TOSHIBA

Security Guide

e-STUDIO2323AMS/2323AMW/2823AMW

e-STUDIO2323AM/2823AM

e-STUDIO2822AM/2822AF

e-STUDIO2329A/2829A

September, 2025

R250813C3400-TTEC

OME25006900

TABLE OF CONTENTS

Trademarks

The trademarks described in this manual are as shown below.

- Windows, and the brand names and product names of other Microsoft products are trademarks of Microsoft Corporation in the US and other countries.

Other company names and precuts names in this document are the trademarks of their respective companies.

1. PREFACE

Toshiba Tec Corporation (hereafter called “Toshiba Tec”) guarantees the security of your data and documents for enabling your business to meet the increased security demands of today’s world. The White-and-Black low-end range MFPs, the related models of this manual, conform with appropriate security standards, preventing your data and documents from any unauthorized access without sacrificing the efficiency and performance of the systems.

The target models of this manual are as follows.

Target Model
e-STUDIO2323AMS/2323AMW/2823AMW
e-STUDIO2323AM/2823AM
e-STUDIO2822AM/2822AF
e-STUDIO2329A/2829A

2. INTERFACE SPECIFICATIONS FOR WHITE-AND-BLACK LOW-END RANGE MFP

The interface specifications supported by each model are as follows.

Target Model	USB	Wired LAN	Wireless LAN	FAX
e-STUDIO2323AM/2823AM	Yes	Yes		
e-STUDIO2323AMS	Yes	Yes	Option	
e-STUDIO2323AMW/2823AMW	Yes	Yes	Yes	
e-STUDIO2329A/2829A	Yes	Yes	Option	Option
e-STUDIO2822AM	Yes	Yes	Option	
e-STUDIO2822AF	Yes	Yes	Option	Yes

3. DATA SECURITY

MFPs encrypt and store important information such as copy, scan, and print settings, network settings, and address book. MFPs without storage devices such as SSDs or HDDs store information in a non-volatile memory.

4. FIRMWARE SECURITY

There are two methods for updating the MFP firmware. In both methods, upon attaching a digital signature to the update data, verification is made during the update and thus no security is compromised.

- Save the update data to a USB storage device and perform the update in the service mode.
- After logging into TopAccess by an administrator, perform the update from [Maintenance] -> [System Updates].

5. NETWORK SECURITY

5.1 Protocol specifications

TOSHIBA MFPs have only the minimum ports opened to provide network services. For example, TCP/UDP ports are opened, and client computers connect to the MFP ports corresponding to each service via the network. Moreover, in order to provide the LPD printing service, the MFP has TCP port 515 opened.
The protocols, default port numbers and port setting methods supported by the appropriate models of this manual are as follows.

Protocol	Port Number	Port Setting Method
FTP	TCP 21	TopAccess
SMTP	TCP 25	TopAccess
SMB	TCP 139, 445	TopAccess
LPD	TCP 515	TopAccess
IPP	TCP 631	TopAccess
RAW	TCP 9100	TopAccess
HTTP HTTPS	TCP 80 TCP 10443	TopAccess, Control panel
SNMP	UDP 161, 162	TopAccess
DHCP	UDP 68	Control panel
DNS	UDP 53	TopAccess
POP3	TCP 110	TopAccess
Network TWAIN	TCP 4567	TopAccess
Status Monitor	TCP 6575	TopAccess

5.2 Network access control

Ports, which do not provide a service, are not opened. Moreover, any port unnecessary for operation can be closed by using the administrator setting. Protocols not to be used should be disabled. Moreover, unnecessary ports should be closed.

5.3 IP address filtering and MAC address filtering

IP address filtering and MAC address filtering are supported. Only an access request from a network node, such as a client PC, with an address registered in the MFP is accepted or access from a registered address can even be refused. Due to this, access from a malicious network node can be restricted. Moreover, a function which accepts an access request only from a client PC with a specific IP address or MAC address registered in the MFP, and one which does not accept an access request from a client PC with a specific IP address or MAC address registered in the MFP, are both supported.

5.4 Communication path protection (wired LAN)

Encrypted communication that flows over the network can protect communications. Although communication data can easily be wiretapped when the Network Trace Tool is used, through encryption, it will not be stolen even when wiretapped.

5.5 SSL (Secure Sockets Layer) / TLS (Transport Layer Security)

Since TOSHIBA MFPs support up to TLS1.2 and TLS1.3, SSL3.0 whose vulnerability has been discovered is not used.

SSL/TLS communication is supported in HTTP and SMTP.

In the HTTP function, SSL/TLS encryption is also carried out for access to TopAccess.

In SMTP, SSL/TLS communication prevents e-mail data from being wiretapped.

Unauthorized usage of the Scan to E-mail function may cause an information leakage through E-mails or wiretapping. To prevent this problem, the Scan to E-mail function provides a security function for E-mail transmission.

As the authentication methods for e-mail authentication, standard protocols (POP before SMTP, SMTP Authentication (LOGIN/PLAIN/CRAM-MD5)) are equipped in the MFP, thus the protocols can be selected in accordance with the corporate policy.

5.6 Communication path protection (wireless LAN)

TOSHIBA MFPs support WPA/WPA2 Mixed Mode and WPA2, which are the wireless LAN security standards established by Wi-Fi Alliance that can prevent third parties from wiretapping and tampering with communication data.

WPA can protect communication paths by encrypting wireless communications to prevent decryption and access by third parties, and by verifying access points to confirm that they are user-configured connections.

WPA was created as a subset of IEEE802.11i, especially for improving user authentication and encryption. Later on, WPA2 that completely complies with IEEE802.11i was released. Compared with WPA, WPA2 provides more enhanced encryption and connectivity. Two connection methods are supported: WPA-PSK allows user authentication and encrypts data when a “passphrase” shared between an access point and a client PC is preset. “Passphrase” is an optional character string set with up to 63 characters. In addition to WPA-PSK, a stronger security system (IEEE 802.1X authentication) through a RADIUS server (authentication server) is supported.

Countermeasures against known wireless LAN vulnerabilities such as KRACK (Key Reinstallation Attack) and FragAttacks (Fragmentation and aggregation Attacks) have also been implemented.

5.7 SMBv3

In addition to v1 and v2, Network Protocol SMBv3 which has a data encryption and enhanced security features has also been supported. Moreover, it is possible to disable SMBv1 whose vulnerabilities have been identified.

6. ACCESS SECURITY

6.1 Access control for control panel and TopAccess

The access security accepts the access for specified users who have an access privilege to designated data or devices. The access to the device is controlled through the operation panel and TopAccess respectively.
By switching the security mode setting in the service mode, it is possible to set a higher security level.
Password authentication is required when accessing data that should be protected during the operation of the [USER FUNCTIONS] menu on the operation panel.
A password authentication screen is displayed when entering the [GENERAL], [FAX], [REPORT SETTING], [LIST], [WIRELESS SETTING] and [ADDRESS BOOK] menus in the [USER FUNCTIONS] menu.In TopAccess operations, access control for administrators or operators is performed. It is possible to set whether to implement access controls for the address book.
By enabling the [Department Management] setting on the operation panel or in TopAccess, access control by the department code becomes possible.
To ensure the security strength of the password authentication, if the password is entered incorrectly 5 times consecutively, the account is locked for 5 minutes.

6.2 Confidential setting of document name and user name

This function allows one to indicate a document name, a user name and a destination are masked with “*” when implementing the confidential setting from [GENERAL] -> [Confidentiality Setting] in the administrator menu of TopAccess.

6.3 Telephone line access control

Regarding telephone line access, the MFPs do not accept another protocol, only the fax. The current fax board supports only a standard G3 fax and the unique procedural protocol of Toshiba Tec. When a connection is made to machines other than a regular one or a TOSHIBA one, the protocol cannot be established. As a result, it becomes a communication error and the line is disconnected. Therefore, you will not be able to access the network through the fax board from a telephone line. Furthermore, there is no chance of improper data becoming mixed. Remote-Maintenance from the fax line is not supported.

7. MEASURES TO VULNERABILITY

7.1 Provision of security patches

If a vulnerability has been disclosed in the firmware, a security patch against it will be timely provided.

7.2 Malware targeted at Windows

There are risks of infection from network viruses (worms) targeted at Windows, infection via websites (TopAccess), and viruses that invade MFPs via USBs. Additionally, there are risks of viruses that invade MFPs via USBs. These risks can be reduced by implementing appropriate security measures.
Moreover, TOSHIBA MFPs are not affected by network malware (viruses, etc.) targeted at Windows.

7.3 Vulnerability to OSS

MFPs use some open sources (OSS). Countermeasures to vulnerabilities to these disclosed OSS have been taken one by one. Cross-Site Request Forgery, Cross Site Scripting, SQL Injection and OS Command Injection are well-known vulnerabilities. Countermeasures to them have been taken in MFPs.

7.4 Invading of viruses from USB Ports

Countermeasures against viruses that make their invading to MFPs via a USB storage device have also been taken.
In USB Direct printing, a file is handled as print data. Therefore, even if Malware or scripts are included in the file, only an image drawing error will occur. Malware or scripts are not executed.
When Scan to USB is performed, the file is just loaded from the MFP to a USB storage device. Malware in the USB storage device is not operated.
Due to this, Malware or scripts in the USB storage device are not executed.

7.5 Vulnerability confirmation by tools

Tests which use a vulnerability scanner and a fuzzing tool have also been carried out and countermeasures are being implemented for the problems detected on an ongoing basis.

8. REGULATORY REQUIREMENTS

8.1 California IoT Security Low (SB-327)

Beginning January 1, 2020, this California IoT Security Law (SB-327) requires a manufacturer of a connected device to equip the device with a reasonable security feature or features that are appropriate to the nature and function of the device, appropriate to the information it may collect, contain, or transmit, and designed to protect the device and any information contained therein from unauthorized access, destruction, use, modification, or disclosure. TOSHIBA MFPs are equipped with reasonable security features as required by the California IoT Security Law.

8.2 EU General Data Protection Regulation (GDPR)

GDPR (General Data Protection Regulation) is a legal regulation aimed at protecting personal data within the European region.
It emphasizes the protection of personal data and privacy, requiring that user information be managed securely.
TOSHIBA MFPs are equipped with the necessary security features to achieve an operational environment compliant with GDPR.

8.3 EU Radio Equipment Directive (RED, 2014/53/EU)

The EU Radio Equipment Directive (RED, 2014/53/EU) is a legal framework that applies to radio equipment sold within the EU.
This directive aims to ensure that products with wireless communication functions meet essential requirements such as safety, electromagnetic compatibility (EMC), and efficient use of radio frequencies. Additionally, from August 1, 2025, cybersecurity requirements under Article 3(3) of the RED Directive will become mandatory, adding new technical requirements for internet-connected radio equipment. Two harmonized standards, EN 18031-1:2024 and EN 18031-2:2024, have been established as standards corresponding to these requirements.
TOSHIBA MFPs have been declared conformity-compliant through evaluation by third-party certification organizations to ensure reliability for compliance with the harmonized standards EN18031-1,2 of RED-DA.

8.4 Security in the organization

As the information society advances, personal information is becoming an increasingly important asset. In the meantime, cases where personal information is illegally collected and used for unexpected purposes without notifying relevant individuals are increasing and the society is becoming more concerned about the handling of personal information.
Once a large amount of personal information leaks, the company will not only lose credibility but also fall into a dangerous situation that may cause serious damage endangering company’s existence. It is a social responsibility for companies to establish a good relationship of trust with customers, make an effective use of personal information, and protect it as well.
Toshiba Tec provides products equipped with a wide variety of the aforementioned security features, to allow its customers to avoid information leak. Toshiba Tec will enhance the partnership with customers and move forward with implementing safer security measures.

Toshiba Tec recognized the importance of personal data protection at an early stage and established the Privacy Policy and the Personal Data Protection Guidelines as in-house regulations, in February, 2001.
The personal data protection system has been improved. The Privacy Policy was amended and published on the website in August, 2004. The Personal Data Protection Guidelines were significantly revised in accordance with regulatory requirements in November, 2004 and re-established as the Personal Data Protection Program (PDPP).
For details about Privacy Policy in Toshiba Tec, refer to the following URL.

http://www.toshibatec.com/privacy/