TOSHIBA

TOSHIBA'S HOLISTIC APPROACH TO

Print Security

December 2025

How to use this paper.

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

Let’s keep your data protected—*at every step*.

Table of Contents

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 cloud better than any other MFP manufacturer. We're proud to say that Toshiba MFPs use carefully selected solid-state drives (SSDs), ensuring the highest levels of performance and security. These SSDs feature advanced technology that makes them among the most secure storage devices available today. Since the SSD stores all the data passing through your MFP and is often considered the highest-risk component in modern devices, we believe its security is a risk that cannot be overlooked.

Toshiba uniquely looks at the entire print 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, fleet and cloud security.

1.1 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

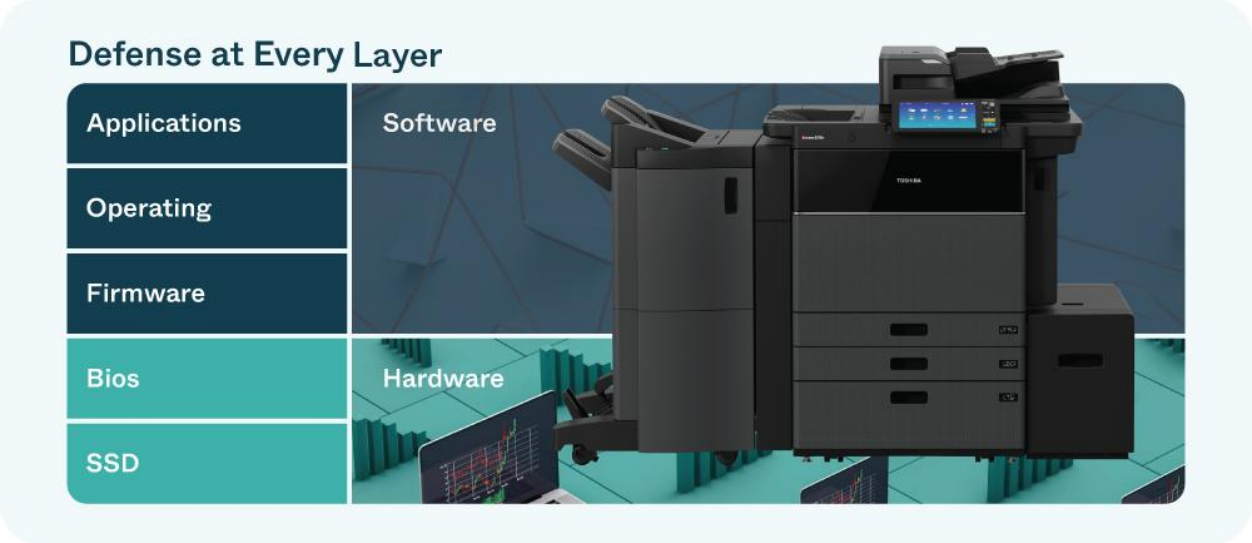
California IoT law (SB-327), effective on January 1, 2020, "requires a manufacturer of a connected device to equip the device with a reasonable security feature or features that are appropriate to the nature and function of the device, appropriate to the information it may collect, contain or transmit, 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 70 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



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 installation 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 kernel, 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.

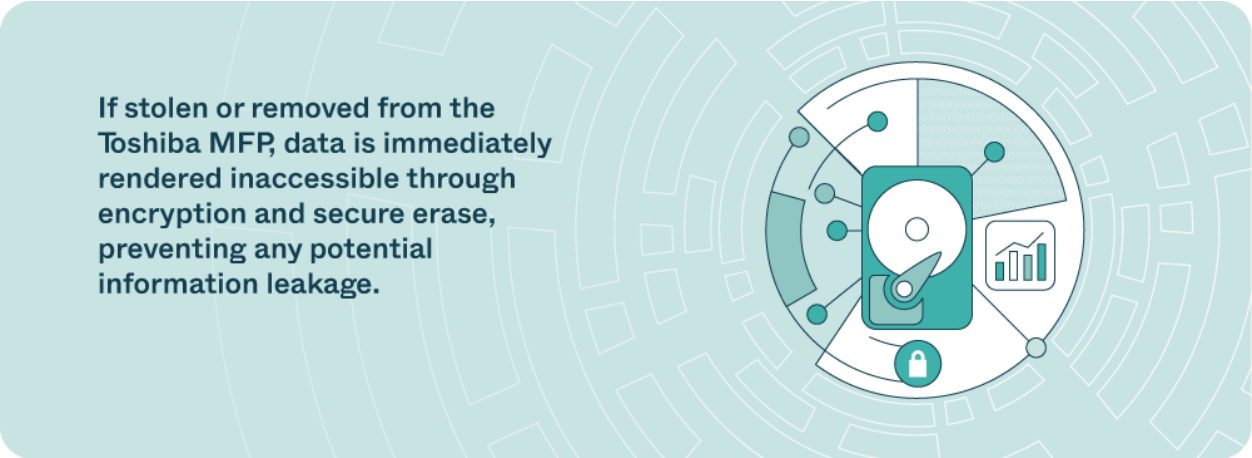
All our firmware is encrypted and digitally signed, and the firmware update process requires a validated digital signature on any firmware being uploaded to the MFP as part of a device updating process. Therefore, firmware from unauthorized sources is rejected by Toshiba devices. Toshiba MFPs also require 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 be installed.

Hardware Security

Toshiba device has several layers of hardware protection; BIOS protection & Trusted Platform Module at the chip level and protection (SSD) 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 140-3 (pending validation) 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.



Trusted Platform Module 2.0

For organizations handling highly sensitive data or operating in regulated environments, enabling and properly configuring TPM 2.0 support for your MFP's storage encryption is a critical security best practice. This proactive measure dramatically enhances data confidentiality, ensures system integrity, and strengthens your overall security posture against evolving threats.

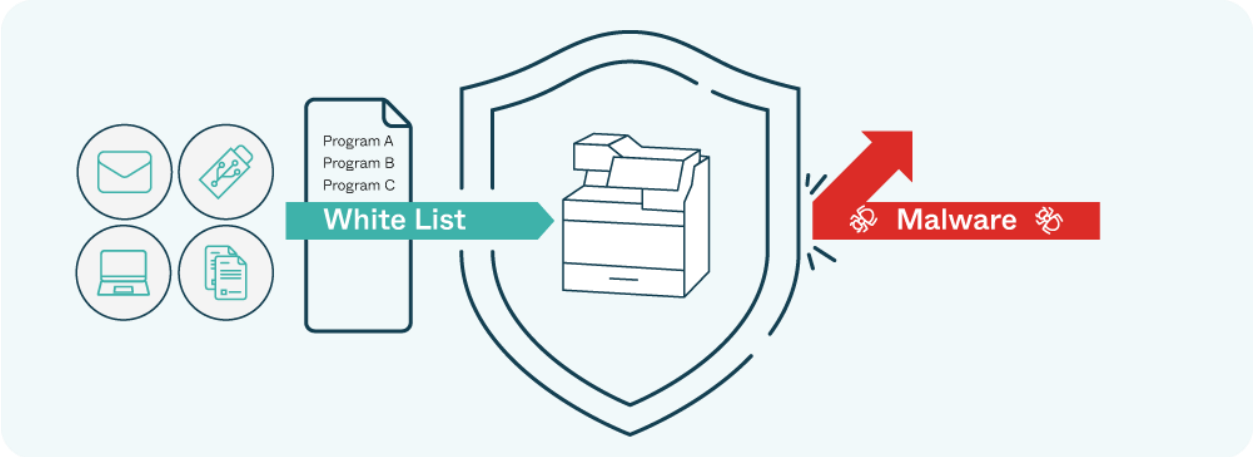
Intel based TPM chips protect all the encryption keys, hashes used for hard drive encryption, firmware protection, and any secure communication between the MFP and other systems. This solution provides another layer of protection in addition to the security features built-in in each component of the MFP. This module inherently creates a root-of-trust that Toshiba devices boot from making the secure boot possible.

The TPM is a secure crypto processor (a dedicated microchip) designed to secure hardware by integrating cryptographic keys into devices. TPM 2.0 represents the latest standard, offering enhanced security features.

Toshiba's TPM application introduce Hardware-Anchored Key Management (HAKM). The ability to enable HAKM allows the Toshiba MFP to act as a secure vault for the encryption keys used by Toshibas Self Encrypting Drives (SED). Instead of keys being solely reliant on the drive itself, keys are generated, stored, and managed within the tamper-resistant TPM chip. Physical security leverages best practices that consider if the disk drive is physically removed from the MFP and placed into another system, the encryption keys remain protected within the TPM, rendering the data on the drive inaccessible without the Toshiba MFP's specific TPM.

Toshiba innovation takes it a step forward with a mindful application of best practices as they relate to measured boot. Toshiba's measured boot establishes a cryptographic chain of trust, starting from an immutable hardware root of trust, and uses this chain to create a verifiable record of every component loaded during the boot process. This technology aligns with standards from NIST, such as SP 800-193, which provides guidelines for platform firmware resiliency by protecting, detecting, and recovering from unauthorized changes. The value of measured boot process is inextricably linked to the Trusted Platform Module (TPM), as the TPM's tamper-resistant Platform Configuration Registers (PCRs) are used to securely store the unique cryptographic hashes (measurements) of each boot component. This best practice ensures that any unauthorized modification to the boot chain—whether to the firmware, bootloader, or OS kernel—will result in a different set of PCR values, which can then be used for remote attestation to prove the integrity of the system to a third party.

[1] National Information Assurance Partnership. (2015, September 11). U.S. government approved protection profile - protection profile for hardcopy devices version 1.0. https://www.niap-ccevs.org/Profile/Info.cfm?PPID=317&id=317



SSD Security

Toshiba MFPs are equipped with carefully selected solid-state drives (SSDs), allowing us to ensure the highest standards of security and reliability. Our SSDs feature multiple layers of protection, including robust data encryption and secure data overwrite capabilities. Additionally, we offer drives that meet stringent industry standards for security, giving customers confidence that their sensitive data is protected throughout the device's lifecycle.

HDD Data Encryption

Toshiba Multi-Function Printers (MFPs) utilizing Hard Disk Drives (HDDs) on select models are equipped with robust data security measures. All data stored on the HDD is protected using AES 256-bit encryption, a standard that ensures strong data confidentiality and integrity. The cryptographic modules and processes employed are designed to align with the rigorous security requirements of FIPS 140-3, assuring administrators and regulatory bodies that the encryption methods meet the latest and most stringent validation standards. Furthermore, even if an MFP is configured without a default secure data wipe function, administrators can leverage Toshiba's embedded software to enable and manage this full-disk encryption, maintaining a consistent and strong security posture across the entire fleet.

Critical to managing the device lifecycle, Toshiba MFPs enable secure data disposal via Cryptographic Erase when the device is decommissioned or leased back. This process, termed "invalidation" involves the instant and irreversible invalidation of the encryption key, which immediately renders all stored data permanently and forensically unrecoverable. This method of media sanitization directly adheres to the guidelines established in NIST Special Publication 800-88, Revision 1, ensuring that data privacy and regulatory compliance obligations are met, thus safeguarding sensitive information from unauthorized retrieval throughout the device's operational lifespan.

Automatic SSD Data Overwrite

The Data Overwrite feature on Toshiba MFPs allows data that is temporarily stored on the SSD 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 SSD 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 140-3 Protection (Pending Validation)

Toshiba also offers a FIPS 140-3 (pending validation) specifically for those government agencies and private sector businesses where data protection is of utmost importance. FIPS 140-3 is designed to address the encryption and tamper resistance of an SSD. 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 140-3 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 SSD is accessed by an unregistered system. Unlike software-based encryption which relies on the system CPU for encryption processing, the SSD leverages its onboard crypto-processor to encrypt at full interface speed without impacting system-level performance. With FIPS 140-3 level 3 compliance, Toshiba's offering provides tamper-evident labeling to deliver a high level of security.

SSD Data Protection

From the latest Toshiba Office Collection models, a self-encrypting SSD is equipped in Toshiba MFPs as a standard storage device. All data stored in SSD are encrypted by an AES (Advanced Encryption Standard) 256-bit algorithm. Data overwrite feature is also standard on these SSDs because they are built-in to the SSD controller via "wear leveling" algorithms. Moreover, an optional FIPS certified HDD may be installed on the MFP in addition to the SSD. If optional FIPS SSD is installed, all use data are stored in the HDD so that the data is protected by encryption certified by FIPS 140-3 (pending validation).

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 SSD 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 Elevate sky Service tools. 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

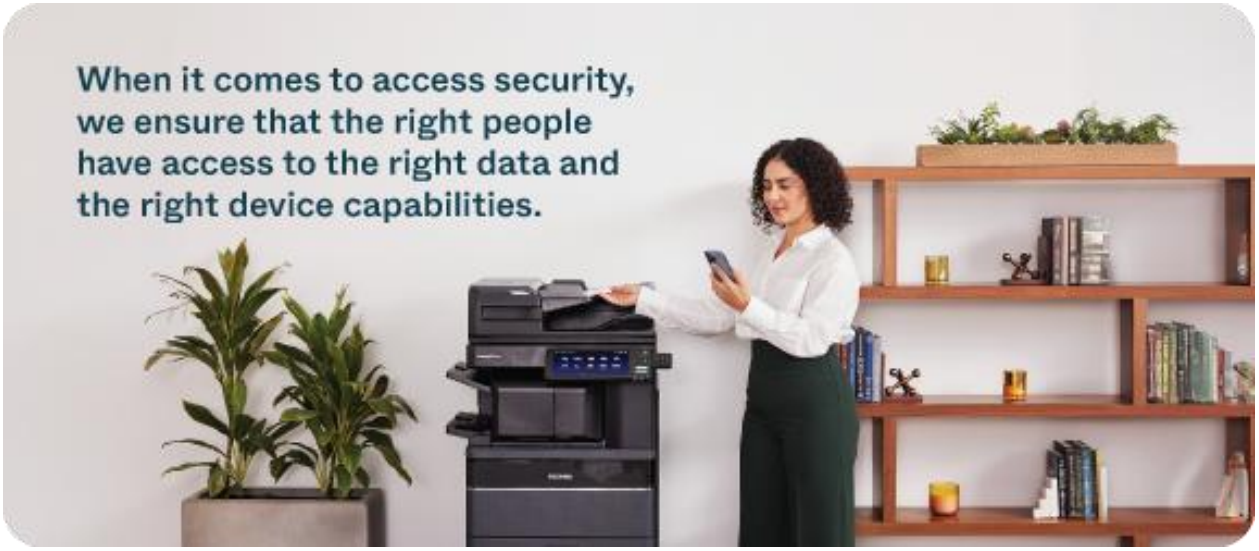
When it comes to access security, we ensure that the right people have access to the right data and the right device capabilities. Our approach to device access may be categorized into the following categories:

- 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.

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 Several authentication methods are supported on Toshiba MFPs:

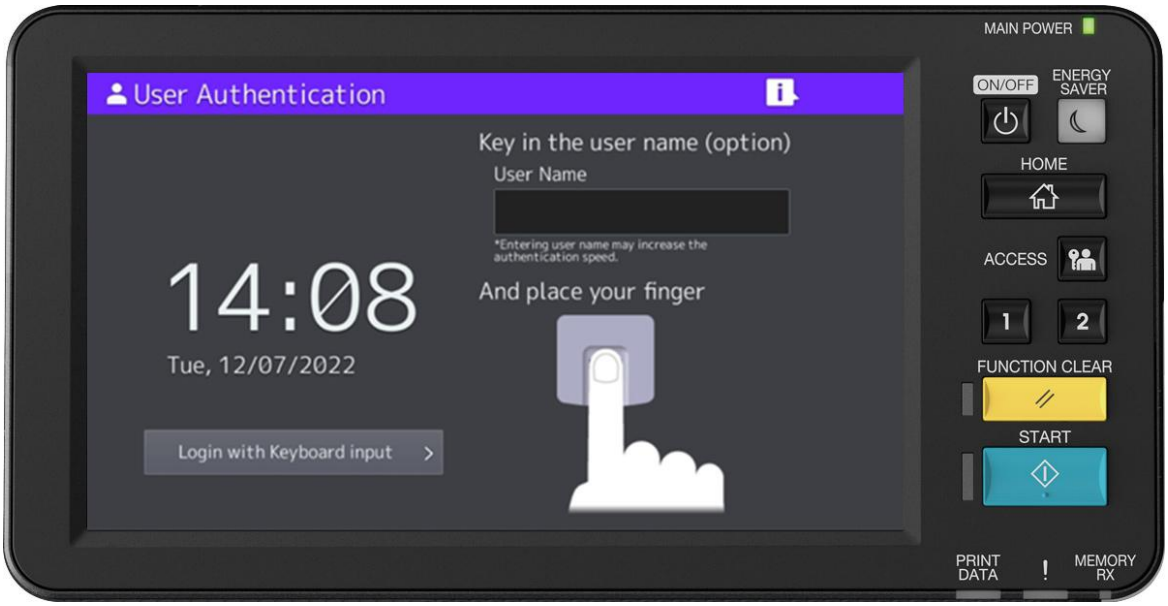
- Department code authentication
- User ID/password authentication
    - Local authentication by the MFP itself
    - Windows domain authentication
    - LDAP/AD server authentication
- PIN authentication
- Badge authentication
- Two-factor authentication, using badge and PIN
- NFC (Near-Field-Communication)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

As organizations continue to build upon these fundamental authentication methods, organizations should implement identity and access management (IAM) strategies that align with industry-recognized security standards. Leveraging a centralized identity provider, such as Microsoft Entra ID (formerly Azure Active Directory), Google Workspace Identity, or other cloud-based Identity as a Service (IDaaS) solutions, allows for consistent enforcement of robust

Multi-Factor Authentication (MFA) policies across all print devices, significantly reducing the risk of credential compromise. Adherence to guidelines like NIST Special Publication 800-63 (Digital Identity Guidelines) are crucial for establishing strong identity proofing and authentication processes. Furthermore, implementing the principle of least privilege ensures users and administrators are granted only the necessary access to MFP functions (e.g., color printing, scanning to specific destinations), and regular access reviews are conducted. This disciplined approach, foundational to a Zero Trust Architecture, extends security from the network to the MFP, while continuously verifying every access request.

Biometric Authentication

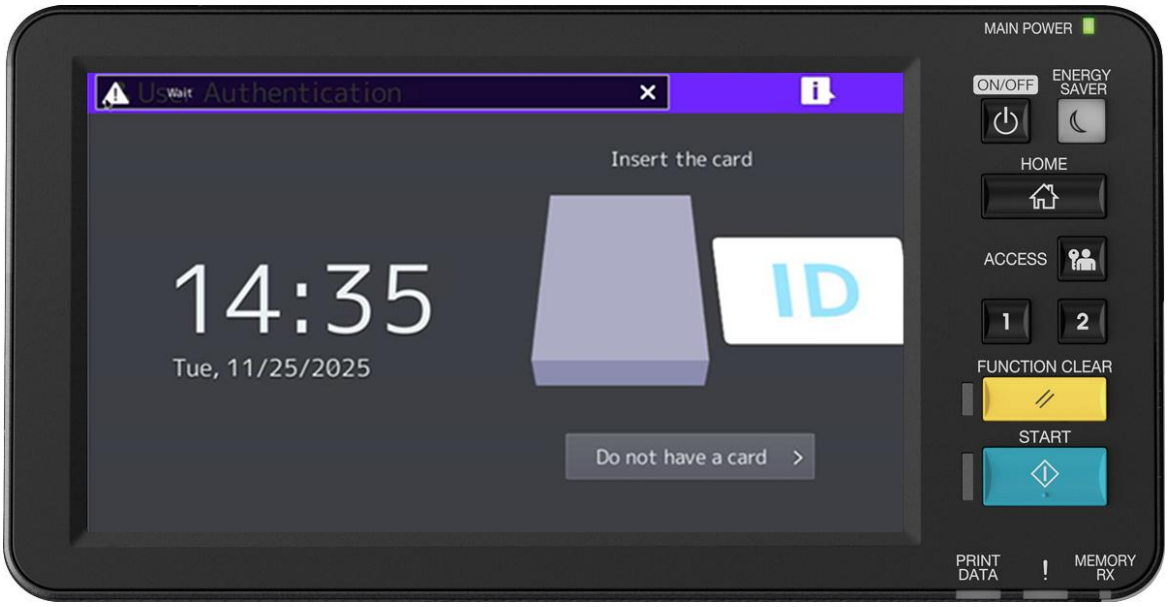
Toshiba MFPs now natively support biometric authentication. Users can self-register by scanning their fingerprint via a fingerprint reader. Fingerprint images collected by fingerprint readers are converted into files (fingerprint template) and are stored in an internal storage device of the MFP. We don’t store scanned fingerprint images, so users’ personal information won’t be compromised. Moreover, you can configure the MFP with two-factor authentication, using CAC/PIV Card or PIN together with fingerprint authentication. In consideration of best practices, it is imperative for organizations to verify user identity, providing a strong, "something you are" factor that is difficult to forge. Toshiba continues to lead the way by aligning with NIST's digital identity guidelines in Special Publication (SP) 800-63. This stringent alignment meets numerous Authenticator Assurance Levels (AALs). Toshiba Biometrics meets AA Level 2(AAL2) and AA Level 3(AAL3) standards, while being used as a cryptographic or multi-factor authenticator that provides a user's identity with a high degree of confidence. The value of biometrics, when implemented correctly, is that they are inherently tied to an individual's unique biological or behavioral traits, providing a robust layer of security that resists common attacks like phishing, password stuffing, and credential theft, thereby significantly reducing the risk of unauthorized access.



CAC/PIV Authentication

Toshiba's implementation of the optional CAC/PIV (Common Access Card/Personal Identity Verification) application for Department of Defense (DoD) and Government agencies significantly elevates the security posture of Toshiba Multi-Function Printers (MFPs). CAC/PIV functionality is crucial for restricting unauthorized access to the MFP and its sub-functions, including print, copy, and scan, by ensuring that such grants are based exclusively on the successful validation of a valid CAC/PIV card. This access control mechanism is fully compliant with Homeland Security Presidential Directive 12 (HSPD-12) and FIPS 201-3, which mandate strong, interoperable identity credentials for all federal employees and contractors accessing controlled facilities and information systems. Once enabled, the CAC/PIV application hardens the system and applies further restrictions to Toshiba's TopAccess management platform, preventing unauthorized configuration changes.

This enhanced security extends deep into the device's operational technology. The enabled CAC/PIV application further improves certificate management and utilizes Online Certificate Status Protocol (OCSP) validation technologies, which verify the real-time revocation status of the credentials, a critical step for security superiority. This rigorous check ensures continuous high assurance for user authentication and authorization. Additionally, a crucial security feature of the CAC/PIV implementation is the lockdown capability: any unauthorized attempt to use a Toshiba MFP configured in CAC/PIV mode will instantly trigger a system lockdown, safeguarding the device and its stored data against persistent threats, thereby enforcing the principle of least privilege.



Password Policy

Building on the foundation of a robust password policy, organizations should elevate their practices by aligning with comprehensive security frameworks. Toshiba's alignment and adherence to both Control IA.3.1.6 (requiring the change of default passwords) and IA.3.1.8 (mandating at least a 15-character passphrase for new accounts) of the NIST Special Publication 800-171 outlines support for critical security best practices. This proactive approach

ensures robust credential strength and directly addresses vulnerabilities stemming from weak or factory-set passwords, thereby providing detailed guidance for protecting controlled unclassified information within print environments. Further key elements of this stringent security posture, as outlined by NIST SP 800-171's Identification and Authentication (IA) family, include implementing account lockout after a maximum number of incorrect attempts (IA.3.1.7) and ensuring the comprehensive protection of authenticators (IA.3.1.5). This disciplined approach, foundational to Zero Trust Architecture, extends security from the network to the individual device, continuously verifying every access request.

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. Toshiba has instituted technology that aligns with the best practice for managing USB ports. The goal of adhering to this best practice is to prohibit or restrict USB use by default on all MFPs and only enable them when there is a strong business justification, aligning with NIST SP 800-171's Media Protection (MP) and Access Control (AC) families. This hardening approach directly addresses controls such as MP-7, which mandates the control of removable media use on system components, and AC-3, which requires the enforcement of access restrictions. The value of this practice lies in its ability to mitigate a significant number of security risks, including the introduction of malware from untrusted devices, the exfiltration of Controlled Unclassified Information (CUI), and the risk of unauthorized data loss from misplaced or stolen media.

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. In consideration of best practices, Toshiba's IP and MAC address filtering focuses on implementing a supplemental

layer of defense in a "deny-by-default" mode, rather than as a primary security control. This approach aligns with the NIST SP 800-171 Access Control (AC) and System and Communications Protection (SC) families, particularly controls like AC-3 and SC-7, which mandate controlling the flow of information and enforcing access restrictions at network boundaries. The value of this filtering is that it provides a basic level of control by limiting connections to known, authorized devices and preventing unauthorized network access from the outset. Although Toshiba has made innovative strides in IP/Mac Address Filtering, it is always noteworthy to highlight limited effectiveness, as both IP and MAC addresses can be easily spoofed. This consideration advocates that organizations should always apply IP/MAC address filtering in conjunction with stronger security measures like robust authentication and encryption, such as Wi-Fi Protected Access (WPA) version 3 / WPA3 for wireless networks.

Transport Layer Security (TLS)

Toshiba MFPs may be configured to allow all communication over secure TLS 1.2 protocol or higher including TLS 1.3, 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 or higher 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.

Toshiba’s focus objective for Transport Layer Security (TLS) is to proactively manage the protocol version and cryptographic suite, using only the most modern and secure options available. This best practice aligns directly with NIST guidelines in SP 800-52 Rev. 2, which requires federal systems and, by extension, non-federal systems handling Controlled Unclassified Information (CUI) under SP 800-171, to support a minimum of TLS 1.2 and transition to TLS 1.3. The value of this practice is its ability to protect data in transit from eavesdropping and tampering by preventing the use of weak or vulnerable older protocols (like SSL and older TLS versions) and ensuring that communication relies on strong, state-of-the-art ciphers, thereby mitigating common security threats like downgrade attacks and man-in-the-middle attacks.

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 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). A key best practice for IP Layer Security is to use IPsec to provide a robust, cryptographic layer of protection for data as it traverses a network. This approach aligns with NIST guidance in SP 800-77, which provides detailed recommendations for implementing IPsec Virtual Private Networks (VPN)s to secure communications over IP networks. The value of IPsec is that it provides authentication, integrity, and confidentiality at the network layer, effectively securing the IP packets themselves. This essential methodology ensures that even if a network is compromised, the data remains protected from eavesdropping and tampering, thereby fulfilling the System and Communications Protection (SC) requirements of NIST SP 800-171 by protecting the confidentiality and integrity of Controlled Unclassified Information (CUI) in transit.

Network Authentication

Toshiba MFPs support several network authentications schemes:

- IEEE 802.1X is the standard for network authentication utilized in Toshiba MFPs. IEEE 802.1X consists of a supplicant, 802.1X switch and an authentication server. IEEE 802.1X 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 (Message Digest 5), MSCHAPv2 (Microsoft Challenge Handshake Authentication Protocol version 2), EAP-TLS (Transport Layer Security), EAP-TTLS (Tunneled Transport Layer Security), and PEAP (Protected Extensible Authentication Protocol) methods. Currently, these methods are supported. For certificate installation with EAP-TLS, EAP-TTLS, and PEAP, manual import or SCEP (Simple Certificate Enrollment Protocol) can be utilized.

- LDAP (Lightweight Directory Access Protocol) / AD (Active Directory) authentication supports CRAM (Challenge-Response Authentication Mechanism)-MD5, Digest-MD5, and Kerberos to protect the username and password required for access to an LDAP/AD server.

- SMTP (Simple Mail Transfer Protocol) authentication supports CRAM-MD5, Digest-MD5, Kerberos, and NTLM (New Technology LAN Manager) (IWA: Integrated Windows Authentication) to protect the username and password required for access to an SMTP server.

- POP3 (Post Office Protocol 3) authentication supports Kerberos, NTLM (SPA: Secure Password Authentication), and APOP (Authenticated Post Office Protocol) to protect the username and password required for access to a POP3 server.

    - SMB (Server Message Block) authentication supports NTLMv2 and Kerberos. Also, the less secure SMBv1 can be disabled.

    - Dynamic DNS (Domain Name System) supports Secure Dynamic DNS. 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.

    - SNTP (Simple Network Time Protocol) supports SNTP authentication, enabling authentication of an SNTP session between the MFP and an SNTP server.

    - Toshiba MFPs also support SNMPv3 (Simple Network Management Protocol version 3), which has both a data encryption and a user authentication function to enhance security features.

The best practice for network authentication schemes is to mandate the use of strong, certificate-based authentication methods like EAP-TLS and PEAP over IEEE 802.1X, while disabling all less secure methods such as EAP-MD5 and MSCHAPv2. Toshiba's authentication methods align with NIST SP 800-171's Access Control (AC) and System and Communications Protection (SC) families, particularly controls like AC-3 and SC-8, which require enforcing access restrictions and protecting the integrity of communications. Toshiba's security approach establishes a mutual trust relationship between the MFP and authentication servers (where applicable), providing a robust, cryptographically secure barrier against unauthorized network access and protecting the authentication process from common attacks such as credential theft and replay attacks.

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 Wi-Fi Protected Access version 3 (WPA3), which encrypts data and allows user authentication. WPA3 is a security standard established by the Wi-Fi Alliance. It's strongly recommended that organizations use WPA3 standard because it provides more enhanced encryption and connectivity. In consideration of best practice for wireless security, Toshiba advocates disabling legacy wireless protocols like WPA and WPA2. Toshiba's stringent approach to wireless security aligns directly with NIST Special Publication (SP) 800-171's System and Communications Protection (SC) family, notably control SC-8, which requires organizations to protect the confidentiality and integrity of Controlled Unclassified Information (CUI) in transit. The value of this practice is that WPA3 uses the Simultaneous Authentication of Equals (SAE) handshake, which provides strong cryptographic protection against offline dictionary attacks and the Key Reinstallation Attack (KRACK), ensuring that wireless transmissions are secure from unauthorized access and eavesdropping.

Two connection methods are typically supported. WPAPSK allows user authentication and encrypt 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.

Multiple NIC Support

Toshiba's latest MFP models support multiple ethernet cards.. As a result, the MFP can be connected to multiple networks at the same time. Thus, the users can print to the same MFP from multiple networks. However, these networks are completely independent and can't be accessed from one another. This helps network administrators keep their corporate network secure from any guest network setup. Organizations should consider best practices for systems with multiple Network Interface Cards (NICs) for network segmentation, physically or logically separating networks based on their security posture. This connectivity approach aligns directly with NIST Special Publication (SP) 800-171's System and Communications Protection (SC) family, especially controls like SC-7 (Boundary Protection) and SC-10 (Network Connections), which require the monitoring and control of communications at network boundaries. The value of this practice lies in its ability to significantly reduce the attack surface and contain a security breach. By isolating systems that process, store, or transmit Controlled Unclassified Information (CUI) from less-trusted networks, network segmentation prevents attackers from pivoting to sensitive systems and data, thereby limiting the scope of a compromise.

The advantages of network segmentation capability also facilitate Network Isolation, which is particularly valuable for Multifunction Printers (MFPs). An MFP with multiple NICs can be configured to receive print requests on entirely independent networks, such as a secure internal network and a separate guest network, without requiring a direct connection between them. This practice reinforces the Access Control (AC) requirements of NIST SP 800-171, ensuring that sensitive data transmitted from the internal network remains logically isolated and is not exposed to the less-trusted network, thereby maintaining the confidentiality of the information in transit.

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 with 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. Additionally, Toshiba's Role-based Access Control (RBAC) model aligns directly with NIST Special Publication (SP) 800-171's Access Control (AC) family, specifically controls AC-3 (Access Enforcement) and AC-2 (Account Management), which require organizations to enforce access restrictions and manage user accounts with defined rights. The value of this best practice is that it ensures the principle of "least privilege" is consistently applied, limiting user access to only the information and resources necessary to perform their duties. Toshiba's application of this approach significantly reduces the administrative burden of managing individual permissions and minimizes the risk of unauthorized access and data exfiltration.

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. As a best practice, organizations should implement a comprehensive and continuous security monitoring program that includes the collection and analysis of audit logs and the deployment of an Intrusion Detection System (IDS). Toshiba's integration of monitoring solutions aligns directly with NIST Special Publication (SP) 800-171's Audit and Accountability (AU) family, which requires organizations to create, retain, and review system audit logs. This highly regarding standard also relates to the System and Communications Protection (SC) family, considering that IDS provides a critical layer of network security. The value of this best practice is that it provides real-time visibility into system and network activity, enabling the early detection of suspicious behavior and potential security incidents. By maintaining a detailed record of events, organizations can effectively trace the source of a compromise, facilitate rapid incident response and reduce the risk of unauthorized access to Controlled Unclassified Information (CUI).

Audit Log

Each operation on the control panel and in the MFP web portal (TopAccess) is recorded as a system log 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.

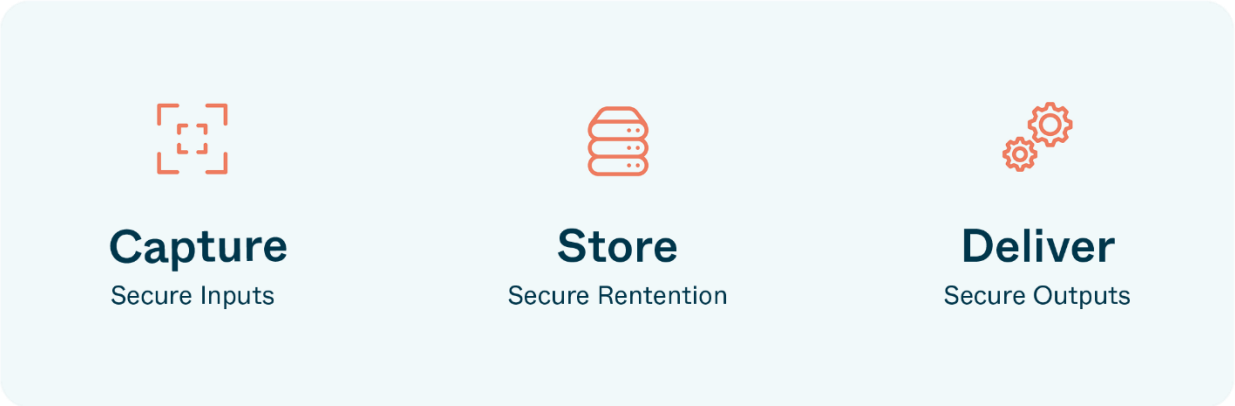
Intrusion Detection

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 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. Considering best practices, Toshiba's approach to document security is to implement a holistic framework that protects documents throughout their entire lifecycle, from capture, storage, to delivery. This approach aligns with multiple control families in NIST Special Publication (SP) 800-171, including Media Protection (MP), Access Control (AC), and System and Communications Protection (SC), which together address the protection of information at rest and in transit. The value of this comprehensive approach is that it ensures the confidentiality and integrity of Controlled Unclassified Information (CUI) at every stage. For document capture, this means authenticating the user and encrypting the data during transmission. For document store, it requires encrypting documents at rest and applying robust access controls to prevent unauthorized viewing. For document delivery, it mandates the use of secure, encrypted channels to ensure that the document remains confidential and is only accessible by the intended recipient.



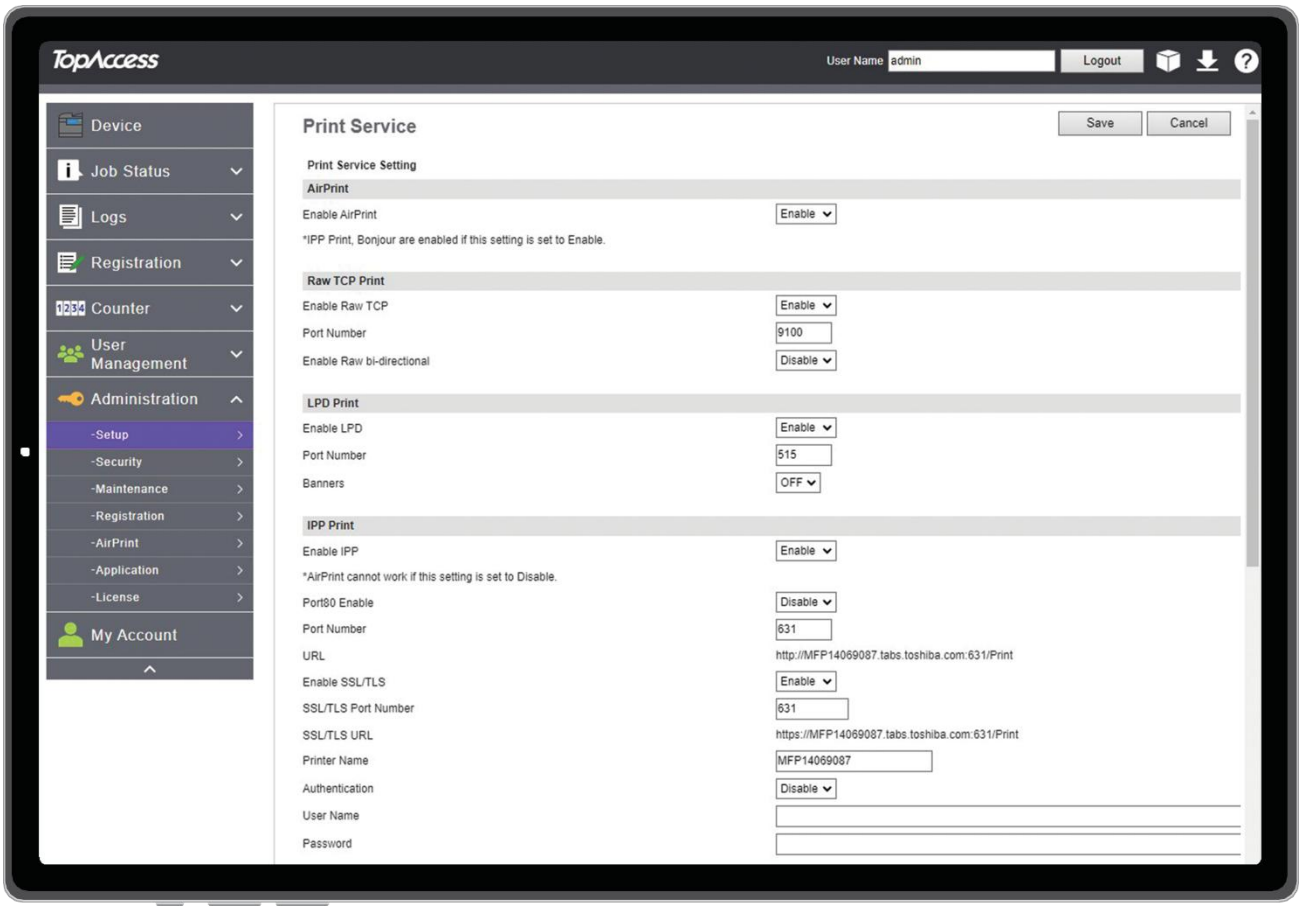
4.1 Capture

provided for each method of entry. Toshiba offers solutions such as Elevate Sky Translate (EST) and Elevate Sky Workflow (ESW) that revolutionize capture technology, but place security front and center. EST and ESW's use of AI-driven Intelligent Document Processing (IDP) is a cutting-edge approach to integrating a secure document lifecycle management system to automate the classification, extraction, and protection of sensitive information from the point of capture. This aligns with multiple control families in NIST SP 800-171, particularly Media Protection (MP) by ensuring secure handling of information captured from physical media, and Access Control (AC. The value of IDP is that it significantly reduces the risk of human error and data exposure by automating the secure handling of documents, ensuring that sensitive data is immediately identified, protected, and routed to a secure repository, thereby strengthening the

overall security posture from the very first step of the document lifecycle. As a best practice organizations should utilize and implement secure print stream, email security, as well as USB malware protection solutions.

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 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.

4.2 Store

Toshiba's MFP Solid State 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 256-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.

PDF With Digital Signature

Documents can be scanned to create PDF file with a digital signature to prevent tampering and guarantee originality. Certificates which are used for a digital signature can also be created natively in the MFP (RSA2048) or can also be imported. Digital signed PDF documents ensure originality and security of the scanned documents.

e-Filing Password Control

It is strongly recommended to set up a password to create a secure 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 Delivery

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 SSD 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 Elevate Sky® Print Management allows users to send a print job securely to the cloud and release it at any authorized Toshiba MFP. The job remains in a protected queue until the user authenticates at the device via PIN or badge, with no additional hardware or software required. This ensures confidential documents never sit unattended on output trays, safeguarding sensitive information. Print jobs are transmitted using robust encryption protocols, providing peace of mind that data remains secure throughout the workflow.

Toshiba's e-BRIDGE® Global Print further secures customers' print environment by providing a pull print solution through the cloud. The user sends their print jobs securely to the Toshiba cloud and releases the print job at any Toshiba MFP by logging into the device via PIN or badge. No additional software or hardware is required. By integrating this solution with Microsoft 365 & Google identity provider, we ensure that user credentials are not duplicated further enhancing security.

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 errors, 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 ensure 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.

Scan to Cloud Security

The optional Scan to Cloud feature available for Toshiba MFPs is built on the core security premise of Role-Based Access Control (RBAC). RBAC allows administrators to strictly control and grant the privilege to scan documents directly to cloud storage platforms, while only allowing authorized users, thereby enforcing the Principle of Least Privilege. Toshiba's scan to cloud feature can be quickly and securely enabled and managed remotely via Toshiba's Elevate Sky Print Management secure cloud management dashboard, simplifying fleet-wide deployment and policy enforcement.

When an end-user initiates a scan, they can have peace of mind knowing the data is protected throughout the entire transit process. Documents scanned by the MFP are securely transported to cloud stores using industry-standard TLS 1.2+ encryption and robust API authentication stacks (such as OAuth 2.0 or SAML) utilized by major cloud providers like Google Drive/Workspace and

Microsoft Azure/365. The scanned documents are ultimately stored on cloud storage platforms (e.g., Microsoft OneDrive, Google Drive) that are managed and further secured by the respective cloud platforms themselves, adhering to global standards like ISO/IEC 27001 and regulatory frameworks like GDPR or HIPAA. This approach ensures end-to-end security, relying on the highest levels of cloud infrastructure security to safeguard the confidentiality and integrity of your digital documents.

5. Cloud Security

Built-In Anti-Malware

Toshiba MFPs are now equipped with built-in anti-malware that protects against ransomware and other malicious software, helping safeguard sensitive data and maintain the integrity of your devices. When enabled, the anti-malware prohibits any unauthorized software from running on the MFP. If any malware is detected the MFP reports the warning on the panel and automatically reboots to last know safe state. This provides another layer of protection against any attack through the cloud.

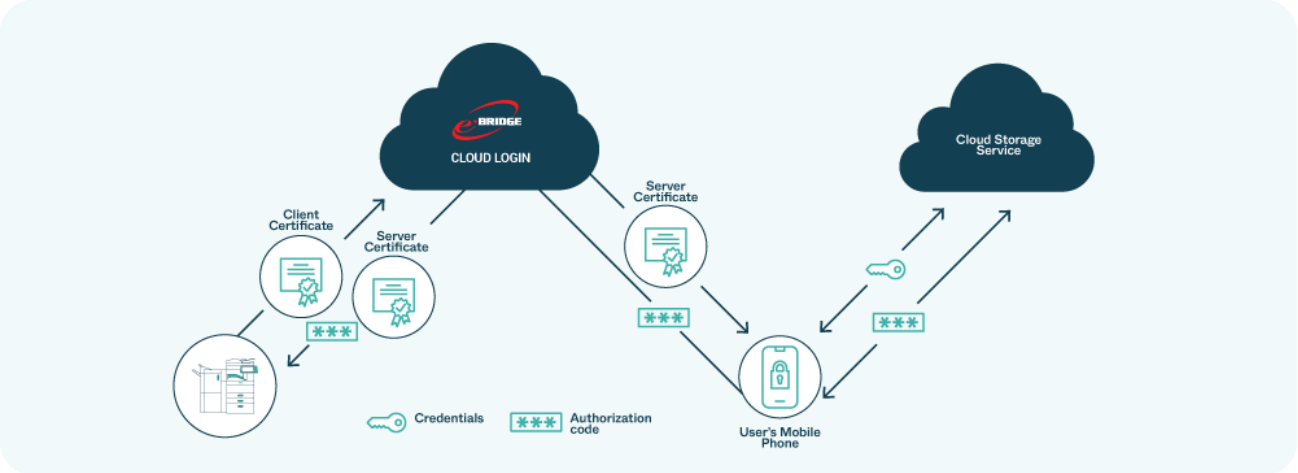
OAuth2 Token-Based Authentication to Cloud Storage Services

All our cloud storage applications take additional measures to ensure that user data is protected at all costs. Our e-BRIDGE Cloud Login (eCL) service ensures that user credentials are never stored at the MFP while still supporting single sign-on (SSO) on the device panel. eCL facilitates user login from the MFP panel by scanning a QR code from a mobile device. The user is then directed to their cloud storage login URL. All communication between eCL and the user's mobile device occurs over secure HTTPS using at least 256-bit encryption and 2048-bit key. No user identifiable data is collected or stored in eCL Only the following data is used to facilitate this login service:

- Access time
- Model name of MFP
- Serial number of MFP

- Application ID of the embedded application
- Authorization code
- Only the authorization code is used to manage user sessions and actions on the panel.

eCL is hosted on AWS (Amazon Web Services) and complies with ISO/IEC 27001 (Information Security Management) & ISO/IEC 27017/27018 (Cloud Service Security). For more details, please refer to the AWS site **https://aws.amazon.com/ security/**. Additionally, Toshiba internal security team conducts routine security checks on the cloud environment, including vulnerability scanning and penetration testing. Toshiba's embrace of best practices embodies the use and application of OAuth2 token-based authentication to cloud storage providers as a mechanism to utilize short-lived access tokens combined with refresh tokens and to enforce strict scoping to the minimum required permissions. Toshiba's use of the OAuth2 methodology aligns with NIST Special Publication (SP) 800-171's Access Control (AC) and System and Communications Protection (SC) families. Specifically, this methodology supports the "least privilege" principle under AC-3 by limiting a token's permissions, and it reinforces SC-8 by ensuring the secure transmission and handling of tokens. The value of this best practice is that it minimizes the window of opportunity for an attacker to use a compromised token, as its short lifespan quickly renders it useless. By enforcing a minimal scope, even if a token is stolen, the attacker's ability to access or manipulate sensitive data is severely restricted, providing a robust layer of protection for Controlled Unclassified Information (CUI).

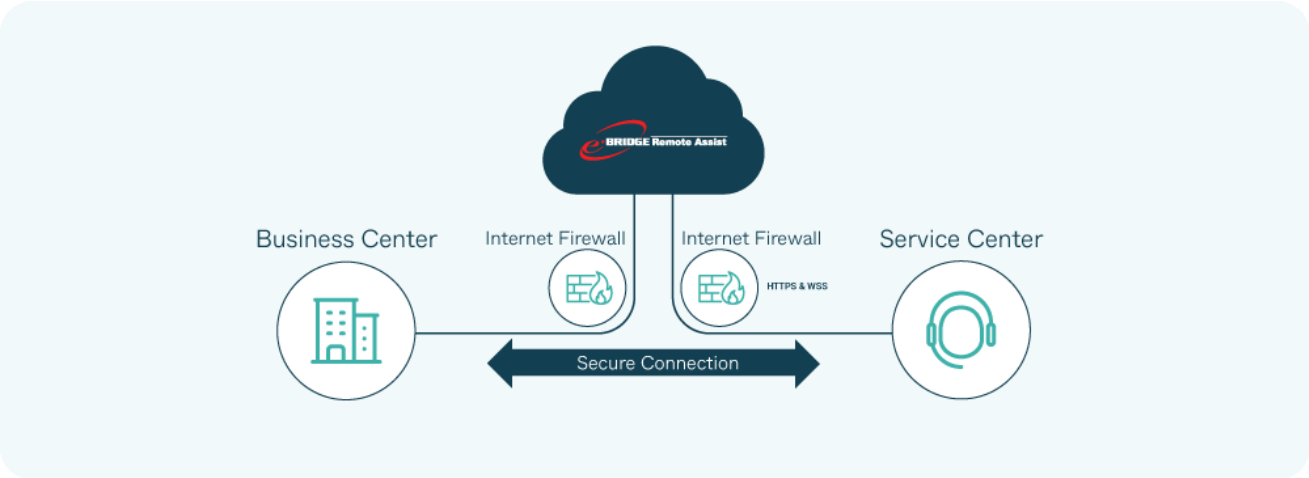


MFP Access Control

Not only is our cloud application designed to protect the privacy and integrity of customer data, but so is our service and support infrastructure. Our cloud-based e-BRIDGE ESS Remote Assist (eRA) tool enables us to provide better support to our customers by connecting to the MFP front panel (with customer's permission) to diagnose any issues. This uses the same principle as connecting to a remote server using a browser over HTTPS with server authentication and encryption.

For any remote connection to happen, the customer must authorize the service technician by entering a code on the MFP panel. Therefore, a connection cannot be started remotely without the customer's consent. To prevent eavesdropping and ensure data is transmitted to the correct cloud server, the MFP authenticates itself to the cloud server before transmitting any data. All transmitted

and received data are encrypted to preserve user confidentiality and to protect against stealing and tampering. Only data related to the MFP panel is handled by eRA. Any other customer data, such as documents, address book, copy, fax, and scan data are not communicated to the cloud. Finally, the security policies on the MFP are strictly maintained and security of our cloud environment is managed in accordance with ISO 27001 international standard for information security management.



Shared Responsibility Model

Toshiba utilizes leading cloud hosting providers such as Microsoft Azure and Amazon AWS for Elevate Sky Services. As with any cloud hosting provider, we follow a shared responsibility model when it comes to security. The cloud hosting providers ensure security of the underlying infrastructure such as OS, network, database, domain etc., whereas Toshiba takes necessary actions to ensure security of cloud applications and customer data. Toshiba's approach to the shared responsibility model goes a step further by actively managing Toshiba's security responsibilities, which includes securing data, user access, and applications, and not solely relying on the cloud service provider's security measures. This shared responsibility model aligns with NIST Special Publication (SP) 800-171's Planning (PL) and Risk Assessment (RA) control families, which mandate that organizations have documented security policies and actively mitigate risks, including those related to cloud services. The value of this approach is that it prevents security gaps and clarifies accountability. By recognizing that the organization is ultimately responsible for the security in the cloud, security teams can focus their efforts on their specific obligations, ensuring that controls for sensitive data, like Controlled Unclassified Information (CUI), are not overlooked and thereby significantly reduce the risk of breach due to misconfiguration. Our data security and application management process is described below.

Collect Data & Security

In order to offer Elevate Sky Services, we collect service and telemetry data for the devices deployed. We don't collect any user identifiable PII data. This information contains data regarding the usage and maintenance, such as counter data (number of used sheets of paper), device failure, consumables replacement, device settings and adjustment. Furthermore, data collected from MFPs

are encrypted by an HTTPS protocol and then can only be sent from MFPs to a Toshiba Elevate Sky server with valid authentication, resulting in the prevention of outside intrusion into the MFP. As a best practice and security data safeguard, Personally Identifiable Information (PII) is never collected. Toshiba implements a strict, zero-tolerance policy against the collection, processing, or storage of PII, and to conduct regular data inventories to ensure that no PII is being inadvertently acquired. This best practice aligns with NIST Special Publication (SP) 800-171's core principle of data minimization as a fundamental risk mitigation strategy. The value of this approach is that it eliminates the organization's exposure to the legal, financial, and reputational risks associated with a PII data breach. By removing PII as a potential attack vector, organizations can streamline their security posture, reduce compliance burdens, and avoid the significant costs and liabilities of safeguarding such sensitive information, thereby ensuring the confidentiality of all data it does handle.

Collected Data

1. ***Device information***
   Serial number, model name, device explanation, others (MFP unique information)

2. ***Counter information***
   Print counter, scan counter, MFP type (B&W or color), other counters

3. ***Consumables' information***
   Toner cartridge remaining amount, drum cartridge status, other consumables' information

4. ***Service-related information***

5. ***Device settings, error code, firmware version, other service-related information***

Operation & Management of Cloud Services

ISO27001/ISO27017 Compliance

Toshiba cloud services are hosted in environments that have obtained ISMS (Information Security Management System) certification (ISO/IEC 27001 & 27017).

Security & Compliance of Microsoft Azure

Toshiba cloud services are hosted by Microsoft Azure, and thus the security of the data center is maintained at the highest standards. Microsoft Azure complies with numerous standards including ISO 27001, ISO 27018, SOC 1, SOC 2, SOC3, FedRAMP, HITRUST, MTCS, IRAP and ENS. For further details, refer to the following URL for the Microsoft Azure website.https://**www.microsoft.com/en-us/TrustCenter/Compliance/**

Periodic Vulnerability Audits

To ensure the utmost security of the systems and services, Toshiba performs vulnerability audits prior to release and on a regular basis. WebInspect by Micro Focus and InsightVM by Rapid 7 are used as a vulnerability check tool to perform vulnerability assessments specific to web applications.

Service Performance Monitoring

This tool collects and analyzes telemetry by using Azure Monitor to ensure the cloud services are available and performing at its peak by proactively identifying and acting on potential problems quickly.

Backup & Recovery

The back-up function provided by Azure is used to back up the database. The back-up data are all encrypted (AES256) and then stored in a storage location in Azure. This back-up data may be used for data recovery during any failure.

Event Logs Management

Azure management service is utilized to monitor & manage event logs. Moreover, appropriate logs required to maintain and manage the service are stored for up to 180 days by using Azure Monitor and Azure Application Insights. Users cannot access these event logs. Only Toshiba and its subsidiary may access these logs.

User Access Security to Cloud Services

User Authentication

A cloud directory service is a cloud-based identity and access management (IAM) solution that manages users, groups, and devices as a central source of truth for user authentication. Unlike traditional on-premise Active Directory, Toshiba’s cloud-based directory services is a managed service that can provide single sign-on (SSO) and multi-factor authentication (MFA) to a wide range of applications without the need for a corporate network. Additionally, cloud-based Directory Services acts as the central identity provider, allowing for the centralized management of access across an organization’s digital resources.

Toshiba advocates using cloud directory services as a best practice (specifically Microsoft Entra ID and Google Workspace) to configure a single, authoritative identity source and enforce a "least privilege" access model across all integrated applications by mandating Multi-Factor Authentication (MFA) and implementing conditional access policies. Toshiba use of TPM cloud directory services for user authentication aligns with NIST Special Publication (SP) 800-171's Identification and Authentication (IA) and Access Control (AC) families. Specifically, it supports IA-2 (Identification of Users) and IA-5 (Authenticator Management) by centralizing identity and enforcing strong MFA, while AC-3 (Access Enforcement) is met by using conditional policies to limit access. The value of this approach is that it provides a centralized and scalable security control plane, drastically

reducing the risk of credential theft and unauthorized access. Cloud based directory services for user authentication simplifies the user lifecycle management process, ensuring that access to all applications is immediately provisioned or de-provisioned, thereby protecting sensitive data and mitigating security risks.

Encrypted Communication

All user communications with this service are protected using HTTPS protocol supporting encryption at TLS 1.2 or higher only. Cloud communication is encrypted in a two-part process. Data is encrypted at rest when it is stored on the provider's servers, typically using strong algorithms like AES-256. Simultaneously, all communication between a user's device consuming Toshiba cloud services or an MFP and the cloud service is encrypted in transit using secure protocols such as TLS (Transport Layer Security) 1.2, which prevents interception of data as it travels across the network.

Server Authentication

Server authentication, as it relates to cloud services, is a critical security process in which a client (e.g., an embedded web browser within the Toshiba MFP or 3rd party application) verifies the legitimacy of a server before sending any data. This process is primarily managed by TLS (Transport Layer Security) or its predecessor, SSL, through the use of digital certificates. TLS/SSL certificates are digital documents issued by a trusted third-party, known as a Certificate Authority (CA). The certificate contains the server's public key, its identity (e.g., the domain name), and a digital signature from the CA. The core function and best practice is to embrace server spoofing prevention. In efforts to deploy server spoofing prevention, the MFP and/or client attempts to connect to a cloud service, the server presents its TLS certificate.

The Toshiba MFP / Embedded Web Browser / 3rd party app acting as a client performs two vital checks:

- It verifies the digital signature on the certificate against its pre-installed list of trusted CAs. If the signature is valid, the client trusts that a legitimate authority issued the certificate.
- It checks that the domain name in the certificate (e.g., aws.amazon.com) matches the domain name the user intended to connect to.

If a malicious actor attempts to spoof a cloud server by creating a fake website, they will not be able to obtain a valid, trusted certificate for the legitimate domain. The client's browser will detect the mismatch or invalid signature, immediately displaying a security warning. Toshiba's server authentication policies prevent users from unknowingly submitting their credentials or sensitive data to an imposter, ensuring the authenticity of the cloud service and the security of the communication channel.

Network Isolation

To avoid security risks from cyber-attacks and data breach, the back-end servers and databases for Elevate Sky Services are disconnected from the internet by a virtual network (VNet). Thus, it is protected from direct access to sensitive data.

WAF (Web Application Firewall)

WAF (Web Application Firewall) minimizes risks by detecting and preventing attacks that exploit web application vulnerabilities, including SQL injection and cross-site scripting.

Malware Protection

Microsoft Defender is deployed in our application environment to protect the system from malware (malicious software), viruses and other threats. Even in the unlikely event that a threat is detected, appropriate measures can be taken to respond quickly and prevent information leaks.

6. Fleet Security

6.1 Elevate Sky Service: Policy Based Security Management

Elevate Sky Service offers a suite of cloud-based applications and services that enables remote monitoring and management of Toshiba MFPs. Using these tools, the administrator can create policies related to the security settings of the MFP and deploy those settings to the fleet via Toshiba cloud. As a best practice for Policy-based security management, a key objective is to take a comprehensive approach where security controls are defined, documented, and enforced through formal, centralized policies and procedures. This approach aligns with the foundational principles of NIST Special Publication (SP) 800-171, particularly within the Planning (PL) and Configuration Management (CM) families, which require organizations to establish a system security plan and configure systems according to defined policies. The value of this practice is that it provides consistency, scalability, and a clear framework for accountability across the entire organization. By formalizing security decisions, it reduces the risk of human error, ensures uniform security posture across all systems, and provides a clear audit trail for compliance, which is essential for the effective and auditable protection of Controlled Unclassified Information (CUI). Any violations to these MFP security policies are flagged and shared with the administrator via notifications.

Elevate Sky Service uses the same principles used by client PC's accessing secure data over a browser with HTTPS (server authentication and encryption). Data can only be sent from MFPs, and access is limited to Elevate Sky Service cloud servers with valid authentication certificates. To prevent server spoofing and to make sure data is transmitted to the correct server, these services feature 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.

Elevate Sky Service only handles the MFP operation status and device telemetry 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 these services do not handle actual document data, copy, fax, print and scan data can't be leaked. On request, a service technician can enable/disable these services 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. These services are also ISO 27017 certified. The key benefits of these services are their ability to help manage and maintain device security policies. MFPs enrolled in Sky Service 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 Elevate Sky Service 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 Elevate Sky Service. 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.

7. Certification & Regulatory Compliance

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).

ISO 27001/27017

Toshiba's Elevate Sky Services are ISO 27001 certified which means all the necessary security measures for information management and control are strictly followed. These controls and processes are further expanded to cloud services further certifying these services for ISO 27017, Code of Practice for Information Security Controls for Cloud Services. Toshiba's Elevate Sky Services are ISO 27001 certified which means all the necessary security measures for information

management and control are strictly followed. These controls and processes are further expanded to cloud services further certifying these services for ISO 27017, Code of Practice for Information Security Controls for Cloud Services.

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.

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. ***Administration 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

Toshiba MFP's adhere to the Japan Cryptographic Module Validation Program (JCMVP). JCMVP is a product certification system operated by the Information-technology Promotion Agency, Japan (IPA). Its purpose is to allow third-party entities to test cryptographic modules and verify that their algorithms are correctly implemented and their sensitive information is protected. 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 SSD with Wipe Function

The security SSD 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 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 of changing 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 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

Inv. Code: 22368 Toshiba MFP Security White Paper 12/25