KONICA MINOLTA

WHITEPAPER

KONICA MINOLTA i-SERIES EMBEDDED BITDEFENDER® ANTIVIRUS SECURITY

bizhub Bitdefender® PROTECTION

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Multifunction printers (MFPs) are often overlooked in cybersecurity strategies, despite being complex, network-connected devices that pose significant security risks. Unlike traditional copiers, modern MFPs feature operating systems, storage capabilities, and cloud connectivity, making them integral to business operations but vulnerable to cyberattacks. Frequently excluded from security assessments, they can operate with outdated firmware and default credentials, creating opportunities for attackers to exploit sensitive data and access networks. With the shift towards Zero Trust architectures, it is essential for organizations to include MFPs in their endpoint protection strategies, ensuring they receive the same level of security scrutiny as other critical devices like laptops and servers.

In today's landscape of escalating cyber threats and stringent data protection regulations, ensuring the security of your organization's devices—especially MFPs—is imperative. Konica Minolta's embedded Bitdefender® Antivirus application directly tackles this challenge by delivering robust, real-time security for MFPs. This product guide delves into how this integrated solution fortifies your print environment, enhances IT security compliance, and bolsters overall enterprise data protection strategies.

INTRODUCTION

Multifunction Printers (MFPs) serve as critical endpoint devices within enterprise networks, integrating an array of advanced functionalities beyond traditional printing. These devices operate on embedded operating systems and feature built-in web servers, supporting a wide range of network protocols, software integrations, and application programming interfaces (APIs) to facilitate seamless communication with external systems.

As a first line of defense, Konica Minolta offers **bizhub SECURE services** – these services protect confidential information that is processed through the MFP. As document distribution devices, MFPs are a shared data resource, located in public areas within the organization. They contain sensitive, confidential or private information and may be moved from secure to non-secure areas. The bizhub SECURE services safeguard against these threats as well as addressing security concerns for end of lease/life and hard disk drive/solid state drive storage risks. With bizhub SECURE, we address the risks with tools like storage media lock passwords, storage media encryption, automatic deletion of temporary image data, and data overwrite of electronic documents on a timed basis.

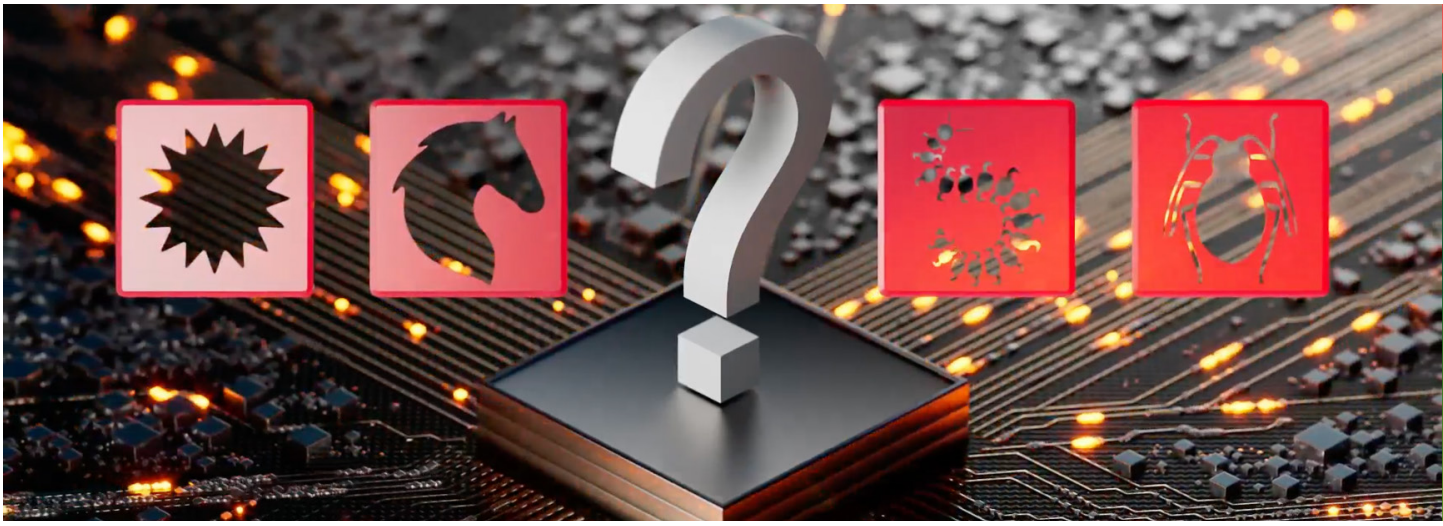
The very capabilities that enhance and expand MFP functionality also introduce potential security vulnerabilities. If not properly secured, MFPs can become entry points for cyber threats, exposing networks and enterprise systems to unauthorized access, data breaches, and service disruptions. As part of a comprehensive cybersecurity strategy, organizations must implement robust security measures to mitigate these risks, ensuring that MFPs remain a productive and secure component of the IT infrastructure.

In an era of increasing cyber threats and strict data protection requirements, securing your organization's devices—particularly multifunctional printers (MFPs)—is no longer optional. Konica Minolta's Bitdefender® Antivirus middleware addresses this challenge directly by providing robust, real-time security for your Konica Minolta bizhub MFPs. This security white paper explores how this integrated solution safeguards your print environment, improves IT security compliance, and supports overall enterprise data protection strategies.

Konica Minolta devices come equipped with standard security features, including a firmware check function that prevents unauthorized firmware versions from running at bootup. Since the introduction of the bizhub i-Series, Konica Minolta offers an additional antivirus solution aimed at detecting and preventing the spread of viruses and malware within the MFP and connected network.

This optional Bitdefender® antivirus module can be activated through an i-Option license.

Although enterprise print environments are often overlooked in comprehensive IT security strategies, they routinely manage sensitive information. Understanding the significance of securing these endpoints, Konica Minolta has partnered with Bitdefender® to provide an integrated antivirus solution—the embedded Bitdefender® Antivirus application—crafted to preemptively neutralize threats before they put critical data at risk.



WHY DOES YOUR BUSINESS NEED BITDEFENDER® ANTIVIRUS PROTECTION?

While bizhub SECURE provides essential protections by locking down your Konica Minolta MFP's settings—such as storage media encryption, password policies, and data auto-deletion—it primarily safeguards the device itself and data at rest.

However, in today's cybersecurity landscape, threats increasingly enter through data in motion—files being scanned, printed, emailed, or transferred via USB or cloud services. That's where embedded Bitdefender® Antivirus becomes critical.

Bitdefender® adds real-time threat detection and malware protection, scanning documents and data as they move through the MFP. This prevents infected files from being printed, emailed, or introduced into your network.

Together, bizhub SECURE and embedded Bitdefender® create a layered, defense-in-depth approach:

- bizhub SECURE protects the device's internal settings and stored data
- Bitdefender® protects against external threats by scanning all incoming and outgoing data in real time

For organizations seeking to maintain strong security standards, support Zero Trust principles, and reduce the risk of breaches through overlooked endpoints, both solutions are essential components of a modern, resilient print security strategy.

Threat Landscape in Printer Environments

Modern MFPs are complex devices that handle massive volumes of data—scanned, printed, and stored. As such, these devices can become attractive targets for cybercriminals:

- **Malware Infections:** Infected files sent for printing can spread malware through shared networks if not adequately screened.
- **Ransomware Attacks:** An unprotected printer can be an access point that spreads ransomware into the broader IT infrastructure.
- **Data Leakage:** Sensitive documents processed by MFPs can be exfiltrated if the device and stored data are not properly secured.

Embedded Bitdefender® Antivirus defends against these threats at the MFP level, thus strengthening the first line of defense in an organization's print ecosystem.

WHAT DOES THIS SOLUTION PROVIDE?

Bitdefender® Antivirus is an optional embedded application that integrates industry-leading anti-malware technology directly into Konica Minolta MFPs

The Bitdefender® Antivirus application provides virus and malware protection and detection throughout the various MFP modes and functions. The data is actively scanned for potential threats based on an up-to-date Pattern File database, rather than solely depending on a whitelisting strategy based on a file's digital signature. This provides an additional layer of security to our standard device security features.

- **Ensures Real-Time Protection:** Scans documents and files as they are processed by the printer.
- **Reduces Network Exposure:** Detects and quarantines malicious files at the device level, preventing threats from propagating across the network.
- **Simplifies IT Management:** Provides central management and reporting capabilities, making it easier for IT administrators to maintain security hygiene.

TECHNICAL ARCHITECTURE

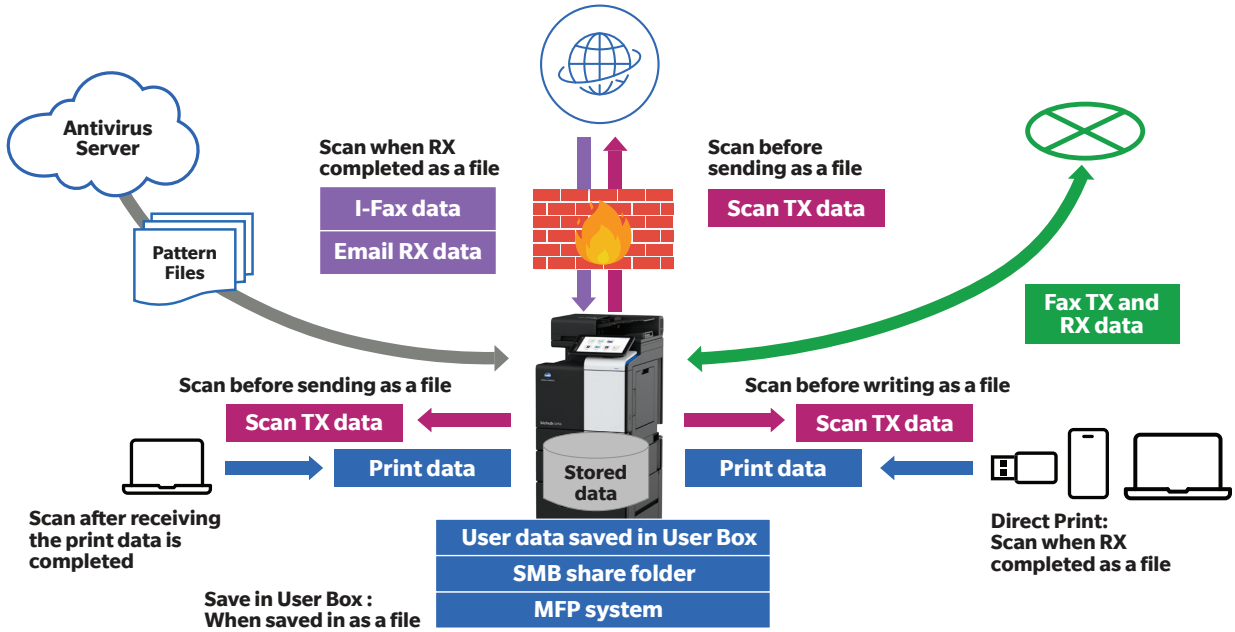
The embedded Bitdefender® Antivirus runs within the Konica Minolta MFP's system software, leveraging both the device's native security framework and Bitdefender's® proprietary scanning engine.

Key elements of the architecture include:

- **MFP Firmware Integration:** The Bitdefender® engine is embedded into the device firmware to enable near real-time scanning without relying on external servers.
- **On-Access Scanning Module:** Monitors all incoming and outgoing data, including print jobs, scanned documents, and firmware updates.
- **Dynamic Analysis and Signature Database:** Uses Bitdefender's® continuously updated malware signature database and behavior-based detection algorithms to identify known and zero-day threats.
- **Quarantine and Alert System:** Suspicious files are automatically deleted. Administrators are notified through the Email/SNMP trap and audit logs. Audit logs can be sent to SIEM/Endpoint Detection & Response protection software for central security management.

This tightly integrated approach yields minimal performance overhead and ensures that security features run transparently without disrupting daily print operations.

Embedded Bitdefender® Antivirus Architecture



1.

Real-Time Scan	Print data, Scan-TX data, i-Fax TX/RX data
Scheduled Scan	Storage Media (User Boxes, SMB)
Manual Scan	End User can invoke a virus scan manually at the MFP provided the MFP setting has been programmed for Manual Scan (vs. Real-time or Scheduled setting)

2.

Processing After Detection	• Suspicious files are automatically deleted. • Administrators are notified through the Email /SNMP trap and risk logs. Risk logs can be sent to SEIM, etc. for central security management monitoring.

Bitdefender® protects against the ongoing threats lurking around multifunctional printers and offers a Unified Threat Management approach to security. With this approach, a more comprehensive and all-encompassing security strategy is in place.

KEY FEATURES AND FUNCTIONALITIES

Real-Time Scanning*

- **Always-On Protection**: Evaluates all data streams passing through the MFP in real time. (**Recommended setting*)
- **Multi-Layer Detection**: Combines signature-based detection with dynamic analysis and machine learning models.

Quarantine Mechanism

- **Isolates Malicious Files**: Prevents infected files from spreading within the network.
- **Secure Storage**: Quarantined objects remain inaccessible to end users until the IT administrator or system determines the next action.

Automatic Updates

- **Live Signature Updates**: Ensures that the Bitdefender® engine is equipped with the latest threat signatures.
- **Cloud-Connected**: Connects to secure Bitdefender® update servers for real-time signature updates (subject to network policies).

Centralized Management

- **Remote Configuration**: Administrators can configure and apply policies across multiple devices simultaneously (when optional Shield Guard platform is enabled).

  Konica Minolta's Shield Guard platform is a cloud-based, device fleet security service that enables organizations to remotely monitor and manage the security status of one or more bizhub devices, making it possible to centrally manage security settings inclusive of the Bitdefender Antivirus application.

Minimal Performance Overhead

- **Optimized Scanning**: The scanning engine is specifically optimized for MFP environments to ensure minimal impact on print/scan performance.

DATA SCANNING CAN BE CARRIED OUT IN THREE DIFFERENT MODES

Real-Time Scanning

Perform the Virus Scan when sending or receiving data, to or from external devices such as Cloud, PC and External Memory. The virus scanning process protects incoming data by preventing the virus from entering the MFP, preventing password theft and the forwarding of the virus to other destinations.

- TX: Data is scanned for viruses before it is transmitted (scanning a file to an FTP site, SMB Folder, etc.)
- RX: When the reception of data is completed:
  - RX Print (Received Prints): MFP scans the file that was temporarily generated from the received data for viruses
  - RX Save (Saved Receptions): MFP scans the file that was generated from the received data for virus before it is saved into the storage location.

Manual Scan

Administrator can manually initiate the Virus Scan in Administrator mode.

- Target: SSD/MicroSD (User Box, SMB folders, MFP system)

Scheduled Scan

Schedule a scan to be run on a specific date or day.

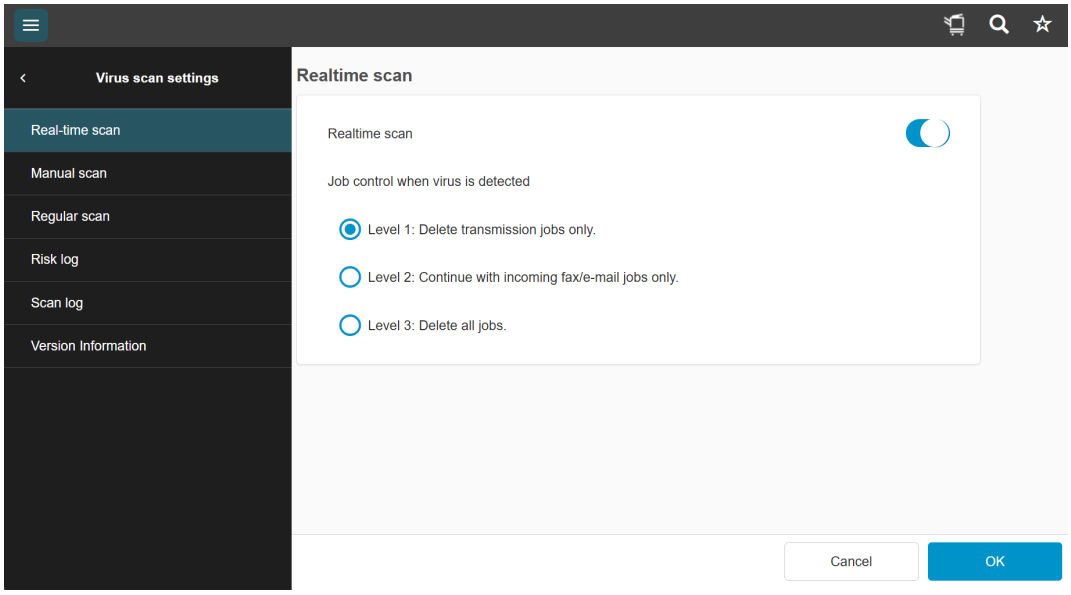
- Target: SSD/MicroSD (User Box, SMB folders, MFP system)

VIRUS SCAN NOTIFICATION SETTINGS AND LOGS

Virus Scan Setting (Administrative Mode)

Virus Scan configurations settings are controlled by the Administrator. They determine how a detected virus job will be treated after the detected virus is deleted. When the bizhub device sends or receives data (e.g. print data, Email receptions, data read from a USB flash drive, data written to a User Box), the Administrator can select the treatment options that best meet company security guidelines.

Real-Time Virus Scan Setting Screen



When Level 1 is selected, if a virus is detected, only the following job types are not executed:

- Scan to PC
- Scan to Cloud
- Scan to USB
- I-Fax TX
- IP Address Fax TX
- SMB Shared Folder

At level 2, if a virus is detected, the following jobs are not executed in addition to jobs identified at Level 1. Under these conditions, only the Fax RX or Email RX job is executed:

- PC Print (Normal Printing)
- PC Print (Save in User Box)
- Document Print from USB Flash Drive

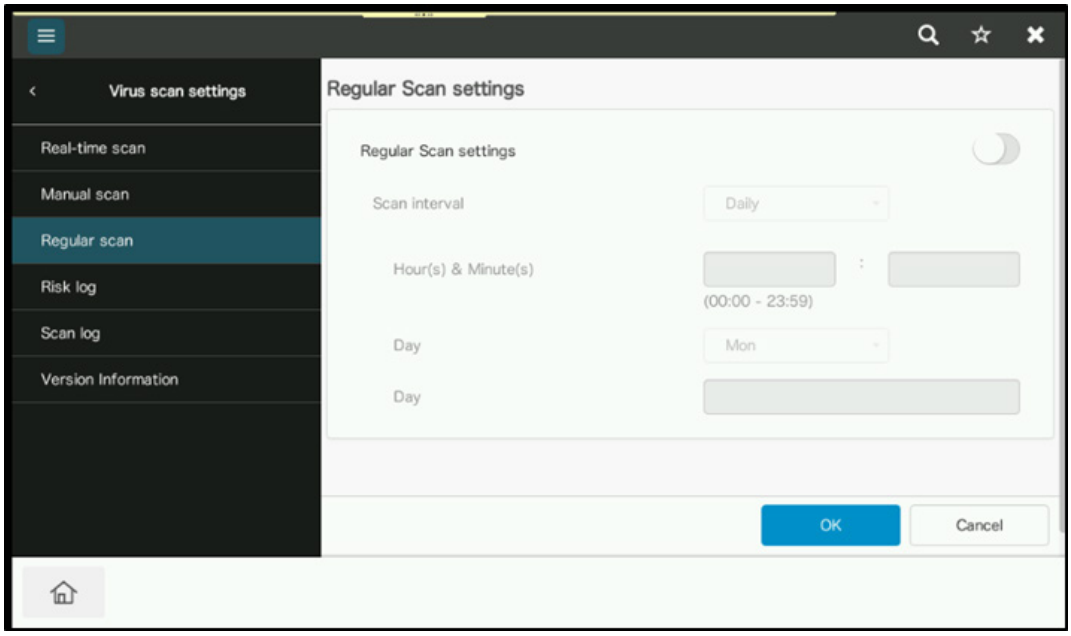
- Document Scan from USB Flash Drive
- Direct Print (Normal Printing)
- Direct Print (Save in User Box)
- Password Encrypted PDF User Box

At level 3, if a virus is detected, the following jobs are not executed in addition to jobs at Level 1 and Level 2.

- Email RX (Normal Printing)
- Email RX (Save in User Box)
- I-Fax RX
- IP Address Fax RX

Scheduled Scan Setting

The Scheduled Scan setting allows administrators to set the virus scan to check at specified times (days and times can be entered).



If a Scheduled Scan occurs when the MFP is in Power Saving Mode, the scheduled scan is suspended and will resume when MFP comes out of power saving mode

- Scan Interval can be set to Daily, Weekly, Monthly
  - If Daily is selected, the hour and minute intervals can be set
  - If Weekly is selected, Administrator can select the day of the preferred day of the week to perform the scan
  - If Monthly is selected, the Administrator can pick the date and scan time intervals on that particular date

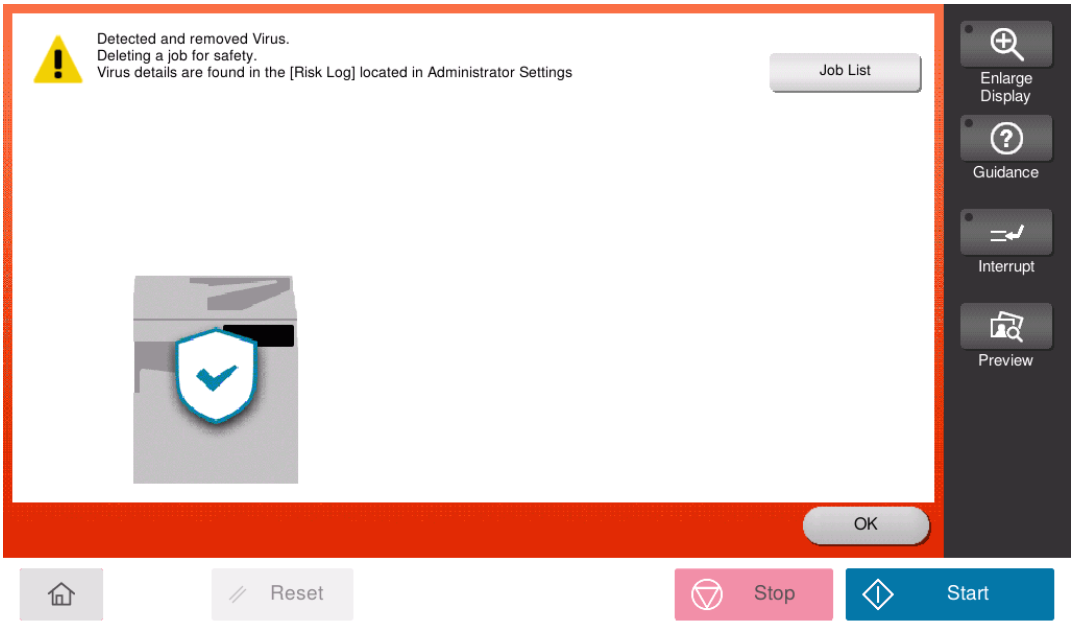
Manual Scan Setting

The Manual Scan setting enables End Users to invoke a virus scan manually.

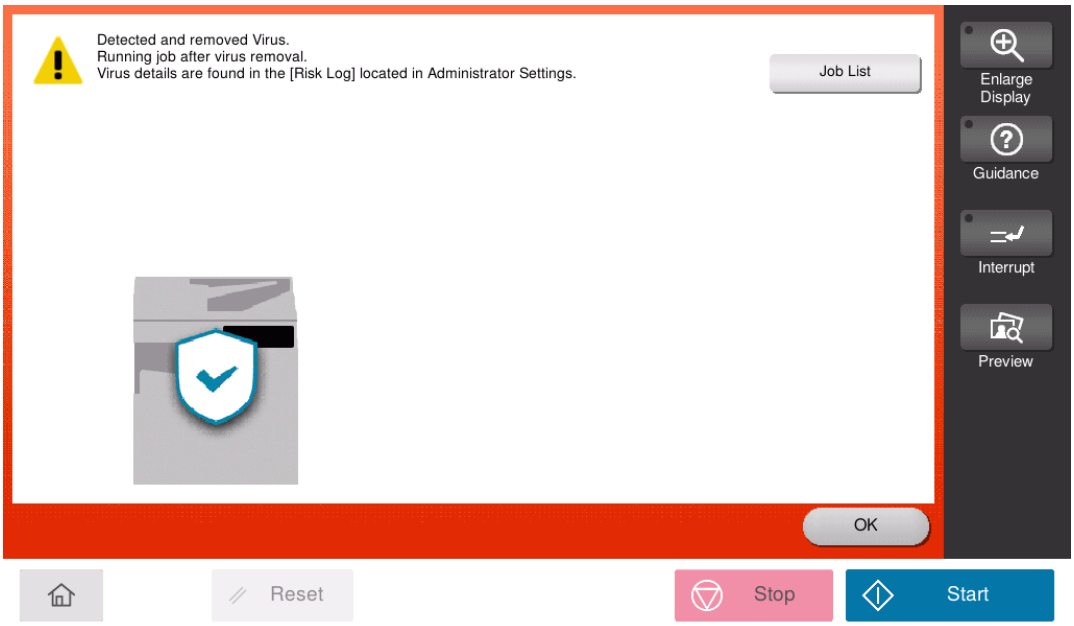
Screen Notifications

On screen notifications (MFP panel) will be clearly displayed when a virus has been detected (alert message shown depends on the selected treatment of the virus scan).

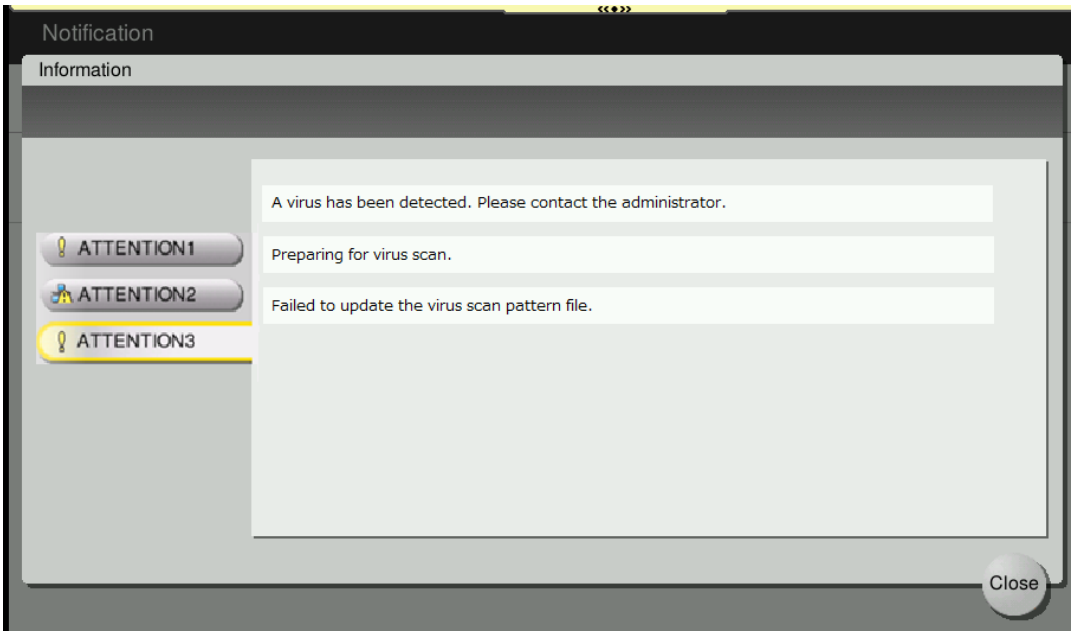
- An ALERT message is clearly displayed if an infected file is detected. The following message will appear if the selected setting is configured to delete the job:



- The following message will appear if the selected setting is to execute the job once the virus has been removed:



The screen shown below depicts the notification that will appear if the Virus Scan Pattern File update was unsuccessful. This warning will remain clearly displayed on the control panel until the update is successful. This is to ensure that the Administrator takes the necessary steps to download the latest Pattern File (reboot or wait 4 hours for next update cycle) so the bizhub engine is protected with the most recent version of the Virus Scan Pattern File.



A pseudo virus scan-related attention message is also displayed at the same time.

Set the "Update Failure of Pattern File" setting to ON.

- Access Administrator Mode
- Select Security
- Virus Scan Settings
- Version Information
- Update failure of Pattern File (listed under Alert Settings) to ON (default: ON)

Status Notifications

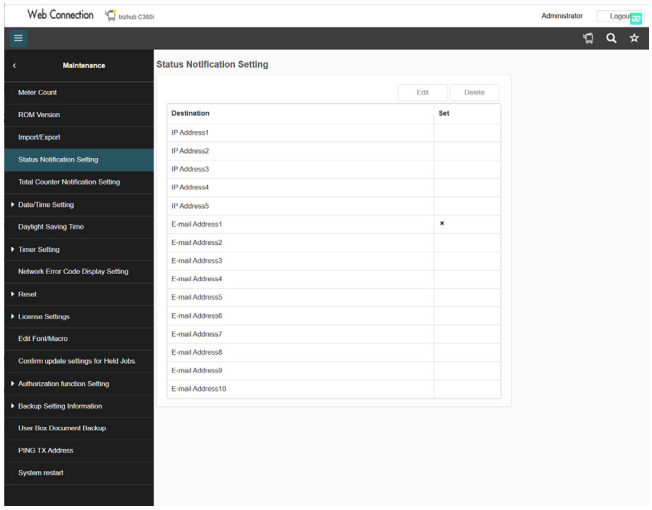
A virus detection notification via SNMP or Email can be set through the "Status Notification Setting".

The receipt of an SNMP or Email notification is an expedient means of alerting the Administrator that the Pattern File update was unsuccessful, which provides an opportunity for quicker action to safeguard against potential viruses.

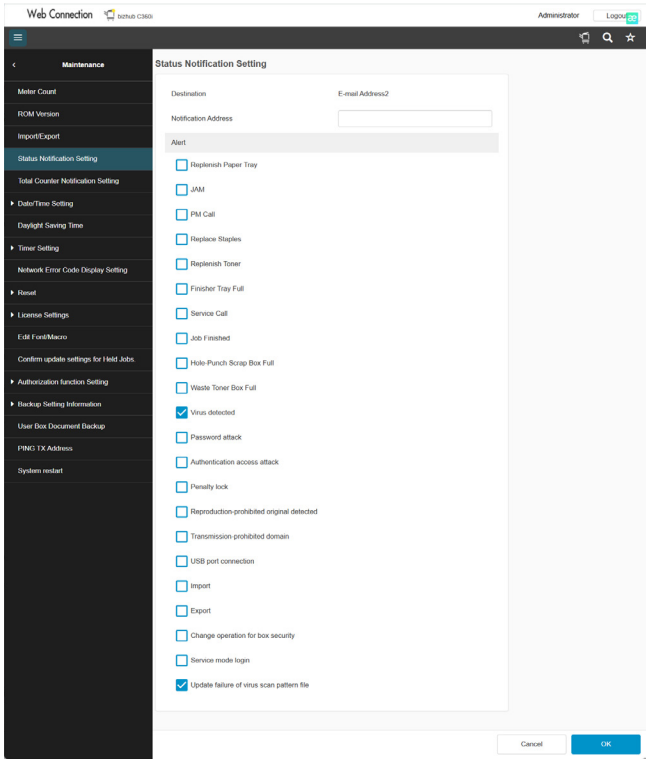
Set the "Status Notification Setting" settings:

- Access administrator Mode
- Select Maintenance
- Status Notification Setting
- Set [IP Address X] for SNMP notification or [Email Address X] for Email notification
- Set [Virus detected] to ON (default: OFF),
- Set [Update failure of virus scan Pattern File] to ON (default: OFF)

bizhub MFP Web Connection
Status Notification Setting Options



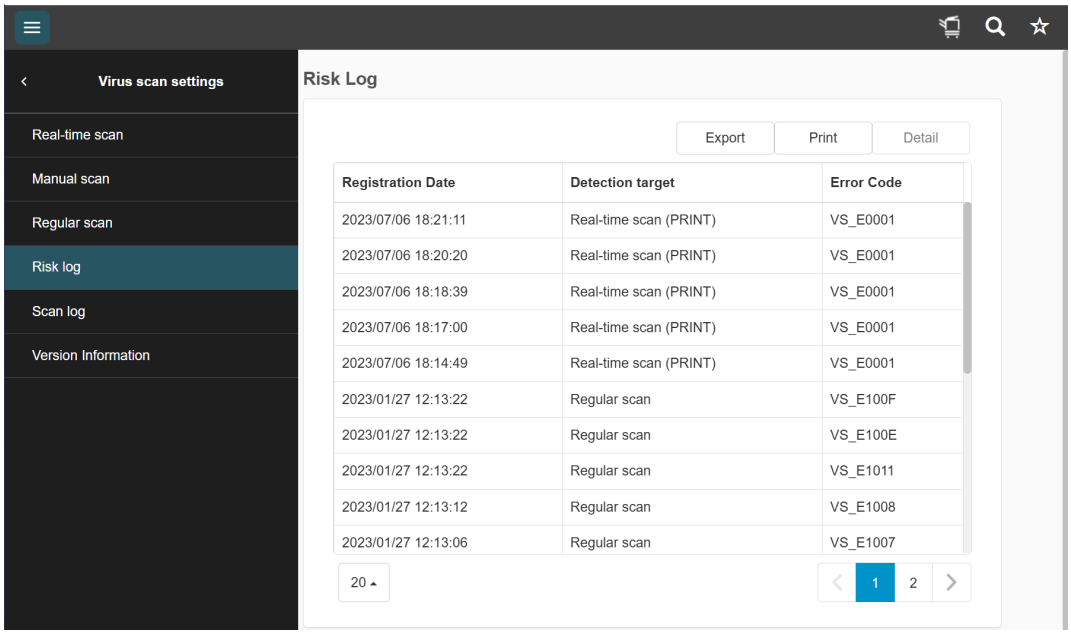
bizhub MFP Web Connection Status
Notification Alert Setting Options



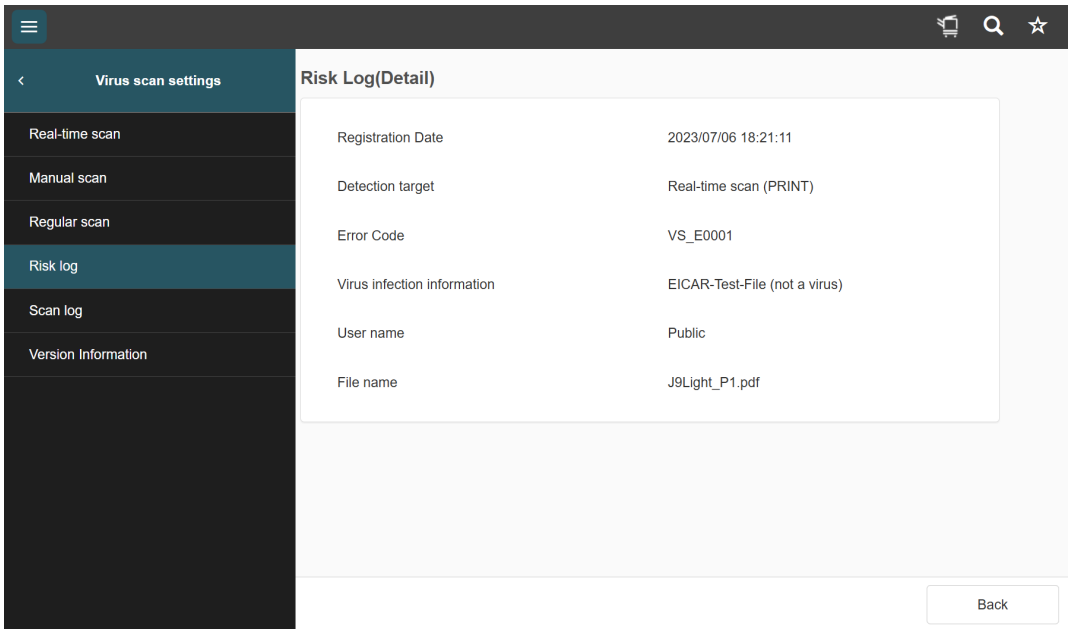
Risk Log

- Displays any detected risks with corresponding registration date and error code
- Lists each time a virus was detected (max. 100 events)

For additional information regarding the indicated error codes, please refer to Appendix C.

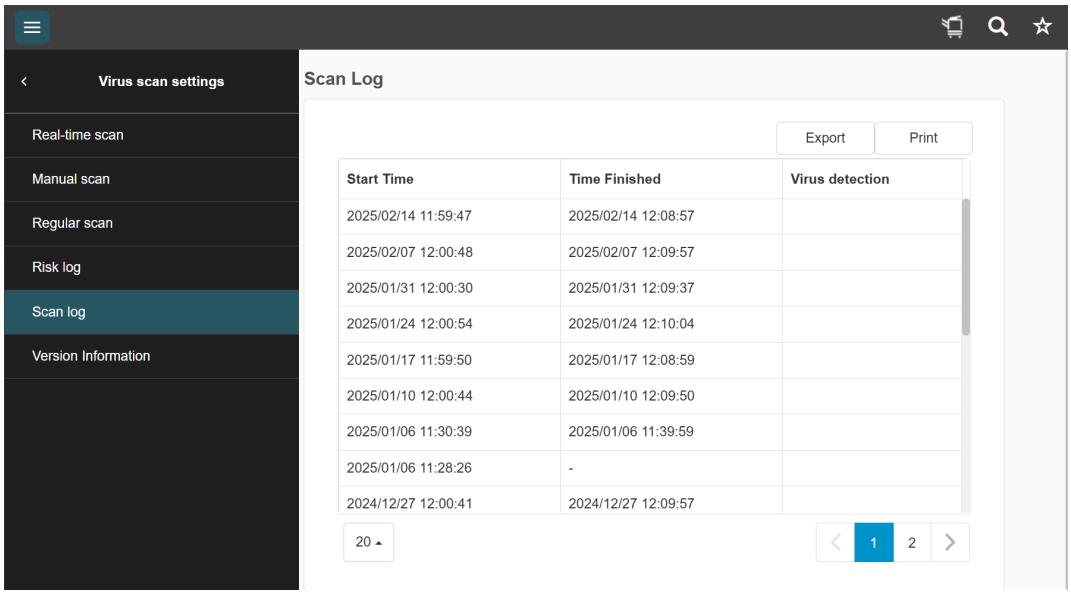


- **Risk Log (Detail)**: By selecting the event, more specifics will be provided. The additional information enables Administrators to identify a threat more easily.

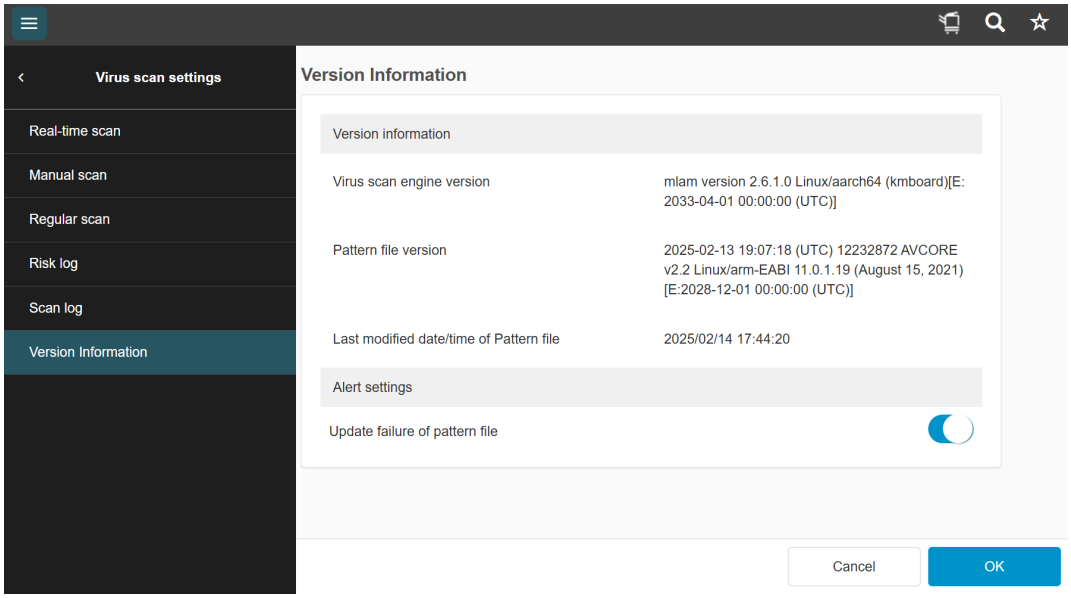


Scan Log

- Provides scan start time, scan finish time and information regarding the virus detected



- **Version Information** - Provides the Virus Scan engine version and Pattern File version (including the last modified date/time)



SYSTEM UPDATES

Pattern File

There are two options available to perform the Pattern File update:

- At Bootup of the MFP
- Every 4 hours after the MFP is started

A Pattern File serves as a database that enables Antivirus software to recognize viruses. The download process will only take place if a more recent Pattern File is accessible from the server. The Pattern File is safeguarded against tampering through a digital signature and will be updated solely after a successful integrity check of the new file.

Please note that you cannot change the frequency of the Pattern File updates. Bitdefender® will check for updates every 4 hours (provided the device is connected to the internet). In addition, it is not possible to turn off the Virus Pattern File update check every four hours.

Note: Upon activation of the Bitdefender® license, the initial Pattern File download will be approximately 250 MB. Subsequent updates will be in the form of differential updates, resulting in varying file sizes based on the circumstances.

Virus Scan Engine Software Application

- Will be updated during the MFP firmware upgrade procedure if applicable. This is not part of the Pattern File update.
- Only the Bitdefender® software version is updated when the MFP engine firmware is upgraded. Firmware upgrades do not include Pattern File updates.

Note: For optimum security, functionality and performance, bizhub engine firmware should always be kept up to date.

SERVER CONNECTIVITY

- Bitdefender® servers for Pattern Files are hosted in Japan.
- Pattern File delivery is backed by the Amazon Web Services CloudFront content delivery network in individual areas. Edge servers are in the following countries:
  - U.S.A. and Canada (origin server is in the U.S.A)
  - Europe and Israel
  - South Africa, Kenya and Middle East
  - Japan
  - Singapore
  - Korea, Taiwan, Hong Kong, Philippines
  - India

The MFP should access the server closest to its location. For example, in US, the MFP should communicate with the edge server of U.S.A. and Canada.

- The communication path with the server is encrypted using TLS.

The Pattern File update is encrypted using TLS. The TLS version depends on the Bitdefender® server's TLS version (the bizhub MFPs can support up to TLS v1.3).

- The distribution server information for download:
  - URLs for Pattern Files:
    - This is a license confirmation server (validates Bitdefender® license)
      URL: https://mlamsvc.cdn.miraclelinux.com/api/v1/get-license
    - This is the Pattern Files download server URL: https://mlam-mirror-prod.miraclelinux.net/arm-eabi32
- Port Number: 443

Note: The sole purpose of the distribution server is just to provide the virus definition file (Pattern File) to the bizhub MFP. No customer or user information is included in the communication between the server and MFP.

COMPLIANCE AND SECURITY STANDARDS

Organizations deploying **embedded Bitdefender® Antivirus** can more easily meet a variety of security regulations and industry standards, including:

- **GDPR (General Data Protection Regulation)**: Protect personal data and demonstrate appropriate technical security measures.
- **HIPAA (Health Insurance Portability and Accountability Act)**: Safeguard patient health information by preventing unauthorized access through the MFP.
- **PCI-DSS (Payment Card Industry Data Security Standard)**: Enhance protection of cardholder data in environments that process credit card information.

By integrating virus/malware scanning on the MFP itself, businesses can address security controls related to **endpoint protection** and **network access**.

DATA COLLECTION AND DATA PROTECTION

Embedded Bitdefender® Antivirus application collects the following information and protects against the data as shown below:

DATA TYPE	PURPOSE/ FUNCTION	STORAGE LOCATION	STORAGE PERIOD	CONFIDENTIALITY	DATA PROTECTION
Virus Scan Engine	Bitdefender® application residing on a bizhub MFP, that runs virus scans and updates the pattern files	SSD or MicroSD	Saved until Secure Erase is performed	Does not collect any personal information or other user data	Not Applicable
Pattern Files	Virus definition files for virus detection	SSD or MicroSD	Saved until license is no longer valid	Does not collect any personal information or other user data	Protected against manipulation by a digital signature and will only be updated once the integrity check for the new file is successful
Virus Scan Log	Saves the history of scheduled and manual virus scans	SSD or MicroSD	Saved until license is no longer valid	• Only Administrators can view/obtain the logs. • The logs do not contain personal information or other user data	Not Applicable
Virus Risk Log	Saves the history of virus detections	SSD or MicroSD	Saved until license is no longer valid	• Only Administrators can view/obtain the logs. • The logs do not contain personal information or other user data	Not Applicable
Virus Scan Temporary Data	Stores temporary data to perform virus scanning	SSD or MicroSD	Until virus scanning of all data is completed	There is no way to access or obtain data from outside (externally)	Not Applicable

Bitdefender® Logs

- **Scan Log:** All executed Manual Scans and Scheduled Scans are logged with start and end time -- whether or not a virus is detected. This log keeps track of when the operations are performed. If Real-Time Scan is enabled, a scan log of all activities is not logged (Real-Time Scan is continuously working as MFP jobs are executed).
- **Risk Log:** Logs the virus risk information when a virus is detected each time, Real-Time Scan, Manual Scan and Scheduled Scan are performed.
- **Audit Log:** Includes Risk Log data and all access /activities such as User Login and other MFP operations.

SYSTEM AND CONFIGURATION REQUIREMENTS

- Requires Bitdefender® Antivirus license.
- The bizhub engine storage type must be one of the following:
  - 256GB SSD
  - 16GB MicroSD
  - 1TB SSD (when optional memory is installed)
- The MFP must be able to connect to the internet.
- Depending on your network environment, the following proxy settings are required for downloading Pattern Files:

Utility → **Administrator** → **Network** → **Machine Update Settings** → **HTTP Proxy Settings**

Note: The Bitdefender® Antivirus license module can operate without internet access following the initial connection. However, without ongoing connectivity, updates cannot be downloaded and applied. Consequently, the security efficacy of the Bitdefender® Antivirus module may diminish.

For example, if a USB drive contains a file infected by a virus that was identified months after the last Pattern File *update, the system may be unable to detect, remove and halt the spread of this virus.*

CONCLUSION

Konica Minolta's embedded Bitdefender® Antivirus application is a critical component for organizations aiming to bolster their print security infrastructure. By integrating industry-leading virus and malware detection and prevention capabilities directly into Konica Minolta MFPs, this solution helps protect sensitive data, simplifies compliance efforts, and provides peace of mind for IT administrators.

As cyber threats continue to evolve, ensuring every endpoint—including MFPs—remains secure is essential. Through mutual development and collaboration, Konica Minolta and Bitdefender® offer a sophisticated and user-centric cybersecurity solution designed to address the stringent security requirements of modern enterprises.

For Additional Information

To learn more about Konica Minolta's embedded Bitdefender® Antivirus application, including compatible models, licenses and best practices for deployment, please visit Konica Minolta's official website or contact your local Konica Minolta sales representative.

APPENDIX A

REAL-TIME VS SCHEDULED/MANUAL SCANNING ITEMIZED LIST AND PROCESSING AFTER DETECTION

REAL-TIME VS SCHEDULED/MANUAL SCANNING ITEMIZED LIST AND PROCESSING AFTER DETECTION

TYPE	OPERATOR	FUNCTION	INPUT/ OUTPUT	SCAN TIMING	SCAN TARGET DATA	PROCESSING AFTER DETECTION		
						LEVEL 1	LEVEL 2	LEVEL 3
User Function	User	PC Printing (Normal printing)	Input	Scan after receiving all data	Spool data	Print	Delete Job	Delete Job
		PC Printing (Box data storage)	Input	Scan after receiving all data	Spool data	Save to Box	Delete Job	Delete Job
		Scan to PC	Output	Scan just before sending	General-purpose file in storage before sending	Delete Job	Delete Job	Delete Job
		Scan to Cloud	Output	Scan just before sending	General-purpose file in storage before sending	Delete Job	Delete Job	Delete Job
		Scan to USB	Output	Scan just before sending	General-purpose file in storage before sending	Delete Job	Delete Job	Delete Job
		Email Receive (Normal printing)	Input	Scan after receiving all data	Spool data	Print	Print	Delete Job
		Email Receive (Box data storage)	Input	Scan after receiving all data	Spool data	Save to Box	Save to Box	Delete Job
		I-Fax Receive	Input	Scan after receiving all data	Spool data	Print	Print	Delete Job
		IP Address Fax Receive	Input	Scan after receiving all data	Spool data	Print	Print	Delete Job
		I-Fax Send	Output	Scan just before sending	General-purpose file in storage before sending	Delete Job	Delete Job	Delete Job
		IP Address Fax Send	Output	Scan just before sending	General-purpose file in storage before sending	Delete Job	Delete Job	Delete Job
		USB to Print	Input	Scan after receiving all data	Spool data	Print	Delete Job	Delete Job

TYPE	OPERATOR	FUNCTION	INPUT/ OUTPUT	SCAN TIMING	SCAN TARGET DATA	PROCESSING AFTER DETECTION		
						LEVEL 1	LEVEL 2	LEVEL 3
User Function	User	USB to Box	Input	Scan after receiving all data	Spool data	Save to Box	Delete Job	Delete Job
		Direct Printing (Normal printing)	Input	Scan after receiving all data	Spool data	Print	Delete Job	Delete Job
		Direct Printing (Box data storage)	Input	Scan after receiving all data	Spool data	Save to Box	Delete Job	Delete Job
		SMB Shared Folder	Input/Output	• When files are added to the SMB folder • When the file is opened	General-purpose file in storage before sending	Input: Delete Output: Delete	Input: Delete Output: Delete	Input: Delete Output: Delete
		Browser	Input	Scheduled scan	Content data / Download file	Warnings only appear in the risk log	Warnings only appear in the risk log	Warnings only appear in the risk log
		Encrypted PDF Box	Input	Scan after receiving is complete	PDF file	Save to Box	Delete Job	Delete Job
	Admin	Import Data	Input	Scan after receiving is complete	XML/CSV data	Delete (Import failure)	Delete (Import failure)	Delete (Import failure)
		Application (IWS/ MarketPlace App)	Input	Scheduled scan	Application data	Warnings only appear in the risk log	Warnings only appear in the risk log	Warnings only appear in the risk log
		Application (OpenAPI)	Input	Scan after receiving is complete	Application data	Delete (Installation failure)	Delete (Installation failure)	Delete (Installation failure)
		Device Certificate	Input	Scan on install	Certificate	Delete (Import failure)	Delete (Import failure)	Delete (Import failure)
		S/MIME Certificate	Input	Scan on install	Certificate	Delete (Import failure)	Delete (Import failure)	Delete (Import failure)
		Printer Font Data	Input	Scan on install	Font data	Delete (Import failure)	Delete (Import failure)	Delete (Import failure)

TYPE	OPERATOR	FUNCTION	INPUT/ OUTPUT	SCAN TIMING	SCAN TARGET DATA	PROCESSING AFTER DETECTION		
						LEVEL 1	LEVEL 2	LEVEL 3
Service Function	Service	Voice Data	Input	Scheduled scan	Voice data	Warnings only appear in the risk log	Warnings only appear in the risk log	Warnings only appear in the risk log
		Movie Data	Input	Scheduled scan	Movie data	Warnings only appear in the risk log	Warnings only appear in the risk log	Warnings only appear in the risk log
		Searchable PDF Dictionary Data	Input	Scheduled scan	Searchable PDF dictionary data	Warnings only appear in the risk log	Warnings only appear in the risk log	Warnings only appear in the risk log
		PDF/A Font Data	Input	Scheduled scan	PDF/A font data	Warnings only appear in the risk log	Warnings only appear in the risk log	Warnings only appear in the risk log
		Panel Sound Data	Input	Scheduled scan	Panel sound data	Warnings only appear in the risk log	Warnings only appear in the risk log	Warnings only appear in the risk log
		OEM Name Customization Data	Input	Scheduled scan	OEM name customization data	Warnings only appear in the risk log	Warnings only appear in the risk log	Warnings only appear in the risk log
		Authentication Customization Data	Input	Scan on install	Authentication customization data	Delete (import failure)	Delete (import failure)	Delete (import failure)
		Loadable Driver	Input	Scheduled scan	Loadable driver	Warnings only appear in the risk log	Warnings only appear in the risk log	Warnings only appear in the risk log

APPENDIX B

RISK LOG ERROR CODE LIST

RISK LOG ERROR CODE LIST

	ERROR CODE	FUNCTION	REAL-TIME SCAN	SCHEDULED SCAN
Real-Time Scan	VS_E0001	PC Printing (Normal printing)	✓	-
		PC Printing (Box data storage)	✓	-
		Email Receive (Normal printing)	✓	-
		Email Receive (Box data storage)	✓	-
		I-Fax Receive	✓	-
		IP Address Fax Receive	✓	-
		USB to Print	✓	-
		USB to Box	✓	-
		Direct Printing (Normal printing)	✓	-
		Direct Printing (Box data storage)	✓	-
		Scan to PC	✓	-
		Scan to Cloud	✓	-
		Scan to USB	✓	-
		I-Fax Send	✓	-
		IP Address Fax Send	✓	-
		Printer Font Data	✓	-
	VS_E0002	SMB Shared Folder	✓	-
	Screen customization data: VS_E0003 Certificate (temporary import area): VS_E0003 Browser: VS_E0003 Other than those above: VS_E0001	Import Data	✓	-
	VS_E0004	Application (OpenAPI)	✓	-
	VS_E1007	Device Certificate	✓	-
	VS_E1008	S/MIME Certificate	✓	-
Scheduled Scan	VS_E1001	SMB Shared Folder	-	✓
	VS_E1002	Browser	-	✓
	VS_E1003	Encrypted PDF Box	-	✓
	VS_E1005	Application (IWS)	-	✓

	ERROR CODE	FUNCTION	REAL-TIME SCAN	SCHEDULED SCAN
Scheduled Scan	VS_E1006	Application (OpenAPI)	-	✓
	VS_E1007	Device Certificate	-	✓
	VS_E1008	S/MIME Certificate	-	✓
	VS_E1011	Font Data (Emperon)	-	✓
Service Function	VS_E1009	Voice Data	-	✓
	VS_E100A	Movie Data	-	✓
	VS_E100B	Searchable PDF Dictionary Data	-	✓
	VS_E100C	PDF/A Font Data	-	✓
	VS_E100D	Panel Sound Data	-	✓
	VS_E100E	OEM Name Customization Data	-	✓
	Real-Time Scan: VS_E0005 Scheduled Scan: VS_E100F	Authentication Customization Data	✓	✓
	VS_E1010	Loadable Driver	-	✓

This Risk Log is an individual log with a maximum 100-event limitation. When the number of risk log events reaches 101, the oldest event will be overwritten.

The information saved in the Risk Log is also saved in the Audit Log. The Bitdefender Antivirus Audit Log data storage is based on storage limitation (vs. time period limitation). The maximum storage is 112MB for all log type files (audit/credit/job logs). When the maximum storage is reached, new logs will overwrite old log files if the "Overwrite" permission is enabled in MFP Admin Settings.

Note: The rule is first in first out for deletion.

APPENDIX C

SHIELD GUARD CENTRALIZED MANAGEMENT

SHIELD GUARD CENTRALIZED MANAGEMENT

Shield Guard security settings are **only supported** on i-Series devices that meet the following criteria:

- The embedded Bitdefender Antivirus (LK-116) Scan i-Option is supported
- The embedded Bitdefender Antivirus (LK-116) Virus Scan i-Option has been installed

The following **table** lists the **security** settings as well as descriptions of the device's corresponding bizhub SECURE Ultimate Security settings and how Shield Guard assesses those settings.

SHIELD GUARD SETTING	FUNCTIONALITY AT THE DEVICE	SHIELD GUARD ASSESSMENT	AUTOMATIC REMEDIATION?
Virus Scan License	Devices have no corresponding setting. Instead, if the LK-116 Virus Scan i-Option is licensed on the device, then security settings are available on the device and Shield Guard can monitor the settings.	Monitors the LK-116 i-Option on the device. If the LK-116 i-Option has been licensed (installed and enabled) on the device, Shield Guard assesses the setting as Secure.	N
Log Pattern File Version	Devices have no corresponding setting. Instead, the LK-116 Virus Scan i- Option installs a pattern file (a database of virus information) onto the device to identify and eradicate viruses.	Polls the device for the version of the **antivirus pattern file**. If a change is detected, the Shield Guard agent sends the updated value to the log in the Shield Guard portal.	N
Pattern File Updates	Displays an alert on the MFP panel when the virus scan pattern file fails to update.	Monitors the "Update failure of pattern file" setting at the device. If enabled, Shield Guard assesses the setting as Secure.	Y
Real-Time Scanning	Enables admins to enable/disable the Real-Time Scanning option on the device. This option scans all files sent, scanned, or accessed by the device, as well as files located on USB drives.	Monitors the Real-Time Scanning setting on the device. If enabled, the **Job Control Levels** appear where you can specify how you want the device to respond when the LK-116 kit detects a virus. If the configuration at the device matches the Shield Guard policy setting, Shield Guard assesses the setting as Secure.	Y
Regular Scan	Enables admins to enable/disable the Regular Scan option on the device. This option performs a full virus scan of the device at a userspecified interval. **Note:** Enabling this option on the device can impact device performance, so we recommend you schedule the scan to occur at off-peak hours.	Monitors the Regular Scan setting on the device. If the configuration at the device matches the Shield Guard policy setting, Shield Guard assesses the setting as Secure. **Note:** When scheduling a regular scan to occur monthly, if the day of the month you select exceeds the number of days in a given month, the scan will occur on the final day of that month. For example, if you select 31, then in April, the scan will occur on April 30 (the last day in April). Note that, for scheduling purposes, devices always consider February to have 28 days.	Y

Note: If none of the above scanning options are enabled on the device, then:

- No virus scanning occurs
- No check of the Pattern File version occurs
- No update of the Pattern File occurs, so no log indicating a change to the Pattern File will be generated

The Antivirus Pattern File

The embedded Bitdefender Antivirus (LK-116) Scan i-Option includes an antivirus Pattern File. This file is a database of virus information that is constantly updated to include the latest antivirus information from around the globe. As part of the installation, the antivirus Pattern File is installed onto the device.

In order for the embedded Bitdefender Antivirus (LK-116) Scan i-Option to maintain the latest version of the Pattern File on a device, note the following:

- The device must be connected to the internet
- Virus scanning must occur. That is, at least one of the scanning options (Real-Time Scanning or Regular Scan) must be enabled on the device

A virus scan triggers a check of the Pattern File. If an updated version is available, it is downloaded to the device and the scan proceeds using the existing Pattern File. If no new version is available, the scan proceeds using the existing Pattern File.

Monitoring Changes to the Antivirus Pattern File

Shield Guard can monitor changes to the antivirus Pattern File on each device assigned to a security policy. If the following is true, then Shield Guard will create a log for every change detected in the antivirus Pattern File on a device:

- The device supports the embedded Bitdefender Antivirus (LK-116) Scan i-Option
- The embedded Bitdefender Antivirus (LK-116) Scan i-Option has completed its initial installation. If Shield Guard assesses the device before the installation is complete, a log will be generated showing a device value of "Pending"
- The Log Pattern File Version setting is enabled in the policy
- At least one of the virus scanning options (Real-Time Scanning or Regular Scan) is enabled on the device

BITDEFENDER ANTIVIRUS bizhub COMPATIBILITY

bizhub Engines Compatible with Bitdefender® Antivirus License

- C750i
- C650i/C550i/C450i
- C360i/C300i/C250i

- C751i
- C651i/C551i/C451i
- C361i/C301i/C251i

- 751i
- 651i/551i/451i
- 361i/301i

- 950i/850i
- 750i
- 650i/550i/450i
- 360i/300i

- C4751i/C4051i/C3351i
- C4050i/C3350i

- C3321i
- C3320i

- 4751i/4051i
- 4750i/4050i

Disclaimer: This document is provided for informational purposes only. Product specifications, capabilities, and compatibility may vary based on region and MFP model. Always consult official Konica Minolta documentation for the most accurate and up-to-date information.

For complete information on Konica Minolta products and solutions, please visit: CountOnKonicaMinolta.com

KONICA MINOLTA

KONICA MINOLTA BUSINESS SOLUTIONS U.S.A., INC.
100 Williams Drive, Ramsey, New Jersey 07446

CountOnKonicaMinolta.com

Item#: BitdefenderWhitePaper
12/25-PD