

Kofax SafeCom Go HP Administrator's Guide

Version: 10.6.0

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	12
Related documentation.....	12
Training.....	12
Getting help with Kofax products.....	12
Chapter 1: Introduction	14
Requirements.....	14
SafeCom Go HP products.....	15
SafeCom P:Go HP products.....	16
SafeCom ID devices.....	16
Supported languages.....	17
HP Universal Print Driver.....	17
Check the Printer properties.....	18
Make the printer use the SafeCom Pull Port.....	18
Print a test page.....	19
HP Universal Print Driver Remarks.....	19
Chapter 2: Device Server installation	20
Install SafeCom Device Server.....	20
Windows firewall – Ports that must be opened.....	20
Configure SafeCom Device Server.....	23
Log in to SafeCom Device Server.....	23
Add SafeCom Server.....	23
Device Server config.ini.....	25
Add device to the SafeCom Device Server.....	26
Device icons.....	27
Add device through the SafeCom Administrator.....	27
Add device through the SafeCom Device Server.....	28
Adding Sx devices to the Device Server.....	28
Configure the device on the device web page.....	29
Set up device server address.....	30
Set sign-in method and access control.....	30
Verify Quota Server address.....	31
Configure device in SafeCom Device Server.....	31
Configure device server failover.....	34
SafeCom Go HP web interface.....	35

Login.....	35
Product and version information web page.....	35
Configure and log information web page.....	35
SafeCom Go HP - How to.....	36
Select login method.....	36
Enable Copy Control.....	37
Enable Scan to Folder.....	38
Enable E-mail.....	39
Control user access rights.....	40
Enable Client Billing and the account icon on the device.....	41
Enable third party authentication.....	41
Enable using the Home Folder.....	41
Enable SafeCom Mobile Pull Print.....	42
Determine the version.....	42
Handle new MAC address (Jetdirect network card).....	43
Verify that SafeCom Go HP is loaded.....	43
Register device.....	43
Configure Push Print Post Tracking.....	43
Configure users and devices to allow modifying job setting.....	46
Restore factory default settings.....	46
Uninstall SafeCom Go HP.....	47
HP OPS installation.....	48
Prerequisites for OPS.....	48
Installation example - through installer.....	48
Installation example - through command line.....	54
Partial Disk Clean on M525 and M575 devices.....	55
SafeCom Go HP device trace facility.....	56
Enable the SafeCom trace facility through the Configuration web page.....	56
Enable the trace facility through the SafeCom Device Server.....	56
See the trace files generated by the Device Server.....	56
Configure the size and number of the trace files.....	56
Chapter 3: SafeCom Go HP installation.....	58
SafeCom Go HP hardware installation.....	58
SafeCom HP hardware installation.....	58
Embedded ID device in Hardware Integration Pocket.....	59
SafeCom Go HP software installation.....	60
Send SafeCom Go HP FS (*.b95) file to FutureSmart devices.....	61
Send SafeCom Go HP (*.b49) and (*.b89) files to legacy Chai devices.....	61

Install to FutureSmart devices through Solution Installer.....	62
Control Device Sign in CM8050 MFP and CM8060 MFP.....	64
Send to E-mail on CM8050 MFP and CM8060 MFP.....	65
Deploy SafeCom Go HP on multiple devices.....	65
Create a device configuration file.....	65
Send configuration file to devices.....	66
Make changes to the configuration file.....	67
Login.....	68
SafeCom Go HP web interface.....	68
Information web page.....	68
Configuration web page.....	69
Register web page.....	74
Log web page.....	74
SafeCom Go HP – How to.....	75
Get the SafeCom Go HP software.....	75
Specify SafeCom Server.....	75
Register device.....	76
Resend configuration.....	76
Disable Encrypt All Web Communication.....	76
Set password to prevent unauthorized access.....	76
Set password using HP Web Jetadmin.....	77
Disable TCP/IP(v6).....	77
Verify the IP Address of the DNS Server.....	77
Check SNMP Settings.....	77
Set SNMP v3.....	78
Allow installation of legacy packages.....	79
Select login method.....	79
Login with Windows without specifying the domain.....	79
Login without PIN code.....	80
Change PIN code.....	80
Disable Pull Print.....	80
Enable Copy Control.....	80
Enable device memory usage.....	81
Enable Send to Folder.....	81
Enable Send to Folder – with password.....	82
Enable Send to E-mail – Pre-filled From: and To: field.....	82
Enable Send to E-mail – with password.....	83
Enable SafeCom Smart Scan.....	84

Control user access rights.....	84
Enable Client Billing and the Account icon.....	84
Enable Third party authentication.....	85
Control max length of encryption keys.....	85
Restore factory default.....	86
Determine the version.....	87
Handle hard disk replacement.....	87
Handle new MAC address (Jetdirect network card).....	87
Use another server in a multi server solution.....	88
How to obtain svcErr.log from the printer.....	88
How to open the SafeCom Loader web page.....	89
HP Access Control USB proximity card reader.....	89
SafeCom Go HP update software.....	91
Is the SafeCom Go HP software loaded?.....	91
Uninstall SafeCom Go HP.....	91
Uninstall SafeCom Go HP on FutureSmart devices.....	91
Uninstall SafeCom Go HP on non-FutureSmart devices.....	92
Make all printing through SafeCom.....	92
SafeCom Go HP device trace facility.....	92
Chapter 4: Using SafeCom Go HP.....	93
HP LaserJet (Enterprise) M525, M575, CM4540 MFP, M4555 MFP, MFP 725, MFP 775, MFP 830, and MFP M880 variants.....	93
Login.....	93
Register card at device with Windows credentials.....	95
Register card at device with PUK code.....	95
Pull Print – Document list.....	96
Copy.....	96
Folder.....	96
E-mail.....	96
Account – Select Billing Code.....	96
Smart Scan.....	97
Logout.....	97
Hide document name.....	97
HP LaserJet M3035 MFP, CM3530 MFP, CM4730 MFP, M5035 MFP, M5039 MFP, CM6030 MFP, CM6040 MFP, CM6049 MFP, M9040 MFP, M9050 MFP, and M9059 MFP.....	98
Control panel.....	99
Login.....	99
Pull Print – Document list.....	101

Copy.....	101
Folder.....	101
E-mail.....	102
Account – Select Billing Code.....	102
Logout.....	102
Register card at device.....	103
Change PIN code.....	104
HP Color LaserJet CM8050 MFP and 8060 MFP.....	104
Control panel.....	104
Login.....	104
Pull Print – Document list.....	105
Copy.....	106
Folder.....	106
E-mail.....	106
Logout.....	106
Register card at device.....	106
HP Scanjet Enterprise 7000n, HP Digital Sender Flow 8500 fn1.....	107
Control panel.....	108
Login.....	108
Register card at device.....	109
Save to Network Folder.....	110
E-mail.....	110
Account.....	110
Logout.....	110
HP 9250C Digital Sender.....	111
Control panel.....	111
Login.....	111
Folder.....	113
E-mail.....	113
Account – Select Billing Code.....	113
Logout.....	114
Register card at device.....	114
Change PIN code.....	115
HP LaserJet M602, M603, M712.....	115
Login.....	115
Pull Print.....	116
Logout.....	116
HP LaserJet M855, M806, and M750.....	116

Login.....	116
Register card at device.....	117
Pull Print.....	117
Logout.....	117
HP LaserJet CP5525, M551, and M601.....	117
Control panel.....	118
Login.....	118
Pull Print.....	118
HP Color LaserJet 3000, CP3505, and 3800.....	118
Control panel.....	118
Login.....	118
Pull Print.....	119
Logout.....	119
HP LaserJet P3005.....	119
Control panel.....	120
Login.....	120
Pull Print.....	120
Logout.....	120
HP LaserJet P3015.....	120
Control panel.....	121
Login.....	121
Pull Print.....	122
Logout.....	122
Register card at device.....	122
HP Color LaserJet CP3525.....	122
Control panel.....	122
Login.....	122
Pull Print.....	123
Logout.....	123
HP LaserJet P4014.....	123
Control panel.....	124
Login.....	124
Pull Print.....	124
Logout.....	125
HP LaserJet P4015 and P4515.....	125
Control panel.....	125
Login.....	125
Pull Print.....	126

Logout.....	126
Register card at device.....	126
HP Color LaserJet CP4525.....	126
Control panel.....	127
Login.....	127
Pull Print.....	127
Logout.....	128
HP Color LaserJet CP6015.....	128
Control panel.....	128
Login.....	128
Pull Print.....	129
Logout.....	129
Register card at device.....	129
HP MFP SXXXdn series.....	129
Login.....	129
Main menu.....	131
Pull Print – Document list.....	131
Copy.....	131
Account – Select billing code.....	131
Register card with PUK code.....	132
Logout.....	132
HP OfficeJet Pro series.....	133
Login.....	133
Main menu.....	133
Pull Print – Document list.....	133
Copy.....	134
Logout.....	134
Chapter 5: Automatic installation through HP Web Jetadmin.....	135
Pre-requisites.....	135
Download SafeCom Go HP software.....	136
Start HP Web Jetadmin.....	138
Add relevant firmware.....	138
Import files to solutions repository.....	138
Create solution templates.....	139
First template.....	140
Second template.....	140
Edit solution settings.....	140
Create groups to automate installation.....	141

Set up groups.....	142
Set up subgroups.....	143
Find devices through discovery.....	145
Register device.....	145
Uninstall SafeCom Go HP.....	145
Sample configuration files.....	146
hp_xml_config.txt.....	146
hp_ds_xml_config.txt.....	147
Chapter 6: Troubleshooting.....	148
SafeCom Help Desk Assistant.....	148
Servlets.....	148
SafeCom Go HP software installation troubleshooting.....	148
SafeCom Go HP log entries dated 1 January 1970.....	149
SafeCom Go HP has incorrect IP address.....	149
The device does not send tracking data to the SafeCom Server.....	150
Device Server: Configuration of devices failed.....	150
Device Server: Error when upgrading existing Device Server installation.....	150
Device Server: Cannot re-add FutureSmart device.....	150
Device Server: Devices are not configured against failover device server.....	151
Device Server: No HP OPS server configured on device.....	151
Device Server: HP OPS running on Windows Server 2003.....	151
Device Server: HP OPS service fails to start during system restart.....	151
Check if third-party components are running.....	151
Check the installed file set.....	152
Check the device configuration.....	152
Handling known installation issues.....	152
HP Pro connectivity and certificate issues.....	153
Checking network settings.....	153
Check timezone settings.....	154
Check the certificate.....	154
Special symptoms.....	154
Go FS cannot access Print Engine.....	155
FutureSmart device cannot be configured.....	155
At the Printer: Loading SafeCom.....	155
At the printer: No Pull Print icon.....	155
At the Printer: No automatic logout.....	155
At the Printer: Card reader not working.....	155
At the Printer: Authentication failed.....	156

At the Printer: Error Printing: 194.....	156
At the Printer: Printer busy, retry later.....	156
At the Printer: Printing disabled.....	156
At the Printer: Source not reachable / Job inaccessible.....	157
At the Printer: OXPd Application Error Message 45.00.07.....	157
At the Printer: USB Error.....	158
At the Printer: error cc = 500.....	158
At the Printer: Log out button and timeout.....	158
At the Printer: Concurrent job tracking issues.....	158
Tracking records state issues.....	158
Low resolution icons displayed on FutureSmart devices.....	158
At the Printer: 49.08.06 DEVICE ERROR after installing or upgrading the Go HP bundle through SafeCom Administrator.....	159
At the Printer: 49.38.03 DEVICE ERROR after installing the Go HP bundle through SafeCom Administrator.....	159
At the Printer: OK button inactive on Login denied screen.....	159
Chapter 7: Regulatory information.....	160

Preface

This guide includes instructions for installing and using Kofax SafeCom Go HP.

Related documentation

To access the full documentation set for Kofax SafeCom, use this link:

<https://docshield.kofax.com/Portal/Products/SafeCom/10.530-jaah72kksf/SafeCom.htm>

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 HP is a solution for HP LaserJet MFPs. It integrates with the touch-screen control panel of the HP MFP and offers user authentication by code or card. SafeCom P:Go HP is the internal solution for HP LaserJet printers and offers user authentication by card.

SafeCom Go HP 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 and scalable solutions.

Requirements

SafeCom Go HP supports any networked HP LaserJet MFP, printer, and scanner listed at https://knowledge.kofax.com/MFD_Productivity/00_Supported_Devices/Supported_Devices.



- On M527/M553/M577/M605 devices, registration, MAC and firmware detection may result in issues due to SNMP limitations. In such cases, ensure that the CONFIG/NET/MAC nodes of the config.xml are set correctly and you are using the correct xml.
- Starting with the 2014 HP FutureSmart firmware, you must decide between using the more secure SHA-256 Hashing algorithm and the legacy SHA-1 Hashing algorithm. SafeCom Go HP FS and Device Server are distributed as signed with SHA-1 Hashing algorithm. For additional information, see [Allow installation of legacy packages](#).

Users who would prefer using SHA-256 must purchase and use special edition SafeCom device software files that are SHA-256 signed.

- HP devices can run SafeCom Go inside by installing SafeCom Go HP software on the device's hard disk (HDD) or on the SafeCom supplied media, that is, USB key or Flash Memory Card (FMC). HP devices with FutureSmart firmware can run the SafeCom Go solution inside (FS) or through the SafeCom Device Server (DS). The HP Sx devices and HP Officejet Pro devices requires the SafeCom Device Server (DS).
- A SafeCom G4 Server and a SafeCom ID device license for the device are required to use the HP Access Control USB proximity card reader (CZ208A).
- **HP Sx** series devices support only keyboard (KBD) emulating SafeCom ID devices in addition to the HP Access Control USB proximity card reader. HP Sx devices do not support Auto-sense login method and logout by card. The web interface and behaviour is different from other HP devices.
- **HP Officejet Pro** series devices require installation of the HP server component HP OPS (OXPd Professional Services) which can be downloaded from the SafeCom website (for more

information, see [HP OPS installation](#)). Due to device limitations, there is no tracking of Copy, E-mail, and Scan and prints are tracked at the server only.

- Due to limitations in the HP Officejet firmware, only HP Access Control USB proximity card reader (see [HP Access Control USB proximity card reader](#)) and SafeCom ID devices with [R] marked USB readers are supported. Support for remaining readers, including [E] marked readers will happen with future HP firmware.
- If users are to log in by card and the device has no Hardware Integration Pocket or external USB port, it is necessary to install a SafeCom Go HP ID Kit in either an empty EIO slot or mounting together with the device's HP Jetdirect network card (bracket is replaced using the supplied screwdriver with Torx 8 bit).

SafeCom Device Server:

- The SafeCom Device Server needs to be installed on a Windows 2008 or 2003 SP2 server with at least 1.4 GHz CPU and 2 GB RAM.
- A SafeCom Device Server can handle between 100 - 200 devices. This is of course subject to the use pattern, computer resources and network. Once it is installed, it runs as a Service (SafeCom Device Server).



- If you are using the Device Server on a Windows 2003 SP2 server with HP Officejet Pro devices, check the Troubleshooting section (see [Device Server: HP OPS running on Windows Server 2003](#) and [Device Server: HP OPS service fails to start during system restart](#)) for known HP OPS issues.
- If your device fleet includes HP Pro devices, ensure that the HP Pro devices are using a dedicated device server.

SafeCom Go HP products

<p>SafeCom Go HP</p>	<p>Identification by ID code on: MFP M525, MFP M575, MFP M725, MFP M775, M3035 MFP, CM3530 MFP, CM4540 MFP, M4555 MFP, CM4730 MFP , M5035 MFP, M5039 MFP, CM6030 MFP, CM6040 MFP, CM6049 MFP, M9040 MFP, M9050 MFP, M9059 MFP. Scanjet 7000n, Digital Sender Flow 8500 fn1 (formerly ScanJet Enterprise 8500fn1), MFP 830, MFP M880, MFP S970dn, MFP S962dn, MFP S951dn, S956dn, X576dw MFP, X476dw MFP, X476dn MFP, 276dw MFP and Digital Sender 9250C.</p> <p>Identification by USB ID device on: M3035 MFP, CM4730 MFP, M5035 MFP, M5039 MFP, CM6030 MFP, CM6040 MFP, CM6049 MFP, M9040 MFP, M9050 MFP, M9059 MFP, MFP S970dn, MFP S962dn, MFP S951dn, S956dn, X576dw MFP, X476dw MFP, X476dn MFP, 276dw MFP. Digital Sender 9250C.</p> <p>Identification by mini-USB ID device mounted in hardware integration pocket on: MFP M525, MFP M575, MFP M725, MFP M775, CM3530 MFP, CM4540 MFP, M4555 MFP. Scanjet 7000n, Digital Sender Flow 8500 fn1 (formerly ScanJet Enterprise 8500fn1), MFP 830 and MFP M880.</p> <p>Order the license and USB ID device separately.</p>
-----------------------------	--

SafeCom Go High-end HP	<p>Identification by ID code on: CM8050 MFP, CM8060 MFP.</p> <p>Identification by USB ID device on: CM8050 MFP, CM8060 MFP.</p> <p>Order the license and USB ID device separately.</p>
-------------------------------	--

SafeCom P:Go HP products

SafeCom P:Go HP	<p>Identification by ID code on: M855, M806, M750, X551dw Printer, 251dw Printer</p> <p>Identification by USB ID device on: M551, M601, M602, M603, M712, M750, 3000 (incl. HDD), CP3505 (incl. HDD), CP3525 (incl. HDD), 3800 (incl. HDD), P4014 (incl. HDD), P4015 (incl. HDD), P4515 (incl. HDD), CP4525 (incl. HDD), CP4025, CP5525, CP6015 (incl. HDD), X551dw Printer, 251dw Printer.</p> <p>Identification by mini-USB ID device mounted in hardware integration pocket on: M855, M806</p> <p>Order the license and USB ID device separately.</p>
SafeCom HP USB Key	<p>Identification by USB ID device on: 3000 (excl. HDD), P3005, P3015, CP3505 (excl. HDD), CP3525 (excl. HDD), 3800 (excl. HDD), P4014 (excl. HDD), P4015 (excl. HDD), P4515 (excl. HDD), CP4525 (excl. HDD), CP4025, CP6015 (excl. HDD).</p> <p>SafeCom HP USB Key: USB Key.</p> <p>Order the license and USB ID device separately.</p>

SafeCom ID devices

SafeCom Go HP supported SafeCom ID devices

Identification Method	USB p/n	Serial p/n	Mini-USB E12 p/n
Kofax MX Proximity Reader	970920	970910	970940
Kofax MX Proximity Reader - Legic	976920	976910	976940
SafeCom Barcode Reader	694020	694010	
SafeCom Magnetic Card Reader (Tr 1)		959010	
SafeCom Magnetic Card Reader (Tr 2)		954010	
SafeCom Magnetic Card Reader (Tr 3)		657010	
SafeCom Magnetic Card Reader DD (Tr 1)	692010		
SafeCom Magnetic Card Reader DD (Tr 2)	691020		
SafeCom Magnetic Card Reader DD (Tr 3)	692020		

Additional information about the ID devices is available in the *SafeCom G4 Administrator's Manual*.



- 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.
- SafeCom also supports the HID OMNIKEY 5427 CK Rijkspas reader, if the user acquires the above-mentioned relevant third-party licenses.

Supported languages

The following list of languages and their suffixes are supported by the SafeCom Device Server.


Suffix	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

HP Universal Print Driver

HP Universal Print Driver version 5.9 is available for PCL5, PCL6, and PostScript to be used with SafeCom Pull Print if it is installed and run in Traditional mode, where UPD forwards the print data to the SafeCom Pull Port.

1. Obtain a copy of the HP Universal Print Driver and unpack it. Double-click **install.exe** that came with the HP Universal Print Driver.
2. Click **Yes** to accept the license agreement.
3. Select **Traditional mode** and click **Install**.
4. The Add Printer Wizard appears.

5. On Windows 2008 and 2012: Click **Add a local printer**. On Windows 2003: Click **Next**. Select **Local printer** and clear **Automatically detect and install my Plug and Play printer**. Click **Next**.
6. Select **Create a new port** and select **Standard TCP/IP Port** from the dropdown list. Click **Next**.

 To allow the UPD to optimize its output and reduce print files, it should connect to the HP device through a Standard TCP/IP port once before it is changed to use a SafeCom Pull Port.


7. The Add Standard TCP/IP Printer Port Wizard appears, click **Next**.
8. Enter **Printer Name or IP Address**. Click **Next**. Click **Finish**.
9. Select the HP Universal Printing variant (PCL5, PCL6, or PS) that match your needs and click **Next**.
10. Enter a **Printer Name** and select if this printer is your default Windows printer. Click **Next**.
11. Check **Share this printer...** and enter **Share name**. Click **Next**.
12. On Windows 2008 and 2012: Do not click **Print a test page** to verify the system. Click **Finish**. On Windows 2003: Select **No** to print a test page to verify the system. Click **Next**. Click **Finish**.
13. The UPD is now installing which may take some minutes. Please be patient.
14. When the **HP Universal Printing Installation** dialog reports that the installation has completed, you can click **Finish**.

Check the Printer properties

1. Right-click the printer and click **Printer properties**.
2. On the **Device Settings** tab, scroll to **Installable options** and change **Automatic Configuration** to **Update Now**. This will cause the UPD to contact the device and get information about its configuration.
3. Click **Apply**.
4. On the **Advanced** tab, check **Start printing after last page is spooled** as this allows faster spooling.
5. Click **Apply**.

Make the printer use the SafeCom Pull Port

1. Click on the **Ports** tab in the **Printer properties** dialog.
2. Clear **Enable bidirectional support**. Click **Apply**.
3. Click **Add Port...**
4. Select **Create a new port** and select **SafeCom Pull Port** from the dropdown list. Click **Next**.
5. Enter a unique name of your choice for the port in **Port Name**. Click **OK**.
6. The **Configure SafeCom Pull Port** dialog prompts you to enter the IP address or host name of the SafeCom Server and select **Use network logon** as method of **Authentication**. Click **OK**.

 It is possible to configure the SafeCom Pull Port to override the HP Universal Printing driver name.

7. Click **OK**. The **SafeCom User Logon** dialog appears. Enter **User logon** and **Password** of a user that has SafeCom Administrator or Technician rights.

8. Click **OK**.
9. Click **Apply**.

Print a test page

1. Click on the **General** tab in the **Printer properties** dialog.
2. Click **Print Test Page** to verify the system. Click **Close** when prompted to confirm that the test page printed correctly.

For high load systems you can minimize the wait for documents to be processed and transferred to the SafeCom server by checking **Enable printer pooling** on the **Ports** tab and add multiple identically configured SafeCom Pull Ports. In our experience 1-4 ports is sufficient and no more than 12 ports should be added.

HP Universal Print Driver Remarks

- The installation of the UPD may take several minutes, be patient.
- The print jobs produced with UPD can be quite large in size as everything is always rendered in color, even if the device does not support color. This goes for PCL5, PCL6, and PostScript. To improve performance, it may be necessary to use the printer's "normal" driver. To investigate print to file and compare the respective file sizes.
- In a Microsoft Clustered Environment, the UPD must be installed on the virtual server. However, if you wish the UPD to appear on the nodes that make up the cluster server it must be installed on each of these nodes.

The HP Universal Print Driver can also be used for together with the SafeCom Push Port for tracking of documents that are sent directly to the device.



- Post tracking data is not available for HP Officejet Pro devices.
- Some applications may split (for example, when using mixed page size) the print job at the device to multiple jobs, which are then tracked and charged (for the start-up cost) separately.

Chapter 2

Device Server installation

Make sure the SafeCom G4 Server software installation has been completed as described in the *Kofax SafeCom G4 Server Administrator's Guide*.

For HP FutureSmart devices, it is also possible to enable SafeCom Go HP through the SafeCom Device Server.

Install SafeCom Device Server

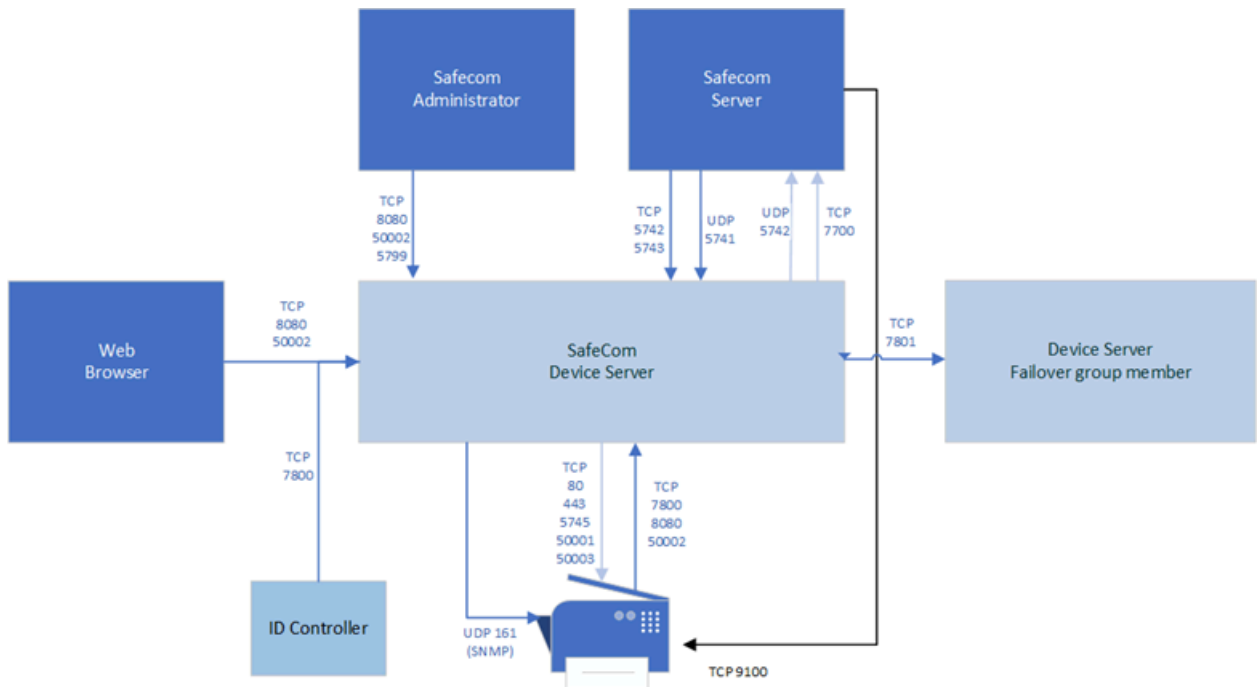
1. Download the `SafeCom_Device_Server_x64_build_{version_number}.exe` file from the link supplied to you or insert the SafeCom CD. The installation must be **Run as administrator**.
2. When the installation program is launched, click **Next**.
3. Select the destination folder for the files. Click **Next**.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



TCP	Inbound on SafeCom Device Server	Protocol
7800	Used when supporting SafeCom ID controller	SafeCom
7801	Device Server Failover Coordination	SafeCom
UDP	Inbound on SafeCom Device Server	Protocol
5741	Used between the SafeCom Administrator, SafeCom Go, SafeCom Device Server, and SafeCom Controller	SafeCom
TCP	Outbound on SafeCom Device Server	Protocol
7627	SOAP Interface on HP FutureSmart devices	HTTPS
7801	Device Server Failover Coordination	SafeCom


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)

 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

Setting	Description	Default
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.preferIP	Allows administrator to control if devices should contact the Device Server by its IP or its host name. <div style="background-color: #e6f2ff; padding: 5px; border: 1px solid #add8e6;"> <p>i Setting this option to false requires that the DNS settings (and search domains) on the devices are set correctly, otherwise the devices will be left in a non-working state.</p> </div>	true
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**.

If the SNMP Community name is not the default, ensure that you set the device password correctly to be able to add the device to SafeCom.

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 **SafeCom Go HP** 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**.

 This note is only included in go hp.
If your device is detected incorrectly, you can mark the **Add as generic device** box to add the device as a generic device.

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.

Adding Sx devices to the Device Server

When adding Sx series devices to the SafeCom Device Server, you need to perform the following additional steps:

1. Add the Sx device to the SafeCom Device Server as outlined above in [Add device through the SafeCom Device Server](#).
2. Open the device web page in a browser.
3. Login as administrator.

4. Ensure that SSL is enabled by browsing to **Security Setting > SSL Setting** and setting **HTTPS** to **Enabled** on both server and client ports. Click **Submit (U)**.
5. Setup SafeCom as the authentication application:
 - a. Browse to **Application Settings > External Applications Settings > External Accounting Application Settings**.
 - b. Set **External Account Control** to **Enable**.
 - c. Check **Set Authentication Server (Server 1)**.
 - d. Set **Server 1** to **Enable**.
 - e. Set **Application Name** to **SafeCom Go**.
 - f. Set **Address for Application UI** to `https://{device_server_IP}:50002/safecomosa/go`.
 - g. Set **Address for Web Service** to `https://{device_server_IP}:50002/safecomosa`.
 - h. Set **Display Style** to **Full**.
 - i. Click **Submit (U)**.
6. Register the Pull Print application.
 - a. Browse to **Application Settings > External Applications Settings > Standard Application Registration**.
 - b. Click **Add (Y)**.
 - c. Set **Application Name** to **Pull Print**.
 - d. Set **Address for Application UI** to `https://{device_server_IP}:50002/safecomosa/PullPrintScreen`.
 - e. Optionally, check **Use Custom Icon** and upload an icon if you want to use a custom icon for Pull Print.
 - f. Click **Submit (U)**.
7. Reboot the device.
 - a. Browse to **Status > Power Reset**.
 - b. Click **Execute (J)** next to the **Reboot the MFP** label. Click **Execute (J)** again.

Configure the device on the device web page

The device is now added to the SafeCom Device Server, but a few things must be verified manually on the web page for each device.

For both MFPs and Printers:


- Set up device server address

For MFPs only:

- Verify the sign-in method and access control
- Verify the Quota Server Address






Set up device server address

1. Access the SafeCom configuration page, by clicking the **General** tab and then **SafeCom** in the menu on the left.
2. Under **Configuration**, verify that the server address specified in the **Server Address** field points to the SafeCom Device Server.
 - Server port 50002 is specified when using SSL (secure socket layer).
 - Server port 8080 is specified when using unencrypted.

 By adding more server addresses under **Configuration**, it is possible to set up the server failover list for the device. This is then automatically updated on the device server web page and vice versa.

3. Click **Apply** at the bottom of the web page.

The following 5 icons represent the status of the devices:


	Connected: This is the device server that the device is connected to.
	Valid, but not connected: The device server is running but the device is connected to another device server.
	Testing: The server address is being tested.
	Invalid: The server address is NOT that of a SafeCom Device Server.
	Not responding: The device server is not responding.

Set sign-in method and access control

1. Open the device web page in a web browser.
2. Click **Sign In** in the upper-right corner of the web page and enter username and password.
3. Click the **Security** tab and then **Access Control** in the menu to the left.
4. Under **Sign In and Permission Policies**, make sure that the general sign-in method is set to **SafeCom**.
5. If needed, change the sign-in method for each of the **Control Panel Applications** listed.
6. For all applications that must be controlled by SafeCom, select the **Device guest** check box, so the yellow pad lock symbol appears. This means that login is required.
7. Make sure to select the **SafeCom** check box for each application that a SafeCom user must have access to at the device.
8. Click **Apply** at the bottom of the web page.

Verify Quota Server address

1. Click the **General** tab, and then **Quota and Statistics Services** in the menu on the left.
2. Check the **Connect this device to a Quota server**.
3. Make sure that the name specified in the **Quota Server URL** field is correct - it must be the same as the SafeCom Device Server address. If necessary, correct the address manually.


 With SafeCom Go HP version S89 nnn.050*13 and S95 nnn.050*13 or later, the quota server is set up automatically.

4. Click **Apply** at the bottom of the web page.

Configure device in SafeCom Device Server

The **Device** tab is used to configure SafeCom Go HP, 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.

 If you click **Save** and then in the **Device Message** field see the message "Unable to configure device because: Device is configured against a different server", the device is configured to a different server. To be able to make changes to the device configuration, first click **Reconfigure device**, which configures the device to your server, make the necessary changes, and then click **Save**.


Device Settings

Manufacturer:	HP		
Model:	HP Color LaserJet MFP E77830		
MAC Address:	F430B9EF8567		
Serial number:	CNB8K8G0ZG		
Device Message:	<input type="text"/>		
Device information			
Contact:	<input type="text"/>	Location:	<input type="text"/>
Description:	<input type="text" value="NP1EF8567"/>		
Network settings			
Address:	<input type="text" value="10.144.200.135"/>	RAW print port:	<input type="text" value="9100"/>
Select SNMP version:	<input type="text" value="SNMP2"/>		
SNMP get community:	<input type="text" value="public"/>	SNMP put community:	<input type="text"/>
Device settings			
Administrator name:	<input type="text" value="admin"/>	Administrator password:	<input type="password" value="****"/>
Login method:	<input type="text" value="Auto-sense"/>	Default domain:	<input type="text"/>
Language:	<input type="text" value="(Auto)"/>	Idle timeout:	<input type="text" value="30 seconds"/>
<input type="checkbox"/> Hide domain <input type="checkbox"/> Enable post tracking <input type="checkbox"/> Reverse document list <input type="checkbox"/> Mask ID code			
Drivers Device applications Enable user authentication and tracking per application.			
<input checked="" type="checkbox"/> E-mail <input checked="" type="checkbox"/> Copy <input checked="" type="checkbox"/> Color Copy <input checked="" type="checkbox"/> Fax <input checked="" type="checkbox"/> Scan to Folder <input checked="" type="checkbox"/> Scan to USB <input checked="" type="checkbox"/> USB print			
<input checked="" type="checkbox"/> Enable logging			
			<input type="button" value="Restore factory default"/>
			<input type="button" value="Reconfigure device"/>

Change the settings according to the following descriptions:


- **Device information**
 - **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.
- **Network settings**
 - **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.
 - **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**
- **Device settings**
 - **Administrator name:** The username with which the administrator can log in to the device.
 - **Administrator password (mandatory):** The device password with which the administrator can log in to the device.
 - **Login method:** This determines how users log in. Select between:
 - **Auto-sense.** Auto-sense maps to **Card or Windows** if an ID device is connected to the MFP and on devices it maps to **Card**. Otherwise, it maps to **ID code**. Mapping changes within 10 seconds after the ID device is either connected or disconnected. If it does not change a restart of the device may be required.
 - **Card**
 - **ID code**
 - **Card or ID code**
 - **Card or Windows:** Allows the user to log in either by card or by entering their Windows username, password, and domain.

 Identification by card requires connecting a USB ID device (card reader). The option **Card or Windows** allows the user to log in either by 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.

- **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. 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).
- **Language:** Specify a specific language if you want SafeCom Device Server to override the language on the device.
- **Idle timeout:** Specifies in seconds when a logged in user is automatically logged out if there is no activity.
- **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 rxe "Tracking data adjustment"xe "Post track"levant only with SafeCom Tracking. Refer to the *SafeCom G4 Administrator's Manual*.

- **Reverse document list:** Check to show the latest 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.

 Be aware that post tracking is not available for HP Officejet Pro devices.

- **Drivers:** 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.
 - Click **Get All** to obtain the list of drivers from the SafeCom Server, or add and delete drivers manually.
- **Device Properties:**
 - **3rdPartyAuthDomain** (optional): Specify the string where the third party domain is specified.
 - **3rdPartyAuthEnable:** To enable third party authentication, change the property value from **False** to **True**.
 - **3rdPartyAuthIDcode:** Specify the string where the third-party ID code is specified. Either `3rdPartyAuthIDcode` or `3rdPartyAuthUserLogon` *must* be specified.
 - **3rdPartyAuthUserLogon:** Specify the string for where the third-party user logon is specified. Either `3rdPartyAuthIDcode` or `3rdPartyAuthUserLogon` *must* be specified.
 - **SafeComGoVersion:** The SafeCom Go version used on the device.
 - **BillingEnabled:** Set to **True** to display the **Account** icon on the device screen, allowing you to set up the billable account. Set to **False** to remove the icon.
- **Device applications:** Lists what users are allowed to access. Uncheck the applications that do not require user authentication.
- **Enable logging:** Select if log information should be collected.
- **Restore factory default:** Sets all settings back to their default values, except the password.
- **Reconfigure device:** Reference the device to the current SafeCom Device Server.

Configure device server failover

SafeCom Administrator allows you to group your device servers, enabling a failover solution.

Device servers belonging to the same group monitor the status of the group members, and in case of a group member failing or shutting down, the rest of device server group distributes the workload of the downed device server among the rest.



- If device failover occurs while a user is logged in, the fallback to the "home" device server does not occur until the user logs out and the device goes into idle state; this prevents user session interrupts.
- When a device failover or device server fallback occurs, the device may need rebooting, depending on the vendor (the device reboot is handled automatically).

1. Log in to **SafeCom Administrator**.
2. Open the **Device Server** list.
3. Click **Add device server group**.
4. Enter a name and optionally a description for the device server group.
5. Click **OK**.
6. Drag and drop the device servers to incorporate them into the newly created group.

SafeCom Go HP web interface

The SafeCom Go HP web interface adheres to the structure and design of the HP Embedded Web Server (EWS).

Login

1. Open the device in a web browser by entering the device address in the address field. JavaScript (Active Scripting) must be enabled.
2. Click **Sign In** in the upper-right corner of the page and enter the username and password.
3. Click **OK**.

Product and version information web page

1. Open the device in a web browser.
2. Click the **Information** tab.
3. Click **SafeCom** on the menu to open the **Information** web page with product name and version.




This option is not available for HP Sx-series devices.

Configure and log information web page

1. Open the device in a web browser and log in.
2. Click on the **General** tab.
3. Click **SafeCom** on the menu to access the SafeCom specific page with configuration and log information.

4. Under **Configuration**, it is possible to change the Server Address and the Server Port for the SafeCom Device Server.
5. Under **Log Information**, select to enable or disable the log, to **Show complete log**, or to **Clear log**.

 This option is not available for HP Sx-series devices.

SafeCom Go HP – How to

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


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** drop down menu under **SafeCom Settings**, select how users must identify themselves at the device.

Select between:

- Auto-sense (default)¹
- ID code
- Card
- Card or ID code
- Card or Windows
- Keypad²

- 
- Identification by card requires the installation of a SafeCom ID device (card reader), potentially SafeCom Go HP ID Kit. Identification by ID code is possible on devices with touch-screen, built-in keypad, or external SafeCom Keypad (see the table in [SafeCom Go HP products](#)).
 - For card registration to work when using Windows credentials, you must have at least one valid PUK code available in the G4 system.

¹ For the HP Sx series, auto-sense is not available and, instead, the default login method is Card or ID Code.

² Keypads are no longer sold. This option is only relevant on selected printer.

Enable Copy Control

The SafeCom solution can control access to the MFP's copy function.

For SafeCom to be able to control and track Copy and Copy color, it needs to be set up as follows:

Tracking of copy and copy color must be enabled in SafeCom Device Server.

The authentication method must be set up to SafeCom on the web page for the individual device.

Setup of copy color on the device's web page must correspond to the settings made on the device server.

First enable SafeCom to do tracking on copy and copy color on the Device server:

See [Enable SafeCom to do tracking on copy and copy color on the Device server](#).

Secondly, the authentication method on the web page must be set up for the copy application on the device³:


See [Set up the authentication method on the web page](#).

Thirdly, make sure that the Main Color Settings are set up correctly on the device's web page. The settings need to match the setting on the device server.

See [Open the Main Color Settings](#).

Enable SafeCom to do tracking on copy and copy color on the Device server

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. Click **Device applications**.
4. Check **Copy** in the list of applications. To allow the user to copy in color as well, select the **Copy color** check box.
5. Click **Save**.

 By default, both **Copy** and **Copy color** are checked. Enabling access control for color copy only is not recommended if the SafeCom solution is also to track copies. Mono copy jobs that are produced after the user has logged in to the color copy function are tracked as long as the user remains logged in. Mono copies are obviously not tracked when there is no user logged in. Similar situations arise if **Copy** is checked and **Copy color** is cleared.

Set up the authentication method on the web page

1. Open the device in a web browser and log in.
2. Click the **Security** tab and then **Access Control**.

³ For HP Sx series, no setup is required on the web page.

3. Under **Control Panel Application**, restrict the access for all copying by selecting the **Device Guest** check box for **Copy application**.
4. If you want to restrict access only for copy color then expand **Copy application** menu and check **Device Guest** for **Make a color copy**.
5. Select **SafeCom** as the sign-in method.
6. Click **Apply** at the bottom of the web page.

i On the device HP CM 6040 MFP, it is possible to disable user authentication for Color copy, but leave Copy authentication enabled. But if a user has copy enabled and color copy disabled set up on the SafeCom Server, the user will only be able to make a B&W copy and Color copy is denied. This is because the settings on the SafeCom Server overwrite the settings on the device.

Open the Main Color Settings

To open the Main Color Settings:

1. Open the device in a web browser and log in.
2. Click the **Copy/Print** tab and then **Restrict Color**.
3. Verify that the copy color settings under **Main Color Settings** are set up so they match the settings on the device server. If for example copy color is enabled in the device server, the **Enable Color** on the web page must be checked as well.
4. Click **Apply** at the bottom of the web page.

Enable Scan to Folder

For SafeCom to be able to control access and track **Scan to Folder**, it needs to be set up as follows:

- Tracking of **Scan to Folder** must be enabled in SafeCom Device Server.
- The authentication method must be set up to SafeCom on the web page for the individual device.
- The save to folder application for each device must be enabled on the device's web page.

First enable SafeCom to do tracking of **Scan to Folder** on the Device Server:

See [Enable SafeCom to do tracking of Scan to Folder on the Device server](#).

Second, the authentication method on the web page must be set up for the **Save to Network Folder** application on the device⁴:

See [Set up the authentication method on the web page for the Save to Network Folder application](#).

Third, make sure that Save to Network Folder is enabled on the device's web page.

See [Enable Save to Network Folder on the device's web page](#).

Enable SafeCom to do tracking of Scan to Folder on the Device server

1. Open a web browser and log in to the SafeCom Device Server.

⁴ For HP Sx series, no setup is required on the web page.

2. Click on **Device server** in the menu on the left, and then click on the device.
3. Click **Device applications**.
4. Make sure that **Scan To Folder** is checked in the list of applications.
5. Click **Save**.

Set up the authentication method on the web page for the Save to Network Folder application

1. Open the device in a web browser and log in.
2. Click the **Security** tab and then **Access Control**.
3. Under **Control Panel Application**, restrict the access for the copying by selecting the **Device Guest** check box for **Network Folder application**.
4. If you want to restrict access for editing the network folder path, expand **Network Folder application** and check **Device Guest** for **Ability to edit network folder path**.
5. Select **SafeCom** as the sign-in method.
6. Click **Apply** at the bottom of the web page.

Enable Save to Network Folder on the device's web page

1. Open the device in a web browser and log in.
2. Click the **Scan/Digital Send** tab and then **Save to Network Folder Setup**.
3. Select the **Enable Save to Network Folder** check box and verify that the other save to network folder settings are set up according to your needs.
4. Click **Apply** at the bottom of the web page.

Enable E-mail

SafeCom can control access to the MFP's Send to E-mail function. For SafeCom to be able to control access and track e-mails, it needs to be set up as follows:

- Tracking of **E-mail** must be enabled in SafeCom Device Server.
- The authentication method must be set up to SafeCom on the web page for the individual device.
- The **E-mail** application for each device must be enabled on the device's web page.

First enable tracking on e-mails on the SafeCom Device server:

See [Enable tracking e-mails on the SafeCom Device server](#).

Second, the authentication method on the web page must be set up for the **Send to E-mail** application on the device⁵:

See [Set up the authentication method on the web page for the Send to E-mail application](#).

Third, make sure that **E-mail** is enabled on the device's web page.

See [Enable E-mail on the device's web page](#).

⁵ For HP Sx series, no setup is required on the web page.

Enable tracking e-mails on the SafeCom Device server


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. Click **Device applications**.
4. Check **E-mail** in the list of applications.
5. Click **Save**.

Set up the authentication method on the web page for the Send to E-mail application

1. Open the device in a web browser and log in.
2. Click the **Security** tab and then **Access Control**.
3. Under **Control Panel Application**, restrict the access for the e-mail by selecting the **Device Guest** check box for **E-mail application**.
4. Select **SafeCom** as the sign-in method.
5. Click **Apply** at the bottom of the web page.

Enable E-mail on the device's web page

1. Click the **Scan/Digital Send** tab and then **E-mail Setup**.
2. Select the **Enable Send to E-mail** check box and verify that the other save to network folder settings are set up according to your needs. For example, the default from and to e-mail addresses are set up under the **Address and Message Field Control** pane. To set up for example the default from address to the user's e-mail address, select **User's address (Sign-in required)** in the **From:** field.
3. Click **Apply** at the bottom of the web page.

 Be aware that the set-up of default **From:** and **To:** e-mail addresses is no longer handled by SafeCom. Now the settings are available on the device web page on the **Scan/Digital Send** tab under **E-mail Setup**.

Control user access rights

When using SafeCom G3 server version S82 070.440*03 or newer, you can control users' access rights to specific features through SafeCom Administrator, refer to the *SafeCom G4 Administrator's Manual*. You can control access rights to the following features:

- Copy
- Copy in color
- E-mail
- Scan
- Fax
- USB memory print
- USB memory scan


- Print all button

Enable Client Billing and the account icon on the device

The **Account** application and icon is already installed and available on HP MFPs and scanners when the SafeCom solution is enabled through the Device Server.

Note that the following two settings must be set up in the **SafeCom Administrator** for the billing code to become part of the tracking record.

- **Client Billing** must be checked on the **License** tab in the **Device properties** dialog in SafeCom Administrator.
- **Bill clients for cost** must be checked on the **Settings** tab in the **User properties** dialog in SafeCom Administrator.

 Be aware that Client Billing is not available for HP Officejet Pro devices.

Enable third party authentication

To enable users to log in using an authentication method unknown by SafeCom:

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. Click **Device properties** and change the property value for **3rdPartyAuthEnable** to **True**.
4. Enter the property values for **3rdPartyAuthIDcode**, **3rdPartyAuthUserLogon**, and **3rdPartyAuthDomain**.

The property values must be the field names where the login information is stored.

As a minimum, the property values for either **3rdPartyAuthIDcode** or the **3rdPartyAuthUserLogon** must be specified.

5. Click **Save**.

Enable using the Home Folder

The Home Folder feature allows users to save their work to a personal network folder. Using the folder requires meeting the following requirements:

- The folder name is given as a fully qualified domain name.
- The users to be assigned for using the feature must be members of the domain.
- The default domain must be set through the SafeCom Go web page.
- The applications (scan, fax, email, and so forth) to be used for jobs destined to the Home Folder must have the proper access rights for the folder (read, write).
- The applications (scan, fax, email, and so forth) to be used for jobs destined to the Home Folder must have the relevant credentials to access the folder (preferably the user's own credentials should be used).
- Home Folder name must not contain the % character.
- The device must have FW version 3.5.1 or newer.
- SafeCom Go FS *30 or newer.

i Due to limitations of firmware versions older than 3.8, the User Name field on the Sign In form of the device is not filled, meaning that users must enter their credentials manually. On firmware version 3.8 or newer, the issue is no longer present.

When using CSV import with Home Folder, ensure that you use the full folder path of the users (\{IP address}\Home\{username}).

To set the usage of the Home Folder, do the following:

1. Open the device in a web browser and log in.
2. Click the **Scan/Digital Send** tab and then **Save to Network Folder Setup**. Select Add or Configure, as appropriate.
3. Set the **Save to a personal shared folder** option and enter **HomeFolder** (case sensitive) in the **Retrieve the device user's home folder using this attribute** field.
4. Select the **Save to Network Folder** check box, then click **Apply settings**.
5. Click **Next**, then **Save**.
6. Login to SafeCom Administrator.
7. Set the Home Folder for users through either:
 - Enter the **Home folder** property manually on the **Identification** tab of **User Properties**.
 - Use the **Import Home Folder** AD field in the **Active directory configuration** page of **User Import Configuration**.

Enable SafeCom Mobile Pull Print

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 device 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*.

Make sure that the default domain is configured on the device in SafeCom Device Server (see [Configure 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*.

Determine the version

i Not applicable to HP Color MFP S970dn, S962dn, S951d, HP MFP S956dn.

The version of the SafeCom Device Server can be seen in SafeCom Administrator.

The version of the SafeCom Go HP software can be determined from the Information web page.

1. Open the device in a web browser and log in.
2. Click the **Information** tab.

3. Click **SafeCom** to view the product information (Product name, Version, Version date, and Version time). The version number is in the format: S95 nnn.xxx

Handle new MAC address (Jetdirect network card)

In the SafeCom database, the device is recorded by its unique MAC address. The device's MAC address changes if the Jetdirect network card is changed. On devices with Jetdirect Internal (JDI), the MAC address changes if the formatter board with the network connector is replaced.

To resolve this, it is recommended to delete the device from the SafeCom database and add it again by re-registering it.

1. Open **SafeCom Administrator**.
2. Right-click the device and click **Delete device**.
3. Open the **Register** web page re-registering it and click **Register**.
4. Refresh the list of devices in **SafeCom Administrator** to verify that it has been registered again.

Verify that SafeCom Go HP is loaded

To establish if SafeCom Go HP software is loaded you can access the web page for the device⁶:

1. Open the device in a web browser and log in.
2. Click **General**.
3. Click **Solution Installer** and verify under the **Installed Solutions** pane that SafeCom Go is installed.

Register device

The device must be registered with the SafeCom solution in one of the following ways:

- Add the device in the SafeCom Administrator using **Add device**.
- A user with Technician or Administrator rights must log in at the device.

Configure Push Print Post Tracking

SafeCom Push Print Post Tracking is an extension of the tracking feature of the SafeCom solution. The tracking and charging data was based on the information that former versions of SafeCom components were able to collect while documents were printing at the workstation or the server. This data is not accurate enough to calculate the precise tracking information and the price of the jobs. The software utilizes the detailed information that is sent by the printing device itself and all information is calculated from these reports.

Configuring Post Tracking push print jobs

The feature does not require extra steps to configure devices for post tracking push print jobs, as all SafeCom components automatically recognize whether the feature is available in the specific configuration. You simply have to add the device to the SafeCom G4 Server and associate it to a

⁶ For HP Sx series, this does not apply.

SafeCom Push port. By enabling the Post-Track option on the Web configuration page of the device or in SafeCom Administrator, both push and pull jobs will be tracked based on the job information reported by the device itself.

Using Push Print Post Tracking

The SafeCom push print post tracking extends the usage of the existing tracking feature, allowing you to track push print jobs in more detail.

All Push Print jobs for which Post Tracking is enabled are created in a **Pending** state, and remain in this state while awaiting post tracking data; this state can last up to 48 hours. The length of time jobs spend in **Pending** state can be configured using the CleanPushTrackPendingInterval 32-bit DWORD registry setting under `HKEY_LOCAL_MACHINE\SOFTWARE\SafeCom\SafeComG4`. The default value is 48 hours. The system will update the track list every 6 hours.

- If the post tracking data is received within the **Pending** time period, the tracking record is updated with the precise counters and the job status is set to **Completed**, and if necessary (based on the cost calculated based on the post tracking data). In pay environment, the price is recalculated and the pay user's balance is modified through an Adjustment transaction. Be aware that while the job is in **Pending** state, the pay user's balance is reduced according to the initial job data.
- If no post tracking data is received within the specified **Pending** duration, the job goes into **Completed** state, and in case of pay users, all costs are refunded through a **Withdrawal** transaction. These jobs are marked accordingly in the SafeCom Tracking database.

User transactions can be checked in the scPurse database directly or in SafeCom Administrator, **User Properties/Account** tab. SafeCom Web Interface provides a UI for the end-users to review their transactions

The following screenshot displays the lifecycle of a job when Push Print Post Tracking is enabled:

20 latest From: 10-02-2016 00:00:00 To: 10-02-2016 23:59:59 Refresh

Current values
Account 1: 100,00 Account 2: 153,70 Low limit: 0,00 Reserved: 0,00 Disposable: 253,70

GID	Date/Time	Author	Type	Comment	Value	Account 1	Account 2
365	10-02-2016 16:06:51	ADMIN	Cashier	Add 100 to account	100,00	100,00	-
366	10-02-2016 16:06:56	ADMIN	Cashier	Add 200 to account	200,00	-	200,00
369	10-02-2016 16:16:45	USER 1345	Printing	Pull Print: A4 3 pages Szines PC.pdf	-15,10	-	184,90
372	10-02-2016 16:16:49	USER 1345	Push Printing	Push Print: A4 3 pages Szines PC.pdf	-15,10	-	169,80
373	10-02-2016 16:16:53	USER 1345	Push Printing	Push Print: Job k original price A4.pdf	-20,10	-	149,70
372	10-02-2016 16:17:07	USER 1345	Adjustment	Push Print: A4 3 pages Szines PC.pdf	0,00	-	149,70
373	10-02-2016 16:17:15	USER 1345	Adjustment	Push Print: Job k original price A4.pdf	4,00	-	153,70
****	4 Reservations	****	****	Reservations not shown	****	****	****

Summary (11 transactions): Show reservations Reverse reserved...

Account 1 changed with 100,00 in 1 transactions. Deposited: 100,00. Subtracted: 0,00.
Account 2 changed with 153,70 in 6 transactions. Deposited: 204,00. Subtracted: 50,30.
Reserved changed with 0,00 in 4 transactions. Deposited: -600,00. Subtracted: 600,00.

Print... Close

The value of Price 2 is also calculated precisely according to the page counters reported by the device.

In pay environments, the Push Printing, Adjustment and Withdrawal transactions are performed on the accounts of the users accordingly. Both accounts can be changed with each transaction.

If the push print post tracking requirements are not met during printing (for example, due to the older version of Print Client or SafeCom Go software), the job immediately goes into a **Completed** state, the pay user's balance is reduced accordingly, and the post tracking data is not taken into account by the SafeCom G4 Server. Activities on devices other than HP are tracked based on the information collected during printing. This data can still be inaccurate.

The Tracking service can be configured in online or offline mode in multiserver environment. The final storage of the tracking data is always the SafeCom Primary server. The records are created on the primary server database immediately in online mode. In case of Offline Tracking mode, the records are stored temporarily on the server that is bound to the SafeCom Push port until the job reaches **Completed** state. The records are then moved to the primary server depending on the scheduled tracking collection.

If the device fails to send the post tracking data (because of the device home server being unavailable), it is stored and the device resends it after the next printing. In every 4 hours, the job contexts which are older than 4 hours are cleaned up.



- The Device Server keeps the tracking information for 48 hours by default, after that time period elapses, the information is deleted. Restarting the Device Server also results in the loss of tracking information.
- Since the SafeCom Web Interface is configured to the primary server, users see their tracking data after the scheduled tracking collection.

Configure users and devices to allow modifying job setting

The Force Mono-Duplex (FMD) feature allows the user to force monochrome and/or duplex printing on the device. The feature can be enabled and disabled per user and per device. To control this user setting, open SafeCom Administrator and bring up the **User Properties** dialog.

The figure above indicates how the feature can be enabled for a user by setting the **Allow changing print settings** option. The setting can be managed for a group of users if the **Property** dialog is opened when multiple users are selected from the user list. If applied, users can see the relevant control buttons on the device (**B/W** or **Clear B/W, Duplex** or **Clear Duplex**, as appropriate).



If this setting is applied to the Default user correctly, all new users inherit this value of the setting.

The setting for the device can be controlled either in SafeCom Administrator or the Configuration Web interface of the device.

Open the **Device properties** page in SafeCom Administrator. On the **Configure** tab, you can find the options as the screenshot below indicates it. The available options are the following:

- **Enabled** - the device allows users to control their print jobs independently from the settings of the specific user.
- **Disabled** - the device hides the options from all users and the job settings cannot be changed.
- **User Setting** - the device enables or disables the features according to the currently logged on user's settings.

The same options are available on the Web Configuration page of the device as shown below:



To properly calculate job prices, ensure that the duplex and color capabilities of the device are set correctly on the **Settings** tab of the **Device Properties** in SafeCom Administrator.

In pay environment the prices of jobs are recalculated if the user requests B&W or duplex printing. The new prices are shown in the job list. The displayed prices are just estimates, as they are based on not necessarily accurate data coming from the server side calculated when the documents were printed. The correct price can be calculated knowing the accurate page counters, the number of color pages and page sizes.

Restore factory default settings

1. Open a web browser and log in to the SafeCom Device Server.
2. Click **Restore factory default settings** 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	Auto-sense
	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	
	Location	
	Description	
	Manufacturer	
Drivers		
Device Properties	User timeout	10
	Operator Name	Admin
	Operator Password	
	SafeCom Go Version	
	Configuration Time Stamp	Date and time of configuration
Device Applications	MFP authentication, E-mail	Checked (Yes)
	MFP authentication, Pull Print	Checked (Yes)
	MFP authentication, Copy	Checked (Yes)
	MFP authentication, Copy Color	Checked (Yes)
	MFP authentication, Fax	Checked (Yes)
	MFP authentication, Scan to Folder	Checked (Yes)

Uninstall SafeCom Go HP

To uninstall the SafeCom Go HP software from the device server:

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**.
5. Open the device web page and log in.
6. Click the **Security** tab and then **Access Control** in the menu to the left.
7. Select the general **Device Guest** check box to make sure that no yellow pad lock symbols appear in the list. This means that access again is granted to all applications.
8. Verify that none of the sign-in methods are set to SafeCom.
9. Click **Apply** at the bottom of the web page.

HP OPS installation

i This section is only applicable to older HP Pro devices; newer models like the PageWide Pro devices come with an embedded version of OPS, and do not require additional steps; they can be simply added through the SafeCom Device Server.

HP OPS (OXPd Professional Services) is essentially a web server with some HP-specific functionality communicating over SSL. Since the communication is encrypted, the HP OPS CA certificate needs to be imported into any device that talks to the HP OPS. This is a hard requirement; the device does not talk to an untrusted HP OPS server. An HP OPS server must be configured on the device before Pull Print can be installed.

Changing either the HP OPS CA certificate or the HP OPS server's IP address or host name necessitates a new setup.

i For more information, refer to the HP OPS documentation. Be aware that OPS is an HP product, so OPS-related enquiries should be directed to HP.

Prerequisites for OPS

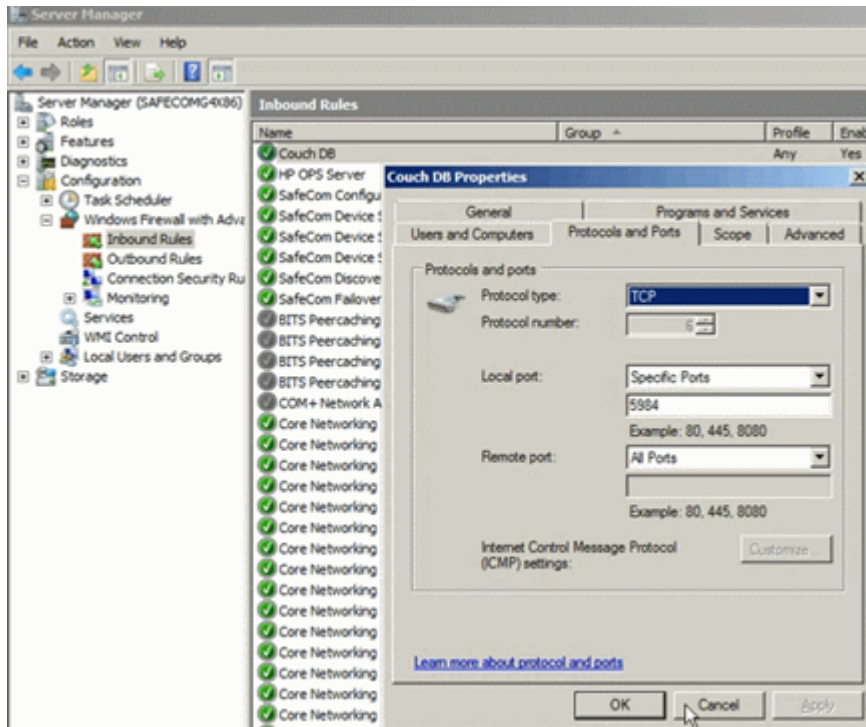
- OPS supports Windows Server 2008 R2, and Windows Server 2012 R2 64-bit versions.
- As OPS is tied to the machine name to which it is deployed, device server failover does not work with devices requiring OPS.
- SafeCom Device Server must be installed prior to launching OPS installation.
- .NET Framework 4.0 must be installed.

Installation example – through installer

i When using newer HP Pro devices with OPS 1.0.20., steps 13-17 are unnecessary, as they are performed automatically. For device fleets using both older and newer HP Pro devices, the aforementioned steps are required.

These steps must be performed once for the OPS server.

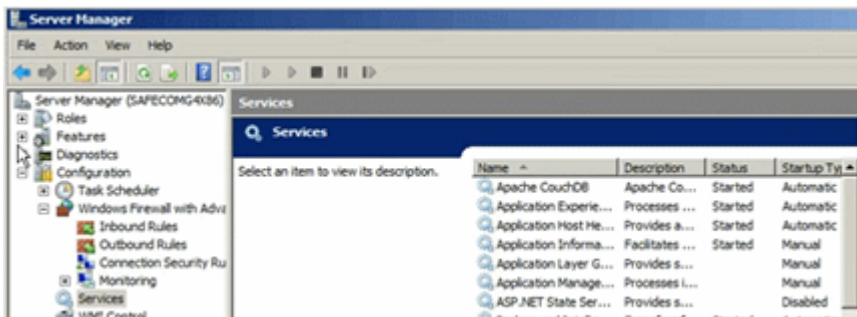
1. Ensure that SafeCom Device Server is installed on the machine you want to deploy OPS to.
2. Open your firewall for the CouchDB port 5984.



3. Browse to the OPS installer and run it as administrator.
4. Wait for the installer to finish installing the prerequisite CouchDB until the screen below is shown, at which point, pause the installation.



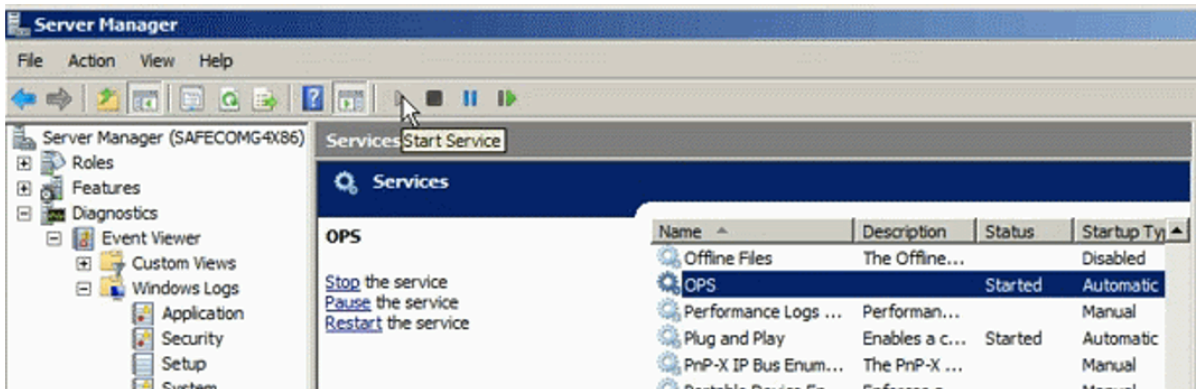
5. Check if the Apache CouchDB process is running:



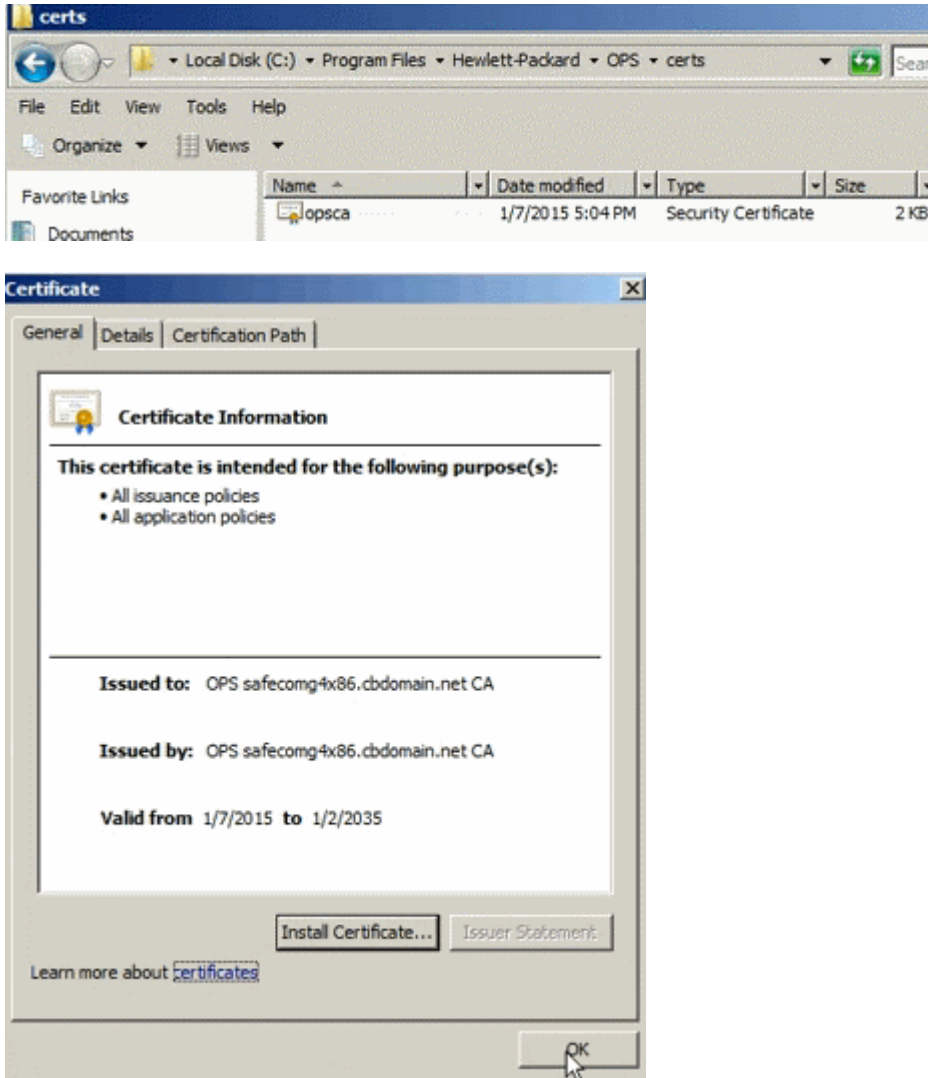
6. Use a browser to see if you can connect to CouchDB. If you can connect to it, you can proceed to the next step.
By default, CouchDB is bound to http://127.0.0.1:5984/_utils.
7. Continue with the OPS installation.



8. Enter the hostname - ensure that you enter a fully qualified domain name (FQDN).
9. Set the password.
We recommend using **admin** as the password for both CouchDB and OPS.
10. Do not launch OPS and do not open the readme file yet.
11. Start the OPS service:




12. Check if the certificate file has been created in your OPS directory (by default, C:\Program Files\Hewlett-Packard\OPS\certs) and that it contains the FQDN of the server running OPS:



13. Use a browser to connect to the MFP, and check that the OPS certificate is added to the list of available certificates:

Certificate Authority (CA) Certificate

A Certificate Authority (CA) certificate is required for some authentication methods. For example, it is used to verify the certificate of the e-mail server and to verify the 802.1x authentication server.

	Issued To	Issuer	Expires On
	CN=OPS safecomg4x86.cbdomain.net CA	CN=OPS safecomg4x86.cbdomain.net CA	2035-01-02

14. Run OPSSetup.bat as administrator:

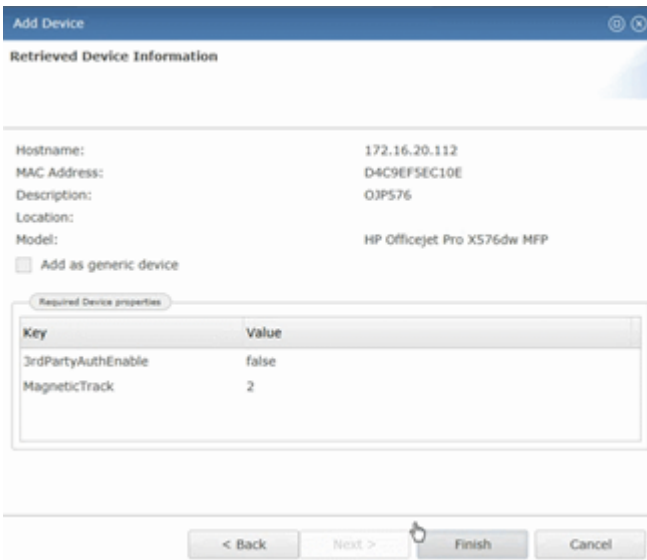
```
C:\Program Files\Hewlett-Packard\OPS\bin>OPSSetup.bat
Please select an option from below:
1. Create an instance of OPS Server
2. Create an instance of OPS Server using config file
3. Register a device to the OPS server
4. Unregister a device to the OPS server
5. Retrieve the device current OPS server details
6. Exit Setup
```

15. Select option 3 and provide the following information:

- Device IP, device username, and device password
- OPS server URL, OPS server username, and OPS server password

When prompted for the URL, ensure that you use HTTPS when adding the full path: https://{FQDN of the OPS Server:8081}

16. Add the device to the Device Server:



Add Device

Retrieved Device Information

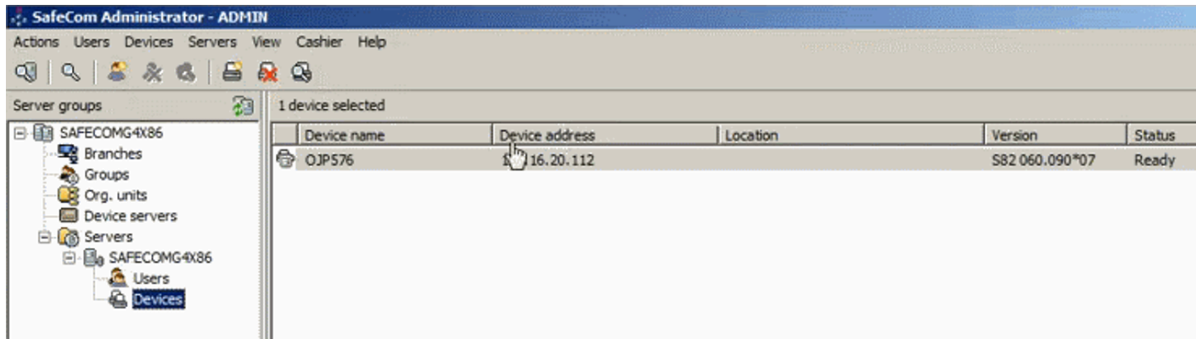
Hostname: 172.16.20.112
 MAC Address: D4C9EF5EC10E
 Description: O3P576
 Location:
 Model: HP Officejet Pro X576dw MFP

Add as generic device

Key	Value
3rdPartyAuthEnable	false
MagneticTrack	2

< Back Next > Finish Cancel

17. Check your device in SafeCom Administrator:



Installation example – through command line

i We recommend using the command line interface if you want to repair or modify your OPS installation.

1. Launch the HP OPS installer.
2. Set the fully qualified domain name (FQDN) of the OPS server and ensure it is in the domain.
3. Launch the OPS server.
4. Add inbound rule for port 8081 to your firewall.
5. Check your network settings, and correct the domain name if necessary.
6. Clean device settings, if necessary.
7. Setup CouchDB.
8. Use the CouchDB Test Suite to create an Admin Party, and click Remove Admins.
9. Recreate the CouchDB administrator.
10. Reconfigure OPS by running OPSSetup.bat. Follow the on-screen instructions.

If you run into an "HTTP 400" error during OPS installation, see [Troubleshooting HTTP 400 error during OPS installation](#).

To update the setup of CouchDB and OPS, see [Update the setup of CouchDB and OPS](#).

To reinstall CouchDB, see [Reinstall CouchDB](#).

Troubleshooting HTTP 400 error during OPS installation

As administrator:

1. Ensure that the OPS server is inside your domain.
2. Uninstall the following: OPS, CouchDB, OpenSSL 0.9.8.
If your OpenSSL version is different, you need this specific version.
3. Restart the server.
4. Retry the installation.
If it does not succeed, proceed to the next step.
5. If the device registration fails, delete the OXPDPPro service of the device.

6. On the device, enable IPv4 only.
7. On the device, configure WINS manually.
8. On the device, configure DNS manually.
9. On the device, enable DHCPv4 FQDN and disable DHCPv6.
10. Install the certificate to the server.
11. Install the certificate to the device.
12. Start a browser on the server and open the device web page.
13. Ensure that the administrator page is set to US English.
14. Set server region to US English.
15. Set server default language and keyboard to US English.
16. Open a new command prompt.

Update the setup of CouchDB and OPS


1. Open the CouchDB Futon page (<http://{IP:port}/utils>)
2. Log in as administrator.
3. Use the Test Page to create an Admin Party.
4. Fix the Admin Party by clicking the **Fix** option on the bottom-right part.
5. Add the administrator user with the standard SafeCom credentials.
6. Rerun OPSSetup.bat and select **Create an instance of OPS server**.
7. Add a device to OPS.
8. Use OPSSetup.bat to check whether the device is registered properly by selecting **Retrieve the device current OPS server details**.


Reinstall CouchDB

1. Install and restart the OPS server.
2. Follow the steps outlined in the Re-setup CouchDB and OPS section above.

Partial Disk Clean on M525 and M575 devices

To remove the SafeCom Go solution from the device, first perform a partial disk clean.

1. Delete the device from the **SafeCom Device Server** where the device is added.
The device must be in the idle state  in order for the deletion to be performed correctly.

 If the device is configured to another server, click **Reconfigure Device** to force a reconfiguration of the device to your server.

2. Turn off the device.
3. Turn the device back on again.
4. Tap the HP icon when it appears.
5. When the next HP icon appears, tap it as soon as the device starts counting (for example 1/8) to enter the **Administrator** menu.

For further support, refer to the device manual or contact HP support.

SafeCom Go HP device trace facility

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

Used for troubleshooting, the SafeCom trace facility is enabled through the **Configuration** web page. See [Enable the SafeCom trace facility through the Configuration web page](#).

Alternatively, enable the trace facility through the **SafeCom Device Server**. See [Enable the trace facility through the SafeCom Device Server](#).

In order to see the trace files generated by the Device Server, see [See the trace files generated by the Device Server](#).

You can configure the size of the trace files as well as how many are generated by following the steps in [Configure the size and number of the trace files](#).

Enable the SafeCom trace facility through the Configuration web page

1. Open the device web page and log in.
2. Click the **General** tab, and then click **SafeCom** in the menu to the left.
3. If the log is disabled, click the **Enable** button to the right.
4. To save the log, click **Show complete log** select the log information and copy it into a *.txt file and save it.

Enable the trace facility through the SafeCom Device Server

1. Open the SafeCom Device Server and log in.
2. Select a device in the device server pane and make sure that the check box **Logging enabled** at the bottom of the page is selected.
3. Click **Save**.

See the trace files generated by the Device Server

1. Go to the destination folder for the log files:
The default installation folder is `C:\Program Files\ SafeCom\SafeCom Device Server \logs`.
On Windows 64-bit, it is `C:\Program Files (x86)\ SafeCom\SafeCom Device Server \logs`.
2. If you need to send the log files, make sure to save and send the folder logs as a compressed/ zipped folder.

Configure the size and number of the trace files

1. Browse to the config.ini file at `C:\Program Files\ SafeCom\SafeCom Device Server \equinox\config.ini`.

On Windows 64-bit, it is at `C:\Program Files (x86)\ SafeCom\SafeCom Device Server\equinox\config.ini`.

2. 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 10 KB, ten megabytes is 10 MB, and one gigabyte is 1 GB.
 - `deviceserver.trace.file.count` - to configure how many trace files are generated. Enter the number of files you want to generate as a number.
3. After configuring the trace files, restart the SafeCom service.

Chapter 3

SafeCom Go HP installation

Make sure the SafeCom G4 Server software installation has been completed as described in SafeCom documentation, for example the *Kofax SafeCom G4 Server Administrator's Guide*.

- [SafeCom Go HP hardware installation](#)
- [SafeCom Go HP software installation](#)

SafeCom Go HP hardware installation

This section is only relevant if users will log in by card. Otherwise, proceed to installation of the SafeCom Go HP software.

i 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.

If user will log in by card, then install as described below:

- **A USB ID device was supplied:** Connect the SafeCom ID device directly to the external USB. The USB port may be covered by sticker that has to be removed first. On some devices the USB port is next to the network port. Proceed to [SafeCom Go HP software installation](#).
- **A USB ID Kit and USB ID device was supplied:** The installation of the SafeCom HP USB Key, and the SafeCom ID device is covered in [SafeCom HP hardware installation](#).
- **Hardware integration pocket with supplied embedded ID device:** The installation of embedded ID device in hardware integration pocket is covered in [Embedded ID device in Hardware Integration Pocket](#).

SafeCom HP hardware installation

The SafeCom HP USB installation can be simplified depending on the capabilities of the device and if a SafeCom ID device (card reader) is required to log in users.

- If the MFP or printer is equipped with a HDD or SSD, you can skip installing the SafeCom HP USB key as the SafeCom Go HP software can be loaded onto and run from the device's hard disk.
- The device has an external USB port labeled ACC.
- The device has a HIP pocket and an embedded card reader is used.

After the [SafeCom HP USB Key](#) and the [external USB ID device](#) are installed, proceed to [SafeCom Go HP software installation](#) for the steps required to install the SafeCom Go HP software.

Install the SafeCom HP USB Key

1. Turn the device off and disconnect all power and interface cables.
2. Get access to the device's formatter board as described in the device manual.
3. Insert the SafeCom USB key into an available USB port.
4. If an ID device (card reader) is to be used, proceed to the relevant section below. Otherwise, connect all cables, plug in your device, and turn the power on.

Install an external USB ID device

Connect the SafeCom USB ID device directly to the external USB port labeled ACC.

i A label covering the USB port may have to be removed first. On M602 the USB port is hidden behind an USB icon at the rear of the printer that must be cut clear in order to install the USB ID device.

Embedded ID device in Hardware Integration Pocket

Items supplied:

- One ID device without casing.
- One 12 cm mini-USB cable for mounting on the ID device.
- Four holders with self adhesive tape.
- One "Present card here" label (p/n 621010).

The installation goes as follows:

1. Turn the device off and disconnect all power cables.
2. Remove the cover from the hardware integration pocket as described in the device's manual. Opening the cover can be done by inserting a metal blade at the center of the top edge of the cover. Take care not to scratch the cover or hurt yourself.
3. Hold the ID device with the cable connector facing upwards and the antenna facing downwards. On the cable connector side place a holder in each of the four corner holes.
4. Do one of the following:
 - **MFP M525, MFP M575, MFP M775, CM3530 MFP, CM4540 MFP, M4555 MFP, M551, M712, and ScanJet Enterprise 8500fn1:** Connect the 12 cm mini-USB cable to the ID device and to the mini-USB connector in the lower right corner of the pocket.

i For M551 the Hardware Integration Pocket is not available for the M551n.

- **P3015:** Disconnect the 12 cm mini-USB cable from the ID device. Connect the supplied 33 cm cable (p/n 344020) to the ID device and to the USB connector on the device's motherboard. Pass the cable through the square hole in the hardware integration pocket.
- **M651, M806, M855, X555, M602, M603, and Scanjet 7000n:** Connect the card reader using the E12 USB Cable, Female, 12 cm cable (p/n 344030).

i For the M601 there is no Hardware Integration Pocket. For X555 and M651 devices, ensure that you have the device-side preinstalled cable ending in the HIP which must be connected to the E12f.

5. Remove the tape from the four holders mounted on the ID device.
6. Center and mount the ID device in the bottom of the pocket.
The cable connector on the ID device should face left and downwards.



SafeCom ID device mounted in the hardware integration pocket

The shown ID device is SafeCom Mifare Reader. Other SafeCom ID devices may have the antenna layered in the print circuit board.

7. Plug in the power cord and connect all cables. Turn the device on.
8. Verify that the LED on the ID device is on.
9. Put the cover back on the hardware integration pocket (it can only fit one way).
10. Remove the plastic from the "Present card here" and mount it centered on the cover of the hardware integration pocket.
11. Proceed to [SafeCom Go HP software installation](#) for the steps required to install the SafeCom Go HP software.

SafeCom Go HP software installation


- [On FutureSmart devices](#)
- [On legacy Chai devices](#)

Send SafeCom Go HP FS (*.b95) file to FutureSmart devices

On SafeCom Administrator version 10.52.4.4 and later, you have the option to install the SafeCom Go to FutureSmart devices directly.


1. Make sure the device is powered on and ready, and enable **TLS 1.2** through **Networking > Mgmt Protocols > Web Mgmt > Secure Communications > SSL/TLS Protocol** of the device web page.
2. Start SafeCom Administrator and log in to the server.
3. Invoke the **Add device** function from the **Devices** menu, the **Toolbar** button, or the **System overview**.
4. Enter the **Device address** (hostname or IP address) and the SNMP community name (by default, it is set to **public**). Click **Next**.
5. Information is retrieved from the device to establish the type of device. Click **Next**.
6. On the **Settings** tab, specify the properties of the device (**Duplex supported** and **Color supported**).
7. Click **Add** to register the device and save it in the database.
8. Open the device in a web browser by entering the IP address in the address field.
9. Sign in using the device login and password.
10. Click the **General** tab and then click **SafeCom** to open the **Configuration** web page.
11. Under **Device**, make sure to specify the **Administrator password** for the device.
The password must be the same as the one used to sign in to the printer. The **Pull Print** icon will not appear unless a correct password is specified.
12. Click **Apply**.
13. In SafeCom Administrator, invoke the **Configure** tab through **Device Properties**.
14. Enter the **Group name** the device will belong to.
15. Provide the server address into the **Add Server** field, and click **Add**.
16. Set **Login method** and **Password** as appropriate.
17. Set **Print all** behavior and **MFP auth** functions by selecting the relevant check boxes.
18. Select the **Send configuration to device after pressing the OK button** check box.
19. Click **OK**.

Send SafeCom Go HP (*.b49) and (*.b89) files to legacy Chai devices

 On HP LaserJet CM8050 MFP and CM8060 MFP, you must first disable encryption.


1. Make sure the device is powered on and ready.
2. Start **SafeCom Administrator** and log in to the server.
3. Invoke the **Add device** function from the **Devices** menu, the **Toolbar** button, or the **System overview**.
4. Enter the **Device address** (hostname or IP address). Click **Next**.
5. Information is retrieved from the device to establish the type of device. Click **Next**.

6. On the **Settings** tab, specify the properties of the device (**Duplex supported** and **Color supported**).
7. Click **Add** to register the device and save it in the database.
8. Click **Send** to send the SafeCom Go HP Loader file (*.b49) to the device. If file is not present you need to get the file first.
The **Device authorization** dialog appears. If no device password (see [Set password to prevent unauthorized access](#)) is set, the dialog will allow you to enter the device **Password**.
9. Enter the admin **Username** and the device **Password**.
10. Click **Close** when the download is completed.
11. Click **Send** to send the SafeCom Go HP software file (*.b89) to the device.
12. Click **Close** when the download is completed. The device restarts and after a few minutes the device's control panel will say **Ready**. After another 2-7 minutes (depending on model) the control panel will say **Loading SafeCom** for 1-2 minutes.

 The HP LaserJet CM8050 MFP and CM8060 MFP require additional setup in regards to sign-in method (see [Set sign-in method and access control](#)) and Send to E-mail (see [Send to E-mail on CM8050 MFP and CM8060 MFP](#)).

SafeCom Go HP is now installed and configured in the device. You can proceed and use the SafeCom-enabled device to collect your documents.

Install to FutureSmart devices through Solution Installer

 If the FutureSmart device ran with SafeCom Device Server make sure the SafeCom Device Server no longer references the device and conduct a partial disk clean on the FutureSmart device (see [HP OPS installation](#)) before proceeding.

To install SafeCom software on FutureSmart devices, see [Install SafeCom software on FutureSmart devices](#).

SafeCom Go HP for FutureSmart devices is installed through the HP Solution Installer from the device web page. See [Install SafeCom Go HP for FutureSmart devices through HP Solution Installer from the device web page](#).

Connect to quota server: See [Connect to quota server](#).

After all steps in the mentioned sections are completed, SafeCom Go HP is installed and configured in the device. You can proceed and use the SafeCom-enabled device to collect your documents.

Install SafeCom software on FutureSmart devices

1. Install software through Solution Installer (steps 1-7 in [Install SafeCom Go HP for FutureSmart devices through HP Solution Installer from the device web page](#)).
2. Add device in SafeCom Administrator (steps 8-14 in [Install SafeCom Go HP for FutureSmart devices through HP Solution Installer from the device web page](#)).

3. On MFPs configure Administrator Password and HP Quota Service (steps 15-24 in [Install SafeCom Go HP for FutureSmart devices through HP Solution Installer from the device web page](#)).

Install SafeCom Go HP for FutureSmart devices through HP Solution Installer from the device web page

1. Get and download the SafeCom Go HP *.b95 file.
 2. Make sure the device is powered on and ready, and enable **TLS 1.2** through **Networking > Mgmt Protocols > Web Mgmt > Secure Communications > SSL/TLS Protocol** of the device web page.
 3. Open the device in a web browser by entering the IP address in the address field.
 4. Sign in using the device login and password. If the password is not set, set it.
 5. Click the **General** tab and then **Solution Installer**.
 6. Under **Install New Solution**, click **Browse** to browse to the location of the SafeCom Go HP *.b95 file.
 7. Click **Install**.
The message "Receiving upgrade" appears on the device. When installation is completed successfully, the message on the device says "Ready".
 8. Make sure the device is powered on and ready, and enable **TLS 1.2** through **Networking > Mgmt Protocols > Web Mgmt > Secure Communications > SSL/TLS Protocol** of the device web page.
 9. Start **SafeCom Administrator** and log in to the server.
 10. Invoke the **Add device** function from the **Devices** menu, the **Toolbar** button, or the **System overview**.
 11. Enter the **Device address** (hostname or IP address). Click **Next**.
 12. Information is retrieved from the device to establish the type of device. 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.
- The remaining steps are only required for MFPs and not for printers.
15. Open the device in a web browser by entering the IP address in the address field.
 16. Sign in using the device login and password.
 17. Click the **General** tab and then click **SafeCom** to open the **Configuration** web page.
 18. Under **Device**, make sure to specify the **Administrator password** for the device. The password must be the same as the one used to sign in to the printer. The **Pull Print** icon will not appear unless correct password is specified.
 19. Click **Apply**.

Connect to quota server

i With SafeCom Go HP version S89 nnn.050*13 and S95 nnn.050*13, the quota server is set up automatically.

1. Click the **General** tab, and then **Quota and Statistics Services** in the left hand menu.
2. In the **Quota Server URL** field, enter this URL:
`http://127.0.0.1:5744/hp/device/dk.safecom.hp.webservice.JSWebEntryPoint?quota`
3. Check the **Connect this device to a Quota server**.
4. Click **Apply** at the bottom of the web page.

Control Device Sign in CM8050 MFP and CM8060 MFP

To sign in to the Control Device with SafeCom, see [SafeCom as sign-in method](#).

To gain custom access to the Control Device, see [Custom Access Control](#).

SafeCom as sign-in method

1. Open the device's web page.
2. Click the **Settings** tab.
3. Click **Device Sign In** on the menu.
4. Click the **Sign In Methods** tab.
5. Scroll to **Other Available Sign In Methods** at the bottom of the web page and check **SafeCom**.
6. Click **Apply**.
7. Select **SafeCom as Default Sign In Method at the device**.
8. Click **Apply**.

Custom Access Control

1. Open the device's web page.
2. Click the **Settings** tab.
3. Click **Device Sign In** on the menu.
4. Click the **Device Access** tab.
5. Scroll to **Access Control Level for Device Functions**.
6. Check **Custom Access Control** and click **Define Custom**.
7. Check the applications you wish SafeCom to control and remember to also check these under **MFP authentication** on the SafeCom **Configuration** web page. See the table below.

Device Sign In > Device Access > Custom Access Control	SafeCom > Configuration MFP authentication
Administration application	
Copy application	Copy
Job Status	

Device Sign In > Device Access > Custom Access Control	SafeCom > Configuration MFP authentication
Job Storage application	
E-mail application	E-mail
Fax application	Fax
Network Folder application	Folder
Supply Status application	
Document Capture application	
SafeCom Pull Print	Pull Print

8. If the default sign-in method at the device is not SafeCom, change the default sign-in method from **Default** to **SafeCom** for each application that is to be controlled by SafeCom.

Send to E-mail on CM8050 MFP and CM8060 MFP

1. Open the **Configuration** web page.
2. Check **E-mail** in **MFP authentication**.
3. Click **Apply**.
4. Click the **Settings** tab.
5. Click **Device Sign In** on the menu.
6. Click the **Device Access** tab.
7. Scroll to **Access Control Level for Device Functions**.
8. Check **Custom Access Control** and click **Define Custom**.
9. Check **E-mail application**.
10. Click the **Digital Sending** tab.
11. Click **E-mail Setup** on the menu.
12. Select one of the **Address Field Control** options.
13. Click **Apply**.

Deploy SafeCom Go HP on multiple devices

This section covers how to deploy SafeCom Go on multiple HP devices.

With **SafeCom Device Utility**, it is possible to load SafeCom device software onto devices as part of preparing devices for a staged roll-out. It does not require SafeCom server software and databases to be running and it will not do any registration of devices.

Create a device configuration file

The device configuration file is created with custom settings using the **SafeCom tool GoBuild**.

To open and configure a device configuration file, see [Open and configure a device configuration file](#).

To generate a compiled configuration file, see [Generate a compiled configuration file](#).

i Refer to *Tech note SafeCom GoBuild D20127* for more information on SafeCom Device Utility.

Open and configure a device configuration file

1. Download and unzip the SafeCom GoBuild package to your local C: drive.

i SafeCom GoBuild can be downloaded from the SafeCom website.

2. Execute the gobuild.exe and click **File** and **Open**.
3. Select the file configuration_mfp.xml and click **Open**.
4. Locate and change the appropriate lines to configure the settings as required.

i Do not change port 7500.

5. Save the configuration file.

Generate a compiled configuration file

1. Open the file gobuild.xml.
2. Edit the placement in the tags <OUTPUT> and <FILEPATH> so it corresponds to the location on your C: drive.

i Do not change the tag <LOCALPATH>!

3. Change <ACTION TYPE="6"> to "3" - this means the device does not restart after receiving the configuration.
4. Select **File** and **Run** to generate a compiled configuration file: configuration_mfp.b89.

Send configuration file to devices

Send the configuration file and the SafeCom Go software to the device using the SafeCom tool SafeCom Device Utility (scDevUtil.exe).

Pre-requisites:

- Do a DISK INIT on the HP device to ensure it has no SafeCom software installed.
- Copy the SafeCom Go HP device software to C:\ProgramFiles\SafeCom\SafeComG4\device_software.
- Copy the configuration_mfp.b89 file created in the previous section to the same directory C:\ProgramFiles\SafeCom\SafeComG4\device_software.

Load files to devices and verify configuration:

1. Start SafeCom Device Utility by executing the file scDevUtil.exe in the C:\Program Files\SafeCom\SafeComG4 directory.
2. Add the HP devices that must be loaded with the files to the list of devices.


There are three ways to get the devices into the list of devices:

- **Load from file:** Create a plain text file with one address (IP address or hostname) per line and save it with the extension dip (Device IP file). In the **File** menu, click **Load device list from file...**
- **Add device individually:** Enter the **Device address** and click **Add**.
- **Broadcast for devices:** Click **Broadcast** to broadcast for devices.


Use the SafeCom Device Utility to load the following 3 files to the devices:

- The appropriate nnn*.b49 file (the SafeCom loader)
- The configuration_mfp.b89 file
- The appropriate nnn*.b89 file (the SafeCom Go code)

3. Select one or more devices in SafeCom Device Utility.
4. Right-click the devices and click **Send Go Loader** to send the *.b49 file to the selected devices.
5. Browse for the *.b49 file and click **Send**.
6. Select the devices again, right-click and click **Update software**.
7. Browse for the *.b89 file and click **Send**.

 The device should not restart until after the last file has been loaded according to the configuration made in [Create a device configuration file](#).

8. When it has restarted completely, check that it has been configured correctly according to your settings from [Create a device configuration file](#).
9. Register the device at your SafeCom server in one of the following three ways:
 - Use the **Add device** function in **SafeCom Administrator**.
 - Log in at the printer by a user with Technician or Administrator rights.
 - Log in to the **Register** web page and click **Register**.

 Once the device is registered it appears in the **SafeCom Administrator**.

- The Color Laser Jet 4700 only allows the go loader to be sent as a .jar file through the web page. See [How to open the SafeCom Loader web page](#).
- Refer to the *SafeCom G4 Administrator's Manual* for more information on SafeCom Device Utility.

Make changes to the configuration file

To edit the configuration file:

1. Start GoBuild.exe again.
2. Load the file configuration_mfp.xml.
3. Make the necessary changes.
4. Load gobuild.xml, change <ACTION TYPE> back to "6", and compile (Run).
5. Use SafeCom Device Utility to send it to the device.

Login

1. Open a web browser and enter the IP address of the device in the address field.
JavaScript (Active Scripting) must be enabled.
2. The EWS opens on the **Information** tab. Click **SafeCom** on the menu to open the **Information** web page with version and status information.
3. Click on the **Settings** tab to configure SafeCom Go.

i If you do not see the **Settings** tab, it is because the HP Embedded Web Server (EWS) is password-protected. Click the **Log In** link in the upper-right corner of the page. Type "admin" for the username, type the device password and then click **OK**.

4. Click **SafeCom** on the menu to access the SafeCom specific screens with the tabs:
 - **Configuration** - specify SafeCom server, login method, driver names and MFP authentication.
 - **Register** - register the device with SafeCom server.
 - **Log** - enable logging for troubleshooting purpose.

SafeCom Go HP web interface

The SafeCom Go HP web interface adheres to the structure and design of the HP Embedded Web Server (EWS). The SafeCom Go HP web interface consists of two parts, 1) a public part accessible through the **Information** tab and 2) a password-protected part accessible through the **Settings** tab.

i For FutureSmart devices, ensure that **TLS 1.2** is enabled through **Networking > Mgmt Protocols > Web Mgmt > Secure Communications > SSL/TLS Protocol** of the device web page. For devices using 4.x firmware, you can find the option under **Networking > Secure Communications > SSL/TLS Protocol**.

Information web page

The **Information** web page shows version, configuration summary and up time.

The screenshot shows the HP Color LaserJet CM3530 MFP Series web interface. At the top, there is a green header with the HP logo and the text 'HP Color LaserJet CM3530 MFP Series'. To the right of the header, there is a user status bar showing 'User: admin' and a 'Log Off' button. Below the header, the IP address 'NP122121E / 172.16.6.109' is displayed. The main navigation menu includes 'Information', 'Settings', 'Digital Sending', and 'Networking'. The 'Information' page is active, showing a sidebar with various links like 'Device Status', 'Configuration Page', 'Supplies Status', 'Event Log', 'Usage Page', 'Diagnostics Page', 'Device Information', 'Control Panel', 'Color Usage Job Log', 'Print', 'SafeCom', and 'Other Links'. The main content area is titled 'Information' and features the SafeCom logo. It contains three sections: 'Product Information' with details like Product name (SafeCom Go), Version (S89 140.030*39), Version date (2009.06.24), Version time (13:54:00), and Loader version (S49 140.020*16); 'System Information' with details like Group name (WSLEJ2), Server IP (172.16.6.190), Up time (0 days 3:29:08), Is the log enabled (No), and ID device (OEM - RFID Device); and 'User Information' showing the current user as 'No user'. A 'Mail to SafeCom Support' button is located at the bottom of the page.

i When the **Information** web page is opened the above information and additional debug information is copied to the clipboard. The information can be pasted into an editor such as Notepad or into the body of your e-mail message by pressing Ctrl + V.

Configuration web page

The **Configuration** web page is used to configure SafeCom Go HP as to which server it should connect to, how users should be identified, and so on.



The **SafeCom Server** section is used to specify the SafeCom server. You can either click **Broadcast** to get a list of servers to select from or directly enter **Group name**, **TCP port** (default is 7500), and the SafeCom server IP address in **Add server**. See also in [Specify SafeCom Server](#).


Use the **Move up** and **Move down** button to prioritize the order in which the servers are contacted in case the first one on the list becomes unavailable.

i After you click **Apply**, you should wait one minute before the changed SafeCom Server settings take effect. Otherwise, you may get a login error at the printer.

The **Encryption** section can be used to configure max length of encryption keys, and whether you are using **Legacy** or **TLS** encryption.


Select the max. size according to the descriptions below:

- **Asymmetric max. size:** Select between **Default**, **512**, **1024**, or **2048**. If **Default** is chosen, then the device complies with the length of the encryption keys that is specified on the **Encryption** tab in the **Server properties** dialog in **SafeCom Administrator**.
- **Symmetric max. size:** Select between **Default**, **128**, or **256**. If **Default** is chosen, then the device complies with the length of the encryption keys that is specified on the **Encryption** tab in the **Server properties** dialog in **SafeCom Administrator**.
- **TLS encryption:** Select from the available suites. Be aware that the default option (**TLS_DHE_RSA_WITH_AES_256_GCM_SHA384**) is the strongest encryption level. The operating system running your SafeCom G4 Server and Print Client must support the selected encryption suite.


 On FutureSmart devices, enabling TLS encryption may result in the device displaying an "Out of order" message for 2 minutes for the duration of the encryption key generation due to device limitations.

The **Networking** section is where you modify your network settings.

- **Administrator password:** This is available on FutureSmart devices only. Enter the password for the device. The password must be the same as the one used to sign in to the devices web pages. The Pull Print icon will not appear unless correct password is specified.

 By default, the firmware of FutureSmart devices has the Password Complexity option enabled. This requires users to have passwords between 8 and 16 characters, and use at least three options from uppercase letters, lowercase letters, numbers, and special characters. Be aware that feedback about wrong password may be absent.


- **SNMP v1/v2:** Set if your device is using either SNMP v1 or SNMP v2. The **Community name SET** must match the **Community Name GET** if this is different from public. By default, **Community name** is public.
- **SNMP v3:** Set if you are using the device with SNMP v3. For more information, see below.
 - **Username:** Set your username.
 - **Authentication protocol:** Set the authentication protocol to be used, and add the relevant **passphrase**.
 - **Privacy protocol:** Set the privacy protocol to be used, and add the relevant **passphrase**.

 Ensure that the **Authentication protocol** and **Privacy protocol** are the same on the device and in SafeCom.


The **Device section** is where the specifications of the device are managed. Configure the device according to the descriptions below.

- **Device name:** Automatically filled in with the name of the device.
- **Device model:** Automatically filled in with the model of the device.
- **Device location:** Enter the location of the device to provide useful information in maintaining the SafeCom solution.


- **Contact person:** Enter the name of the contact person to provide useful information in maintaining the SafeCom solution. The name, model, and location are also viewable in the **Device properties** dialog in **SafeCom Administrator**.
- **Login method:** Specifies how users must identify themselves to log in to the device. Select between:
 - **ID code**

 On devices with 110xxx and 132xxx SafeCom Go, the ID code must be max 32 characters long.

- **Card**
- **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.
- **Keypad** - only relevant if an external keypad is connected (for Chai-based, single-function printers, and similar older devices, an external keypad is required to mask ID code).
- **Auto-sense** (default). Auto-sense maps to **Card or Windows** if an ID device is connected to the MFP and on printers it maps to **Card**. Otherwise, it maps to **ID code**. Mapping changes within 10 seconds after the ID device is either connected or disconnection. If it does not change a restart of the device may be required.

 For card registration to work when using Windows credentials, you must have at least one valid PUK code available in the G4 system.

- **Default domain:** Specify a default domain for all users at login.
- **Pre-fill domain:** Specify how to show the domain field on the device. Select between:
 - **Blank** (default): Select this if users belong to different domains. This means that all users need to enter their domain when they log in with their Windows username and password.
 - **Default domain:** Select this if a majority of users belong to a particular domain as the specified **Default domain** will be pre-filled making it easier for these users to log in with their Windows username, password and domain.
 - **Hide:** Select this if all users belong to the same domain, as it saves users from being prompted for the domain when they log in with their Windows username and password. Be sure to have specified the **Default domain**, otherwise the choice will revert back to **Blank** when you click **Apply**.

 The SafeCom G4 Server must be a member of the domain or trusted by the domain.


- **Mask ID code:** Check to increase security by using the asterisk (*) character to mask the entered ID code. Supported by HP multifunction devices, and newer single-function printers (for example, HP FutureSmart devices).

For older, Chai-based single-function printers (for example, P4015 or P3015), an external USB keypad is required to mask ID code. Note that only numeric ID codes can be entered with an external keypad.

- **Login without PIN code:** Check if users do NOT need to enter a 4-digit PIN code at login. This setting applies to the device and overrules the equivalent user property on the SafeCom G4 Server. Use of PIN code is possible on devices with touch-screen or keypad.
- **Enable third party authentication:** Check to make the SafeCom solution check for user credentials that is provided using a non-SafeCom login method. The alternate login method is assumed to be Windows authentication. In the event that additional configuration should be necessary this can be accomplished with the XML-based configuration file and the XML tags: <ID_CODE>, <USER_LOGON>, and <DOMAIN>. The XML tags must be enclosed by the XML tag: <THIRD_PARTY_AUTH>. Extract from XML file:


```
<THIRD_PARTY_AUTH>
<ID_CODE />
<USER_LOGON>UserName</USER_LOGON>
<DOMAIN>Domain</DOMAIN>
</THIRD_PARTY_AUTH>
```

The entire XML-based configuration can be uploaded and edited using the **SafeCom Device Utility** as described in the *SafeCom G4 Administrator's Manual*.

 If the SafeCom solution checks and finds both an ID code and a user logon, then the ID code is prioritized and used. As a minimum, either the ID code or the User logon must be entered.

- **High speed print:** Check this to allow faster printing. With high speed print the print speed becomes comparable to printing a document directly to the printer.
The downside is that documents that are submitted through a Standard TCP/IP port may be printed between the logged in user's print and copy jobs. In other words, the logged in user cannot assume that the documents in the output bin belongs to him. If the directly printed document instead is submitted through a SafeCom Push Port that is referencing the same tracking device, then these documents can be held off.
- **Print all at login:** Check if all the user's documents should be printed as soon as the user logs in. This setting applies to the device. If checked this overrules the equivalent user property on the SafeCom G4 Server.
- **Show newest first:** Check to have documents listed and printed in last-in first-out order. **Print all at login** and **Show newest first** are not present if **Pull Print** is cleared in **MFP authentication**.
- **Prevent printing at low toner level:** Checking this option disables the **Print** and **Print All** functions when the toner level is low.
- **Allow changing print settings:** Select if you want to allow users to modify job settings.
- **Authentication and tracking:** This is available on MFPs only. SafeCom Go HP can handle authentication for other applications, such as **AutoStore**. You can select if users are required to log in to SafeCom before they can:
 - **Pull Print** - collect documents at any device.
 - **Copy** - make hardcopies of scanned documents.
 - **Save to device memory** - allows saving job data to the device memory. The option is not accessible from SafeCom Administrator, only through the device configuration page.
 - **Retrieve from device memory** - allows retrieving saved job data from the device memory. The option is not accessible from SafeCom Administrator, only through the device configuration page.
 - **Color copy** - make color hardcopies of scanned documents.
 - **Folder** - send scanned documents to a network folder.

- **Fax** - send scanned documents through fax.
- **E-mail** - send scanned documents as attachments to e-mail⁷.
- **Smart Scan** - allow scanning documents through SafeCom Smart Scan. Smart scan is only supported on HP FutureSmart devices with an embedded SafeCom Go solution installed.
- **Account** - allow selection of billing code.

 On HP LaserJet CM8050 MFP and CM8060 MFP, you are required to setup **SafeCom** as sign-in method (see [Set sign-in method and access control](#)).

- **Trusted drivers:** When Pull Printing, the SafeCom solution 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.

To add drivers, see [Add drivers](#).

- **Add driver:** Add a driver manually to the list of drivers, by entering the driver name in the **Add driver** field and then click **Add**.
- **Timeout:** Specify the number of seconds before a user is logged out. Default is 60 seconds. The timer is halted if the device requires intervention (IRQ) so the user is not logged out while a paper out condition is being cleared. On a MFP the user is NOT automatically logged out if **Timeout** is greater than the MFP's **Inactivity timeout** specified under **Copy/Send settings**. Default is 60 seconds.
- **Post track:** Relevant only with SafeCom Tracking. Refer to the *SafeCom G4 Administrator's Manual*.
- **Restore factory default:** Click **Restore factory default** at the bottom of the web page to set all settings, except the device password, to their default value.

The **E-mail** section is present for non-FutureSmart MFPs and is relevant only if SafeCom handles user authentication for E-mail (if **E-mail** is checked in **MFP authentication**). SafeCom provides seamless authentication for **Send to E-mail**.

Fill in the fields for managing e-mail according to the descriptions below:

- **Default From: address:** Enter the default **From: address** for e-mails sent from the device.
- **Pre-fill From: field:** Select to pre-fill the **From:** field with either **User e-mail**, **Device name**, **Blank** or **Default From: address**.
- **Editable:** Check to make the **From:** addresses available for change to the user at the device.
- **Default To: address:** Enter the default **To: address** for e-mails sent from the device.
- **Pre-fill To: field:** Select to pre-fill the **To:** field with either **User e-mail**, **Blank** or **Default To: address**.
- **Editable:** Check to make the **To:** addresses available for change to the user at the device.
- **Force BCC to user:** Check to have the **BCC:** field pre-filled with the user's e-mail address. This cannot be changed by the user at the device.

⁷ The SafeCom Go Configuration web page for FutureSmart devices does not include the E-mail section. To configure e-mail on FutureSmart devices, use the device's own web page.

Add drivers

1. Click **Get all** to retrieve a list of driver names from the SafeCom server.
2. Click **Apply**.
3. To remove a driver from the list, select the individual driver name and click **Remove**.

Register web page

The Register web page is used to register the device with the SafeCom server.



The device can be used with SafeCom once it has been registered with the SafeCom server.

The device can also be registered with the SafeCom solution when:

- Using the Add device function in SafeCom Administrator.
- Log in at the printer as a user with Technician or Administrator rights.
 1. Enter the **User logon** and **PIN code** of a user with Technician or Administrator rights.
The user must have a PIN code.
 2. Click **Register**.

Log web page

The **Log** web page allows enabling, disabling, and viewing of logging information.




Logging should only be enabled if advised to do so as part of a troubleshooting process.

To enable or disable logging, check or uncheck the **Log enabled** check box.

If the device has a hard disk, logging data is written on the hard disk for best performance. When the log file reaches the 1 MB maximum, the log file is overwritten with new data.

If **Upload log to server** is enabled, the device uploads the log to the server when the device log is full. The feature should only be enabled as per instruction by SafeCom Support. If the device is unable to upload to the server, the device deletes the log, except for the last 100 lines, which are kept and uploaded once the connection to the server succeeds.

If **Upload log to server** is enabled, the **Show complete log** button is transformed to **Upload log to server**, and the log can be accessed from the server.

 The device always logs 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).

SafeCom Go HP – How to

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

Get the SafeCom Go HP software

The SafeCom Go HP Loader files (*.b49), SafeCom Go HP software files (*.b89) and SafeCom Go HP uninstall files (*.uin) were installed from the SafeCom CD, or a software package can be downloaded.

1. Download the safecom_go_hp_xxx.exe file from the link supplied to you.
2. Double-click the safecom_go_hp_xxx.exe file.
3. Click **Next**.
4. Select the destination folder. Click **Next**.

Normally the destination folder is: C:\Program Files\SafeCom
\SafeComG4\device_software

5. Click **Install**.
6. Click **Finish**.

To install software through HP Web Jetadmin, use the manifest-nnn.xml and nnnxxx-ilc.jar files located in the subfolder, /hp_web_jetadmin.

Specify SafeCom Server

1. Open the **Configuration** web page.
2. Optionally enter the **Group name** to exclude broadcast results from SafeCom servers that does not belong to the SafeCom group.

This is particular useful in a multi server solution.

3. Click **Broadcast**. Please wait 5 seconds before the broadcast result is populated in the **Server address** list.


If the SafeCom server has multiple IP addresses there will be an entry for each. If the SafeCom server is clustered you must ensure that it is only the entry matching the IP address of the virtual server and not the nodes.

In a multiserver solution you can click the **Move up** and **Move down** button to prioritize the order in which the servers are contacted in case the first one on the list becomes unavailable.

If the device is added through **SafeCom Administrator** the list of SafeCom servers includes the list of prioritized failover servers. For additional information about failover servers, refer to the *SafeCom G4 Administrator's Manual*.

If broadcasting fails you may have to directly enter the server address (hostname or IP address) in **Add server** and click **Add**.

4. Click **Apply**.

 After you click **Apply**, you should allow one minute before the changed SafeCom Server settings take effect. Otherwise, you may get a login error at the printer.

Register device

This section shows the default method to register the device.

The device can also be registered with the SafeCom solution by:


- Using the Add device function in SafeCom Administrator.
- Log in at the printer by a user with Technician or Administrator rights.
 1. Open the **Register** web page.
 2. Enter the **User logon** and **PIN code** of a user with Technician or Administrator rights. The user must have a PIN code.
 3. Click **Register**.

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.

Disable Encrypt All Web Communication

On CM8050 MFP and CM8060 MFP you must disable encryption while the SafeCom Go HP Loader (*.b49) is being downloaded to the HP device.

1. Open the device's web page.
2. Click on the **Networking** tab.
3. Click **Mgmt. Protocols** on the menu.
4. On the **Web Mgmt** tab, uncheck **Encrypt All Web Communication**.
5. Click **Apply**.

Set password to prevent unauthorized access

Refer to the *HP Embedded Web Server User Guide* for your HP device.

1. Open the device's web page.
2. Click the **Networking** tab.
3. Click **Authorization** on the menu.
4. Click the **Admin. Account** tab.

5. Enter **Password** for the device admin account and re-enter the password in **Confirm Password**. Click **Next**.

Set password using HP Web Jetadmin

This applies to HP Web Jetadmin version 10.


1. Open **HP Web Jetadmin**. If you do not already have a list of devices from previous use the **Device Discovery** function available on the **Tools** menu to open the Configuration Wizard and begin the discovery process, perhaps by broadcasting.
2. In the list of devices select the devices.
To select all, press Ctrl + A.
3. Open the **Config** tab page.
4. Click **Security** and scroll to **Embedded Web Server** password.
5. Enter the desired password (for example, nimda) and click **Apply**.

Disable TCP/IP(v6)

1. Open the device's web page.
2. Click on the **Networking** tab.
3. Click **TCP/IP Settings** on the menu.
4. Click on the **TCP/IP(v6)** tab.
5. Clear **Enable** for **IPv6**. Scroll to the bottom of the page and click **Apply**.

Verify the IP Address of the DNS Server

1. Open the device's web page.
2. Click on the **Networking** tab.
3. Click **Other Settings** on the menu.
4. On the **Misc. Settings** tab, enter the IP address of the DNS Server⁸ or 0.0.0.0 if there is no DNS Server.
5. Click **Apply**.

 If the IP address does not take effect, try to set it through the control panel.

Check SNMP Settings

If SNMP v1/v2 is disabled, SafeCom Go HP is unable to obtain the correct MAC address of the device and will report the MAC address 111badadd111 instead. Follow these steps to check and correct the SNMP settings.

If the check box Disable SNMPv1/v2 default Get Community Name of "public" is selected, you should go through the below steps to clear it.


1. Open the device's web page.

⁸ Some printers have both a primary and a secondary DNS Server.


2. Click on the **Networking** tab.
3. Click **Network Settings** on the menu.
4. On the **SNMP** tab, you should select **Enable SNMPv1/v2 read-write access** and clear the check box **Disable SNMPv1/v2 default Get Community Name of "public"** as this is used by SafeCom Go HP to obtain the IP address of the device.
Optionally you may wish to enter **Set Community Name** and **Get Community Name**.
If **Get Community Name** is different from public the **Community Name** on the **Configuration** web page must be set to the same name.
5. Click **Apply**.
If you want read-only access you should continue with [Step 6](#) and [Step 7](#).
6. Select **Enable SNMPv1/v2 read-only access**.
7. Click **Apply**.
8. Remember to delete the device with the bad MAC address **111badadd111** and register it again.

Set SNMP v3

1. Set up and register the HP FutureSmart device normally in SafeCom.
2. Open the device's web page.
3. Click on the **Networking** tab.
4. Click **Network Settings** on the menu.
5. On the **SNMP** tab, you should select both **Disable SNMPv1/v2** and the **Enable SNMPv3** check box.
6. Set the following:
 - **Username:** {username}
 - **Authentication protocol:** MD5
 - **Passphrase:** {pass phrase}
 - **Privacy Protocol:** AES-128
 - **Passphrase:** {pass phrase}

 Ensure that the **Authentication protocol** and **Privacy protocol** are the same on the device and in SafeCom.

7. Click **Apply**.


 Devices using SNMP v3 are displayed with a status of **Not responding** in SafeCom Administrator. Due to the SNMP v3 peculiarities, you cannot directly add such devices through SafeCom Administrator. Either add and register the device without SNMP v3 and then set SNMP v3 as described above, or use the device EWS page to install the SafeCom solution, set SNMP v3, and then register the device.

- You cannot create a device using SNMP v3 when adding a Push port; the device must be added and set prior to adding the Push port.


Allow installation of legacy packages

Spring 2014 HP FutureSmart firmware feature improved firmware upgrade security with the choice between the more secure SHA-256 Hashing algorithm and the legacy SHA-1 Hashing algorithm. The SafeCom Go HP FS is distributed and signed with SHA-1 and will work as long as the HP device allows this. If the SafeCom Go software does not install, then follow these steps.

1. Open the device's web page.
2. Click on the **Security** tab.
3. Click **General Security** on the menu.
4. Scroll to the **Firmware Upgrade Security** section and check **Allow installation of legacy packages signed with SHA-1 Hashing algorithm**.

 If the check box is unchecked, the SHA-1 signed SafeCom Go software file 31005025.b95 will not install. Instead, you must use the SHA-256 signed SafeCom Go software file 31205025.b95 or 21201037.b95 (on FutureSmart devices).

5. Click **Apply**.

- 
- Users who prefer using SHA-256 must purchase and use special edition SafeCom device software files that are SHA-256 signed.
 - The HP Scanjet Enterprise 7000n only supports SHA-1 and therefore the SHA-1 signed SafeCom Go software file 32005025.b95 must be used.

Select login method

Identification by card requires the installation of a SafeCom ID device (card reader) and maybe also SafeCom Go HP ID Kit. Identification by ID code is possible on devices with touch-screen, built-in keypad, or external SafeCom Keypad (see table in [SafeCom Go HP products](#)).

1. Open the **Configuration** web page.
2. Change **Login method** to any of the following: **Auto-sense**, **Card**, **Card or ID code**, **Card or Windows**, or **Keypad**. **Keypad** is relevant only if an external SafeCom Keypad is connected.
3. Click **Apply**.

Login with Windows without specifying the domain

On MFPs with touch-screen, it is possible to log in by entering your Windows username, password, and domain. If all users belong to the same domain you can avoid prompting users to enter the domain at the printer.

1. Open the **Configuration** web page.
2. Specify a **Default domain**.
3. Change **Pre-fill domain** to **Hide**.
4. Click **Apply**.

Login without PIN code

Use of PIN code is possible on devices with keypad or touch-screen. This setting applies to the device and overrules the equivalent user property. Requesting the user to enter a personal 4-digit PIN code as he identifies himself at the printer can enhance document security.

1. Open the **Configuration** web page.
2. Clear **Login without PIN code** if you want to prompt users for PIN code.
3. Click **Apply**.

Change PIN code

If Allow users to change PIN code is checked on the Users tab in the Server properties dialog in SafeCom Administrator users can change their PIN using the Change PIN menu after login.

1. Log in at the printer.
2. Access the menu and scroll to **Change PIN**.
3. Select/Tap **PIN Code** and enter the PIN code.
4. Select/Tap **PIN again** and enter the PIN code again.
5. Select/Tap **Apply**.

The exact steps for the newer HP LaserJet MFPs are covered in [Change PIN code](#).

Disable Pull Print

If you do not want the Pull Print icon to appear on the MFP's control panel, you can disable Pull Print.


1. Open the **Configuration** web page.
2. Clear **Pull Print** in **MFP authentication**.
3. Click **Apply**.

Enable Copy Control

The SafeCom solution can control access to the MFP's copy function.

See [Control access to the MFP's copy function](#).

On color MFPs with SafeCom Go HP version S89 nnn.030*39 or newer **MFP authentication** offers two check boxes: **Copy** and **Color copy**. By default, both are checked and as a result the **Authentication Manager** will have **SafeCom** listed as the sign-in method for **Copy** and **Color Copy**.

 Always make changes on the **Configuration** web page first before making changes on the **Authentication Manager** web page, as the SafeCom solution does not read any settings back from the **Authentication Manager** web page.

To only have the SafeCom solution control access to the MFP's color copy function:

See [Control access to the MFP's color copy function only by SafeCom](#).

i Enabling access control for color copy only is NOT recommended if the SafeCom solution is also to track copies. Mono copy jobs that are produced after the user has logged in to the color copy function are tracked as long as the user remains logged in. Mono copies are obviously not tracked when there is no user logged in. Similar situations arise if Copy is checked and Color copy is cleared.

On CM8050 MFP and CM8060 MFP, it is also possible to control if copies can be made with professional color quality XE "Professional Color Quality". When SafeCom Go HP is installed, it creates a **Permission Set** XE "Permission Set" named **SafeCom**.

See [Control making copies with professional color quality](#).

Control access to the MFP's copy function

1. Open the **Configuration** web page.
2. Check **Copy** in **MFP authentication**.
3. Click **Apply**.

Control access to the MFP's color copy function only by SafeCom

1. Open the **Configuration** web page.
2. Clear **Copy** and check **Color copy** in **MFP authentication**.
3. Click **Apply**.

Control making copies with professional color quality

1. Log in to the EWS and click the **Settings** tab.
2. Click Device Sign In on the menu.
3. Scroll to **Permission Sets**, select **SafeCom**, and click **Edit**.
4. Clear **Make a Copy with Professional Color Quality**. Click **OK**.
5. Click **Apply**.

Enable device memory usage

The SafeCom solution can control access to the MFP's memory usage to store and retrieve jobs from the MFP's storage memory.

1. Open the **Configuration** web page.
2. Check **Save to device memory** in **MFP authentication**.
3. Check **Retrieve from device memory** in **MFP authentication**.
4. Click **Apply**.

Enable Send to Folder

The SafeCom solution can control access to the MFP's send to folder function.

1. Open the **Configuration** web page.
2. Check **Folder** in **MFP authentication**.

3. Click **Apply.**

The above works if the folder's **Access Credentials** is **Public**. Relevant settings and online help are available on the **Send to Folder** menu on the **Digital Sending** tab.

If the folder's **Access Credentials** is **MFP User**, you should go to [Enable Send to Folder – with password](#).

Enable Send to Folder – with password

The SafeCom solution can control access to the MFP's send to folder function while also prompting the user for a device password. This is required if the folder's Access Credentials is MFP User. Relevant settings and online help are available on the Send to Folder menu on the Digital Sending tab.

To get the SafeCom solution to prompt for the user's password, the login method for Send to Folder must be changed to SafeCom P on the Authentication Manager web page.

1. Open the **Configuration** web page.
2. Check **Folder** in **MFP authentication**.
3. Click **Apply**.
4. Open the **Authentication Manager** web page.
5. Change the login method for **Send to Folder** to **SafeCom P**.
6. Click **Apply**.



- The SafeCom solution does not store or validate the entered device password but simply parses the password, user logon and domain to the Digital Sending function in the HP LaserJet.
- Always make changes on the **Configuration** web page first before making changes on the **Authentication Manager** web page, as the SafeCom solution does not read any settings back from the **Authentication Manager** web page.

Enable Send to E-mail – Pre-filled From: and To: field

SafeCom can control access to the MFP's Send to E-mail function⁹.

1. Open the **Configuration** web page.
2. Check **E-mail** in **MFP authentication**.
3. Make your selections in the **E-mail** section.
4. Click **Apply**.

⁹ The SafeCom Go Configuration web page for FutureSmart devices does not include the E-mail section. To configure e-mail on FutureSmart devices, use the device's own web page.



- On HP FutureSmart devices the set up of default From: and To: e-mail addresses is performed on the device web page on the **Scan/Digital Send** tab under E-mail Setup.
- On HP LaserJet CM8050 MFP and CM8060 MFP address field control is NOT controlled as described below, but must be controlled through the E-mail Setup menu on the Digital Sending tab (see [Send to E-mail on CM8050 MFP and CM8060 MFP](#)).

By default, the **From:** field is not editable at the device and the **To:** field is editable. Both fields are by default pre-filled with the **User e-mail**.

The **From:** field can be pre-filled with **User e-mail**, **Device name**, **Blank**, or **Default From: address**.

An e-mail sent with pre-filled **User e-mail** of the user John Smith with the e-mail address {js@safecom.eu} will appear as:

```
From: John Smith {js@safecom.eu}
```

If the user does not have an e-mail address the **Default From: address** is used. If this is not configured, then {no_reply@safecom.invalid} is used. An e-mail sent from pre-filled **Device name** HP LaserJet M5035 MFP appears as:

```
From: HP LaserJet M5035 MFP {no_reply@safecom.invalid}
```

Here {no_reply@safecom.invalid} is replaced with what is specified in **Default From: address**.

The **To:** field can be pre-filled with **User e-mail**, **Blank** or **Default To: address**. The **CC:** and **BCC:** fields are only editable if the **To:** field is editable.

Check **Force BCC to user** to have the **BCC:** field pre-filled with the user's e-mail address.

Enable Send to E-mail – with password

If the mail system (SMTP server) requires users to be validated by their user logon and password before e-mails are sent, then users need to be prompted for their password when use the Send to E-mail function.

To get SafeCom to prompt for the user's password, the login method for Send to E-mail must be changed to SafeCom P on the Authentication Manager web page.

1. Open the **Configuration** web page.
2. Check **Folder** in **MFP authentication**.
3. Click **Apply**.
4. Open the **Authentication Manager** web page.
5. Change the login method for **Send to E-mail** to **SafeCom P**.
6. Click **Apply**.



- SafeCom does not store or validate the entered password but simply parses the password, user logon, and domain to the Digital Sending function in the HP LaserJet.
- Always make changes on the **Configuration** web page first before making changes on the **Authentication Manager** web page, as the SafeCom solution does not read any settings back from the **Authentication Manager** web page.

Enable SafeCom Smart Scan

The SafeCom Smart Scan feature allows users to scan a document and then manage and download the scanned files from either the SafeCom Web Interface (*SafeCom G4 Web Interface Administrator's Manual*) or from the SafeCom Move (*SafeCom G4 Administrator's Manual*).

1. Open the **Configuration** web page.
2. Scroll to the **Device** section and under MFP authentication, check **Smart Scan**.
3. Click **Apply**.



SafeCom Smart Scan is only supported for SafeCom Go HP on HP FutureSmart devices.

Control user access rights

When using SafeCom G3 server version S82 070.440*03 or newer, you can control users' access rights to specific features through SafeCom Administrator, refer to the *SafeCom G4 Administrator's Manual*. You can control access rights to the following features:

- Copy
- Copy in color
- Copy in simplex*
 - * Copy in simplex can only be controlled on embedded devices.
- E-mail
- Scan
- Fax
- USB memory print
- USB memory scan
- Print all button
- Extended functions

Enable Client Billing and the Account icon

1. Open the **Configuration** web page.
2. Check **Account** in **MFP authentication**.
3. Click **Apply**.

The following two settings must be checked for the billing code to become part of the tracking record.

- **Client Billing** is checked on the **License** tab in the **Device properties** dialog in **SafeCom Administrator**.
- **Bill clients for cost** is checked on the **Settings** tab in the **User properties** dialog in **SafeCom Administrator**.

i Be aware that Client Billing is not available for HP Officejet Pro and the embedded solution for HP FutureSmart devices. For HP FutureSmart devices configured through the SafeCom Device Server, the Client Billing is available.

Enable Third party authentication

1. Open the **Configuration** web page.
2. Scroll to the **Enable third party authentication** section at the bottom of the page.
3. Check **Enable third party authentication** and this overrides any settings made to the SafeCom login method.
4. Enter the field name that contains the user's optional ID code.
5. Enter the field name that contains the user's logon.
As a minimum, either the **ID code** or the **User logon** must be entered.
6. Enter the field name that contains the user's domain.
7. Click **Apply**.

Control max length of encryption keys

i When connected to a SafeCom G2 server, this section is ignored and the Asymmetric key is always 512-bit, the Symmetric key is always 128-bit, and TwoFish is encrypted.

1. Open the **Configuration** web page.
2. Scroll to the **Encryption** section at the bottom of the page.
3. Set the key lengths.
Asymmetric key max length can be: **Default, 512, 1024, or 2048.**
Symmetric key max length can be: **Default, 128, or 256.**
Leave it at **Default** and the device will comply¹⁰ with the length of the encryption keys that has been specified on the **Encryption** tab in the **Server properties** dialog in **SafeCom Administrator**.
4. Click **Apply**.
 - SafeCom control data to and from the device is always encrypted. Control data includes user details, such as ID code, PIN code, and Password.

¹⁰ If 2048-bit has been specified on the Server, due to performance reasons, the device will only use 1024-bit.

- Pull print documents are always encrypted when transferred from the SafeCom Pull Port to their storage location.
- Pull print documents are always encrypted while they are stored and waiting to be collected.
- Pull print documents (print data) are normally not sent encrypted to the device as it will reduce the print speed. For print data to be sent encrypted to the device the user must have **Encrypt documents** checked on the **Settings** tab in the **User properties** dialog and **Encryption** must be checked in the **Device properties** dialog.

Restore factory default

1. Open the **Configuration** web page.
2. Click **Restore factory default**.

The factory default values are:

Configuration settings	Default value
Group name	
TCP port	7500
Server address	
Device name	
Device model	
Device location	
Login method	Auto-sense
Default domain	
Pre-fill domain	Blank
Mask ID code	Cleared (No)
Login without PIN code	Checked (Yes)
Print all at login	Cleared (No)
Document list, Show newest first	Checked (Yes)
MFP authentication, Pull Print	Checked (Yes)
MFP authentication, Copy	Checked (Yes)
MFP authentication, Color copy	Checked (Yes)
MFP authentication, Folder	Cleared (No)
MFP authentication, Fax	Cleared (No)
MFP authentication, E-mail	Checked (Yes)
MFP authentication, Account	Cleared (No)
Drivers	
Timeout	60 seconds
Post track	Cleared (No)
High speed print	Checked (Yes)

Configuration settings	Default value
E-mail, Default From: address	
E-mail, Pre-fill From: field	User E-mail
E-mail, Editable	Cleared (No)
E-mail, Default To: address	
E-mail, Pre-fill To: field	User E-mail
E-mail, Editable	Checked (Yes)
E-mail, Force BCC to user	Cleared (No)
Enable third party authentication	Cleared (No)
ID code	
User logon	
Domain	
Asymmetric key max length	Default
Symmetric key max length	Default
Log settings	Default value
Log	Disabled

Determine the version

The version of the SafeCom Go HP software can be determined from the Information web page.

Open the **Information** web page.

The version can also be seen in the **Device properties** dialog in **SafeCom Administrator**.

Handle hard disk replacement

If the device had a hard disk when you installed SafeCom Go HP initially, replacing the hard disk will remove the SafeCom Go HP software from the device.

To get it working again, send the SafeCom Go HP Loader and SafeCom Go HP Software and configure it as before.

1. Open **SafeCom Administrator**.
2. Right-click the device and click **Send Go Loader**.
3. Right-click the device and click **Update software**.
4. After the device has restarted, right-click the device and click **Open in web browser**.
5. Open the **Configuration** web page to configure it as before and click **Apply**.

Handle new MAC address (Jetdirect network card)

In the SafeCom database, the device is recorded by its unique MAC address. The device's MAC address changes if the Jetdirect network card is changed. On devices with Jetdirect Internal (JDI) the MAC address changes if the formatter board with the network connector is replaced.

To resolve this, it is recommended to delete the device from the SafeCom database and add it again.

1. Open **SafeCom Administrator**.
2. Browse to devices and right-click the device and click **Delete device**.
3. Add the device again by right-clicking **Devices** and selecting **Add device**.
4. Go through the Add Device Wizard to add the device again.

Use another server in a multi server solution

To better spread the workload among the SafeCom servers you may want to move a device from one server to another.

1. Open the **Configuration** web page and change the **SafeCom server IP address** to that of the new server.



- After you click **Apply**, you should allow one minute before the changed SafeCom Server settings take effect. Otherwise, you may get a login error at the MFP.
- On a cluster server, the IP address must be that of the virtual server.

2. Open the **Device properties** dialog in **SafeCom Administrator** and point to the new **Home server**.

How to obtain svcErr.log from the printer

HP printers with hard disk drive (HDD) and newer HP firmware maintain a service error log file with useful information. You should only obtain this file if instructed to do so by Support personnel as part of troubleshooting.



If the HP LaserJet is reporting some sort of service error, you need to restart the device before you can extract the svcErr.log file.

1. Open the device's web page.
2. Change the URL to be the following:

```
http://{ip address}/hp/device/svcErr.log
```

3. Press **Enter** to view the svcErr.log file.

The content will look something like:

```
<device_error
time="Tue Jan 15 12:50:50 2008"
time_t="1200401450"
device_uptime="4"
model_number="9050mfp"
firmware_version="08.081.5"
pid="0"
tid="0"
error_code="0xFF81"
error_msg1=""
error_msg2=""
file_name="unknown.c"
line_num="0" >
```



```
</device_error>
```

4. Save the file.

How to open the SafeCom Loader web page

The SafeCom Loader web page is primarily used in connection with troubleshooting.

1. Open the device's web page.
2. Change the URL to be the following:

```
http://{ip address}/hp/device/this.loader
```

i To access the **Package Loader**, a password must be set for the admin account.

3. On the **Package Loader** web page, scroll to table of **Reloadable Packages**.
4. Click **SafeCom Go Loader** to open the **SafeCom Loader** web page.
 - Click **About** to see contact information.
 - Click **File Directory** to see listing of what is stored on the device.
 - Click **Restart device** to restart the device.

HP Access Control USB proximity card reader

To use the HP Access Control USB proximity card reader, you need to use SafeCom G4 and you must have an ID device license associated with the device. In SafeCom Administrator, open the Device properties dialog, go to the License tab, and ensure that ID device is checked.

i Expect card numbers to differ between HP and SafeCom supplied card readers. To work-around, allow user to register multiple cards (ID codes).

The HP reader can support two different technologies. HP Officejet and FutureSmart devices that are controlled by the SafeCom Device Server, the HP reader must be configured before it is attached to the HP device.

For other HP devices this is controlled, not from the Configuration page, but from the configuration file of the device. SafeCom Device Utility can be used to configure this.

1. Browse to the SafeCom G4 installation folder.

Example:

```
C:\Program Files\SafeCom\SafeComG4
```

2. Run the **scDevUtil.exe** file.
3. Enter the address of the HP printer/MFP and click **Add**.
4. Right-click the device and click **Edit configuration**.
5. In the XML file, scroll to the <LOGIN> section and edit the HEX code between the <CARDTYPE1> and <CARDTYPE2> tags.
For example, a value of EF04 indicates a HID Prox card.
6. When finished editing, click **Update**.

i It is possible to use the GoBuild program to make a B89 file that can be used to configure multiple HP devices based on the Chai platform, refer to *Tec note SafeCom GoBuild D20127*.

HEX code	Card type
6F01	iClass CSN ISO1443A CSN ISO15693A CSN (RDR-758x Compatible)
7D01	HID iClass CSN
7E01	ISO 15693A CSN I-Code CSN my-d CSN Etag CSN (Secura Key) Tag-It CSN (Texas Instruments)
7F01	ISO 14443A CSN Advant CSN (Legic) DESFire CSN I-tag CSN MiFare CSN (Philips, NXP) MiFare Ultralight CSN (Philips, NXP)
EA01	Farpointe Data NXT UID Keri NXT UID Pyramid UID
EA02	Farpointe Data 26 Bit Keri NXT 26 Bit, Pyramid 26 Bit
EB02	Radio Key (Secura Key -02) (RDR-6Z8X Compatible)
EC01	SecuraKey - 01
ED02	Indala ASP+ UID (Motorola) - No decryption, raw data returned.
EF04	HID Prox
F004	ReadyKey PRO UID
F201	HiTag 2 Primary (RDR-6HXX Compatible)
F204	HiTag 2 Alternate
F302	HiTag 1 and S Primary (RDR-6H8X Compatible)
F304	HiTag 1 and S Alternate
F401	Deister UID
F503	GProx-II UID
F602	Cardax UID Russwin UID
F702	2Smart Key (Honeywell) KeyMate Nexwatch (Honeywell) Nexkey QuadraKey
F801	Keri UID (RDR-6K8X Compatible)
F802	Keri 26 Bits
F902	IoProx (Kantech)
FA02	Awid
FB01	DIGITAG EM/Marin EM410x/Rosslaire Primary (RDR-6E8X Compatible)
FB02	EM/Marin EM410x/Rosslaire Alternate
FC02	Casi-Rusco
FD01	Indala ASP UID (Motorola) - No Script used, raw data is returned.
FD02	Indala ASP 26 Bit (Motorola) - Indala 26 bit script used.

SafeCom Go HP update software


Initially the SafeCom Go HP Loader (see [SafeCom Go HP software installation](#)) needs to be installed on the device. Subsequent update of the main SafeCom Go HP software can be accomplished by using the **SafeCom Administrator** to upload the appropriate *.b89 or *.b95 file to the device.

Is the SafeCom Go HP software loaded?

To establish if SafeCom Go HP software is loaded, you can access and check the Package Loader.

1. Open the device's web page.
2. Change the URL to be the following:

```
http://{ip address}/hp/device/this.loader
```

 To access the **Package Loader**, a password must be set for the admin account (see [Set password to prevent unauthorized access](#)).

3. On the **Package Loader** web page, scroll to table of **Reloadable Packages**.

The list of installed SafeCom Go packages are:

- SafeCom Go
- SafeCom Go Loader
- SafeCom Go Library

Uninstall SafeCom Go HP

To uninstall SafeCom Go HP from a FutureSmart device, see [Uninstall SafeCom Go HP on FutureSmart devices](#).

To uninstall SafeCom Go HP from a non-FutureSmart device, see [Uninstall SafeCom Go HP on non-FutureSmart devices](#).

Uninstall SafeCom Go HP on FutureSmart devices

SafeCom Go HP can also be removed by performing a partial disk clean on the device (see [HP OPS installation](#)).

1. Open the device in a web browser by entering the IP address in the address field.
2. Sign in using the device login and password.
3. Click the **General** tab and then click **SafeCom** in the menu on the left. In the **Configuration** pane under **MFP authentication**, uncheck **Pull Print** (and **Smart Scan**, if applicable) and click **Apply**.
4. Click the **Security** tab, click **Access Control** in the menu on the right. In the **Access Control** pane under **Sign In and Permission Policies**, click **Manage Permission Sets**. Select **SafeCom** and click **Delete**.

5. On the **General** web page, click **Solution Installer**.
6. Under **Installed Solutions**, check the SafeCom Go solution and click **Remove**.
7. Click **Remove** to confirm deletion of the SafeCom Go HP solution from the device and the device restarts.

Uninstall SafeCom Go HP on non-FutureSmart devices

The SafeCom Go HP software can be uninstalled from the device by loading a SafeCom Go HP uninstall file (*.uin) through **SafeCom Administrator**. The SafeCom Go HP Loader (very small in size) is not removed by SafeCom Go HP uninstall.

This means that you can temporarily disable SafeCom Go HP by uninstalling and then re-enable it by sending the SafeCom Go HP software file (*.b89) to it and configure it again.

The SafeCom Go HP Loader can be removed using the printer's **Package Loader**. Do a DISK INIT on the device to remove everything.

Make all printing through SafeCom

Follow the steps below to restrict printing to SafeCom.

Refer to the *HP Embedded Web Server User Guide* for your HP device.

1. Open the device's web page.
2. Click on the **Settings** tab.
See the note in [Login](#) if the tab is missing.
3. Click **Security** on the menu.
4. Clear **Print Page** and check **Disable Direct Ports** (USB and parallel). Click **Apply**.
5. Click on the **Networking** tab.
6. Click **Authorization** on the menu.
7. Click on the **Access Control** tab.
8. Enter the **IP Address** of the SafeCom server and check **Enable**.
If the SafeCom server is clustered, it is necessary to enter the IP address of each physical node.
9. Enter the **IP Address** of the device and check **Enable**.
10. Click **Apply**.

SafeCom Go HP device trace facility

Use the **Mail to SafeCom Support** button on the SafeCom Go HP **Information** web page to collect information from the device, such as HP firmware version and last device states.

The SafeCom Go HP log facility is also useful in troubleshooting situations, but it should only be enabled upon request from SafeCom support personnel. The log facility is enabled on the SafeCom Go HP Log web page. You may also be asked to obtain the svcErr.log file (see [How to obtain svcErr.log from the printer](#)).

Chapter 4


Using SafeCom Go HP

Select the appropriate device from the sections below.

HP LaserJet (Enterprise) M525, M575, CM4540 MFP, M4555 MFP, MFP 725, MFP 775, MFP 830, and MFP M880 variants

This section contains information about the following devices:

- HP LaserJet
 - M525 MFP
 - M575 MFP
 - CM4540 MFP
 - M4555 MFP
- HP LaserJet Enterprise
 - 500 MFP M525
 - flow MFP M525
 - Color MFP M575
 - flow Color MFP M575
 - MFP 725
 - Color MFP 775
 - MFP 830
 - MFP M880

 The size and looks of the touch-screens of the above mentioned devices do vary, but the workflows are the identical.


Login

The login sequence is initiated if you are not already logged in and tap any icon (**Pull Print**, **Copy**, **E-mail**, **Fax**, or **Network Folder**) that requires SafeCom to handle the **MFP authentication**.



If the copy function requires SafeCom authentication, pressing the **Start** button will also initiate the login sequence. Once logged in, the documents placed in the automatic document feeder (ADF) will be copied.

The recommended login sequences are described in the following sections.

 A PIN code only is required if both the user and the device is set up to require PIN code. This applies to both the login sequences and when the user registers a card using a PUK code.

- To log in with card, see [Login with card](#).
- To log in with card and PIN code, see [Login with card and PIN code](#).
- To log in with ID code, see [Login with ID code](#).
- To log in with ID code and PIN code, see [Login with ID code and PIN code](#).
- To log in with Windows, see [Login with Windows](#).

If **Login method** is set to **Card or Windows**, it is possible to log in by either using your card or entering your Windows login credentials.

Login with card

Use the card reader.

Login with card and PIN code

1. Use the card reader.
2. Enter **PIN code** on the keypad or touch-screen.
3. Tap **OK**.

Login with ID code


1. Tap the **Sign In** icon (or press the **Start** button to copy).
2. Enter **ID code** on the keypad or touch-screen.
3. Tap **OK**.

Login with ID code and PIN code


1. Tap the **Sign In** icon (or press the **Start** button to copy).
2. Enter **ID code** on the keypad or touch-screen.
3. Tap **OK**.
4. Enter **PIN code** on the keypad or touch-screen.
5. Tap **OK**.

Login with Windows

1. Tap **Domain** and specify the Domain.
2. Tap **Username** and enter username on the touch-screen. Tap **OK**.

 Username cannot be blank.

3. Tap **Password** and enter password on the touch-screen. Tap **OK**.

 Password cannot be blank.

4. Tap **OK**.

Register card at device with Windows credentials

1. Use the card reader.

If the card is unknown, the **SafeCom Card Registration** page appears.

i If there is an available PUK code in the SafeCom system, the user also has the option to register the card using a PUK code (see screenshot in [Register card at device with PUK code](#)).

2. Select the appropriate domain from the **Domain** dropdown menu.

i

- Domains are added in **SafeCom Administrator** under the **Users** menu.
- The domain dropdown list only refreshes after resubmitting the SafeCom Go settings or restarting the device.

3. Tap the **User name** field and enter the Windows user name using the keypad or touch-screen. Tap **OK**.
4. Tap the **Password** field and enter the Windows password on the keypad or touch-screen. Tap **OK**.
5. Tap **OK**.
The card is now registered and the user is prompted to log in again.
6. Tap **OK** and then **Cancel** before logging in with the card reader again.

Register card at device with PUK code

1. Use the card reader.

If the card is unknown and there is an available PUK code in the SafeCom system, the **SafeCom Card Registration** page appears with the options to register the card using a PUK code or Windows credentials.

2. Tap the **PUK** field and enter the PUK code on the keypad or touch-screen.
3. If required, enter the PIN code and tap **OK**.

i

- A PIN code is only required if both the user and the device are set up to require PIN code.
- Be aware that if you log in using a PUK code for a registered card that already has a PIN code, and you enter a PIN code when prompted, the system will treat this as a PIN code change, thus rendering your old PIN code invalid. You can enter your existing PIN code if you want to keep using that.

The card is now registered and you are asked to log in again.

4. Tap **OK** then **Cancel** before logging in using the card reader again.

Pull Print – Document list

Tap the **Pull Print** icon to access the **Document list** that allows you to print individual documents. Documents appear in chronological order with the newest at the top of the list. If **Print all at login** is checked any documents pending collection will be printed first.

In the document list a document with a preceding R shows the document is retained. A delegated document will have a preceding D. Tap the **Info** button to see information about who delegated the document. A group print document will have a preceding G. The figure preceding the document name (for example, 1.60) is the cost of the document.

- Tap **Print all** to print all documents, excluding any retained documents. Documents are printed in chronological order (oldest first).
- Tap **Refresh** to update the list of documents with pending documents that has finished spooling after the user logged in.
- Tap **Print** to print the selected documents.
- Tap **Retain** if you want the selected documents to remain on the list (server) after they have been printed. A retained document is marked with a preceding R.
- Tap **Delete** to delete the selected documents.
- Tap **Info** to see information about the selected documents, including cost, driver name, use of color and duplex.
- Tap **Copies** to request multiple copies of a document. **Print all** always prints one copy of each document.

Copy

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

Folder

Tap the **Network Folder** icon. Tap **Start** to scan and send the document to folder.

E-mail

Tap the **E-mail** icon. It is configurable if the fields should be editable or not. For each field, tap the field button and enter the value on the keypad or touch-screen. Tap **Start** to scan and e-mail the document.

Account – Select Billing Code

Tap the **Account** icon to select a billing code.

Select the billing code among the available codes. The **Favorites** tab lists the user's favorite billing codes in alphabetical order. The **Last used** tab lists up to 10 of the user's last used billing codes with the last used at the top of the list.

- Tap **Billable** to use the selected billing code.

- Tap **Not billable** to use the selected billing code, but keep it off the invoice to the customer (client). The button is only available if the administrator has recorded the selected billing code as billable.
- Tap **Personal** to return to the home screen without selecting a billing code. When selecting Personal, the tracking data will contain "Personal" for code and "Used for personal billing" for description. This is to differentiate it from tracking data without billing at all, for example, from a device without billing license.
- Tap **Info** to see information about the selected billing code, including the unabbreviated description.

Smart Scan

Put the document in the document feeder and tap the **Smart Scan** icon.


Enter a prefix for the document. The document name is the prefix followed by a timestamp. If a scanned file entails more than one page, the file name is also followed by a number that increments by 1 for each new file (for example, agenda20121010152801-01).

The default file name is the timestamp and the scanned files are always saved in the selected format.

Tap **More Options** to make changes to the scan properties. For example, allow a multiple page document to be scanned to a single file, by turning on **Job Build**.

Tap **Scan** to scan the document.

Now the scanned files are available for download in either the SafeCom Web Interface or SafeCom Move.


 Refer to *SafeCom G4 Web Interface Administrator's Manual* or *SafeCom G4 Administrator's Manual* for more information on SafeCom Move.

Logout

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

To logout actively perform one of the following actions:

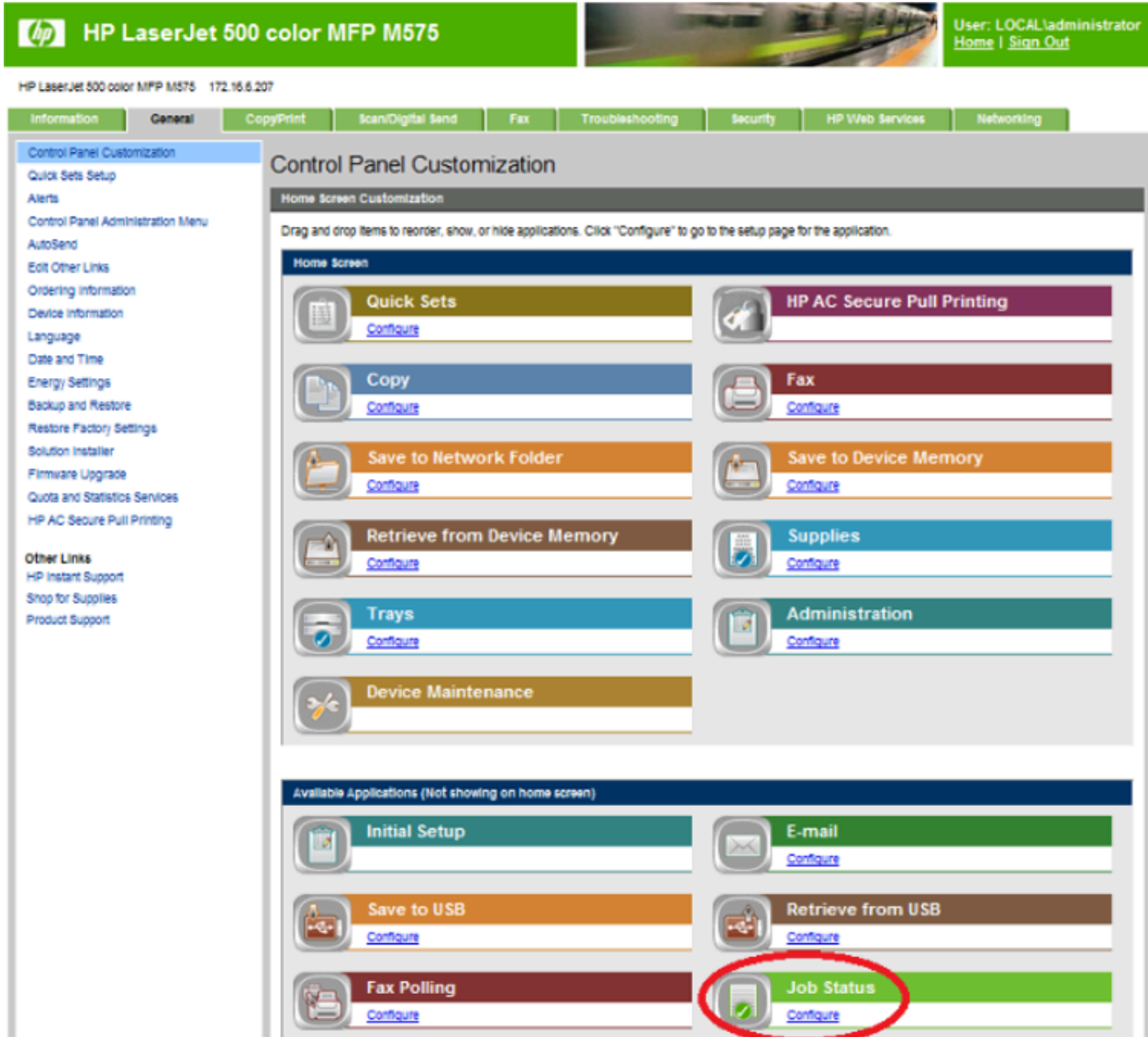
- Tap **Sign Out**.
- Use your card again (if a card reader is connected and you logged in by card).

 If Copy Control is enabled, the "Logging out" message is displayed until the MFP is in idle state. This is required to allow correct reading of the MFP's copy page counters.

Hide document name

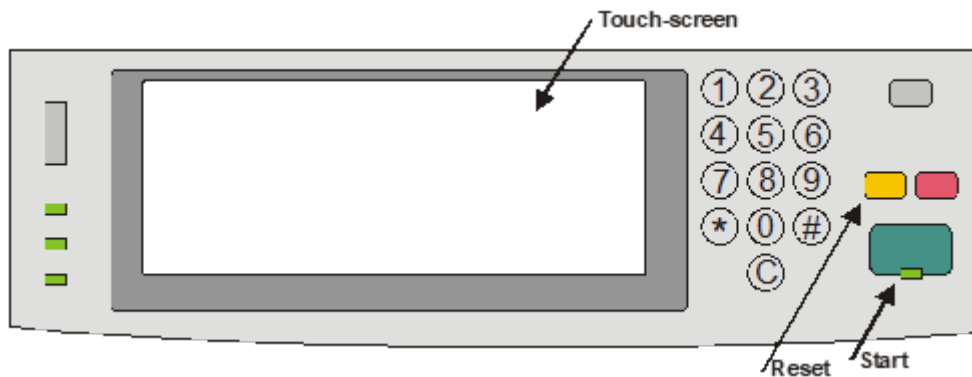
On some devices, users have the opportunity to access a list of recently printed documents. SafeCom Go HP provides a function which allows administrators to limit user access to the **Job**

Status application. To access the functionality, access the web interface of the device, click **Control Panel Customization**, then drag-and-drop **Job Status** to the list of available applications:



HP LaserJet M3035 MFP, CM3530 MFP, CM4730 MFP, M5035 MFP, M5039 MFP, CM6030 MFP, CM6040 MFP, CM6049 MFP, M9040 MFP, M9050 MFP, and M9059 MFP

Control panel



Login

The login sequence is initiated if you are not already logged in and tap any icon (**Pull Print, Copy, E-mail, Fax, or Network Folder**) that requires SafeCom to handle the **MFP authentication** (see [Configuration web page](#)).

If the copy function requires SafeCom authentication, pressing the **Start** button will also initiate the login sequence. Once logged in, the documents placed in the automatic document feeder (ADF) will be copied.

i On the CM3530 MFP, the control panel is in color.

The recommended login sequences are described in the following sections.

- To log in with card, see [Login with card](#).
- To log in with card and PIN code, see [Login with card and PIN code](#).
- To log in with ID code, see [Login with ID code](#).
- To log in with ID code and PIN code, see [Login with ID code and PIN code](#).
- To log in with card or ID code, see [Login with ID code and PIN code](#).
- To log in with Windows, see [Login with Windows](#).

If **Login method** is **Card or Windows**, it is possible to log in by either using your card or entering your Windows login credentials.

- To log in with password, see [Login with password](#).


Login with card

1. Use the card reader.
2. Before 10 seconds have elapsed, tap the icon (or press the **Start** button to copy).

i If you tap an icon before using the card, a dialog saying **Use card then tap OK** will appear.

Login with card and PIN code

1. Use the card reader.
2. Before 10 seconds have elapsed, tap the icon (or press the **Start** button to copy).
3. Enter **PIN code** on the keypad or touch-screen.
4. Tap **OK**.

 If you tap an icon before using the card, a dialog saying **Enter PIN code then use card and tap OK** will appear.

Login with ID code

1. Tap any icon (or press the **Start** button to copy).
2. Enter **ID code** on the keypad or touch-screen.
3. Tap **OK**.

Login with ID code and PIN code


This login sequence is also recommended if Login method (see [Allow installation of legacy packages](#)) is Card or ID code.

1. Tap any icon (or press the **Start** button to copy).
2. Enter **ID code** on the keypad or touch-screen.
3. Tap **OK**.
4. Enter **PIN code** on the keypad or touch-screen.
5. Tap **OK**.


For the Card or ID code login method, if you tap an icon before using the card, a dialog saying **Enter ID code OR use card then tap OK** will appear. If you also need to enter PIN code, the dialog will say **Enter ID code OR use card then enter PIN code and tap OK**.

Login with Windows

1. Tap **Username** and enter **Username** on the touch-screen. Tap **OK**.

 Username cannot be blank.

2. Tap **Password** and enter **Password** on the touch-screen. Tap **OK**.

 Password cannot be blank.

3. Tap **Domain** and enter **Domain** on the touch-screen. Tap **OK**.
The solution can be configured to not prompt for the domain.
4. Tap **OK**.

Login with password

If SafeCom P has been selected as the Login method in the Authentication Manager, the user is prompted for a password (max 33 characters) and there are two additional steps in the login sequence. Prompting for password can be relevant when using Send to Folder (see [Enable Send to Folder – with password](#)) and Send to E-mail (see [Enable Send to E-mail – with password](#)).

1. Enter **Password** on the touch-screen.
2. Tap **OK**.

Pull Print – Document list

Tap the **Pull Print** icon to access the **Document list** that allows you to print individual documents. Documents appear in chronological order with the newest at the top of the list. If **Print all at login** is checked any documents pending collection will be printed first.

In the document list, a document with a preceding **R** shows the document is retained. A delegated document will have a preceding **D**. Tap the **Info** button to see information about who delegated the document. A group print document will have a preceding **G**. The figure preceding the document name (for example **1.10**) is the cost of the document.

- Tap **Print all** to print all documents, excluding any retained documents. Documents are printed in chronological order (oldest first).
- Tap **Print** to print the selected documents.
- Tap **Retain** if you want the selected documents to remain on the list (server) after they have been printed.
- Tap **Delete** to delete the selected documents.
- Tap **Info** to see information about the selected documents, including cost, driver name, use of color, and duplex.
- Tap **Refresh** to update the list of documents with pending documents that has finished spooling after the user logged in.
- Tap **Copies** to request multiple copies of a document. **Print all** will always be one copy of each document.
- Tap **Back** to return to the home screen.

Copy

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

Folder

1. Tap the **Network Folder** icon. Tap **Start** to scan and send the document to folder.
See also [Enable device memory usage](#).
The SafeCom solution can control access to the MFP's memory usage to store and retrieve jobs from the MFP's storage memory.
2. Open the **Configuration** web page.
3. Check **Save to device memory** in **MFP authentication**.

4. Check **Retrieve from device memory** in **MFP authentication**.
5. Click **Apply**.
Enable Send to Folder.

E-mail

Tap the **E-mail** icon. It is configurable if the fields should be editable or not. The **To:** field can be pre-filled with the **User e-mail**, **Blank**, or **Default To: address**. The **From:** field can be pre-filled with **User e-mail**, **Device name**, **Blank**, or **Default From: address**. See [Enable Send to E-mail – Pre-filled From: and To: field](#). For each field, tap the field button and enter the value on the keypad or touchscreen. Tap **Start** to scan and e-mail the document.

Account – Select Billing Code

Tap the **Account** icon to select a billing code.

Select the billing code among the available codes. The **Favorites** tab lists the user's favorite billing codes in alphabetical order. The **Last used** tab lists up to 10 of the user's last used billing codes with the last used at the top of the list.


- Tap **Billable** to use the selected billing code.
- Tap **Not billable** to use the selected billing code, but keep it off the invoice to the customer (client). The button is only available if the administrator has recorded the selected billing code as billable.
- Tap **Personal** to return to the home screen without selecting a billing code. When selecting Personal the tracking data will contain "Personal" for code and "Used for personal billing" for description. This is to differentiate it from tracking data without billing at all, for example, from a device without billing license.
- Tap **Info** to see information about the selected billing code, including the unabbreviated description.

Logout

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

To logout actively, do any of the following:

- Press the **Reset** button.
- Tap **Sign Out**.
- Use your card again (if a card reader is connected and you logged in by card).

 If Copy Control is enabled, the "Logging out" message is displayed until the MFP is in idle state. This is required to allow correct reading of the MFP's copy page counters.

Register card at device

There are two ways the user can register a card while standing at the device:

- To register a card by entering Windows user logon, password, and domain, see [Register card with Windows credentials](#).
- To register a card by entering an 8-digit PUK code, see [Register card with PUK code](#).

Register card with Windows credentials

The user must have a network logon.

1. Use the card reader.
 - If there are any available PUK codes on the system, tap **Cancel** in the **Please enter PUK** dialog. The **Login to register card** dialog appears.
 - If there are no available PUK codes, the user gets the **Login to register card** dialog.
2. Tap **OK** to log in to register card.
3. Tap **Username** and enter **Username** on the touch-screen. Tap **OK**.
4. Tap **Password** and enter **Password** on the touch-screen. Tap **OK**.
5. Tap **Domain** and enter **Domain** on the touch-screen. Tap **OK**.
The solution can be configured to not prompt for the domain.
6. Tap **OK**.
The card is registered and you are logged in.

Register card with PUK code

The PUK code must be supplied to the user in advance, typically through e-mail.

1. Use the card reader.
If the card is unknown and there is an available PUK code in the SafeCom system, the user is prompted to enter his PUK code.
2. Enter **PUK code** on the keypad or touch-screen.
3. Tap **OK**.

Steps 4-7 are relevant only if the device requires login by PIN code (**Login without PIN code** is not checked).

4. Enter **PIN code** on the keypad or touch-screen.
5. Tap **OK**.
6. Enter **PIN again** on the keypad or touch-screen.
7. Tap **OK**.
The card is registered and you are asked to log in again.

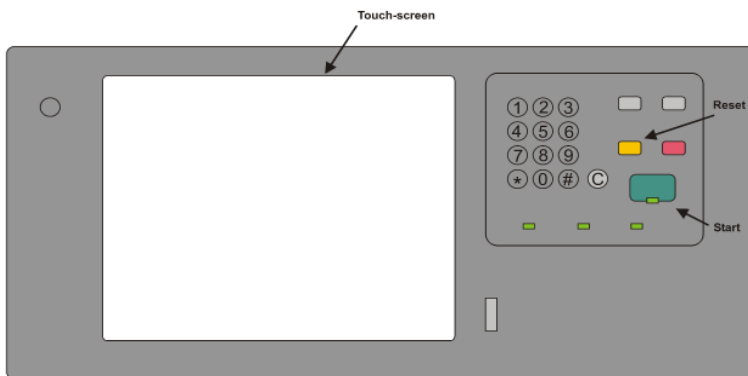
Change PIN code

If Allow users to change PIN code is checked on the Users tab in the Server properties dialog in SafeCom Administrator, users can change their PIN using the Change PIN menu after login. However, the Change PIN menu is not available when the Document list is open.

1. Log in at the Device.
2. Tap the **Administration** icon.
3. Tap **Change PIN**.
4. Tap **PIN code**.
5. Enter **PIN code** on keypad or touch-screen. Tap **OK**.
6. Tap **PIN again**.
7. Enter **PIN code** on keypad or touch-screen. Tap **OK**.
8. Tap **Apply**.

HP Color LaserJet CM8050 MFP and 8060 MFP

Control panel



Login

The login sequence is initiated if you are not already logged in and tap **Sign In** or any icon (**Pull Print**, **Copy**, **E-mail**, **Fax**, or **Network Folder**) that requires SafeCom to handle the **MFP authentication**.

The recommended login sequences are described in the following sections.

- To log in with card, see [Login with card](#).
- To log in with card and PIN code, see [Login with card and PIN code](#).
- To log in with ID code, see [Login with ID code](#).
- To log in with ID code and PIN code, see [Login with ID code and PIN code](#).

- To log in with card or ID code, see [Login with ID code and PIN code](#).

Login with card

1. Use the card reader.
2. Before 10 seconds have elapsed, tap an icon or tap **Sign In**.

i If you tap an icon before using the card, a dialog saying **Use card then touch OK** will appear.

Login with card and PIN code

1. Use the card reader.
2. Before 10 seconds have elapsed, tap an icon or tap **Sign In**.
3. Enter **PIN code** on the keypad or touch-screen.
4. Tap **OK**.

i If you tap an icon before using the card, a dialog saying **Enter PIN code then use card and touch OK** appears.

Login with ID code

1. Tap any icon or tap **Sign In**.
2. Enter **ID code** on the touch-screen.
3. Tap **OK**.

Login with ID code and PIN code

This login sequence is also recommended if the Login method is Card or ID code.

1. Tap any icon or tap **Sign In**.
2. Enter **ID code** on the touch-screen.
3. Enter **PIN code** on the keypad or touch-screen.
4. Tap **OK**.

For the Card or ID code login method, if you tap an icon before using the card, a dialog saying **Enter ID code OR use card then tap OK** will appear. If you also need to enter PIN code, the dialog will say **Enter ID code OR use card then enter PIN code and tap OK**.

Pull Print – Document list

Tap the **Pull Print** icon to access the **Document list** that allows you to print individual documents. Documents appear in chronological order with the newest at the top of the list. If **Print all at login** is checked any documents pending collection will be printed first.

In the document list a document with a preceding **R** shows the document is retained. A delegated document will have a preceding **D**. Tap the **Info** button to see information about who delegated the

document. A group print document will have a preceding **G**. The figure preceding the document name (for example **0.50**) is the cost of the document.

- Tap **Print all** to print all documents, excluding any retained documents. Documents are printed in chronological order (oldest first).
- Tap **Print** to print the selected documents.
- Tap **Retain** if you want the selected documents to remain on the list (server) after they have been printed.
- Tap **Delete** to delete the selected documents.
- Tap **Info** to see information about the selected documents, including cost, driver name, use of color and duplex.
- Tap **Refresh** to update the list of documents with pending documents that has finished spooling after the user logged in.
- Tap **Copies** to request multiple copies of a document. **Print all** will always be one copy of each document.

Copy

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

Folder

Tap the **Network Folder** icon. Tap **Start** to scan and send the document to folder.

E-mail

Tap the **E-mail** icon. For each field, tap the field button and enter the value on the keypad or touch-screen. Tap **Start** to scan and e-mail the document.

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, do any of the following:

- Press the **Reset** button.
- Tap **Sign Out**.
- Use your card again (if a card reader is connected and you logged in by card).

i If Copy Control is enabled, the **Logging out** message is displayed until the MFP is in idle state. This is required to allow correct reading of the MFP's copy page counters.

Register card at device

There are two ways the user can register a card while standing at the device:

- To register a card by entering Windows user logon, password, and domain, see [Register card with Windows credentials](#).

- To register a card by entering an 8-digit PUK code, see [Register card with PUK code](#).

Register card with Windows credentials

The user must have a network logon.

1. Use the card reader.
 - If there are any available PUK codes on the system, tap **Cancel** in the **Please enter PUK** dialog. The **Login to register card** dialog appears.
 - If there are no available PUK codes, the user gets the **Login to register card** dialog.
2. Tap **OK** to log in to register card.
3. Tap **Username** and enter **Username** on the touch-screen. Tap **OK**.
4. Tap **Password** and enter **Password** on the touch-screen. Tap **OK**.
5. Tap **Domain** and enter **Domain** on the touch-screen. Tap **OK**.
The solution can be configured to not prompt for the domain.
6. Tap **OK**.
The card is registered and you are logged in.

Register card with PUK code

The PUK code must be supplied to the user in advance, typically through e-mail.

1. Use the card reader.
If the card is unknown and there is an available PUK code in the SafeCom system, the user is prompted to enter his PUK code.
2. Enter **PUK code** on the keypad or touch-screen.
3. Tap **OK**.

Steps 4-7 are relevant only if the device requires login by PIN code (**Login without PIN code** is not checked).

4. Enter **PIN code** on the keypad or touch-screen.
5. Tap **OK**.
6. Enter **PIN again** on the keypad or touch-screen.
7. Tap **OK**.
The card is registered and you are asked to log in again.

HP Scanjet Enterprise 7000n, HP Digital Sender Flow 8500 fn1

Control panel



Login

The login sequence is initiated if you are not already logged in and tap **Sign In** or any icon (**E-mail**, **Fax**, or **Save to Network Folder**) that requires SafeCom to handle the **MFP authentication**.

- To log in with card, see [Login with card](#).
- To log in with card and PIN code, see [Login with card and PIN code](#).
- To log in with ID code, see [Login with ID code](#).
- To log in with ID code and PIN code, see [Login with ID code and PIN code](#).

Login with card


1. Use the card reader.
2. Before 10 seconds have elapsed, tap an icon or tap Sign In.

i If you tap an icon before using the card, a dialog saying Use card then touch OK appears.

Login with card and PIN code

1. Use the card reader.
2. Before 10 seconds have elapsed, tap an icon or tap **Sign In**.

3. Enter **PIN code** on the touch-screen.
4. Tap **OK**.

 If you tap an icon before using the card, a dialog saying **Enter PIN code then use card and touch OK** appears.

Login with ID code

1. Tap any icon or tap **Sign In**.
2. Enter **ID code** on the touch-screen.
3. Tap **OK**.

Login with ID code and PIN code

1. Tap any icon or tap **Sign In**.
2. Enter **ID code** on the touch-screen.
3. Tap **OK**.
4. Enter **PIN code** on the keypad or touch-screen.
5. Tap **OK**.

Register card at device

There are two ways the user can register a card at the device:

- To register a card by entering Windows user logon, password, and domain, see [Register card with Windows credentials](#).
- To register a card by entering an 8-digit PUK code, see [Register card with PUK code](#).

Register card with Windows credentials


The user must have a network logon.

1. Use the card reader.

 If there is an available PUK code in the SafeCom system, the user also has the option to register the card using a PUK code.

If the card is unknown, the SafeCom Card Registration page appears.

2. Select the appropriate domain from the **Domain** menu.

 Domains are added in **SafeCom Administrator** under the **Users** menu.

- The domain dropdown list only refreshes after resubmitting the SafeCom Go settings or restarting the device.


3. Tap the **User name** field and enter the Windows user name using the keypad or touch-screen, then tap **OK**.

4. Tap the **Password** field and enter the Windows password on the keypad or touch-screen, then tap **OK**.
5. Tap **OK**.
The card is now registered and the user is prompted to log in again.
6. Tap **OK** and then **Cancel** before logging in with the card reader again.

Register card with PUK code

The PUK code must be supplied to the user in advance, typically through e-mail.

1. Use the card reader.
If the card is unknown and there is an available PUK code in the SafeCom system, the **SafeCom Card Registration** page appears with the options to register the card using a PUK code or Windows credentials.
2. Tap the **PUK** field and enter the PUK code on the keypad or touch-screen.
3. Tap **OK**.

 Even though the user is required to use a PIN code, it is not necessary when registering a card. Once the card is registered and the user logs in again, the user is required to enter the PIN code.

The card is now registered and you are asked to log in again.

4. Tap **OK** and then **Cancel** before logging in with the card reader again.

Save to Network Folder

1. Tap the **Save to Network Folder** icon.
2. Enter the network folder path and file name, and specify the file type.
3. Press the **Start** button to scan and send the document to folder.

E-mail

1. Tap the **E-mail** icon.
2. For each field, tap the field button and enter the value on the keypad or touch-screen.
3. Press the **Start** button to scan and e-mail the document.

Account

To select a billing code for the job:

1. Tap the **Account** icon and select the billing code from the list of last used or favorites.
2. Tap **Billable**, **Not billable**, or **Personal**.
3. Tap **Home** and select the appropriate function (e-mail, save to network folder, or fax).

Logout

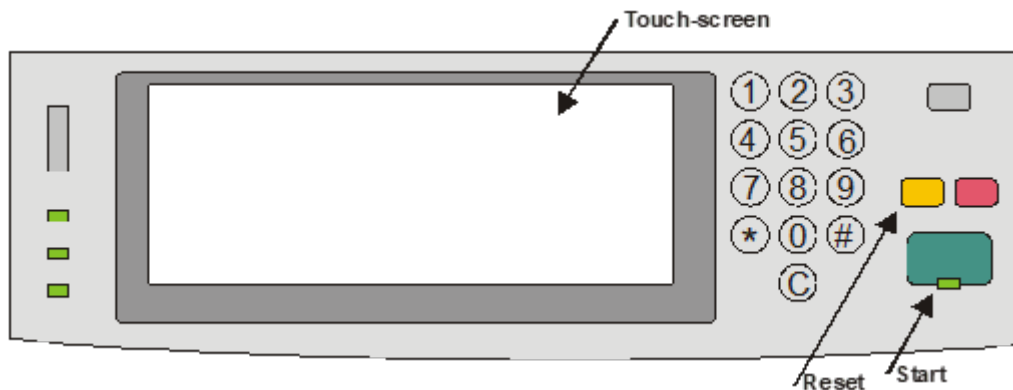
There is a configurable timeout that defaults to 60 seconds. The logout process is initiated if no buttons are tapped for this period.

To logout actively, do any of the following:

- Tap **Sign Out** on the main screen.
- Use your card at the card reader again - if you logged in using a card.

HP 9250C Digital Sender

Control panel



Login

The login sequence is initiated if you are not already logged in and tap any icon (**E-mail**, **Fax**, or **Network Folder**) that requires SafeCom to handle the **MFP authentication**.

The recommended login sequences are described in the following sections.

- To log in with card, see [Login with card](#).
- To log in with card and PIN code, see [Login with card and PIN code](#).
- To log in with ID code, see [Login with ID code](#).
- To log in with ID code and PIN code, see [Login with ID code and PIN code](#).
- To log in with card or ID code, see [Login with ID code and PIN code](#).
- To log in with Windows, see [Login with Windows](#).
- To log in with password, see [Login with password](#).


Login with card

1. Use the card reader.
2. Before 10 seconds have elapsed, tap an icon.

i If you tap an icon before using the card, a dialog saying **Use card then touch OK** will appear.

Login with card and PIN code

1. Use the card reader.
2. Before 10 seconds have elapsed, tap an icon.
3. Enter the **PIN code** on the keypad, touch-screen, or keyboard.
4. Tap **OK**.

 If you tap an icon before using the card, a dialog saying **Enter PIN code then use card and touch OK** will appear.

Login with ID code

1. Tap any icon (or press the **Start** button to copy).
2. Enter **ID code** on the keypad, touch-screen, or keyboard.
3. Tap **OK**.

Login with ID code and PIN code

This login sequence is also recommended if the Login method is Card or ID code.


1. Tap any icon.
2. Enter **ID code** on the keypad or touch-screen.
3. Tap **OK**.
4. Enter **PIN code** on the keypad or touch-screen.
5. Tap **OK**.

For the Card or ID code login method, if you tap an icon before using the card, a dialog saying **Enter ID code OR use card then touch OK** will appear. If you also need to enter PIN code, the dialog will say **Enter ID code OR use card then enter PIN code and touch OK**.


Login with Windows

If Login method is Card or Windows, it is possible to log in by either using your card or entering your Windows login credentials:

1. Tap **Username** and enter **Username** on the touch-screen. Tap **OK**.

 Username cannot be blank.

2. Tap **Password** and enter **Password** on the touch-screen. Tap **OK**.

 Password cannot be blank.

3. Tap **Domain** and enter **Domain** on the touch-screen. Tap **OK**.
The solution can be configured to not prompt for the domain.
4. Tap **OK**.

Login with password

If SafeCom P:Go has been selected as the login method in the Authentication Manager the user is prompted for a password (max 33 characters) and there are two additional steps in the login sequence. Prompting for password can be relevant when using Send to Folder (see [Enable Send to Folder – with password](#)) and Send to E-mail (see [Enable Send to E-mail – with password](#)).

1. Enter **Password** on the touch-screen or keyboard.
2. Tap **OK**.

Folder

Tap the Network Folder icon. Tap Start to scan and send the document to folder. See also in [Enable device memory usage](#).

The SafeCom solution can control access to the MFP's memory usage to store and retrieve jobs from the MFP's storage memory.

1. Open the **Configuration** web page.
2. Check **Save to device memory** in **MFP authentication**.
3. Check **Retrieve from device memory** in **MFP authentication**.
4. Click **Apply**.
5. Enable Send to Folder.

E-mail

Tap the **E-mail** icon. It is selectable whether the fields should be editable. The **To:** field can be pre-filled with the **User e-mail**, **Blank**, or **Default To: address**. The **From:** field can be pre-filled with **User e-mail**, **Device name**, **Blank**, or **Default From: address**. See [Enable Send to E-mail – Pre-filled From: and To: field](#). For each field, tap the field button and enter the value on the keypad or touch-screen. Tap **Start** to scan and e-mail the document.

Account – Select Billing Code

Tap the **Account** icon to select a billing code.

Select the billing code among the available codes. The **Favorites** tab lists the user's favorite billing codes in alphabetical order. The **Last used** tab lists up to 10 of the user's last used billing codes with the last used at the top of the list.

- Tap **Billable** to use the selected billing code.
- Tap **Not billable** to use the selected billing code, but keep it off the invoice to the customer (client). The button is only available if the administrator has recorded the selected billing code as billable.
- Tap **Personal** to return to the home screen without selecting a billing code. When selecting Personal the tracking data will contain "Personal" for code and "Used for personal billing" for description. This is to differentiate it from tracking data without billing at all, for example, from a device without billing license.

- Tap **Info** to see information about the selected billing code, including the unabbreviated description.

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 **Reset** button.
- Tap **Sign Out**.
- Use your card again (if a card reader is connected and you logged in by card).

i If Copy Control is enabled, the **Logging out** message is displayed until the MFP is in idle state. This is required to allow correct reading of the MFP's copy page counters.

Register card at device

There are two ways the user can register a card at the device:

- To register a card by entering Windows user logon, password, and domain, see [Register card with Windows credentials](#).
- To register a card by entering an 8-digit PUK code, see [Register card with PUK code](#).

Register card with Windows credentials

The user must have a network logon.

1. Use the card reader.
 - If there are any available PUK codes on the system, tap **Cancel** in the **Please enter PUK** dialog. The **Login to register card** dialog appears.
 - If there are no available PUK codes, the user gets the **Login to register card** dialog.
2. Tap **OK** to log in to register card.
3. Tap **Username** and enter **Username** on the touch-screen. Tap **OK**.
4. Tap **Password** and enter **Password** on the touch-screen. Tap **OK**.
5. Tap **Domain** and enter **Domain** on the touch-screen. Tap **OK**.
The solution can be configured to not prompt for the domain.
6. Tap **OK**.
The card is registered and you are logged in.

Register card with PUK code

The PUK code must be supplied to the user in advance, typically through e-mail.

1. Use the card reader.
If the card is unknown and there is an available PUK code in the SafeCom system, the user is prompted to enter his PUK code.
2. Enter **PUK code** on the keypad or touch-screen.
3. Tap **OK**.

Steps 4-7 are relevant only if the device requires login by PIN code (**Login without PIN code** is not checked).

4. Enter **PIN code** on the keypad or touch-screen.
5. Tap **OK**.
6. Enter **PIN again** on the keypad or touch-screen.
7. Tap **OK**.

The card is registered and you are asked to log in again.

Change PIN code

If Allow users to change PIN code is checked on the Users tab in the Server properties dialog in SafeCom Administrator, users can change their PIN using the Change PIN menu after login. However, the Change PIN menu is not available when the Document list is open.

1. Log in at the device.
2. Tap the **Administration** icon.
3. Tap **Change PIN**.
4. Tap **PIN code**.
5. Enter **PIN code** on the keypad, touch-screen, or keyboard. Tap **OK**.
6. Tap **PIN again**.
7. Enter **PIN code** on the keypad, touch-screen, or keyboard. Tap **OK**.
8. Tap **Apply**.

HP LaserJet M602, M603, M712



Login

- To log in with a card, see [Login with card](#).
- To log in with ID code, see [Login with ID code](#).

Login with card

Use the card reader.

i Even if a user is set up to use card and PIN code, the PIN code is not required at the device.

Login with ID code

1. Press **OK**.
2. Scroll to **Sign In** and press **OK**.
3. Make sure that SafeCom is selected and press **OK**.
4. Enter ID code on keypad or by pressing **Down** to select a number between numbers 0-9, then press **OK**.
5. Continue entering the code by pressing **Down** and then **OK**.
6. When the code is entered, press **OK** again.

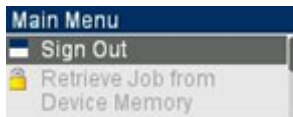
When the login is successful, a welcome message appears on the screen.

Pull Print

All is by default printed at login.

Logout

When the printing is complete, the **Main Menu** changes to the following:



- Click **Sign Out** > **OK** to sign out.

HP LaserJet M855, M806, and M750

Login

- To log in with card, see [Login with card](#).
- To log in with ID code, see [Login with ID code](#).

Login with card

Use the card reader.

i Even if a user is set up to use card and PIN code, the PIN code is not required at the device.

Login with ID code

1. Press **OK**.
2. Scroll to **Sign In** and press **OK**.
3. Make sure that SafeCom is selected and press **OK**.
4. Enter ID code on keypad or by pressing **Down** to select a number between numbers 0-9 and press **OK**.
5. Continue entering the code by pressing **Down** and then **OK**.
6. When the code is entered, press **OK** again.

When the login is successful, a welcome message appears on the screen.

Register card at device

The user can register a card while standing at the device by entering an 8-digit PUK code, which is supplied in advance, typically through email.

1. Use the card reader.
If the card is unknown and there is an available PUK code in the SafeCom system, the user is prompted to enter his PUK code.
2. Enter **PUK code** on the keypad or touch-screen.
3. Tap **OK**.

Steps 4-7 are relevant only if the device requires login by PIN code (**Login without PIN code** is not checked).

4. Enter **PIN code** on the keypad or touch-screen.
5. Tap **OK**.
6. Enter **PIN again** on the keypad or touch-screen.
7. Tap **OK**.

The card is registered and you are asked to log in again.

Pull Print

All is by default printed at login.

Logout

To logout actively, do any of the following:

- Tap **SIGN OUT**.
- Use your card again (if a card reader is connected and you logged in by card).

HP LaserJet CP5525, M551, and M601

Control panel



Login

To log in with card:
Use the card reader.

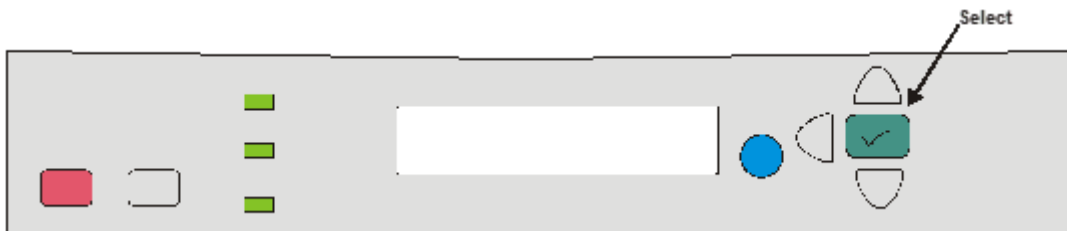
i Even if a user is set up to use card and PIN code, the PIN code is not required at the device.

Pull Print

All is by default printed at login.

HP Color LaserJet 3000, CP3505, and 3800

Control panel



Login

- To log in with card, see [Login with card](#).
- To log in with ID code on SafeCom Keypad, see [Login with ID code on SafeCom Keypad](#).
- To log in with ID code and PIN code on SafeCom Keypad, see [Login with ID code and PIN code on SafeCom Keypad](#).

Login with card

Use the card reader.

Login with ID code on SafeCom Keypad

Enter the ID code on the keypad and press **Enter**.

Login with ID code and PIN code on SafeCom Keypad

1. Enter the ID code on the keypad and press **Enter**.
2. Enter the PIN code on the keypad and press **Enter**.

Pull Print

- Press **Select** ([), scroll to **Print all (x)** and press **Select** ([).
- Press **Select** ([), scroll to **Document list...** and press **Select** ([). To print the listed document (**Doc: {name}**), scroll to **Print job** and press **Select** ([). To select another document, press **Doc: {name}**, and scroll to the document, press **Select** ([), scroll to **Print job**, and press **Select** ([).

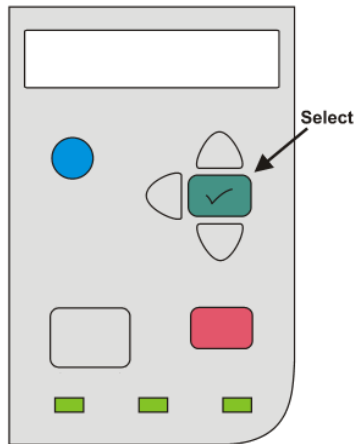
Logout

There is a configurable timeout that defaults to 60 seconds. The logout process is initiated if no buttons are tapped for this period. To actively logout, do any of the following:

- Press **Select** ([), scroll to **Logout**, and press **Select** ([).
- Use your card again (if a card reader is connected and you logged in by card).
- Press **Enter** on the SafeCom Keypad (if a SafeCom keypad is connected).

HP LaserJet P3005

Control panel



Login

To log in with card:
Use the card reader.

Pull Print

- Press **Select** ([]), scroll to **Print all (x)**, and press **Select** ([]).
- Press **Select** ([]), scroll to **Document list...**, and press **Select** ([]). To print the listed document (**Doc: {name}**), scroll to **Print job** and press **Select** ([]). To select another document, press **Doc: {name}**, and scroll to the document, press **Select** ([]), scroll to **Print job**, and press **Select** ([]).

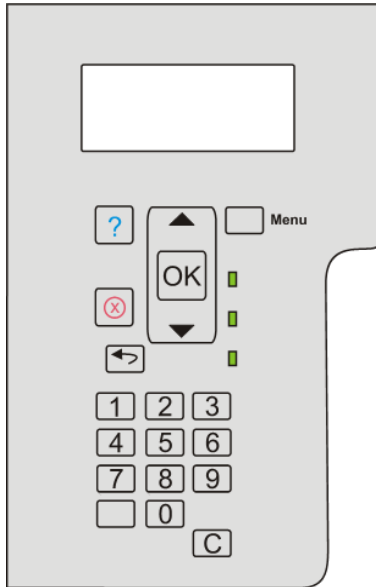
Logout

There is a configurable timeout that defaults to 60 seconds. The logout process is initiated if no buttons are tapped for this period. To actively logout, do any of the following:

- Press **Select** ([]), scroll to **Logout**, and press **Select** ([]).
- Use your card again (if a card reader is connected and you logged in by card).

HP LaserJet P3015

Control panel



Login

- To log in with card, see [Login with card](#).
- To log in with card and PIN code, see [Login with card and PIN code](#).
- To log in with ID code, see [Login with ID code](#).
- To log in with ID code and PIN code, see [Login with ID code and PIN code](#).

Login with card

Use the card reader.

Login with card and PIN code

1. Use the card reader.
2. Scroll to **PIN code**. Press **OK**.
3. Enter PIN code on keypad. Press **OK**.

Login with ID code

1. Press **OK** or **Menu**.
2. Scroll to **ID code**. Press **OK**.
3. Enter ID code on keypad. Press **Down** once, then press **Enter**. Press **OK**.

Login with ID code and PIN code

1. Press **OK** or **Menu**.

2. Scroll to **ID code**. Press **OK**.
3. Enter ID code on keypad. Press **Down** once, then press **Enter**. Press **OK**.
4. Scroll to **PIN code**. Press **OK**.
5. Enter PIN code on keypad. Press **OK**.

Pull Print

- Press **OK** or **Menu**, scroll to **Print all (x)**, and press **OK**.
- Press **OK**, scroll to **Document list...**, and press **OK**. To print the listed document (**Doc: {name}**), scroll to **Print job** and press **OK**. To select another document, press **Doc: {name}**, and scroll to the document, press **OK**, scroll to **Print job**, and press **OK**.

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 actively logout, do any of the following:

- Press **OK**, scroll to **Logout**, and press **OK**.
- Use the card again (if a card reader is connected and you logged in by card).

Register card at device

The user goes to the device to log in by entering an ID code or using a card (if card reader is connected). If the ID code or card is unknown and there is an available PUK code in the SafeCom system, the user is prompted to enter his PUK code. Unless **Login without PIN code** is enabled for the device, the user is also asked to enter a 4-digit PIN code of his choice twice.

HP Color LaserJet CP3525

Control panel



Login

- To log in with card, see [Login with card](#).
- To log in with ID code on SafeCom Keypad, see [Login with ID code on SafeCom Keypad](#).

- To log in with ID code and PIN code on SafeCom Keypad, see [Login with ID code and PIN code on SafeCom Keypad](#).

Login with card

Use the card reader.

Login with ID code on SafeCom Keypad

Enter the ID code on the keypad and press **Enter**.

Login with ID code and PIN code on SafeCom Keypad

1. Enter the ID code on the keypad and press **Enter**.
2. Enter the PIN code on the keypad and press **Enter**.

Pull Print

- Press **OK** or **Menu**, scroll to **Print all (x)**, and press **OK**.
- Press **OK**, scroll to **Document list...**, and press **OK**. To print the listed document (**Doc: {name}**), scroll to **Print job** and press **OK**. To select another document, press **Doc: {name}**, and scroll to the document, press **OK**, scroll to **Print job**, and press **OK**.

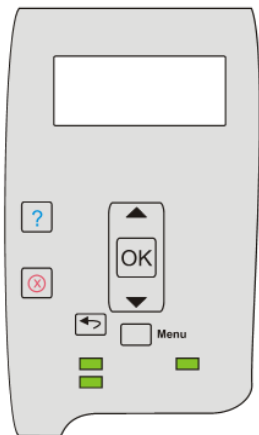
Logout

There is a configurable timeout that defaults to 60 seconds. The logout process is initiated if no buttons are tapped for this period. To actively logout, do any of the following:

- Press **OK**, scroll to **Logout**, and press **OK**.
- Use the card again (if a card reader is connected and you logged in by card).
- Press **Enter** on the SafeCom Keypad (if a SafeCom keypad is connected).

HP LaserJet P4014

Control panel



Login

- To log in with card, see [Login with card](#).
- To log in with ID code on SafeCom Keypad, see [Login with ID code on SafeCom Keypad](#).
- To log in with ID code and PIN code on SafeCom Keypad, see [Login with ID code and PIN code on SafeCom Keypad](#).

Login with card

Use the card reader.

Login with ID code on SafeCom Keypad

Enter the ID code on the keypad and press **Enter**.

Login with ID code and PIN code on SafeCom Keypad

1. Enter the ID code on the keypad and press **Enter**.
2. Enter the PIN code on the keypad and press **Enter**.

Pull Print

- Press **OK** or **Menu**, scroll to **Print all (x)**, and press **OK**.
- Press **OK**, scroll to **Document list...**, and press **OK**. To print the listed document (**Doc: {name}**), scroll to **Print job** and press **OK**. To select another document, press **Doc: {name}** and scroll to the document, press **OK**, scroll to **Print job**, and press **OK**.

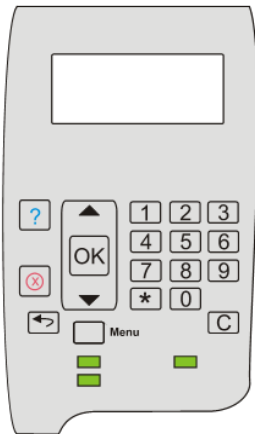
Logout

There is a configurable timeout that defaults to 60 seconds. The logout process is initiated if no buttons are tapped for this period. To actively logout, do any of the following:

- Press **OK**, scroll to **Logout**, and press **OK**.
- Use the card again (if a card reader is connected and you logged in by card).
- Press **Enter** on the SafeCom Keypad (if a SafeCom keypad is connected).

HP LaserJet P4015 and P4515

Control panel



Login

- To log in with card, see [Login with card](#).
- To log in with card and PIN code, see [Login with card and PIN code](#).
- To log in with ID code, see [Login with ID code](#).
- To log in with ID code and PIN code, see [Login with ID code and PIN code](#).

Login with card

Use the card reader.

Login with card and PIN code

1. Use the card reader.
2. Scroll to **PIN code**. Press **OK**.
3. Enter PIN code on keypad. Press **OK**.

Login with ID code

1. Press **OK** or **Menu**.
2. Scroll to **ID code**. Press **OK**.
3. Enter ID code on keypad. Press **Down** once, then press **Enter**. Press **OK**.

Login with ID code and PIN code

1. Press **OK** or **Menu**.
2. Scroll to **ID code**. Press **OK**.
3. Enter ID code on keypad. Press **Down** once, then press **Enter**. Press **OK**.
4. Scroll to **PIN code**. Press **OK**.
5. Enter PIN code on keypad. Press **OK**.

Pull Print

- Press **OK** or **Menu**, scroll to **Print all (x)**, and press **OK**.
- Press **OK**, scroll to **Document list...**, and press **OK**. To print the listed document (**Doc: {name}**), scroll to **Print job** and press **OK**. To select another document, press **Doc: {name}** and scroll to the document, press **OK**, scroll to **Print job**, and press **OK**.

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 actively logout, do any of the following:

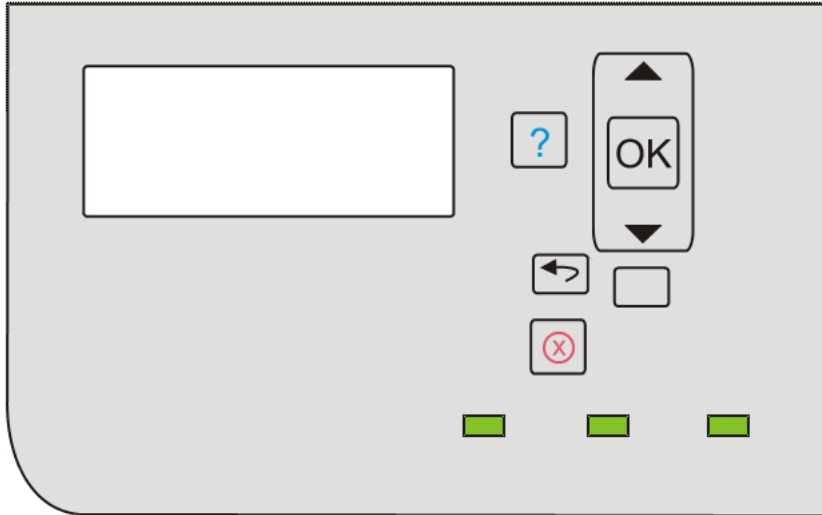
- Press **OK**, scroll to **Logout**, and press **OK**.
- Use the card again (if a card reader is connected and you logged in by card).

Register card at device

The user goes to the device to log in by entering an ID code or using a card (if card reader is connected). If the ID code or card is unknown and there is an available PUK code in the SafeCom system, the user is prompted to enter his PUK code. Unless **Login without PIN code** is enabled for the device, the user is also asked to enter a 4-digit PIN code of his choice twice.

HP Color LaserJet CP4525

Control panel



Login

- To log in with card, see [Login with card](#).
- To log in with ID code on SafeCom Keypad, see [Login with ID code on SafeCom Keypad](#).
- To log in with ID code and PIN code on SafeCom Keypad, see [Login with ID code and PIN code on SafeCom Keypad](#).

Login with card

Use the card reader.

Login with ID code on SafeCom Keypad

Enter the ID code on the keypad and press **Enter**.

Login with ID code and PIN code on SafeCom Keypad

1. Enter the ID code on the keypad and press **Enter**.
2. Enter the PIN code on the keypad and press **Enter**.

Pull Print

- Press **OK** or **Menu**, scroll to **Print all (x)**, and press **OK**.

- Press **OK**, scroll to **Document list....** and press **OK**. To print the listed document (**Doc: {name}**), scroll to **Print job** and press **OK**. To select another document, press **Doc: {name}** and scroll to the document, press **OK**, scroll to **Print job**, and press **OK**.

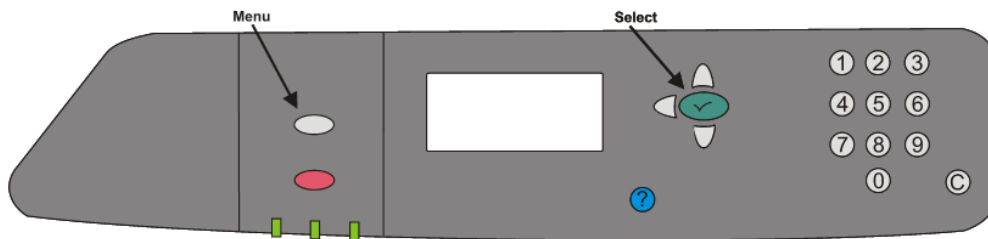
Logout

There is a configurable timeout that defaults to 60 seconds. The logout process is initiated if no buttons are tapped for this period. To actively logout, do any of the following:

- Press **OK**, scroll to **Logout**, and press **OK**.
- Use the card again (if a card reader is connected and you logged in by card).
- Press **Enter** on the SafeCom Keypad (if a SafeCom keypad is connected).

HP Color LaserJet CP6015

Control panel



Login

- To log in with card, see [Login with card](#).
- To log in with card and PIN code, see [Login with card and PIN code](#).
- To log in with ID code, see [Login with ID code](#).
- To log in with ID code and PIN code, see [Login with ID code and PIN code](#).

Login with card

Use the card reader.

Login with card and PIN code

1. Use the card reader.
2. Scroll to **PIN code**. Press **Select ([)**.
3. Enter PIN code on keypad. Press **Select ([)**.

Login with ID code

1. Press **Select ([)**.

2. Scroll to **ID code**. Press **Select** ([]).
3. Enter ID code on keypad. Press **Down** once, then press **Enter**. Press **Select** ([]).

Login with ID code and PIN code

1. Press **Select** ([]).
2. Scroll to **ID code**. Press **Select** ([]).
3. Enter ID code on keypad. Press **Down** once, then press **Enter**. Press **Select** ([]).
4. Scroll to **PIN code**. Press **Select** ([]).
5. Enter PIN code on keypad. Press **Select** ([]).

Pull Print

- Press **Select** ([]), scroll to **Print all (x)**, and press **Select** ([]).
- Press **Select** ([]), scroll to **Document list...**, and press **Select** ([]). To print the listed document (**Doc: {name}**), scroll to **Print job** and press **Select** ([]). To select another document, press **Doc: {name}** and scroll to the document, press **Select** ([]), scroll to **Print job**, and press **Select** ([]).

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, do any of the following:

- Press **Select** ([]), scroll to **Logout**, and press **Select** ([]).
- Use the card again (if a card reader is connected and you logged in by card).

Register card at device

The user goes to the device to log in by entering an ID code or using a card (if card reader is connected). If the ID code or card is unknown and there is an available PUK code in the SafeCom system, the user is prompted to enter his PUK code. Unless **Login without PIN code** is enabled for the device, the user is also asked to enter a 4-digit PIN code of his choice twice.

HP MFP SXXXdn series

This section contains information about the following devices:

- HP Color MFP S970dn
- HP Color MFP S962dn
- HP Color MFP S951dn
- HP MFP S956dn

Login

The different login sequences are described in the following sections. The Welcome screen is by default enabled, but if it is disabled, the user is guided directly to the login sequence.

- To log in with card, see [Login with card](#).

- To log in with card and PIN code, see [Login with card and PIN code](#).
- To log in with ID code, see [Login with ID code](#).
- To log in with ID code and PIN code, see [Login with ID code and PIN code](#).
- To log in with Windows, see [Login with Windows](#).

Login with card

1. Tap the **Login** icon.
2. Use the card reader.

Login with card and PIN code

1. Tap the **Login** icon.
2. Use the card reader.
3. Enter **PIN code** using the touch-screen or keypad.
4. Tap **OK**.

Login with ID code


1. Tap the **Login** icon.
2. Enter the **ID code** using the touch-screen or keypad.
3. Tap **OK**.

Login with ID code and PIN code


1. Tap the **Login** icon.
2. Enter the **ID code** using the touch-screen or keypad.
3. Tap **OK**.
4. Enter **PIN code** on the touch-screen.
5. Tap **OK**.

Login with Windows

1. Tap the **Windows login** icon.
2. Tap **Username** and enter **Username** on the touch-screen. Tap **OK**.

 Username cannot be blank.

3. Tap **Password** and enter **Password** on the touch-screen. Tap **OK**.

 Password cannot be blank.

4. If domain is required, tap the **Domain** dropdown list and select domain.
5. Tap **OK**.

Main menu

Once logged in you can select an option from the touch-screen.

- Tap **Pull Print** to print individual documents.
- Tap **Copy** to start copying.
- Tap **Account** to select billing code.
- Tap **Logout** to log out.

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 preceding **R** shows the document is retained. A delegated document will have a preceding **D**. Tap the **Info** button to see information about who delegated the document. A group print document will have a preceding **G**.

- Tap **Print All** to print all documents, excluding any retained documents. Documents are printed in chronological order (newest first).
- Tap **Print** to print the selected documents.
- Tap **Retain** if you want the selected documents to remain on the list (server) after they have been printed.
- Tap **Delete** to delete the selected documents.
- Tap **Info** to see information about the selected documents, including cost, driver name, use of color and duplex.
- Tap **Back** to return to the main screen.
- Tap **Copies** to request multiple copies of a document. **Print All** will always be one copy of each document.

Copy

1. Tap **Copy / Scan** in the login screen to start copy or scan.
2. Press the **COPY** button on the MFP to bring it into copy mode.
3. Press the **Start** button to copy the documents placed in the automatic document feeder (ADF).
On some MFPs there are two **Start** buttons - one for black/white copies and one for color copies.

Account – Select billing code

1. Tap the **Account** icon to select a billing code.
2. Tap **Favorites** to select from the list of the user's favorite billing codes.
They are listed in alphabetical order.
3. Tap **Last used** to select from the list of up to 10 of the user's last used billing codes.
The last used code is at the top of the list.

4. Continue by selecting one of the following options:
 - Tap **Billable** to use the selected billing code.
 - Tap **Not billable** to use the selected billing code, but keep it off the invoice to the customer (client). The button is only available if the administrator has recorded the selected billing code as billable.
 - Tap **Personal** to return to the home screen without selecting a billing code. When selecting Personal the tracking data will contain "Personal" for code and "Used for personal billing" for description. This is to differentiate it from tracking data without billing at all, for example, from a device without billing license.
 - Tap **Info** to see information about the selected billing code, including the unabbreviated description.
5. Finish the job at the device.

i Whether the user has the options to work with billing codes when printing depends on how the **User properties** and the **Device Properties** are set up in **SafeCom Administrator**. The user must have **Bill clients for cost** checked on the **Settings** tab, and on the **Device properties** must have **Client Billing** checked on the **License** tab. If client billing is set up correctly in the user properties, but not in the **Device properties**, the client billing user is able to select the **Account** icon on the device, but there will be no billing codes to work with.

Register card with PUK code

The user logs in by entering an ID code or using a card. If the ID code or card is unknown and there is an available PUK code in the SafeCom system, the user is prompted to enter his PUK code.

- To enter PUK code, see [Enter PUK code](#).
- To enter PUK code and PIN code, see [Enter PUK code and PIN code](#).

Enter PUK code

1. Tap **PUK code**.
2. Enter **PUK code** on the touch-screen. Tap **OK**.
3. Tap **OK**.

Enter PUK code and PIN code

1. Tap **PUK code**.
2. Enter **PUK code** on the touch-screen. Tap **OK**.
3. Tap **PIN code**.
4. Enter **PIN code** on the touch-screen. Tap **OK**.
5. Tap **OK**.

Logout

There is a configurable timeout that defaults to 30 seconds. The logout process is initiated if no buttons are tapped for this period.

To logout actively:

Tap **Log out** on the main screen.

HP OfficeJet Pro series

This section contains information about the following devices:

- HP OfficeJet Pro 276dw MFP
- HP OfficeJet Pro X476dw MFP
- HP OfficeJet Pro X576dw MFP
- HP OfficeJet Pro 251dw
- HP OfficeJet Pro X551dw

 The S82 060.090*06 version of the Device Server does not support HP Pro devices.

Login

The different login sequences are described in the following sections.

- To log in with card, see [Login with card](#).
- To log in with ID code, see [Login with ID code](#).

Login with card

1. Tap **Login**.
2. Use the card reader.

Login with ID code

1. Tap **Login**.
2. Enter the **ID code** using the touch-screen or keypad.
3. Tap **OK**.

Main menu

Once logged in you can select an option from the touch-screen.

- Tap **Copy** to start copying.
- Tap **Fax** to start faxing.
- Tap **Scan** to start scanning.
- Tap **Apps** to access the **Pull Print** menu.

Pull Print – Document list

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

1. Tap **Apps**.

2. Tap **Pull Print**.

3. Tap **Menu**.

Documents appear in chronological order with the newest at the top of the list.

The preceding **R** shows the document is retained. A delegated document will have a preceding **D**. Tap the **Info** button to see information about who delegated the document. A group print document will have a preceding **G**.

- Tap **Print All** to print all documents, excluding any retained documents. Documents are printed in chronological order (newest first).
- Tap **Print** to print the selected documents.
- Tap **Retain** if you want the selected documents to remain on the list (server) after they have been printed.
- Tap **Delete** to delete the selected documents.
- Tap **Info** to see information about the selected documents, including cost, driver name, use of color and duplex.
- Tap **Back** to return to the main screen.
- Tap **Copies** to request multiple copies of a document. **Print All** will always be one copy of each document.

Copy

1. Tap **Copy** in the login screen to start copying.
2. Press the **Start** button to copy the documents placed in the automatic document feeder (ADF).

Logout

There is a configurable timeout that defaults to 30 seconds. The logout process is initiated if no buttons are tapped for this period.

Chapter 5

Automatic installation through HP Web Jetadmin

This chapter describes how to use HP Web Jetadmin version 10.2 or higher to perform an automatic installation of SafeCom Go HP.

For further information on HP Web Jetadmin, please refer to HP documentation.

1. Check that the requirements are met.
2. Get the SafeCom Go HP software for **HP Web Jetadmin**.
3. Start **HP Web Jetadmin**.
4. Add relevant firmware.
5. Import files to solutions repository.
6. Create solution templates.
7. Create groups to automate installation.
8. Find devices through discovery.
9. Register device.
10. Uninstall SafeCom Go HP.
11. Configuration files.

Pre-requisites

- HP Web Jetadmin 10.2 or higher supplied by HP.
- HP firmware must support OXPd:SolutionInstaller. In general, this means that the HP firmware must be released after August 2009.
- SafeCom Go HP version S89 nnn.030*42 / S49 nnn.020*18 or higher. For FutureSmart device SafeCom Go HP S95 nnn.050*08 or higher.
- SafeCom provided policy files (manifest_nnn.xml) and image files (nnnxxx-ilc.jar) must exist for the HP device. [SafeCom Go HP policy and image files for MFPs](#), [SafeCom Go HP policy and image files for scanners](#), and [SafeCom P:Go HP policy and image files for printers](#) list the policy and image files required for the various HP devices.
- A running web server (for example, ISS) with a subfolder hosting the application and configuration files. For example, C:\Inetpub\wwwroot\safecom_go_hp. Samples of the configuration files are available in [Sample configuration files](#).
- SafeCom GoBuild. This includes sample xml-files that give you an idea of how to create configuration files.

- Any SafeCom Go HP software previously installed on the device through SafeCom Administrator must be completely removed prior to installation through HP Web Jetadmin. Remove the files by doing a DISK INIT or using the Package Loader to remove: SafeCom Go, SafeCom Go Loader, and SafeCom Go Library.

Download SafeCom Go HP software

Installation through **HP Web Jetadmin** requires access to and use of special SafeCom Go HP policy files (manifest_nnn.xml) and image files (nnnxxx-ilc.jar).

The files can be downloaded, see [Get the SafeCom Go HP software](#). Normally, the destination folder is C:\Program Files\SafeCom\SafeComG4\device_software.

The files are located in the subfolder: \hp_web_jetadmin.

As HP Web Jetadmin needs to reference the image files (nnnxxx-ilc.jar) through a URL, these files must be copied to a web server, for example, the web server hosting HP Web Jetadmin or the SafeCom G4 Web Interface.

On the web server, create the \safecom_go_hp subfolder.

Example:

C:\InetPub\wwwroot\safecom_go_hp

 The tables below list the policy and image files required for the various HP devices.

SafeCom Go HP policy and image files for MFPs

HP MFP	Policy file	Image file
HP LaserJet 525 MFP	manifest_fs.xml	310xxx.b95
HP Color LaserJet 575 MFP	manifest_fs.xml	310xxx.b95
HP LaserJet MFP M725	manifest_fs.xml	310xxx.b95
HP LaserJet Color MFP M775	manifest_fs.xml	310xxx.b95
HP LaserJet MFP M830	manifest_fs.xml	310xxx.b95
HP Color LaserJet MFP M880	manifest_fs.xml	310xxx.b95
HP Color LaserJet CM4540 MFP	manifest_fs.xml	310xxx.b95
HP LaserJet M4555 MFP	manifest_fs.xml	310xxx.b95
HP LaserJet M3035 MFP	manifest_110.xml	110xxx-ilc.jar
HP Color LaserJet CM3530 MFP	manifest_140.xml	140xxx-ilc.jar
HP Color LaserJet CM4730 MFP	manifest_110.xml	110xxx-ilc.jar
HP LaserJet M5035 MFP	manifest_110.xml	110xxx-ilc.jar
HP LaserJet M5039 MFP	manifest_110.xml	110xxx-ilc.jar

HP MFP	Policy file	Image file
HP Color LaserJet CM6030 MFP	manifest_132.xml	132xxx-ilc.jar
HP Color LaserJet CM6040 MFP	manifest_132.xml	132xxx-ilc.jar
HP Color LaserJet CM6049 MFP	manifest_132.xml	132xxx-ilc.jar
HP Color LaserJet CM6040 MFP	manifest_132.xml	132xxx-ilc.jar
HP Color LaserJet CM6040 MFP	manifest_132.xml	132xxx-ilc.jar
HP LaserJet M9059 MFP	manifest_110.xml	110xxx-ilc.jar

SafeCom Go HP policy and image files for scanners

HP Scanner	Policy file	Image file
ScanJet Enterprise 7000n	manifest_fs.xml	320xxx.b95
Digital Sender Flow 8500 fn1/ Scanjet Enterprise 8500 fn1	manifest_fs.xml	310xxx.b95
HP 9250C Digital Sender	manifest_110.xml	110xxx-ilc.jar


SafeCom P:Go HP policy and image files for printers

HP printer	Policy file	Image file
HP LaserJet 500 Color M551	manifest_fs.xml	310xxx.b95
HP LaserJet 600 M601	manifest_fs.xml	310xxx.b95
HP LaserJet 600 M602	manifest_fs.xml	310xxx.b95
HP LaserJet 600 M603	manifest_fs.xml	310xxx.b95
HP LaserJet 700 M712	manifest_fs.xml	310xxx.b95
HP LaserJet M750	manifest_fs.xml	310xxx.b95
HP LaserJet M806	manifest_fs.xml	310xxx.b95
HP Color LaserJet M855	manifest_fs.xml	310xxx.b95
HP Color LaserJet CP5525	manifest_fs.xml	310xxx.b95
HP LaserJet P3005	manifest_111.xml	111xxx-ilc.jar
HP LaserJet P3015	manifest_150.xml	150xxx-ilc.jar
HP Color LaserJet CP3505	manifest_121.xml	121xxx-ilc.jar
HP Color LaserJet CP3525	manifest_141.xml	141xxx-ilc.jar
HP LaserJet P4014	manifest_130.xml	130xxx-ilc.jar
HP LaserJet P4015	manifest_130.xml	130xxx-ilc.jar
HP LaserJet P4515	manifest_130.xml	130xxx-ilc.jar
HP Color LaserJet P4525	manifest_151.xml	151xxx-ilc.jar
HP Color LaserJet CP6015	manifest_131.xml	131xxx-ilc.jar

Start HP Web Jetadmin

1. Start a web browser and enter the IP address of the computer hosting **HP Web Jetadmin** followed by :8000.

Example: http://172.16.7.42:8000

 JavaScript (Active Scripting) must be enabled.

2. Click **Start HP Web Jetadmin**.
3. Enter **User name** and **Password**.
4. Click **OK**.

Add relevant firmware

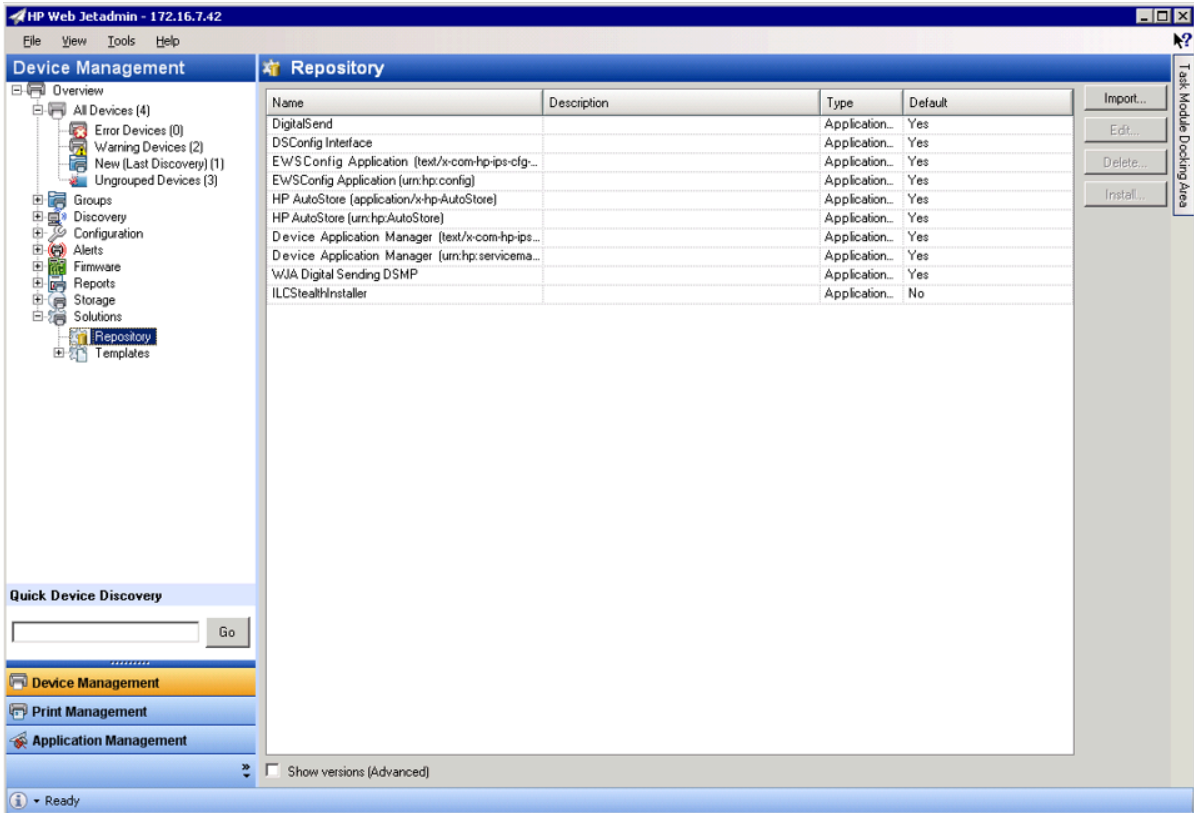
Follow these steps to add all relevant firmware to the firmware repository in HP Web Jetadmin.

1. Start **HP Web Jetadmin**.
2. In the **Device Management** pane, click **Overview > Firmware > Repository**.
3. Click **Get images** and select the relevant printer models from the list.
4. In the pop up dialog, click **OK** to allow for web access.
5. Select the needed images and click **Next**.
6. Select destination folder and click **Next**.
7. Confirm the chosen images and click **Get images**.

Import files to solutions repository

The SafeCom policy and image files must be imported to the solutions repository in HP Web Jetadmin.

1. Start HP Web Jetadmin.
2. In the **Device Management** pane, click **Solutions** and then **Repository**.



3. Click **Import**.
4. Browse to the policy file (manifest-*nnn.xml*) that matches the device.
Example: The manifest_110.xml file matches HP LaserJet M3035 MFP.

i SafeCom Go HP policy and image files for MFPs and SafeCom P:Go HP policy and image files for printers list the policy and image files required for the various HP devices.

5. When all relevant files have been selected for import, click **Import**.

Create solution templates

Two templates must be configured in HP Web Jetadmin in order to handle the automatic installation of the SafeCom solution.

The first template is required for non-FutureSmart devices only and will install OXPd:solutioninstaller. See [First template](#).

The second template is required for all devices and will install the SafeCom Go solution. See [Second template](#).

First template

1. In the **Device Management** menu, click **Overview**, **Solutions**, and then **Templates** in the menu to the left.
2. Click the **Create** button in the upper-right corner and the **Create Solution Template** opens.
3. Check **Install** and click **Next**.
4. In the **Select Solution** dialog, check **Install managers if necessary**.
5. Select ILCStealthUpdater (OXPd:solutioninstaller) and click **Next**.
6. Enter a name for the template (for example, install OXPd) and click **Next**.
7. Click **Create template**.

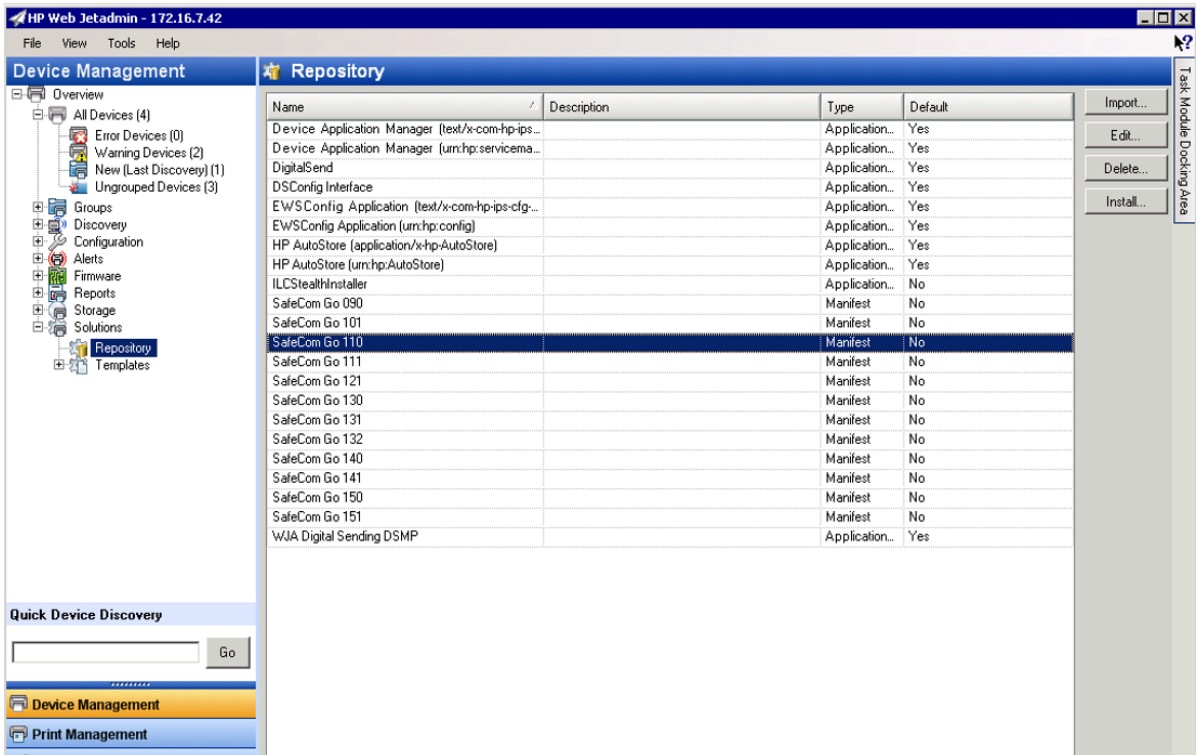
Second template

1. Start **HP Web Jetadmin**.
2. In the **Device Management** menu, click **Overview** > **Solutions** > **Templates** in the menu to the left.
3. Click the **Create** button in the upper-right corner and the **Create Solution Template** opens.
4. Under **Operations**, select **Install** to create an install template. Click **Next**.
5. In the **Select Solution** dialog, check **Install managers if necessary**.
6. Select the appropriate file to install and click **Next**.
 - **SafeCom Go** must be selected for FutureSmart devices like HP Color LaserJet CM4540 MFP.
 - **SafeCom Go {nnn}** must be selected for non-FutureSmart devices. The {nnn} must match the model as listed in the tables in [Download SafeCom Go HP software](#). For example, 110 for an HP LaserJet M3035 MFP.
7. Enter a name (for example, SafeCom solution install) for the template and click **Next**.
8. Click **Create template**.

Edit solution settings

When the templates have been created, they need to be configured with information on the SafeCom application and configuration files.

1. Select an entry in the **Repository** pane. Click **Edit**.



- In **Application URL**, enter the **URL** of the image file.
Example: One example is that 31005008.b95 matches SafeCom Go HP version S95 310.050*08 for a FutureSmart device like HP Color LaserJet CM4540 MFP.
 Another example is that 11005003-ilc.jar matches SafeCom Go HP version S89 110.050*03 for HP LaserJet M3035 MFP.
- If access to the web server requires credentials, enter **User name** and **Password**. Enter an optional **Description**.
- In **Configuration URL**, you must reference a configuration file. The **License URL** (scroll to the bottom of the **Edit Solution Settings** dialog) is not used by SafeCom Go HP and should be left blank.
- Click **OK**.

Create groups to automate installation

To automate the installation of SafeCom on HP devices, a set of groups must be created in HP Web Jetadmin to handle the configuration of the devices.

The setup of groups and configurations are numerous in HP Web Jetadmin, so the following is merely a suggestion to the setup of an automatic installation of SafeCom.

In the following, HP Web Jetadmin is set up to accommodate a simple scenario:

A company has both SPFs and MFPs in their printer fleet, and depending on the type the devices must be configured differently.

The groups required for this scenario are as follows:

Groups	
MFP	FW Upgrade
	OXPd Install
	SafeCom Solution Install
	Completed
Printer	FW Upgrade
	OXPd Install
	SafeCom Solution Install
	Completed

i If, for example, a company operates across many locations that has different network configurations and/or different SafeCom servers, it is beneficial to create groups that sort the devices according to location before sorting them as MFPs or Printers.

Set up groups

Create the groups MFP and Printer to lead the devices though to the subgroups containing the correct upgrade and install files for the respective types. Once new devices are found, for example, through broadcasting or device discovery, they run through the subgroups according to the filters and policies defined.

Create two groups named MFP and Printer to sort the devices between MFPs and printers:

1. Open a browser and start HP Web Jetadmin.
2. In the menu, click **Overview > Groups**.
3. Click the **New group** button.
The **Create Group** dialog opens.
4. Enter "MFP" as the **Group name**.
5. Under **Group membership type**, select **Automatic group**.
6. Click **Next**.

Specify the filter criteria for the automatic grouping:

7. In the **Specify filter criteria** dialog, click **Add** to specify the filter.
8. Specify the following filters:
 - **Device Property:** Device model
 - **NOT:** Leave blank (for the Printer group, enter "Not" in this field)
 - **Function:** Contains
 - **Value:** MFP
9. Click **Next** but there is no need to add a group filter.

10. Click **Next**.
11. Confirm and then click **Save Group**.
12. Go through steps 1-11 again to create the group **Printer**.

Set up subgroups

For each group (MFP and Printer), create four subgroups with the following specifications:

i To create a subgroup, right-click the parent group and then select **New group**. The process of setting up a subgroup is identical to how the two groups MFP and Printer were set up in [Set up groups](#).

Group 1 - Firmware Upgrade:

The first group upgrades new devices to the firmware version specified in the **Value** field. Once the device has been upgraded, it moves on to **Group 2**.

	Field	Value
General	Name	FW Upgrade
	Parent group	MFP or Printer
Filter criteria	Device Property	Device Firmware Version
	Filter Function	Less Than
	Value	For example, 53.080.5
	Options	Ignore Case
Group policy	Policy	Upgrade printer firmware
	Trigger	Upgrade to qualified version
	Policy action	Upgrade to latest version (this is the latest version of printer firmware imported to the Firmware Repository)

Group 2 - OXPd Install:

The second group installs the SafeCom image file on the device. Note that two filter criteria must to be set up for this group.

	Field	Value
General	Name	OXPd Install
	Parent group	MFP or Printer
Filter criteria1	Device Property	Device Firmware Version
	Filter Function	Equal
	Value	53.080.5
	Options	Ignore Case

	Field	Value
Filter criteria2	Device Property	Solution manager installed
	Filter Function	Equal
	Value	No
	Options	Ignore Case
Group policy	Policy	Manage Device Solutions
	Trigger	Devices added to group
	Policy action	Install OXPd (name of the template created in First template)

Group 3 - SafeCom Solution Install:

The third group installs the SafeCom manifest file on the device.

	Field	Value
General	Name	SafeCom Solution Install
	Parent group	MFP or Printer
Filter criteria	Device Property	Solution manager installed
	Filter Function	Equal
	Value	Yes
	Options	Ignore Case
Group policy	Policy	Manage Device Solutions
	Trigger	Devices added to group
	Policy action	SafeCom solution install (name of the template created in Second template)

i Here the filter criteria **Device Property** is set to **Solution manager installed**. However, that only works if there are no other solution managers installed on the device. If you have other solution managers installed on your device, you must change the filter criteria to determine whether or not the SafeCom solution is installed in your setup.

Group 4 - Completed:

The fourth group stores the devices that have completed the install.

	Field	Value
General	Name	Completed
	Parent group	MFP or Printer
Filter criteria	Device Property	Solutions
	Filter Function	Contains

	Field	Value
	Value	1

i Here the filter criteria **Device Property** is set to **Solutions** and the **Value** is set to **1**. However, this only works if there are no other solutions installed on the device. If you have other solution managers installed on your device, you must change the filter criteria in a way that determines whether or not the SafeCom solution is installed in your set up. For example, the **Value** can be changed to **2** if there is, apart from SafeCom, one other solution installed.

Find devices through discovery

If you do not already have a list of devices from previous use the **Device Discovery** function available on the **Tools** menu to open the Configuration Wizard and begin the discovery process, perhaps by broadcasting. It is also possible to set up the discovery process to run automatically. Click **Overview**, **Discovery** and then **Templates** to set up such a discovery templates. Refer to HP documentation for further information.

Register device

All devices must be registered after SafeCom is installed.

There are three ways in which a device can be registered on the SafeCom server after the installation:

1. A person with TECH/ADMIN rights has to authenticate on each device.
2. Add the devices to the server through the SafeCom Administrator.
3. Register the devices through the web page. Note that this option is not available for all HP devices.

Uninstall SafeCom Go HP

1. In the **Device Management** pane (left pane), click **All Devices** or **Groups**.
2. In the **Devices** pane (top center pane), click a device.
3. In the bottom center pane, click the **Solutions** tab.
4. In the **Solutions** pane, click a device and click **Remove...**
5. In the **Select options** dialog, check **Specify Solution** and click **Next**.
6. Click the Manifests and Applications to remove. Click **Next**.
The **Confirm** dialog appears.
7. Click **Uninstall**.
The **Progress** dialog appears.
8. Click **Done** when the **Results** dialog reports success.

Sample configuration files

For hp_xml_config.txt, see [hp_xml_config.txt](#).

For hp_ds_xml_config.txt, see [hp_ds_xml_config.txt](#).

hp_xml_config.txt

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<CONFIGURATION>
  <SERVERS>
    <SERVER>
      <IP_ADDRESS></IP_ADDRESS>
      <IP_PORT>7500</IP_PORT>
    </SERVER>
  </SERVERS>
</CONFIGURATION>
```

The <IP_ADDRESS> tag corresponds to the **SafeCom server IP address** field in the **SafeCom Server** section on the **Configuration** web page. The <IP_PORT> tag corresponds to the **TCP port** field in the **SafeCom Server** section on the **Configuration** web page.

For additional information about the syntax of the SafeCom Go HP configuration.xml file, please refer to chapter 6 in *SafeCom Tech Note SafeComGoBuild*.

The entire configuration can be uploaded using the **SafeCom Device Utility** as described in the *SafeCom G4 Administrator's Manual*.

For FutureSmart devices there are additional XML tags of interest, namely <EWS_PASSWORD> which matched the **Administrator password** field on the SafeCom Go Configuration web page. When the configuration is uploaded the <EWS_PASSWORD> will contain the password encrypted. To set the password the XML tag <EWS_PASSWORD_RAW> should be used. To set the password to nimda, for example you would have the configuration file contain the line:

```
<EWS_PASSWORD_RAW>nimda</EWS_PASSWORD_RAW>
```

On FutureSmart devices, you can also set the UDP response timeout and the priority order of the connection properties for the Print Engine through the <UDP_TIMEOUT> and <NAME_RESOLUTION_RULE> tags, respectively, for example:

```
<NET>
  <NAME_RESOLUTION_RULE>HN,FQDN,IP</NAME_RESOLUTION_RULE>
  <UDP_TIMEOUT>1500</UDP_TIMEOUT>
</NET>
```

For example, in environments where DNS resolution is unreliable, adding a <NAME_RESOLUTION_RULE>IP</NAME_RESOLUTION_RULE> tag can be used to restrict the connection to IP addresses only.

On FutureSmart devices, you can set whether print settings can be changed through the <ALLOW_CHANGING_PRINT_SETTINGS> tag:

```
<ALLOW_CHANGING_PRINT_SETTINGS>Enable</ALLOW_CHANGING_PRINT_SETTINGS>
```

hp_ds_xml_config.txt

The below configuration applies to FutureSmart device that are run through the SafeCom Device Server.

```
<?xml version="1.0" encoding="UTF-8" ?>
<CONFIGURATION>
  <SOCKET_TIMEOUT>4000</SOCKET_TIMEOUT>
  <LOGOUT_TIME>30</LOGOUT_TIME>
  <LANGUAGE>en</LANGUAGE>
  <GET_SNMP_COMMUNITY_NAME>public</GET_SNMP_COMMUNITY_NAME>
  <ADMIN_PASSWORD/>

  <AUTHENTICATE>
    <PULLPRINT>true</PULLPRINT>
    <ACCOUNT>true</ACCOUNT>
    <COPY>true</COPY>
    <COLORCOPY>true</COLORCOPY>
    <EMAIL>true</EMAIL>
    <FOLDER>true</FOLDER>
    <FAX>true</FAX>
  </AUTHENTICATE>

  <LOG>
    <ENABLED>true</ENABLED>
    <LEVEL>6</LEVEL>
    <MAX_FILE_SIZE>1048576</MAX_FILE_SIZE>
  </LOG>

  <SERVERS>
    <SERVER>
      <SERVER_IP>172.16.6.94</SERVER_IP>
      <SERVER_PORT>50002</SERVER_PORT>
    </SERVER>
  </SERVERS>

  <NET>
    <NAME_RESOLUTION_RULE>HN,FQDN,IP</NAME_RESOLUTION_RULE>
    <UDP_TIMEOUT>1500</UDP_TIMEOUT>
  </NET>
</CONFIGURATION>
```

i The password is mandatory and only one server can be listed.

Chapter 6

Troubleshooting

This chapter contains troubleshooting hints for the SafeCom Go HP product. Additional troubleshooting hints are available in the Troubleshooting chapter in the *SafeCom G4 Administrator's Manual*.

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.

SafeCom Go HP software installation troubleshooting

If you experience problems installing the SafeCom Go HP on the device using **SafeCom Administrator**, you should check the following:

- Check that the printer has the required level of HP firmware. Older HP firmware may not allow enough resources for SafeCom Go HP to function properly. The latest firmware can be downloaded from www.hp.com.
- If the printer appears in **SafeCom Administrator** with the MAC address **11badadd111**, it is because SafeCom Go HP was unable to obtain the printer's correct MAC address. Delete the

device in **SafeCom Administrator** and check the **SNMP Settings** on the HP EWS and register the printer again.

- If no SafeCom Go menus (icons) appear in the printer's control panel after the printer has been restarted (and you have waited 10 minutes), it could be because the SafeCom Go HP Flash Memory Card is in the slot marked FIRMWARE SLOT or SYSTEM CODE. Please move the SafeCom Go HP Flash Memory Card to another available slot and install the SafeCom Go HP software again.
- If "Error authorizing!" is reported when sending the SafeCom Go HP Loader (*.b49) to the printer, it is because the printer is not connected to the network.
- If "Authorization failed. Access denied!" is reported when sending the SafeCom Go HP Loader (*.b49) to the printer, it is because either no password is set or the password is wrong.
- If "Download Failed. Login Error" is reported, it is because the specified username and password is wrong. The username **MUST** be admin (all lower case) and the password must be specified in the right case.
- If "Loading failed!" is reported when sending the SafeCom Go HP Software (*.b89) to an HP Color LaserJet 4650 or 5550 without hard disk, SafeCom Administrator may report "Loading failed!". Just ignore this, wait a minute and refresh the status in SafeCom Administrator. If SafeCom Administrator continues to report "Awaiting code", restart the printer and try again.
- If "Authorization failed. Bad response!" is reported when sending the SafeCom Go HP Loader (*.b49) to the printer, it is most likely because encryption is enabled for all web communication. Please uncheck **Encrypt All Web Communication** on the printer. Alternatively, it might be because the printer's Embedded Web Server is not responding. Try to power the printer off and on.
- Verify that the printer's configuration page says that **Write Protect** is **Disabled** for the disk and the SafeCom Go HP card slot and **File System Access** is **Enabled** for **PJL**. These settings are controlled through **HP Web Jetadmin** (Configuration category: File System).
- Ensure that the **Service Loading** option is checked in the **Options for Services** menu of the device, and **Command Load and Execute** option of the **HP Web Jetadmin** is checked.

SafeCom Go HP log entries dated 1 January 1970

The entries in the SafeCom Go HP log file remain unchanged and fixed at 1 January 1970 00.00.00 GMT. This is because the printer has been unable to locate an SNTP (Simple Network Time Protocol) compatible time service on your network. For additional information we recommend that you search for SNTP on www.hp.com and www.microsoft.com.

SafeCom Go HP has incorrect IP address

SafeCom Go does not support TCP/IP(v6), so if you are in such an environment you must disable use of TCP/IP(v6). See [Disable TCP/IP\(v6\)](#).

The device does not send tracking data to the SafeCom Server

If an HP device with SafeCom embedded software does not send tracking data to the SafeCom Server, it might be because of the setting "Information tab requires administrator access". This setting has to be unchecked, otherwise no tracking data is sent from the device to the SafeCom 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. See [Device Server config.ini](#).

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"

The following must be completed 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.

Device Server: Cannot re-add FutureSmart device

If you cannot re-add a FutureSmart device to a working Device Server, perform a partial clean on the device and re-add it to the Device Server.

Device Server: Devices are not configured against failover device server

If device server failover is initiated and the devices are not configured against the failover device server, make sure that failover is enabled on the failover device server.

Device Server: No HP OPS server configured on device

If you have an existing Device Server, and you add new HP Officejet Pro devices, you must set up the HP OPS service before using the new devices with the Device Server. See [HP OPS installation](#) about installing HP OPS.

Device Server: HP OPS running on Windows Server 2003

If you created an HP OPS instance on a Windows 2003 machine and the HP OPS Windows service is not starting, you must change the **Log On As** setting of the HP OPS service to the currently logged in user under the **Properties > Log on** tab of the HP OPS Windows service.

Device Server: HP OPS service fails to start during system restart

If you run HP OPS as a Windows service, it may not start successfully after a system restart due to the CouchDB connectivity. If this issue occurs, you have to manually start the HP OPS Windows service.

The following sections outline a number of other OPS-related or HP Pro series-related issues and their possible solutions.

Check if third-party components are running

Check in Services (Control Panel/Administrative Tools) panel if the following services are running:

- Apache CouchDB (1.2.0)
- OPS (1.0.6)

Using the netstat -a -b command from elevated command prompt, check if the components are listening:

```
TCP 0.0.0.0:5984 [COMPUTERNAME]:0 LISTENING
[erl.exe]
TCP [Server IP]:8081 [COMPUTERNAME]:0 LISTENING
[node.exe]
```

The installer of the Device Server enables port 8081 for OPS service for incoming calls.

If the server IP is 0.0.0.0, that would mean the server is listening on all network interfaces.

If the file set is inappropriate, or the services are either not running or not listening, restart your computer, and recheck the above. If the problem is still present, you have to reinstall the SafeCom package, and consult the HP OXPd User Guide for post-installation configuration settings.

Check the installed file set

Check if CouchDB is installed to the following folder:

c:\Program Files (x86)\Apache Software Foundation\CouchDB\

Check if the erl.ini file is present in the bin subfolder, with a content of

```
[erlang]
Bindir=C:\\Program Files (x86)\\Apache Software Foundation\\CouchDB\\erts-5.9\\bin
Progname=erl
Rootdir=C:\\Program Files (x86)\\Apache Software Foundation\\CouchDB
```

Check if OPS is installed to the following folder:

C:\Program Files (x86)\Hewlett-Packard\OPS

Check if the certificate file (opsca.cer) exists in the certs subfolder and that it corresponds to the one in the config subfolder of the Device Server installation folder (you can check this by doing a binary comparison of the two certificate files using, for example, the `fc /b` command).

Check the device configuration

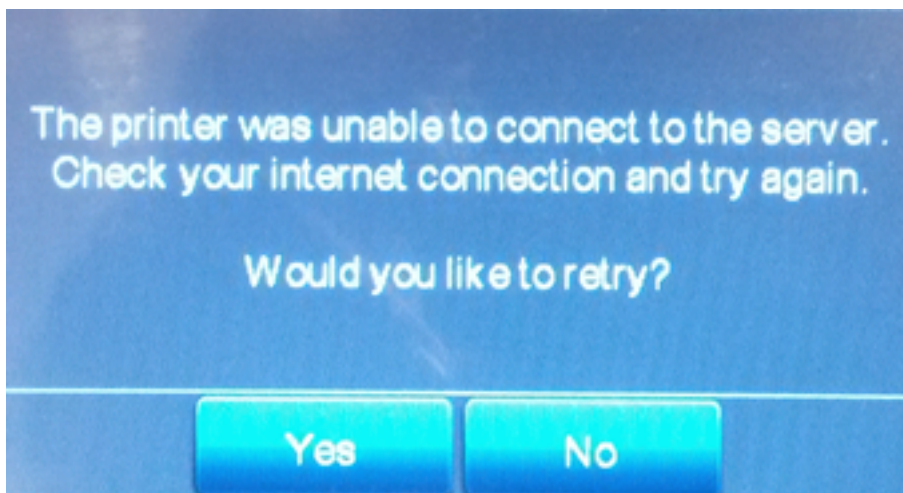
- Before adding the device to the Device Server, synchronize the date, time and time zone of the device and the SafeCom Device Server.
- Before adding the device, remove all unnecessary certificates from the device.
- After adding the device to the Device Server, there should be two new certificates on it.

Handling known installation issues

1. If you receive an "Invalid parameter" error message while configuring the device on the administrative UI of SafeCom Device Server, restart services in the following order:
 - a. Restart Apache Couch DB.
 - b. Restart OPS.
 - c. Restart the SafeCom Device Server.
2. If you receive a "Concurrency" error message, Synchronize the date, time, and time zone of the device and SafeCom Device Server.
3. If OPS certificate is missing from the device configuration, install the certificate manually to the device. Use the opsca.cer file located in the config subfolder of the Device server installation folder.

HP Pro connectivity and certificate issues

If you have intermittent connectivity problems when hitting Pull Print on HP Pro devices, you may need to perform a number of troubleshooting steps. The typical indication is the following error screen:



Prior to doing any of the troubleshooting, you must ensure the following:

- OPS must be installed.
- Device Server certificate must be installed (if it is not, read the device to both OPS and the Device Server).
- The certificate store must contain the **CN=OPS** and **CN=SafeCom** lines in the **Issued To** column.

If these prerequisites are met, you can proceed with the troubleshooting. You do not have to complete all procedures outlined below; either may solve your issue. The procedures are listed from the least effort-intensive to the most effort-intensive.

If these procedures do not solve your issues, provide the following when requesting further assistance:

- Contents of the log subfolder of the Device Server installation directory
- The config.ini file from the equinox subfolder of the Device Server installation directory
- Do you use HP WebjetAdmin?
- Do you use HP Digital Sending Software (DSS)?
- Do you use external Jetdirect devices?
- Does the MFP connect wirelessly or directly into your network?

Checking network settings

HP Pro devices are sensitive to network settings, thus ensure that both the Domain Name and fully qualified domain name of the Device Server is registered in the DNS.

1. Check and set the WINS and DNS servers on the MFP.

2. Wait until the Device Server domain name is transmitted to the MFP. Depending on your network settings, this may take over 30 minutes.
3. Restart the MFP.
4. Check that Pull Print works correctly.

Check timezone settings

If your network settings are fine, there may be a discrepancy between the time zones of the MFP and the Device Server. You may either set the time on the device web page and restart the device, or wait for 24 hours.

Check the certificate

i Use the steps below if your domain name is different from the standardized domain naming scheme (for example, it is not .org, or .com) and Pull Print does not work.

If both the network and timezone settings are correct, the certificate on the Device Server may not be suitable for HP Pro. This may be a typical issue if using DHCP or virtual machines.

i This procedure requires you to delete all MFPs from the Device Server and add them again.

1. Ensure that the Device Server has a fixed IP, and that it is set to IPv4.
2. Delete all printers (if any) added to the Device Server.
3. Stop the Device Server.
4. Create a backup copy of the config\keystore.jks file.
5. Delete config\keystore.jks.
6. Open the equinox\config.ini for editing.
7. Add deviceserver.serverAddress=X.X.X.X to the end of the file.
X.X.X.X is the IPv4 address of the Device Server.
8. Start the Device Server.
9. Add the HP Officejet Pro MFP.
10. Check that Pull Print works.
11. Add the deleted printers (if necessary).

Special symptoms

Check whether the DNS recognizes the given name.

1. Connect the network cable of the MFP to a PC or laptop and ensure that only the Network Interface assigned to that socket is enabled.
2. Type the following to the command line: nslookup DOMAIN_NAME_OF_DS DNS_ADDRESS.
DOMAIN_NAME_OF_DS is the name of the Device Server (not its FQDN) and DNS_ADDRESS is the IP address of the DNS server.
3. If the DNS does not recognize the given name, see [Check the certificate](#).
That procedure is the only solution if this symptom is present.

Go FS cannot access Print Engine

If the Go FS cannot access the Print Engine, check your configuration.xml, and ensure that the {NAME_RESOLUTION_RULE} tag is set properly (see [Sample configuration files](#)). The entire XML-based configuration can be uploaded and edited using the SafeCom Device Utility as described in the *SafeCom G4 Administrator's Manual*.

FutureSmart device cannot be configured

If the FutureSmart device can be identified but cannot be configured, the communication between the SafeCom device server and the SafeCom Go installed on the device may be broken. A partial clean of the device should solve the issue.

At the Printer: Loading SafeCom

The Loading of the SafeCom Go HP software takes a couple of minutes and is started as soon as the printer's embedded web server (EWS) is loaded. As soon as the loading has completed the SafeCom menus will be available in the EWS.

At the printer: No Pull Print icon

- If it is a FutureSmart device, the Pull Print icon will not appear if a wrong or no **Administrator password** is set on the **Configuration** web page. If the Device Server is used, the **Administrator password** is set on the **Device Settings** web page.
- Are the SafeCom Go HP *.b49 and *.b89 files installed in the printer? You verify this by logging into to web page of the printer. If SafeCom appears on the menu, then it is installed.
- Did you install the correct types of these files? If you suspect that you installed the wrong type of files you may have to do a DISK INIT before installing the correct version.
- If **Pull Print** is not checked on the **Configuration** web page you will not see the Pull Print icon.

At the Printer: No automatic logout

On an HP LaserJet MFP, the user is **not** automatically logged out if the **Timeout** specified on the SafeCom Go HP configuration web page is greater than that of the MFP's **Inactivity timeout** specified under **Copy/Send settings**. Default is 60 seconds.

At the Printer: Card reader not working

- Is the card reader powered and firmly connected?

- Is the card compatible with the reader?
- Try to move the card reader away from the printer to check that if it is electrical interference that prevents the reader from working.
- If the card reader is USB connected, it must be present during power on. With the exception of MFPs with August 2008 or newer HP firmware, most HP printers do not support hot swapping of USB devices.
- Is the card reader used with SafeCom Go HP on an HP LaserJet without hard disk and is RAM DISK set to OFF? Change the RAM DISK to AUTO on the printer's System Setup menu.
- If you are using a SafeCom Go HP Flash Memory Card, you may also want to re-seat the SafeCom Go HP Flash Memory Card in another slot on the formatter board. Do NOT use the slot labeled FIRMWARE SLOT or SYSTEM CODE. If it still does not work and you have another SafeCom Go HP-enabled device that works, then you may wish to swap the hardware components one at a time to establish which one is faulty. The components are: SafeCom Card Reader, SafeCom Go HP Flash Memory Card, and SafeCom Go HP Bracket with cable.

At the Printer: Authentication failed

When you tap and icon, you might see the message "Authentication failed" or the icon might appear dim with the text "Not available" on it. This is the case if SafeCom Go HP was installed previously and the printer is still attempting to use SafeCom as login method. To fix this problem, make sure the printer's login method in the **Authentication Manager** is not SafeCom or SafeCom P:Go.

If the login method is **Removed or unknown** for the functions that you would expect to be controlled by the SafeCom solution, then you should restart the printer and try again.

At the Printer: Error Printing: 194

Pull Print is cleared on the **License** tab in the printer **properties** dialog in **SafeCom Administrator**.

At the Printer: Printer busy, retry later

The "Print busy, retry later" message in the printer's control panel indicates that SafeCom cannot get exclusive ownership of the printer. With exclusive ownership, it is ensured that only your documents print while you are logged in. If you get this message for no apparent reason, it could also be because SNMP is disabled on the printer. Please enable SNMP on the printer.

At the Printer: Printing disabled

If the device is not ready to print, the **Print** and **Print all** buttons are disabled (removed) and when logging out an attempt is made to resume printing of any waiting prints. Users may see

the message: "Printing disabled, check status, {status code}". These status codes (0-7) and their descriptions are listed below; the ones marked with asterisks (*) prevent printing:

- 0: Service Requested
- 1: Offline *
- 2: Jammed *
- 3: Door Open *
- 4: No Toner *
- 5: Low Toner
- 6: No Paper *
- 7: Low Paper

To override this and enable printing, use SafeCom DeviceUtil (located in the G4 folder) for editing the configuration. Change the **true** values to **false**, save the configuration, and resend it to the device.

```
<BLOCK_PRINT_WHEN>
<OFFLINE>true</OFFLINE> (1)
<JAMMED>true</JAMMED> (2)
<DOOR_OPEN>true</DOOR_OPEN> (3)
<NO_TONER>true</NO_TONER> (4)
<NO_PAPER>true</NO_PAPER> (6)
<PAUSED>true</PAUSED>
</BLOCK_PRINT_WHEN>
```

At the Printer: Source not reachable / Job inaccessible

The user is trying to collect a document that resides in a folder on a computer that is not reachable for the printer.

The "Job inaccessible" message may also result from improper licensing. Ensure that the **Pull Print** and **Smart Scan** check boxes are set properly under **Device properties > Licenses** in SafeCom Administrator.

Also check the license status on the EWS page, and ensure that they are set properly. If Pull Print or Smart Scan are unchecked on the EWS, registering the device removes the license.

At the Printer: OXPd Application Error Message 45.00.07

This error message appears on the device 5-10 seconds after having tapped the Pull Print icon or the Account icon. This means that the SafeCom Device Server is down and that the access control has not yet been configured for the Pull Print icon and the Account icon.

Restart the SafeCom Device Server and configure the access control for the Pull Print and Account icons.

At the Printer: USB Error

If you get the message ""The USB storage device that was just inserted is not supported"", it is likely that you have installed the USB ID device on the device before installing the SafeCom solution on the device.

Make sure to always install the SafeCom solution on the device before installing any USB ID devices.

At the Printer: error cc = 500

If you receive the error message "error cc = 500" when trying to load the installation file on old devices, use the internal HP Go loader (this.loader) and rename the loader to a .jar file in order to make this work.

At the Printer: Log out button and timeout

If you logged in to your pull print document list, but the device times out, then you are taken back to the main device screen, with a "Logout safely" message. You have to click the **Log out** button, then log in on the device again to access your pull print documents.

At the Printer: Concurrent job tracking issues

To avoid job tracking issues resulting from concurrent device usage by multiple users, ensure that only a single active workflow is running on the device at times. That is, do not log in and attempt to perform any jobs while the device is already actively processing another user's job.

Tracking records state issues

If the tracking records remain in **Pending** state or become **Completed** immediately, check or consider the following:

- The feature works only with HP FutureSmart devices.
- Check the Windows Events for driver compatibility warnings.
- Ensure that the device is registered properly at the SafeCom G4 Server.

Low resolution icons displayed on FutureSmart devices

If you install the latest SafeCom Go HP FutureSmart client over an earlier version, the icons of the old version may be displayed on the device screen. To display the icons for the new firmware,

disable then re-enable Pull Print and SmartScan on the SafeCom EWS configuration page under **Tracking settings > Authentication and tracking**.

At the Printer: 49.08.06 DEVICE ERROR after installing or upgrading the Go HP bundle through SafeCom Administrator

If you encounter this error message, deploy the SafeCom Go HP bundle through the EWS page of the device.

At the Printer: 49.38.03 DEVICE ERROR after installing the Go HP bundle through SafeCom Administrator

If you encounter this error message, deploy the SafeCom Go HP bundle through the EWS page of the device.

At the Printer: OK button inactive on Login denied screen

On some devices the **OK** button may become inactive on the Login denied screen in case of a failed login attempt. In such cases, press the **Back** button in the top-left corner of the screen.

Chapter 7

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.