

SafeCom HP Unified Client Administrator's Manual




Version: 5.10.0.1000

Date: 2020-09-17
Version: 5.10.0.1000

KOFAX

Document Revision Date	Revision List
March 31, 2020	Release for HP UC 1.1
July 10, 2019	Final release.
April 30, 2019	Interim release.
December 21, 2018	Preview release.
December 1, 2018	Draft release.

Symbols Used In This Guide

	The accompanying text provides cross-reference links, tips, or general information that can add to your understanding of a topic.
	The accompanying text provides key information about a step or action that might produce unexpected results if not followed precisely.
	<i>Read the accompanying text carefully.</i> This text can help you avoid making errors that might negatively affect program behavior.

2020 © 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.

Trademarks

Trademarks: Kofax, the Kofax logo, SafeCom, SafeCom Go, SafeCom P:Go, SafeCom ePay and the SafeCom logo are trademarks of Kofax Inc. or its affiliates in the United States and/or other countries. All other trademarks referred to herein are the property of their respective owners. Kofax Inc. cannot be held responsible for any technical or typographical errors and reserves the right to make changes to products and documentation without prior notification.

Third Party Software: This software may contain third party software which requires notices and/or additional terms and conditions.

Patent: Kofax Inc. has received the following British patent GB 2350 713 B, US patent US 6,952,780 B2 and Europe EUR EP1 120 701.

© Copyright 1995 - 2020 Kofax Inc. All rights reserved

Kofax Inc.

Web: <https://www.kofax.com/Products/safecom>

Table of Contents

Chapter 1: Introduction	7
SafeCom HP Unified Client.....	7
Supported languages.....	7
Requirements.....	8
Network requirements.....	8
Partial Disk Clean on supported devices.....	8
SafeCom ID Devices.....	9
HP Universal Print Driver.....	9
Install HP Universal Print Driver.....	10
Check the Printer properties.....	10
Make the printer use the SafeCom Pull Port.....	11
Print a test page.....	11
Available documentation.....	11
About this manual.....	12
Chapter 2: SafeCom HP Unified Client - Device Web Server	13
Overview.....	13
SafeCom HP Unified Client – Device Web Server installation.....	13
Installation.....	13
Windows Firewall - ports that must be opened.....	13
Add the device via SafeCom Administrator.....	14
Configure device in SafeCom Administrator.....	19
Settings tab.....	20
Charging scheme tab.....	21
Device configuration.....	22
Application access control.....	26
Card reader configuration.....	26
How to add a card reader.....	27
DWS failover and groups.....	27
Configure Device Web Server failover.....	28
SafeCom Mass Deployment Tool (Device Clone Tool).....	28
Converting an existing SafeCom Go HP FutureSmart fleet to a HP Unified Client fleet.....	32
Parameter file format for importing a list of new devices.....	32
The cloning workflow.....	34
Performance, logging, error handling.....	35

Support for 4.3" and 2.7" devices.....	35
Mixed mode authentication.....	36
SafeCom HP Unified Client - How to.....	39
Select login method.....	39
Control user access rights.....	40
Enable Client Billing on the device.....	41
Enable using the Home Folder.....	42
Determine the DWS version.....	43
Determine the HP Unified Client version.....	43
Configure Push Print Post Tracking.....	43
Configure users and devices to allow modifying job settings.....	45
Uninstall SafeCom HP Unified Client.....	47
Relocate DWS application log folder.....	48
SafeCom HP Unified Client device trace facility.....	48
Chapter 3: Using SafeCom HP Unified Client.....	50
Login.....	50
Login with card.....	50
Login with card and PIN code.....	51
Login with ID code.....	51
Login with ID code and PIN code.....	51
Login with Windows.....	51
Register card at device with Windows credentials.....	51
Register card at device with PUK code.....	52
Change PIN code.....	53
Server status verification.....	53
Pull Print - Document list.....	55
Copy.....	56
Folder.....	56
E-mail.....	56
Selecting a Billing Code.....	56
Logout.....	57
Chapter 4: Troubleshooting.....	58
Introduction.....	58
At the Printer: Card reading not working.....	58
At the printer: Card swipe results in unexpected behavior when using 3rd party authorization.....	58
At the Printer: Device freezes as Register with Windows credentials pressed.....	58
At the printer: Handling stale connections by G4 server.....	59
At the Printer: SafeCom inactivity timeout does not work on device home screen.....	59

At the Printer: Sign-in failed.....	59
At the Printer: Source not reachable / Job inaccessible.....	59
At the Printer: Undesired timeout.....	60
At the Printer: USB Error.....	60
At the Printer: User cannot log out until the last job is spooled.....	60
Add device to device controller service failed error.....	60
Certificate generation for DWS fails.....	60
Incorrect tracking information.....	61
OXPd Application Error - Mime type not supported.....	61
Prevent low toner feature does not work.....	61
Prices do not match.....	61
Problems when adding a device - valid certificate required.....	61
Problems when adding a device - device already configured.....	62
The device is registered in the SafeCom database.....	62
The device is registered in the DWS.....	62
Problems when adding a device - device is not discoverable.....	63
SafeCom HP Unified Client has incorrect IP address.....	63
Sign-In methods are disabled on the device.....	64
Signing in message appears while canceling.....	64
Unable to find device.....	64
Unexpected unattended push prints appear.....	64
Wrong tracking or negative balance of the user in case of duplex printing.....	64

Chapter 1

Introduction

SafeCom HP Unified Client

SafeCom HP Unified Client is a solution for HP LaserJet, LaserJet Enterprise and PageWide Enterprise MFPs. It integrates with the touch-screen control panel of the HP MFP and offers user authentication by code and/or card.

SafeCom HP Unified Client works together with 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.

Supported languages

SafeCom HP Unified Client supports the following display and input languages on the device:

- Chinese (S)
- Chinese (T)
- Czech
- Danish
- Dutch
- English
- Finnish
- French
- German
- Hungarian
- Italian
- Japanese
- Korean
- Norwegian
- Polish
- Portuguese
- Russian
- Spanish
- Swedish
- Thai

- Turkish

Safecom G4 Server and Safecom Administrator support English only.

Requirements

- Any networked HP LaserJet, LaserJet Enterprise and PageWide Enterprise MFP, printer, and scanner listed <https://www.kofax.com/Products>.
- SafeCom G4 Server installed
 - This release of SafeCom HP Unified Client requires SafeCom G4 Server version 5.10.0.1000 or above.
- HP device requirements in details:
 - Firmware 4.10 or newer
 - Screen sizes of 8", 4.3" and 2.7", with resolution 1024x768, 800x600, 480x272 or 320x240.
 - It is recommended to perform a partial clean if you are installing the SafeCom HP Unified Client onto a device which had the SafeCom Go HP client earlier or it was added to Device Server.

Note If your SafeCom solution uses both Device Web Server and Device Server instances, then these must be installed on a separate server.

Network requirements

The network must allow communication via certain network ports, including TCP ports 7500 and 7700, and UDP port 5742. If there is a Device Web Server in use, then port 8444 should be open too.

Refer to chapter *TCP and UDP port numbers used by SafeCom* in SafeCom G4 Administrator's Manual.

Partial Disk Clean on supported devices

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

To perform a partial disk clean:

1. Delete the device from the **SafeCom Device Web Server** where the device is added (see [Uninstall SafeCom HP Unified Client](#) for details). The device must be in the idle state  in order for the deletion to be performed correctly.

Note If the device is configured to another server, click the **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.
6. Select the **Partial clean** option.
7. Press **OK**.
8. Press **Back**.
9. Press **Continue**.

SafeCom ID Devices

Table 1 SafeCom HP Unified Client supported SafeCom ID devices

- Kofax Micro Card Reader
- Kofax MX
- Kofax MX (Keyboard)
- HP Reader (CZ208A/X3D03A)
- Elatec TWN3
- Elatec TWN3 (Keyboard)
- RFIDeas pcProx (Y7C05A)

Additional information about the ID devices is available in the *SafeCom G4 Administrator's Manual* (D60650).

Note 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.

HP Universal Print Driver

Note HP Universal Print Driver is mandatory in order to have appropriate tracking of the push print jobs.

Download HP Universal Print Driver from the HP website. It can be used for PCL5, PCL6 and PostScript with SafeCom Pull Print if it is installed and run in **Traditional mode**, where UPD forwards the print data to the SafeCom Pull Port.

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 model-specific 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 together with the SafeCom Push Port for tracking of documents that are sent directly to the device.

Note Be aware that 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.

Note Any paper sizes that cannot be specified in the charging scheme will be tracked as Other.

Install HP Universal Print Driver

To install HP Universal Print Driver do the following:

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. Click **Add a local printer**.
6. Choose **Create a new port** and select **Standard TCP/IP Port** from the dropdown list. Click **Next**.

Note 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 matches your needs and click **Next**.
10. Enter a **Printer Name** and choose whether or not this printer should be your default Windows printer. Click **Next**.
11. Check **Share this printer...** and enter **Share name**. Click **Next**.
12. Do not click **Print a test page** to verify the system. 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. Choose **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 choose **Use network logon** as method of **Authentication**. Click **OK**.

Note 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.

Available documentation

SafeCom G4

- *SafeCom G4 Administrator's Manual* (D60650) — A comprehensive manual that the administrator should consult to set up a successful SafeCom solution. Includes information about SafeCom Tracking, SafeCom Rule Based Printing, SafeCom Client Billing, and SafeCom Pay.

SafeCom HP Unified Client

- *SafeCom HP Unified Client Administrator's Manual* — (**this manual**) Manual on how to install, configure and use SafeCom HP Unified Client.

About this manual

This manual applies to SafeCom G4 Server version 5.10.0.1000 and Device Web Server version 5.10.0.1000 or above.

This manual is organized as follows:

- Chapter [Introduction](#) lists the supplied SafeCom documentation, system requirements and describes how this manual is organized.
- Chapter [SafeCom HP Unified Client - Device Web Server](#) describes the installation of SafeCom HP Unified Client via the SafeCom Device Web Server.
- Chapter [Using SafeCom HP Unified Client](#) describes how to interact with the HP device's control panel when SafeCom HP Unified Client is installed.
- Chapter [Troubleshooting](#) contains troubleshooting hints.

Chapter 2

SafeCom HP Unified Client - Device Web Server

Overview

Make sure the SafeCom G4 Server software installation has been completed prior to installing SafeCom HP Unified Client.

SafeCom HP Unified Client – Device Web Server installation

Installation

After installing SafeCom G4 Server and HP Universal Print Driver complete the following steps to install the Device Web Server (DWS):

To install SafeCom Device Web Server do the following:

1. Select and run the installer file to launch the Setup Wizard.
2. On the Welcome screen, click **Next** to begin the installation process.
3. Read and accept the terms of the End User License Agreement and click **Next**.
4. On the Destination Folder screen, accept the default installation folder or click **Change** to select a new folder.

Application data for SafeCom Device Web Server will be stored at:

```
c:\Windows\System32\config\systemprofile\AppData\Local\Nuance\
```

5. Click **Next**.
6. Review settings before copying of files starts. Click **Install**.
7. Click **Finish**.

Windows Firewall - ports that must be opened

If Windows Firewall is enabled, it may prevent the SafeCom solution from working. Disable the firewall or open the ports listed below.

TCP	Inbound on SafeCom Device Web Server	Protocol
-----	--------------------------------------	----------

8444	Device Web Server communication	SafeCom
------	---------------------------------	---------

Note If the Device Web Server and G4 Server are installed on the same server, then additional port configuration is required. Refer to the SafeCom G4 Administrator's Manual for details.

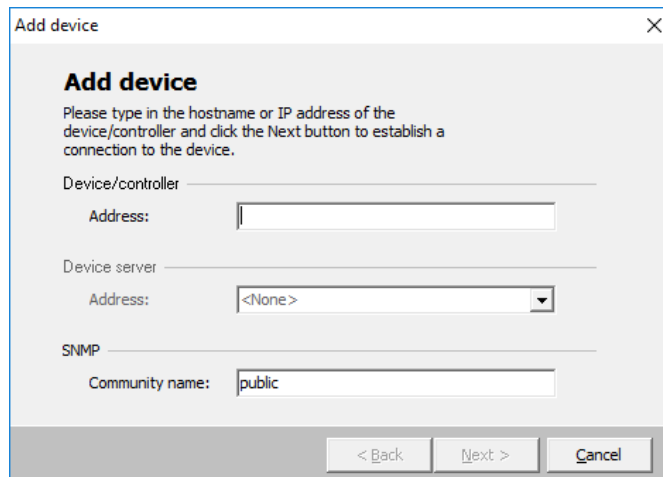
Add the device via SafeCom Administrator

Before adding a device, IPP (Internet Printing Protocol) has to be enabled for device discovery to work properly. As IPP is disabled by default in recent HP devices, make sure to enable it (see [Problems when adding a device - device is not discoverable](#) for detailed instructions). After configuration is completed, you may disable IPP protocol on the device again.

During setup, make sure that the server time of the device and the DWS server match, otherwise tracking data can be inaccurate.

To add a device do the following:

1. Click the **Devices** container, right-click the content area and then click **Add device**. The **Add device** wizard displays.
Backwards compatibility: G4 versions prior to 520.12 are not supported with DWS 5.10, which is the DWS component of HP UC 1.1. G4 520.12 supports DWS version 5.9, which is the DWS component of HP UC 1.0.
2. From the **Device server** drop down menu, select the desired server. If the server is not listed, then type the host name or the IP. Click **Next**.



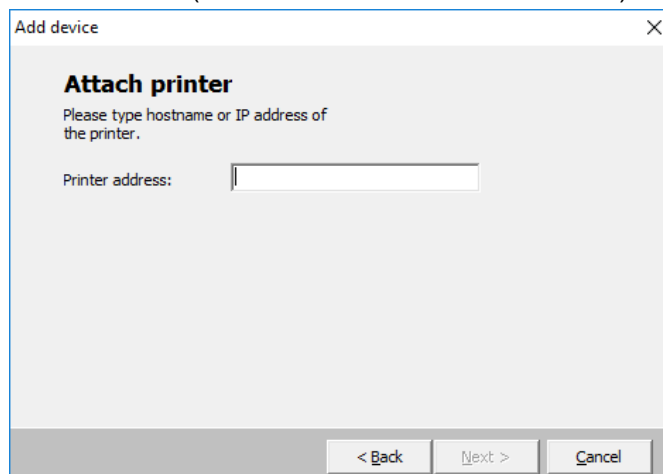
Note If the server runs on Windows Server 2012 R2, then specifying Device Web Server by IP address may not work, in this case use host name instead.

Note Name resolution is essential for certification in the SafeCom solution. If the Device Web Server is in a network environment where name resolution does not work, devices may not be added to the server properly. Ensure that the server has a valid FQDN, and DNS name resolution works.

Note SNMP is not used during discovering HP Unified Clients. The Community name property is requested here only for supporting devices from other vendors.

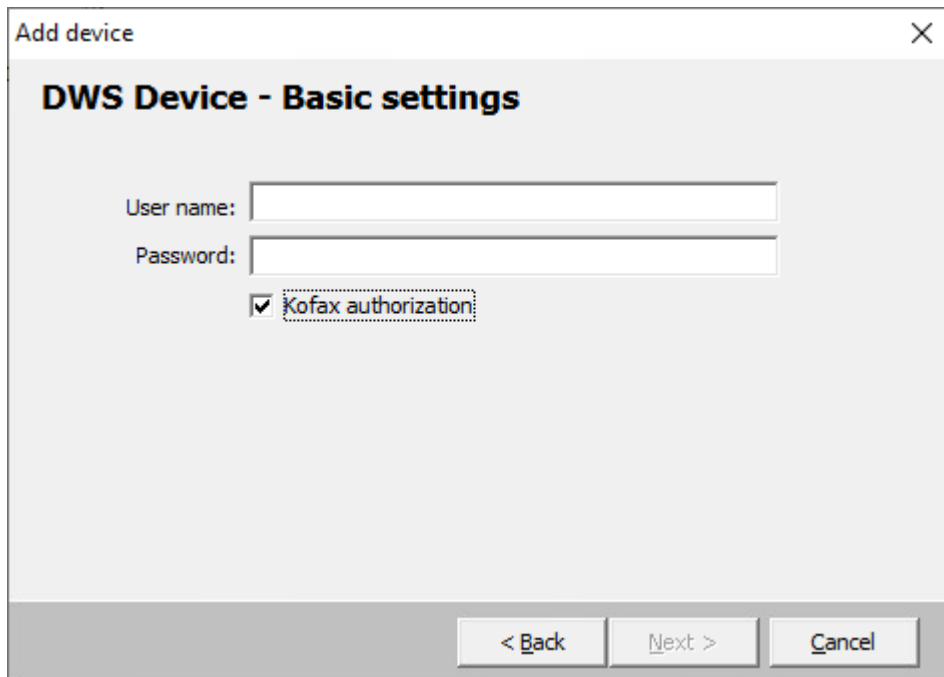
Status information is retrieved from the Device Web Server. Click **Next**.

3. Enter the **Printer address** (the device IP address or host name) and click **Next**.



4. If the device discovered properly, a summary of device information appears. Click **Next**.

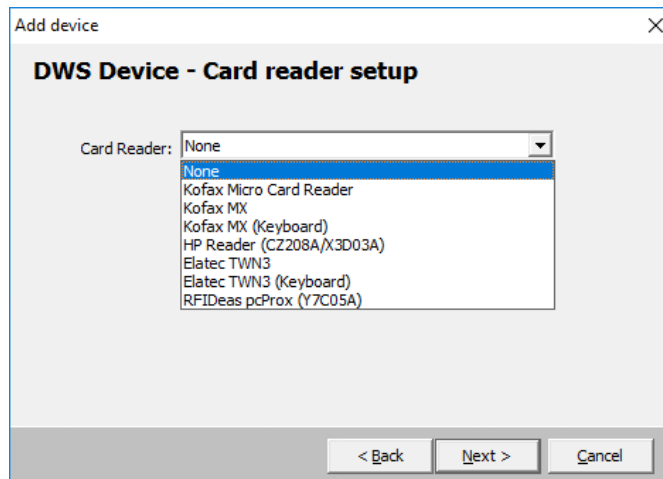
5. Provide administrator credentials for the device. These should match with the ones specified in the device's security settings. Administrator credential is used for the registration of buttons and agents at the device.



The screenshot shows a dialog box titled "Add device" with a close button (X) in the top right corner. Below the title bar, the text "DWS Device - Basic settings" is displayed. There are three input fields: "User name:" followed by a text box, "Password:" followed by a text box, and a checked checkbox labeled "Kofax authorization". At the bottom of the dialog, there are three buttons: "< Back", "Next >", and "Cancel".

The administrator password of the device cannot be changed after the device is added to SafeCom. To change the administrator password, remove the device from SafeCom, change the password, and add the device again to SafeCom using the new password.

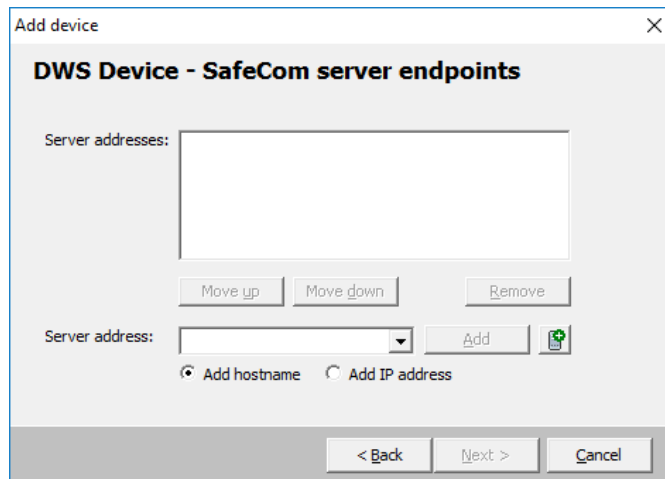
- a. Enter the **User name** and **Password** as specified on the device web page.
 - b. If Kofax authorization check box is selected, the function access control of the device can be managed by a SafeCom Administrator. Otherwise, to manage permissions, visit Security/ Access control page on the EWS of the device. For details on this setting, please see section [Mixed mode authentication](#).
 - c. Click **Next**.
6. Select a Card Reader:




Note If your card reader is not in the list, then you need to add it to SafeCom. For details see [Card reader configuration](#).

Note Some card readers may not work right after the device installation. In this case unplug the card reader and plug it in again.

7. Fill the list of SafeCom server endpoints:



- a. Choose one of the **Add hostname** or **Add IP** address options to determine the way addressing the server.
- b. Select a server in the **Server address** drop down list.
- c. Click **Add** to add the selected server to the **Server addresses** list above. Optionally, use the  button on the right to add the current server. Repeat from step 7.b on if you want to add multiple servers to the list to configure SafeCom server failover.
- d. Use the **Move up** and **Move down** buttons to define the priority of the servers. The first server in the list controls the device primarily. Other servers take over the control if the previous servers are out of order.

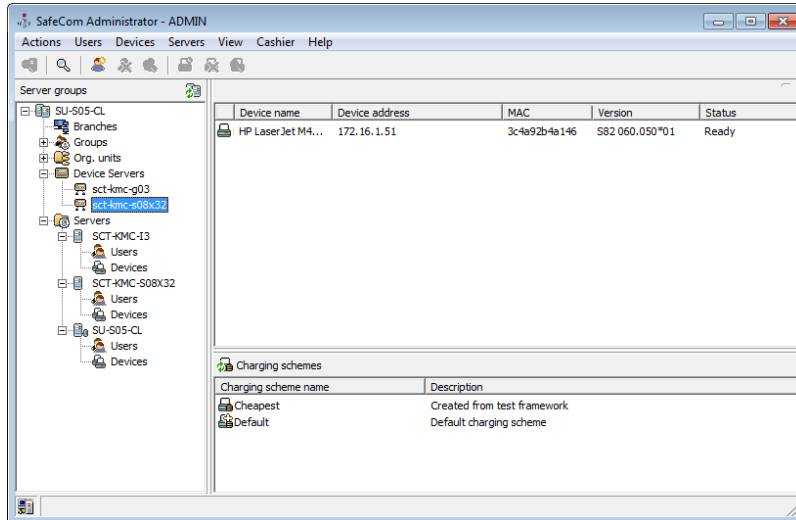
Note It is recommended to add secondary servers only to the list of server. Primary server is less effective at device control.

8. The **Device Properties** dialog now opens.

Note The Name parameter can only contain alphanumeric characters, underscore (_) and hyphen (-), and must be unique. By default, this parameter contains the host name of the device.

- Click **Add** to register the device and save it in the database. After approx. 1 minute the device is added to the server.

The device is now added and listed under **Devices**.



- Go to section [Configure device in SafeCom Administrator](#) to continue with the configuration of the device.

In case of any problems while adding a device, check [Troubleshooting](#).

Configure device in SafeCom Administrator

Use the Device properties dialog to configure the behavior of HP Unified client on the device. This dialog box consists of three tabs:

- Settings – Set or verify general settings, such as device name, server, and address. Control capabilities such as duplex or color. See [Settings tab](#) for details.
- Charging scheme – Select from available primary and secondary charging schemes for the device. See [Charging scheme tab](#) for details.
- Device configuration – Set access control, licenses, log on methods, printing engine and toner options, tracking on device, and menu elements. See [Device configuration](#) for details.
- Application access control – For details on client application access control see [Application access control](#).

Settings tab

Device properties - NPI78CDC1

Settings | Charging scheme | Device configuration

HP Unified client ID: 6

Version: MAC: fc15b478cdc1
Status: Ready Serial: MX2CG410BQ

General

Name: NPI78CDC1
Model: hp laserjet mfp m630
Home server: HG-NEUF58
Device server: HG-NEUFDWS2
Location:
Device address: 10.140.202.13

Capabilities

<input checked="" type="checkbox"/> Duplex supported	<input type="checkbox"/> Restricted access
<input type="checkbox"/> Color supported	<input checked="" type="checkbox"/> Push print
<input type="checkbox"/> Large format print	<input type="checkbox"/> Allow Pay user

OK Cancel

This tab provides basic information on the device and the client in these sections:

- *Device name* – The title section displays the following:
 - *Device name* – It must be a unique alphanumeric text. DWS uses this property as a unique identifier.

Note It has to be set at device addition and cannot be changed later.

- Version
- Status
- MAC address
- Serial
- ID (in the upper right corner)

Hover the mouse pointer over the device name to display the following wiring information:

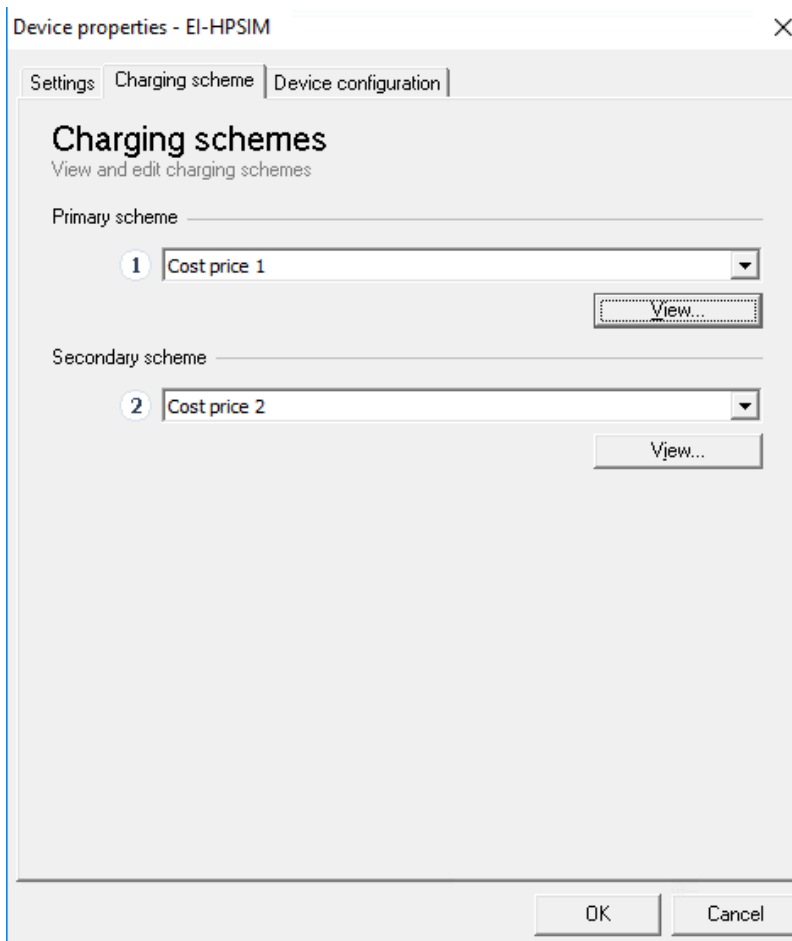
- Authentication
- Card reader information
- SafeCom server IPs
- General section – This section contains the following properties:
 - Name – Device name

Note Changing the host name or the IP address of the device after installation is not supported.

- Model – Device model name
- Home server – G4 Server instance name, always disabled
- Device server – DWS name, always disabled
- Org. unit – organization unit
- Location – Geographical location
- Device address – IP address of the device (read only)
- Capabilities section – This section offers the capability options listed below. Clear the corresponding check box to turn off the feature or select the check box to turn on.
 - Duplex supported
 - Color supported
 - Large format print
 - Restricted access
 - Push print
 - Allow Pay user

Charging scheme tab

This tab lets you select and edit the primary and secondary charging schemes for the device. You may select from the lists, click the corresponding View button to edit the selected scheme.



Note Secondary prices may be different, as they are calculated only on the server side.

Device configuration

The **Device configuration** tab is used to configure SafeCom HP Unified Client in the following subjects:

- Access control – Setup permissions for device features. See [Access control](#).
- Licenses – Allocate licenses for SafeCom features. See [Licenses](#).
- Login – Login methods, card, domain and masking options. See [Login](#).
- Printing – Printing engine, toner and driver options. See [Printing](#).
- Tracking – Tracking on device and timeout options. See [Tracking](#).
- User Interface – Menu and Quick select bar elements and order. See [User interface](#).



Change the settings according to the following descriptions:

- Access control (authorization)

- Lock device

Using this property, you simply revoke all permissions from the device guest user. If the property is set to true, authentication is required for using any feature of the device. The control panel shows the HP Mandatory sign-in screen. The user can swipe their card or start manual login procedure by pressing the sign-in button. If the property is false, the device home screen is visible on the control panel, and users can log in by their card or by pressing the sign-in button or any icons marked with the lock icon.

Terms in use: Device Level Authentication mode (DLA) - when the device is locked; Function Level Authentication mode (FLA) - when the device is unlocked because guest is allowed to use the device at some extent.

- Permission control

This set of properties is visible when Kofax authorization is selected during device registration. It shows all access points and the associated permissions available on the device. Please note that this list is actively queried from the device and it shows the available features. The list depends on the device capabilities and the installed applications. See [Mixed mode authentication](#).

- Licenses

Note For details on licensing refer to chapter *Device license and user settings dependencies* in the *SafeCom G4 Administrator's Manual (D60650)* document.

- Tracking: This license is needed for tracking activities, such as copy or scan at the device.
- Rule-based printing: This license is needed if you want to enable the Rule-based printing feature for the users on this device.
- Client billing: If this license is allocated, the users who have billing codes can select one of them immediately after login or may create Personal jobs.
- Pay: A Pay user (where cost control is Pay) can log in to a device with a SafeCom Pay license and to a device with a Tracking license provided.
- Pull Print: Set to True to enable pull printing on the device.
- ID device: ID devices require unique ID device licenses. SafeCom ID devices come with ID device licenses, whereas ID device licenses for 3rd party ID devices must be purchased separately.

- Login

Note For Windows authentication, the card reader cannot be used. To use a card reader and Windows authentication, users should select Auto-sense.

- Login method: This determines how users log in. Choose between:

- **Auto-sense:**

- If there is a card reader connected to the device, then users may login by Card, or by Windows authentication.
- If there is no card reader connected to the device, then users may login by ID code.

- **Card:** Users may log in by card-swipe only, entering user credentials or ID is not allowed.

The Sign in button is always visible and enabled on HP device screens, with or without the Mandatory sign-in screen, in other words, in FLA (Function Level Authentication) or DLA (Device Level Authentication) modes.

- In FLA mode: Pressing the Sign in button shows a message box instructing the user to swipe his card. When the device is idle, the device home screen is displayed with small lock symbols on locked applications.
- In DLA mode - Pressing the Sign in button shows the Welcome screen with a label Swipe your card. When the device is idle, a sign-in screen (also called the mandatory sign-in screen) covers the home screen.

Note The Quick Select bar is always visible, this allows the user to change the default application to be launched after a successful login. Welcome screen does not accept tapping.

- **ID code** (default): Users need to use the authentication screen to enter one of their ID codes manually. Card-swipe is not allowed if ID code is selected.

Tip Tap Sign in to reach the authentication screen.

- **Card or ID code:** Both card-swipe and ID code are allowed. For details see the Card or the ID code option.
- **Windows authentication:** Allows the user to log in by entering their Windows user name, password, and domain. The SafeCom administrator may configure the way how user domains display on the screen.

Note The option Windows authentication allows the user to log in by entering their Windows user name, password, and domain. The SafeCom G4 server must be a member of the domain or trusted by the domain.

Note Card identification cannot be used if Windows authentication is selected. If you want to use Windows authentication with card-swipe, then choose Auto-sense as Login method instead.

- Mask user code: Set this value to True to mask the ID code with asterisk (*) when entered at the device.
- Login without pin: Set this value to True if users do NOT need to enter a 4-digit PIN code at login. This setting applies to the device and overrides the equivalent user property on the SafeCom G4

server. Use of PIN code is possible on devices with touch-screen, keypad or optional external keyboard.

- Length of user ID code: Specify the maximum length of the ID code (typed or read from the card). Default value is 39.
- Default domain name: 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).
- Hide domain name: Can be used if you specified a default domain name. Set this value to True to allow the users to log in without typing in the domain.
- Show domain list: Set this value to True to enable SafeCom to offer the list of domains registered in SafeCom Administrator.
- Inactivity timeout: Specifies the amount of time of inactivity (in seconds) after which a user is automatically logged out.
- Guest login ID: Specify an existing user ID for the rule of the guest user. This allows users to tap a Guest button on the SafeCom HP Unified Client login screen. All guest activities will be tracked according to that user's settings. Device guest user is different from SafeCom guest, because a guest user is allowed to use the device without authentication.

Note For Guest login, the user's Login without PIN setting controls if the Guest user must enter a PIN code. It is recommended to allow that Guest users log in without a PIN code.

- Register card by Windows credentials: Set this value to True to let the users assign a new card by providing their Windows credentials, without entering a PUK code.

Note DWS restart may be needed for this server setting to take effect.

- Printing
 - Reverse document list: Set this value to True to show the latest printed documents at the top of the document list.
 - Allow changing print settings: Set this to Enabled to let all users change their finishing options on this device. Select the Per user settings value to manage this feature on a per user basis.
 - Prevent printing on low toner: Set this value to True to disable printing activities if the toner is low.
 - Print Engine access method: Set the method for finding the print engine.
 - Print Engine resolution rule: Specify the identifiers and their precedence to use to find the print engine by editing the print engine resolution configuration. Click the browse button on the right of the value to display the Print Engine resolution configuration dialog box. Select (enable) or clear (disable) the items of the list and use drag and drop to reorder items. Click OK to save the settings and close the dialog box.
 - Supported 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 **SafeCom Administrator**, the document appears with a fidelity warning icon [⚠] in the document list. This way the user is warned that fidelity is low and the document may print incorrectly.

- Tracking
 - Print post-tracking: Set this value to True to track pull and push print jobs based on statistics reported by the device.
 - Timeout for tracking push-print jobs: Specify the time (in hours) that the server waits for job statistics to arrive from the device. If statistics data does not arrive in this time period, the job will be tracked as an Unattended job. The default value is 48.
- - In this group of properties, you can specify which types of jobs must be tracked:
 - Copy
 - Mail
 - Folder
 - Save to job storage
 - Print from job storage
 - Fax
- User interface

Note In case of DLA, the content of the Quick Select bar is also configurable in this group.

- Visibility and order of menu elements: Set the visibility and order of the menu items of the Pull Print screen. Click the browse button on the right of the value to display the Client menu configuration dialog box. Select (enable) or clear (disable) the items of the list and use drag and drop to reorder items. Click OK to save the settings and close the dialog box.

Application access control

HP Unified Client controls access to third-party applications. These applications are automatically detected when [adding the device to SafeCom](#), but they will be accessible only after a successful login. Permission for third-party applications can also be managed on Configure Device tab of Device properties dialog box. They are listed in section Applications of Access control group.

Card reader configuration

All card reader hardware should be added to SafeCom to appear in the Add device list (see [How to add a card reader](#) for details).

Supported card readers

The following readers are included in the default configuration:

- Kofax Micro Card Reader
- Kofax MX
- Kofax MX (Keyboard)
- HP Reader (CZ208A/X3D03A)
- Elatec TWN3
- Elatec TWN3 (Keyboard)
- RFIDeas pcProx (Y7C05A)

How to add a card reader

You may add any card reader to SafeCom by specifying the appropriate Vendor ID (VID) and Product ID (PID) values. Refer to the card reader documentation for these values, then proceed with the following steps.

1. Open `scCardReaders.ini` in a plain text editor such as Notepad.

If you used the default installation path, then the `scCardReaders` file is located on the computer running the SafeCom G4 Server, in the following folder:

```
c:\Program Files\SafeCom\SafeComG4\Device_software
```

2. Navigate to the [HPUC] section, then add a new line for the card reader, following this scheme:

```
<name>=<VID>,<PID>,<is keyboard>
```

- *name* – The name of the device to display in the list of card readers when adding a device.
- *VID* – The VID specified in the documentation of the card reader.
- *PID* – The PID specified in the documentation of the card reader.
- *is keyboard* – Use either 1 for keyboard readers or use 0 for non-keyboard readers.

A typical example:

Example RFIdeas pcProx,0104,3BFA,0

3. Save the changes.

DWS failover and groups

Failover service notification

SafeCom Administrator allows you to group your Device Web Servers, enabling a failover solution.

SafeCom failover service monitors the status of the group members, and in case of a group member failing or shutting down, the rest of the group members distribute the workload of the offline server.

DWS Failover service notifies the job-server service when controllers of devices are changing either due to outage of a DWS node or restoring the original controller of devices. It implies database change and the `DeviceServerId` field of `scDeviceInfo` table in `scCore` database is updated accordingly. The Device properties dialog box shows the controller server in the Device Server field.

Device server & DWS group representation in SafeCom Administrator

Device servers node in tree view has two types of child nodes:

- DS / DWS groups
- DS / DWS servers that are not members of any group

The group member servers are child elements of group nodes.

Selecting a node makes the right pane of SafeCom Administrator adopt to the type of the node:

- Device servers – List of DS / DWS server that are not organized into groups

- Device server group – List of group members
- DS /DWS – List of devices controlled by the server (DS / DWS)

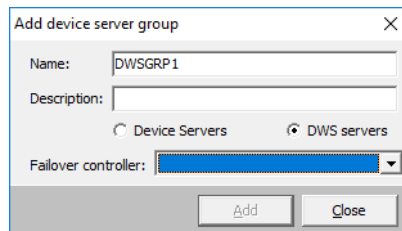
Double clicking on any list item displays the appropriate property dialog box:

- Clicking on a Device Server or Device Web Server (DS / DWS) shows the Server properties dialog box. Failover tab appears in case of DWS group members that shows the list of controlled devices and their primary DWS.
- Clicking on a device shows the Device properties dialog.

Configure Device Web Server failover

Follow these steps to add and populate a DWS failover group:

1. Log in to **SafeCom Administrator**.
2. Open the **Device Servers** list.
3. Right click on the node, then select **Add device server group** in the context menu.
4. Enter a name and optionally a description for the device server group.
5. Select the **DWS servers** option.
The **Failover controller** list below gets populated according to the selected option.
6. Select the controller from the list to use for failover.



7. Click **Add**.
The newly added group shows up under the **Device servers** node.
8. Drag and drop the device servers to incorporate them into the newly created group.

SafeCom Mass Deployment Tool (Device Clone Tool)

Introduction

The SafeCom Mass Deployment Tool (MDT) provides a convenient way for administrators to add a device to the SafeCom system, customize its configuration, then easily add any number of devices with the same configuration.

SafeCom includes a separate tool to setup and configure multiple devices running the HP Unified Client. This helps expediting a deployment, and ensures uniform configuration across multiple devices.

The tool can run as a standalone executable without special installation, although it is part of both the Server and the Tools flavors of the SafeCom Server Installer. The tool can also be invoked from SafeCom Administrator.

The administrator must register one or more devices with a given set of features and configure it using the Add Device Wizard in SafeCom Administrator. Then the tool can be utilized to create clones of these devices. Initial parameters of new printers (like IP address or admin credentials) must be specified either manually or by importing an INI file in order to register them in SafeCom.

It is recommended to differentiate the original devices based on their functionality in terms of capabilities (SFP / MFP) and installed applications. Different HP UC configurations are another grouping factor. It is recommended to add representative devices first for all different groups, and then create the clones.

Note Cloning devices with different screen sizes can cause problems. For example, settings, like requiring a PIN code can make devices with a screen of 2.7" size unusable. It is recommended to specify batches of devices with similar capabilities and screen sizes, and perform individual cloning on these batches. It must be assured that all applications which are installed on the target device exist on the source device, so authorization settings for these applications can be transferred properly.

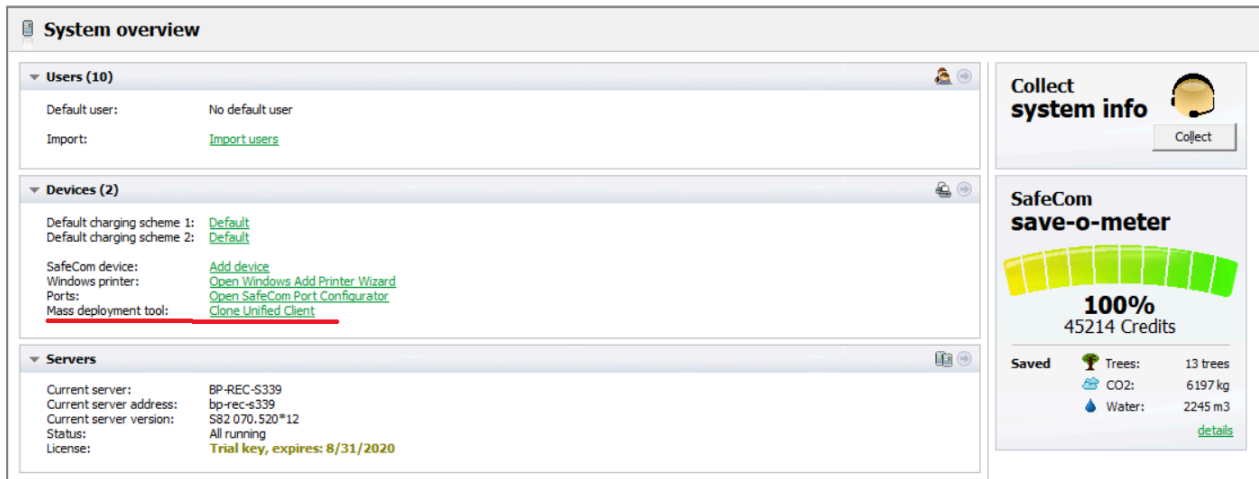
In case of an error, click on the device with the error status. The status message about the error appears at the bottom of the window.

Launching the SafeCom Mass Deployment Tool

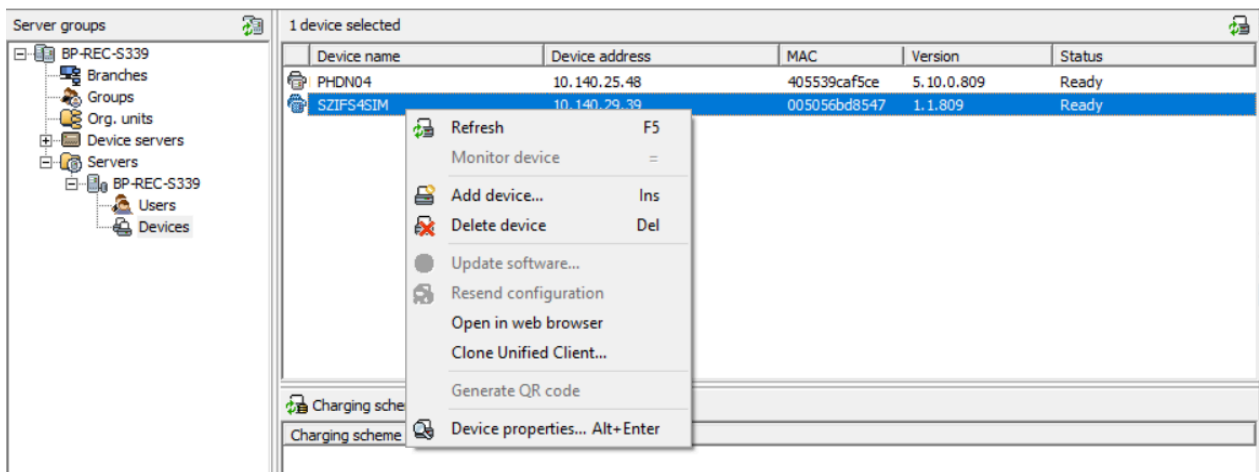
The tool as a standalone executable accepts the following command line options:

- `/usr`: the administrator's username
- `/pwd`: the administrator's password
- `/srv`: SafeCom server name to connect to (optional, local server can be used by default)
- `/devId`: Id of registered HP Unified client to clone (optional)
- `/imp`: name of import file

The tool can also be launched directly from SafeCom Administrator using the system overview panel or the context menu of an existing HP Unified client.



System overview panel



Context menu of an existing HP Unified client

Registry settings of the SafeCom Mass Deployment Tool

The Mass Deployment Tool can be configured through the following parameters specified in the registry.

Registry path:

[HKEY_CURRENT_USER\Software\SafeCom\scDeviceClone]

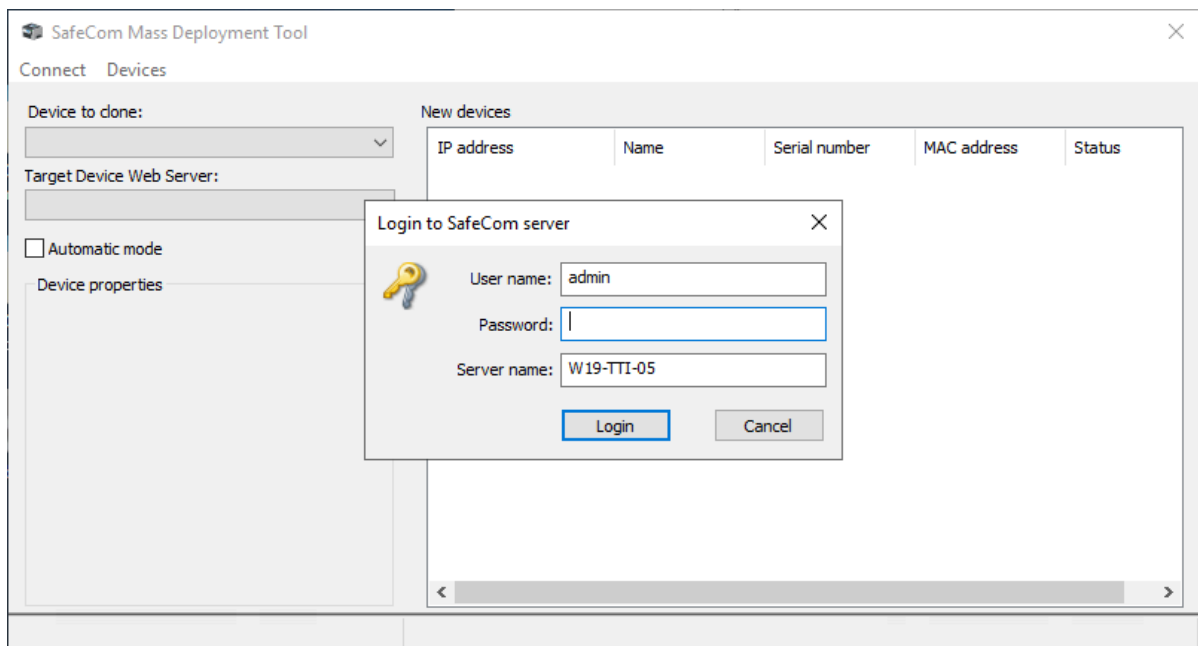
Settings:

- "Admin"="admin" is the user name used for the last successful login
- "Servername"="SERVER_NAME" is the server name used for the last successful login
- "AutoMode"=dword:00000000 handles if automatic mode is enabled by default
- "ThreadCount"=dword:00000004 is the number of worker threads executing the device registration (default is 8, accepted values are between 4 and 16)

Usage

The following is an example workflow of using the SafeCom MDT tool.

1. Add and configure a SafeCom HP Unified Client device in SafeCom Administrator.
2. Start the SafeCom Mass Deployment Tool by running **scDeviceClone.exe** in the folder where SafeCom G4 Server is installed.
3. Authenticate as a SafeCom administrator user. If the tool is running on a machine where SafeCom G4 Server is hosted, the **Server name** field is optional. Otherwise specify the SafeCom G4 Server in the **Server name** field.



Authentication screen

4. In the **Device to clone** combo box, select the device to be cloned.
5. In the **Target Device Web Server** combo box, select the DWS server where the clones will be added.

6. Add target devices.
 - a. To add target devices manually:
 1. Click **Devices > Add device**.
 2. Fill in the **IP address** or the **Hostname** of the device.
 3. Specify the administrator credentials for the device.
 4. Optional: select the **Use as default** checkboxes if you would like to use the same user name or password for subsequently added devices.
 5. Click **Add**.
 6. Repeat this process for all devices you would like to include in the cloning process.
 - b. To add target devices by importing a list of devices in an INI file:
 1. Click **Devices > Import devices**.
 2. Select the INI files that contains the list of target devices. The devices are automatically added to the list of devices to be cloned. For details on the format of the INI file, please refer to section Parameter file format for importing devices. For details on the format of the INI file, please refer to section **Parameter file format for importing devices**.
7. To remove any device from the list of new devices, select the device or devices, then click **Devices > Delete devices**.
8. To start the cloning process for the devices in the **New devices** list, click **Devices > Clone**.

Note The About dialog of the SafeCom Mass Deployment Tool is accessible by clicking the top left icon in the application screen.

Converting an existing SafeCom Go HP FutureSmart fleet to a HP Unified Client fleet

MDT enables administrators to automatically convert an existing Go HP FutureSmart fleet to a HP Unified Client fleet. To do so, manually add or import target devices to the tool, then select **Devices > Convert**. MDT guides you through the conversion process.

The embedded software must be removed from these devices in advance. The user name and password of the device administrator must be provided using the Devices > Troubleshooting menu.

Parameter file format for importing a list of new devices

The tool enables importing parameter files that contain initial data of new devices. This ini file has a predefined structure. Certain options are optional.

Note: this file contains sensitive data (device administrator passwords). It is recommended to store it at a secure place, and delete it after the import process is completed.

Defaults

In the “Defaults” section of the INI file the administrator can provide data that is applicable for multiple or all devices. The Administrator and Password settings will be in use for devices where the administrator does not specify the device’s administrator credentials.

All properties in this section are optional.

Default properties

Value name	Description	Example
Administrator	Administrator’s user name at the device	admin
Password	Administrator’s password at the device	password
UseHostname	Specifies the name – identifier – of the device at g4 and dws servers. 1 – use the device host name discovered during identification process 0 – use the name specified in this ini file	1

HPUC

The devices to add must be specified in this section. Each entry has the following format:

```
{devicename}={device IP address},{administrator name},{administrator password}
```

The device name and IP address are mandatory parameters. When these parameters are not specified for a device, the values from the “Defaults” section will be in use. Please note the following:

- the device name can only contain alphanumeric characters.
- the comma separator has to be added to each line even if the default values are going to be used.

Below are the contents of a sample parameter file:

```
[Defaults]  
Administrator=admin  
Password=defaultpassword  
UseHostname=0  
[HPUC]  
Device1=192.168.1.101,,  
Device2=192.168.1.102,,custompassword
```

Device1 is going to be added with the default administrator credentials. In case of Device2, the administrator password is different, and other parameters are the defaults.






Note The Administrator and Password values must be predefined in the Defaults section when importing from a file, even if these values are not used later in the file. Omitting these values can cause an unsuccessful import.

The cloning workflow

Once the administrator has created one device, the cloning process can start. When cloning a device, the tool performs the same steps as the Add Device Wizard in SafeCom Administrator.


Identification


When a new device is added to the MDT target list, the tool attempts to identify the device. The identification process can have the following results, indicated by a status icon and a status message in the New devices list.

Icon	Indicated status
	The device identification has not started yet. The operation will start as soon as a processing thread becomes available.
	Identification completed, the device is an HP FutureSmart device, and it is not added to any existing servers.
	Identification failed for the device. If the IP address specified for the device is incorrect, the device must be removed from the list. Errors causing this status are usually unrecoverable, the device must be removed from the list and added again.
	There were problems found during the identification process that can likely be corrected by updating parameters of the device. To start troubleshooting, double-click the device in the list, or select the device in the list, and click Devices > Troubleshooting .
	The device has been cloned successfully, it is registered in G4 and DWS.

In case of invalid device administrator credentials, a warning appears, and the Troubleshooting command allows changing both the username and password specified for the device. Please note that this warning can also result from other issues, for example inappropriate device or DWS certificates. Refer to the Kofax SafeCom HP Unified Client Administrators' Manual to check the requirements.

Cloning

When the identification process is completed, the administrator can select the devices with Identified  status, and start the cloning process by clicking **Devices > Clone**. Properties of the source device – except the administrator credentials – will be used in the configuration process when adding the new device.

When the cloning procedure succeeds, the *Registered* status message appears in the list and the sixth icon  indicates this state.

Performance, logging, error handling

Time-consuming procedures like identification, device registration and deletion are performed on background worker threads. These procedures can run simultaneously. The number of working threads is configurable depending on the number of devices to be added. The number of processing threads can be configured between 4 and 16 (the default number is 8).

If SafeCom logging is enabled on the computer where the tool is running, the details of each run can be checked in the DeviceClone*.trc logfiles.

Support for 4.3" and 2.7" devices

Overview

Starting with version 1.1, SafeCom HP Unified Client supports devices with screen sizes 4.3" and 2.7".

For 4.3" screen devices, the same workflows are supported as on 8" screen devices. For information on 8" screen devices, refer to [Using SafeCom HP Unified Client](#).

Note On 4.3" screen devices, users can specify their domain and username using the `username@domain` or the `domain\username` format.

For 2.7" screen devices, SafeCom HP Unified Client only supports Print All at Login workflows with Card only authentication. In this workflow, users swipe their card at a card reader which is attached to the device to authenticate. After authentication, all jobs in the user queue are printed automatically. User interaction is not involved on the screen in case of these small screen devices.

Screen sizes and resolutions supported by the HP Unified Client

Starting with version 1.1, SafeCom HP Unified Client supports the following HP FutureSmart screen sizes and resolutions.

Screen sizes and resolutions supported by the HP Unified Client

Screen size	Pixels	HPUC 1.1
8"	1024x768	All workflows are supported
8"	800x600	All workflows are supported
4.3"	480x272	All workflows are supported (screens are optimized for smaller size)
2.7"	320x240	Swipe and release (Print All at Login)

Device settings for 2.7" devices

When a 2.7" screen device is added, SafeCom Administrator applies the following preset properties:

Device settings for 2.7" devices

Setting	Value(s)	Comments
Licenses		
Client billing	False	Hidden field to prevent appearance of billing code screen
Login		
Login method	Card	To force the Swipe & Release feature. Property is visible with single choice
Mask user code	False	Hidden field due to lack of login screen support
Login without PIN	True	Avoid displaying login screen. Property is visible with single choice
Print All at login	True	To force the Swipe & Release feature Property is visible with single choice
Length of user ID code	39	Hidden field due to lack of login screen support
Default domain	Empty string	Hidden field due to lack of login screen support
Hide domain name	False	Hidden field due to lack of login screen support
Show domain list	False	Hidden field due to lack of login screen support
Guest login	Empty string	Hidden field due to lack of login screen support
Register card by Windows credentials	False	Hidden field due to lack of login screen support
User Interface		
Visibility of menu elements		Hidden field due to lack of Pull Print application support

Note The device stays logged in after printing all documents. Logout is required manually.

Mixed mode authentication

Introduction

Starting with version 1.1, SafeCom HP Unified Client supports configurations where external authentication/authorization agents are set up on a HP FutureSmart device. SafeCom Pull Print and Print All are still available to users, but will require further authentication to access documents in the SafeCom user's queue.

Authentication

HP Unified Client registers authentication agent when the device is added to SafeCom. HP devices enable authentication agent selection. It is designed this way to avoid scenarios when devices become inaccessible due to the failure of external authentication server. It means that the Unified Client manages authentication by 3rd party agents. Version 1.1 can cooperate with those authentication agents which share the domain and the user name of the logged-in user.

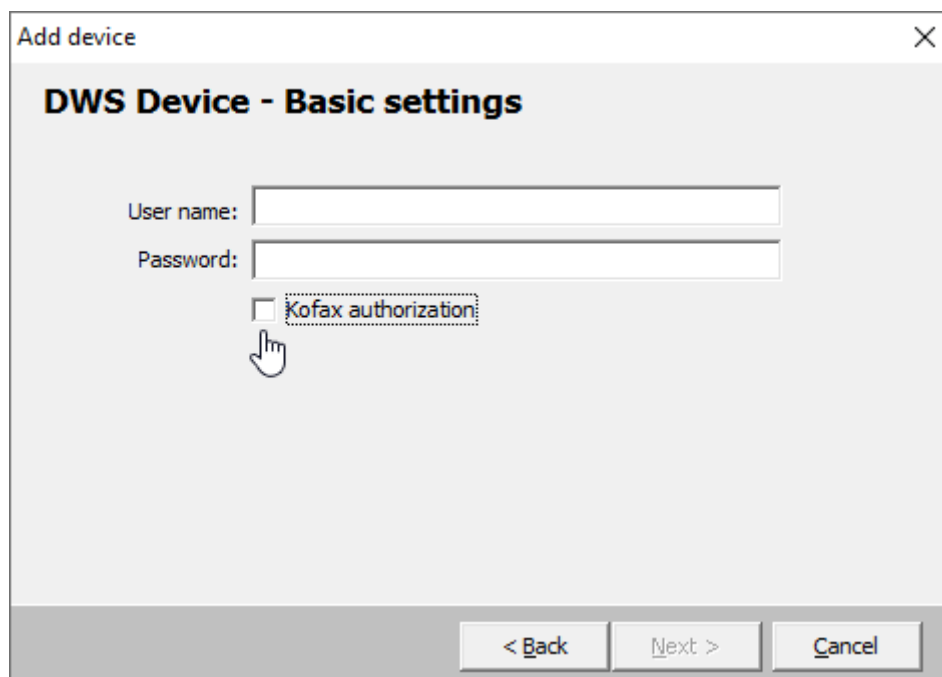
If the user is authenticated by Kofax, all operations are controlled by HP UC. This includes SafeCom features and job tracking.

The user may select other 3rd party authentication. HP UC does not control the activities of users in this case, they can run jobs freely. HP UC tracks these activities according to the tracking settings. These tracking records are not linked to SafeCom users, they are recorded in SafeCom tracking database as unattended jobs. They indicate the appropriate device and job data.

If users who are authenticated by a 3rd party agent want to use SafeCom features, for example Pull Print or Print All, an extra user identification must be performed. The Identification screen is displayed on the device when the top-level button is selected which prompts for the Windows password of the user. If the G4 server can find an associated SafeCom user for the provided credentials, and the Windows login succeeds, the requested operation can continue. This then shows the Pull Print application or prints all non-retained documents.

Authorization

HP Unified Client 1.0 registers authorization agent. It locks EWS, Security, or Access control page, which is not desirable in certain configurations. With HP UC 1.1, agent registration is optional. The Add device wizard feature of Administrator enables the activation of Kofax agent or the access control managed by other application, for example by EWS.

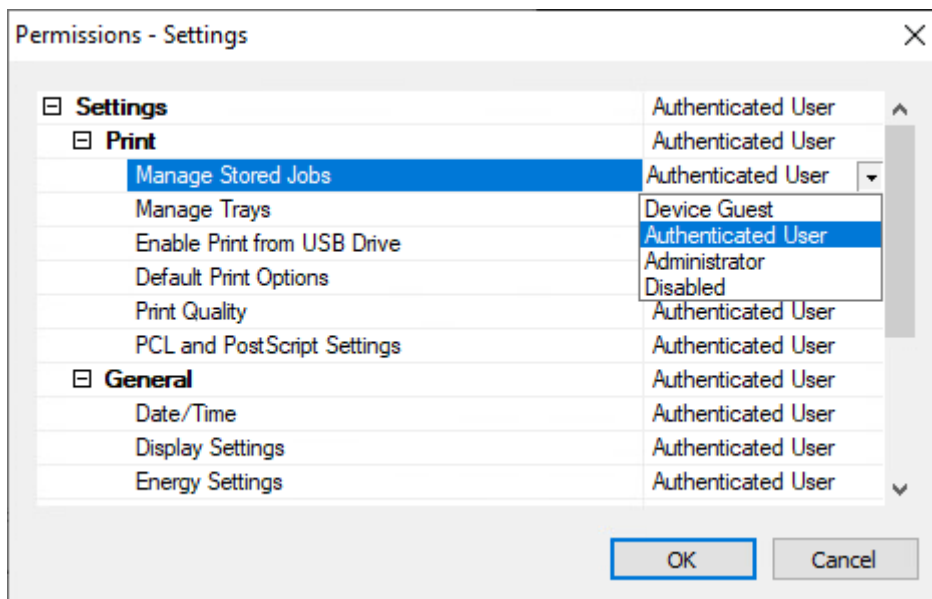


The screenshot shows a dialog box titled "Add device" with a close button (X) in the top right corner. The main content area is titled "DWS Device - Basic settings". It contains three input fields: "User name:" followed by a text box, "Password:" followed by a text box, and a checkbox labeled "Kofax authorization:" which is currently unchecked. A mouse cursor is pointing at the checkbox. At the bottom of the dialog, there are three buttons: "< Back", "Next >", and "Cancel".

Kofax authorization

If Kofax authorization is selected, the Property page of device in Administrator shows all access points and related permissions which are installed on the device. The access points are grouped under two nodes of Applications and Device features. The set of permissions associated with a given access point can be managed in a separate dialog box. The following levels of access rights exist:

- Disabled: the feature is inaccessible.
- Administrator: only SafeCom administrators are allowed to perform the operation.
- Authenticated user: the feature is accessible after successful authentication.
- Guest: the feature can be used by anyone without authentication.



Dialog box for permissions of an access point

Changing the permission level of a parent node modifies the permission level of each child to the same value. The child permissions are manageable individually. The parent node shows the most permissive access right of its children if they had different values. It is also true for the access points in Device Properties dialog.

The *Lock device* property refers to the initial screen, which is displayed to the user. When it is set to True, the mandatory sign-in screen is visible on the device. Otherwise, the home screen of the device is displayed. This behavior is bound to the permissions which are granted for guest users. If all permissions are revoked from guest users, the device is locked. The behavior of the property indicates this relation between the permissions and the user experience. If the property is set to True, all permissions that was previously set to *Guest* are changed to *Authenticated user*. Also, when a permission is granted to the *Guest* the property is changed to False. So, the level of permissions and the value of the property is continuously synchronized.

HP authorization

If Kofax authorization is not selected in Add device wizard, the agent is not registered on the device. The Device Properties windows does not show the tree of access points and permissions. The access control of the device must be managed in the standard user interface of EWS or by another third party tool.

The granted permissions affect how HP UC presents the Welcome and Login screens. When the device is locked, these screens allow the preselection of the function before login. This is done by displaying the Quick Select Bar.

The only property in the Access Control group in the Device Properties window is the *Lock device* in this mode. It must be set according to the final set of permissions. If guest users are not allowed to use the device, the value of this property must be set to True. Synchronization of the permissions and the *Lock device* property is important to show Quick Select Bar.

Note Pull Print and Print All buttons must be set up to have Kofax authentication as default.

SafeCom HP Unified Client - 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. Log in to SafeCom Administrator.
2. Click **Devices** in the left-hand menu, and then select the desired device in the list.
3. Right-click on the device, then select **Device properties** from the context menu. The **Device properties** dialog box appears.
4. On the **Device configuration** page scroll to the **Login** section, then select one of the values for the **Login methods** property.

Choose from the following:

- Auto-sense
 - If there is a card reader attached, then login by card or entering Windows credentials are enabled.
 - If there is no reader attached, then user can authenticate by entering ID code (and maybe PIN code).
- ID code
- Card
- ID code or card
- Windows authentication

Note Identification by card requires the installation of a SafeCom ID Device (card reader).

5. Click **OK** to save the settings and close the dialog box.

Note Devices supplied with 2.7" control panel support Card-only authentication. You cannot change this property in SafeCom Administrator for this type of devices.

Control user access rights

An initial decision about authorization must be made when a new device is added to SafeCom. SafeCom is allowed to control access rights to the device or another application – typically by EWS by Security or Access control page. Permissions can be granted for a certain group of users. A device or its access points can be used by the following categories:

- Used by administrators
- Used by every authenticated user
- Used by anybody without authentication (also called guest access)
- Disabled and prohibited to use by anyone

Kofax authorization

This option can be set at the Basic settings page of the Add device wizard in SafeCom Administrator. The Device properties dialog box presents a complete permission set, which is retrieved from the device in a form of permission tree. This is similar to how the EWS page shows it. Lock device property handles guest access, which means that anybody without authentication can use the device.

Note Choosing this option, Kofax authentication is set as default for each access point, but users can select other authentication method if it is allowed.

3rd party authorization

If the Kofax authorization check box is turned off at the Basic settings page of the Add device wizard in SafeCom Administrator, SafeCom does not install the authorization agent at the device. EWS, Security, Access Control page, or other third-party applications can be used to set up function access control.

Note Depending on the enabled guest permissions in the third party application, the Lock device property must be set properly in SafeCom Administrator. If the guest does not have permission on the device, the device is locked.

Note It is mandatory to set Kofax authentication as default for Print All and Pull Print applications.

User level permissions

The Kofax authenticated users are those users who selected the Kofax authentication at login. The function access of the Kofax authenticated users can be controlled by user properties on the Settings tab of User properties dialog box, in the Access rights section if Kofax authorization is selected. Selecting the appropriate check box enables a function, and clearing the box disables it.

Control access rights for the following features can be controlled:

- Copy
- Copy in color

- E-mail
- Scan
- Fax
- USB memory print
- USB memory scan
- Print all button

This means that the permissions of authenticated users can be fine tuned per user basis.

Note These settings are user-based and device capabilities are not considered. For example Scan permission is not applicable on printer only devices.

Further considerations

HP Unified client has complete control over the access control if the user is logged in by the Kofax agent and the Kofax authorization is enabled.

If the user is logged in by third party authentication, and Kofax authorization is enabled, all access rights are granted to the user because SafeCom user is not associated with this user and no user level permissions are available.

In case of 3rd party authorization, access control is not managed by the Unified Client.

Note SafeCom functions can be used by users logged in through Kofax authorization, or in case of 3rd party authentication, after a user identification.

Enable Client Billing on the device

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

1. Enable **Client Billing** on the Device configuration tab in the Device properties dialog in SafeCom Administrator:
 - a. Log in to SafeCom Administrator.
 - b. Click **Devices** in the left-hand menu, and then select the desired device in the list.
 - c. Right-click on the device, then select **Device properties** from the context menu. The **Device properties** dialog box appears.
 - d. On the **Device configuration** page in the **Licenses** section select the **True** value for the **Client billing** property.
 - e. Click **OK** to save the settings and close the dialog box.

2. Enable **Bill clients for cost** on the **Settings** tab in the **User properties** dialog in SafeCom Administrator.
 - a. Log in to SafeCom Administrator.
 - b. Click **Users** in the left-hand menu, and then select the desired user(s) in the list. You may select multiple users.
 - c. Right-click on the user(s), then select **User properties** from the context menu.
 - d. Make sure that **Bill clients for cost** is selected in the Print documents section of the Settings page.

Tip If the **Bill clients for cost** check box is disabled, then select either the **Tracking** or the **Pay** option in the **Cost control** section below.

- e. Click **OK** to save the settings and close the dialog box.

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 via 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.

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

1. Open the device's embedded web server web page in a web browser and log in.
2. Click the **Scan/Digital Send** tab.
3. Click **Scan to Network folder** > **Quick Sets** on the left menu.

Note A Quick Set for Scan to Network Folder requires user credentials to retrieve the network folder path from the network directory. A network sign-in method should be selected for the device before using the Home Folder feature.

4. Select **Add** or **Configure**, as appropriate.

Note Use the **Previous**, **Next**, **Finish** and **Cancel** buttons on the bottom right to navigate between the pages of the wizard.

The Quick Sets Setup Wizard starts.

5. Specify **Quick Set Name**, **Quick Set Description** and **Quick Set Start Options**.

6. Navigate to the Folder options page. Select 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.
7. Optionally, navigate between the rest of the pages and set up details in the Notification, Scan Settings, and File Settings pages.
8. Click **Finish** to save the Quick Set.
9. Login to SafeCom Administrator.
10. Set the Home Folder for users via 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**.

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

Determine the DWS version

You may check the version of the **SafeCom Device Web Server** the following way:

In **SafeCom Administrator**, select **Device servers** from the left-hand pane. The version number is displayed in the Version column. If the server is the member of a group, the group must be selected in the tree view. The left pane shows the version number.

Determine the HP Unified Client version

You may check the version of the **HP Unified Client** the following way:

At the device, tap **About** in the menu. The version number is displayed in the about box. The device shows version 1.1.<revision>.<build number> in Safecom Administrator device pane.

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.

Note The device needs to be up and running, connected to the network, to be able to send tracking data to the SafeCom server. Disconnecting or powering off the device while some tracking data is still pending may result in inaccurate tracking.

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 Safecom

Push port. By enabling the Print post-tracking device configuration setting 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

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 (based on the cost calculated from the post tracking data), and the job status is set to Completed. In pay environments, the price is recalculated and the pay user's balance is modified via 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.

Tracking record	
Field	Value
Job	
Name	Test Page
Generated	9/17/2015 10:10:31 AM
Size	0 B
Paper	A4
Duplex	No
Color	No
Driver	HP Universal Printing PCL 6 (v6.0)
Type	PUSH
Destination	
User	
ID	3
User logon	CARD
Full name	
Description	
Cost code	N/A
Device	
ID	11
Name	M630
Model	HP LaserJet MFP M630
Location	N/A
Duplex	Yes
Color	No
MAC	fc15b478cdc1
Page count	
Tracking state	PENDING
Tracking pages	1
Driver pages	1
Parser pages	1
Color pages	0
Sheets	1

- 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 via 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, under **User properties > Account**. 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:

ID	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 Saines PC.pdf	-15,10	-	184,90
372	10-02-2016 16:16:49	USER 1345	Push Printing	Push Print: A4 3 pages Saines 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 Saines 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

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.

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 an 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.

The Tracking service can be configured in online or offline mode in a multi-server environment. The final storage location of the tracking data is always the Safecom Primary server. In online mode, the records are created on the primary server database immediately. In 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.

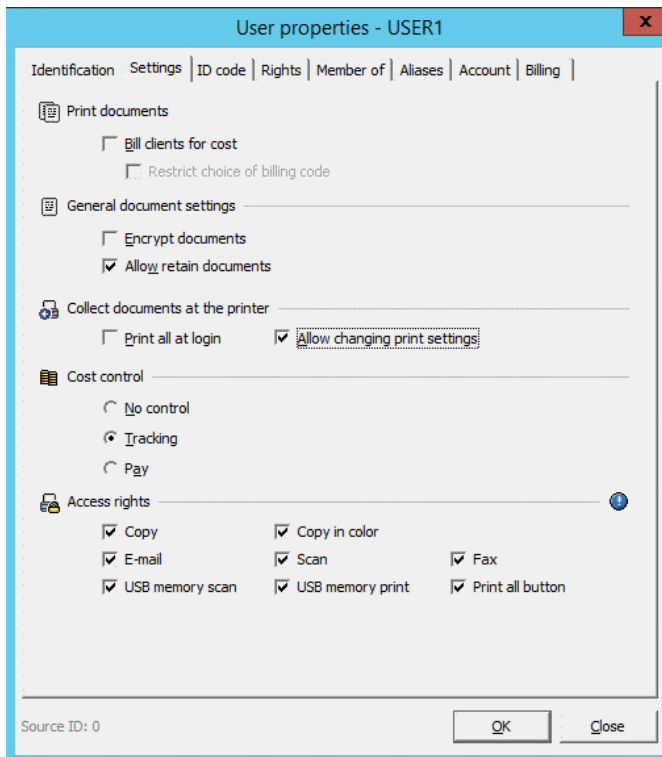
If the device fails to send the post tracking data (because of the device home server being unavailable), it is stored and the device resends it after the next printing.

Note Since the SafeCom Web Interface is configured to use the primary server, users see their tracking data after the scheduled tracking collection.

Note Secondary prices may be different, as they are calculated only on the server side.

Configure users and devices to allow modifying job settings

The Force Mono-Duplex (FMD) feature allows the users 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.



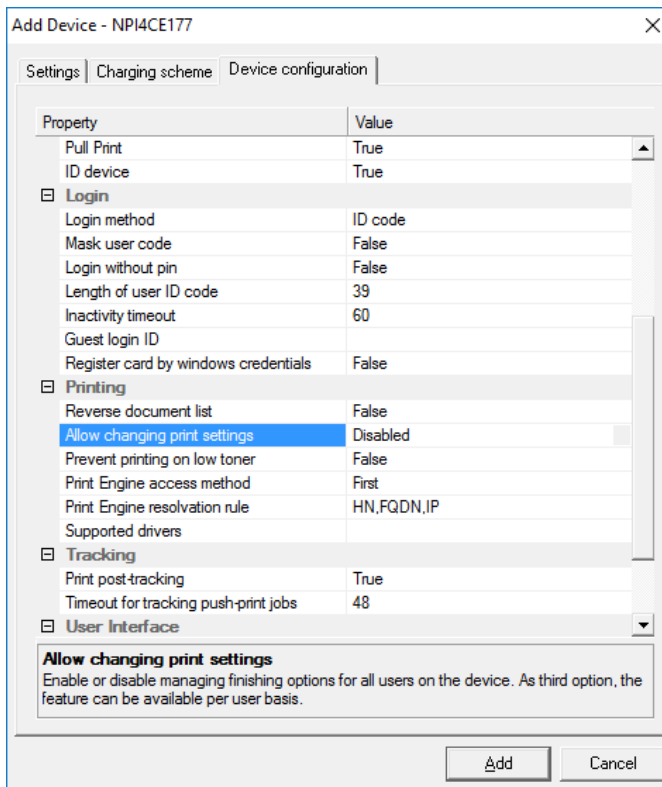
The figure above indicates how the feature can be enabled for a user by setting the **Allow changing print settings** option. The setting can be managed for a group of users if the **Property** dialog is opened when multiple users are selected from the user list. If applied, users can see the relevant control icons on the device.

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

The setting for the device can be controlled in SafeCom Administrator.

Open the device property page in SafeCom Administrator. On the **Device configuration** page 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.
- **Per user setting** – the device enables or disables the features according to the currently logged on user's settings.



Note 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.

Uninstall SafeCom HP Unified Client

Note Deleting the device not only detaches it from the SafeCom server but also uninstalls the HP Unified Client from the device. If the same device connects to multiple SafeCom servers, then uninstallation makes the device inaccessible to those servers also.

1. Log in to SafeCom Administrator.
2. Click devices in the left-hand menu, and then select the device from which the SafeCom solution must be uninstalled.

3. Perform any of the following steps to remove the device:
 - a. Right-click on the device, then select **Delete device** from the context menu.
 - b. Click the **Delete** icon in the top menu.
4. Click **Yes**.

Note After uninstalling a device the icons on the device screen do not disappear automatically, it must be reset. In other cases, the KOFAX sign-in method remains registered on the device.

Relocate DWS application log folder

Relocation of your log folder to a more accessible path pays off when archiving log files or contacting support. Do the following to relocate log files to the `C:\safecom_trace` folder, which is the established position of application logs in SafeCom solutions.

1. Locate your DWS folder, which is `C:\Windows\System32\config\systemprofile\AppData\Local\Nuance\Integrated\DWS\webserver\conf` by default.
2. Open the `DWSSettings.properties` file in a plain text editor, such as Notepad.
3. Append a new line with the `LOG_FILE_PATH` setting, specifying the new location for log files:

```
LOG_FILE_PATH=C:\\safecom_trace
```

Note If the file already has the `LOG_FILE_PATH` setting, then edit the existing line instead.

Note Make sure to use a double backslash when separating the drive name (C:) from the path.

4. Save the changes and close the plain text editor.
5. Restart the Device Web Server service.

SafeCom DWS will save the application log files into the `C:\safecom_trace` folder from now on.

SafeCom HP Unified Client device trace facility

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

1. Log in to SafeCom Administrator.
2. Click **Servers** in the left-hand menu, and then select the desired server in the list.
3. Right-click on the server, then select Server properties from the context menu.
4. Make sure that the check box **Write event to Windows event log** is selected on the Server page.
5. Click OK to save the settings and close the dialog box.

To check the logged events, right-click on the server, then select Event log from the context menu.

In case you need to provide logs, visit the following locations and gather the files within.

Note Compress the log files in ZIP format prior sending to the support team.

- Client side log:

```
https://<your device ip address>/hp/device/oxpd/oxpdlog.txt
```

- Application log:

```
C:\Windows\System32\config\systemprofile\AppData\Local\Nuance\Integrated\
DWS\webserver\webapps\DwsMain\WEB-INF\felix-cache\<bundle folder with log>\data
```

Locate the DATA folder under the bundle*** folders (e.g. bundle177).

Tip It is recommended to set up a more accessible location (C:\safecom_trace by standard) for the application log files. See [Relocate DWS application log folder](#) for details.

- Web server log:

```
C:\Windows\System32\config\systemprofile\AppData\Local\Nuance\
Integrated\DWS\webserver\logs
```

Chapter 3

Using SafeCom HP Unified Client

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

Login

The login sequence is initiated if you are not already logged in and tapped any icon (such as **Pull Print** or **Copy**) that requires SafeCom to handle **MFP authentication**.



Device Main Screen

If the copy function requires SafeCom authentication pressing the green **Copy** button will also initiate the login sequence. Once logged in the documents placed in the automatic document feeder (ADF) will be copied. If Print all at login is selected on the server in **User properties** > **Settings** then HP Unified Client devices will print all documents at login, excluding retained ones.

The recommended login sequences are described in the following chapters:¹

- [Login with card](#)
- [Login with card and PIN code](#)
- [Login with ID code](#)
- [Login with ID code and PIN code](#)
- [Login with Windows](#)

Note Do not power off the device prior to Logout (see [Logout](#)). The device needs to be up and running, connected to the network, to be able to send tracking data to the SafeCom server. Disconnecting or powering off the device while some tracking data is still pending may result in inaccurate tracking.

Note After adding the device to SafeCom, the first login may take a longer time.

Login with card

Use the card reader.

¹ 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.

Login with card and PIN code

1. Use the card reader.
2. Enter **PIN code** on the touch-screen or on an optional external keyboard.
3. Tap **OK**.

Login with ID code

1. Tap **Sign In** (or press the green **Copy** button to copy).
2. Enter **ID code** on the touch-screen or on an optional external keyboard.
3. Tap **OK**.

Login with ID code and PIN code

1. Tap **Sign In** (or press the green **Copy** button to copy).
2. Enter **ID code** on the touch-screen or on an optional external keyboard.
3. Tap **OK**.
4. Enter **PIN code**.
5. Tap **OK**.

Login with Windows

If **Login method** is set to **Windows authentication**, it is possible to log in by entering your Windows login credentials:

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

Note **User name** cannot be blank.

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

Note **Password** cannot be blank

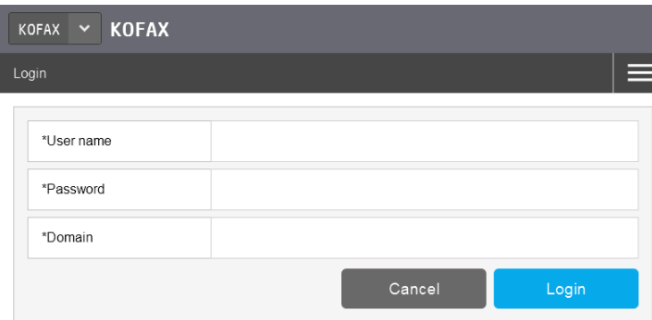
4. Tap **OK**.

Register card at device with Windows credentials

Tip *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 section [Register card at device with PUK code](#)).*

Tip For Windows authentication, the card reader cannot be used. To use a card reader and Windows authentication, users should select Auto-sense.

1. Use the card reader and if the card is unknown the **SafeCom Card Registration** page appears.

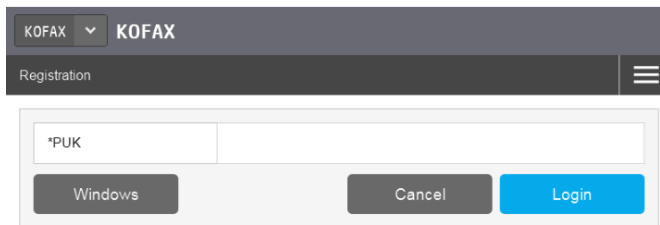


The screenshot shows a login interface for a KOFAX device. At the top, there is a header with 'KOFAX' and a dropdown menu. Below the header is a 'Login' button and a hamburger menu icon. The main area contains three text input fields labeled '*User name', '*Password', and '*Domain'. At the bottom right, there are two buttons: 'Cancel' and 'Login'.

2. Specify the appropriate domain in the **Domain** text box.
3. Tap the **User name** field and enter the Windows user name on the touch-screen or on an optional external keyboard. Tap **OK**.
4. Tap the **Password** field and enter the Windows password. Tap **OK**.
5. Tap **OK**.
6. The card is now registered and the user is logged in.

Register card at device with PUK code

1. When using a 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.



The screenshot shows a mobile application interface for registration. At the top, there is a dark header bar with 'KOFAX' on the left and a dropdown arrow. Below the header, the word 'Registration' is displayed on the left, and a menu icon (three horizontal lines) is on the right. The main content area features a text input field with the placeholder text '*PUK'. Below the input field, there are three buttons: 'Windows' (dark grey), 'Cancel' (dark grey), and 'Login' (blue).

2. Tap the **PUK** field and enter the PUK code on the touch-screen or on an optional external keyboard.
3. The card is now registered.

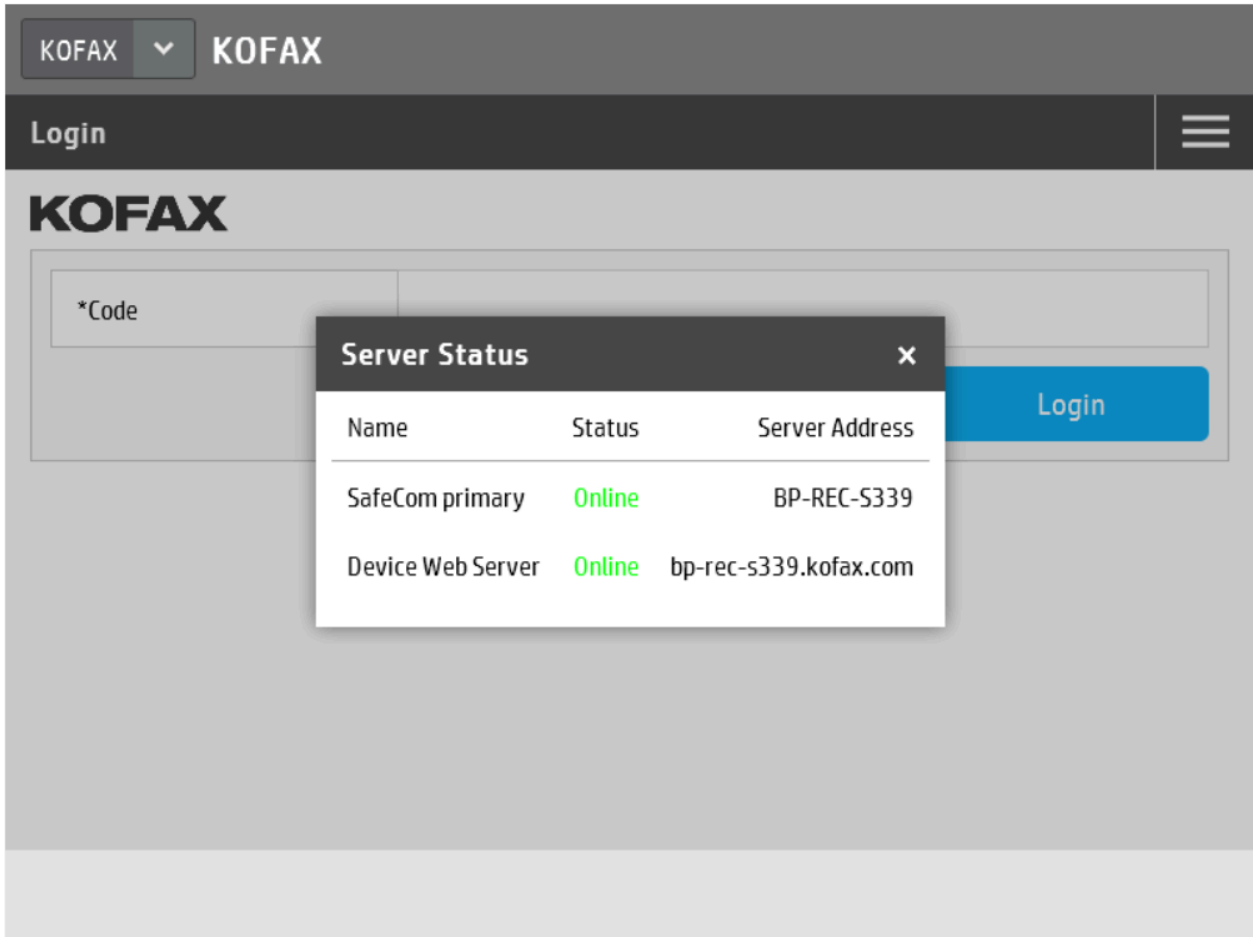
Change PIN code

If users are allowed to change their PIN, Change PIN screen appears after successful card registration. The new PIN code must be confirmed by entering it twice.

If the card was registered by PUK code the Change PIN screen appears after the user's first successful login.

Server status verification

Users can check the availability of the server using the drop-down menu of the Login screen. DWS and SafeCom G4 server status can be verified this way. It is useful in case of failover situations, because the window shows the current state of the controlling DWS server and G4 server.



Server information

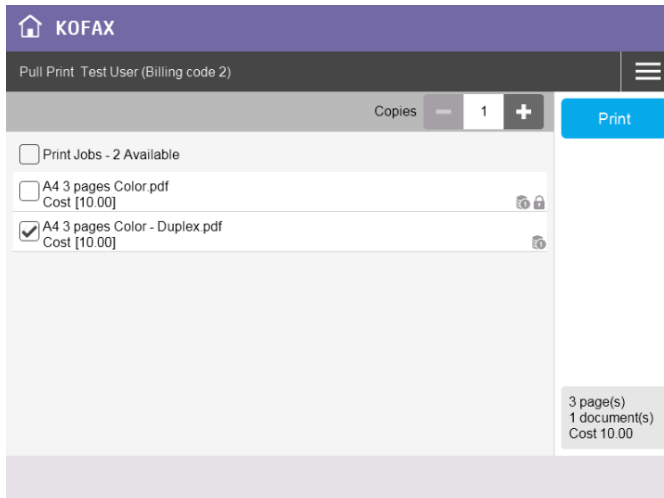
The server information window has the following statuses:

- The green Online label shows that indicates that the servers are available, they function normally.
- The yellow connecting status message shows that the server is available, but the connection is not established yet.
- The red Offline label means disconnected servers. The device is only usable if both G4 and DWS are online.

Note The device show another error message if it has no direct connection to its controller DWS server.

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 by default. The administrator can change the order of the job list.



In the document list, the following icons may mark the document:

- : shows the document is retained.
- : shows the document has a billing code.
- : shows the document is delegated. Tap the Info button to see information about who delegated the document.
- : shows the document is group printed.
- : shows the document is forced to print in black and white.
- : shows the document is forced to print in duplex.
- : shows the document fidelity is low and the document may print incorrectly.

The printing cost of the document (for example, **1.60**) is below the document name.

- 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 .
- 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.

Note The controls of the finishing options, which are Force duplex or Force mono print, are shown before the control of the copy number if the user is allowed to perform these operations.

Copy

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

Folder

Tap the Scan icon, then tap the Scan to Network Folder icon to scan and send the document to a folder.

E-mail

Tap the Scan icon, then tap the Scan to Email 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 touch-screen or on an optional external keyboard. Tap the **Send** button to scan and e-mail the document.

Selecting a Billing Code

If billing codes are enabled by the administrator and the device is supplied with Client billing license, the following screen appears during the login process. In this case, the user is required to select a billing code.



The screenshot shows a mobile application interface for selecting a billing code. At the top, there is a dark header with 'KOFAX' and a dropdown arrow, followed by 'KOFAX'. Below this is a 'Billing Details' section with a hamburger menu icon on the right. The main content area contains a form with the following elements:

- A field labeled '*Select filter type' with the value 'Favorites' and a three-dot menu icon to its right.
- A field labeled '*Select details' with a magnifying glass icon to its right.
- A checkbox labeled '*Billable'.
- At the bottom, there are two buttons: 'Cancel' (grey) and 'Done' (blue).

The screen offers the following:

- Select filter type: Filter the list of billing codes by the options below:
 - Favorites
 - Last used
 - Personal

Note If Personal is selected, the tracking data will contain “Personal” as the code, and “Used for personal billing” as the description. This differentiates it from the tracking data not subjected to billing (for example data from a device which does not have a billing license).

- Select Details: This box is active if Favorites or Last used was chosen in Select filter type. Searches among billing codes.
- Billable: Select this check box to use the selected billing code in invoicing. If this check box is cleared, then the selected billing code is still applied, but not detailed in the customer invoice.

Note This check box is only available if the administrator has recorded the selected billing code as billable.

Logout

There is a configurable Inactivity timeout that defaults to 60 seconds. The logout process is initiated if the user does not interact with the screen or any other device buttons.

Note Set a high Inactivity timeout value in order to avoid undesired automatic log out during those time-consuming operations not requiring any user interaction on the device screen. See [At the Printer: Undesired timeout](#) as a troubleshooting example.

To log out actively perform one of the following actions:

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

Note The Cancel print jobs after unattended error feature is disabled by default. If this feature is enabled, then jobs pending due to unattended errors, such as paper jam or out of paper, will be automatically deleted from the print queue as the user logs out. Visit **Security > General Security > Printing > Cancel print jobs after unattended error** on the HP device web page to enable or disable this feature.

Note If you experience users being intermittently logged out during workflows, check [At the Printer: Undesired timeout](#) for a solution.

Chapter 4

Troubleshooting

Introduction

This chapter contains troubleshooting hints for the SafeCom HP Unified Client product. Additional troubleshooting hints are available in the Troubleshooting chapter in the *SafeCom G4 Administrator's Manual* (D60650).

At the Printer: Card reading not working

- Is the card reader powered and firmly connected?
- Is the card compatible with the reader?
- Make sure you used the correct VID/PID values when adding the device to SafeCom Administrator.
- If the card reader was added or changed after adding the device to SafeCom Administrator, then you need to remove the device and add it again together with its card reader.

At the printer: Card swipe results in unexpected behavior when using 3rd party authorization

Card swipe results in unexpected behavior when using 3rd party authorization.

Solution: Do not use card authentication when using 3rd party authorization, because this is not a supported scenario.

At the Printer: Device freezes as Register with Windows credentials pressed

If the device is installed in DLA mode and Card is selected for login method then tapping the Register with Windows credentials button may result in a freeze. The Present your card screen appears and the device does not react to further card swipes.

Solution: Use HP devices with firmware version 24.7.2 or newer.

At the printer: Handling stale connections by G4 server

After a longer period of inactivity (sleep) of device time, the G4 server closes connection. It can cause issues, for example failed login or connection problems in the first user session, which reactivates the device. The second login attempt is successful.

Solution: The G4 side behavior is configurable with the following registry settings:
HKEY_LOCAL_MACHINE\SOFTWARE\SafeCom\SafeComG4

TcpServerLogicalSocketTimeout (default is 3600000 ms, 1 hour): logical connections represented by devices

TcpServerSocketTimeout (default is -1 infinite): physical connections.

At the Printer: SafeCom inactivity timeout does not work on device home screen

SafeCom timeout does not work on the home screen or on native application screens, for example Copy. SafeCom timeout does not work on screens other than SafeCom screens.

Solution: Please use the device timeout.

At the Printer: Sign-in failed

If a DWS is registered by host name then Sign-in on the device will fail in network environments lacking name resolution.

Solution: Provide name resolution on the network.

Workaround: Open the Server Properties dialog box in SafeCom Administrator and update the IP address manually in the Server address box.

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** value is set to True under **Device properties > Licenses** in SafeCom Administrator.

At the Printer: Undesired timeout

If you experience users being intermittently logged out during workflows, it is recommended to use the device's native timeout feature instead of SafeCom's inactivity timeout to control automatic logout.

To do so, increase the SafeCom inactivity timeout to a large value (such as 3600 seconds), and set the device's timeout at **General > Control Panel Customization > Display Settings > Inactivity Timeout** to the desired timeout value. (See [Inactivity timeout](#) for details.)

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.

This error disappears when SafeCom is installed on the device.

This error also may occur if the card reader was added with an invalid VID/PID.

At the Printer: User cannot log out until the last job is spooled

When printing a large number of jobs or a large number of copies of the same job, a user cannot log out from the device until the last job is spooled to ensure correct accounting. This may cause a delay in logging out for users who are printing a large number of documents.

Add device to device controller service failed error

SafeCom HP Unified Client allows using special characters in device passwords but using some of these characters may result in unexpected behavior. The following special characters are safe to use:

- + * ? ! % = . \$ / { } _ , () :

Workaround: It is not recommended to use any special characters other than the ones in the list above in device passwords.

Certificate generation for DWS fails

If certificate generation fails for the DWS server, ensure that the server has a valid FQDN (Fully Qualified Domain Name), and DNS name resolution works.

Incorrect tracking information

Using non-supported drivers for Pull Print may result in incorrect tracking information. There are known issues with Kyocera ClassicUniversalDriver_v31.

Solution: Use a supported driver.

OXPd Application Error - Mime type not supported

This error message appears if you try to print to a device which has a name that includes accented characters.

Solution: Remove the device from SafeCom, then add the device again, specifying a name without accented characters in Name. For details, see number 8.

Prevent low toner feature does not work

Some HP devices do not notify on low toner level, though Low Warning Tresholds are set correctly and Low Warning Treshold Message is enabled on the device. (Meanwhile, the Document Feeder Kit Low message displays correctly.) This causes SafeCom's Prevent low toner feature fail.

Prices do not match

Price1 and Price2 can be different in case of using a paper size unsupported by SafeCom or the device.

Use the kind of media supported by both SafeCom and the printing devices in order to keep consistency.

Problems when adding a device - valid certificate required

To install SafeCom HP Unified Client on a HP device, a valid certificate must be present on the device. If the certificate is invalid, then adding the device fails.

Possible causes:

- If the certificate changes on the device (for example, due to certificate regeneration) then the device may need to be re-added to SafeCom.
- Using Partial Disk Clean may result in invalid certification if using a self-signed certificate.
- Any changes altering time zone settings can result in a certificate validation failure.

Solution: Remove the device, then create a new certificate and add the device again.

Problems when adding a device - device already configured

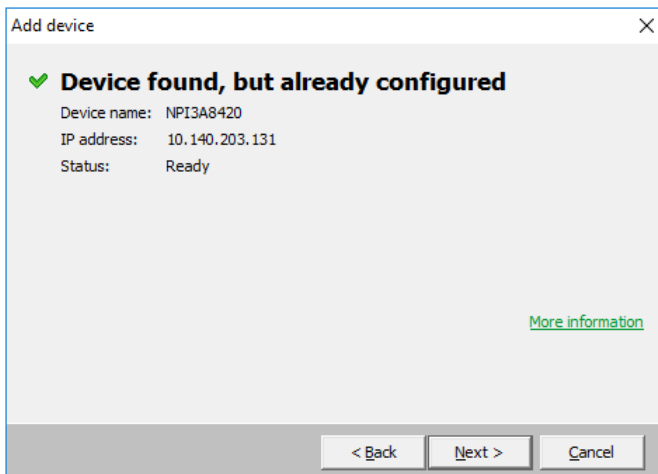
It might happen that the device to be added to the SafeCom system has been configured before. In this case you should follow the troubleshooting procedure that fits your situation.

The device is registered in the SafeCom database

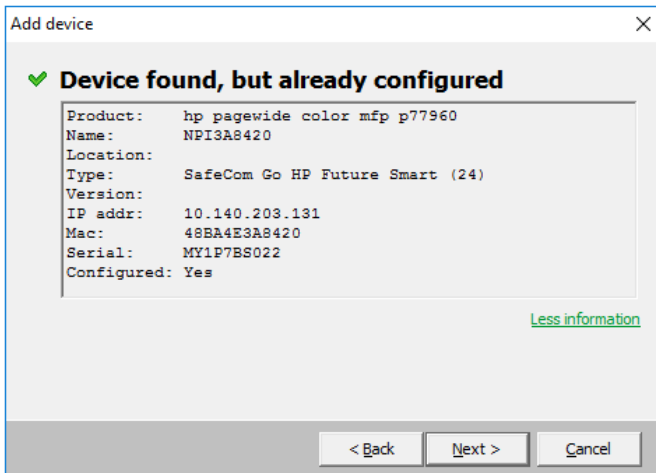
If the device exists in the SafeCom database and it is assigned to one or more servers then there is no way to add it again. The SafeCom Administrator displays a warning and optionally shows the property dialog of the device.

The device is registered in the DWS

It may lead to inconsistency if a device has been deleted from the SafeCom database while the corresponding Device Web Server was temporarily out of order. The device remains registered in the Device Web Server, but it is missing from the SafeCom database. When you try to add this device again, the Add Device wizard displays the following screen:



Optionally, click More information to verify that the device already has been added to the selected Device Web Server:



If you continue with the Add device wizard (click Next), then the wizard performs the following steps:

1. Removes the device from the Device Web Server.
2. Registers the same device to the Device Web Server again.
3. Adds the device to the SafeCom database as a new device.

Problems when adding a device - device is not discoverable

If IPP (Internet Printing Protocol) is not enabled on an HP device, then the Add device wizard fails to add the device. Do the following to fix the problem:

1. Log in to the device.
2. Navigate to **Networking > Other Settings > Misc. Settings** on the device web page.
3. Make sure to enable Internet Printing Protocol by selecting the IPP Printing and IPPS Printing check boxes, then save the settings.
4. Start over the Add device wizard and complete the installation. (See [Add the device via SafeCom Administrator](#) for details.)

SafeCom HP Unified Client has incorrect IP address

SafeCom does not support TCP/IPv6, so if you are in such an environment you must disable the use of TCP/IPv6.

Sign-In methods are disabled on the device

Installing an authorization agent (such as SafeCom) on HP FutureSmart 4 devices disables all manual authorization controls. Users may not be able to manually configure authorization on the affected devices once SafeCom is installed.

Signing in message appears while canceling

"Signing in" message appears if the user taps Cancel during authentication on the ID Code screen. This issue has no effect on functionality.

Unable to find device

When using a Push port, the Unable to find device error message appears after a device was removed and then added again.

To solve this problem, remove the device in SafeCom Administrator, then add it again with another push port.

Unexpected unattended push prints appear

If you see any unsolicited unattended push prints, then make sure that the device is not in use as a TCP/IP printer.

Wrong tracking or negative balance of the user in case of duplex printing.

When using duplex printing or printing more copies of the same document, the balance of the user can go under zero. Normally, when not using duplex or printing more copies of the same document, SafeCom does not allow that the balance goes under zero. The user cannot continue printing if the balance is under zero.