

SS730EX Plus

Release Notes
March 2020

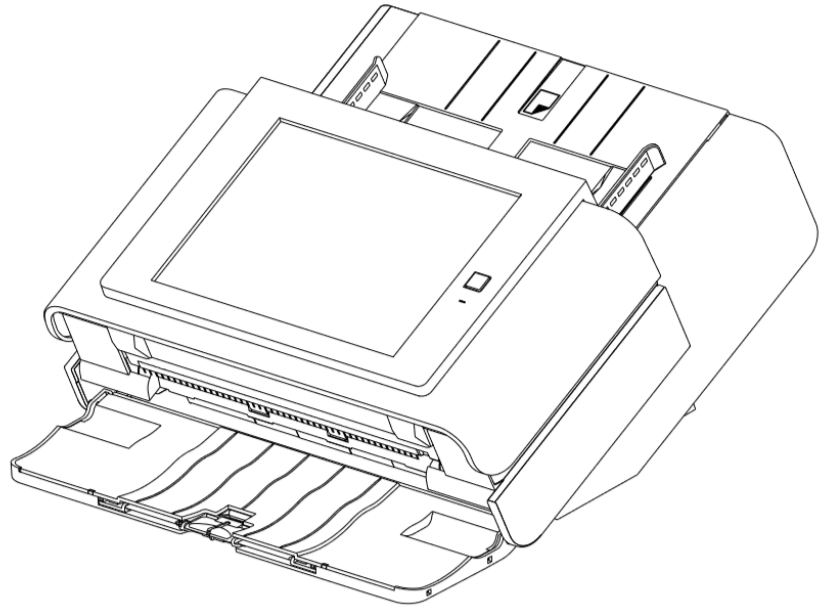


Table of Contents

- Introduction
- Initial Release Information
- Scan Station Portfolio Overview
- Specifications
- Warranty
- Scan Station 730EX Plus Security
- Windows Security Updates on the SS730EX Plus
- Scanner Administration Tool (SAT) Updates

New Windows 10 Scan Station

- The **Scan Station 730EX Plus** is a new model of the Scan Station, leveraged from the existing Scan Station 710 and 730EX with the internal operating system updated to **Windows 10 IoT Enterprise LTSC 2019 version**
- The **Windows 10 IoT version** was chosen because with this version Microsoft will only provide updates to security related features
 - This eliminates the risk of Microsoft feature updates affecting the Kodak or custom scanning applications
- Certified to Energy Star 3.0

Initial Release Information

KODAK Scan Station Application

- Version 1.5.40
- Includes the latest scanner drivers and flatbed driver support
 - Scanner Driver Patch 4.6
 - Flatbed Image Processing Patch 4.0

Scanner Administration Tool

- Version 1.4.23

Scan Station Portfolio

| Current Models | PPM | Flatbed Accessary | Duty Cycle | Operating System | TLS Support | Note: |
|--------------------|-----|-------------------|------------|------------------|---------------|--|
| Scan Station 710 | 70 | Y | 6K | Win 8.0 | 1.0 only | No 3 rd party Integrations |
| Scan Station 730EX | 70 | Y | 6K | Win 8.1 | 1.0, 1.1, 1.2 | 3 rd party Integrations Allowed |

| New Model | PPM | Flatbed Accessary | Duty Cycle | Operating System | TLS Support | Note: |
|-------------------------|-----|-------------------|------------|------------------|-------------|---|
| Scan Station 730EX Plus | 70 | Y | 6K | Win 10 IoT | 1.1 and 1.2 | Kodak Scan Station application and 3 rd party Integrations Allowed |

Pages Per Minute for all Scan Stations:

- B&W/Gray: 70ppm at 200 or 300 DPI
- Color 200: 60ppm
- Color 300: 40ppm

Specifications

The **Scan Station 730EX Plus** Specifications (Hardware and KODAK Scan Station application capabilities) have not changed from the SS710 and SS730EX with the exception of the Windows 10 embedded operating system

Specifications can be found on the web at:

<https://www.alarisworld.com/en-us/solutions/document-scanners/desktop/scan-station-730ex-plus#Specifications>

The screenshot shows a web browser window displaying the Alaris website. The URL is <https://www.alarisworld.com/en-us/solutions/document-scanners/desktop/scan-station-730ex-plus#Specifications>. The page features a navigation menu at the top right, a 'Specifications' section with a table of specifications, and a 'Support' sidebar on the right. A 'Print' button is visible next to the 'Connectivity' section.

| Category | Specification |
|--|--|
| Recommended Daily Volume | Up to 6,000 pages per day |
| Connectivity | 10/100/1000 Base T and no host PC required |
| Output Methods | Scan to network share, scan to print, scan to e-mail, scan to fax server, scan to portable USB drive, scan to KOFAX Front Office Server, FTP, SFTP, FTPS (anonymous, authenticated, with proxy support), and scan to MICROSOFT SHAREPOINT (on-premise) |
| Network Protocols | FTP, HTTP, WINS, TCP/IP, SMB, authenticated SMTP (login, plain text, CRAM, NTLM), DHCP (or static IP), Network domain authentication |
| Security Features | Automatic, ongoing installation of Microsoft's latest security updates via default update feature; PDF private key encryption, optional password access, option to enable/disable the ability to scan to portable USB drives, secure login via LDAP, activity logging by Login ID, IP port blocking |
| Remote Administration (for system administrators only) | Secure login with a customizable password, ability to create and manage lists of Scan Station 730EX Plus devices, group and easily classify managed devices, update the configuration and/or embedded software of one, some or all managed devices, view the status of managed devices, remotely access and manage the logs of a single managed device, restart or power off a single managed device |
| Embedded Operating System | Windows 10 IoT Enterprise LTSC 2019 version |
| File Format Outputs | Text searchable PDF using the industry leading Abbyy OCR engine, Single and multipage TIFF, JPEG, PDF, PDF, PDF/A, Microsoft Word, Microsoft Excel, RTF, encrypted PDF, JPEG-compressed TIFF, WAV audio files |
| Control Panel | 9.7 in. (24.6cm) 1024 x 768 Touchscreen LCD |

Warranty

The **SS730EX Plus** will continue to have the same warranty as the SS710 and SS730EX

- **US&C:** 3 months AUR
- **EMEA:** 1 year AUR
- **Japan:** 1 year AUR
- **Rest of World:** 1 year with On-Site or “Return to Base” service by either Alaris or 3rd party service providers

Scan Station 730EX Plus Security

The Scan Station 700 Plus Series is configured to prevent external attacks from the Internet and from direct access by users. The following security features will block access to the Scan Station's operating system:

- **Microsoft Windows Security updates**

- The Windows update service is turned on by default in the 700EX Plus Series
- The scanner will check for security updates and apply them as needed

- **Microsoft Windows Defender**

- The Windows Defender service is always updating and running on the 700EX Plus Series. The service will ensure security through:
 - Anti-virus checking
 - Verification that installed applications are signed

- The Scan Station uses a **firewall** and blocks nearly all incoming network traffic
 - Most inbound ports are blocked and will not respond to queries from the network
- The Scan Station is also configured to respond to an echo (also known as a *ping*)
 - This can be useful for diagnosing connectivity issues

Scan Station 730EX Plus Security (continued)

Continuation of security features that will block access to the Scan Station's operating system:

- The Scan Station is **protected from external intrusions** via the Scan Station USB ports
 - The operating system is configured to disable any auto-run action that could occur when presenting a new USB device to the system
 - The Scan Station recognizes the presence of a USB removable device, but will only open and read files that have been created and encrypted specifically for use by the Scan Station
 - Any file found on a removable device that is not properly encrypted will be ignored
 - This makes it almost impossible to introduce a virus by inserting a removable device with an infected executable.
- Viruses frequently find their way into a network-connected computer via email. Most viruses are spread as email attachments and infect a computer after the email has been opened and the attachment executed.
 - The Scan Station does not receive any incoming emails, therefore, it cannot be infected in this manner.
- The Scan Station will only read a **valid, encrypted configuration file**
- The **underlying operating system is not available** to the administrator or user.
 - Updates to the operating system and/or the Scan Station firmware will be made available on the Kodak Alaris website as needed

Scan Station 730EX Plus Security (continued)

Continuation of security features that will block access to the Scan Station's operating system:

- To help secure the Scan Station, the customer can set up a **Remote Access Password** and/or a **Local Access Password**
 - The **Remote Access Password** protects the Scan Station from being modified by another (unauthorized) installation of the Scanner Administration Tool
 - The **Local Access Password** prevents a walk-up user from modifying the Scan Station via a USB removable device
- **Notes:**
 - A Remote or Local Access Password that is lost or forgotten may be able to be recovered by the Alaris Service and Support organization.
 - The Service case that is established must be escalated to **Level 3 Support in Rochester** for assistance
- The customer can configure the Scan Station to **require a user to log in** before scanning

Windows Security Updates on the 730EX Plus

- The new 730EX Plus scanner will (by default) automatically apply **Windows Security Updates** to the operating system.
 - Microsoft Windows Feature Updates will not be applied
- The scanner will attempt to connect to the public Microsoft Update server daily to download **security updates**.
 - Local update servers are not currently supported
- Any security updates that have been downloaded will, by default, be applied at 3:00am local time
 - If the Scan Station is in Power Saver mode at that time, it will get woken up
 - Security updates (if available) may also be applied upon reboot of the Scan Station
- Can only be enabled/disabled from the Scanner Administration Tool (SAT)
 - Can not be enabled/disabled from the Scan Station itself
 - The time at which to apply any Security Updates (that have been downloaded) is also be configurable

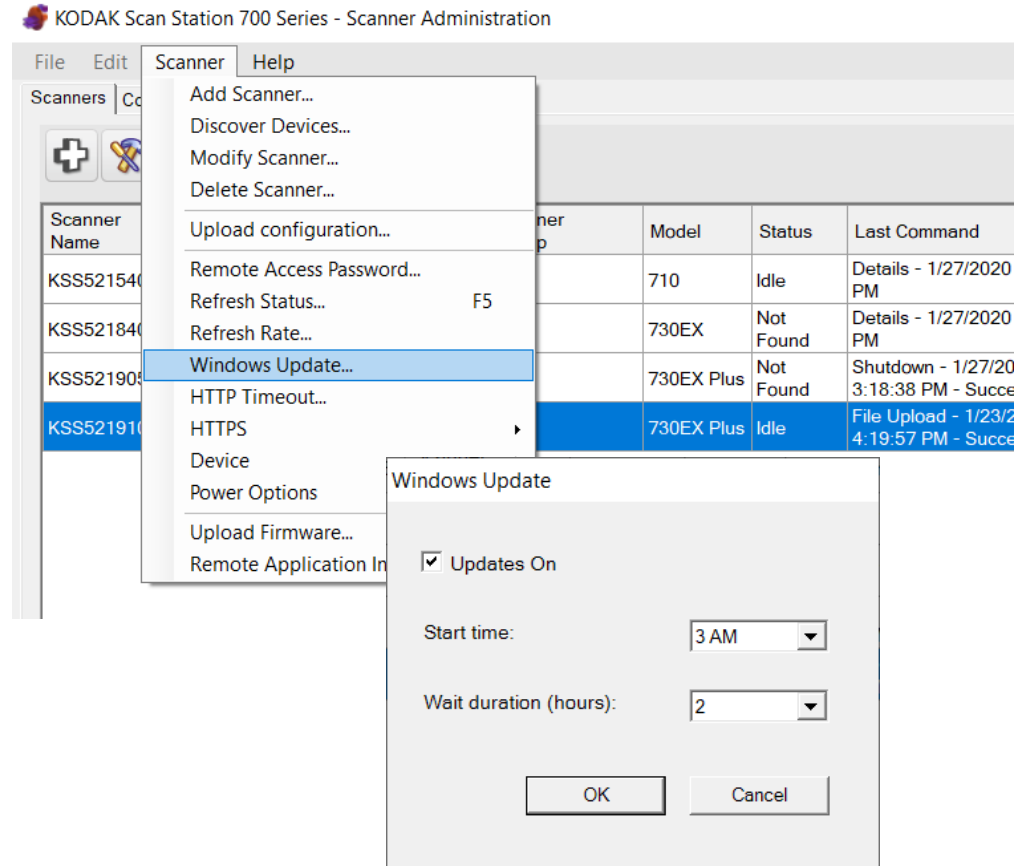
Windows Security Updates on the 730EX Plus (continued)

- If the end user is present when the Windows security update is taking place they will likely see the following during the updates:



Scanner Administration Tool Updates

- The updated **Scanner Administration Tool (SAT)** will support all SS700 Scan Stations including SS710, SS730EX, and SS730EX Plus
 - Existing SS710/SS730EX customers who add SS730EX Plus scanners to their fleet should upgrade to **Version 1.4.23** of the SAT Tool
- Ability to change **Windows Security Update configuration** is only available for the SS730EX Plus
 - **Wait duration** is the amount of time the system will wait for any security updates to be applied before going back into Power Saver mode.



Scanner Administration Tool Updates (continued)

- In order for the Scanner Administration Tool to work with and **Add** an SS730EX Plus, the PC's Local Security Policy for **LAN Manager Authentication Level** must be set to **NTLMv2**
 - Customers should work with their IT organization to review and modify this setting as necessary

The screenshot displays the Windows Security Settings application. On the left, the navigation pane shows 'Security Settings' expanded to 'Local Policies' > 'Security Options'. The main pane lists various security policies, with 'Network security: LAN Manager authentication level' selected and highlighted in blue. A 'Properties' dialog box is open over this policy, showing the 'Local Security Setting' tab. The setting is 'Network security: LAN Manager authentication level'. Below this, a dropdown menu is open, showing the following options: 'Send NTLM response only', 'Send LM & NTLM responses', 'Send LM & NTLM - use NTLMv2 session security if negotiated', 'Send NTLM response only', 'Send NTLMv2 response only' (which is selected), 'Send NTLMv2 response only. Refuse LM', and 'Send NTLMv2 response only. Refuse LM & NTLM'. A yellow warning icon is visible next to the selected option.

| Policy | Security Setting |
|--|----------------------------------|
| Network access: Shares that can be accessed anonymously | Not Defined |
| Network access: Sharing and security model for local accounts | Classic - local users auth... |
| Network security: Allow Local System to use computer identity for NTLM | Not Defined |
| Network security: Allow LocalSystem NULL session fallback | Not Defined |
| Network security: Allow PKU2U authentication requests to this computer to use online identities. | Not Defined |
| Network security: Configure encryption types allowed for Kerberos | Not Defined |
| Network security: Do not store LAN Manager hash value on next password change | Not Defined |
| Network security: Force logoff when logon hours expire | Not Defined |
| Network security: LAN Manager authentication level | Send NTLMv2 response only |
| Network security: LDAP client signing requirements | Not Defined |
| Network security: Minimum session security for NTLM SSP based (including secure RPC) servers | Not Defined |
| Network security: Minimum session security for NTLM SSP based (including secure RPC) servers | Not Defined |
| Network security: Restrict NTLM: Add remote server exceptions for NTLM authentication | Not Defined |
| Network security: Restrict NTLM: Add server exceptions in this domain | Not Defined |
| Network security: Restrict NTLM: Audit Incoming NTLM Traffic | Not Defined |
| Network security: Restrict NTLM: Audit NTLM authentication in this domain | Not Defined |

Scanner Administration Tool Updates (continued)

If the user's PC is not configured for NTLMv2, they will get the following message when attempting to **Add** the SS730EX Plus machine:

