

Xerox® Healthcare MFP Solution

Quick Start Guide

Congratulations! You are minutes away from turning your Xerox® Healthcare MFP into a streamlined tool for securely sharing patient information. Included with your device is more than just traditional print, copy, fax and scan functionality...your new healthcare multifunction printer (MFP) enables you to *share* patient information in a secure and efficient manner by installing and activating the *Share Patient Information App*.



You will need the Kno2™ Connector License Key located in your Welcome Letter to complete the steps below to begin using your Xerox® Healthcare MFP.

Creating your Kno2 Account

The Xerox® Healthcare MFP Solution and the *Share Patient Information App* work with the Kno2 cloud service to connect the community of care. Follow the simple steps outlined below to sign up for Kno2 and activate your free, 1-year subscription.

Create a Kno2 Account

1

Create Account and Confirm Plan

Visit <https://kno2.com/register/healthcaremfp> to register your primary user and confirm your Kno2 account under the Stay Connected plan¹.

2

Verify Identity and Activate Your Account

- Set a password and complete identification and security questions to allow your office to exchange patient information online with other providers.
- You'll be prompted to make a decision regarding your fax volume - acquire new or transition your existing fax number(s) into your Kno2 account and receive documents in a way that can easily be saved to your patient charts. You will receive an email confirmation within 24-48 hours notifying you that your account is active.

3

Add the License Key Included with Your Xerox® Healthcare MFP

Log in to your Kno2 portal account and enter the device license key located in the Xerox® Healthcare MFP Welcome Letter.

- Select the gear icon in the upper right corner; select **Add-Ons**.
- Select the **Licenses** tab, then select **Enter Additional Licenses**.
- Enter the connector license key located in the Xerox® Healthcare MFP Welcome Letter and select **Save Changes**.



Once the connector license key has been saved, you will receive an email confirming your Kno2 account has been upgraded to a FREE 1-year subscription for up to three users.

¹ Your Kno2 account will be automatically upgraded from Stay Connected to the full-year, three-user Step Into Interoperability plan when you add your first Xerox® Healthcare MFP license.

Installing the Xerox® Healthcare MFP App on your device

The Xerox® Healthcare MFP App works with your Kno2™ cloud service account to allow you to securely share patient information right from your device. The app is readily available to anyone with a Xerox App Gallery account and can be installed directly from the Xerox App Gallery App or by accessing the Xerox App Gallery Web Portal.

Install Xerox® Healthcare MFP App

4

Enable Security

You already know how important it is to protect your patient's information. Enable the recommended security features for your Xerox® Healthcare MFP. To begin, open a browser and enter the IP address of your Xerox® Healthcare MFP, log in and select the Properties tab.



The following steps apply only to the ConnectKey and AltaLink devices. To enable the security settings on VersaLink devices, see step f.

a. Enable Security Certificates

- From the “General Setup” group, select **Extensible Services Setup**.
- On the resulting page, check the “Verify Server Certificates” box and select **Apply**.

b. Image Overwrite Security

- In the “Security” group, select **Image Overwrite Security**.
- Select the **Immediate Job Overwrite** tab and verify that the Image Job Overwrite is “Enabled”. If not, select **Enabled** and then select **Apply**.



When the time comes for your Xerox® Healthcare MFP to leave your premises, it is recommended that you run a full disk image overwrite. (This only needs to be done prior to the Xerox® Healthcare MFP leaving your possession! For normal day -to-day use, turning on Immediate Job Overwrite is sufficient.) To do this, click on the “Disk Overwrite” tab, then the “Overwrite Now” tab, then select “Advanced Settings.” In the resulting screen (shown below) select the “Full” radio button, then click on “Start Disk Overwrite Now.”

Security

Image Overwrite Security

Immediate Job Overwrite **Disk Overwrite**

Status: Overwrite has never been performed.

Schedule **Overwrite Now**

Confirmation Report
Errors Only

☒ Advanced Settings

Overwrite Mode
☐ Standard
☒ Full

Start Disk Overwrite Now

Notes:

- Takes the machine offline
- Approximately 60 minutes for "Full" mode
- Cannot be cancelled

Full overwrites all user stored data from hard disk(s).
 To backup "Save Jobs", go to: [Services > Recent Saved Jobs > Backup Jobs](#).
 Will take approximately 60 minutes.
 Refer to <http://www.xerox.com/security> for more information.

c. Turn on the Audit Log

- In the “Security” group, select **Audit Log**.
- If “Device Audit Log” is disabled, select **Enable** and then select **Apply**.

Audit Log

Device Audit Log

☐ Enabled **Export Audit Log**

Protocol Log

☒ Enabled

Changes to this setting will require a Reboot.

Apply

d. McAfee Embedded Control

- In the “Security” group, select **McAfee Embedded Control**.
- If the feature is disabled, select **Edit** and then **Enhanced Security** and **Audit Log**, then **Save**.

Security > **McAfee Embedded Control**

Device Security Levels

Security Level

☒ Enhanced Security
☐ Integrity Control
☐ Disable McAfee Embedded Control

Alert Feedback Methods

☒ Locally on the Device
☐ Email Alerts

McAfee Remote Solutions

☐ McAfee's ePolicy Orchestrator Server

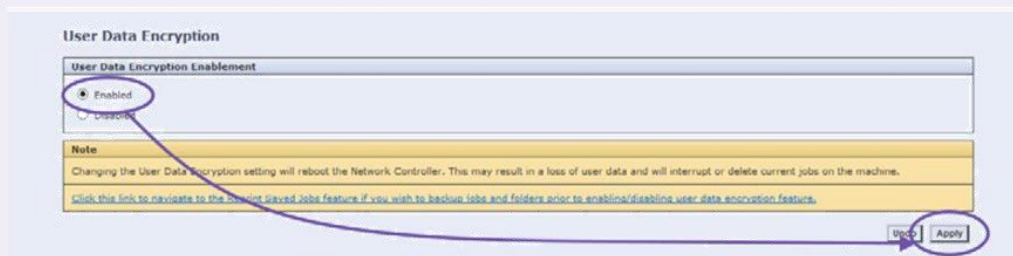
Xerox Remote Solutions

[ServiceNow Web](#)
[Xerox Device Manager](#)

Save

e. User Data Encryption

- i. In the “Security” group, select **Encryption Group** and then select **User Data Encryption**.
- ii. If the feature is disabled, select **Enabled** and then select **Apply**.



To enable security on **VersaLink** devices, follow the steps below:



Only a person who has MFP Administrator privileges and is logged onto the MFP as Administrator may perform this procedure. A MFP may have more than one Administrator. If you are not an Administrator of the MFP, contact a MFP Administrator for assistance.

f. Installing SSL Certificates

1. Open an Internet browser on your computer.
2. Save the Certificate files to your computer:
 - a. Navigate to the location where the Certificate files are located.
http://www.support.xerox.com/KB_Connect/KB_Connect.asp?ArtId=XAG_CertificateBundle&Xcntry=USA&Xlang=en_US&prodID=APP_GALLERY
 - b. Select Save or Save As to download the Certificate File to your local computer.
3. Install the Certificates:
 - a. From an Internet browser, enter the IP address of the multifunction printer (MFP) / device in the **Address** field, and press **Enter**. The CentreWare Internet Services page for the MFP opens.
 - b. Login as Administrator.
 - c. Select the **System** tab.
 - d. Select **Security**.
 - e. Under Security select **Security Certificates**. The Security Certificates page displays.
 - f. Select the **Trusted Root CA Certificates** from the dropdown.
 - g. Select the **Import** button.
 - h. Browse to the location on your computer where the Certificate File is stored.
 - i. Select the certificate file, and then select **Open**.
 - j. Select **Import** on the Install Certificate window. The security certificate appears in the list of installed certificates.
 - k. Select **Close**.
4. Enable Verification of SSL Certificates by performing the following steps:
 - a. Select **Apps**.
 - b. Select **EIP Settings**. The Extensible Interface Platform page displays.
 - c. For the EIP Browser, change the toggle to off. This disables the Extensible Services Browser.
 - d. Toggle the **Verify server certificates** on.

- e. Select **System**.
- f. Select **Security**.
- g. Under Certificates, select **Certificate Path Validation** and select **On**
- h. Select **OK**
- i. Under Network Security, select **SSL/TLS Settings** and toggle on **Verify Remote Server Certificate**
- j. Select **OK**
- k. Select **Apps**.
- l. Select **EIP Settings**.
- m. Toggle the **EIP Browser** back on.

IMPORTANT: Toggling this setting off and then on is essential and ensures verification of the SSL Certificates. This re-enables (resets) the Extensible Services Browser.

Enabling Verify server certificates is a global setting that affects all Extensible Interface Platform (EIP) Applications installed on your MFP.

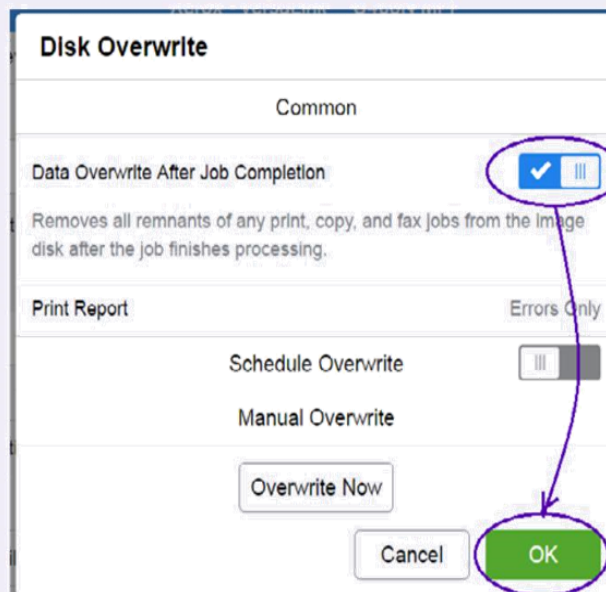


IMPORTANT: If SSL certificates are disabled, the secure communications of private or sensitive information is vulnerable. Therefore, it is recommended that Verify server certificates is enabled on your MFP.

The following settings come configured in the recommended state for this App from the factory. If your Xerox® Healthcare MFP is newly installed, it is likely that no further changes are required. Please take a moment to confirm the remaining security items are enabled.

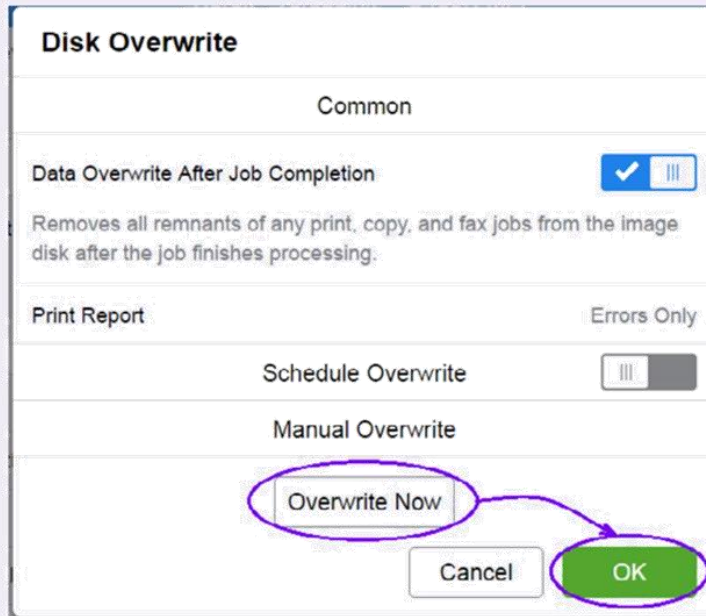
g. Image Overwrite Security

- i. Select the **System** tab
- ii. Then select **Security**
- iii. Under **Disk Overwrite**, Select **Edit**
- iv. Toggle on **Data Overwrite after Job completion**
- v. Select **OK**



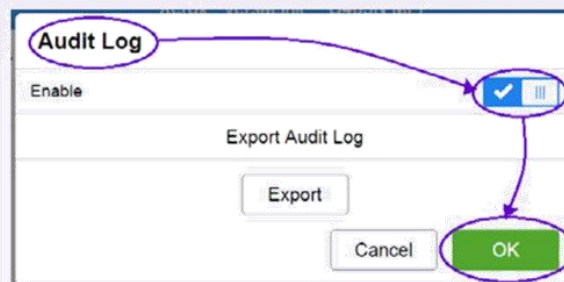
When the time comes for your Xerox® Healthcare MFP to leave your premises, it is recommended that you run a full disk image overwrite. (This only needs to be done prior to the Xerox® Healthcare MFP leaving your possession! For normal day-to-day use, turning on Immediate Job Overwrite is sufficient.) To do this, follow these steps:

- i. Under Disk Overwrite, select **Edit**
- ii. Select **Overwrite Now** and then select **OK**



h. Turn on the Audit Log

- i. Click **System** and then click Logs
- ii. Click **Audit Log**
- iii. Toggle on **Enable**
- iv. Select **OK**



5

Install the Xerox®Healthcare MFP App on Your Device

Access the Xerox App Gallery to locate and install the *Share Patient Information App* on your Xerox® Healthcare MFP.

- a. Go to the Xerox App Gallery URL and log in.
https://appgallery.external.xerox.com/xerox_app_gallery/login

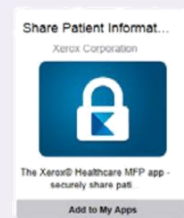


If you do not have a Xerox App Gallery account, click on **Log In** and then **Create Account** and follow the instructions to create an account.

- b. On the **All Apps** tab, browse for **Share Patient Information** (the display name for the Xerox® Healthcare MFP App) and select **Add to My Apps**.
- c. Select the **Devices** tab, and add a multifunction device if necessary.
- d. Select **My Apps** tab and locate the Xerox® Healthcare MFP from the list.
- e. In the Action column, select **Install**, and follow the on-screen instructions for installing the app.
- f. Once installed, you should see a **Share Patient Information** button on your Xerox® Healthcare MFP.



If you have the Xerox App Gallery App on your Xerox® Healthcare MFP, you may also install the **Share Patient Information App** in that way. Simply follow the on-screen instructions for installing the app.



Connecting your Xerox® Healthcare MFP to your Kno2 Account

Associate your Xerox® Healthcare MFP to your Kno2 Account and “link” it to your license key to begin sharing patient information with other providers.

Connect Your Xerox® Healthcare MFP

6

Associate your Xerox® Healthcare MFP to your Kno2 Account

From the Xerox® Healthcare MFP, select the *Share Patient Information* button to associate your Kno2 organization to your device.

- a. Log in to Kno2. Two-factor Authentication may be required.
- b. Select the Kno2 Organization that will be associated with the device.




A message displays saying: “Link Successful. This device may be used after your Kno2 Administrator assigns a license.”

7

Connect your License Key to Your Xerox® Healthcare MFP

Log in to your Kno2 portal account to link your license key to your device.

- a. Select the gear icon in the upper right corner and select **Add-Ons**.
- b. Select the **Devices** tab and locate the unlicensed device.
- c. Select the Attach to License button  and choose the license key from the drop-down menu, and select **Save Changes**.

8

Share Patient Information

Create and send messages directly from your Xerox® Healthcare MFP across a HIPAA-compliant, secure network to better coordinate care.

- a. Select the **Share Patient Information** button from your Xerox® Healthcare MFP touch panel, and log in to your Kno2 account.
- b. Follow the on-screen instructions for creating and sending a message with patient information attached.



Confirm your connection to the healthcare network. Follow the steps outlined in “Confirm Connection – How to share patient information” right from your Xerox® Healthcare MFP. (This document is available at: <http://www.office.xerox.com/latest/SO1GD-09U.PDF>)

Support

For additional help with your Xerox® Healthcare MFP Solution please follow your usual Xerox support process. Additionally, the following support resources are available.

App Help

Help on creating a Kno2 account can be found at <http://go.kno2.com/healthcare-mfp/>.

Online Help and Documentation

Xerox App Gallery Knowledge Base	http://www.support.xerox.com/support/xerox-app-gallery
Xerox App Gallery Documentation	http://www.support.xerox.com/support/xerox-app-gallery/documentation/enus.html
Kno2 Knowledge Base	http://intercom.help/kno2
Kno2 YouTube Channel	https://www.youtube.com/channel/UC7NRzQWyijaAjzzd34q5Ylg

Customer Support Forum

The customer support forum can be found at <http://forum.support.xerox.com/>

Supported MFPs

The list of supported MFPs can be found under the Compatible Products section at the following location:

www.xerox.com/healthcaremfp