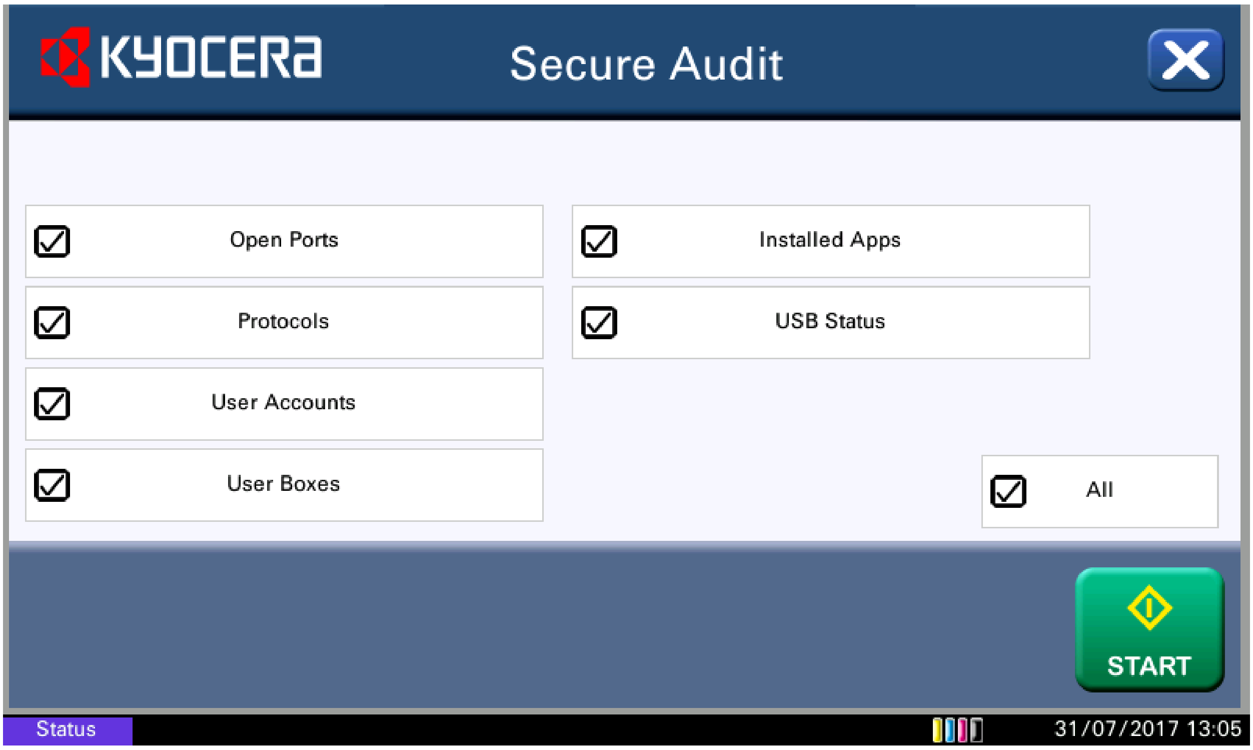
SETUP AND
OPERATION GUIDE

KYOCERA SecureAudit

Version 1.0

KYOCERA
Document Solutions

1.0 KYOCERA SecureAudit Usage Guide



Secure Audit

☑ Open Ports

☑ Installed Apps

☑ Protocols

☑ USB Status

☑ User Accounts

☑ User Boxes

☑ All

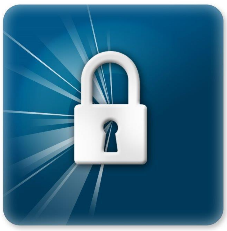
START

Status

31/07/2017 13:05

1.1 Starting the Application

1. After KYOCERA SecureAudit is activated successfully, it can be executed from the main Application screen (opened by pressing the ‘Home’ key on the control panel).



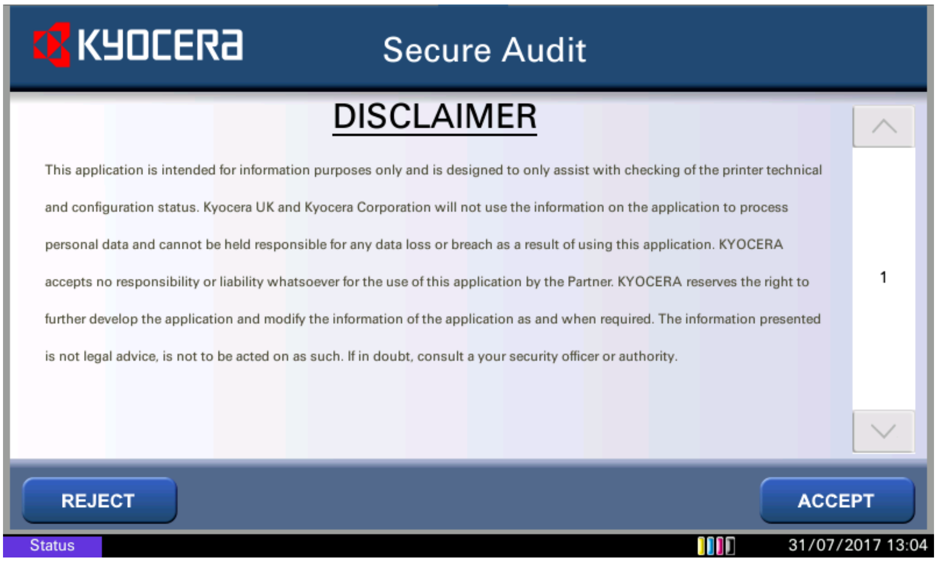
1.2 **The Purpose of KYOCERA Secure Audit**

2. The application is designed to scan the MFP for potential vulnerabilities and alert the user via a printed report and an electronic file. The file can be exported to a USB storage device attached to the device.
3. The MFP is checked for:
    - **Device information:** Model Name, MAC address, IP address, firmware level.
    - **Open Ports:** All open ports on the device.
    - **Protocols:** All currently enabled protocols on the device.
    - **User Accounts:** All user accounts registered on the device are represented by a figure; those accounts with administrator level access are listed.
    - **User Boxes:** All electronic user 'Job Boxes' are listed.
    - **Installed Applications:** All current HyPAS applications installed on the device are listed together with their status (Active/Inactive).
    - **Optional Functions:** Any of the optional functions that are available to the device are listed. E.g. Data security Kit, Wireless, NFC option.
    - **USB Status:** Whether the USB host is active and available.

4. With this information, a network administrator or consultant can assess the MFP for potential data risk and be more informed about the security status of the MFP.

1.3 **Running the Application**

5. To use the application you must be logged in as an administrator.
6. Upon starting KYOCERA SecureAudit a disclaimer will be displayed:

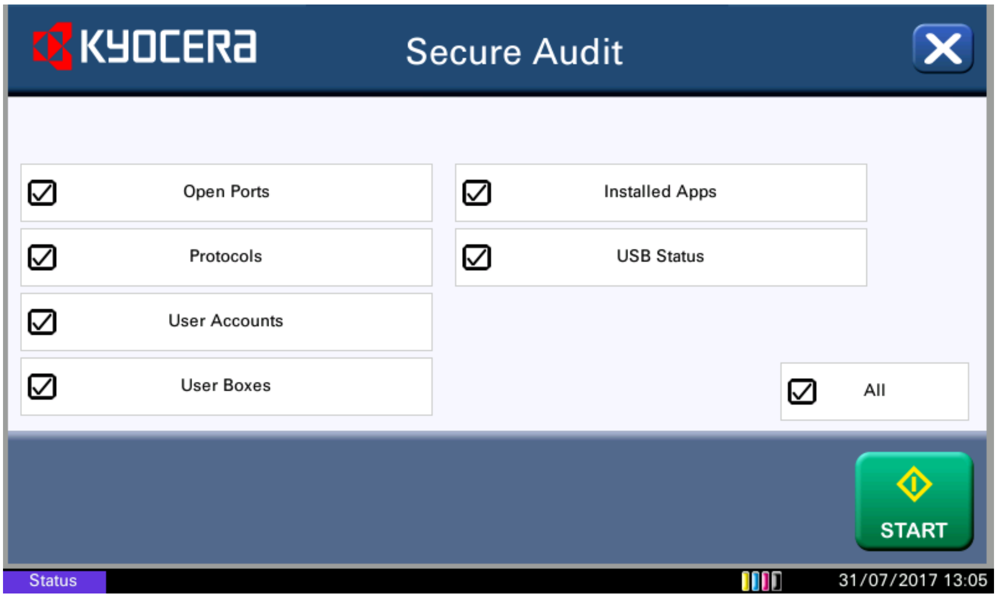


DISCLAIMER

This application is intended for information purposes only and is designed to only assist with checking of the printer technical and configuration status. Kyocera UK and Kyocera Corporation will not use the information on the application to process personal data and cannot be held responsible for any data loss or breach as a result of using this application. KYOCERA accepts no responsibility or liability whatsoever for the use of this application by the Partner. KYOCERA reserves the right to further develop the application and modify the information of the application as and when required. The information presented is not legal advice, is not to be acted on as such. If in doubt, consult a your security officer or authority.

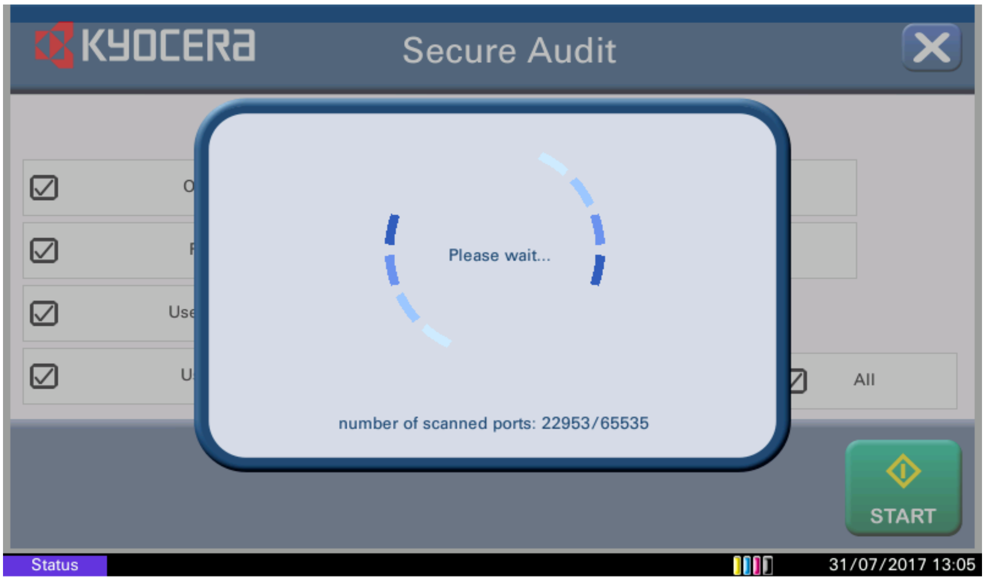
7. Selecting 'Reject' will close the application. 'Accept' will advance to the next screen.

8. On opening the main screen will display:



☑ Open Ports
☑ Protocols
☑ User Accounts
☑ User Boxes
☑ Installed Apps
☑ USB Status
☑ All

9. You can select individual areas to be checked, or press the ‘ALL’ button to select all options.
10. Pressing ‘Start’ will allow the application to start the scanning process.

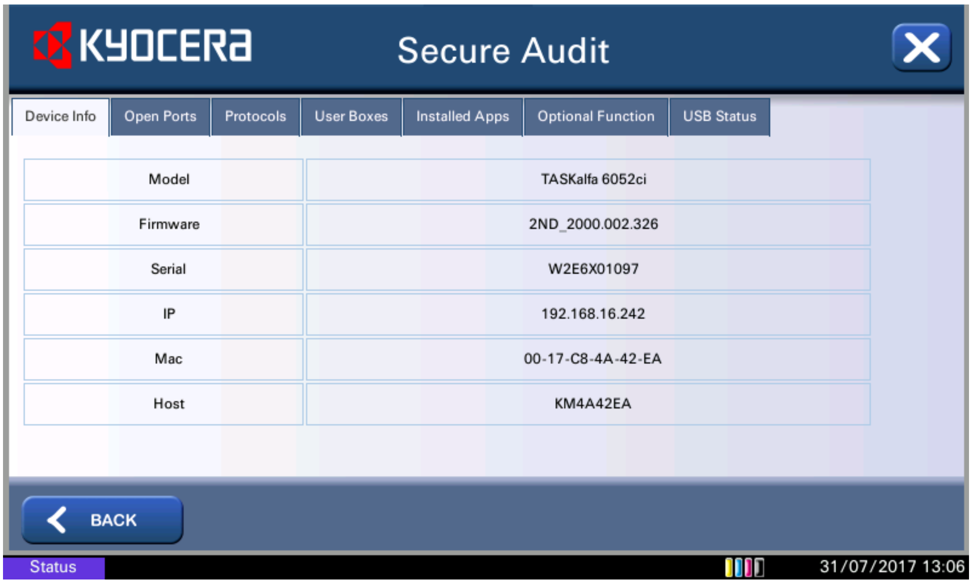


Please wait...

number of scanned ports: 22953/65535

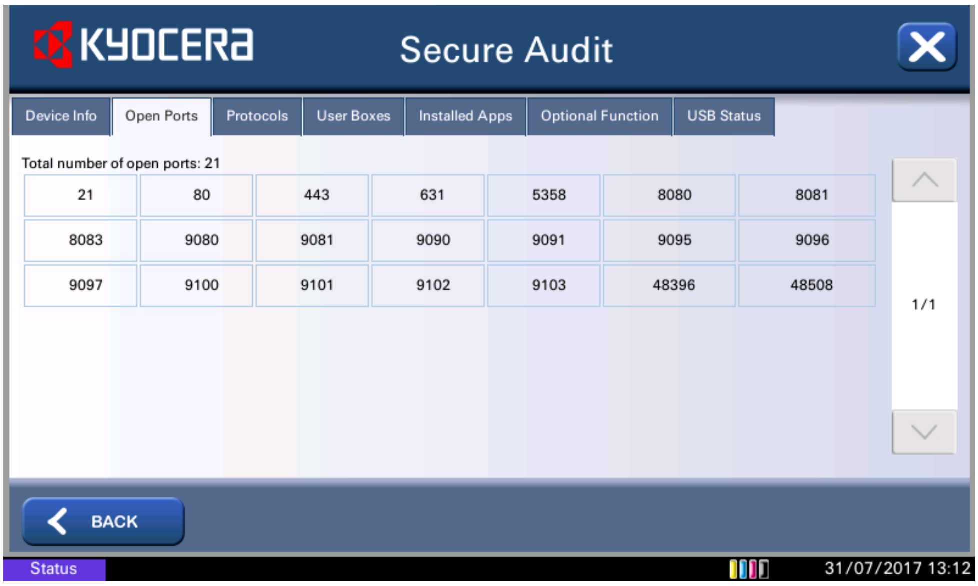
11. If the ‘Ports’ check is selected, the screen will display the progress of the ports it has queried. The process will take around 90 – 120 seconds depending on the information stored on the device. If Ports are not selected the process will be substantially faster.

12. Once complete the device will automatically print a report and display a summary screen.



Model	TASKalfa 6052ci
Firmware	2ND_2000.002.326
Serial	W2E6X01097
IP	192.168.16.242
Mac	00-17-C8-4A-42-EA
Host	KM4A42EA

13. Pressing the different tabbed sections will display information about that area.

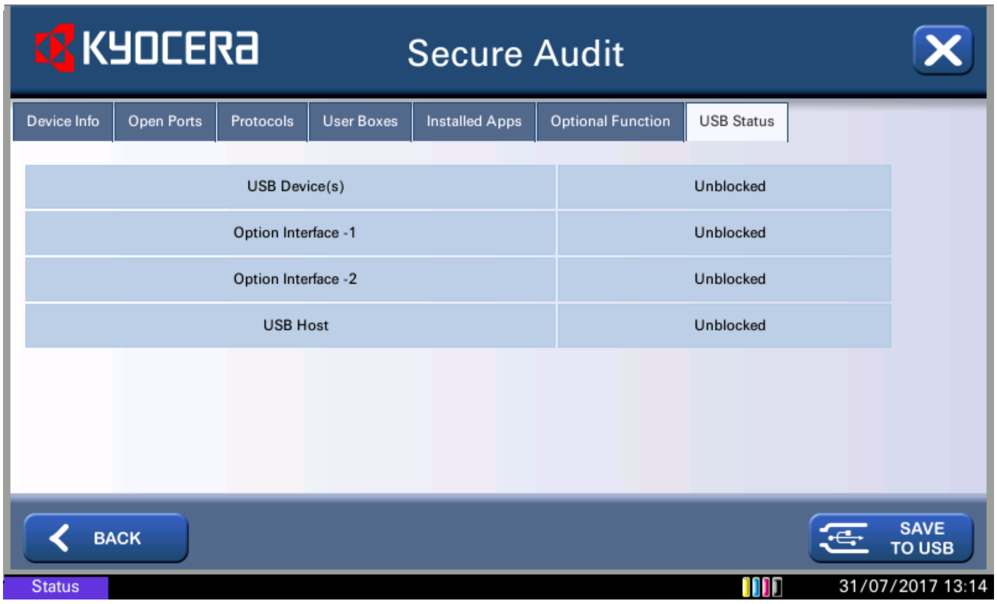


Total number of open ports: 21

21	80	443	631	5358	8080	8081
8083	9080	9081	9090	9091	9095	9096
9097	9100	9101	9102	9103	48396	48508

14. A complete list of ports and protocols is contained in the appendix ‘Security Guide’.
15. Pressing ‘Back’ will reset the machine back to the initial starting screen where a check can be performed again.

16. When a USB storage device is inserted, the option to export the data will be visible on the screen. If the USB host interface is disabled the option will NOT appear.



USB Device(s)	Unblocked
Option Interface -1	Unblocked
Option Interface -2	Unblocked
USB Host	Unblocked

17. The file will be exported in a JSON format to enable import into other software.

1.4 **Security Guide**

18. Data Security Kit: The information below relates to the optional Data Security Kit (DSK) and is an option for KYOCERA devices. Please contact your authorised reseller for information and pricing.

HDD/SSD Data Protection
Sensitive or confidential information can be stored on the device HDD or SSD and extra protection can be implemented which conforms to the Common Criteria Certification (ISO 15408). These functions include:

HDD/SSD Encryption (Option)
HDD/SSD encryption function is a security function that encrypts documents, user settings and device information that is stored on the HDD or SSD. Encryption is applied to the data with using the 128-bit and 256-bit AES (Advanced Encryption Standard: FIPS PUB 197) algorithm. If the HDD or SSD is removed from the MFP, the sensitive or confidential information stored in the HDD or SSD would not be accessible.

HDD Overwrite-Erase (Option)
A security function that disables a third party's ability to read a variety of data such as user settings, device information and image data stored on the HDD.
When printing or copying scanned data is temporarily stored in the HDD and then output. Users can also register various settings such as scan destinations and email addresses which are stored on the device. This information still remains on the HDD until the data is overwritten with other data, even after the output or deletion of the data by users. There is a possibility that the data remaining on the HDD can be restored using special tools and utilities, leading to leakage of information.
The HDD overwrite-erase function is configured to overwrite the actual data area of the output or deleted data with random meaningless data so that the actual data cannot be restored. The overwrite-erase process is performed automatically so no manual operation is required from the user. HDD data is immediately overwritten even when respective jobs are cancelled during operation or directly after entire job has finished.

Three overwrite-erase methods are available and subject to model.

One-time Overwrite-Erase
Unnecessary data area is overwritten once with null data, making the data to be difficult to be restored or recovered.

Three-time Overwrite-Erase
Unwanted data area is overwritten twice with random data, and then once with null data. The three-time overwrite-erase function removes the ability to restore the data even if using highly skilful restoration techniques. The three-time overwrite-erase method is more rigorous compared to the one-time overwrite erase method. In case of overwrite-erasing bulk data, the three-time overwrite-erase method may take longer time compared to the once-time overwrite-erase method.

The U.S. Department of Defence DoD 5220.22-M (Three passes)
The U.S. DoD 5220.22-M compliant three pass overwrite is a very powerful mode to overwrite the data area of the HDD. The unwanted data area (in case of overwrite) or all areas (in case of system initialisation) is overwritten with any character (at first pass), its complement (at second pass), random character (at last pass), and then with verification. The U.S. DoD 5220.22M three–pass mode initially erases the unwanted data first, and then verifies that the unwanted data has been completely erased. Even through a sophisticated restoration process, it would be extremely difficult to restore the erased data. The DoD 5220.22-M three-pass is the highest level security mode, compared to "One-time Overwrite-Erase" and "Three-time Overwrite-Erase". It significantly reduces the risk of information leakage.

19. Below is a list of ports and protocols typically used on a networked device.

Authentication Protocols

IEEE802.1x

This protocol allows communications only to authorised users (and authenticated devices) when connecting to the network, and prevents unauthorised devices from connecting to network. KYOCERA devices support the IEEE802.1x which would not allow unauthorised access by unauthenticated clients to the network, preventing unauthorised disclosure of information. The KYOCERA MFPs/Printers employ four types of authentication modes as described below.

PEAP-TLS/PEAP (Protected Extensible Authentication Protocol-Transport Layer Security)

The client is authenticated based on the ID and certificate and the certificate of authentication server is checked at the same time.

EAP-PEAP (Extensible Authentication Protocol-Protocol Extensible Authentication Protocol)

The client is authenticated based on the ID/password and only the common name of the authentication server certificate is checked.

EAP-FAST (Extensible Authentication Protocol-Flexible Authentication via Secure Tunnelling)

EAP-FAST is an IEEE802.1.x/EAP authentication method developed by Cisco System, Inc. Mutual authentication is performed for the client and authentication server based on the user ID and password and PAC (Protected Access Credential) establishes a tunnel for the user based on the unique shared secret key.

EAP-TTLS (Extensible Authentication Protocol-Tunnelled Transport Layer Security)

The client is authenticated based on the user ID and password, and also authentication server is authenticated based on the electric certificate. Using EAP-TLS, Client and server electric certificates are required for authentication, whereas for EAP-TTLS, the user ID and password are used instead of a client certificate. This makes EAP-TTLS easier to introduce compared to EAP-TLS. Electric certificates are used to prove the validity of authentication server. Therefore, it helps improve more secure and trusted communications.

SMTP Authentication

SMTP authentication is a function that permits to send an e-mail only when the ID and password are successfully authenticated on SMTP server. The function prevents unauthorised users to send e-mails through the SMTP server by limiting access to the SMTP server.

POP before SMTP

POP before SMTP performs POP authentication before sending e-mails from the SMTP server. The emails can be sent within the specified period after completion of POP authentication. POP authentication before sending an e-mail prevents masquerading.

Ports and Protocols

Protocol	Port No.	Setting	Note
FTP Server	TCP 21	Enable/Disable	FTP server is a protocol for receiving a document
HTTP	TCP 80	Enable/Disable	HTTP is a protocol that is used when receiving/sending data from a web page between www server and browser.
NetBEUI	TCP 139	Enable/Disable	NetBEUI is a protocol for a small network that is used for file sharing and print services, as well as for receiving a document.
HTTPS	TCP 443	Enable/Disable	HTTPS is a protocol that performs encryption using SSL/TLS.
IPP over SSL/TLS	TCP 443	Enable/Disable	IPP over SSL/TLS is a protocol that combines SSL/TLS which encrypts a channel, and IPP which is used for internet printing. In addition, the IPP over SSL/TLS can have a valid certificate.
LPD	TCP 515	Enable/Disable	LPD is a printing protocol that is used for printing text files or Postscript.
IPP	TCP 631	Enable/Disable	IPP is a protocol that controls to send/receive print data via TCP/IP including internet, or print devices.
ThinPrint	TCP 4000	Enable/Disable	ThinPrint is a print technology available in Thin client environment, and also supports SSL/TLS.
WSD Scan	TCP 5358	Enable/Disable	Windows Vista WSD is a protocol that enables MFPs/Printers for a network connection. This also enables users to detect (install) MFPs/Printers device or send/receive data easier. Original documentation image scanned through MFP/Printer can be stored in WSD PC as a file.
WSD Print	TCP 5358	Enable/Disable	Windows Vista WSD is a protocol that enables MFPs/Printers for a network connection. This also enables users to detect (install) MFPs/Printers device or send/receive data easier.
Enhanced WSD	TCP 9090	Enable/Disable	Enhanced WSD takes a procedure for easily connecting the various devices connected to a network, and using. The status monitor through this port 9090 can monitor the status of MFP/Printer.
Enhanced WSD over SSL/TLS	TCP 9091	Enable/Disable	Enhanced WSD (SSL/TLS) is a security protocol as well as an enhanced WSD with using SSL/TLS. This provides encryption, authentication and safety (Protect against alteration).
RAW	TCP 9100 - 9103	Enable/Disable	RAW protocol takes different steps, compared to LPR for printing. In general, MFP/Printer uses port number 9100, and also uses SNMP or MIB to configure and monitor printer status
SNMPv1/v2	UDP 161	Enable/Disable	SNMP protocol is used in network management system. Normal communication will be performed using read and write community names.
SNMPv3	UDP 161	Enable/Disable	SNMP protocol is used in network management system. Normal communication will be performed using user name and password. Authentication option or encryption option can be used.

DSM Scan		Enable/Disable	DSM (Distributed Scan Management) uses Windows Server 2008 R2 that is used for handling large amounts of user data in a large organisation.
FTP Client		Enable/Disable	FTP client is a communication protocol for forwarding a file via a network.
LDAP		Enable/Disable	Address Book on LDAP server is referred as an external address book. FAX number and email address can be designated as destination.
POP3		Enable/Disable	POP3 is a standard protocol for receiving emails.
POP3 over SSL/TLS		Enable/Disable	POP3 over SSL/TLS is a protocol that combines POP3 which is used for receiving an email, and SSL/TLS which is used for encrypting a channel.
SMTP		Enable/Disable	SMTP is a protocol for sending emails
SMTP over SSL/TLS		Enable/Disable	SMTP over SSL/TLS is a protocol that combines SMTP which is used for sending an email, and SSL/TLS which is used for encrypting a channel.
SMB Client		Enable/Disable	SMB is a protocol that performs file or printer sharing through a network.
eSCL		Enable/Disable	eSCL is a protocol that is used for remote scan from Mac OS X.
eSCL over SSL/TLS		Enable/Disable	eSCL over SSL is eSCL communication protocol using SSL certificate. All eSCL over SSL communications are encrypted
LLTD		Enable/Disable	LLTD is a protocol for network topology discovery and quality of service diagnostics.
REST		Enable/Disable	REST is the software architecture of the web application that supports multiple software in a distributed hypermedia system.
REST over SSL/TLS		Enable/Disable	REST over SSL is REST communication protocol using SSL certificate. All REST over SSL communications are encrypted.

Secure Communication Protocols

SNMP v3

SNMP is a standard protocol that monitors and controls devices connecting to the network. Moreover, SNMPv3 provides ability to protect data confidentiality through authentication and encryption.

IPv6

KYOCERA has obtained the IPv6 Ready Logo up to Phase2. IPv6 support, which is available in the KYOCERA MFPs/Printers, can connect to the router, and use basic control protocol like ping. In addition to the above-mentioned basic connections, a more secure connection is ensured by implementing rigorous security measures.

IPSec

A protocol with a functionality that protects data in transit from tapping or alteration by encrypting respective IP packets. Encryption using IPSec is applied to print data sent from a PC to a MFP/Printer, and scanned data to be sent from a MFP to a PC. Therefore, IPSec supports a more secure exchange of data.

SSL/TLS

A system to encrypt data for transmissions such as Web access or others, and also has a function to mutually check if communication destination parties are reliable for mutual communications. KYOCERA MFPs/Printers support SSL/TLS encryption protocols including SSL3.0, TLS1.0, TLS1.1, TLS1.2, and thereby preventing alteration of data or tapping data on network.

IPP over SSL/TLS

An internet printing protocol that acts as a combination of IPP, which is for exchanging print data on the internet or TCP/IP network, and SSL/TLS, which is for encryption of a communication channel. This allows users to safely send printed documents to the MFPs/Printers through the network.

HTTP over SSL/TLS

A protocol that acts as a combination of HTTP, which is for sending/receiving data to and from web browser or others on the TCP/IP network, and SSL/TLS, which is for encryption of a communication channel. In transmitting data between a PC and a MFP/Printer, this mitigates risks of alteration and leakage of data by unauthorised users.

FTP over SSL/TLS

A protocol that acts as a combination of FTP, which is used for forwarding a file on the TCP/IP network, and SSL/TLS, which is for encryption of a communication channel. When sending scanned data from a MFP/Printer using the FTP protocol, SSL/TLS encryption is applied to the channel. FTP over SSL/TLS enables more secure transmissions.

SMTP over SSL/TLS

A protocol that acts as a combination of e-mail transmission, and SSL/TLS, which is for encryption of a communication channel between a server and a MFP/Printer. This prevents masquerading, tapping or modifying data in transit.

POP3 over SSL/TLS

A protocol that acts as a combination of POP3, which is an email reception protocol, and SSL/TLS, which is for encryption of a communication channel between a server and a MFP/Printer. This prevents masquerading, tapping or modifying data in transmit.

COMPLIMENTARY INFORMATION:

Data Security Kits provide data encryption that meets ISO criteria for KYOCERA devices, for further information use the link: https://goo.gl/jE8W9n

FOR MORE INFORMATION ABOUT KYOCERA SecureAudit PLEASE VISIT:

www.kyoceradocumentsolutions.co.uk, or call us at 0845 710 3104.