

**TOSHIBA**

# WHITE PAPER: TOSHIBA'S HOLISTIC APPROACH TO PRINT SECURITY



TABLE OF CONTENTS

1. Overview.....4

2. Device Security.....5

    2.1 Installation.....6

        California IoT Law Compliant .....6

        Toshiba High Security Mode.....6

    2.2 Operation.....7

        Software Security.....7

            Application Protection.....7

            e-BRIDGE Platform Security.....7

            Operating System & Firmware Protection.....8

        Hardware Security.....9

            BIOS Protection.....9

            Hard Drive Security.....9

            HDD Data Encryption.....9

            HDD Data Protection.....10

            FIPS 140-2 Protection.....10

    2.3 End-of-Life.....10

        EOL & Hard Drive Scrubbing.....10

3. Access Security.....11

    3.1 Restrict.....12

        Physical Access Security.....12

            User Authentication.....12

            Password Policy.....12

            USB Port Disable.....12

        Digital Access Security.....13

            IP/MAC Address Filtering.....13

            Transport Layer Security (TLS).....13

            IP Layer Security.....13

            Network Authentication.....14

            Wireless Security.....14

- 3.2 Manage..... 15
  - Role-based Access Control..... 15
- 3.3 Monitor..... 15
  - Audit Log..... 15
  - Intrusion Detection..... 15
- 4. Document Security..... 16
  - 4.1 Capture..... 16
    - Secure Print Stream..... 16
    - Email Security..... 17
    - USB Port Malware Protection..... 17
    - Cloud Security..... 18
  - 4.2 Store..... 18
    - PDF Encryption..... 18
    - e-Filing Password Control..... 18
    - Security Stamp..... 18
  - 4.3 Deliver..... 19
    - Print Security..... 19
    - Secure Print Release..... 19
    - Hardcopy Security Printing..... 19
    - FAX Security..... 19
    - Document Tracking..... 20
    - Scan to Email Document Security..... 20
- 5. Fleet Security..... 20
  - 5.1 e-BRIDGE CloudConnect: Security Policy Manager..... 21
- 6. Certification & Regulatory Compliance..... 22

## WHITE PAPER: TOSHIBA'S HOLISTIC APPROACH TO PRINT SECURITY

The purpose of this document is to provide an overview of the built-in security features in Toshiba MFPs. The information outlined in this document also helps facilitate answers to the most common security-related questions in current IT environments.

### 1. OVERVIEW

As one of the most shared resources within your organization, your office multifunction printer (MFP) has access to much of your company's most sensitive information. Not only do these devices work with physical copies of your valuable information, thanks to technological advances such as optical character recognition (OCR), optical mark recognition (OMR) and intelligent character recognition (ICR), these devices are also fully capable of extracting digital information from any document. Therefore, documents copied, printed, scanned, faxed or stored on these devices can make sensitive customer information, company intellectual property and corporate network infrastructure (e.g., ports, endpoints and employee credentials) potentially vulnerable for data breach or misuse.

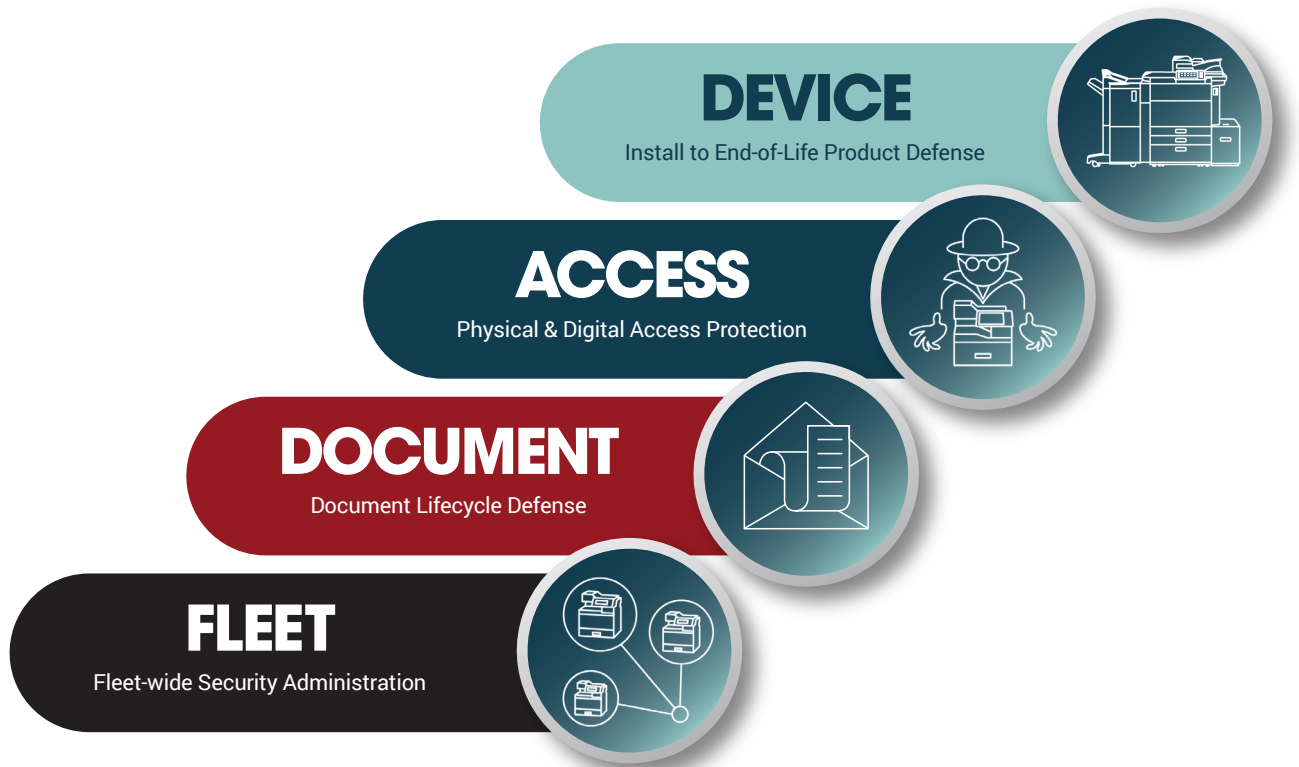
The impact of any security breach cannot be underestimated, and sensitive documents in the wrong hands can cripple a business. With high-profile attacks making headlines, businesses are becoming increasingly aware of the threats and potential vulnerabilities that can impact their organizations. And companies of all sizes are susceptible, with small to medium-sized businesses becoming targets since they often lack the IT resources to ensure that rigorous security protocols are in place. Businesses are all looking for assurances that their MFPs are not putting their sensitive business information at risk.

That's why you need a trusted partner who makes securing your MFP as simple and straightforward as possible. Toshiba understands computers, networks and business better than any other MFP manufacturer. We're proud to say Toshiba is also a leading drive manufacturer, producing the hard disk drives (HDD) used inside our very own MFPs – we're the only one in the industry who can say that. And these HDDs feature unique technology, making them the most secure storage devices available today. Considering that the HDD stores all the data coming through your MFP and is often considered the highest risk component inside today's modern MFP, we believe this is a risk that cannot be overlooked.

Toshiba uniquely looks at the entire MFP environment – from the product itself to the people and processes that interact with the product – in order to provide a holistic approach to security. This document will focus on the product and examine how Toshiba delivers device, access, document and fleet security.



# OUR IN-DEPTH PRINT SECURITY APPROACH



## 2. DEVICE SECURITY

Toshiba not only protects the MFP at every layer of the technology stack, we also ensure that our MFPs are secure during the entire device lifecycle from installation to operation to end-of-life (EOL).



## 2.1 INSTALLATION

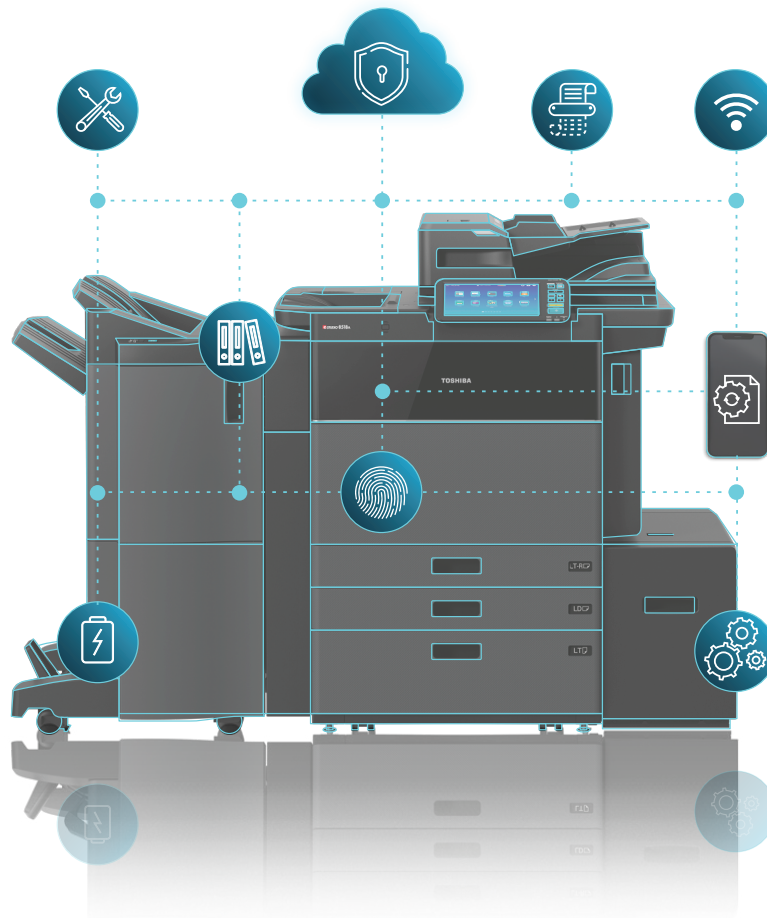
### CALIFORNIA IoT LAW COMPLIANT

California IoT law (SB-327), effective on January 1, 2020, "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 within from unauthorized access, destruction, use or modification."

In compliance with SB-327, Toshiba devices require users to enter a unique admin password during the installation and deployment process. This ensures that the device is tamper-proof against any unauthorized access due to common knowledge of the default password.

### HIGH SECURITY MODE

Toshiba's High Security Mode is one of the unique security features available in Toshiba MFPs that makes security easy for IT administrators. With a single device code, the MFP configures over 60 settings to the most secure mode. This setting ensures that all the security settings on the device are set to maximize security automatically, without any further administrator. These settings include, but are not limited to, network protocol settings, print security settings, scan security settings and device access policy settings. This is considered a very effective solution for environments where security is of utmost importance.



## 2.2 OPERATION

### DEFENSE AT EVERY LAYER



### SOFTWARE SECURITY

Toshiba MFPs have a defense-in-depth strategy across all layers of the software stack, from application to e-BRIDGE platform to firmware.

#### APPLICATION PROTECTION

All internal or external applications installed on Toshiba devices are encrypted and digitally signed by Toshiba engineering. Therefore, any software without the Toshiba digital signature will be blocked and unable to be installed on the device. This protects the device from any spyware, ransomware or any unauthorized third-party software.

#### e-BRIDGE PLATFORM SECURITY

Toshiba's e-BRIDGE Open Platform provides an Embedded Web Browser (EWB) and Web Service interface for the development of web apps for Toshiba MFPs. These interfaces work in conjunction with all the built-in security features on the MFP itself allowing application developers to ensure the security and confidentiality of their data. Toshiba's Embedded Web Browser uses the Apple® WebKit rendering engine for web applications developed on the e-BRIDGE platform. All the standard security applicable to web applications applies to the MFP Embedded Web Browser as well.

The e-BRIDGE platform also allows developers to create embedded applications that run within the device's system memory. Therefore, it is of utmost importance to validate and control what type of code may be allowed to run within the platform. Toshiba's e-BRIDGE embedded platform includes additional features to protect the MFP from malicious application software.

## ***Installation Control***

Installation and uninstallation of the embedded applications can be performed only by an administrator or service technician, such as a user with MFP management privileges. This role is controlled so that a user without these privileges is not allowed to install or uninstall applications, preventing the operation of unintended applications.

## ***Consistency Check of an Application Package***

An application installer of the embedded applications only allows the install of a package that's certified and digitally signed by Toshiba. Therefore, this will prevent the installation of invalid applications such as a falsified package or one created by an unknown creator.

## ***Embedded Applications & User Privilege***

The panel operation of the app is controlled through role-based access. Therefore, when users operate embedded applications on the touch panel of the MFP, they cannot perform operations beyond the privilege given by the role of the user on the MFP. So, operations—which are not permitted to normal users by an administrator—cannot be performed through embedded applications.

## ***Separation Between Embedded Applications***

File storage of embedded applications is separated, so one app cannot access data from another app – even when multiple embedded applications are installed. Due to this, confidential data for each app can be stored securely in the file storage of the embedded applications.

## ***Separation Between the MFP & Embedded Applications***

File storage of embedded applications and the MFP is separated, so any confidential data stored in the MFP cannot be viewed by the embedded applications directly. Therefore, protection against the leakage of confidential data, such as a user password/PIN from the embedded applications, is strictly ensured.

## **OPERATING SYSTEM & FIRMWARE PROTECTION**

Toshiba uses a hardened Linux operating system that is widely used in mission-critical systems across the globe. By using the highly secure and reliable Linux system controller, we ensure that Toshiba MFPs are not affected by network malware, ransomware or viruses targeted for Windows systems or other embedded systems, which have been the target of recent attacks on devices of other manufacturers. Viruses like MSBLAST, WannaCry, and others are unable to reach our MFPs as a result. In addition to the platform being secure by design, each version of the controller goes through a formal assessment by security experts before they are released.

These assessments include validation and verification of common vulnerabilities and exposures such as Cross-Site Request Forgery, Cross Site Scripting, SQL Injection and OS Command Injection. In addition, countermeasures to the recently reported vulnerabilities (e.g., POODLE, FREAK, GHOST, Heartbleed, Shellshock, KRACK, Spectre and Meltdown) have already been addressed via firmware patches. Toshiba's firmware team proactively addresses any security vulnerability to ensure that both the platform and the controller are secure to the latest standards through our security patch update process.

As part of the IEEE P2600 Protection Profile for Hardcopy Devices, whitelisting ensures that only firmware from a trusted source is accepted by the MFP, thus preventing malware from wreaking havoc on a network by entering through an innocuous source – the MFP – and protecting the system from any external malicious software. Toshiba MFPs use whitelisting as a critical safeguard for managing firmware updates.



All our firmware is encrypted and digitally signed, and the firmware update process requires a validated digital signature on any firmware being uploaded to the MFP as part of a device updating process. Therefore, firmware from unauthorized sources is rejected by Toshiba devices. Toshiba MFPs also require that all third-party software must be digitally signed before they can be installed on the MFP. Without this digital signature, the software simply won't install.

## HARDWARE SECURITY

Toshiba device has two layers of hardware protection; BIOS protection at the chip level and hard-drive protection at a storage level.

### BIOS PROTECTION

Toshiba MFP BIOS (also referred to as COREBOOT) is a set of boot instructions that load the device firmware during system startup. Toshiba MFP BIOS and firmware are digitally signed with SHA-256 encryption. Because of this, any unauthorized changes to the firmware will cause the MFP to discard the faulty firmware, and previous firmware may be restored. In turn, this addresses any concerns related to malicious software affecting the system firmware thus protecting the system BIOS. In addition, when the FIPS 140-2 Validated HDD is added, all our latest Toshiba MFP models are HCD-PP1 (Hardcopy Device Protection Profile) compliant, which requires that the system provides mechanisms to verify the authenticity of software updates.

**If the HDD is stolen or removed from the Toshiba MFP, the data is invalidated immediately to avoid any information leakage.**



### HARD DRIVE SECURITY

Toshiba manufactures its own hard drives, so we can control both the quality of the HDD security and the entire supply chain. Our HDDs are built with two layers of security: data encryption and Data Overwrite. Additionally, we offer a FIPS 140-2 Validated HDD.

### HDD DATA ENCRYPTION

All Toshiba MFPs are equipped with self-encrypting HDD with Wipe function which ensures that the data stored on the HDD are encrypted with an AES 256-bit algorithm. Therefore, even if the HDD is stolen or removed from the Toshiba MFP, the data is invalidated immediately to avoid any information leakage.

<sup>1</sup><https://www.niap-ccevs.org/Profile/Info.cfm?PPID=317&id=317>



**With FIPS 140-2 Level 2 compliance, Toshiba's offering provides tamper-evident labeling to deliver a high level of security.**

## HDD DATA PROTECTION

The Data Overwrite feature on Toshiba MFPs allows data that is temporarily stored on the HDD from copying, printing, scanning or faxing operations to be automatically overwritten and erased by a DoD standards-compliant method once they're completed. This Data Overwrite feature also has the function of completely erasing the data in all HDD areas. On Toshiba MFPs, evidence of the overwriting appears on the front panel as "Erasing Data" immediately after the device is done with any temporary data gathered during the copying, printing, scanning or faxing process. Other manufacturers' MFPs do not erase the data immediately, but rather wait and erase at scheduled times of the day, holding on to potentially sensitive data longer than is necessary.

## FIPS 140-2 PROTECTION

Toshiba also offers a FIPS 140-2 Validated HDD specifically for those government agencies and private sector businesses where data protection is of utmost importance. FIPS 140-2 is designed to address the encryption and tamper resistance of an HDD. Under certain regulations, U.S. federal agencies must use FIPS-140 certified systems to meet security requirements in order to protect sensitive information in computers, telecommunication systems and other IT-related products, such as MFPs). FIPS 140-2 is a published security standard (Federal Information Processing Standard).

Toshiba's approach to the encryption is unique in that it leverages Toshiba's Wipe security feature which automatically erases data when the HDD is accessed by an unregistered system. Unlike software-based encryption which relies on the system CPU for encryption processing, the HDD leverages its onboard crypto-processor to encrypt at full interface speed without impacting system-level performance. With FIPS 140-2 level 2 compliance, Toshiba's offering provides tamper-evident labeling to deliver a high level of security.

## 2.3 END-OF-LIFE

### EOL & HARD DRIVE SCRUBBING

Toshiba has a strict, documented process to ensure that no customer data leaves the customer facility when the devices are decommissioned at the end of the lease. It is also recommended that organizations have an internal policy in place to ensure MFP and printer assets fully eliminate sensitive data through hard drive scrubbing as devices reach their end-of-life or come to the end of the lease term. Toshiba MFPs already have all the necessary features and

functionality to ensure that the data is encrypted and protected.

Additionally, these features are strictly enforced when the device is decommissioned at the end of the lease or the end of a temporary loan. At the end of the lease period, all data on the HDD is instantly invalidated or reset to default factory settings using a service code on the device. This service code may also be triggered remotely through our e-BRIDGE CloudConnect tool. This process ensures that data retrieval is completely disabled after the service technician has performed this operation on the MFP according to the customer's instructions.

### 3. ACCESS SECURITY

When it comes to access security, we ensure that the right people have access to the right data and the right device capabilities. Our approach to device access may be categorized into the following categories:

- First, we **restrict** the device so that only authorized individuals or sites can access the device physically or digitally.
- Next, we **manage** and enforce security policies centrally so it's easy to ensure the highest levels of access security.
- And finally, we **monitor** access and proactively send alerts to any intrusions.

When it comes to access security, we ensure that the right people have access to the right data and the right device capabilities.



## 3.1 RESTRICT

### PHYSICAL ACCESS SECURITY

You do not want everyone in your organization, or visitors to your building, to have access to the valuable and often sensitive documents printed on your device. Nor do you want anyone having access to make changes to the physical device. To enforce this, Toshiba MFPs restrict physical access in the following ways:

### USER AUTHENTICATION

Authentication may be enabled on Toshiba MFPs to prevent unauthorized access to MFP functions. The user authentication feature allows an administrator to restrict operations on the touch panel, including restricting access to MFP configurations or log information, restricting available operations such as copying, printing, scanning or faxing to users, managing the meter counter on a per-user basis and setting user authentication requirements for each function.

Several authentication methods are supported on Toshiba MFPs:

- Department code authentication
- User ID/password authentication
  - Local authentication by the MFP itself
  - Windows domain authentication
  - LDAP/AD server authentication
- PIN authentication
- Badge authentication
- Two-factor authentication, using badge and PIN
- NFC (Near-Field-Communication) authentication

### PASSWORD POLICY

Additionally, password policies may be set so that the user password is required to have the following attributes:

- Minimum password length
- Password validity period
- Prohibited character strings in a password
- Account lockout caused by login failure

### USB PORT DISABLE

As an additional security measure, the USB ports on Toshiba MFPs may be completely disabled so that those ports cannot be used for intrusion attacks. Even if these ports are open, they are already equipped with protection from malware or harmful scripts.



## DIGITAL ACCESS SECURITY

In addition to managing physical access to the device, Toshiba MFPs also have numerous built-in features to protect themselves from unauthorized digital access.

### IP/MAC ADDRESS FILTERING

All Toshiba MFPs support IP/MAC address filtering so that access requests from only a specific network node(s) or a client PC(s) are accepted. Also, certain network devices or segments may be restricted access. This helps ensure that the MFP is accessed from authorized network equipment only. This restriction applies to both IP and MAC addresses. Additionally, the MFP may be configured for port filtering so that only certain ports stay open in the MFP, and an administrator can configure the MFP to respond or reject ICMP requests.

### TRANSPORT LAYER SECURITY (TLS)

Toshiba MFPs may be configured to allow all communication over secure TLS1.2 protocol, with older, less secure SSL protocols (SSL3.0/TLS1.0) no longer supported. TLS1.2 communication is much more secure than its predecessors because it allows the use of more secure algorithms and advanced cipher suites. TLS 1.2 is the de-facto security standard currently used in HTTP Server/Client, IPP, LDAP, SMTP Client, POP3, FTP Server, Web Service Print, FTP Client, Web Services Scan, Syslog and SOAP. All HTTP information, including MFP administration, TopAccess communication and response to the Remote Device Management System (RDMS), is communicated over TLS. A few advantages of TLS 1.2 communication are listed here.

- With IPPS (Internet Printing Protocol), TLS encryption prevents print data from being eavesdropped.
- In POP3/SMTP, TLS communication prevents e-mail data from being compromised.
- For backup and restoration of FTP print data and e-Filing box data, TLS encryption prevents these data from being compromised.
- In Web Service Print, TLS encryption prevents print data from being eavesdropped.
- In Web Service Scan and TWAIN Scan, TLS encryption also prevents data from being eavesdropped.

### IP LAYER SECURITY

Toshiba MFPs support IPV6 with IP Security Protocol (IPsec) which protects data communication in the IP layer, ensuring that both the sender and the receiver are authenticated, and the integrity, as well as the authenticity of the data, is protected in order to secure confidentiality and entirety.

As per IPsec standard, Toshiba MFPs support both AH (Authentication Header) and ESP (Encapsulating Security Payload) security protocols. AH secures the entirety of the IP packet, and ESP secures the confidentiality and entirety. For key management protocol together with IPsec, both IKEv1 and IKEv2 are also supported. Security certificates may be imported manually or automatically via Simple Certificate Enrollment Protocol (SCEP).



## NETWORK AUTHENTICATION

Toshiba MFPs support several network authentication schemes:

- IEEE802.1X is standard for network authentication utilized in Toshiba MFPs. IEEE802.1X consists of a supplicant, 802.1X switch and an authentication server. IEEE802.1X does not accept any communication from clients who are not authorized. EAP (Extensible Authentication Protocol) is used to transmit an authentication message via EAP-MD5 and EAP-TLS methods. Currently, EAP-MD5, MSCHAPv2, EAP-TLS, EAP-TTLS and PEAP are supported. For certificate installation with EAP-TLS, EAP-TTLS and PEAP, manual import or SCEP can be utilized.
- LDAP/AD authentication supports CRAM-MD5, Digest-MD5 and Kerberos to protect the username and password required for access to an LDAP/AD server
- SMTP authentication supports CRAM-MD5, Digest-MD5, Kerberos and NTLM (IWA: Integrated Windows Authentication) to protect the username and password required for access to an SMTP server
- POP3 authentication supports Kerberos, NTLM (SPA: Secure Password Authentication) and APOP to protect the username and password required for access to a POP3 server
- SMB authentication supports NTLMv2 and Kerberos
- Dynamic DNS supports Secure Dynamic DNS (Domain Name System). When Secure Dynamic DNS is used, only the MFP in which the resource record has been registered or device with management authority for a DNS server can update zone information.
- SNMP supports SNMP authentication, enabling authentication of an SNMP session between the MFP and an SNMP server
- Toshiba MFPs also support SNMPv3, which has both a data encryption and a user authentication function to enhance security features

## WIRELESS SECURITY

To prevent unauthorized usage by a third party, such as a falsification of data and spoofing over Wi-Fi, Toshiba's MFP wireless option supports WPA/WPA2 Mixed Mode and WPA2, which encrypts data and allows user authentication. WPA and WPA2 are security standards established by the Wi-Fi Alliance. It's strongly recommended that organizations use WPA2 standard because it provides more enhanced encryption and connectivity.

Two connection methods are typically supported. WPAPSK allows user authentication and encrypts data when a passphrase shared between an access point and a client PC is preset. A passphrase is an optional character string set with 8 to 63 characters.

In addition to WPAPSK, a stronger security system (802.1X authentication) through a RADIUS server (authentication server) is also supported. This is a connection mechanism, which verifies if the connected access point and the client PC are authenticated parties. In 802.1X authentication systems, EAP-TLS with a digital certificate and PEAP with a password are supported. To speed up 802.1X authentication, WPA2 optionally supports Pairwise Master Key (PMK) caching. PMK caching stores authentication results, including an encryption key, to connect to a wireless LAN access point smoothly even if the location is changed.

## 3.2 MANAGE

In addition to the features to restrict access, Toshiba devices also have controls to manage access across devices.

### ROLE-BASED ACCESS CONTROL

It is easy to manage and implement authentication policies and prevent unauthorized usage of the MFP via role-based access control. The administrator may create different roles and assign them to specific users of the MFP. These roles may be defined as MFP local, or they may be retrieved from a corporate directory attribute. When the user logs in, the MFP retrieves the role information allocated to the user from the directory server, checks the access rights allocated to its role from an ACL (Access Control List) and assigns appropriate access to MFP functions.

Access rights can be managed at a very granular level to ensure users only have access to the functions necessary for their job role. Here is a sample list of access rights that can be associated to a role: Device Setting, Copy, Send Email, File Save, iFax Send, Print, e-Filing, Fax Send, Color Output (Copy, Print), Remote Scan, USB Print/Save, Editing Address Book and Log Management.

## 3.3 MONITOR

Finally, monitoring security-related activities on Toshiba devices is also easy. Using several logging and real-time notification features within Toshiba MFPs, system administrators can monitor and prevent any unauthorized access and activities on the devices.

### AUDIT LOG

Each operation on the control panel and in the MFP web portal (TopAccess) is recorded as a system log in order to prevent unauthorized usage of the MFP and ensure traceability. After enabling user authentication, operations initiated by a user (e.g., copying, printing, scanning, fax transmitting and receiving) can be logged, even if the requested operation failed due to an attempt to access a restricted function. Thus, unauthorized access can be closely monitored. And, those audit logs are not accessible to everyone. When user authentication is enabled, users can only browse their own job logs, while administrators can monitor all logs. When user authentication is disabled, job logs can be configured to be shown to authorized users only.

### INTRUSION DETECTION

Toshiba MFPs can take monitoring to the next level with the ability to send alerts. All Toshiba models utilize standard Syslog functionality, which can forward any security-related messages or alerts to an external Security Information & Event Management (SIEM) server for further analysis. This allows any third-party SIEM server or security software to remotely monitor security events on Toshiba devices in real time. This provides flexibility to IT managers to monitor all the network endpoints using a single security software rather than managing the multifunction devices separately.

All Toshiba MFP models are equipped with an integrity checker functionality. This allows administrators to verify and confirm the integrity of the data within the MFP. It is strongly recommended that the administrator periodically performs integrity checks on the MFP so that illegally modified data (if any) can be reported.

## 4. DOCUMENT SECURITY

In addition to protecting the MFP device itself across the entire lifecycle, we also secure documents across their entire lifecycle. We protect sensitive documents as they enter the MFP, as they are stored on the MFP and as they leave the MFP through physical or digital means, including print, fax, scan, copy & more—thus securing the documents from end-to-end.

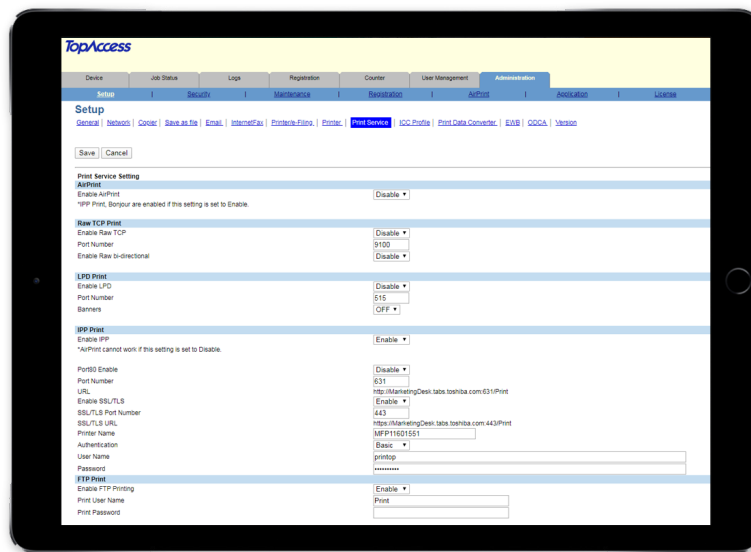


### 4.1 CAPTURE

Documents can enter the MFP from a variety of sources, so Toshiba ensures that the highest levels of security is provided for each method of entry.

#### SECURE PRINT STREAM

All Toshiba devices support Internet Printing Protocol (IPP) print over HTTPS. The IPP is a specialized Internet protocol for communication between client devices (e.g., computers, mobile phones and tablets) and printers (or print servers). It allows clients to submit print jobs to the printer or print server and perform tasks such as querying the status of a printer, obtaining the status of print jobs or canceling individual print jobs. IPP also supports access control, authentication and encryption, making it a much more capable and secure printing mechanism.



## EMAIL SECURITY

Unauthorized usage of the Scan to Email function may cause information leakage through email. This function on Toshiba MFPs provides additional security for email transmission and reception. For outgoing email transmissions, the following security functions are supported:

- **User Authentication:** Standard protocols including POP before SMTP, SMTP Authentication (LOGIN/PLAIN/CRAM-MD5/Digest-MD5/Kerberos) and LDAP/AD Authentication (LOGIN/PLAIN/CRAM-MD5/Digest-MD5/Kerberos) are equipped in the MFP, thus, any of these protocols can be selected in accordance with the corporate policy.
- **Encryption:** Encryption (SMTP SSL/TLS) of the email communication during email transmission is supported to prevent eavesdropping of emails on the network.

Similar security functions are also available for inbound email reception with the following three security features:

- **Protection Against Malware:** Attached files are handled as print data, therefore, even if malware or scripts are included in the file, they are not executed.
- **Protection Against Eavesdropping:** Since data is encrypted by SSL/TLS with POP3 and SMTP protocols, eavesdropping is prevented even when storing attached images from received mail into the e-Filing box.
- **Protection Against Store-and-forward:** The Off-ramp function restricts telephone numbers so that dialing to an arbitrary number from incoming email is impossible.

## USB PORT MALWARE PROTECTION

As an additional security measure, the USB ports on Toshiba MFPs may be completely disabled so that those ports can't be used for intrusion attacks. Even if these ports are open, they are already equipped with protection from malware or harmful scripts.

For example, during USB printing, a file is handled as print data. Therefore, even if malware or scripts are included in the file, they can't be executed from the USB. When Scan to USB is performed, the file is simply loaded from the MFP to a USB storage device, and malware or scripts (if any) in the USB storage device are not executed.

## CLOUD SECURITY

Toshiba's document Scan to Cloud and Print from Cloud functions are fully secure with the latest TLS protocols, with older, less secure protocols no longer supported. This applies to any third-party applications integrated with the Toshiba platform to run on the panel. Therefore, all the documents captured from cloud or on-premises applications are fully encrypted and secure.

## 4.2 STORE

Toshiba's MFP hard drive may be used as a filing cabinet for documents where we ensure that proper encryption and access control is applied to these documents stored within the MFP.

### PDF ENCRYPTION

This feature is available on all Toshiba MFPs and allows users to encrypt PDF documents with a user-defined password. The recipient of the document will be required to enter the password before the document can be opened. Toshiba supports 128-bit AES encryption for PDF documents.

Operation restrictions on the document can also be set for Print, Documents Change, Contents Extraction and Accessibility, respectively. If an encrypted PDF file is sent to a wrong destination or sniffed, this function prevents users who do not know the password from viewing it. This function also protects distributed PDF documents from unauthorized printing or tampering.

### e-FILING PASSWORD CONTROL

It is strongly recommended to set up a password in order to create a secured e-Filing box on Toshiba MFPs, ensuring only authorized users can access the documents in the e-Filing box. This password policy applies to both the MFP control panel as well as the web portal.

### SECURITY STAMP

Security stamping is a simple yet powerful feature to enable the tracing of the MFP's copying and printing documents by forcibly printing information such as the date and time or username onto the printed document. Forced printing of the date and time, username and card ID enables the tracking of the data related to who has performed copying, printing and fax transmission as well.



## 4.3 DELIVER

Let's look at various ways Toshiba MFPs ensure document security when they are delivered via several mechanisms, including print, copy, fax and email.

### PRINT SECURITY

Toshiba MFPs offer several standard print security options.

When user authentication is disabled, private printing can be used to transmit print data with a password up to 64 alphanumeric characters from a client PC to the MFP. The transmitted data is stored temporarily in the HDD of the MFP until the user walks up to the MFP and enters the password to start printing the job on the MFP.

When user authentication is enabled, hold printing or private printing is used for print security. The user must log in at the panel to be able to release print jobs. The MFP can also be set up to require a username and password when a job is sent to the MFP from a printer driver, adding print security to the shared PC used by multiple users. Users can also release their own print jobs using badge authentication with a wide variety of non-contact proximity card options, including MIFARE and HID. Document or usernames can also be hidden on the status screen to ensure security.

### SECURE PRINT RELEASE

Toshiba's multi-station print functionality allows users to send a print job to one print device and release that job from any of the other MFPs around the department or the office. The job stays in a secure queue until the user authenticates at the device to release it. No external hardware or software is required. This protects confidential documents from prying eyes as they do not sit on the output trays unattended. Please note that the MFPs for multi-station print may be configured such that the print job transmission across the MFP is over TLS.

### HARDCOPY SECURITY PRINTING

Hardcopy Security Printing (GP1190A) is a unique option for Toshiba Color MFPs that embeds a hidden fine dot pattern on documents during printing. When these documents are later copied, hidden characters emerge, effectively restricting unauthorized copying and preventing the leakage of information printed on the document.

This optional plug-in application prevents unauthorized copying and performs information tracking. An embedded fine dot pattern is added to a document during printing when the user specifies Hardcopy Security Printing in the printer driver. When this printed document is copied, a security pattern "COPY" will conspicuously appear on them discouraging information leakage. Additionally, when an attempt is made to copy, scan or fax a printed document on a Toshiba MFP equipped with a copy-prohibiting function, the operation stops if this pattern is detected, and the administrator is notified. As a result, the security of confidential documents can be strictly maintained. The dot pattern on the printed document also allows tracking of the print job's origin.

### FAX SECURITY

The current fax board on Toshiba MFPs can only be used for faxing, which ensures that no other communication activity is allowed. The fax board supports a standard G3 fax ONLY and the unique procedural protocol (\*) of Toshiba TEC Corporation. When a connection is made to machines other than a conventional fax or a TOSHIBA fax, it results in communication error and the line is disconnected. Therefore, access to the network through the fax board from a telephone line is not possible. Furthermore, there is no chance of improper data getting mixed with fax data. Remote maintenance from the fax line is also not supported.

Additionally, there are several fax features built into Toshiba MFPs that ensures that the confidential fax documents do not fall into wrong hands.

- Schedule fax jobs to be printed only at a specific time of the day
- Password protect incoming fax jobs
- Use the fax Hold function so that the fax print is held up until the fax operator manually prints the fax jobs

## DOCUMENT TRACKING

To ensure the traceability of the MFP's copying, scanning and faxing data, the documents can be stored as image thumbnail data along with the job information. When copying or scanning is performed or a fax is transmitted or received in the MFP, the data can be transmitted to a designated external server as the image thumbnail data, along with the job information, including date and time, username, file name and serial number of the MFP. This function enables the tracking of data if information leakage does occur after copying, scanning or faxing from the MFP. In order to prevent information leakage resulting from the improper use of this function, this feature is disabled by default.

## SCAN TO EMAIL DOCUMENT SECURITY

Scan to Email documents may be configured with Secure PDF so that the outgoing documents may be password protected. Additionally, the administrator may configure the device so users can send documents to only specific destinations configured in the device address book. Typing a specific email address during Scan to Email may be strictly prohibited. This helps to avoid sensitive documents from being sent to the wrong destination intentionally or by mistake.

## 5. FLEET SECURITY



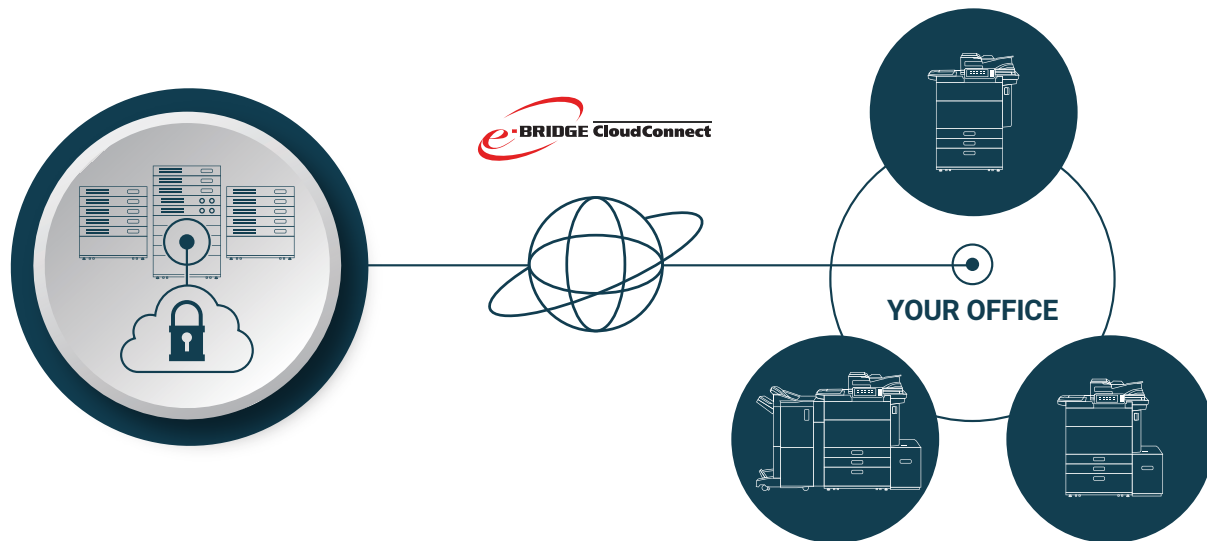
**From a security perspective,  
policy management is a critical  
necessity and key feature of  
e-BRIDGE CloudConnect.**



## 5.1 e-BRIDGE CLOUDCONNECT: SECURITY POLICY MANAGER

e-BRIDGE CloudConnect (eCC) is Toshiba's integrated system of embedded and cloud-based applications that enables remote monitoring and management of Toshiba MFPs. e-BRIDGE CloudConnect securely and reliably collects operation data transmitted from MFPs. Additionally, the administrator can create policies related to the security settings of the MFP and deploy those settings to the fleet via the eCC portal. Any violations to these MFP security policies are flagged and notified to the administrator.

e-BRIDGE CloudConnect uses the same principles used by client PCs accessing secure data over a browser with HTTPS (server authentication and encryption). Data can only be sent from MFPs, and access is limited to e-BRIDGE CloudConnect servers with valid authentication certificates. To prevent server spoofing and to make sure data is transmitted to the correct server, e-BRIDGE CloudConnect features a server authentication functionality that confirms whether the server to be accessed is the actual server that has been specified. All transmitted and received data is encrypted to preserve confidentiality and safety and to protect against stealing, leaking and tampering.



e-BRIDGE CloudConnect only handles the MFP operation status information. This includes data related to counter data, such as the number of sheets used, MFP failures, consumables' replacements and MFP settings and adjustments. Since e-BRIDGE CloudConnect does not handle actual document data, copy, fax, print and scan data can't be leaked. On request, a service technician can set e-BRIDGE CloudConnect to permit or deny transmission. The MFP is operated and managed based on the system's security policy, in accordance with ISO 27001 international standard for information security management.

The key benefit of eCC is its ability to help manage and maintain device security policies. MFPs enrolled in eCC as part of a customer's fleet will have the policy settings of that device continuously compared with the established policy. Should data fall outside the parameters of the policy, such as when a new device is added to the fleet, an alert is triggered, and the violation is displayed on the MFP's page within the e-BRIDGE CloudConnect portal. If the policy was written to trigger actions, the system executes the actions including the ability to update service or security settings or update firmware, keeping the entire fleet in compliance with established security policies.

From a security perspective, policy management is a critical necessity, and, as mentioned, a key feature of e-BRIDGE CloudConnect. In addition to security settings, other MFP settings such as authentication and IP filtering may also be deployed remotely, making the likelihood of a successful attack virtually impossible.

## 6. CERTIFICATION & REGULATORY COMPLIANCE


In addition to the numerous security features, Toshiba MFPs comply with several regulatory requirements as well as third-party certifications applicable to different industry verticals.

### ISO/IEC15408

Information Technology Security Evaluation Criteria, identified as Common Criteria authentication, is an international standard for evaluating and certifying the functionality and quality of IT products. The functionality and quality of certified Toshiba products have been accepted in many countries participating in the Common Criteria Recognition Arrangement (CCRA).

### EAL

EAL stands for Evaluation Assurance Level, which indicates the levels of assuring the evaluations. Target IT products are evaluated in accordance with the requirements defined by EAL. The higher EALs include the evaluations for the lower ones. All Toshiba MFPs are EAL certified at different levels.



**In addition to the numerous security features, Toshiba MFPs comply with several regulatory requirements as well as third-party certifications.**

## HARDCOPY DEVICE PROTECTION PROFILE (HCD-PP)

Toshiba's newest e-BRIDGE MFPs, when configured with the FIPS 140-2 Validated HDD, are HCD-PP certified. HCD-PP is the latest U.S. Government-approved security certification to come out of the NIAP (National Information Assurance Partnership) and Common Criteria Test Laboratories. HCD-PP ensures the MFP meets rigorous security assurance requirements when dealing with digitized documents, including physical documents being scanned, copied or faxed, or digital documents being printed. HCD-PP is particularly important not just because it is the latest review of potential security threats to data within an MFP, but also, unlike other security measures that only address one area, this standard addresses the entire device as it pertains to data (i.e., documents) processed by it.

A conforming hardcopy device (HCD) addresses the following potential security vulnerabilities:

### **1. Identification, Authentication & Authorization to Use HCD Functions**

This means that only users granted access by an administrator can use functions on the device.

### **2. Access Control**

Along with authorization, access control pertains to the methods by which you control access to the device ensuring only authorized users have such access. This can take the form of proximity cards, login names, passwords and more.

### **3. Encryption**

Data encryption ensures that data assets cannot be accessed while in transit on the local network. By policy, data encryption is also used to protect documents and confidential system information on nonvolatile storage devices to protect such data if such a device is removed from the HCD. The effectiveness of data encryption is assured by using internationally accepted cryptographic algorithms.

### **4. Trusted Communications**

Trusted communication paths are established to ensure that communications with the HCD are performed with known endpoints, which are essentially authorized users.

### **5. Administrative Roles**

Tying in with many of the other safeguards, role-based access controls ensure that the ability to configure the security settings of the HCD is available only to users who have been authorized with an administrator role.

### **6. Auditing**

Audit logs are generated by the HCD to ensure that security-relevant events and HCD use can be monitored by authorized personnel. The HCD must generate audit logs and securely transmit them to an External IT entity for storage. Optionally, audit logs may also be stored in the HCD where they can be reviewed by an administrator.

### **7. Trusted Operation**

Software updates to the HCD are verified to ensure the authenticity of the software before applying the update. The HCD performs self-tests to ensure that its operation is not disrupted by some detectable malfunctions.

### **8. PSTN Fax-network Separation (if PSTN fax function is present)**

If a conforming HCD has a PSTN fax function, PSTN fax-network separation ensures that the PSTN fax modem is not used to create a data bridge between the PSTN and the network.

### **9. Data Clearing & Purging (optional)**

Optionally, an HCD may provide functions that actively overwrite image data or that purge all customer-supplied information at the request of an authorized administrator. Toshiba e-BRIDGE MFPs are equipped with Data Overwrite technology that exceeds Department of Defense requirements and performs the overwriting immediately after the MFP is done processing any jobs utilizing this temporarily stored data.



## ENCRYPTION ALGORITHM

The JCMVP is a certification system operated by IPA (Information-technology Promotion Agency, Japan). This system certifies that the encryption module conforms with JIS X 19790 (ISO/IEC 19790). It has been verified that each encryption algorithm has been implemented in the MFPs properly, and the result has been registered in the implementations of IPA. The CAVP (Cryptographic Algorithm Validation Program) is a certification system collectively operated by NIST (National Institute of Standards and Technology, U.S.A.) and CSEC (Communications Security Establishment Canada). By performing the test prescribed in the encryption algorithm implementation requirements, it has been verified that the encryption algorithm has been implemented properly in the software encryption library used for Toshiba MFPs.

## SECURITY HDD WITH WIPE FUNCTION

The security HDD with the Wipe function on Toshiba MFPs has been tested as prescribed in the encryption module implementation requirements based on JIS X 19790 (ISO/IEC 19790), by IPA.

JCMVP has certified that AES, SHS, HMAC and DRBG have been properly implemented as encryption modules, and the result has been registered in the following Cryptographic Module Validation List of IPA. The CMVP (Cryptographic Module Validation Program) is a certification system collectively operated by NIST (National Institute of Standards and Technology, U.S.A.) and CSEC (Communications Security Establishment Canada).

## HIPAA

The Health Insurance Portability and Accountability Act (HIPAA) is designed to ensure that patient information is treated with the highest level of confidentiality, both within the healthcare organization and outside of the organization. Toshiba security solutions offer various features that address the privacy and security of protected patient information. Secure device access, private printing capabilities and an audit trail prevent improper device usage and only allow authorized users to receive the confidential data or documents.

## GLB ACT

The Gramm-Leach-Bliley (GLB) Act relates directly to financial institutions, ensuring that consumers are aware of how their personal financial information is being used and shared. The Financial Privacy Rule and Safeguards Rule govern the disclosure of private financial information and require all financial institutions to design and maintain systems to support the protection of customer information.

## FERPA

The Family Education Rights and Privacy Act (FERPA) is a federal law that protects the privacy of student education records. This requires a heightened level of security for educational institutions complying with the U.S. Department of Education. Password printing, controlled device access and data encryption and/or deletion ensure that sensitive information is not accessible on the multifunction device.

## THE SARBANES-OXLEY ACT (SOX)

The Sarbanes-Oxley Act (SOX) is a federal law that recently introduced stringent rules with the objective to change financial practices and corporate governance regulations. Following high-profile corporate scandals, this was passed to protect investors by improving the accuracy of corporate financial disclosures made in relation to the securities laws. Data security safeguards focus on restricting access to information, the tracking of data and protection of data integrity.

## CALIFORNIA SB-327

Beginning January 1, 2020, this California legislative act requires a manufacturer of a connected device to be equipped 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, as specified.

## CCEVS

Common Criteria Evaluation and Validation Scheme (CCEVS), established by the National Information Assurance Partnership (NIAP), evaluates information technology products for conformance to certain security standards. The Common Criteria program recognizes and validates security solutions based upon an internationally accepted methodology. Toshiba products currently comply with the Common Criteria and are EAL Certified conforming to ISO/IEC15408 (Information Technology Security Evaluation Criteria).

**TOSHIBA**

[business.toshiba.com](https://business.toshiba.com)