

Kofax SafeCom Go Xerox Administrator's Guide

Version: 9.13.0

Date: 2023-05-03

KOFAX

© 1995-2023 Kofax. All rights reserved.

Kofax is a trademark of Kofax, Inc., registered in the U.S. and/or other countries. All other trademarks are the property of their respective owners. No part of this publication may be reproduced, stored, or transmitted in any form without the prior written permission of Kofax.

Table of Contents

Preface	11
Training.....	11
Getting help with Kofax products.....	11
Chapter 1: Introduction	13
SafeCom Go Xerox.....	13
Requirements.....	13
SafeCom ID devices.....	14
Xerox global print driver.....	15
Supported languages.....	15
Chapter 2: Install SafeCom Go Fuji Xerox	16
Xerox Altalink.....	16
Create certificate on the printer.....	16
Enable HTTPS on the printer.....	17
Enable Extensible Service Registration on the printer.....	17
Set up Extensible Service on the printer.....	17
Allow login by code on the printer.....	17
Add the device in SafeCom Administrator.....	18
Configure authentication and access control on the printer.....	18
Xerox Versalink.....	18
Create certificate on the printer.....	18
Enable HTTPS on the printer.....	19
Add the device in SafeCom Administrator.....	19
Configure authentication and access control on the printer.....	19
Allow login by card on the printer.....	19
Xerox WorkCentre 7120, 7125, 7220, Xerox Color 550/560.....	20
Create certificate on the printer.....	20
Enable HTTPS on the printer.....	21
Enable Extensible Service Registration on the printer.....	21
Set up Extensible Service on the printer.....	21
Allow login by code on the printer.....	21
Add the device in SafeCom Administrator.....	22
Configure authentication and access control on the printer.....	22
Xerox ColorQube 92xx and 93xx.....	23
Set up the printer.....	23

Create certificate on the printer.....	23
Enable HTTPS on the printer.....	24
Enable Extensible Service Registration on the printer.....	24
Setup Extensible Service on the printer.....	24
Configure authentication and access control on the printer.....	24
Allow login by code on the printer.....	25
Add the device in SafeCom Administrator.....	25
Xerox WorkCentre 77xx.....	25
Set up the printer.....	25
Create certificate on the printer.....	26
Enable HTTPS on the printer.....	26
Enable Extensible Service Registration on the printer.....	26
Configure authentication and access control on the printer.....	27
Allow login by code on the printer.....	27
Add the device in SafeCom Administrator.....	27
Xerox WorkCentre 76xx.....	28
Set up the printer.....	28
Create certificate on the printer.....	28
Enable HTTPS on the printer.....	29
Enable web services.....	29
Configure authentication and access control on the printer.....	29
Allow login by code on the printer.....	29
Add the device in SafeCom Administrator.....	30
Xerox WorkCentre 58xx and 78xx.....	30
Create certificate on the printer.....	30
Enable HTTPS on the printer.....	30
Enable Extensible Service Registration on the printer.....	31
Configure authentication and access control on the printer.....	31
Enable copy locking using SafeCom copy cable.....	31
Enable extensible services browser.....	31
Allow login by code on the printer.....	32
Add the device in SafeCom Administrator.....	32
Xerox WorkCentre 75xx.....	32
Create certificate on the printer.....	32
Enable HTTPS on the printer.....	33
Enable Extensible Service Registration on the printer.....	33
Configure authentication and access control on the printer.....	33
Enable copy locking using SafeCom copy cable.....	33

Enable extensible services browser.....	34
Allow login by code on the printer.....	34
Add the device in SafeCom Administrator.....	34
Xerox ColorQube 87xx, 89xx.....	35
Create certificate on the printer.....	35
Enable HTTPS on the printer.....	35
Enable Extensible Service Registration on the printer.....	35
Configure authentication and access control on the printer.....	36
Enable extensible services browser.....	36
Allow login by code on the printer.....	36
Add the device in SafeCom Administrator.....	36
Xerox WorkCentre 52xx, 73xx and 74xx.....	37
Set up the printer.....	37
Create certificate and enable SSL on the printer.....	37
Enable custom services.....	38
Enable ports.....	38
Configure authentication and access control on the printer.....	38
Allow login by code on the printer.....	39
Add the device in SafeCom Administrator.....	39
Allow device error messages to appear on 73xx.....	40
Xerox WorkCentre 72xx.....	40
Set up the printer.....	40
Create certificate and enable SSL on the printer.....	40
Enable Extensible Service Registration on the printer.....	41
Enable HTTPS on the printer.....	41
Setup Extensible Service on the printer.....	41
Allow login by code on the printer.....	42
Set User Permissions.....	42
Allow Pull Print.....	42
Allow Tracking.....	42
Set Default Landing Screen.....	43
Add the device in SafeCom Administrator.....	43
Xerox WorkCentre 64xx.....	43
Set up the printer.....	43
Create certificate on the printer.....	43
Enable HTTPS on the printer.....	44
Enable Extensible Service Registration on the printer.....	44
Configure authentication and access control on the printer.....	44

Allow login by code on the printer.....	45
Add the device in SafeCom Administrator.....	45
Xerox WorkCentre 57xx.....	45
Create certificate on the printer.....	45
Enable HTTPS on the printer.....	46
Enable Extensible Service Registration on the printer.....	46
Configure authentication and access control on the printer.....	46
Allow login by code on the printer.....	47
Add the device in SafeCom Administrator.....	47
Xerox WorkCentre 56xx.....	48
Set up the printer.....	48
Create certificate and Enable SSL on the printer.....	48
Enable custom services on the printer.....	49
Enable web services on the printer.....	49
Configure authentication and access control on the printer.....	49
Allow login by code on the printer.....	50
Set custom services as the default entry screen.....	50
Add the device in SafeCom Administrator.....	51
Enable custom services (EIP) on older 56xx.....	51
Xerox Workcentre 53xx.....	51
Set up the printer.....	51
Create certificate and enable SSL on the printer.....	51
Enable extensible services and extensible services browser.....	52
Allow login by code on the printer.....	52
Add the device in SafeCom Administrator.....	53
Configure authentication and access control on the printer.....	53
Xerox WorkCentre Pro 2xx.....	54
Set up the printer.....	54
Create certificate and enable SSL on the printer.....	54
Enable custom services on the printer.....	55
Configure authentication and access control on the printer.....	55
Allow login by code on the printer.....	56
Add the device in SafeCom Administrator.....	56
Check EIP hardware on WorkCentre Pro 2xx.....	56
Xerox Phaser 3635MFP.....	58
Set up the printer.....	58
Enable USB card reader.....	58
Create certificate and Enable SSL on the printer.....	58

Enable custom services on the printer.....	59
Add the device in SafeCom Administrator.....	59
Configure authentication and access control on the printer.....	59
Allow login by code on the printer.....	60
Xerox WorkCentre 3655, 4265, 5945, 5955, 6655, 7970.....	60
Set up the printer.....	60
Create certificate on the printer.....	60
Enable HTTPS on the printer.....	61
Enable Extensible Service Registration on the printer.....	61
Configure authentication and access control on the printer.....	61
Allow login by code on the printer.....	61
Add the device in SafeCom Administrator.....	62
Chapter 3: SafeCom Device Server.....	63
Install SafeCom Device Server.....	63
Windows firewall – Ports that must be opened.....	63
Configure SafeCom Device Server.....	65
Log in to SafeCom Device Server.....	65
Add SafeCom Server.....	66
Device Server config.ini.....	67
Add device to the SafeCom Device Server.....	68
Device icons.....	69
Add device through the SafeCom Administrator.....	69
Add device through the SafeCom Device Server.....	70
Configure device in SafeCom Device Server.....	70
Check device properties.....	75
Installing USB plug-in for keyboard emulating card readers.....	75
Enable the plug-in feature on the device.....	75
Retrieve the USB Card Reader Plug-in.....	76
Upload the USB Card Reader Plug-in.....	76
Activate the plug-in.....	77
Configure the device to use USB card reader plug-in for authentication.....	77
Chapter 4: SafeCom Controller.....	79
Install SafeCom Controller.....	79
Write down the IP address of the device.....	79
Connect hardware.....	79
Add device in SafeCom Administrator.....	80
Enable copy tracking.....	81
SafeCom Go Xerox Controller Web Interface.....	81

Log in to the SafeCom Controller Web Interface.....	82
Advanced Configuration web page.....	82
SafeCom web page.....	82
Printer web page.....	83
Chapter 5: SafeCom Go Xerox - How to.....	86
SafeCom Go Xerox on Device Server.....	86
Enable Plug-in Settings on device web page.....	86
Select login method.....	86
Register device.....	87
Enable SafeCom Mobile Pull Print.....	87
Restore factory default.....	87
Use Device trace facility.....	88
Uninstall SafeCom Go Xerox.....	89
SafeCom Go Xerox on Controller.....	89
Specify SafeCom server and printer connection.....	89
Set password to prevent unauthorized access.....	89
Assign a fixed IP address to the SafeCom Controller.....	90
Register device.....	90
Restore factory default.....	90
Uninstall SafeCom Go Xerox.....	90
Make all printing go through SafeCom.....	90
Enable force logout.....	91
Resend configuration.....	91
Manually upgrade DLM File.....	91
Configure multiple SafeCom Controllers.....	91
Chapter 6: Set up network accounting.....	92
Xerox WorkCentre 5330, 7120 and 7125.....	92
Enable Xerox Network Accounting.....	92
Xerox ColorQube 92xx and 93xx.....	92
Enable Xerox Network Accounting.....	92
Disable prompts for accounting codes.....	92
Xerox WorkCentre 75xx.....	93
Enable Xerox Network Accounting.....	93
Disable Code Entry Validation.....	93
Xerox WorkCentre 56xx and WorkCentre Pro 2xx.....	93
Enable Xerox Network Accounting.....	93
Disable Network Accounting Authentication.....	93
Chapter 7: Using SafeCom Go Fuji Xerox.....	94

Xerox WorkCentre 71xx, 74xx, and 75xx.....	94
Login.....	94
Pull Print - Document list.....	95
Copy.....	96
Logout.....	96
Register card at device with Windows credentials.....	96
Register card with PUK code.....	96
Xerox WorkCentre 76xx and 77xx.....	97
Control Panel.....	97
Login.....	97
Pull Print - Document list.....	98
Copy.....	99
Logout.....	100
Register card with PUK code.....	100
Xerox WorkCentre 52xx, 72xx, 73xx and 74xx.....	100
Control Panel.....	100
Login.....	100
Pull Print - Document list.....	101
Copy.....	102
Logout.....	103
Register card with PUK code.....	103
Xerox WorkCentre 56xx.....	103
Control Panel.....	103
Login.....	103
Pull Print - Document list.....	104
Copy.....	105
Logout.....	106
Register card with PUK code.....	106
Xerox WorkCentre 2xx.....	106
Control Panel.....	106
Login.....	106
Pull Print - Document list.....	107
Copy.....	108
Logout.....	109
Register card with PUK code.....	109
Chapter 8: Troubleshooting.....	110
SafeCom Help Desk Assistant.....	110
Servlets.....	110

Copy jobs are not tracked.....	110
No communication between SafeCom controller and printer.....	111
Cannot access properties tab on printer's web page.....	111
At the printer: Cannot access the Tools menu.....	111
At the printer: Error message: "Communication error" at login.....	111
At the printer: cannot enter Billing screen.....	111
Device Server: Configuration of devices failed.....	112
Device Server: "Unable to configure device because: Device is configured against a different server".....	112
Device Server: Error when upgrading existing Device Server installation.....	112
Native device functions are not tracked.....	113
Chapter 9: Regulatory information.....	114

Preface

This guide is intended for administrators who are responsible for integrating Kofax SafeCom software for use with Xerox MFP devices.

Training


Kofax offers both classroom and online training to help you make the most of your product. To learn more about training courses and schedules, visit the [Kofax Education Portal](#) on the Kofax website.

Getting help with Kofax products

The [Kofax Knowledge Base](#) repository contains articles that are updated on a regular basis to keep you informed about Kofax products. We encourage you to use the Knowledge Base to obtain answers to your product questions.

To access the Kofax Knowledge Base:

1. Go to the [Kofax website](#) home page and select **Support**.
2. When the Support page appears, select **Customer Support > Knowledge Base**.

 The Kofax Knowledge Base is optimized for use with Google Chrome, Mozilla Firefox, or Microsoft Edge.

The Kofax Knowledge Base provides:

- Powerful search capabilities to help you quickly locate the information you need.
Type your search terms or phrase into the **Search** box, and then click the search icon.
- Product information, configuration details, and documentation, including release news.
Scroll through the Kofax Knowledge Base home page to locate a product family. Then click a product family name to view a list of related articles. Please note that some product families require a valid Kofax Portal login to view related articles.

From the Knowledge Base home page, you can:

- Access the Kofax Community (for all customers).
Click the **Community** link at the top of the page.
- Access the Kofax Customer Portal (for eligible customers).

Click the **Support** link at the top of the page. When the Customer & Partner Portals Overview appears, click **Log in to the Customer Portal**.

- Access the Kofax Partner Portal (for eligible partners).

Click the **Support** link at the top of the page. When the Customer & Partner Portals Overview appears, click **Log in to the Partner Portal**.

- Access Kofax support commitments, lifecycle policies, electronic fulfillment details, and self-service tools.

Go to the **General Support** section, click **Support Details**, and then select the appropriate tab.

Chapter 1

Introduction

SafeCom Go Xerox

SafeCom Go Xerox is the embedded solution for Xerox printers. It integrates with the touch-screen control panel of the Xerox printer and offers user authentication by code and/or card.

SafeCom Go Xerox works together the SafeCom G4 Server software and is designed to help companies and organizations gain control over their printing costs and document security. The SafeCom solution can be enhanced with add-on modules to build customer-specific, scalable solutions.

Requirements

- SafeCom Go Xerox supports all printers listed:
https://knowledge.kofax.com/MFD_Productivity/00_Supported_Devices/Supported_Devices
The printers must be EIP-enabled.
- SafeCom Go device license.
- The SafeCom Device Server requires Java Runtime Environment (JRE) version 1.7 or later. If SafeCom Device Server is installed on a 64-bit operating system, a Java version 32-bit needs to be installed. Is included in the installer and is automatically deployed.
- If keyboard emulated readers are to be installed on;
 - WorkCentre 5325, 5330, 5335
 - WorkCentre 7120, 7125
 - WorkCentre 7425, 7428, 7435

running on device server, a USB card reader plug-in must be installed on the device. Please see [Installing USB plug-in for keyboard emulating card readers](#).

i Minimum firmware requirements must be met for the devices to have keyboard emulating USB card readers installed.

SafeCom ID devices

SafeCom Go Xerox supported SafeCom ID devices

Keyboard emulating ID devices
Kofax MX Proximity Reader, USB ¹
Kofax Micro Multi-Card Reader, USB, KBD ²
SafeCom AWID Reader, USB, KBD, [R]
SafeCom Casi-Rusco Reader, USB, KBD, [R]
SafeCom EM Reader, USB, KBD, [E]
SafeCom Felica Reader, USB, KBD, [R]
SafeCom HID Prox Reader, USB, KBD, [R]
SafeCom iCLASS Reader, USB, KBD, [R]
SafeCom Indala Reader, USB, KBD, [R]
SafeCom Indala Reader 29 bit, USB, KBD, [R]
SafeCom Inditag Reader, USB, KBD, [E]
SafeCom IoProx Reader, USB, KBD, [R]
SafeCom Legic Reader, USB, KBD, [R]
SafeCom Mag. Reader DD, USB Tr1, KBD ³
SafeCom Mag. Reader DD, USB Tr2, KBD ³
SafeCom Mag. Reader DD, USB Tr3, KBD ³
SafeCom Mifare Reader, USB, KBD, [E]
SafeCom MultiISO Reader, USB, KBD, [E]
SafeCom NexWatch Reader, USB, KBD, [R]

The ID device is either fitted or supplied with a 1.8 - 2.0 m cable. Additional information about the ID devices is available in the *SafeCom G4 Administrator's Guide*.

¹ The MX Reader only works with ConnectKey-compatible devices having the requisite firmware. For more information, contact your Xerox reseller or representative.

² Ensure that the **XSA > Embedded** setting is enabled on the web configuration interface of the device.

³ The SafeCom Mag. Reader DD requires use of either SafeCom ID Controller or SafeCom Controller.



- Be aware that the sleep mode of Versalink devices disables the card reader attached to the device, so wake up through cardswipe does not work.
- To run keyboard emulating USB card readers on Xerox WorkCentre 5325, 5330, 5335, 7120, 7125, 7425, 7428, 7435, see [Installing USB plug-in for keyboard emulating card readers](#).
- ID devices require unique ID device licenses. SafeCom ID devices come with ID device licenses, whereas ID device licenses for third-party ID devices must be purchased separately.

Xerox global print driver

Xerox Global Print Driver (X-GPD) is available for PCL5, PCL6, and PostScript at xerox.com/global and can be used with SafeCom Pull Print if bi-directional communication is disabled. The PostScript version is recommended in all scenarios.

Supported languages

The languages, with their postfixes, listed below are supported by SafeCom.

Postfix	Language
<i>None</i>	English
da	Danish
de	German
es	Spanish
fr	French
it	Italian
iw	Hebrew
ja	Japanese
ko	Korean
nl	Dutch
no	Norwegian
sv	Swedish
zh	Chinese
zh_tw	Chinese, Taiwan

Chapter 2

Install SafeCom Go Xerox

This chapter covers how to set up and configure various Xerox devices to SafeCom Go Xerox.

Depending on the device model and the configuration, be aware of the following issues:

- Authentication by ID code varies between the Xerox device series, so a different login process should be expected. If possible, limit variety in the selection of Xerox devices.
- With **Xerox Network Accounting** enabled on the Xerox device, it is possible to track E-mail, Scan, and Fax and to do detailed tracking of page sizes for copy and print jobs. Furthermore, post tracking of Pull Print jobs is without delay between jobs. How to setup **Xerox Network Accounting** is covered in chapter 6.

For devices without **Xerox Network Accounting** enabled, tracking of copy and Pull Print jobs is done through SNMP.

If SafeCom is enabled through the **SafeCom Controller**, it is possible to do tracking through both **Xerox Network Accounting** and SNMP. However, if SafeCom is enabled through the **SafeCom Device Server**, it is only possible to do tracking through **Xerox Network Accounting**. If **Xerox Network Accounting** is not setup, when using **SafeCom Device Server**, tracking cannot be done.

i If tracking is done through SNMP, then all copy jobs made within a single login session is tracked as one job.

Xerox Altalink

Create certificate on the printer

Be aware that when you create a certificate on the printer, it might take a few hours before the certificate becomes valid.

To create a certificate:

1. Open the printer's web page and click on the **Properties** tab. Enter the Device Administrator Password to log in.
2. Click **Security** and then **Certificates** on the menu. View the **Xerox Digital Certificate** area and confirm that the **Status** of the **Xerox Digital Certificate** indicates that the printer does not have a Certificate established on the printer. If a certificate is established, proceed to enable HTTPS.

3. Click **Create New Xerox Device Certificate**.
4. Select **Self Signed Certificate**. Click **Continue**.
5. The maximum **Days of Validity** allowed are 1800.
6. Select the Hash Algorithm.
7. Click **Finish**.

After creating the certificate, check the date and time for when the certificate becomes valid on the device web page by clicking the certificate in the address field. Click View certificates, then the Details tab and make a note of the Valid from and Valid to dates and times.

Enable HTTPS on the printer

1. Open the printer's web page and click on the **Properties** tab.
2. Click **Connectivity > Setup** and then **Edit** the **HTTP** settings and check that **Force Traffic over Secure Connection (HTTPS)** is enabled on port 443.
3. Click **Save**.
4. Click **OK** to restart the device's web server.
5. Click **Reboot Machine**. Click **OK** to reboot.

Enable Extensible Service Registration on the printer

1. Open the printer's web page and click on the **Properties** tab. See [Cannot access properties tab on printer's web page](#) if you have problems accessing the **Properties** tab.
2. Click **General Setup** and then **Extensible Service Setup**.
3. In **Extensible Service Registration** click **Edit**. Scroll down to Remote System Management and select **Enable** next to **Extensible Service Registration**.
4. Click **Save**.

Set up Extensible Service on the printer

1. Open the printer's web page and click on the **Properties** tab.
2. Click **General Setup > Extensible Service Setup**.
3. Check **Export password to Extensible Services**.
4. Check **Enable the Extensible Services Browser**.
5. Check **Verify server certificates**.
6. Click **Apply**.

Allow login by code on the printer

If users are to log in by card only then nothing needs to be configured. However, if users are to log in by entering an ID code on the printer's control panel then the printer must be configured to allow keyboard access.

1. Open the printer's web page and click on the **Properties** tab.
2. Click **Login/Permissions/Accounting > Login Methods > Xerox Secure Access Setup**, and then click **Edit**.

3. Click **Manually Override Settings**.
4. Under **Device Login Methods**, select **Xerox Secure Access Device + alternate on-screen authentication method**.
5. Click **Save**, then **Close**.
6. Click **Reboot Machine**. Click **OK** to reboot.

Add the device in SafeCom Administrator

1. Make sure the SafeCom server software installation has been completed.
2. Add a device either through the **SafeCom Administrator** (this is the preferred method) or through the **SafeCom Device Server**.
3. Configure the device.

Configure authentication and access control on the printer

1. Open the printer's web page and click on the **Properties** tab.
2. Click **Login/Permissions/Accounting > Login Methods**, and then click **Edit** for **Control Panel & Website Login Methods**.
3. For **Control Panel Login**, select **Xerox Secure Access** from the dropdown list.
4. Click **Save**.
5. Reboot the device if prompted.
6. Click **Login/Permissions/Accounting > User Permissions**, and then click the **Edit** for **User Permission Roles**.
7. Click **Edit** for **Non-Logged-In Users**.
8. On the **Apps&Tools** tab, ensure that all applications that require authentication are set to **Not Allowed**.

Xerox Versalink

Create certificate on the printer

Be aware that when you create a certificate on the printer, it might take a few hours before the certificate becomes valid.

To create a certificate:

1. Open the printer's web page log in and click on the **System** tab.
2. Click **Security** and then **Security Certificates** on the menu. If a certificate is established, proceed to enable HTTPS.
3. Select **Device Certificates** and click **Create**.
4. Select **Create Self-Signed Certificate**.
5. Click **Finish**.

After creating the certificate, check the date and time for when the certificate becomes valid on the device web page by clicking the certificate in the address field. Click View certificates, then the Details tab and make a note of the Valid from and Valid to dates and times.

Enable HTTPS on the printer

1. Open the printer's web page and click on the **System** > **Connectivity** tab.
2. Click **HTTP** and check that **HTTPS (SSL)** is enabled on port 443.
3. Click **Ok**.
4. Click **OK** to restart the device's web server.
5. Click **Reboot Machine**. Click **OK** to reboot.

Add the device in SafeCom Administrator

1. Make sure the SafeCom server software installation has been completed.
2. Add a device either through the **SafeCom Administrator** (this is the preferred method) or through the **SafeCom Device Server**.
3. Configure the device.

Configure authentication and access control on the printer

1. On the device webpage, select **Log In**, and then log in to the device as **Admin**.
2. Select **Permissions**.
3. Click **Edit** on **Guest Access**.
4. Select **Device User Role**.
5. Under **Control Panel Permissions**, select **Custom Permissions** and click **Setup**.
6. Select **PullPrint** then select **Restrict**. Click **OK**.
7. Select **Account** then select **Restrict**. Click **OK**.
8. Optionally, repeat this for all functions you want to lock.
9. Click **Close**, then **OK**. The device restarts automatically.

Allow login by card on the printer

You can download the required files from the Xerox website, or contact your supplier for providing the relevant files.

1. Activate the Plug-in feature:
 - a. On the device webpage, select **Log In**, and then log in to the device as **Admin**.
 - b. Select **System**.
 - c. Select **Plug-in Settings**.
 - d. Slide **Plug-in Feature** to the right to the checked position.
 - e. Select **Restart Now** when prompted.

2. Enable Convenience Authentication Plugin:
 - a. Extract all files from the zip file to a convenient location on your computer.
 - b. On the device webpage, select **Log In**, and then log in to the device as **Admin**.
 - c. Select **System**.
 - d. Select **Plug-in Settings**.
 - e. Select **Add**.
 - f. Browse to the location of the Generic_CardReader.jar file you previously extracted from the .zip file.
 - g. Select **OK**.
 - h. Connect your USB Convenience Authentication card reader device at this time.
 - i. Select **Close**.
 - j. Reboot the printer to activate the plug-in.
 - k. When the system is back online return to the **Plug-In settings** page and ensure that the **USB Card Reader** plug-in is **Activated**.
 - l. You can now select and configure **Convenience Authentication** through the device webpage under **Permissions > Login/Logout Settings**.

Xerox WorkCentre 7120, 7125, 7220, Xerox Color 550/560

Create certificate on the printer

Be aware that when you create a certificate on the printer, it might take a few hours before the certificate becomes valid.

To create a certificate:

1. Open the printer's web page and click on the **Properties** tab. Enter the Device Administrator Password to log in.
2. Click **Security** and then **Machine Digital Certificate Management** on the menu. View the **Machine Digital Certificate** area and confirm that the **Current Status** of the **Machine Digital Certificate** indicates that the printer does not have a Certificate established on the printer. If a certificate is established, proceed to enable HTTPS.
3. Click **Create New Certificate**.
4. Select **Self Signed Certificate**. Click **Continue**.
5. The maximum **Days of Validity** allowed are 1800 (and not 9999 as indicated).
6. Click **Apply**.
7. Disable verification of remote server certificate:
 - a. On the printer's web page, click the **Properties** tab.
 - b. In the left menu click **Security** and then **SSL/TLS Settings**.
 - c. For **Verify Remote Server Certificate**, clear the **Enabled** check box.

- d. Click **Apply**.

After creating the certificate, check the date and time for when the certificate becomes valid on the device web page by clicking the certificate in the address field. Click View certificates, then the Details tab and make a note of the Valid from and Valid to dates *and* times.

Enable HTTPS on the printer

1. Open the printer's web page and click on the **Properties** tab.
2. Click **Connectivity > Protocols > HTTP** and check that **Secure HTTP (SSL)** is enabled on port 443.
3. Click **Apply**.
4. Click **OK** to restart the device's web server.
5. Click **Reboot Machine**. Click **OK** to reboot.

Enable Extensible Service Registration on the printer

1. Open the printer's web page and click on the **Properties** tab. See [Cannot access properties tab on printer's web page](#) if you have problems accessing the **Properties** tab.
2. Click **General Setup** and then **Extensible Service Setup**.
3. In **Extensible Service Registration** click **Configure**. Scroll down to Remote System Management and select **Enable** next to **Extensible Service Registration**.
4. Click **Apply**. Click **OK**.

Set up Extensible Service on the printer

1. Open the printer's web page and click on the **Properties** tab.
2. Click **General Setup** and then **Extensible Service Setup**.
3. Check **Export password to Extensible Browser**.
4. Check **Enable the Extensible Services Browser**.
5. Check **Verify server certificates**.
6. Click **Apply**.

Allow login by code on the printer

If users are to log in by card only then nothing needs to be configured. However, if users are to log in by entering an ID code on the printer's control panel then the printer must be configured to allow keyboard access.

1. Open the printer's web page and click on the **Properties** tab.
2. Click **Security, Remote Authentication Servers** and then **Xerox Secure Access Settings**.
3. The **Xerox Secure Access Settings** web page appears.
4. Check **Enabled** for **Local Login**.
5. Click **Apply**.
6. Click **Reboot Machine**. Click **OK** to reboot.

Add the device in SafeCom Administrator

Depending on how SafeCom is enabled on these models, add the device according to the following:

If SafeCom is enabled through the SafeCom Device Server

1. Make sure the SafeCom server software installation has been completed.
2. Add a device either through the **SafeCom Administrator** (this is the preferred method) or through the **SafeCom Device Server**.
3. Configure the device.

If SafeCom is enabled through the SafeCom Controller

1. Make sure the SafeCom server software installation has been completed.
2. Connect the SafeCom Controller.
3. In **SafeCom Administrator** use **Add device** to add the SafeCom Controller. Remember to select **SafeCom Go Xerox** as the SafeCom type.
4. If relevant **Enable copy tracking** on the **Printer** web page of the SafeCom Controller.

Configure authentication and access control on the printer

1. Open the printer's web page and click on the **Properties** tab.
2. Click **Security** and then **Authentication Configuration**.
3. The **Authentication Configuration > Step 1 of 2** web page appears. In **Login type** select **Xerox Secure Access Device**.
4. Click **Apply**.
5. Click **Reboot Machine**. Click **OK** to reboot. This reboot **MUST** occur otherwise the subsequent steps cannot be performed. After the reboot continue with the remaining steps.
6. Open the printer's web page and click on the **Properties** tab.
7. Click **Security** and then **Authentication Configuration**.
8. The **Authentication Configuration > Step 1 of 2** web page appears.
9. Click **Next**. The **Authentication Configuration > Step 2 of 2** web page appears.
10. From the **Device Default State Configuration** area you can configure:
 - **Device Access**

By locking the Service Pathway (recommended) users will be requested to authenticate to access all available services: Copy, E-mail, Pull Print, and more. Proceed with [Configure device access](#).
 - **Service Access**

Instead of device access, it is possible to control access on a per-service basis. However, Pull Print must always be locked, because otherwise the SafeCom solution does not know who the user is. Proceed with [Configure service access](#).

Configure device access

Use Device Access to lock or unlock tools and features for all users:

1. Under **Device Default State Configuration**, next to **Device Access**, click **Configure**.
2. Select **Locked** for **Services Pathway** to require authentication for all services at the control panel. It is recommended to leave the **Job Status Pathway** and **Machine Status Pathway** unlocked. They control the access to the Job status and the Machine Status button.
3. Click **Apply** to accept the changes or **Undo** to retain the previous settings.

Configure service access

Use Service Access to lock, unlock or hide individual services for all users:

1. Under **Device Default State Configuration**, next to **Service Access**, click **Configure**.
2. Select **Locked (Show Icon)** for **Pull Print** so users must authenticate to access the Pull Print icon on the control panel. Select **Locked** to require authentication for any additional services. **Print** should remain unlocked.
3. Click **Apply** to accept the changes or **Undo** to retain the previous settings.

Xerox ColorQube 92xx and 93xx

Set up the printer

1. Open the printer's web page and click on the **Properties** tab.
2. Click on **General Setup** on the menu. Skip to [Create certificate on the printer](#) if **Extensible Service Setup** is in the menu. Otherwise, visit www.xerox.com search for Custom Services (EIP). Read the instructions carefully, download the DLM file that matches your printer model and perform a manual upgrade (see [Manually upgrade DLM File](#)).

Create certificate on the printer

Be aware that when you create a certificate on the printer, it might take a few hours before the certificate becomes valid.

To create a certificate:

1. Open the printer's web page and click on the **Properties** tab.
2. Click **Security** and then **Machine Digital Certificate Management** on the menu. View the **Machine Digital Certificate** area and confirm that the **Current Status** of the **Machine Digital Certificate** indicates that the printer does not have a Certificate established on the printer. If a certificate is established, proceed to [Enable HTTPS on the printer](#).
3. Click **Create New Certificate**.
4. Select **Self Signed Certificate**. Click **Continue**.
5. Complete the details required for the Self Signed Certificate. Note that the **Letter Country Code** is a required field.

i If you are able to enter **Days of Validity**, note that the maximum number of days allowed are **997** (for models where you can enter 3 digits) and **1800** (for models where you can enter 4 digits). The maximum number indicated (999 and 9999 respectively) will not create the certificate.

6. Click **Apply**. You will need the Device Administrator Password to apply the certificate.

After creating the certificate, check the date and time for when the certificate becomes valid on the device web page by clicking the certificate in the address field. Click View certificates, then the Details tab and make a note of the Valid from and Valid to dates and times.

Enable HTTPS on the printer

1. Open the printer's web page and click on the **Properties** tab.
2. Click **Connectivity, Protocols**, and then **HTTP** and check that **Secure HTTP (SSL)** is enabled on port 443.
3. Click **OK**.

Enable Extensible Service Registration on the printer

1. Open the printer's web page and click on the **Properties** tab. See [Cannot access properties tab on printer's web page](#) if you have problems accessing the **Properties** tab.
2. Click **Connectivity, Protocols**, and then **HTTP** in the menu. Select the **Web Services** tab and select **Enable** next to **Extensible Service Registration**.
3. Click **Apply**.

Setup Extensible Service on the printer

1. Open the printer's web page and click on the **Properties** tab.
2. Click **General Setup** and then **Extensible Service Setup**.
3. Check **Export password to Extensible Browser**.
4. Check **Enable the Extensible Services Browser**.
5. Check **Verify server certificates**.
6. Click **Apply**.

Configure authentication and access control on the printer

1. Open the printer's web page and click on the **Properties** tab.
2. Click **Security, Access Rights**, and then **Tools & Feature Access** on the menu.
3. Under **Presets** select **Custom Access**. Choose if the users must authenticate to use the features by locking or unlocking each feature. If you set **Service Pathway** to Unlocked or Lock, all features underneath is set to the same. Remember that **Pull Print** and **Billing** must be locked in order to work.
4. Click **Apply**.
5. Click **OK** when the properties have been saved.

Allow login by code on the printer

If users are to log in by card only then nothing needs to be configured. However, if users are to log in by entering an ID code on the printer's control panel then the printer must be configured to allow keyboard access.

1. Open the printer's web page and click on the **Properties** tab.
2. Click **Security, Access Rights** and then **Setup** on the menu.
3. The **Authentication Configuration** web page appears. In the **Current Configuration** area click the **Edit Methods** button for **Authentication**.
4. In **Device User Interface Authentication** select **Xerox Secure Access Device**.
5. Click **Save** to return to the **Authentication Configuration** web page.
6. In the **Current Configuration** area click on the **Configure** button for **Device User Interface Authentication - Xerox Secure Access**.
7. Click the **Manually Configure** button.
8. Click **Xerox Secure Access Device + alternate on-screen authentication method** to allow logging in by entering an ID code on the printer's control panel. A button labeled **Alternate Login** is displayed on the **Instructional Blocking Window**.
9. Click **Save**.

Add the device in SafeCom Administrator

Depending on how SafeCom is enabled on these models, add the device according to the following:

If SafeCom is enabled through the SafeCom Device Server:

1. Make sure the SafeCom server software installation has been completed.
2. Add a device either through the **SafeCom Administrator** (this is the preferred method) or through the **SafeCom Device Server**.
3. Configure the device.

If SafeCom is enabled through the SafeCom Controller:

1. Make sure the SafeCom server software installation has been completed.
2. Connect the SafeCom Controller.
3. In **SafeCom Administrator** use **Add device** to add the SafeCom Controller. Remember to select **SafeCom Go Xerox** as the **SafeCom type**.
4. If relevant **Enable copy tracking** on the **Printer** web page of the SafeCom Controller.

Xerox WorkCentre 77xx

Set up the printer

1. Open the printer's web page and select the **Properties** tab.


2. Click **Services** in the menu. Skip to [Create certificate on the printer](#) if **Custom Services** is in the menu. Otherwise, visit www.xerox.com search for Custom Services (EIP). Read the instructions carefully, download the DLM file that matches your printer model and perform a manual upgrade (see [Manually upgrade DLM File](#)).

Create certificate on the printer

Be aware that when you create a certificate on the printer, it might take a few hours before the certificate becomes valid.

To create a certificate:

1. Open the printer's web page and click on the **Properties** tab.
2. Click **Security** and then **Machine Digital Certificate Management** on the menu. View the **Machine Digital Certificate** area and confirm that the **Current Status** of the **Machine Digital Certificate** indicates that the printer does not have a Certificate established on the printer. If a certificate is established, proceed to [Enable HTTPS on the printer](#).
3. Click **Create New Certificate**.
4. Select the **Select Self Signed Certificate** option if not already selected.
5. Complete the details required for the Self Signed Certificate. Note that the **Letter Country Code** is a required field.

 If you are able to enter **Days of Validity**, note that the maximum number of days allowed are **997** (for models where you can enter 3 digits) and **1800** (for models where you can enter 4 digits). The maximum number indicated (999 and 9999 respectively) will not create the certificate.

6. Click **Apply**. You will need the Device Administrator Password to apply the certificate.

After creating the certificate, check the date and time for when the certificate becomes valid on the device web page by clicking the certificate in the address field. Click View certificates, then the Details tab and make a note of the Valid from and Valid to dates and times.

Enable HTTPS on the printer

1. Open the printer's web page and click on the **Properties** tab.
2. Click **Connectivity, Protocols** and then **HTTP** and check that **Secure HTTP (SSL)** is enabled on port 443.
3. Click **Apply**.
4. Click **OK** to restart the device's web server.
5. Click **Reboot Machine**. Click **OK** to reboot.

Enable Extensible Service Registration on the printer

1. Open the printer's web page and click on the **Properties** tab. See [Cannot access properties tab on printer's web page](#) if you have problems accessing the **Properties** tab.
2. Click **Connectivity, Protocols** and then **HTTP** in the menu.

3. Click **Web Services** at the top of the page. Select **Enable** next to **Extensible Service Registration**.
4. Click **Apply**. Click **OK**.

Configure authentication and access control on the printer

1. Open the printer's web page and select the **Properties** tab.
2. Click **Security > Access Rights > Tools & Feature Access**.
3. Under **Presets**, select **Custom Access**.
4. Set **Services Pathway** to **Locked** if you want SafeCom to authenticate for all services and continue to step 9. Otherwise select **Unlocked**.
5. Click **Next** to continue.
6. Select the services you wish to have locked by the SafeCom authentication system. The service named Pull Print has to be set to either **Locked** or **Hidden**.
7. Click **Next** to continue.
8. Select whether or not color copying is allowed on the printer.
This setting only applies when using the printers Local Login, so it does not matter what is selected here.
9. Click **Finished**.

Allow login by code on the printer

If users are to log in by card only then nothing needs to be configured. However, if users are to log in by entering an ID code on the printer's control panel then the printer must be configured to allow keyboard access.

1. Open the printer's web page and click on the **Properties** tab.
2. Click **Security > Access Rights > Setup**.
3. In **Authentication Configuration**, click **Next**.
4. In the **Xerox Secure Access** window, click the **Next** button.
5. For the setting **Device User Interface Authentication** click **Edit**.
6. Click **Manually Override Settings**.
7. Under **Device Login Methods** select:
 - **Xerox Secure Access Device Authentication** to allow logging in by card.
 - **Xerox Secure Access Device Authentication + alternate on-screen authentication method** to allow logging in by entering an ID code on the printer's control panel.
8. Click **Save**.

Add the device in SafeCom Administrator

With this model, SafeCom must be enabled with the [SafeCom Controller](#):

1. Make sure the SafeCom server software installation has been completed.
2. Connect the SafeCom Controller.

3. In **SafeCom Administrator** use **Add device** to add the SafeCom Controller. Remember to select **SafeCom Go Xerox** as the **SafeCom type**.
4. If relevant **Enable copy tracking** on the **Printer** web page of the SafeCom Controller.

Xerox WorkCentre 76xx

Set up the printer

1. Open the printer's web page and click on the **Properties** tab.
2. Click **Services** on the menu. Skip to [Create certificate on the printer](#) if **Custom Services** is in the menu. Otherwise, visit www.xerox.com search for Custom Services (EIP). Read the instructions carefully, download the DLM file that matches your printer model and perform a manual upgrade (see [Manually upgrade DLM File](#)).

Create certificate on the printer

Be aware that when you create a certificate on the printer, it might take a few hours before the certificate becomes valid.

To create a certificate:

1. Open the printer's web page and click on the **Properties** tab.
2. Click **Security** and then **Machine Digital Certificate Management** on the menu. View the **Machine Digital Certificate** area and confirm that the **Current Status** of the **Machine Digital Certificate** indicates that the printer does not have a Certificate established on the printer. If a certificate is established, proceed to [Enable HTTPS on the printer](#).
3. Click **Create New Certificate**.
4. Select the **Select Self Signed Certificate** option if not already selected.
5. Complete the details required for the Self Signed Certificate. Note that the **Letter Country Code** is a required field.

i If you are able to enter **Days of Validity**, note that the maximum number of days allowed are **997** (for models where you can enter 3 digits) and **1800** (for models where you can enter 4 digits). The maximum number indicated (999 and 9999 respectively) will not create the certificate.

6. Click **Apply**. You will need the Device Administrator Password to apply the certificate.
7. Click **Connectivity, Protocols** and then **HTTP** and check that **Secure HTTP (SSL)** is enabled on port 443.
8. Click **OK**.

After creating the certificate, check the date and time for when the certificate becomes valid on the device web page by clicking the certificate in the address field. Click View certificates, then the Details tab and make a note of the Valid from and Valid to dates and times.

Enable HTTPS on the printer

1. Open the printer's web page and click on the **Properties** tab.
2. Click **Services, Custom Services** and then **Custom Services** on the menu.
3. Confirm that the SSL is enabled. Otherwise, return to [Create certificate on the printer](#).
4. Select **Enabled** in the **Enablement** area and then click **Apply**.

Enable web services

1. Open the printer's web page and click on the **Properties** tab. See [Cannot access properties tab on printer's web page](#) if you have problems accessing the **Properties** tab.
2. Click **Connectivity > Protocols > HTTP** in the menu.
3. Select the **Web Services** tab and check that all **Web Services** are enabled.

Configure authentication and access control on the printer

1. Open the printer's web page and click on the **Properties** tab.
2. Go to **Security** and click **Authentication Configuration** in the menu.
3. Click **Edit** next to **Access Setup Wizard**.
4. Set **Services Pathway** to **Locked** if you want SafeCom to authenticate for all services and continue to step 9. Otherwise select **Unlocked**.
5. Click **Next** to continue.
6. Select the services you wish to have locked by the SafeCom authentication system. The service named Pull Print has to be set to either **Locked** or **Hidden**.
7. Click **Next** to continue.
8. Select whether or not color copying is allowed on the printer.
This setting only applies when using the printers Local Login, so it does not matter what is selected here.
9. Click **Finished**.

Allow login by code on the printer

If users are to log in by card only then nothing needs to be configured. However, if users are to log in by entering an ID code on the printer's control panel then the printer must be configured to allow keyboard access.

1. Open the printer's web page and click on the **Properties** tab.
2. Click **Security** and **Access Rights**. Click **Setup** submenu.
3. In **Authentication Configuration** click **Next**.
4. In the **Xerox Secure Access** window, click the **Next** button.
5. For the setting **Device User Interface Authentication** click **Edit**.
6. Click **Manually Override Settings**.
7. Under **Device Login Methods** select:
 - **Xerox Secure Access Device Authentication** to allow logging in by card. Or

- **Xerox Secure Access Device Authentication + alternate on-screen authentication method** to allow logging in by entering an ID code on the printer's control panel.
8. Click **Save**.

Add the device in SafeCom Administrator

With this model, SafeCom must be enabled with the [SafeCom Controller](#):

1. Make sure the SafeCom server software installation has been completed.
2. Connect the SafeCom Controller.
3. In **SafeCom Administrator** use **Add device** to add the SafeCom Controller. Remember to select **SafeCom Go Xerox** as the **SafeCom type**.
4. If relevant **Enable copy tracking** on the **Printer** web page of the SafeCom Controller.

Xerox WorkCentre 58xx and 78xx

Create certificate on the printer

Be aware that when you create a certificate on the printer, it might take a few hours before the certificate becomes valid.

To create a certificate:

1. Open the printer's web page and click on the **Properties** tab. Refer to [Cannot access properties tab on printer's web page](#) if you have problems accessing the **Properties** tab.
2. Click **Security** and then **Security Certificates**. If a certificate is established, proceed to [Enable HTTPS on the printer](#).
3. Click **Add**.
4. Select **Create Xerox Device Certificate**.
5. Click **Continue**.
6. Complete the form with the requested information.
7. Click **Finish**. You will need the Device Administrator Password to apply the certificate.

After creating the certificate, check the date and time for when the certificate becomes valid on the device web page by clicking the certificate in the address field. Click View certificates, then the Details tab and make a note of the Valid from and Valid to dates and times.

Enable HTTPS on the printer

1. Open the printer's web page and select the **Properties** tab. See [Cannot access properties tab on printer's web page](#) if you have problems accessing the **Properties** tab.
2. Click **Connectivity** > **Setup**.
3. On the **Connectivity** page, click **Edit** next to **HTTP**.

4. In the **Force Traffic over SSL** section on the **HTTP** page, select the **Yes (All HTTP requests will be switched to HTTPS)** radio button and check that **Port Number** 443 is used. Click **Save** and then click **OK** to restart the device's web server.
5. Click **Reboot Machine**. Click **OK** to reboot.

Enable Extensible Service Registration on the printer

1. Open the printer's web page and select the **Properties** tab. See [Cannot access properties tab on printer's web page](#) if you have problems accessing the **Properties** tab.
2. Click **Connectivity**, and then **Setup**.
3. On the **Connectivity** page click **Edit** next to **HTTP**.
4. On the **HTTP** page click **Web Services** at the top of the page.
5. Select **Enable** next to **Extensible Service Registration**. Click **Apply**. Click **OK**.

Configure authentication and access control on the printer

1. Open the printer's web page and select the **Properties** tab. See [Cannot access properties tab on printer's web page](#) if you have problems accessing the **Properties** tab.
2. Expand **Login/ Permissions/ Accounting** and click **Login Methods**.
3. On the **Manual Override** page, in the **Device Log In Methods** section select the **Xerox Secure Access Device + alternate on-screen authentication method** button.
4. On the **Manual Override** screen, in the **Device Log In Methods** section, select **Xerox Secure Access Device + alternate on-screen authentication method**.
5. Click **Save**.
6. In the **Properties** menu to the left click **User Permissions**.
7. On the **Manage User Permissions (Non-Logged-in User)** page, in the **Presets** section select the **Restrict access to all Services and Tools** radio button. Click **Apply**.

Enable copy locking using SafeCom copy cable

1. To access the relevant web page on the Xerox device use the following URL, replacing xxx.xxx.xxx.xxx with the IP address of the Xerox device:
http://xxx.xxx.xxx.xxx/diagnostics/holdFdiPrintJobs.php
If prompted for login, then log in as administrator.
2. On the web page, clear the **Hold Foreign Device Interface Network Print Jobs** check box.
3. Click **Apply**.

Enable extensible services browser

When running with a controller based SafeCom Go Xerox the Enable the Extensible Services Browser needs to be enabled, otherwise it is not possible to choose pull print at the printer.

1. Open the printer's web page and click on the **Properties** tab.
2. Click **General Setup** and then **Extensible Service Setup**.
3. Under **Browser Settings** check the **Enable the Extensible Services Browser**, and click **Apply**.

Allow login by code on the printer

If users are to log in by card only then nothing needs to be configured. However, if users are to log in by entering an ID code on the printer's control panel then the printer must be configured to allow keyboard access.

1. Open the printer's web page and select the **Properties** tab. Refer to [Cannot access properties tab on printer's web page](#) if you have problems accessing the **Properties** tab.
2. Expand **Login/ Permissions/ Accounting** and click **Login Methods**.
3. On the **Manual Override** page, in the **Device Log In Methods** section, select the **Xerox Secure Access Device + alternate on-screen authentication method** button.
4. On the **Manual Override** screen, in the **Device Log In Methods** section, select **Xerox Secure Access Device + alternate on-screen authentication method**.
5. Click **Save**.

Add the device in SafeCom Administrator

Depending on how SafeCom is enabled on these models, add the device according to the following:

If SafeCom is enabled through the SafeCom Device Server

1. Make sure the SafeCom server software installation has been completed.
2. Add a device either through the **SafeCom Administrator** (this is the preferred method) or through the **SafeCom Device Server**.
3. Configure the device.

If SafeCom is enabled through the SafeCom Controller

1. Make sure the SafeCom server software installation has been completed.
2. Connect the SafeCom Controller.
3. In **SafeCom Administrator** use **Add device** to add the SafeCom Controller. Remember to select **SafeCom Go Xerox** as the **SafeCom type**.
4. If relevant **Enable copy tracking** on the **Printer** web page of the SafeCom Controller.

Xerox WorkCentre 75xx

Create certificate on the printer

Be aware that when you create a certificate on the printer, it might take a few hours before the certificate becomes valid.

To create a certificate:

1. Open the printer's web page and click on the **Properties** tab.

2. Click **Security** and then **Security Certificates**. If a certificate is established, proceed to [Enable HTTPS on the printer](#).
3. Click **Add**.
4. Select **Create Xerox Device Certificate**.
5. Click **Continue**.
6. Complete the form with the requested information.
7. Click **Finish**. You will need the Device Administrator Password to apply the certificate.

After creating the certificate, check the date and time for when the certificate becomes valid on the device web page by clicking the certificate in the address field. Click View certificates, then the Details tab and make a note of the Valid from and Valid to dates and times.

Enable HTTPS on the printer

1. Open the printer's web page and click on the **Properties** tab.
2. Click **Connectivity > Protocols > HTTP**, and check that **Secure HTTPS** is **Enabled** on port 443.
3. Click Apply.
4. Click OK to restart the device's web server.
5. Click Reboot Machine. Click OK to reboot.

Enable Extensible Service Registration on the printer

1. Open the printer's web page and click on the **Properties** tab. See [Cannot access properties tab on printer's web page](#) if you have problems accessing the **Properties** tab.
2. Click **Connectivity, Protocols** and then **HTTP** in the menu.
3. Click **Web Services** at the top of the page. Select **Enable** next to **Extensible Service Registration**.
4. Click **Apply**. Click **OK**.

Configure authentication and access control on the printer

1. Open the printer's web page and click on the **Properties** tab.
2. Click **Security > Authentication > Tools & Feature Access**.
3. Under **Presets**, select **Custom Access**.
4. Set **Services Pathway** to **Locked** if you want SafeCom to authenticate for all services and continue to step 6. Otherwise select **Unlocked**.
5. Select the services you wish to have locked by the SafeCom authentication system. The service named **Pull Print** has to be set to either **Locked** or **Hidden**.
6. Click **Apply**.

Enable copy locking using SafeCom copy cable

1. To access the relevant web page on the Xerox device use the following URL, replacing xxx.xxx.xxx.xxx with the IP address of the Xerox device:

`http://xxx.xxx.xxx.xxx/diagnostics/holdFdiPrintJobs.php`

If prompted for login, then log in as administrator.

2. On the web page, clear the **Hold Foreign Device Interface Network Print Jobs** check box.
3. Click **Apply**.

Enable extensible services browser

When running with a controller based SafeCom Go Xerox the Enable the Extensible Services Browser needs to be enabled, otherwise, it is not possible to choose pull print at the printer.

1. Open the printer's web page and click on the **Properties** tab.
2. Click **General Setup > Extensible Service Setup**.
3. Under **Browser Settings**, check the **Enable the Extensible Services Browser**, and click **Apply**.

Allow login by code on the printer

If users are to log in by card only then nothing needs to be configured. However, if users are to log in by entering an ID code on the printer's control panel then the printer must be configured to allow keyboard access.

1. Open the printer's web page and click on the **Properties** tab.
2. Click **Security > Authentication > Setup**.
3. In **Authentication and Authorization Methods** click **Edit Methods....**
4. For the setting **Device User Interface Authentication** select **Xerox Secure Access**. Click **Save**.
5. Scroll to **Xerox Secure Access Setup** and click **Edit....**
6. Click **Manually Override Settings**.
7. Under **Device Login Methods** select:
 - **Xerox Secure Access Device Authentication** to allow logging in by card. Or
 - **Xerox Secure Access Device Authentication + alternate on-screen authentication method** to allow logging in by entering an ID code on the printer's control panel.
8. Click **Save**.

Add the device in SafeCom Administrator

Depending on how SafeCom is enabled on these models, add the device according to the following:

If SafeCom is enabled through the SafeCom Device Server

1. Make sure the SafeCom server software installation has been completed.
2. Add a device either through the **SafeCom Administrator** (this is the preferred method) or through the **SafeCom Device Server**.
3. Configure the device.

If SafeCom is enabled through the SafeCom Controller

1. Make sure the SafeCom server software installation has been completed.

2. Connect the SafeCom Controller.
3. In **SafeCom Administrator** use **Add device** to add the SafeCom Controller. Remember to select **SafeCom Go Xerox** as the **SafeCom type**.
4. If relevant **Enable copy tracking** on the **Printer** web page of the SafeCom Controller.

Xerox ColorQube 87xx, 89xx

Create certificate on the printer

Be aware that when you create a certificate on the printer, it might take a few hours before the certificate becomes valid.

To create a certificate:

1. Open the printer's web page and go to the **Properties** tab.
2. Expand **Security** and then **Certificates**. If a certificate is established, proceed to [Enable HTTPS on the printer](#).
3. Click **Security Certificates**.
4. Go to the **Xerox Device Certificate** tab.
5. Select **Create New Xerox Device Certificate**.
6. Click **OK** to the message that Secure HTTP (SSL) must be disabled and then enabled.
7. Complete the form with the requested information.
8. Click **Finish**. You will need the Device Administrator Password to apply the certificate.

After creating the certificate, check the date and time for when the certificate becomes valid on the device web page by clicking the certificate in the address field. Click View certificates, then the Details tab and make a note of the Valid from and Valid to dates and times.

Enable HTTPS on the printer

1. Open the printer's web page and go to the **Properties** tab.
2. Expand **Connectivity, Protocols** and then **HTTP**.
3. In the **Secure HTTPS** section select **Enabled**.
4. Click **OK** to restart the device's web server.

Enable Extensible Service Registration on the printer

1. Open the printer's web page and go to the **Properties** tab. See [Cannot access properties tab on printer's web page](#) if you have problems accessing the **Properties** tab.
2. Expand **Connectivity, Protocols** and then **HTTP** in the menu.
3. Click **Web Services** at the top of the page. Select **Enable** next to **Extensible Service Registration**.
4. Click **Apply**. Click **OK**.

Configure authentication and access control on the printer

1. Open the printer's web page and go to the **Properties** tab.
2. Click **Security, Authentication** and then **Setup**.
3. Next to the **Xerox Secure Access Setup** click **Edit...**
The **User Permissions** page opens.
4. On the **User Permissions** page, next to the **Non-Authenticated User** click **Edit...**
The **Manage User Permissions (Non-Authenticated User)** page opens.
5. On the **Manage User Permissions (Non-Authenticated User)** page click **Services & Tools** at the top of the page.
6. Under **Presets**, click **Custom**. Select the services you wish to have locked by the SafeCom authentication system. The service named **Pull Print** has to be set to either **Not allowed** or **Hidden**.
7. Click **Apply**.

Enable extensible services browser

When running with a controller based SafeCom Go Xerox the Enable the Extensible Services Browser needs to be enabled, otherwise, it is not possible to choose pull print at the printer.

1. Open the printer's web page and go to the **Properties** tab.
2. Expand **General Setup** and then **Extensible Service Setup**.
3. Under **Browser Settings** check the **Enable the Extensible Services Browser**, and click **Apply**.

Allow login by code on the printer

If users are to log in by card only then nothing needs to be configured. However, if users are to log in by entering an ID code on the printer's control panel then the printer must be configured to allow keyboard access.

1. Open the printer's web page and go to the **Properties** tab.
2. Expand **Security** and **Authentication**, and then select **Setup**.
3. Scroll to **Xerox Secure Access Setup** and click **Edit...**
4. Click **Manually Override Settings**.
5. Under **Device Login Methods** select:
 - **Xerox Secure Access Device Authentication** to allow logging in by card. Or
 - **Xerox Secure Access Device Authentication + alternate on-screen authentication method** to allow logging in by entering an ID code on the printer's control panel.
6. Click **Save**.

Add the device in SafeCom Administrator

With this model, SafeCom must be enabled with the [SafeCom Controller](#):

1. Make sure the SafeCom server software installation has been completed.

2. Connect the SafeCom Controller.
3. In **SafeCom Administrator** use **Add device** to add the SafeCom Controller. Remember to select **SafeCom Go Xerox** as the **SafeCom type**.
4. If relevant **Enable copy tracking** on the **Printer** web page of the SafeCom Controller.

Xerox WorkCentre 52xx, 73xx and 74xx

Set up the printer


1. Open the printer's web page and click on the **Properties** tab.
2. Click **Services** on the menu. Skip to [Create certificate and enable SSL on the printer](#) if **Custom Services** is in the menu. Otherwise, visit www.xerox.com search for Custom Services (EIP). Read the instructions carefully, download the DLM file that matches your printer model and perform a manual upgrade (see [Manually upgrade DLM File](#)).

Create certificate and enable SSL on the printer

Be aware that when you create a certificate on the printer, it might take a few hours before the certificate becomes valid.

To create a certificate:

1. Open the printer's web page and click on the **Properties** tab.
2. Click **Security** and then **Machine Digital Certificate Management** on the menu. View the **Machine Digital Certificate** area and confirm that the **Current Status** of the **Machine Digital Certificate** indicates that the printer does not have a Certificate established on the printer. If a certificate is established, proceed to [Enable custom services](#).
3. Click **Create New Certificate**.
4. Select the **Select Self Signed Certificate** option.
5. Complete the details required for the Self Signed Certificate. Note that the **Letter Country Code** is a required field.

 If you are able to enter **Days of Validity**, note that the maximum number of days allowed are **997** (for models where you can enter 3 digits) and **1800** (for models where you can enter 4 digits). The maximum number indicated (999 and 9999 respectively) will not create the certificate.

6. Click **Apply**. You will need the Device Administrator Password to apply the certificate.
7. Click **Security** and then **SSL / TLS Settings** in the menu and confirm that **HTTP - SSL / TLS Communication** is enabled.
8. Click **Connectivity** > **Protocols** > **HTTP** and check that **Secure HTTP (SSL)** is enabled on port 443.
9. Click **OK**.

i WorkCentre 73xx and 74xx devices may have newer Xerox base firmware installed. If the Custom Services option can be found under the General > Properties section of the printer webpage, this is the case.

After creating the certificate, check the date and time for when the certificate becomes valid on the device web page by clicking the certificate in the address field. Click View certificates, then the Details tab and make a note of the Valid from and Valid to dates and times.

Enable custom services

1. Open the printer's web page and click on the **Properties** tab. See [Cannot access properties tab on printer's web page](#) if you have problems accessing the **Properties** tab.
2. Click **Services, Custom Services** and then **Custom Services** on the menu.
3. Select **Enabled** in the **Enabled** area and then click **Apply**.
4. The **Custom Services** button should now be present on the touch-screen of the printer when All Services is selected. If not, you may have to power cycle the printer.

- i**
- If changes were made to the SSL settings, you may have to power cycle the printer.
 - If your WorkCentre 73xx or 74xx has a newer Xerox base firmware installed, ensure that **Services > Custom Services > Validation options > Validation** is selected, as well as the **Export user name** check box.

Enable ports

1. Open the printer's web page and click on the **Properties** tab.
2. Click the **Connectivity** and then **Port Settings**.
3. Check **SNMP, SMB, FTP Client** and **SOAP**.

Configure authentication and access control on the printer

1. Open the printer's web page and click on the **Properties** tab.
2. Click **Security** and then click **Authentication Configuration** in the menu.
3. Ensure that **Xerox Secure Access** is selected in the **Login Type** box.
4. Click **Apply**.
5. Click **Reboot Machine**. Click **OK** to reboot. This reboot must occur otherwise the subsequent steps cannot be performed. After the reboot continue with the remaining steps.
6. Open the printer's web page and click on the **Properties** tab.
7. Click **Security** and then click **Authentication Configuration** in the menu.
8. Click **Next**.
9. From the **Device Default State Configuration** area you can configure:
 - **Device Access**

By locking the Service Pathway (recommended) users will be requested to authenticate to access all available services: Copy, E-mail, Custom Services, etc. Proceed with [Use Device Access to lock or unlock tools and features for all users](#).

- **Service Access**

Instead of device access, it is possible to control access on a per-service basis. However, Custom Services must always be locked, because otherwise the SafeCom solution does not know who the user is. Proceed with [Use Service Access to lock, unlock or hide individual services for all users](#).

Use Device Access to lock or unlock tools and features for all users

1. Under **Device Default State Configuration**, next to **Device Access**, click **Configure**.
2. Select **Locked** for **Services Pathway** to require authentication for all services at the control panel. It is recommended to leave the **Job Status Pathway** and **Machine Status Pathway** unlocked. They control the access to the Job status and the Machine Status button.
3. Click **Apply** to accept the changes or **Undo** to retain the previous settings.

Use Service Access to lock, unlock or hide individual services for all users

1. Under **Device Default State Configuration**, next to **Service Access**, click **Configure**.
2. Select **Locked (Show Icon)** for **Custom Services** so users must authenticate to access the Pull Print icon on the control panel. Select **Locked** to require authentication for any additional services.
3. Click **Apply** to accept the changes or **Undo** to retain the previous settings.

Allow login by code on the printer

If users are to log in by card only then nothing needs to be configured. However, if users are to log in by entering an ID code on the printer's control panel then the printer must be configured to allow keyboard access.

1. Open the printer's web page and click on the **Properties** tab.
2. Click **Security, Remote Authentication Servers** and then **Xerox Secure Access Settings**.
3. Check **Local Login** to allow logging in by entering an ID code on the printer's control panel.
4. Click **Apply**.

Add the device in SafeCom Administrator

Depending on how SafeCom is enabled on these models, add the device according to the following:

If SafeCom is enabled through the SafeCom Device Server

1. Make sure the SafeCom server software installation has been completed.
2. Add a device either through the **SafeCom Administrator** (this is the preferred method) or through the **SafeCom Device Server**.
3. Configure the device.

If SafeCom is enabled through the SafeCom Controller

1. Make sure the SafeCom server software installation has been completed.
2. Connect the SafeCom Controller.
3. In **SafeCom Administrator** use **Add device** to add the SafeCom Controller. Remember to select **SafeCom Go Xerox** as the **SafeCom type**.
4. If relevant **Enable copy tracking** on the **Printer** web page of the SafeCom Controller.

Allow device error messages to appear on 73xx

On the 73xx series the Auto Job Promotion feature prevents dialogs with device error messages, for example paper out, paper jam, from being displayed to the user. To have the messages appear follow these steps to disable Auto Job Promotion.

1. Go to the Xerox printer.
2. Press the **Key** button to log in.
3. Log in as local administrator.
4. Press the **Settings** button.
5. Tap the **Tools** tab.
6. In **Group**, choose **Common Service Settings**.
7. Under **Features**, choose **Other Settings**.
8. Tap **Auto Job Promotion**.
9. Tap **Change Settings**.
10. Tap **Disable**.
11. Tap **Save**.
12. Press the **Key** button and select **Logout**.

Xerox WorkCentre 72xx

Set up the printer

1. On the device control panel, tap **Reset Settings**.
2. Log in to the device as administrator.
3. Go to **Tools**, then click **Software Reset**.
4. Open the printer's web page and click on the **Properties** tab.


Create certificate and enable SSL on the printer

Be aware that when you create a certificate on the printer, it might take a few hours before the certificate becomes valid.

To create a certificate:

1. Open the printer's web page, login as administrator, and click on the **Properties** tab.

2. Click **Security** and then **Certificates** on the menu.
3. Click **Create New Xerox Device Certificate**.
4. Select the **Select Self Signed Certificate** option if not already selected.
5. Complete the details required for the Self Signed Certificate. Note that the **2 Letter Country Code** is a required field.

 If you are able to enter **Days of Validity**, note that the maximum number of days allowed are **997** (for models where you can enter 3 digits) and **1800** (for models where you can enter 4 digits). The maximum number indicated (999 and 9999 respectively) will not create the certificate.

6. Click **Finish**.

After creating the certificate, check the date and time for when the certificate becomes valid on the device web page by clicking the certificate in the address field. Click View certificates, then the Details tab and make a note of the Valid from and Valid to dates and times.

Enable Extensible Service Registration on the printer

1. Open the printer's web page and click on the **Properties** tab.
2. Click the **General Setup > Extensible Service Setup**.
3. Click on **Web Services**.
4. Click **Enable All**.
5. Click **Save**.

Enable HTTPS on the printer

1. Go to **Properties > General Setup > Extensible Service Setup**, and click **EDIT** on the Extensible Service Registration.
2. Click **HTTP**.
3. Set the **Connection** to **Enabled**, the **Port Number** to 80.
4. Set the **Force Traffic over SSL** to **Yes (All HTTP requests will be switched to HTTPS)** and the **Port Number** to 443.
5. Set the **Keep Alive Timeout** to 10 seconds.
6. Set the **Choose Device Certificate** to **Default Xerox Device Certificate**.
7. Click **Save**.

Setup Extensible Service on the printer

1. Go to **Properties > General Setup > Extensible Service Setup**.
2. Check **Export Password to Extensible Services**.
3. Check **Enable the Extensible Services Browser**.
4. Check **Verify server certificates**.
5. Click **Apply**.

Allow login by code on the printer

If users are to log in by card only then nothing needs to be configured. However, if users are to log in by entering an ID code on the printer's control panel then the printer must be configured to allow keyboard access.

1. Open the printer's web page and click on the **Properties** tab.
2. Click **Login > Permissions > Accounting > Login Methods** .
3. Click **Edit**.
4. Select **Xerox Secure Access - Unified ID System** for **Touch UI Method**.
5. Select **User Name/Password - Validate on the Device** for **Web UI Method**.
6. Click **Save**.
7. Go to **Properties > Security > Authentication (Login)**.
8. Click **Edit** for **Xerox Secure Access Setup**.
9. Click **Manually Override Settings**.
10. For **Server Communication**, ensure that **IPv4** is selected, the IP address of the SafeCom Device Server is correct, and the port is set to 50002. The **Path** must be services \XeroxConvenienceAuth, and the **Enabled** option of **Embedded** must be cleared.
11. Set the **Device Log In Method** to **Xerox Secure Access Device + alternate on-screen authentication method**.
12. Set the **Accounting Information (Requires Network Accounting)** to **Automatically apply Accounting Codes from the server**.
13. Click **Save**.

Set User Permissions

1. Open the printer's web page and click on the **Properties** tab.
2. Click **Login > Permissions > Accounting > User Permissions > Non-Logged-In Users** .
3. Click **Edit** for **Non-Logged-In User**.
4. Select **Services and Tools**.
5. Select **Restrict Access to Everything**.
6. Click **Save**.

Allow Pull Print

1. Open the printer's web page and click on the **Properties** tab.
2. Click **Services > Service Registration** .
3. Ensure that **Pull Print** is checked.
4. Click **Save** (if applicable).

Allow Tracking

1. Open the printer's web page and click on the **Properties** tab.
2. Click **Login > Permissions > Accounting > Accounting Method** .

3. Click **Edit** for **Accounting Workflow**.
4. Select **Capture Usage** for the services you want to track (usually, Copy Jobs, Print Jobs, Scan Jobs, and Email Jobs).
5. Click **Save**.

Set Default Landing Screen

1. Open the printer's web page and click on the **Properties** tab.
2. Click **General Setup** > **Entry Screen Defaults**.
3. Select **Pull Print** under **Services**.
4. Select **Services** under **Default Walkup Screen**.
5. Select **None (Take No Action)** under **Default Screen when Originals are Detected**.
6. Click **Save**.

Add the device in SafeCom Administrator

Depending on how SafeCom is enabled on these models, add the device according to the following:

If SafeCom is enabled through the SafeCom Device Server:

1. Make sure the SafeCom server software installation has been completed.
2. Add a device either through the **SafeCom Administrator** (this is the preferred method) or through the **SafeCom Device Server**.
3. Configure the device.

Xerox WorkCentre 64xx

Set up the printer

1. Open the printer's web page and click on the **Properties** tab.
2. Click on **General Setup** on the menu. Skip to [Create certificate on the printer](#) if **Extensible Service Setup** is in the menu. Otherwise, visit www.xerox.com search for Custom Services (EIP). Read the instructions carefully, download the DLM file that matches your printer model and perform a manual upgrade (see [Manually upgrade DLM File](#)).

Create certificate on the printer

Be aware that when you create a certificate on the printer, it might take a few hours before the certificate becomes valid.

To create a certificate:

1. Open the printer's web page and click on the **Properties** tab.
2. Click **Security** and then **Machine Digital Certificate Management** on the menu. View the **Machine Digital Certificate** area and confirm that the **Current Status** of the **Machine Digital**

Certificate indicates that the printer does not have a Certificate established on the printer. If a certificate is established, proceed to [Enable HTTPS on the printer](#).

3. Click **Create New Certificate**.
4. Select **Self Signed Certificate**. Click **Continue**.
5. Complete the details required for the Self Signed Certificate. Note that the **Letter Country Code** is a required field.

i If you are able to enter **Days of Validity**, note that the maximum number of days allowed are **997** (for models where you can enter 3 digits) and **1800** (for models where you can enter 4 digits). The maximum number indicated (999 and 9999 respectively) will not create the certificate.

6. Click **Apply**. You need the Device Administrator Password to apply the certificate.

After creating the certificate, check the date and time for when the certificate becomes valid on the device web page by clicking the certificate in the address field. Click View certificates, then the Details tab and make a note of the Valid from and Valid to dates and times.

Enable HTTPS on the printer

1. Open the printer's web page and click on the Properties tab.
2. Click Connectivity, Protocols and then HTTP and check that Secure HTTP (SSL) is enabled on port 443.
3. Click **OK**.

Enable Extensible Service Registration on the printer

1. Open the printer's web page and click on the **Properties** tab. See [Cannot access properties tab on printer's web page](#) if you have problems accessing the **Properties** tab.
2. Click **Connectivity > Protocols > HTTP** .
3. Select the **Web Services** tab and select **Enable** next to **Extensible Service Registration**.
4. Click **Apply**.

Configure authentication and access control on the printer

1. Open the printer's web page and click on the **Properties** tab.
2. Click **Security > Access Rights > Tools & Feature Access** .
3. Under **Presets** select **Custom Access** and make your selections.
4. Make sure that **Local UI Tools & CWIS Properties Tab** is set to **Locked**, otherwise it is not possible to log in with code.
5. Make sure that **Pull Print** is set to **Locked**.
6. Click **Apply**.
7. Click **OK** when the properties have been saved.

Allow login by code on the printer

If users are to log in by card only then nothing needs to be configured. However, if users are to log in by entering an ID code on the printer's control panel then the printer must be configured to allow keyboard access.

1. Open the printer's web page and click on the **Properties** tab.
2. Click **Security, Access Rights** and then **Setup** on the menu.
Step 1 of 3 steps appears.
3. If this is the first time you have configured authentication, click **Next** otherwise, click **Edit Methods**.
4. In **Device User Interface Authentication** select **Xerox Secure Access Device**.
5. Under **Web User Interface Authentication**, select **Locally on the Device (Internal Database)**.
6. Under **Authorization**, select **Locally on the Device (Internal Database)**.
7. Click **Next**.

Add the device in SafeCom Administrator

With this model, SafeCom must be enabled with the [SafeCom Controller](#):

1. Make sure the SafeCom server software installation has been completed.
2. Connect the SafeCom Controller.
3. In **SafeCom Administrator** use **Add device** to add the SafeCom Controller. Remember to select **SafeCom Go Xerox** as the **SafeCom type**.
4. If relevant **Enable copy tracking** on the **Printer** web page of the SafeCom Controller.

Xerox WorkCentre 57xx

Create certificate on the printer

Be aware that when you create a certificate on the printer, it might take a few hours before the certificate becomes valid.

To create a certificate:

1. Open the printer's web page and click on the **Properties** tab.
2. Click **Security** and then **Machine Digital Certificate Management** on the menu. View the **Machine Digital Certificate** area and confirm that the **Current Status** of the **Machine Digital Certificate** indicates that the printer does not have a Certificate established on the printer. If a certificate is established, proceed to [Enable HTTPS on the printer](#).
3. Click **Create New Certificate**.
4. Select **Self Signed Certificate**. Click **Continue**.

5. Complete the details required for the Self Signed Certificate. Note that the **Letter Country Code** is a required field.

i If you are able to enter **Days of Validity**, note that the maximum number of days allowed are **997** (for models where you can enter 3 digits) and **1800** (for models where you can enter 4 digits).The maximum number indicated (999 and 9999 respectively) will not create the certificate.

6. Click **Apply**. You will need the Device Administrator Password to apply the certificate.

After creating the certificate, check the date and time for when the certificate becomes valid on the device web page by clicking the certificate in the address field. Click View certificates, then the Details tab and make a note of the Valid from and Valid to dates and times.

Enable HTTPS on the printer

1. Open the printer's web page and click on the **Properties** tab.
2. Click **Connectivity > Protocols > HTTP** and check that **Secure HTTP (SSL)** is enabled on port 443.
3. Click **Apply**.

Enable Extensible Service Registration on the printer

1. Open the printer's web page and click on the **Properties** tab. See [Cannot access properties tab on printer's web page](#) if you have problems accessing the **Properties** tab.
2. Click **General Setup** and then **Custom Service Setup**.
3. In the **Setup (Required)** area, for **Custom Service Registration**, click on the **[Configure]** button to display the **HTTP:Web Services** web page.
4. In the **Remote System Management** area:
 - a. Check **Custom Service Registration**.
 - b. Check **Device Configuration**.
5. In the **Security Area**, check **Xerox Secure Access**.
6. Click **Save**.
7. Click **OK**.
8. In the **Enable Custom Services** area, check **Export passwords to Custom Services**.
9. In the **Browser Settings** area:
 - a. Check **Enable the Custom Services Browser**.
 - b. Check **Verify Server Certificates**.
10. Click **Apply**.
11. Click **OK**.

Configure authentication and access control on the printer

1. Open the printer's web page and click on the **Properties** tab.
2. Click **Security** and then **Authentication Configuration** on the menu.

3. Click on the **Edit Methods/Configure** button for **Authentication**.
4. In **Device User Interface Authentication** select **Xerox Secure Access**.
5. Under **Web User Interface Authentication**, select **Locally on the Device (Internal Database)**.
6. Under **Authorization**, select **Locally on the Device (Internal Database)**.
7. Click **Save**.

Allow login by code on the printer

If users are to log in by card only then nothing needs to be configured. However, if users are to log in by entering an ID code on the printer's control panel then the printer must be configured to allow keyboard access.

1. Open the printer's web page and click on the **Properties** tab.
2. Click **Security** and then **Authentication Configuration** on the menu.
3. Under **Device Login Methods** select:
 - **Xerox Secure Access Device Authentication** to allow logging in by card. Or
 - **Xerox Secure Access Device Authentication + alternate on-screen authentication method** to allow logging in by entering an ID code on the printer's control panel.
4. Click **Save**.

Add the device in SafeCom Administrator

Depending on how SafeCom is enabled on these models, add the device according to the following:

If SafeCom is enabled through the SafeCom Device Server

1. Make sure the SafeCom server software installation has been completed.
2. Add a device either through the **SafeCom Administrator** (this is the preferred method) or through the **SafeCom Device Server**.
3. Configure the device.

If SafeCom is enabled through the SafeCom Controller

1. Make sure the SafeCom server software installation has been completed.
2. Connect the SafeCom Controller.
3. In **SafeCom Administrator** use **Add device** to add the SafeCom Controller. Remember to select **SafeCom Go Xerox** as the **SafeCom type**.
4. If relevant **Enable copy tracking** on the **Printer** web page of the SafeCom Controller.

Xerox WorkCentre 56xx

Set up the printer

- 1.
2.
 1. Open the printer's web page and click on the **Properties** tab.
 2. Click **General Setup** on the menu.

i On older 56xx with firmware 21.133.xxx.xxx you need to click **Services** instead of **General Setup**.

Skip to [Create certificate and Enable SSL on the printer](#) if **Custom Services** is in the menu. Otherwise, visit www.xerox.com search for Custom Services (EIP). Read the instructions carefully, download the DLM file that matches your printer model and perform a manual upgrade (see [Manually upgrade DLM File](#)).

Create certificate and Enable SSL on the printer

Be aware that when you create a certificate on the printer, it might take a few hours before the certificate becomes valid.

To create a certificate:

1. Open the printer's web page and click on the **Properties** tab.
2. Click **Security** and then **Machine Digital Certificate Management** on the menu. View the **Machine Digital Certificate** area and confirm that the **Current Status** of the **Machine Digital Certificate** indicates that the printer does not have a Certificate established on the printer. If a certificate is established, go to step 7.
3. Click **Create New Certificate**.
4. Select the **Select Self Signed Certificate** option if not already selected.
5. Complete the details required for the Self Signed Certificate. Note that the **Letter Country Code** is a required field.

i If you are able to enter **Days of Validity**, note that the maximum number of days allowed are **997** (for models where you can enter 3 digits) and **1800** (for models where you can enter 4 digits). The maximum number indicated (999 and 9999 respectively) will not create the certificate.

6. Click **Apply**. You will need the Device Administrator Password to apply the certificate.
7. Click **Connectivity, Protocols** and then **HTTP** and check that **Secure HTTP (SSL)** is enabled on port 443.
8. Click **OK**.

After creating the certificate, check the date and time for when the certificate becomes valid on the device web page by clicking the certificate in the address field. Click View certificates, then the Details tab and make a note of the Valid from and Valid to dates and times.

Enable custom services on the printer

i If your 56xx is an older one with firmware 21.113.xxx.xxx you need to proceed as described in [Set up the printer](#).

1. Open the printer's web page and click on the **Properties** tab.
2. Click **General Setup** and then **Custom Service Setup** on the menu.
3. Confirm that the SSL is enabled. Otherwise, return to [Create certificate and Enable SSL on the printer](#).

Enable web services on the printer

1. Open the printer's web page and click on the **Properties** tab. See [Cannot access properties tab on printer's web page](#) if you have problems accessing the **Properties** tab.
2. Click **Connectivity, Protocols** and then **HTTP** in the menu. Select the **Web Services** tab and check that all Web Services are enabled.

Configure authentication and access control on the printer

1. Open the printer's web page and click on the **Properties** tab.
2. Go to **Security** and then click **Authentication Configuration** in the menu.
3. Ensure that **Xerox Secure Access** is selected under **Device User Interface Authentication**.
4. Click **Apply**.
5. Click **Reboot Machine**. Click **OK** to reboot. This reboot must occur otherwise the subsequent steps cannot be performed. After the reboot continue with the remaining steps.
6. Open the printer's web page and click on the **Properties** tab.
7. Go to **Security** and then click **Authentication Configuration** in the menu.
8. Click **Next**.
9. From here you can configure:
 - **Device Access**
By locking the Service Pathway (recommended) users will be requested to authenticate to access all available services: Copy, E-mail, Pull Print, etc. Proceed with step A1 - A3.
 - **Service Access**
Instead of device access, it is possible to control access on a per-service basis. However, Pull Print must always be locked, because otherwise the SafeCom solution does not know who the user is. Proceed with step B1 - B3.

Use Device Access to lock or unlock tools and features for all users

1. Under **Device Default State Configuration**, next to **Device Access**, click **Configure**.

2. Select **Locked for Services Pathway** to require authentication for all services at the control panel. It is recommended to leave the **Job Status Pathway** and **Machine Status Pathway** unlocked. They control the access to the **Job status** and the **Machine Status** button.
3. Click **Save**.
4. Click **Finished**.

Service Access to lock, unlock or hide individual services for all users

1. Under **Device Default State Configuration**, next to **Service Access**, click **Configure**.
2. Select **Locked/Visible** for **Custom Services** so users must authenticate to access the **Pull Print** icon on the control panel. Select **Locked** to require authentication for any additional services.
3. Click **Save**.
4. Click **Finished**.

Allow login by code on the printer

If users are to log in by card only then nothing needs to be configured. However, if users are to log in by entering an ID code on the printer's control panel then the printer must be configured to allow keyboard access.

1. Open the printer's web page and click on the **Properties** tab.
2. Click **Security** and then **Authentication Configuration**.
3. Confirm that the **Device User Interface** is set to **Xerox Secure Access**.
4. Click **Next**.
5. Click **Edit** next to **Device User Interface Authentication**.
6. Check **Enable alternate access through on-screen keyboard** to allow logging in by entering an ID code on the printer's control panel.

Set custom services as the default entry screen

1. Go to the Xerox printer.
2. Press the **Access** button to log in.
3. Tap **Login** and enter the user name and pin.
4. Tap **Tools Pathway**.
5. Tap **Screen Defaults**.
6. Tap **Entry Screen**.
7. Tap **Features**.
8. Tap **Save**.
9. Tap **Feature Defaults and Priority Order**.
10. Scroll down then select **Custom Services** and promote it to the top.
11. Tap **Save**.
12. Exit **Tools**.

Add the device in SafeCom Administrator

With this model, SafeCom must be enabled with the [SafeCom Controller](#):

1. Make sure the SafeCom server software installation has been completed.
2. Connect the SafeCom Controller.
3. In **SafeCom Administrator** use **Add device** to add the SafeCom Controller. Remember to select **SafeCom Go Xerox** as the **SafeCom type**.
4. If relevant **Enable copy tracking** on the **Printer** web page of the SafeCom Controller.

Enable custom services (EIP) on older 56xx

1. Open the printer's web page and click the **Properties** tab.
2. Click **Services > Custom Services > Custom Services** on the menu.
3. Confirm that the SSL is enabled. If not then return to step 6 in [Create certificate and Enable SSL on the printer](#).
4. Select **Enabled** in the **Enablement** area and then click **Apply**.
The Custom Services button should now be present on the touch-screen of the printer when All Services is selected. If not, you may have to power cycle the printer.

Xerox Workcentre 53xx

Set up the printer

1. Open the printer's web page and click on the **Properties** tab.
2. Click **General Setup** on the menu.

 On older 53xx click **Services** instead of **General Setup**.

Skip to [Create certificate and enable SSL on the printer](#) if **Custom Services** is in the menu. Otherwise, visit www.xerox.com and search for Custom Services (EIP). Read the instructions carefully, download the DLM file that matches your printer model and perform a manual upgrade (see [Manually upgrade DLM File](#)).

Create certificate and enable SSL on the printer

Be aware that when you create a certificate on the printer, it might take a few hours before the certificate becomes valid.

To create a certificate:

1. Open the printer's web page and click on the **Properties** tab.
2. Click **Security** and then **Machine Digital Certificate Management** on the menu. View the **Machine Digital Certificate** area and confirm that the **Current Status** of the **Machine Digital**

Certificate indicates that the printer does not have a Certificate established on the printer. If a certificate is established, proceed to *Enable custom services*.

3. Click **Create New Certificate**.
4. Select the **Select Self Signed Certificate** option if not already selected.
5. Complete the details required for the Self Signed Certificate. Note that the **Letter Country Code** is a required field.

i If you are able to enter **Days of Validity**, note that the maximum number of days allowed are **997** (for models where you can enter 3 digits) and **1800** (for models where you can enter 4 digits). The maximum number indicated (999 and 9999 respectively) will not create the certificate.

6. Click **Apply**. You will need the Device Administrator Password to apply the certificate.
7. Click **Security** and then **SSL / TLS Settings** in the menu and confirm that **HTTP - SSL / TLS Communication** is enabled.
8. Click **Connectivity > Protocols > HTTP** and check that **Secure HTTP (SSL)** is enabled on port 443.
9. Click **OK**.

After creating the certificate, check the date and time for when the certificate becomes valid on the device web page by clicking the certificate in the address field. Click View certificates, then the Details tab and make a note of the Valid from and Valid to dates and times.

Enable extensible services and extensible services browser

1. Open the printer's web page and click on the **Properties** tab. See [Cannot access properties tab on printer's web page](#) if you have problems accessing the **Properties** tab.
2. Click **General Setup** and then **Extensible Service Setup**.
3. In the **Setup (Required)** area, click **Configure**.
4. Select **Extensible Services** and click **Apply**.

i Other services are enabled by default.

5. Click **OK**.
6. In the **Enable Extensible Services** area, check the **Export password to Extensible services** check box.
7. In the **Browser Settings** area, check the **Enable Extensible Services Browser** box.
8. Click **Apply**.

Allow login by code on the printer

If users are to log in by card only then nothing needs to be configured. However, if users are to log in by entering an ID code on the printer's control panel then the printer must be configured to allow keyboard access.

1. Open the printer's web page and go to the **Properties** tab.
2. Click **Security > Remote Authentication Servers > Xerox Secure Access Settings**.

3. The **Xerox Secure Access Settings** web page appears.
4. Check **Enabled** for **Local Login**.
5. Click **Apply**.
6. Click **Reboot Machine**. Click **OK** to reboot.

Add the device in SafeCom Administrator

Depending on how SafeCom is enabled on these models, add the device according to the following:

If SafeCom is enabled through the SafeCom Device Server

1. Make sure the SafeCom server software installation has been completed.
2. Add a device either through the **SafeCom Administrator** (this is the preferred method) or through the **SafeCom Device Server**.
3. Configure the device.

If SafeCom is enabled through the SafeCom Controller

1. Make sure the SafeCom server software installation has been completed.
2. Connect the SafeCom Controller.
3. In **SafeCom Administrator** use **Add device** to add the SafeCom Controller. Remember to select **SafeCom Go Xerox** as the **SafeCom type**.
4. If relevant **Enable copy tracking** on the **Printer** web page of the SafeCom Controller.

Configure authentication and access control on the printer

1. Open the printer's web page and click on the **Properties** tab.
2. Click **Security > Authentication Configuration**.
The **Authentication Configuration > Step 1 of 2** web page appears.
3. In **Login type** select **Xerox Secure Access**.
4. Click **Apply**.
5. Click **Reboot Machine**. Click **OK** to reboot.
This reboot must occur otherwise the subsequent steps cannot be performed. After the reboot continue with the remaining steps.
6. Open the printer's web page and click on the **Properties** tab.
7. Click **Security** and then **Authentication Configuration**.
The **Authentication Configuration > Step 1 of 2** web page appears.
8. Click **Next**.
The **Authentication Configuration > Step 2 of 2** web page appears.
9. From the **Access Control** area you can configure:
 - Device Access:
By locking the Service Pathway (recommended) users will be requested to authenticate to access all available services: Copy, E-mail, Pull Print, etc. Proceed with [Use Device Access to lock or unlock tools and features for all users](#).

- Service Access:

Instead of device access, it is possible to control access on a per-service basis. However, Pull Print must always be locked, because otherwise the SafeCom solution does not know who the user is. Proceed with [Use Service Access to lock, unlock or hide individual services for all users](#).

Use Device Access to lock or unlock tools and features for all users

1. Under **Access Control**, next to **Device Access**, click **Configure**.
2. Select **Locked** for **Services Pathway** to require authentication for all services at the control panel. It is recommended to leave the **Job Status Pathway** and **Machine Status Pathway** unlocked. They control the access to the **Job status** and the **Machine Status** button.
3. Click **Apply** to accept the changes or **Undo** to retain the previous settings.

Use Service Access to lock, unlock or hide individual services for all users

1. Under **Access Control**, next to **Service Access**, click **Configure**.
2. Select **Locked (Show Icon)** for **Pull Print** so users must authenticate to access the Pull Print icon on the control panel. Select **Locked** to require authentication for any additional services. **Print** should remain unlocked.
3. Click **Apply** to accept the changes or **Undo** to retain the previous settings.

Xerox WorkCentre Pro 2xx

Set up the printer

i WorkCentre Pro 2xx requires EIP hardware (see [Check EIP hardware on WorkCentre Pro 2xx](#)).

1. Open the printer's web page and click on the **Properties** tab.
2. Click **Services** on the menu. Skip to [Create certificate and enable SSL on the printer](#) if **Custom Services** is in the menu. Otherwise, visit www.xerox.com search for Custom Services (EIP). Read the instructions carefully, download the DLM file that matches your printer model and perform a manual upgrade (see [Manually upgrade DLM File](#)).

Create certificate and enable SSL on the printer

Be aware that when you create a certificate on the printer, it might take a few hours before the certificate becomes valid.

To create a certificate:

1. Open the printer's web page and click on the **Properties** tab.

2. Click **Security** and then **SSL** on the menu. View the **Machine Digital Certificate** area and confirm that the **Current Status** of the **Machine Digital Certificate** indicates that the printer does not have a Certificate established on the printer. If a certificate is established go to step 7.
3. Click **Create New Certificate**.
4. Select the **Select Self Signed Certificate** option if not already selected.
5. Complete the details required for the Self Signed Certificate. Note that the **Letter Country Code** is a required field.

i If you are able to enter **Days of Validity**, note that the maximum number of days allowed are **997** (for models where you can enter 3 digits) and **1800** (for models where you can enter 4 digits). The maximum number indicated (999 and 9999 respectively) will not create the certificate.

6. Click **Apply**. You will need the Device Administrator Password to apply the certificate.
7. Confirm that the **SSL Protocol** is enabled on port 443 in the **Configure SSL** area. If not, then select the box and click **Apply**.
8. Click **OK**.

After creating the certificate, check the date and time for when the certificate becomes valid on the device web page by clicking the certificate in the address field. Click View certificates, then the Details tab and make a note of the Valid from and Valid to dates and times.

Enable custom services on the printer

1. Open the printer's web page and click on the **Properties** tab. See [Cannot access properties tab on printer's web page](#) if you have problems accessing the **Properties** tab.
2. Click **Services, Custom Services** and then **Custom Services** on the menu.
3. Confirm that the SSL is enabled. Otherwise, return to [Create certificate and enable SSL on the printer](#).
4. Select **Enabled** in the **Enablement** area and then click **Apply**.

The Custom Services button should now be present on the touch-screen of the printer when All Services is selected. If not, you may have to power cycle the printer.

Configure authentication and access control on the printer

1. Open the printer's web page and click on the **Properties** tab.
2. Click **Security, Authentication Server** and then **General** on the menu.
3. Under **Feature Coverage** there are two options:
 - **All Features**: This makes SafeCom control all features on the printer, making the printer completely locked until a user is logged in. Furthermore, the fact that SafeCom controls all services, gives the user a more consistent user experience.
 - **Scanning Features Only**: This leaves the copying screen open, but will still demand login for other services, e.g. Email and Custom Services (and SafeCom Pull Print).

i It is recommended to select access control **All Features**. Selecting **Scanning Features Only** leaves the copy function with no access control.

Allow login by code on the printer

If users are to log in by card only then nothing needs to be configured. However, if users are to log in by entering an ID code on the printer's control panel then the printer must be configured to allow keyboard access.

1. Open the printer's web page and click on the **Properties** tab.
2. Click **Security, Authentication Server > General** .
3. Scroll to **Login Initiation** and check **Allow Local User Interface Initiation** to allow logging in by entering an ID code on the printer's control panel.

Add the device in SafeCom Administrator

With this model SafeCom must be enabled with the SafeCom Controller:

1. Make sure the SafeCom server software installation has been completed.
2. Connect the SafeCom Controller.
3. In **SafeCom Administrator** use **Add device** to add the SafeCom Controller. Remember to select **SafeCom Go Xerox** as the **SafeCom type**.
4. If relevant **Enable copy tracking** on the **Printer** web page of the SafeCom Controller.

Check EIP hardware on WorkCentre Pro 2xx

The Xerox EIP hardware is located on the rear top left side, and it is connected with a USB cable to the formatter on the rear bottom left side.



Xerox Phaser 3635MFP

Set up the printer

i Phaser 3635MFP may require EIP hardware.

To establish whether your Phaser 3635MFP is EIP ready, look at the Configuration Report under the Web Services section. If Custom Services is not listed here your Phaser 3635MFP is not EIP ready.

1. Open the printer's web page and click on the **Properties** tab.
2. Click **Services** on the menu.
3. Skip to [Create certificate and Enable SSL on the printer](#) if **Custom Services** is in the menu. Otherwise, visit www.xerox.com search for Custom Services (EIP). Read the instructions carefully, download the DLM file that matches your printer model and perform a manual upgrade (see [Manually upgrade DLM File](#)).
4. If after the manual upgrade **Custom Services** is still not in the menu, please contact Xerox to find out if additional hardware is needed.

Enable USB card reader

1. At the printer, log in with administrator credentials.
2. Press the **Machine Status** button.
3. Select the **Tools > User Interface > General > SFO** .
4. Go to **SFO 35** and select it, then press the **Enable** button.
The **SFO 35** now indicates **Yes**.
5. Save and log out.

i The only way to establish whether the USB card reader is enabled is to verify that the SFO 35 reads Yes.

Create certificate and Enable SSL on the printer

Be aware that when you create a certificate on the printer, it might take a few hours before the certificate becomes valid.

To create a certificate:

1. Open the printer's web page and click on the **Properties** tab.
2. Click **Security** and then **Machine Digital Certificate** on the menu. View the **Machine Digital Certificate** area and confirm that the **Current Status** of the **Machine Digital Certificate** indicates that the printer does not have a Certificate established on the printer. If a certificate is established, go to step 7.
3. Click **Create New Certificate**.

4. Select the **Select Self Signed Certificate** option if not already selected.
5. Complete the details required for the Self Signed Certificate. Note that the **Letter Country Code** is a required field.

i If you are able to enter **Days of Validity**, note that the maximum number of days allowed are **997** (for models where you can enter 3 digits) and **1800** (for models where you can enter 4 digits). The maximum number indicated (999 and 9999 respectively) will not create the certificate.

6. Click **Apply**. You will need the Device Administrator Password to apply the certificate.
7. Click **Connectivity, Protocols** and then **HTTP** and check that **Secure HTTP (SSL)** is enabled on port 80.
8. Click **OK**.

After creating the certificate, check the date and time for when the certificate becomes valid on the device web page by clicking the certificate in the address field. Click View certificates, then the Details tab and make a note of the Valid from and Valid to dates and times.

Enable custom services on the printer

1. Open the printer's web page and click on the **Properties** tab.
2. Click **Services** and then **Custom Services** on the menu.
3. Confirm that the **Customer Services** is enabled. Click **Apply**. Otherwise, return to [Create certificate and Enable SSL on the printer](#).

Add the device in SafeCom Administrator

Depending on how SafeCom is enabled on these models, add the device according to the following:

If SafeCom is enabled through the SafeCom Device Server

1. Make sure the SafeCom server software installation has been completed.
2. Add a device either through the **SafeCom Administrator** (this is the preferred method) or through the **SafeCom Device Server**.
3. Configure the device.

If SafeCom is enabled through the SafeCom Controller

1. Make sure the SafeCom server software installation has been completed.
2. Connect the SafeCom Controller.
3. In **SafeCom Administrator** use **Add device** to add the SafeCom Controller. Remember to select **SafeCom Go Xerox** as the **SafeCom type**.
4. If relevant **Enable copy tracking** on the **Printer** web page of the SafeCom Controller.

Configure authentication and access control on the printer

1. Open the printer's web page and click on the **Properties** tab. See [Cannot access properties tab on printer's web page](#) if you have problems accessing the **Properties** tab.

2. Click **Security > Authentication > Authentication** .
3. Ensure that **Require Network Authentication** is selected under **Setup**.
4. Ensure that **Xerox Secure Access** is selected under **General**.
5. Click **Apply**.
6. Reboot the machine

Allow login by code on the printer

If users are to log in by card only then nothing needs to be configured. However, if users are to log in by entering an ID code on the printer's control panel then the printer must be configured to allow keyboard access.

1. Open the printer's web page and click on the **Properties** tab.
2. Click **Security, > Authentication > Authentication** .
3. Ensure that **Allow Local User Interface Initiation** is selected under **Login information** to allow logging in by entering an ID code on the printer's control panel.
4. Click **Apply**.

Xerox WorkCentre 3655, 4265, 5945, 5955, 6655, 7970

Set up the printer

1. Open the printer's web page and click on the **Properties** tab.
2. Click on **General Setup** on the menu. Skip to [Create certificate on the printer](#) if **Extensible Service Setup** is in the menu. Otherwise, visit www.xerox.com search for Custom Services (EIP). Read the instructions carefully, download the DLM file that matches your printer model and perform a manual upgrade (see [Manually upgrade DLM File](#)).

Create certificate on the printer

Be aware that when you create a certificate on the printer, it might take a few hours before the certificate becomes valid.

To create a certificate:

1. Open the printer's web page and click on the **Properties** tab.
2. Click **Security** and then **Machine Digital Certificate Management** on the menu. View the **Machine Digital Certificate** area and confirm that the **Current Status** of the **Machine Digital Certificate** indicates that the printer does not have a Certificate established on the printer. If a certificate is established, proceed to [Enable HTTPS on the printer](#).
3. Click **Create New Certificate**.
4. Select **Self Signed Certificate**. Click **Continue**.
5. Complete the details required for the Self Signed Certificate. Note that the **Letter Country Code** is a required field.

i If you are able to enter **Days of Validity**, note that the maximum number of days allowed are **997** (for models where you can enter 3 digits) and **1800** (for models where you can enter 4 digits).The maximum number indicated (999 and 9999 respectively) will not create the certificate.

6. Click **Apply**. You will need the Device Administrator Password to apply the certificate.

After creating the certificate, check the date and time for when the certificate becomes valid on the device web page by clicking the certificate in the address field. Click View certificates, then the Details tab and make a note of the Valid from and Valid to dates and times.

Enable HTTPS on the printer

1. Open the printer's web page and click on the **Properties** tab.
2. Click **Connectivity > Protocols > HTTP** and check that **Secure HTTP (SSL)** is enabled on port 443.
3. Click **OK**.

Enable Extensible Service Registration on the printer

1. Open the printer's web page and click on the **Properties** tab. See [Cannot access properties tab on printer's web page](#) if you have problems accessing the **Properties** tab.
2. Click **Connectivity, Protocols** and then **HTTP** in the menu. Select the **Web Services** tab and select **Enable** next to **Extensible Service Registration**.
3. Click **Apply**.

Configure authentication and access control on the printer

1. Open the printer's web page and click on the **Properties** tab.
2. Click **Login/Permissions/Accounting > Login method** .
3. Select **Convenience** as the login method.
4. Navigate to **Login/Permissions/Accounting > User Permissions** .
5. Make sure that **Pull Print** is set to **Locked**.
6. Click **Apply**.
7. Click **OK** when the properties have been saved.

Allow login by code on the printer

If users are to log in by card only then nothing needs to be configured. However, if users are to log in by entering an ID code on the printer's control panel then the printer must be configured to allow keyboard access.

1. Open the printer's web page and click on the **Properties** tab.
2. Click **Security > Access Rights > Setup** .
The **Step 1 of 3** window appears.

3. If this is the first time you have configured authentication, click **Next** otherwise, click **Edit Methods**.
4. In **Device User Interface Authentication** select **Xerox Secure Access Device**.
5. Under **Web User Interface Authentication**, select **Locally on the Device (Internal Database)**.
6. Under **Authorization**, select **Locally on the Device (Internal Database)**.
7. Click **Next**.

Add the device in SafeCom Administrator


With this model SafeCom must be enabled with the SafeCom Controller:

1. Make sure the SafeCom server software installation has been completed.
2. Connect the SafeCom Controller.
3. In **SafeCom Administrator** use **Add device** to add the SafeCom Controller. Remember to select **SafeCom Go Xerox** as the **SafeCom type**.
4. If relevant **Enable copy tracking** on the **Printer** web page of the SafeCom Controller.

Chapter 3

SafeCom Device Server

SafeCom can be enabled either through the SafeCom Device Server or through the SafeCom Controller. In the following part, it is covered how SafeCom is enabled through the SafeCom Device Server.

 Refer to [Requirements](#) to see which Xerox models can be used with SafeCom Device Server.

In this chapter the following topics are covered:

- Install SafeCom Device Server
- Configure SafeCom Device Server
- Add device to the SafeCom Device Server
- Configure device in SafeCom Device Server

Install SafeCom Device Server

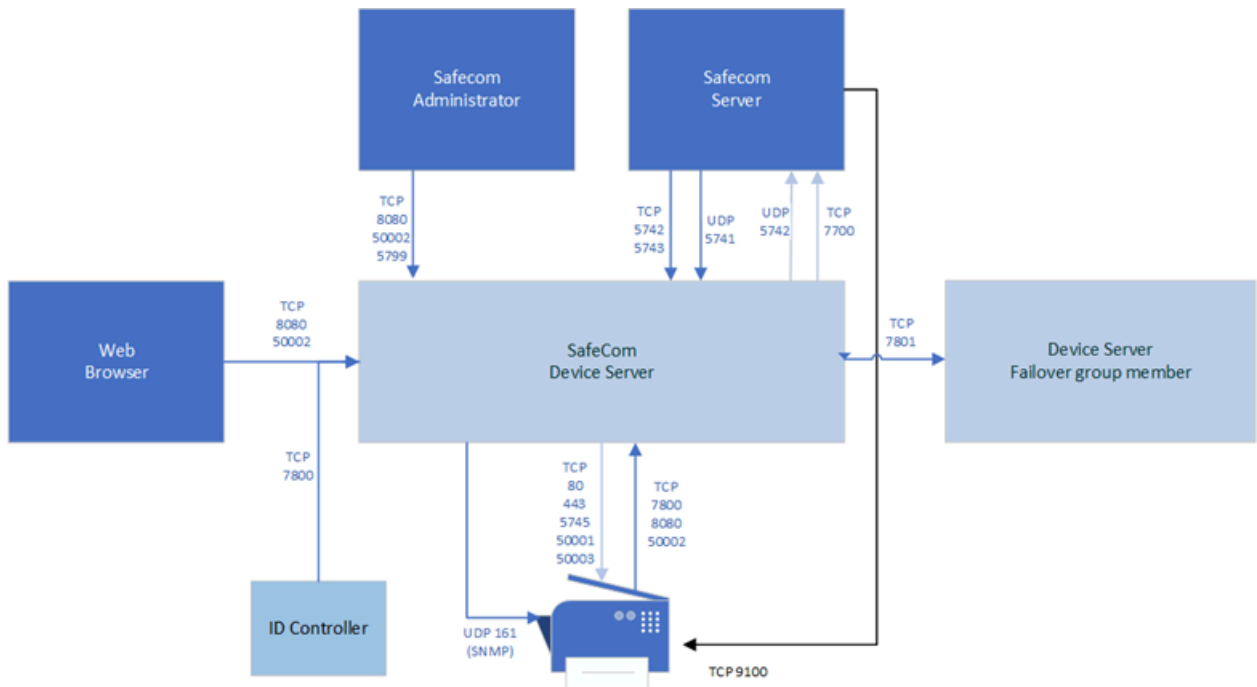
1. Download the `SafeCom_Device_Server_x64_build_{version_number}.exe` file from the link supplied to you. The installation must be **Run as administrator**.
2. When the installation program is launched, click **Next**.
3. Select the destination folder for the files. Click **Next**.
The default installation folder is `C:\Program Files\SafeCom\SafeCom Device Server`.
4. Click **Next**.
5. Review settings before copying of files starts. Click **Next**.
6. Click **Finish**.

Windows firewall – Ports that must be opened

If Windows Firewall is enabled, it may prevent the SafeCom Device Server from working. Disable the firewall or run the following script:

1. Browse to the **SafeCom Device Server** installation folder.
2. Right-click `open_firewall_safecom_device_server.cmd` and select **Run as administrator**.
You can see the opened TCP and UDP ports in the file.

You can also manually ensure that the port numbers below are open.



Inbound connections

5741	UDP	SafeCom Server: SafeCom identification
5742	TCP (RAW)	SafeCom Server: Push requests
5743	TCP (TLS 1.2)	SafeCom Server: Push requests (version 9.13 and later)
5799	TCP (RAW)	SafeCom Administrator (versions earlier than 10.6): Device status
7800	SafeCom (TCP)	SafeCom ID controller
7801	TCP (RAW)	Failover: data exchange
8080	HTTP	Device Server Web Configurator SafeCom Administrator (versions earlier than 10.6): device configuration MFP
8081	HTTP	HP OPS Server for HP Pro devices (legacy)
50002	HTTPS	SafeCom Web Configurator SafeCom Administrator (version 10.6 or later): device configuration and device status MFP

Outbound connections

161	SNMP (UDP)	Device discovery
443	HTTPS	Used to contact MFP during operation
5742	UDP	SafeCom identification (SafeCom G4 Server / Broadcast Server)
5745	TCP	HP Jedi call back
7627	HTTP	HP Jedi Web services (unsecure)
7700	TCP	SafeCom Server (Job Server), Configurable to 7500 Protocol: <ul style="list-style-type: none"> • Version 9.13 and later - Configurable TLS 1.2 or SafeCom • Versions earlier than 9.13 - SafeCom
7801	TCP (RAW)	Failover: data exchange
50001	HTTPS	MFP
50003	HTTPS	MFP (Konica Minolta)

i Make sure that the firewall script provided with G4 server is also executed and all necessary ports are open.

Configure SafeCom Device Server

SafeCom Device Server needs an active SafeCom G4 Server to work properly. If Device Server is installed on a computer running SafeCom G4 Server, then the components connect to each other automatically. Otherwise the connection must be established manually using the Device Server configuration page.

Log in to SafeCom Device Server

1. Open a web browser and enter the following URL to access the Device Server configuration page:

`https://[hostname or IP address]:50002/safecom`

Example: `https://localhost:50002/safecom`



- The use of JavaScript (Active Scripting) must be enabled.
- It is possible to use an unsecure HTTP port 8080 for this purpose (`http://localhost:8080/safecom`).

2. Enter the SafeCom Administrator's Username (default is admin) and Password (default is nimda).
3. Click **OK**.
 - If a Limited access dialog opens, click **OK**.

Add SafeCom Server

1. Open a web browser and log in to the **SafeCom Device Server**.
2. Click **Device Server** in the menu on the left.



3. Under **SafeCom Servers**, click the **[+]** icon to add one or more SafeCom Servers.
4. Enter the server address and click **OK**.
 - To add localhost as the server, leave the **Address** field blank and click **OK**.

The screenshot above indicates that the local SafeCom G4 Server is automatically connected.

If several servers are added to the list, then their order can be managed by the arrow buttons and any of them can be deleted by the [x] button. The server on the top of the list serves as the primary connection for the Device Server. The other servers get in use if the primary server is out of order. The first available one is connected in this case. Once the primary server becomes available again, Device Server connects to it automatically.

5. Configure the communication protocol. This can be custom SafeCom protocol (Legacy) or TLS 1.2.

Legacy protocol must be selected if the connected version of SafeCom servers is earlier than 10.520.10, or the TLS communication is disabled on at least one server. Otherwise TLS connection is recommended.

If both protocols are enabled, TLS is the preferred encryption. Legacy protocol is used if the G4 server does not support TLS.



- The protocol switch controls the channel encryptions between Device Server and PrintClient in the same manner.
- If the peers support TLS, but the connection cannot be established (for example, due to a TLS handshake problem, or when TLS 1.2 is not enabled), then the Legacy connection will not be used. The issue with the TLS connection must be resolved, or the TLS protocol must be disabled on the configuration page of Device Server.
- The encryption settings are common for all added G4 servers and for print clients as well.

6. Optionally, you can enable the Device Server logging feature for diagnostic purposes.

7. When all settings are configured, click **Save**.

This page can be visited at any time to change the connection settings. The asterisk after the protocol type indicates the actual protocol in use. If the protocol settings are changed, the SafeCom Device Server service must be restarted.



Device Server instances can be organized into failover groups in SafeCom Administrator. Device Servers belonging to the same group monitor the status of the group members, and when a group member fails or shuts down, the device server group distributes the workload of the downed device server among the rest of the group members. For more information, see the *Group device servers* section in the *SafeCom Administrator* chapter of [SafeCom G4 Server Administrator's Guide](#). Check the ports used by SafeCom Device Server (see [Windows firewall – Ports that must be opened](#)) to ensure the communication between group members.

The SafeCom Server is now added, and devices can be added to the device server.

Device Server config.ini

The following settings can be set by modifying the config.ini file located in the <installation folder>/equinox folder.

After editing the config.ini file, the SafeCom Device Server service must be restarted so that the changes take effect.



Do not use Windows Notepad, as it will not preserve line endings. WordPad, or another editor that understands Unix line endings, is recommended. Editing the config.ini file must be done with due diligence as otherwise it breaks the runtime.

Setting	Description	Default
deviceserver.encryptconfig	Defines if configuration file is encrypted. 'true'=enable 'false'=disable	true
deviceserver.configureddevices	Option to disable the configuration code against devices. Useful mostly for testing purposes to support simulated devices.	true
deviceserver.trace	If it is set to 'true', it enables the server trace files.	false
deviceserver.protocol.trace	If it is set to 'true', it enables the SafeCom protocol trace files.	false
deviceserver.serverAddress	Sets the address that the devices must refer to.	InetAddress.getLocalHost()
deviceserver.config.dir	Sets the location of the configuration directory.	config
deviceserver.trace.file.size	Defines the maximum size of each trace file. Defined in bytes but takes a postfix for larger units: KB, MB, or GB.	10MB
deviceserver.trace.file.count	Defines the number of old trace files to keep.	5
deviceserver.thirdparty.trace.file.size	Defines the maximum size of each third party trace file. Defined in bytes but takes a postfix for larger units: KB, MB, or GB. Set only if needed.	N/A
deviceserver.thirdparty.trace.file.count	Defines the number of third party trace files to keep. Set only if needed.	N/A
deviceserver.includedProtocols	TLS/SSL protocols can be enabled for 3rd party Jetty component with this setting. For old models of KM devices, SSLv2Hello protocol must be enabled using this value: SSLv3,TLSv1,TLSv1.1,TLSv1.2,SSLv2Hello (Comma separated list with no whitespaces).	Empty string. Jetty enables each SSL/ TLS protocol except SSLv2Hello.







Add device to the SafeCom Device Server

The device can be added to the SafeCom Device Server in one of the following two ways:

- Through the SafeCom Administrator:
This is the recommended method and it works for SafeCom G3 Server version S82 070.410*05 or higher.
- Through the SafeCom Device Server:
Solutions based on SafeCom G2 must use this method.

Device icons


In the SafeCom Device Server, the following device icons represent the status of the device.

Icon	Description
	User is logged in at the device.
	Device is idle, no user logged in.
	Wait for at least 2 minutes. If the warning signal is gone, the printer is now configured. If the warning signal remains, the printer cannot be configured because, for example the SSL is not on, or another device server is trying to configure the printer.
	An error occurred.
	The printer is receiving print data.
	Device server cannot contact the printer.

Add device through the SafeCom Administrator

Before adding a device server device in SafeCom Administrator, a SafeCom Device Server must be added to SafeCom.

If the device server is not yet added in the SafeCom Administrator, see the instructions above for configuring a SafeCom Device Server and adding it to a SafeCom Server. If the device server is already added in the SafeCom Administrator, go to the steplist below.

 To delete the device server, right-click the device server and select Delete device server, then click OK.

The SafeCom Device Server is now added to SafeCom Administrator and you can add a device.

Add a device server device

1. Click the **Devices** container, right-click the content area and select **Add device**.
The Add Device Wizard appears.
2. From the **Device server** menu, select the **SafeCom Device Server** and click **Next**.
Information is retrieved from the device server to establish the status of the device server.
3. Click **Next**.
4. Enter the **Printer address** (the device IP address or host name) and click **Next**.
Information is retrieved from the device.
5. Click **Next**.
6. Select as the type of device and click **Next**.
7. Enter the username and password as specified on the device web page, then click **Next**.
The device properties dialog box opens.



8. Make sure to specify on the **Settings** tab the device server and the capabilities of the device.
9. Click **Add** to register the device and save it in the database.


After approximately 2 minutes, the device is added to the device server and is available to be configured in the **SafeCom Device Server**.

The device server device is now added and listed both under **Devices** and under the device server under **Device servers**.

10. Go to the [Configure device in SafeCom Device Server](#) section to continue with the configuration of the device.

Add device through the SafeCom Device Server

1. Click **Device Server** in the left menu.
2. Click the **Add device**  button.
The Add Device Wizard appears.
3. Enter the hostname or the IP address of the device.
If you want to use dynamic IP address, enter the device hostname in the **Address** field.
4. Enter the administrator name and password for the device and click **Next**.
Information is retrieved from the device to establish the type of device.
5. Make the necessary adjustments to the **Required Device properties**.
6. Click **Finish**.
7. On the device settings page, make sure the settings are correct, then click **Save** .

 The device is now added to the SafeCom solution, but it does not appear in the SafeCom Administrator before a user logs in at the device.

Configure device in SafeCom Device Server

The **Device** tab is used to configure SafeCom Go Xerox with regards to which device it is connected to, how users are to be identified, and so on.

To save any changes you make to the configuration, click **Save** in the upper right corner of the web page.

Expect between 60 and 90 seconds for the saved changes to take effect if they involve changes to select settings like the **Login method**. During the update, the device icon has a yellow warning sign and the device shows the text: **Now Remote Operating. Please do not turn off the Power.**

Device Settings

Manufacturer: Xerox
 Model: Xerox WorkCentre 7830 v1 Multifunction System
 MAC Address: 9C934E2F9FD4
 Serial number: 3912833959
 Device Message:

Device information

Contact: Location:
 Description:

Network settings

Address: RAW print port:
 Select SNMP version:
 SNMP get community: SNMP put community:

Device settings

Administrator name: Administrator password:
 Login method: Default domain:
 Language:

- Hide domain
- Enable post tracking
- Reverse document list
- Mask ID code

▶ ID Controller

▶ Drivers

▼ Device properties

Property Key	Property Value
BillingEnabled	true
CheckEIPStatus	true
ForceCardSetup	false
LockFeaturesPathway	skip
LockJobStatusPathway	skip
LockMachineStatusPathway	skip
MagneticCardTrack	1
UserDefinedBlockingScreen	false

Enable logging

Change the settings according to the following descriptions:

Option	Description
<p>Device information</p>	<ul style="list-style-type: none"> • Manufacturer and Description are automatically filled-in and together with Location they are also viewable in the Device properties dialog in SafeCom Administrator. • Contact and Location provides useful information in maintaining the SafeCom solution.
<p>Network settings</p>	<ul style="list-style-type: none"> • Address: The IP address of the device. • RAW print port: The TCP port used to send print data. • Select SNMP version: These properties must match the SNMP settings of the device. First, select the SNMP version configured on the device. The SNMP related fields change according to the selected version. <ul style="list-style-type: none"> • SNMP v2: Provide SNMP Get and Put Community name. The default value of these properties is public. • SNMP v3: Provide the Username, select the Authentication protocol and enter the passphrase, select Privacy Protocol and enter the passphrase
<p>Device settings</p>	<ul style="list-style-type: none"> • Administrator name: The user name with which the administrator can log in to device. • Administrator password (mandatory): The device password with which the administrator can log in to device. • Login method: This determines how users log in. Choose between: <ul style="list-style-type: none"> • Card • ID code • Card or ID code • Card or Windows: Allows the user to log in by either card or by entering their Windows username, password, and domain. <div data-bbox="873 1507 1450 1738" style="background-color: #e0f2f7; padding: 5px; margin-top: 10px;"> <p>i Identification by card requires connecting a USB ID device (card reader). The option Card or Windows allows the user to log in by either card or by entering their Windows username, password, and domain. The SafeCom G4 server must be a member of the domain or trusted by the domain.</p> </div>

Option	Description
Default domain	Specify the domain to pre-fill the domain for users when logging into a device. If using SafeCom Mobile Pull Print the domain must be specified, as the users are not prompted for domain when logging into a device using a smart phone.
Language	Specify a specific language if you want SafeCom Device Server to override the language on the device.
Hide domain	Usable if you specified a default domain. Check to allow the users to log in without typing in the domain.
Enable post tracking	This is relevant only with SafeCom Tracking. Refer to the <i>SafeCom G4 Administrator's Manual</i> .
Reverse document list	Check to show the first printed documents at the top of the document list.
Mask ID code	Check to mask the ID code with asterisk (*)when entered at the device.
ID Controller	Select from the drop-down list which ID Controller should be associated with the device, if any. Refer to the <i>SafeCom ID Controller Administrator's Manual</i> .

Option	Description
Drivers	<p>When Pull Printing, SafeCom compares the driver name embedded in the print job with its list of driver names. If no match is found and if Show fidelity warning is checked in the Server properties in the SafeCom Administrator, the document appears with a question mark [?] in the document list. This way the user is warned that fidelity is low and the document may print incorrectly.</p> <p>Click Get All to obtain the list of drivers from the SafeCom Server, or add and delete drivers manually.</p>
Device Properties	<ul style="list-style-type: none"> • BillingEnabled: Set to True in order to enable the Account icon on the device. Set to False to remove the Account icon from the device display. • CheckEIPStatus: Default property value is 'true' which means that SafeCom Go automatically checks if the devices is EIP enabled. This might cause trouble during the configuration, in which case the property value can be set to 'false'. • ForceCardSetup: Set property value to 'true', in order to force the installation and configuration of the card reader plugin even though SafeCom Device Server might not recognise the model. Default is 'false'. • LockFeaturesPathway: Set value to 'true' to require users to log in to see the features available on the device. Set to 'false' to allow users to see the features available without logging in first. The default value is 'skip' which means that the features available are shown according to the settings on the device. • LockJobStatusPathway: Set value to 'true' to require users to log in to see the job status on the device. Set to 'false' to allow users to see the job status without logging in first. The default value is 'skip' which means that the job status is shown according to the settings on the device. • LockMachineStatusPathway: Set property value to 'true' to require users to log in to see the machine status on the device. Set to 'false' to allow users to see the machine status without logging in first. The default value is 'skip' which means that the machine status is shown according to the settings on the device. • UserDefinedBlockingScreen: Set property value to 'true' to allow custom blocking screen text. Set property value to 'false' to allow the Device Server to overwrite any user-defined custom screen texts.

Option	Description
Enable logging:	Select if log information should be collected. <div data-bbox="873 380 1451 590" style="border: 1px solid #add8e6; padding: 5px; margin-top: 10px;"> <p>i The device will always log performance data (network latency, authentication duration of successful logins, number of Out of order occurrences and duration, failover and failback between G4 servers, device reboots, changes in firmware and Go versions).</p> </div>
Restore factory default	Set all settings to their default value. Except from the password.
Reconfigure device	Reference the device to the current SafeCom Device Server.

Check device properties

If the device was added through the SafeCom Device Server it was also added to the SafeCom solution and appears in the list of devices in SafeCom Administrator.

To update the device properties in the SafeCom Administrator:

1. Click **Start**, point to **All Programs, SafeCom G4**, and click **SafeCom Administrator**.
2. In **SafeCom Administrator** click on the server to log in.
3. Enter **User logon** (default is ADMIN) and **Password** (default is nimda).
4. Open the list of devices. If the device you added is not present press F5 to refresh the list. Double-click the device to open the **Device properties** dialog.
5. On the **Settings** tab make the appropriate changes. Make sure that the Home server and Device server are specified and that the **Capabilities** are set correctly.
6. On the **Charging scheme** tab select the appropriate charging scheme.
7. On the **License** tab check the appropriate licenses.
8. Click **OK**.

Installing USB plug-in for keyboard emulating card readers

If keyboard emulating card readers are to run on the following printers/MFPs, a USB plug-in must be installed:

- 5325, 5330, 5335
- 7120, 7125
- 7425, 7428, 7435

Enable the plug-in feature on the device

1. Open an internet web browser.


2. Enter the device IP address in the address field.
3. Press **Enter** to go to CentreWare Internet Services.
4. Select the **Properties** tab.
5. If prompted, enter the system administrator user name and password.
6. Press **OK**.
7. Navigate to **Security > Plug-in Settings > Plug-in Settings** .
8. Within the **Plug-in Settings** section:
 - a. Check the Plug-in Settings **Enabled** box.
 - b. Press **Apply**.A message is displayed stating that the machine must be rebooted before the new settings can take effect.
9. Select **Reboot Machine**.
A message displays asking: "Do you want to reboot?"
10. Press **OK**.

Retrieve the USB Card Reader Plug-in

1. Download the USB Card Reader Plug-in from the Xerox software download section.
2. Double-click the cr.1.0.13.zip file to access the card reader plug-in.
3. Unzip and save the file to a location on your computer where it can be easily retrieved at a later time.

Upload the USB Card Reader Plug-in

1. Open an internet web browser.
2. Enter the device IP address in the address field.
3. Press **Enter** to go to Centroware Internet Services.
4. Select the **Properties** tab.
5. If prompted, enter the system administrator user name and password.
6. Press **OK**.
7. Navigate to **Security > Plug-in Settings > List of Embedded Plug-ins**.
8. Select the **Upload** button to display the **Plug-in** page.
9. From the Upload Plug-in page perform the following:
 - a. Press the **Browse** button.
 - b. Navigate to the location where you stored the Cardreader.jar file, select the file and press **Open**.
 - c. Press **Upload**.


 A device reboot is necessary for the plug-in to be successfully added to the device.

10. Reboot the machine.
 - a. Select the **Status** tab.

- b. Press **Reboot Machine**.
A message displays asking: "Do you want to reboot?"
- c. Press **OK**.

Activate the plug-in


1. Open an internet web browser.
2. Enter the device IP address in the address field.
3. Press **Enter** to go to CentreWare Internet Services.
4. Select the **Properties** tab.
5. If prompted, enter the system administrator user name and password.
6. Select **OK**.
7. Navigate to **Security > Plug-in Settings > List of Embedded Plug-ins** .
8. Under the **Status** heading, check the status of the plug-ins. Locate the USB Card Reader Plug-in.
9. Check the USB Card Reader plug-in and press **Start** to activate the plug-in. A message displays asking, "Do you want to start the selected plug-in?".
10. Press **OK**.
11. Recheck that the status for the plug-ins.

 The internet browser may need to be refreshed for status to reflect the current state.

12. Reboot the machine to activate the plug-in.
 - a. Select the **Status** tab.
 - b. Press **Reboot Machine**.
A message displays asking, "Do you want to reboot?"
 - c. Press **OK**.After the machine reboots, recheck the status by navigating back to the **Properties > Security > Plug-in Settings > List of Embedded Plug-ins** . The status should change to **Activated**.
13. Ensure that the correct version of the plug-in was uploaded and activated.
 - a. Select the **Card Reader Plug-in**.
 - b. Select the **Details** to view the correct version of the plug-in.
 - c. Select **Close** to return to the **List of Embedded Plug-Ins**.

Configure the device to use USB card reader plug-in for authentication

The following steps are required for the Xerox MFP to communicate with the authentication feature.

 The SSL (Secure Socket Layer) must be enabled if not already done so.

1. Open an internet browser.

2. Enter the device IP address in the address field.
3. Press **Enter** to go to CentreWare Internet Services.
4. Select the **Properties** tab.
5. If prompted, enter the system administrator user name and password.
6. Press **OK**.
7. Navigate to **Security > Authentication Configuration**.
The **Authentication Configuration > Step 1 of 2** page displays.
 - a. Select **Xerox Secure Access** from the **Login Type** drop-down menu.
The other default settings can be left alone.
 - b. Press **Apply**.
A pop-up message displays indicating loss of stored data.
 - c. Press **OK**.
 - d. Select the **Status** tab.
 - e. Press **Reboot Machine**.
A message displays asking, "Do you want to reboot?"
 - f. Press **OK**.
8. Log in to the device (repeating steps 1-5) and navigate to **Security > Authentication Configuration**.
The **Authentication Configuration > Step 1 of 2** displays.
9. Press **Next**.
The **Authentication Configuration > Step 2 of 2** page displays.
10. In the **Access Control** section, select the **Configure...** button for **Service Access**.
11. Select one of the following settings for each service you want to control:
 - **Unlocked**: This selection allows unrestricted access.
 - **Locked (Show Icon)**: This selection requires the user to log in in order to gain access. The service icon is visible to all users in the **All Services** screen.
 - **Locked (Hide Icon)**: This selection requires the user to log in in order to gain access. The service icon is hidden until an authorized user logs in.
12. Press **Apply**. If prompted, provide the system administrator user name and password.
13. Reboot the machine for new settings to take effect.
 - a. Press **Reboot Machine**.
A message displays asking, "Do you want to reboot?"
 - b. Press **OK**.

Chapter 4

SafeCom Controller

This chapter covers how to enable SafeCom through SafeCom Controller.

In this chapter the following topics are covered:

- Install SafeCom Controller
- Connect hardware
- Add device in SafeCom Administrator
- Enable copy tracking

Install SafeCom Controller

1. Make sure the SafeCom G4 Server software installation has been completed as described in the *SafeCom Smart Printing Administrator's Quick Guide*.
2. Connect the SafeCom Controller.
3. In **SafeCom Administrator** use **Add device** to add the SafeCom Controller. Remember to select **SafeCom Go Xerox** as the type of device.
4. Configure the Xerox web interface.

Write down the IP address of the device

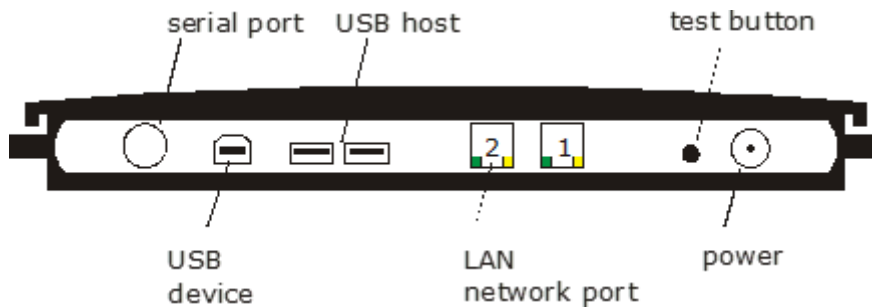
The IP address can normally be found in the device's control panel and on the configuration page. For more information, see the device's manual.

IP address /
hostname:

i The SafeCom Controller must reference the Xerox device by a fixed IP address or a fixed fully qualified hostname.

Connect hardware

Make sure that the SafeCom software installation has been completed before you connect the hardware. When powered up, the hardware automatically discovers the server software.



SafeCom Controller's rear panel

1. Switch off the power to the device.
2. Connect a network cable to the **LAN** port on the rear panel of the SafeCom Controller. Connect the other end of the cable to the network.
3. Connect a network cable to the device. Connect the other end of the cable to the SafeCom Controller's other network port.
4. Connect the SafeCom Controller and the optional SafeCom Card Reader.
5. Connect the power supply to the SafeCom Controller.
When you power on, you must wait approximately 1 minute while SafeCom initializes.
6. Switch on the power to the device.

Add device in SafeCom Administrator

The SafeCom Controller's LAN light changes from flashing to on when an IP address is set. Next you need to determine the IP address of the SafeCom Controller so you can add it to the SafeCom solution.

Find IP address through broadcasting

Use SafeCom Administrator and its Broadcast function. However, if the SafeCom Controller is on a different VLAN broadcasting will not work. In such cases you may have to configure the SafeCom Controller with a static IP address and gateway.

Find IP address in the DHCP server


Log in to the DHCP server and look up the assigned IP address based on the MAC address. The MAC address of the SafeCom Controller is printed on the white label on the bottom of the SafeCom Controller. The MAC address is a 12-digit hexadecimal number. For example, 00C076FF00F2.

1. Start SafeCom Administrator.
2. Log in to the server by double-clicking its Group name listed to the left.
3. Enter **User logon** (default is ADMIN) and **Password** (default is nimda).
4. Add a device.
 - IP address known from DHCP server: Click **Add device** and proceed to step 7.
 - Find it through Broadcasting: Click on the **Find** button and select **Devices**.
5. Click **Broadcast....**

6. Right-click on the SafeCom Controller in the list and click **Add device**.
The Add Device Wizard appears.
7. Enter the **IP address** of the SafeCom Controller. Click **Next**.
Information is retrieved from the device to establish the type of device.
8. Click **[change]** as the **SafeCom type** needs to be changed from **Other (SafeCom Controller)** to **Xerox**.
9. Select **Xerox** as the type of device. Click **Next**.
10. Enter the **Printer address** (IP address or host name) of the Xerox printer connected to the SafeCom Controller. Click **Next**.
11. Information is retrieved from the Xerox printer. Click **Next**.
12. Enter the **User name** and **Password** of the Xerox printer. Click **Next**.
13. On the **Settings** tab specify the properties of the device (**Duplex supported** and **Color supported**).
14. Click **Add** to register the device and save it in the database.

After approx. 1 minute the SafeCom Controller has restarted and you can verify the connection to the Xerox printer by pressing the test button once on the rear panel of the SafeCom Controller.

After the restart the SafeCom Pull Print icon should appear on the printer's control panel. On the 2xx and 56xx printers, the Pull Print icon will be under the Custom Services menu.

 If the Pull Print icon does not appear restart the Xerox printer, and wait until it has restarted completely. Then restart the SafeCom Controller.

Enable copy tracking

By default, copy tracking is disabled. To manually enable copy tracking, follow these steps:

1. Open the SafeCom Controller's **Printer** web page.
2. Change **Copy Enabled** to **YES** and click **Save and Continue**.
3. Click **Restart**.

 link


Tracking of E-mail and scan is not supported, and Copy jobs are only tracked if the SafeCom license includes SafeCom Tracking. For more details, see [Servlets](#)

SafeCom Go Xerox Controller Web Interface

The SafeCom Go Xerox web interface is shared with the SafeCom Controller and consists of multiple web pages, some of which can be password protected. Most web pages include online help. The web interface is available in English.

Log in to the SafeCom Controller Web Interface

1. Open a web browser and enter the IP address of the SafeCom Controller in the address field. JavaScript (Active Scripting) must be enabled.
2. Click **Advanced Configuration** to open the **Advanced Configuration** web page.

 If a password is set you will be prompted for the password.

Advanced Configuration web page

The **Advanced Configuration** web page can be accessed from the link on the SafeCom Controller opening page. If the page is password-protected you will be prompted for a user name and password.



SafeCom 

Home | [Advanced Configuration](#) | [Status](#) | [How To](#) | [Technical Support](#) | [Overview](#)

SafeCom Controller Administration

Note: Configuration modifications are activated by a **Restart SafeCom Controller**

- [General](#)
- [Printer](#)
- [SafeCom](#)
- [TCP/IP](#)
- [LAN](#)
- [SNMP](#)
- [Mail Notification](#)
- [Cash Deposits](#)
- [Password](#)

- [Logout](#)
- [Restart](#)
- [Restart to mini-FTP](#)
- [Restore Factory Default](#)

Summary

SafeCom Controller Name: SafeCom Controller 2 Port

Contact:

Location:

Firmware: S80 508.000*00

Ethernet

MAC Address: 00C076FF04AC

IP Address: 172.16.6.213

SafeCom web page

The **SafeCom** web page can be opened from the **Advanced Configuration** web page by clicking on **SafeCom**.

SafeCom Settings

Home | Advanced Configuration | Status | How To | Technical Support | Overview

To record changes, click **Save & Continue** at the **bottom** of the page.

SafeCom Group Name: WSLEJ3

SafeCom Server IP Address: 172.16.6.58

Write one server per line. Highest priority on top. Example: 192.168.1.5

SafeCom Server Port Number: 7500

Broadcast Subnets: 255.255.255.255

Write one subnet per line. Example: 255.255.255.255

Front End Language: English

Front End Identification: CODE_CARD Front End Timeout: 60 (min 30 max 300 seconds)

Save & Continue

SafeCom Controller Administration

SafeCom Controller

Summary

SafeCom Controller Name: SafeCom Controller 2 Port

Contact: Location: S80 506.790*42

Firmware: Ethernet MAC Address: 00C076FF1403 IP Address: 172.16.6.100

SafeCom Group Name, **SafeCom Server Address** and **SafeCom Server Port Number** must be specified for the SafeCom Controller to work.

You can specify multiple SafeCom servers for the purpose of failover. The SafeCom Controller will attempt to contact the servers in their order of appearance.

If the IP Address is 0.0.0.0 the SafeCom Controller will send a broadcast on the **Broadcast subnets**.

Front End Language: The supported language is English.

Front End Identification determines how users are identified. It can be **CODE_CARD** (default), **CODE_CARD** or **Windows_Auth**. The latter allows users to login with Windows user logon and Windows password.

The **Front End Timeout** default value is 60 seconds. Users will be logged out if they do not perform an operation on the Sharp MFP's touchscreen or buttons for this period.

Printer web page

The **Printer** web page can be opened from the **Advanced Configuration** web page by clicking on **Printer**.

The screenshot shows the 'Printer Settings' page in the SafeCom Controller administration interface. The page is divided into two main sections: 'Printer Settings' on the left and 'Summary' on the right.

Printer Settings:

- Print using:**
 - Network - Port 9100** (selected):
 - Printer Port Number: 9100
- General:**
 - Printer IP Address: 172.16.6.116
 - Use auto configuration: NO
 - Printer Manufacturer: SHARP
 - Printer Model: MX2300
 - SafeCom Go: YES
 - Force logout: NO
 - Copy Enabled: NO
 - Copy Idle Timeout: 60 (minimum 30 seconds)
 - High Speed Print Enabled: NO
 - Post Tracking: NO
 - Driver Names: (empty text area)

Summary:

- SafeCom Controller Name:** SafeCom Controller 2 Port
- Contact Location:** S80 508.780*44
- Ethernet MAC Address:** 00C076FF1403
- Ethernet IP Address:** 172.16.6.51

At the bottom of the 'Printer Settings' section, there is a 'Save & Continue' button and a link to 'SafeCom Controller Administration'.

Select **Network – Port 9100** if the SafeCom Controller connects to the device through the network.

Printer IP Address value must be that of the Xerox printer.

Use auto-configuration value should normally be set to **YES** allow the SafeCom Controller to automatically determine the **Printer Manufacturer** and **Print Model**.

Printer Manufacturer value should be XEROX.

SafeCom Go value must be **YES**.

Force logout⁴: When Force Logout is enabled SafeCom Go Xerox can send a request to the Xerox device asking it to logout the user. This means users can logout by card instead of going through a key press sequence consisting of up to 4 steps (depending on model).

Copy Enabled value must be **YES** if you wish SafeCom to track the number of copies. Requires a SafeCom Tracking device license.

⁴ Force Logout was introduced in SafeCom Go Xerox version S80 508.780*25.

Copy Idle Timeout: When the printer has been idle for this timeout the SafeCom controller automatically logs out the user. Idle timeout = 0 means no timeout.

High Speed Print Enabled value should be **YES** to allow faster printing. With high speed print, the print speed becomes comparable to that of printing the document directly to the device.



- High Speed Print is ignored if the document is sent as encrypted.
- With High Speed Print enabled in environments where users are allowed to do both Push and Pull printing, there is a potential risk that the user standing at the device printing and copying experience that other users' Push Prints are printed in between jobs.

Post Tracking will cause tracking data to be adjusted to reflect the actual number of mono and color pages printed.

Drivers: When Pull Printing, SafeCom will compare the driver name embedded in the print job with its list of driver names. If no match is found the document will appear with a question mark [?] in the document list. This way the user is warned that fidelity is low and the document may print incorrectly.

Chapter 5

SafeCom Go Xerox – How to

The following subsections contain step-by-step instructions for some of the administrator's common tasks for:

- SafeCom Go Xerox on Device Server
- SafeCom Go Xerox on Controller

SafeCom Go Xerox on Device Server

Enable Plug-in Settings on device web page

For the card reader to work, the plug-in settings must be activated on the device web page:

1. Open the device web page and log in with device username and password.
2. Click the **Properties** tab and then **Security** in the left menu.
3. Click **Plug-in Settings** and then **Plug-in Settings** again.
4. Make sure to enable **Plug-in Settings** by selecting the **Enabled** box.
5. Click **Apply**.
6. Reboot the Xerox device.
7. Go to **List of Embedded Plug-ins** and make sure that the SafeCom plug-in (SafeCom HID Reader Provider) is activated. If not, select the plug-in and click **Start**.

Select login method

To set the method of user identification:

1. Open a web browser and log in to the SafeCom Device Server.
2. Click on **Device server** in the left-hand menu, and then click on the device.
3. In the **Login method** menu under **SafeCom Settings**, select how users must identify themselves at the device.

Choose between:

- ID code
- Card
- Card or ID code
- Card or Windows

i When upgrading from previous versions with Auto-sense selected the login method will be set to Card or Windows since auto-sense is no longer supported.

Register device

Register the device with the SafeCom solution in one of the following ways:

- Add the device in the SafeCom Administrator, using the **Add device** function.
- Log in at the device, if the user has Technician or Administrator rights.

Enable SafeCom Mobile Pull Print

1. To allow users to Pull Print documents through their smart phone, a QR code must be printed for each device. Users then scan the QR code label at the MFP/printer with their phone, thus identifying themselves and declaring their presence at the specific device.
For details on how to print a QR code for the device, refer to the *SafeCom G4 Administrator's Manual*.
2. Make sure that the default domain is configured on the device in SafeCom Device Server, as the users are not prompted for domain when logging into a device using a smart phone. If the default domain is not specified, but the users are required to use domains, they can enter the domain with their username (domain\username).

For more details on how to Pull Print from a smart phone refer to the *SafeCom Mobile Pull Print User's Guide*.

Restore factory default

1. Open a web browser and log in to the SafeCom Device Server.
2. Click **Restore factory default** at the bottom of the web page.

The factory default values are:

Configuration settings	Field	Default value
Device Settings	Model	
	MAC Address	
	Device Message	
SafeCom Settings	Login Method	Card or Windows
	Idle timeout	60 seconds
	Post tracking	Cleared (No)
Network Settings	Address	Device IP address
	SNMP Get Community	Public
	SNMP Put Community	Private
	RAW print port	
Device Information	Contact	

Configuration settings	Field	Default value
	Location	
	Description	
	Manufacturer	
Drivers		
Device Properties	LockJobStatusPathway	skip
	LockMachineStatusPathway	skip
	LockFeaturePathway	skip
	OverrideLanguage	None
	DefaultDomain	
	HideDomain	false
	CheckEIPStatus	true

Use Device trace facility

i Use the SafeCom trace facility only if SafeCom Support instructs you to do so.

1. Enable the trace facility through the SafeCom Device Server:
 - a. Open the SafeCom Device Server and log in.
 - b. Select a device in the device server pane and make sure that the **Logging enabled** check box at the bottom of the page is selected.
 - c. Click **Save**.
2. Check the trace files generated by the Device Server
 - a. Go to the destination folder for the log files:
The default installation folder is:
 - On Windows 32-bit: C:\Program Files\SafeCom\SafeCom Device Server\logs
 - On Windows 64-bit: C:\Program Files (x86)\SafeCom\SafeCom Device Server\logs
 - b. If you need to send the log files, make sure to save and send the folder logs as a compressed/zipped folder.
3. Configure the size and number of the generated trace files.
 - a. Browse to the config.ini file:
 - On Windows 32-bit: C:\Program Files\SafeCom\SafeCom Device Server\equinox\config.ini
 - On Windows 64-bit: C:\Program Files (x86)\SafeCom\SafeCom Device Server\equinox\config.ini

- b. Double-click the config.ini file. In the open file, scroll to the bottom and add:
 - `deviceserver.trace.file.size` - to configure file size. Size is written as a number with an optional qualifier. For example: ten is 10 bytes, ten kilobytes is 10KB, ten megabytes is 10MB, and one gigabyte is 1GB.
 - `deviceserver.trace.file.count` - to configure how many trace files are generated. Enter the number of files you want to generate as a number.
4. After configuring the trace files restart the SafeCom service.

Uninstall SafeCom Go Xerox

To uninstall the SafeCom Go Xerox software from the device:

1. Open a web browser and log in to the **SafeCom Device Server**.
2. Click **Device server** in the menu and select the device from which the SafeCom Go solution must be uninstalled.
3. Click the **Delete** icon in the top menu to uninstall.
4. Click **Save**.

SafeCom Go Xerox on Controller

Specify SafeCom server and printer connection

1. Open the **Advanced Configuration** web page.
2. Click **SafeCom** and enter the **SafeCom Server address** (Hostname or IP address).

It is possible to specify multiple SafeCom servers for the purpose of failover. The SafeCom Controller will attempt to contact the servers in their order of appearance. If the SafeCom server is clustered you must specify the address of the virtual server.
3. Click **Save and Continue**.
4. Click **Printer** and check **Network - Port 9100**.
5. Enter the **Printer IP address**.
6. Click **Save and Continue**.
7. Click **Restart**.

After approx. 1 minute the SafeCom Controller has restarted and you can make a settings printout.


Set password to prevent unauthorized access

To prevent unauthorized access to the SafeCom Controller's configuration we recommend that you change the password from the default: "adm". To disable security, change the password back to "adm".

1. Open the **Advanced Configuration** web page.
2. Click **Password**.
3. Enter the **Old Password**, **New Password** and **Verify Password**.

The password is maximum 8 characters.

4. Click **Save and Continue**.
5. Click **Restart**.

 Make sure to store the password in a secure place. If you forget the password you need to return the SafeCom Controller to SafeCom for unlocking.


Assign a fixed IP address to the SafeCom Controller

The IP address can be assigned through DHCP (dynamic or fixed) or manually. The steps below describe how to assign a fixed IP address through the SafeCom Controller web interface.

1. Open the **Advanced Configuration** web page.
2. Click **TCP/IP**.
3. Check **Manual** and enter the **IP address** and other parameters.
4. Click **Save and Continue**.
5. Click **Restart**.

Register device

The device can be registered when a user with Technician or Administrator rights has logged in at the device. Once the device is registered it will appear in the SafeCom Administrator. The device is also registered when you add it in SafeCom Administrator.

 You can use the built-in Technician account TECH with the default PUK code 12345678 and default PIN code 1234.

Restore factory default

You can either restore settings by holding down the test button of the SafeCom Controller for 8 seconds, or from the SafeCom Controller web interface:

1. Open the **Advanced Configuration** web page.
2. Click **Restore Factory Default**.

Uninstall SafeCom Go Xerox

1. On the SafeCom Controller **Printer** web page change **SafeCom Go** to **No**. Click **Save and Continue**. Click **Restart**.
2. Open the printer's web page and click on the **Properties** tab.
3. Go through the various screens and reset the values. Apply changes and reboot the printer.

Make all printing go through SafeCom

1. Open the printer's web page.

2. Click the **Properties** tab.
3. Click **Security** and then **IP Filtering** on the menu.

Refer to the Xerox printer's documentation for additional information.

Enable force logout


1. Open the **Advanced Configuration** web page.
2. Click **Printer**.
3. Change **Force logout** to **YES**.
4. Click **Save and Continue**.
5. Click **Restart**.

Resend configuration

If a device added in the SafeCom Administrator is not configured correctly, or if the device must be reconfigured to a different server, it is possible to resend the configuration details (Server address and Group name) to the device.

1. Browse to **Devices** in the SafeCom Administrator.
2. Right-click the device and click **Resend configuration**.

The configuration details are now sent to the device and the configuration is successful when the message "Server is reconfigured" appears.

 The Resend configuration functionality does not work with devices that are SafeCom enabled through the device server.

Manually upgrade DLM File

1. Open the printer's web page and click on the **Properties** tab.
2. Click **Services** > **Machine Software** > **Manual Upgrade** .
3. In the **Manual Upgrade** section browse to where the **InstallCustomServices.dlm** is located.
4. Select the file and then click the green **Install Software** button.

Configure multiple SafeCom Controllers

SafeCom Device Utility chapter in the *SafeCom G4 Administrator's Manual* describes how SafeCom Device Utility can be used to set the configuration on multiple SafeCom Controllers.

Chapter 6

Set up network accounting

i A device reboot may be necessary after enabling Xerox Network Accounting on the device.

Xerox WorkCentre 5330, 7120 and 7125

Enable Xerox Network Accounting

1. Log in as a local administrator on the device control panel.
2. Press the **Machine Information** button.
3. Tap the **Tools** tab, then **Accounting**, and then **Accounting Type**.
4. In the **Accounting Type setup**, tap **Network accounting**.
5. Tap **Save**.
6. In the **Tools** menu, tap the **Key** button and accept to logout from the device.

i It is important to have SPAR firmware release 53.11.82 or newer installed on Xerox WorkCentre 5330 in order for this setting to work.

Xerox ColorQube 92xx and 93xx

Enable Xerox Network Accounting

1. Log in as a local administrator on the device control panel.
2. Press the **Machine Information** button.
3. Tap the **Tools** tab, then **Accounting setting**, and then **Accounting Mode**.
4. In the **Accounting Mode setup**, tap **Network accounting**.

Disable prompts for accounting codes

1. Tap **Customize Prompts**.
2. Change the dropdown list to **Display No Prompts**.
3. Tap **Save**.
4. Tap **Save**.

5. In the **Tools** menu, tap the **Key** button and accept to logout from the device.

Xerox WorkCentre 75xx

Enable Xerox Network Accounting

1. Open the printer's web page and click on the **Properties** tab.
2. Click **Accounting** and then **Setup**.
3. Click **Edit**.
4. Change **Current Accounting Method** to **Network Accounting**.
5. Click **Save**.

Disable Code Entry Validation

1. On the row **User Accounting Prompts / Validation** click **Edit**.
2. In the section **Code Entry Validation** click **Disabled**.
3. Click **Save**.
4. Click **Security** and then **Authentication** and then **Setup**.
5. On the row **Xerox Secure Access Setup**, click **Edit**.
6. Click **Manually Override**.
7. In the section **Accounting Information (Requires Network Accounting)** click **Automatically apply Accounting Codes from the server**.
8. Click **Save**.

Xerox WorkCentre 56xx and WorkCentre Pro 2xx

Enable Xerox Network Accounting

1. Log in as a local administrator on the device control panel.
2. Tap **Tools Pathway**.
3. Tap **Access and Accounting**.
4. Tap **Authentication Mode**.
5. Under **Network Accounting** tap **On**, tap **Save**.

Disable Network Accounting Authentication

1. Tap **Tools Pathway**.
2. Tap **Access and Accounting**.
3. Tap **Network Accounting Setup**.
4. Tap **Network Accounting Authentication**.
5. Select **Disable** and **Save**.

Chapter 7

Using SafeCom Go Fuji Xerox

Xerox WorkCentre 71xx, 74xx, and 75xx

Login

The login sequence is initiated if you are not already logged in and taps any icon that requires SafeCom to handle the printer authentication.

The recommended login sequences are described in the following:

Login with card

Use card reader.

Login with card and PIN code

1. Use card reader
2. Enter **PIN code** on the keypad or touchscreen.
3. Tap **Enter**.

Login with ID code

1. Tap **Keyboard Access**.
2. Enter **Code** on the keypad or touchscreen.
3. Tap **Enter**.

Login with ID code and PIN code

1. Tap **Keyboard Access**.
2. Enter **Code** on the touchscreen.
3. Tap **Enter**.
4. Enter **PIN code** on the keypad or touchscreen.
5. Tap **Enter**.

Login with Windows

If Front End Identification is Windows_Auth, it is possible to log in by either using your card or entering your Windows logon credentials:

1. Tap **Username** and enter **Username** on the touchscreen. Tap **OK**.
2. Tap **Password** and enter **Password** on the touchscreen. Tap **OK**.
3. Tap **OK**.

i Username and password cannot be blank.

Pull Print - Document list

Access the Document list that allows you to print individual documents.

Tap **Pull Print**.

Documents appear in chronological order with the newest at the top of the list. The number preceding the document title is the cost of the document. A delegated print is marked with a preceding **D**. Tap the **Info** button to see information about who delegated the document. A retained document has a preceding **R**. A group print document has a preceding **G**. If **Print all at login** is checked any documents pending collection will be printed first.




i The document list looks slightly different from the above.

On the touchscreen there are the following options:

- **Print all:** Prints all documents, excluding any retained documents. Documents are printed in chronological order (oldest first).

- **Refresh:** Updates the list of documents with pending documents that has finished spooling after the user logged in.
- **Back:** Returns to the previous screen.
- **Print:** Prints the selected documents.
- **Retain:** The selected documents remain on the list (server) after they have been printed. When a document has been retained, it is specified in the list with an **R** preceding the document title.
- **Delete:** Deletes the selected documents.
- **Info:** See information about the selected documents, including cost, driver name, use of color and duplex.
- **Copies:** Request multiple copies of a document. **Print all** always prints one copy of each document.

 The maximum number of multiple documents that can be selected at once for printing, deletion, or retention is 48.

Copy


Tap the **Copy** icon to copy the documents placed in the automatic document feeder (ADF).

Logout

There is a configurable timeout that defaults to 60 seconds. The logout process is initiated if no buttons are tapped for this period.

To logout actively:

Press the **Key** button and select **Logout**.

 Logout by card is possible on Xerox firmware that supports the Force Logout request.

Register card at device with Windows credentials

1. Use the card reader.
2. Tap **Exit** to get to the registration with Windows credentials.
3. Enter Windows user name and tap **Enter**.
4. Enter Windows domain and tap **Enter**.
5. Enter Windows password, tap **Enter** and the card is now registered.

Register card with PUK code

Use the card reader and if the card is unknown and there is an available PUK code in the SafeCom system the user is prompted to register with PUK and PIN code.

1. Enter **PUK code** on the keypad or touchscreen.
2. Tap **Enter**.
3. Enter **PIN code** on the keypad or touchscreen.

4. Tap **Enter** and the card is now registered.

Xerox WorkCentre 76xx and 77xx

Control Panel



Login

The login sequence is initiated if you are not already logged in and taps any icon that requires SafeCom to handle the printer authentication.

The recommended login sequences are described in the following:

Login with card

Use card reader.

Login with card and PIN code

1. Use card reader
2. Enter **PIN code** on the keypad or touchscreen.
3. Tap **Enter**.

Login with ID code

1. Tap **Keyboard Access**.
2. Enter **Code** on the keypad or touchscreen.
3. Tap **Enter**.


Login with ID code and PIN code

1. Tap **Keyboard Access**.
2. Enter **Code** on the touchscreen.
3. Tap **Enter**.
4. Enter **PIN code** on the keypad or touchscreen.
5. Tap **Enter**.

Login with Windows

If Front End Identification is Windows_Auth, it is possible to log in by either using your card or entering your Windows logon credentials:

1. Tap **Username** and enter **Username** on the touchscreen. Tap **OK**.
2. Tap **Password** and enter **Password** on the touchscreen. Tap **OK**.
3. Tap **OK**.

 Username and password cannot be blank.

Pull Print - Document list

Access the Document list that allows you to print individual documents.

Tap **Pull Print**.

Documents appear in chronological order with the newest at the top of the list. The number preceding the document title is the cost of the document. If **Print all at login** is checked any documents pending collection will be printed first.



i The document list looks slightly different from the above.

On the touchscreen there are the following options:

- **Print all:** Prints all documents, excluding any retained documents. Documents are printed in chronological order (oldest first).
- **Refresh:** Updates the list of documents with pending documents that has finished spooling after the user logged in.
- **Back:** Returns to the previous screen.
- **Print:** Prints the selected documents.
- **Retain:** The selected documents remain on the list (server) after they have been printed. When a document has been retained, it is specified in the list with an **R** preceding the document title.
- **Delete:** Deletes the selected documents.
- **Info:** See information about the selected documents, including cost, driver name, use of color and duplex.
- **Copies:** Request multiple copies of a document. **Print all** always prints one copy of each document.

i The maximum number of multiple documents that can be selected at once for printing, deletion, or retention is 48.

Copy

Tap the **Copy** icon to copy the documents placed in the automatic document feeder (ADF).

Logout

There is a configurable timeout that defaults to 60 seconds. The logout process is initiated if no buttons are tapped for this period.

To logout actively:

Press the **Key** button and select **Logout**.

i Logout by card is possible on Xerox firmware that supports the Force Logout request.

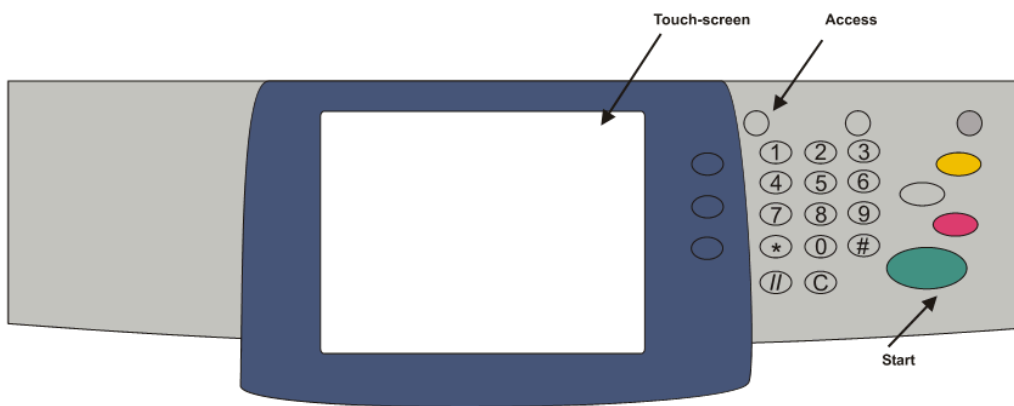
Register card with PUK code

Use the card reader and if the card is unknown and there is an available PUK code in the SafeCom system the user is prompted to register with PUK and PIN code.

1. Enter **PUK code** on the keypad or touchscreen.
2. Tap **Enter**.
3. Enter **PIN code** on the keypad or touchscreen.
4. Tap **Enter** and the card is now registered.

Xerox WorkCentre 52xx, 72xx, 73xx and 74xx

Control Panel



Login

The login sequence is initiated if you are not already logged in and taps any icon that requires SafeCom to handle the printer authentication.

Login with card

Use card reader.

Login with card and PIN code

1. Use card reader
2. Enter **PIN code** on the keypad or touchscreen.
3. Tap **Enter**.

Login with ID code

1. Tap **Keyboard Access**.
2. Enter **Code** on the keypad or touchscreen.
3. Tap **Enter**.


Login with ID code and PIN code

1. Tap **Keyboard Access**.
2. Enter **Code** on the touchscreen.
3. Tap **Enter**.
4. Enter **PIN code** on the keypad or touchscreen.
5. Tap **Enter**.

Login with Windows

If Front End Identification is Windows_Auth, it is possible to log in by either using your card or entering your Windows logon credentials:

1. Tap **Keyboard Access**.
2. Tap **Username** and enter **Username** on the touchscreen. Tap **OK**.
3. Tap **Password** and enter **Password** on the touchscreen. Tap **OK**.
4. Tap **Domain** and enter the domain using the keypad or touchscreen.
5. Tap **OK**.

 Username and password cannot be blank.

Pull Print - Document list

Access the Document list that allows you to print individual documents.

Tap **Pull Print**.

Documents appear in chronological order with the newest at the top of the list. The number preceding the document title is the cost of the document. A delegated print is marked with a preceding **D**. Tap the **Info** button to see information about who delegated the document. A retained document has a preceding **R**. A group print document has a preceding **G**. If **Print all at login** is checked any documents pending collection will be printed first.



i The document list looks slightly different from the above.

On the touchscreen there are the following options:

- **Print all:** Prints all documents, excluding any retained documents. Documents are printed in chronological order (oldest first).
- **Refresh:** Updates the list of documents with pending documents that has finished spooling after the user logged in.
- **Back:** Returns to the previous screen.
- **Print:** Prints the selected documents.
- **Retain:** The selected documents remain on the list (server) after they have been printed. When a document has been retained, it is specified in the list with an **R** preceding the document title.
- **Delete:** Deletes the selected documents.
- **Info:** See information about the selected documents, including cost, driver name, use of color and duplex.
- **Copies:** Request multiple copies of a document. **Print all** always prints one copy of each document.

i The maximum number of multiple documents that can be selected at once for printing, deletion, or retention is 48.

Copy

Press the **Copy** button to copy the documents placed in the automatic document feeder (ADF).

Logout

There is a configurable timeout that defaults to 60 seconds. The logout process is initiated if no buttons are tapped for this period.

To logout actively:

Press the **Key** button and select **Logout**.

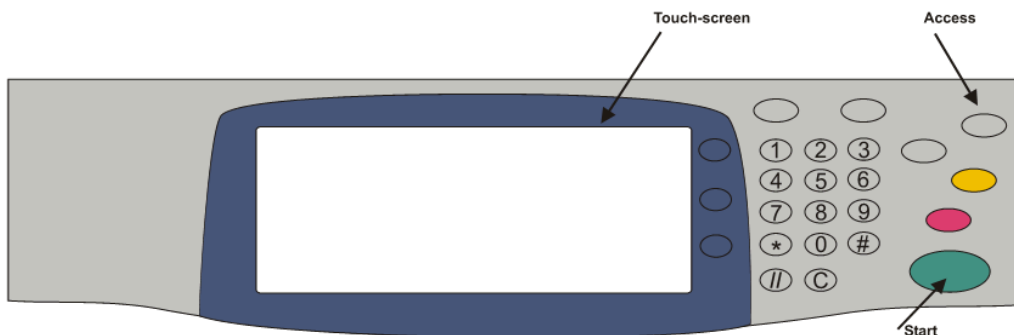
Register card with PUK code

Go to the printer to log in by using a card if card reader is connected. If the card is unknown and there is an available PUK code in the SafeCom system the user is asked to register with PUK and PIN code.

1. Enter **PUK code** on the keypad or touchscreen.
2. Tap **Enter**.
3. Enter **PIN code** on the keypad or touchscreen.
4. Tap **Enter**.

Xerox WorkCentre 56xx

Control Panel



Login

The recommended login sequences are described in the following.

Login with card

Use card reader.

Login with card and PIN code

1. Use card reader
2. Enter **PIN code** on the keypad or touchscreen.
3. Tap **Enter**.

Login with ID code

1. Tap **Keyboard Access**.
2. Enter **Code** on the keypad or touchscreen.
3. Tap **Enter**.

Login with ID code and PIN code

1. Tap **Keyboard Access**.
2. Enter **Code** on the touchscreen.
3. Tap **Enter**.
4. Enter **PIN code** on the keypad or touchscreen.
5. Tap **Enter**.

Login with Windows

If Front End Identification is Windows_Auth, it is possible to log in by either using your card or entering your Windows logon credentials:

1. Tap **Keyboard Access**.
2. Tap **Username** and enter **Username** on the touchscreen. Tap **OK**.
3. Tap **Password** and enter **Password** on the touchscreen. Tap **OK**.
4. If prompted, enter the domain in the **Domain** field.
5. Tap **OK**.

 Username and password cannot be blank.

Pull Print - Document list

Access the Document list that allows you to print individual documents.

1. Tap **All Services**.
2. Tap **Custom Services**.
3. Tap **Pull Print**.

Documents appear in chronological order with the newest at the top of the list. The number preceding the document title is the cost of the document. A delegated print is marked with a preceding **D**. Tap the **Info** button to see information about who delegated the document. A retained document has a preceding **R**. A group print document has a preceding **G**. If **Print all at login** is checked any documents pending collection will be printed first.



On the touchscreen there are the following options:

- **Print all:** Prints all documents, excluding any retained documents. Documents are printed in chronological order (oldest first).
- **Refresh:** Updates the list of documents with pending documents that has finished spooling after the user logged in.
- **Back:** Returns to the previous screen.
- **Print:** Prints the selected documents.
- **Retain:** The selected documents remain on the list (server) after they have been printed. When a document has been retained, it is specified in the list with an **R** preceding the document title.
- **Delete:** Deletes the selected documents.
- **Info:** See information about the selected documents, including cost, driver name, use of color and duplex.
- **Copies:** Request multiple copies of a document. **Print all** always prints one copy of each document.

i The maximum number of multiple documents that can be selected at once for printing, deletion, or retention is 48.

Copy

Press the **Copy** button to copy the documents placed in the automatic document feeder (ADF).

Logout

There is a configurable timeout that defaults to 60 seconds. The logout process is initiated if no buttons are tapped for this period.

To logout actively:

1. Press the **Key** button.
2. Tap **YES** to leave **Custom Services**.
3. Press the **Key** button.
4. Tap **YES** to **logout**.

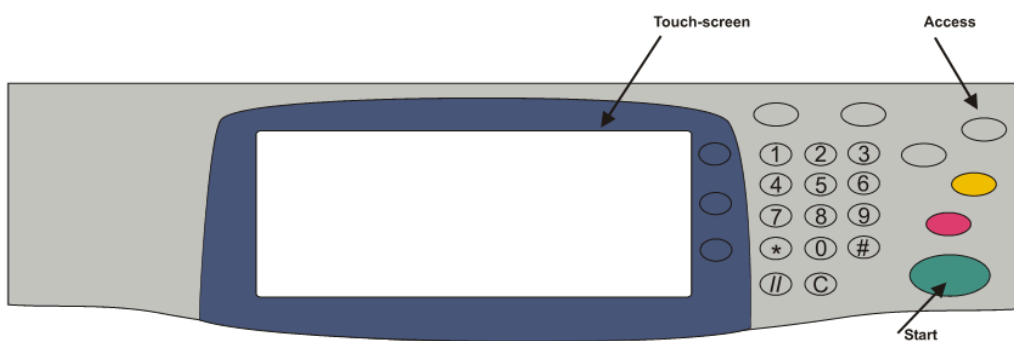
Register card with PUK code

Go to the printer to log in by using a card if card reader is connected. If the card is unknown and there is an available PUK code in the SafeCom system the user is asked to register with PUK and PIN code.

1. Enter **PUK code** on the keypad or touchscreen.
2. Tap **Enter**.
3. Enter **PIN code** on the keypad or touchscreen.
4. Tap **Enter**.

Xerox WorkCentre 2xx

Control Panel



Login

The recommended login sequences are described in the following.

Login with card

Use card reader.

Login with card and PIN code

1. Use card reader
2. Enter **PIN code** on the keypad or touchscreen.
3. Tap **Enter**.

Login with ID code

1. Tap **Keyboard Access**.
2. Enter **Code** on the keypad or touchscreen.
3. Tap **Enter**.


Login with ID code and PIN code

1. Tap **Keyboard Access**.
2. Enter **Code** on the touchscreen.
3. Tap **Enter**.
4. Enter **PIN code** on the keypad or touchscreen.
5. Tap **Enter**.

Login with Windows

If Front End Identification is Windows_Auth, it is possible to log in by either using your card or entering your Windows logon credentials:

1. Tap **Username** and enter **Username** on the touchscreen. Tap **OK**.
2. Tap **Password** and enter **Password** on the touchscreen. Tap **OK**.

 Username and password cannot be blank.

Pull Print - Document list

Access the Document list that allows you to print individual documents.

1. Tap **All Services**.
2. Tap **Custom Services**.
3. Tap **Pull Print**.

Documents appear in chronological order with the newest at the top of the list. The number preceding the document title is the cost of the document. A delegated print is marked with a preceding **D**. Tap the **Info** button to see information about who delegated the document. A retained document has a preceding **R**. A group print document has a preceding **G**. If **Print all at login** is checked any documents pending collection will be printed first.



On the touchscreen there are the following options:

- **Print all:** Prints all documents, excluding any retained documents. Documents are printed in chronological order (oldest first).
- **Refresh:** Updates the list of documents with pending documents that has finished spooling after the user logged in.
- **Back:** Returns to the previous screen.
- **Print:** Prints the selected documents.
- **Retain:** The selected documents remain on the list (server) after they have been printed. When a document has been retained, it is specified in the list with an **R** preceding the document title.
- **Delete:** Deletes the selected documents.
- **Info:** See information about the selected documents, including cost, driver name, use of color and duplex.
- **Copies:** Request multiple copies of a document. **Print all** always prints one copy of each document.

i The maximum number of multiple documents that can be selected at once for printing, deletion, or retention is 48.

Copy

Press the **Copy** button to copy the documents placed in the automatic document feeder (ADF).

Logout

There is a configurable timeout that defaults to 60 seconds. The logout process is initiated if no buttons are tapped for this period.

To logout actively:

1. Press the **Key** button.
2. Select **Logout**.

Register card with PUK code

Go to the printer to log in by using a card if card reader is connected. If the card is unknown and there is an available PUK code in the SafeCom system the user is asked to register with PUK and PIN code.

1. Enter **PUK code** on the keypad or touchscreen.
2. Tap **Enter**.
3. Enter **PIN code** on the keypad or touchscreen.
4. Tap **Enter**.

Chapter 8

Troubleshooting

SafeCom Help Desk Assistant

We want your SafeCom solution to be one that reduces not only print costs but is also easy to support. In the following section, you will find useful troubleshooting hints.

Servlets

Kofax SafeCom has implemented two servlets to improve diagnostics data in SafeCom Device Server:

- /debug/dump/heap
- /debug/dump/threads

Enter the path to the SafeCom Device Server in a browser followed by the paths to the servlets.

For example: `http://{DeviceServerAddress}:8080/debug/dump/heap`

i These servlets have been implemented to assist Kofax Technical Support in diagnosing severe failures regarding SafeCom Device Server. Therefore, we recommend only making the thread and heap dump on request from a Support Technician.

Copy jobs are not tracked

Please check the following:

- a. On the SafeCom Controller's **Printer** web page **Copy Enabled** is **YES**.
- b. In **SafeCom Administrator Tracking** is checked on the **License** tab in the **Device properties** dialog.
- c. In **SafeCom Administrator** cost control is set to **Tracking** or **Pay** on the **Settings** tab in the **User properties** dialog.

No communication between SafeCom controller and printer

Please check if the SSL certificate on the printer is expired.

Cannot access properties tab on printer's web page

If you cannot access the Properties tab on the printer's web page, it is most likely because the installed certificate is not valid or expired. A certificate can be used from its Valid from date. It has been reported that the Valid from date is 1 hour later than the time the certificate was generated. You may therefore have to wait 1 hour before the generated certificate can be used. To work around the problem try changing the machine time back while issuing the self-signed certificate and then set it correctly again once the certificate has been applied but before HTTPS is enabled.

At the printer: Cannot access the Tools menu

On Xerox devices that are based on Fuji Xerox engines, users with Administrator or Technician rights cannot access the Tools menu with the SafeCom login. On these devices users must log in locally in order to access the Tools menu.

The following Xerox devices are based on Fuji Xerox engines:

- WorkCentre 52xx,72xx, 73xx, 74xx
- WorkCentre 71xx
- WorkCentre 550/560

At the printer: Error message: "Communication error" at login

If the network is lost or disconnected, on a device with card reader, when a user is logging out, then the Controller and Xerox device sometimes get out of sync.

When the next user attempts to log in, the error message "Communication error" appears followed by "Please wait logging out".

The device freezes, but this can be fixed by swiping the card.

At the printer: cannot enter Billing screen

If you are trying to access the Account icon on the device, the device may display an error message. To access the Billing screen, ensure that you are logged in on the device, and then press the Account icon. For more information, see [Configure SafeCom Device Server](#).

Device Server: Configuration of devices failed

If the Device Server is installed on a server that has multiple NICs or IPs, the configuration of devices may fail.

This is because the Device Server uses the IP returned by Java, which may be problematic if the IP returned to the Device Server is unavailable (because of network layout) from the devices point of view.

A solution is to configure the property `deviceserver.serverAddress` in the `config.ini` file. This forces the Device Server to use the given IP when configuring devices. For more details, see [Device Server config.ini](#).

Device Server: "Unable to configure device because: Device is configured against a different server"

When making changes to the configuration of the device server device and the Device Message field shows the message "Unable to configure device because: Device is configured against a different server", it is because the device is configured to a different server.

To make changes to the device configuration:

1. Click **Reconfigure device** which configures the device to your server
2. Make the necessary changes
3. Click **Save**.

Device Server: Error when upgrading existing Device Server installation

The following error might appear when upgrading an existing Device Server installation: "Error in action StopWindowsService"

Complete the following steps before running the installer again:

1. Kill the installer process with the following command:

```
taskkill /F /IM scDeviceServer.exe
```
2. Stop the SafeCom Device Server Service with the following command:

```
net stop scDeviceServer
```
3. Start the SafeCom Device Server again with the following command:

```
net start scDeviceServer
```
4. Re-run the SafeCom Device Server installer.

Native device functions are not tracked

If the native functions of a device are not tracked in SafeCom, ensure that you have Xerox Network Accounting configured, and that Enable Post tracking is checked for the device on the Device Server webpage.

Chapter 9

Regulatory information

WARNING NOTE: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation.

This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

CAUTION: Changes or modifications not expressly approved by Kofax, Inc. could void the user's authority to operate this equipment according to part 15 of the FCC rules.

This equipment generates, uses, and can radiate radio frequency energy and if not installed and used in accordance with the instruction manual, may cause interference to radio communications. It has been tested and found to comply with the limits for a Class A computing device pursuant to Subpart B of Part 15 of FCC Rules, which are designed to provide reasonable protection against such interference when operated in a commercial environment. Operation of this equipment in a residential area is likely to cause interference in which case the user will be required to take whatever measures may be required to correct the interference at the user's own expense.

CE conformance: This product has been developed and produced in accordance with the EMC directive and the Low Voltage directive and therefore carries the CE mark.

EMC directive: This product observes the rules and regulations of the EMC directive. If so required, a declaration of conformity in local language stipulating the applied rules and regulations can be obtained.