface

NOTE

- Compatible interfaces will vary depending on the printer.
- RED is a legal regulation for wireless devices. Even if only an Ethernet Interface connection is actively used, system development must be compatible with RED.
- When developing a business system that operates only with a USB Interface connection, a Serial Interface connection, or a Parallel Interface connection, system development is not required to be compatible with RED.

How to Determine if a Printer is Compliant with RED

To determine if a printer is compliant with RED, print a Network Status Sheet. If the printer is compliant with RED, “Security Mode: RED” will be printed on the status sheet.



Printed Information	Result
Security Mode: RED	Compliant with RED
Security Mode: Normal	Not compliant with RED
Security Mode: PSTI	Not compliant with RED
Security Mode: Internal	Not compliant with RED
Nothing printed	Not compliant with RED

NOTE

The character string that follows “Initial Password:” is the default administrator password. This password is the same as the character string on the password label attached to the printer. The administrator password is required to connect the printer to a host device and to change the printer settings. For improved security, we strongly recommend changing the default administrator password. For more information about how to change the administrator password, please refer to the Technical Reference Guide for your printer.

How to Print a Network Status Sheet

Please refer to the Technical Reference Guide for your printer for more information about how to print a status sheet. A summary is provided below. The printing method will vary from printer to printer.

Using the Paper Feed Button

- 1 Make sure the printer is turned on.
- 2 Open the roll paper cover.
- 3 Press and hold the paper feed button (for at least 1 second).

4 Close the roll paper cover.

Printing of the status sheet begins. After printing is finished, the printer returns to normal mode.

Using the Status Sheet Button

1 Make sure the printer is turned on.

2 Make sure the roll paper cover is closed.

3 Press and hold the status sheet button (for at least 3 seconds).

Printing of the status sheet begins. After printing is finished, the printer returns to normal mode.

Software

Operating Systems that are supported by RED compliant products

The following operating systems are compatible with RED.

Regardless of which operating systems are described in the Technical Reference Guide or Software Manual, only the following operating systems are compatible.

- Windows 11
- Windows 10
- Windows 11 IoT
- Windows 10 IoT
- Windows Server 2022
- Windows Server 2019
- Windows Server 2016
- macOS
Available for use with TM-m30III/TM-m30III-H Firmware Ver. 13.17 ESC/POS or later
- Android
- iOS

The following operating systems are not compatible with RED.

These operating systems will only work with products that are out of RED scope or have “Secure Printing Setting” disabled.

- Windows 7
- Windows 8/8.1
- Windows Server 2012/R2
- Windows Server 2008 R2 SP1
- Windows Server 2008 SP2
- Windows Embedded 8.1 Industry
- Windows Embedded Standard 7
- Windows Embedded POSReady 7
- Linux

Software Supporting Devices Compliant with RED

The following software has been updated to be compatible with RED. Please ensure you are using the latest version of the software.

When using a printer that is compliant with RED, you must also use a printer driver that is compatible with RED to operate the device. The software that can be used will vary from printer to printer.

You can download software that is compatible with RED from the following URL:

 <https://epson.sn>

Software	Version Compatible with RED
EPSON Advanced Printer Driver 6	Ver. 6.10 or later
EPSON JavaPOS ADK	Ver. 1.14.38W/L or later
EPSON OPOS ADK	Ver. 3.00E R27 or later
EPSON OPOS ADK for .NET	Ver. 1.14.38 or later
TM-XXXX Utility (provided for each model)	(*)
TM Virtual Port Driver	Ver. 8.70d or later
EpsonNet Config (Windows OS)	Ver. 4.9.11 or later
Epson Deployment Tool	Ver. 3.11.0 or later
Epson Monitoring Tool	Ver. 3.10.0 or later
Epson ePOS SDK for Android	Ver. 2.33.0 or later
Epson ePOS SDK for iOS	Ver. 2.33.0 or later
Epson ePOS SDK for JavaScript	Ver. 2.27.0f or later
TM Utility for Android	Ver. 3.38.0 or later
TM Utility for iOS	Ver. 3.38.0 or later
Epson TM Print Assistant for Android	Ver. 1.17.0 or later
Epson TM Print Assistant for iOS	Ver. 1.17.0 or later
TM Series Printer Driver for Mac	Ver. 3.0.1 or later
TM-XXXX Firmware Updater (provided for each model)	(*)

(*): The version indicated as “Compatible with the cybersecurity requirements of the European Radio Equipment Directive” on the software download page

NOTE

Software that is compatible with RED works with both compliant and non-compliant printers.

	Printers that are Compliant with RED	Printers that are Not Compliant with RED
Software that is Not Compatible with RED	Cannot print	Can print
Software that is Compatible with RED	Can print	Can print

Software Not Supporting Devices Compliant with RED

The following software does not support devices compliant with RED.

The software will only work with products that are out of RED scope or have “Secure Printing Setting” disabled. For more information, see [“Secure Printing Setting” on page 13](#)

- TM Series Printer Driver for Mac
- TM Series Printer Driver for Linux (CUPS)
- EPSON TM Bluetooth Connector
- TM-XXXX Printer Model Setting Utility
- BmpToRaster
- Send Data Tool
- TM FontRunner
- Epson TM-H6000VI Slip Paper Sensor Adjustment Tool

Firmware Update Notification

To ensure that the product meets the latest security requirements, customers can enable the notification of new available firmware updates.

TM-XXXX Firmware Updater for Windows

When you run the TM-XXXX Firmware Updater, a module for notification messages can be installed on your computer. For more information, please refer to the documentation of TM-XXXX TM Firmware Updater and the download page.

TM Utility for Android/TM Utility for iOS

The utility will regularly check whether a new firmware is available and notify the user.

NOTE

Updating a firmware version of a previous, non-RED compliant printer will not automatically activate the security settings required for RED.

System Development Information for RED compliant products

Business System Development Using only Products that are Compliant with RED

When developing a business system that connects printers that are compliant with RED to the following interfaces, a compatible operating system and software must also be used.

- Ethernet Interface
- Wireless LAN Interface
- Bluetooth Interface

NOTE

- When developing a business system that operates only with a USB Interface connection, a Serial Interface connection, or a Parallel Interface connection, system development is not required to be compatible with RED.
- Application software that was developed using the ESC/POS command will not run unless used via a USB Interface, Serial Interface, or Parallel Interface.
- Applications can interface with ESC/POS if the Ethernet/Wireless or Bluetooth Interfaces are mapped to a virtual serial port using TM Virtual Port Driver. The driver will automatically encrypt the ESC/POS data without the need to modify the application.
- When changing the printer settings or updating the firmware, you will be prompted to enter the administrator password.

Adding a Printer that is Compliant with RED to an Existing Business System

When adding a printer that is compliant with RED to a business system already in operation, it will not print properly if connected as is. In this case, the following measures can be taken.

(1) Make the business system compatible with RED.

For a business system that is currently in operation, please ensure that the latest drivers are installed and used.

If operating in a secure and managed environment, printers without “Secure Printing” enabled, can still be used.

NOTE

When connecting the printer to a host device or changing the printer settings, you will be prompted to enter the administrator password.

Secure Printing Setting

Secure Printing Setting is enabled by default on all products that are in scope of RED. The current setting can be confirmed using either a model utility that is compatible with RED, TM Utility, Web Config, or EpsonNet Config (Web version) to change the "Secure Printing" setting.

When this setting is enabled, only software designed to be RED compliant can be used. Older software may work when "Secure Printing" is disabled. However, this is not recommended and might compromise the security of your product and environment!

Secure Printing	Enabled	Must be compliant with RED to print a job (default setting)
	Disabled	Can print a job even if not compliant with RED

NOTE

- Web Config and EpsonNet Config (Web version) are built-in Web pages on your printer that allow you to check and change printer settings from your browser. Please refer to the Technical Reference Guide for your printer for more information about how to access these Web pages.
- Please refer to [“Effect on Print Path Due to Enabling/Disabling the Secure Printing Setting” on page 13](#) for changes that lead to security issues related to compliance with RED.

Effect on Print Path Due to Enabling/Disabling the Secure Printing Setting

RED requires that communication between hosts and printers be protected by a high level of secure encryption. Disabling the Secure Printing setting will reduce the security of the product and allow unencrypted communication.

	Secure Printing Enabled (Default Setting)	Secure Printing Disabled
Port 9100 (RAW)	Cannot print	Can print
Port 9143 (TLS RAW)	Can print (encrypted)	Can print (encrypted)
Port 80 (HTTP)	Cannot print	Can print
Port 443 (HTTPS)	Can print (encrypted)	Can print (encrypted)

	Secure Printing Enabled (Default Setting)	Secure Printing Disabled
Port 8008 (Epson ePOS SDK)	Cannot print	Can print
Port 8009 (Epson ePOS SDK)	Cannot print	Can print
Port 8043 (Epson ePOS SDK)	Can print (encrypted)	Can print (encrypted)
Port 8143 (Epson ePOS SDK)	Can print (encrypted)	Can print (encrypted)
Bluetooth Classic	Can print (encrypted)	Can print
Bluetooth Low Energy	Can print (encrypted)	Can print (encrypted)

Other Settings

In addition to the items that are changed when Secure Printing is enabled, the following items have also been changed to ensure compatibility with RED.

You can use a model utility that is compatible with RED, TM Utility, Web Config, or EpsonNet Config (Web version) to verify these settings. Please be aware of the security implications before making any changes.

The settings available will vary from printer to printer.

	RED Compliant	Previous Versions
Allow LPR Port Printing	Disabled	Enabled
TLS1.0	Disabled	Enabled
TLS1.1	Disabled	Enabled
SSL/TLS Encryption Strength*	High	Medium

*: Only for models on which encryption strength can be set to High/Medium/Low

Troubleshooting

I want to use a printer that is compliant with RED without making changes to my non-compatible business system.

Installing the latest drivers, changing the interface or utilizing TM Virtual Port may be an option for you. Other than that non-compatible business systems will only be able to work with unsecure printers that don't support "Secure Printing" or have it disabled, but is not recommended.

For more information, see ["Secure Printing Setting" on page 13](#).

The printer performance changed on new RED compliant products.

The encryption, decryption and authentication necessary for "Secure Printing" may impact performance under some conditions. Installing latest drivers and firmware will ensure the best performance for the security requirements. Improving performance might also be possible with unsecure printers that don't support "Secure Printing" or have it disabled, but is not recommended.

For more information, see ["Secure Printing Setting" on page 13](#).

Supplementary Information

Audit Log

An audit log function has been added to printers that are compliant with RED.

The audit log function maintains a log of the printing history and changes to settings. Reviewing the audit log on a regular basis can make it easier to track unauthorized access and other security issues. The default setting for the audit log function is enabled. Although this function can be disabled, we recommend that you leave it enabled.

The audit log can be accessed from Web Config and EpsonNet Config (Web version).

For more information about how to start Web Config and EpsonNet Config (Web version), please refer to the Technical Reference Guide for your printer.

NOTE

For the Bluetooth model of the TM-P20II/TM-P80II/TM-P80II Auto Cutter model, use the Epson Deployment Tool software. For details, refer to the following file that is registered when installing the Epson Deployment Tool.

For Windows (64-bit):

C:\Program Files (x86)\EPSON\DeploymentTool\PrinterDeployment\PrinterSettingChanger\
TMRPrinterSettingChanger_ReadMeE.txt

For Windows (32-bit):

C:\Program Files\EPSON\DeploymentTool\PrinterDeployment\PrinterSettingChanger\
TMRPrinterSettingChanger_ReadMeE.txt

How to Use the Audit Log

1 Open the Audit Log page. The administrator password is required.

- For models that support Web Config:
Web Config screen - [Product Security] tab - [Audit Log]
- For models that support EpsonNet Config (Web version):
EpsonNet Config (Web version) screen - [Configuration] - [Network] - [Security] - [Audit Log]

2 Change the settings as needed.

- Audit log setting
Enable/disable the audit log function.
- Export the audit logs to the CSV file
Select “Export” to output log data in CSV file format.
- Deletes all audit logs
Select “Delete” to delete all log data.

NOTE

Depending on the printer, logging might begin before startup is complete (before the network functions are ready). Time stamps are not added to logs during startup, but are added after startup is complete.

Common specifications for RED compliant POS printers

Interface

Interface Type	Remarks
Ethernet interface	Limited to models with an Ethernet (RJ-45).
Wi-Fi interface	Limited to models with a Wi-Fi Direct (Simple AP) service.
Bluetooth interface	Only models with Bluetooth.

Service

Service Name	Service Overview	Remarks
HTTP/HTTPS: Web Service	Service to obtain device information / change settings from the browser.	
HTTPS: IPP Print	Service for printing using IPP protocol.	Only for some models.
HTTP/HTTPS/TCP: ePOS-Print service / ePOS-Device service	Services for printing and peripheral use via XML.	Only for some models.
HTTPS: Firmware Update	Service for firmware update using Epson's proprietary protocol.	Only for some models.
ENPC	Service for obtains or sets equipment information using Epson's proprietary protocol.	
SNMPv1	Service for obtains or sets equipment information.	
mDNS	Service for network device discovery.	
SLP	Service for network device discovery.	
LLTD	Service for network device discovery.	
LLMNR	Service for network device discovery.	
Port 9100 (RAW)	Service for obtaining printer information.	
Port 9143 (TLS RAW)	Service for obtaining printer information.	Only for some models.
Secure printing over Bluetooth	ESC/POS printing via Bluetooth	

SNMPv3 Authentication Algorithm

SHA2 has been added to the SNMPv3 authentication algorithm, and the default setting for printers that are compliant with RED is SHA2-256.

You can use a model utility that is compatible with RED or TM Utility to change this setting.