

# Kofax SafeCom G4 Server Web Interface Administrator's Guide

Version: 10.7.0.1

Date: 2023-10-17

**KOFAX**

# Table of Contents

<b>Chapter 1: Introduction.....</b>	<b>5</b>
SafeCom Web Interface.....	5
SafeCom ePay.....	5
Related documentation.....	5
About this manual.....	6
<b>Chapter 2: Installation and configuration.....</b>	<b>7</b>
Prerequisites.....	7
Install SafeCom Web Interface.....	7
Command line installation.....	8
Manual firewall configuration.....	11
Restart the web server.....	11
Test the web server using a browser.....	11
Configure SafeCom Web Interface.....	11
Configure PayPal as provider.....	13
Customize and translate ePay email message.....	14
Setup ePay Cash Card.....	14
Enable SafeCom Web Interface trace files.....	15
Configuring Kerberos delegation.....	16
Configuring constrained Kerberos delegation.....	16
Configuring resource-based constrained Kerberos delegation.....	18
<b>Chapter 3: Using SafeCom Web Interface.....</b>	<b>22</b>
Log in.....	22
Managing pending print jobs.....	23
Managing scanned files.....	23
View transactions.....	24
Transfer money through ePay.....	24
Managing PayPal transactions.....	25
Manage client billing.....	27
Client billing settings.....	27
Assigning billing codes to completed jobs.....	28
Manage delegates.....	29
Send request.....	29
Pending requests.....	29
Collect my documents.....	30

- Submit documents to me.....30
- Manage codes and set up language..... 30
  - Change PIN.....30
  - Manage PUK and ID codes..... 31
  - Change default language..... 32
- Select appearance.....32

© 1995-2023 Kofax. All rights reserved.

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

## Chapter 1

# Introduction

## SafeCom Web Interface

With SafeCom Web Interface, users can use a standard web browser to see a list of their documents on the SafeCom server. In SafeCom Pay environments users can see their current balance and transactions made on their SafeCom account.

## SafeCom ePay

SafeCom ePay is an add-on to SafeCom Web Interface. SafeCom ePay allows users to deposit money into their SafeCom account through the internet.

Prerequisites:

- A SafeCom license key code supporting SafeCom Pay.

When a user makes a purchase, the user's information is transmitted over a secure connection to the payment-processing gateway which in turn verifies the information against the issuer. If the information is verified, SafeCom ePay gets a response back from the gateway and deposits the equivalent amount into the user's SafeCom account.

SafeCom supports the following providers:

- PayPal (2.8.1)

## Related documentation

For additional information regarding SafeCom, see the following document:

### **Kofax SafeCom G4 Server Administrator's Guide**

A comprehensive manual that the administrators should consult to make a successful SafeCom solution. Includes information about SafeCom Tracking, SafeCom Rule Based Printing, SafeCom Client Billing, and SafeCom Pay.

## About this manual

This manual applies to SafeCom G4 Web Interface version 10.7 and SafeCom G4 Server version 10.7.

## Chapter 2

# Installation and configuration

This section describes the prerequisites, installation process, and configuration of the SafeCom Web Interface.

**i** SafeCom Web Interface 10.7 requires SafeCom G4 Server 10.7 or newer. Previous versions of SafeCom Web Interface are compatible with SafeCom G4 Server 10.7.

## Prerequisites

To install the SafeCom Web Interface, the following options must be enabled in the IIS configuration:

- **Common HTTP Features**
  - Default Document
  - HTTP Errors
  - Static content
- **Health and Diagnostics**
  - HTTP Logging
- **Performance Features**
  - Static Content Compression
- **Security**
  - Request Filtering
  - Windows Authentication
- **Management Tools**
  - IIS Management Console

The installer requires the site to have enable HTTPS enabled and supplied with a certificate. The application can be installed on a secure site only.


## Install SafeCom Web Interface

To install the SafeCom Web Interface:


1. Download the `KofaxSafeComWebInterface-nnn.exe` file from the link supplied to you.
2. Run the downloaded file as administrator.

The SafeCom Web Interface Setup Wizard appears. It is recommended to close all other windows before continuing.

3. Click Next.
4. Read and accept the License Agreement then click Next.
5. Select the target IIS Website from the drop-down list and click Next.

 The list only contains secure web sites that run on this server. Check the configuration of the desired site if it is not shown in the list.

6. Enter the desired Web alias and click Next.
7. Enter the SafeCom server IP address or hostname then Click Next.
8. Select the installation folder and click Next.  
The default location is:  
`C:\Program Files\SafeCom\WebInterface`
9. Click Install to start the installation.

 Depending on the current configuration of the server, the installer may deploy a few missing redistributable packages too.

10. After the automatic IIS configuration, click Next.
11. Select the desired restart method and click Finish to finish the installation.

## Command line installation

Following command line parameters can be used to achieve the desired behavior during deployment.

### **/SILENT, /VERYSILENT**

Instructs the setup to be silent or very silent.

When the setup is silent, the wizard and the background window are not displayed, only the installation progress window is displayed. When the setup is very silent, the wizard and the background window, and the installation progress window are not displayed.

Other functions appear as normal, for example error messages during installation are displayed.

If the setup is silent and a restart is necessary and the `/NORESTART` command is not used (see below), the setup displays a Reboot now? message. If it is very silent, it will reboot without asking.




### **/SUPPRESSMSGBOXES**

Instructs the setup to suppress message boxes. Only has an effect when combined with `'/SILENT'` or `'/VERYSILENT'`.

### **/LOG**

Instructs Setup to create a log file in the user's `TEMP` directory detailing file installation and `[Run]` actions taken during the installation process. This can be a helpful debugging aid. For example, if you suspect a file isn't being replaced when you believe it should be, the log file can tell you if the file was really skipped, and why.

The log file is created with a unique name based on the current date. It will not overwrite or append to existing files.

 The information contained in the log file is technical in nature and therefore not intended to be understandable by end users. Nor is it designed to be machine-parsable; the format of the file is subject to change without notice.

### **/LOG="filename"**

Has the same function as `/LOG`, except it allows you to specify a fixed path and filename for the log file. If a file with the specified name already exists, it is overwritten. If the file cannot be created, Setup will abort with an error message.

### **/NORESTART**


When combined with `'/SILENT'` or `'/VERYSILENT'`, it instructs the setup not to reboot even if it is necessary.

### **/NOCANCEL**

Prevents the user from cancelling during the installation process by disabling the Cancel button and ignoring clicks on the close button. Useful along with `/SILENT`.

### **/DIR="x:dirname"**

Overrides the default directory name displayed on the Select Destination Directory wizard page. A fully qualified pathname must be specified.

 The specified directory must exist. The installer does not create it. Missing directory causes the installation to fail.

### **/LOADINF="filename"**

Instructs Setup to load the settings from the specified file after having checked the command line.


This file can be prepared using the `'/SAVEINF='` command as explained below. Don't forget to use quotes if the filename contains spaces.

```
setup.exe /VERYSILENT /NORESTART /DIR="%ProgramFiles%\SafeCom\TestWebInterface" /
LOG="%USERPROFILE%\Desktop\wiinstall.log" /LOADINF="%USERPROFILE%\Desktop
\wisetup.inf" /SUPPRESSMSGBOXES

setup.exe /SILENT /NORESTART /NOCANCEL /DIR="%ProgramFiles%\SafeCom\TestWebInterface" /
LOG="%USERPROFILE%\Desktop\wiinstall.log" /LOADINF="%USERPROFILE%\Desktop
\wisetup.inf" /SUPPRESSMSGBOXES
```

### **/SAVEINF="filename"**

Instructs the setup to save installation settings to the specified file. If the filename contains spaces, use quotation marks.

 This parameter saves variable data only from the UI. If you specify the variable values used in the installation through the command line interface, this switch is not supported.

```
setup.exe /LOG="%USERPROFILE%\Desktop\wiinstall.log" /SAVEINF="%USERPROFILE%\Desktop
\wisetup.inf"
```

### **/WEBALIAS**

Allows to specify a web alias to your SafeCom web interface.

### **/SCSERVERIP**

The IP address of the SafeCom server or the name of the host where the server is installed.

If the SafeCom server and the Web Interface are installed on the same machine, the server's IP value can be `localhost`.

### **/IISWEBSITE**

In this parameter, the site name under which the installer installs the application container in the IIS can be specified.

When you create an application in IIS, the application's path becomes part of the site's URL. For example, since `TestWebinterface` was added to `ExampleSite` and the site is using the binding over port 443, and HTTPS, the URL to `TestWebinterface` looks like this: `https://hostname:443/TestWebinterface`, where `hostname` is the actual name of the web server.

```
setup.exe /VERYSILENT /NORESTART /DIR="%ProgramFiles%\SafeCom\TestWebInterface" /
LOG="%USERPROFILE%\Desktop\wiinstall.log" /IISWEBSITE="ExampleSite" /
WEBALIAS="TestWebInterFace" /SCSERVERIP="%COMPUTERNAME%" /SUPPRESSMSGBOXES
```

### **Example: INF file containing the Web Interface configuration parameters**

```
[Setup]

IISWebSite=SiteIIIhttps
WebAlias=Testwebinterface
SCServerIp=localhost
```

## Manual firewall configuration

If there is a firewall on the computer running the web server, then it must allow the application communication port.

## Restart the web server


First time you must restart the web server.

1. Open the **Control Panel** on the computer where the IIS software is installed.
2. Click **Administrative Tools**. Click **Services**.
3. Locate the **IIS Admin Service** and right-click it and click **Restart**.

## Test the web server using a browser

Open a web browser and enter the address of the web server that hosts the SafeCom Web Interface followed by `/webinterface`, or the of alias you created.


For example: `http://localhost/safecom`.

 Make sure that your firewall is configured correctly. For more information, see [Manual firewall configuration](#).

## Configure SafeCom Web Interface

SafeCom Web Interface includes a Windows configuration utility that provides a convenient interface to changing the Windows Registry settings used by the SafeCom Web Interface. To configure the Safecom Web Interface:

1. Run `WIConfigurator.exe`. By default, it is located at `C:\Program Files\SafeCom\Web Interface\Configurator`. Alternatively it can be found through the Start menu under the Web Interface group.

 Running the executable requires administrator privileges on the computer.

2. Under **Connection** configure the following parameters:

### Server name

Enter the name or the IP address of the SafeCom server. If the Web Interface installed to the same computer, you can enter `localhost` too.

**Server port**

Communication port for the SafeCom server. It is 7700 by default.

**Login type**

You can select the desired login type for the users in the Web Interface webpage.

**Connection timeout**

Session timeout for users. Defined in minutes.

3. Under **Delegates permissions**, the users can review, setup, accept or cancel delegate connections.
4. Under **ID Code permissions**, you can configure the way the users can handle their own ID Codes on the Web Interface:

**Generate**

Allow users to generate a new ID codes (temporary or permanent).

**Delete**

Allow users to delete ID codes. Users can only delete ID codes that were generated manually.

**Hide**

ID Codes are not displayed on the screen.

**Make permanent**

Allow users to make temporary ID codes permanent.

**Change expiration**

Users can change the expiration date of the temporary ID code.

5. Under **Job / File permissions**, you can configure how the users can control the print jobs:

**Delete jobs**

Allow users to delete pending print jobs.

**Retain jobs**

Allow users to retain their pending print jobs.

**Preview documents**

Allow users to preview their scanned documents in the browser.

6. Under **Pay user**, you can configure the following:

**Show cash card**

Show the user's cash card account.

**ePay provider**

Setup the electronic payment provider.

7. Under **Security code permissions**, you can configure the following:

**Generate PUK code**

Allow users to generate new PUK codes to register their new card.

**Change PIN code**

Allow users to create new PIN codes for login.

8. Under **User interface**, you can configure the following:

**Default theme**

Setup the default type of web pages.

**Default language**

Setup the default language of web pages.

**Use browser language**

Use browser language as default if supported.

**i** Microsoft Narrator reads the type names of user interface elements in the language of the operating system. The following configuration is recommended for the comfort of visually impaired users:

- Set the **Display language** of the operating system to the spoken language of the user.
- Set the browser language to the spoken language of the user.
- Set the Web Interface configuration setting **Use browser language** option to **True**.
- Set Microsoft Narrator language to the spoken language of the user.

## Configure PayPal as provider

To configure PayPal as an ePay provider:

1. In **SafeCom Web Interface Configurator > Pay user > ePay Provider** select **PayPal** from drop-down list.
2. You can configure the following parameters:

**Currency**

Set the currency code for online money transfer. This currency is displayed on the Kofax SafeCom Web Interface pages and used with the external payment provider through the payment process.

**Client ID**

Set the app's client ID. The Client ID is provided by the external payment provider when the registration process is complete.

**Secret**

Set the app's Secret. The Secret is the password for the external payment provider. The Secret usually provided in encrypted form by the provider.

**Environment**

Select between test and live production environment. If the Test environment (provided by the external payment provider) is selected, all transactions are processed through a test system, and do not trigger live transactions.

**i** Transactions through a test environment act as the live transactions from the SafeCom perspective, so use it with extreme cautions for testing and configuring purposes only.

## Customize and translate ePay email message

SafeCom ePay has one English email template that is used to notify users that money was transferred to their SafeCom print and copy account. The `EmailEpay.txt` template can be found at `C:\Program Files\SafeCom\SafeComG4\Templates` by default.

You are free to customize or translate the message to give the users the highest user satisfaction. Dates are written according to the server's short format. Prepare templates using the following variables:

**<%Amount%>**

The amount of money transferred.

**<%Currency%>**

The currency used in the transaction.

**<%Date%>**

The date of the transaction.

**<%TransacNo%>**

The ID of the transaction.

**<%Fee%>**

The fees of the transaction.

**<%TotAmount%>**

The account balance after the transaction.

**<%OrderNo%>**

The order number.

Copy the prepared template to the install folder of SafeCom G4 Server.

**Example: EmailEpay.txt**

```
SafeCom print and copy deposit was successful.  
  
Transaction for the value of: <%Amount%> <%Currency%>  
Payment fee: <%Fee%> <%Currency%>  
Total amount: <%TotAmount%> <%Currency%>  
  
Order number: <%OrderNo%>  
Authorization Date/Time: <%Date%>  
Transaction number: <%TransacNo%>
```

## Setup ePay Cash Card

This section is only relevant if the SafeCom Pay solution stores money on a Smart Card. It allows SafeCom to transfer money deposited through SafeCom ePay to the user's Cash Card when the card is used at the SafeCom-enabled device.

## Enable SafeCom Web Interface trace files

To enable trace files:

1. Stop the IIS service on the computer where the Kofax SafeCom Web Interface is installed.
2. Create the folder `C:\safecom_trace`.
3. Start the IIS service.

### Trace files

Trace files are by default stored in the folder `C:\safecom_trace`. To change the default location of the trace files, modify the following Windows registry settings: `HKEY_LOCAL_MACHINE\SOFTWARE\SafeCom\SafeComG4\Trace`.

Value name (type)	Value data
Enabled (REG_DWORD)	0 = Disabled 1 = Enabled The default value is 0.
TracePath (REG_SZ)	Location for the trace files. The folder must be created before starting the service. Default location is <code>c:\safecom_trace\</code> .  <div style="border: 1px solid #add8e6; padding: 5px; background-color: #e6f2ff;"> <p><b>i</b> If you change the location, make sure that the new path ends with a backslash (\). The location requires restarting the IIS service for the trace files to be created at the new location.</p> </div>
TraceSize (REG_DWORD)	Set the maximum size of a trace file in kilobytes. Default value is 10240 (10240 KB = 10 MB).
TraceMaxLogs (REG_DWORD)	The maximum number of trace files per component. Default value is 2.

Trace file names contain a rolling numeric suffix. After reaching 999, suffix numbering restarts from 1. When a trace file reaches the maximum size (for example, 10 MB), a new trace file is created, and the trace file suffix number is incremented by one. The trace folder can contain as many instances of trace files per component as the `TraceMaxLogs` entry prescribes. Only the newest trace files are kept, older versions are automatically deleted.

The following trace files are created:

- `WebInterface<number>.trc`
- `WIconfigurator<number>.trc`

**i** If the Kofax SafeCom Web Interface is installed on the same computer as the Kofax SafeCom G4 server, the trace folder contains more `.trc` files.

## Configuring Kerberos delegation

To use single sign-on Windows authentication (using logged-in user credentials without asking username and password) add the `https://<web interface machine name>` to **Local intranet sites** in **Control Panel > Internet Options > Security**. Kerberos delegation needs to be set up if the SafeCom server and the Web Interface are installed on different computers and Windows authentication is used.

### Configuring constrained Kerberos delegation

#### SafeCom service runs under a machine account, such as Local System account

If SafeCom service is changed to machine account from a domain user account, the old SafeCom SPN needs to be removed before SafeCom service starts under the new machine account. To remove the old SPN, run `setspn -d SafeCom/<SafeCom server machine name> <domain>\<username>`. The user who runs this command must have `servicePrincipalName read` and `write` permission for the domain user account under which the SafeCom service ran earlier (`<domain>\<username>`). SafeCom service automatically registers the new SPN at startup.

This is the recommended configuration method.

Running under a machine account, the following configuration methods are available:

- If the Web Interface application pool runs under a machine account, such as `ApplicationPoolIdentity`, configure constrained delegation on this machine account to another machine account SafeCom service runs on.

To configure delegation:

1. In **Active Directory Users and Computers**, open **Web Interface machine account properties**.
  2. Navigate to **Delegation** tab .
  3. Select **Trust this computer for delegation to specified services only** .
  4. Select **Use any authentication protocol** .
  5. Add the `SafeCom/<SafeCom server machine name>` SPN to the services list  
It can be selected by browsing SafeCom server machine account.
  6. Click **OK** .
- If the Web Interface application pool runs under a domain user account, configure constrained delegation on this domain user account to the machine account SafeCom service runs on.

To configure delegation:

1. In **Active Directory Users and Computers**, open **Web Interface domain user account properties**.
2. Navigate to **Delegation** tab.



**i** If no SPNs are registered for the Web Interface domain user account, the **Delegation** tab does not appear. For the **Delegation** tab to appear, the registered SPN does not need to be valid, it can be any string.

3. Select **Trust this user for delegation to specified services only** .
4. Select **Use any authentication protocol** .
5. Add the `SafeCom/<SafeCom server machine name>` SPN to services list  
It can be selected by browsing SafeCom server machine account.
6. Click **OK** .

### SafeCom service runs under a domain user account

If the SafeCom service is changed to domain user account from a machine account, first the SafeCom SPN needs to be removed, then the same SPN needs to be registered for the domain user account using `setspn.exe`.

To remove and register SPNs:

1. Remove the old SPN by running `setspn -d SafeCom/<SafeCom server machine name> <domain>\<SafeCom server machine name>`  
The user who runs this command must have `servicePrincipalName` read and write permissions for the machine account under which the SafeCom service ran earlier (`SafeCom/<SafeCom server machine name>`).
2. Register the new SPN by running `setspn -s SafeCom/<SafeCom server machine name> <domain>\<username>`  
The user who runs this command must have `servicePrincipalName` read and write permissions for the domain user account under which the SafeCom service runs.

**i** The SafeCom service automatically registers the SPN at startup if the domain user account under which the SafeCom service runs has `servicePrincipalName` read and write permissions. The previous SPN must be removed before SafeCom service starts under the new service domain account.

Running under a domain user account, the following configuration methods are available:

- If Web Interface application pool runs under a machine account such as `ApplicationPoolIdentity` configure constrained delegation on this machine account to the domain user account.

To configure delegation:

1. In **Active Directory Users and Computers**, open **Web Interface machine account properties**.
2. Navigate to **Delegation** tab.
3. Select **Trust this computer for delegation to specified services only**.
4. Select **Use any authentication protocol**.

5. Add the `SafeCom/<SafeCom server computer name>` SPN to services list  
It can be selected by browsing SafeCom server machine account.
  6. Click **OK**.
- If Web Interface application pool runs under a domain user account, configure constrained delegation on this domain user account to the SafeCom service domain user account. It is recommended to use the same domain user account for both SafeCom service and Web Interface application pool.

To configure delegation:

1. In **Active Directory Users and Computers**, open **Web Interface domain user account properties**.
2. Navigate to **Delegation** tab.

**i** If no SPNs are registered for the Web Interface domain user account, the **Delegation** tab does not appear. For the **Delegation** tab to appear, the registered SPN does not need to be valid, it can be any string.

3. Select **Trust this user for delegation to specified services only**.
4. Select **Use any authentication protocol**.
5. Add the `SafeCom/<SafeCom server computer name>` SPN to services list  
It can be selected by browsing SafeCom server machine account.
6. Click **OK**.

## Configuring resource-based constrained Kerberos delegation

### SafeCom service runs under machine account

Configure the delegation using PowerShell.

If SafeCom service is changed to machine account from a domain user account, the SafeCom SPN needs to be removed before SafeCom service starts under the new machine account.

To remove and register SPNs:

1. Remove the old SPN by running the `setspn -d SafeCom/<SafeCom server machine name> <domain>\<username>` command.

**i** The user who runs this command must have `servicePrincipalName` read and write permissions for the domain user account under which the SafeCom service ran earlier (`<domain>\<username>`).

2. The SafeCom service automatically registers the new SPN at startup.

The PowerShell script must be run by the SafeCom resource owner user. This user must have `msDS-AllowedToActOnBehalfOfOtherIdentity` read and write permissions for the machine account under which the SafeCom service is running.

Running under a machine account, the following configuration methods are available:

- If the Web Interface application pool runs under a machine account, run the following commands:

```
$scidentity = Get-ADComputer -Identity <SafeCom machine account>
$wiidentity = Get-ADComputer -Identity <Web Interface machine account>
Set-ADComputer $scidentity -PrincipalsAllowedToDelegateToAccount $wiidentity
```

To check delegation, run the following command:

```
Get-ADComputer $scidentity -Properties PrincipalsAllowedToDelegateToAccount
```

To clear the delegation, run the following command:

```
Set-ADComputer $scidentity -PrincipalsAllowedToDelegateToAccount $null
```

- If Web Interface application pool runs under a domain user account, an SPN needs to be registered for the domain user account, otherwise the setup fails.

The registered SPN does not need to be valid, it can be any string. For example: `setspn -s dummytext/dummytext <domain>\<username>`.

After the SPN registration, run the following PowerShell commands to setup the Kerberos delegation:

```
$scidentity = Get-ADComputer -Identity <SafeCom machine account>
$wiidentity = Get-ADUser -Identity <Web Interface domain user account>
Set-ADComputer $scidentity -PrincipalsAllowedToDelegateToAccount $wiidentity
```

To check the delegation, run the following command:

```
Get-ADComputer $scidentity -Properties PrincipalsAllowedToDelegateToAccount
```

To clear the delegation, run the following command:

```
Set-ADComputer $scidentity -PrincipalsAllowedToDelegateToAccount $null
```

### SafeCom service runs under a domain user account

If the SafeCom service is changed to domain user account from a machine account, first the SafeCom SPN needs to be removed, then the same SPN needs to be registered for the domain user account using `setspn.exe`.

To remove and register SPNs:

1. Remove the old SPN by running `setspn -d SafeCom/<SafeCom server machine name> <domain>\<SafeCom server machine name>`.  
The user who runs this command must have `servicePrincipalName` read and write permissions for the machine account under which the SafeCom service ran earlier (`<domain>/<SafeCom server machine name>`).
2. Register the new SPN by running `setspn -s SafeCom/<SafeCom server machine name> <domain>\<username>`.  
The user who runs this command must have `servicePrincipalName` read and write permissions for the domain user account under which the SafeCom service runs.

**i** The SafeCom service automatically registers the SPN at startup if the domain user account under which the SafeCom service runs has `servicePrincipalName` read and write permissions. The previous SPN must be removed before SafeCom service starts under the new service domain account.

The PowerShell script must be run by the SafeCom resource owner user. The user must have `msDS-AllowedToActOnBehalfOfOtherIdentity` read and write permissions for the domain user account under which the SafeCom service is running.

Running under a domain user account, the following configuration methods are available:

- If the Web Interface application pool runs under machine account, run the following commands:

```
$scidentity = Get-ADUser -Identity <SafeCom domain user account>
$wiidentity = Get-ADComputer -Identity <Web Interface machine account>
Set-ADUser $scidentity -PrincipalsAllowedToDelegateToAccount $wiidentity
```

To check the delegation, run the following command:

```
Get-ADUser $scidentity -Properties PrincipalsAllowedToDelegateToAccount
```

To clear the delegation, run the following command:

```
Set-ADUser $scidentity -PrincipalsAllowedToDelegateToAccount $null
```

- If the Web Interface application pool runs under an other domain user account or the same domain user account.

It is recommended to use the same domain user account for both SafeCom service and Web Interface application pool.

If a different domain user account is used for the Web Interface application pool, an SPN needs to be registered for the account. The value of the SPN does not matter, it can be any string, for example: `setspn -s dummytext/dummytext <domain>\<username>`.

After the dummy SPN registration, run the following PowerShell commands to setup the Kerberos delegation:

```
$scidentity = Get-ADUser -Identity <SafeCom domain user account>
$wiidentity = Get-ADUser -Identity <Web Interface domain user account>
Set-ADUser $scidentity -PrincipalsAllowedToDelegateToAccount $wiidentity
```

To check the delegation, run the following command:

```
Get-ADUser $scidentity -Properties PrincipalsAllowedToDelegateToAccount
```

To clear the delegation, run the following command:

```
Set-ADUser $scidentity -PrincipalsAllowedToDelegateToAccount $null
```

### Clearing ticket cache

If the Windows authentication fails and delegation needs to be changed, the Kerberos ticket cache needs to be deleted on Web Interface machine.

The Ticket cache can be cleared the following ways:

- Wait at least 15 minutes for the cache to clear automatically.
- Restart the Web Interface machine.
- Using a PowerShell script file.

To clear the cache using a script file, create a file with the following content:


```
if ($args.count -ne 2)
{
    Write-Host "Usage: purge_kerberos.ps1 domain username"
}
else
{
    $users = Get-CimInstance -ClassName Win32_LoggedOnUser
    foreach($u in $users)
    {
        if ($u.Antecedent.Domain -eq $args[0] -and $u.Antecedent.Name -eq $args[1])
        {
            $domain = $u.Antecedent.Domain
            $name = $u.Antecedent.Name
            $logonid = ($u.Dependent.LogonId -as [int]).ToString("X")

            Write-Host "Domain: $domain, Name: $name, Logon session: $logonid"

            $proc = Start-Process -FilePath "klist.exe" -ArgumentList "-li $logonid
            purge" -NoNewWindow -PassThru
            $proc.WaitForExit()
        }
    }
}
```

Run `<created file>.ps1 <domain> <username>` where the username is the account that runs the application pool (see in IIS Manager). The script launches `klist` with the appropriate parameters.

If application pool runs under machine account (`ApplicationPoolIdentity` account on the machine where Web Interface is installed), use the host name as domain parameter and application pool name as username parameter.

 The script must be launched with administrative privileges on the machine where Web Interface is installed on.

## Chapter 3

# Using SafeCom Web Interface

## Log in

The Web Interface can be accessed through a browser, as described in [Test the web server using a browser](#). It can be configured for automatic authentication or interactive login.

The web application authenticates the user first. If Windows authentication is selected as login method, then Web Interface automatically logs into the G4 server on behalf of the domain user logged into the computer. The domain user must be a SafeCom user.

**i** For configuring Web Interface to support Windows authentication, you have to configure either **Kerberos** or **Resource-based constrained delegation**.

The application can be configured to prompt for the user credential. The following options available for interactive login depending on configuration by the administrator:

### User logon

Users can log in using their User logon and PIN Code.

### ID code

Users can log in using their ID Code and PIN Code.

**i** If domain users are added to SafeCom and you want to use user logon authentication method, then these users must be supplied with alias using their domain name.

Once logged in, the **Home** screen opens with the user's name displayed in the top right corner. From here, depending on the configuration, the user can access the following:

- Pending print jobs
- Print and copy history
- Balance and deposits of the account
- Billing codes
- ID codes
- Scanned files
- Settings

If SafeCom ePay is used, the user can deposit money through the internet.


## Managing pending print jobs

1. Log into the **SafeCom G4 Web Interface** in a web browser.
2. Click the **Pending print jobs** tile or select Documents > Pending print jobs in the menu.

**Charging scheme:** Selecting a charging scheme shows the specific price for each document. You can hide charging schemes in SafeCom Administrator, by selecting the **Hide this scheme from Web Interface users** checkbox in the charging scheme properties.

The Document list contains all pending print jobs. Check one or more documents to perform the following actions:

- Click **Delete** to delete the selected documents.
- Click **Retain** to keep the selected documents on the SafeCom server after being printed and thus available for printing again later.
- Click **Unretain** to remove the retained state of the selected documents. Not retained jobs are deleted after printing.
- Click **Refresh page** to update the document list.
- Click **Find** and start typing to filter the document list.



 The availability of the **Delete**, **Retain**, and **Unretain** options depends on the current configuration of the SafeCom Web Interface by the administrator.

You can click the table headers to sort the table based on the selected column.


## Managing scanned files

1. Log into the **SafeCom G4 Web Interface** in a web browser.
2. Click the **Files** tile or select Documents > Files in the menu.

Check one or more documents to perform the following actions:

- Click **Delete** to delete the selected files.
- Click **Download** to get all selected files in a ZIP file.
- Click **Refresh page** to refresh the document list.
- Click **Find** and start typing to filter the document list.
- Click the inline  icon to download the related file. The operation does not impact the selected elements in the list.
- Click the inline  icon to preview the related file. You can preview files one by one.

You can click the table headers to sort the table based on the selected column.

 Depending on your browser, you may need to install a separate PDF viewer to handle PDF files.

## View transactions

1. Log into the **SafeCom G4 Web Interface** in a web browser.
2. Click the **Transactions** tile or select Transactions in the menu.

In the **Transactions** window, you can check the balance of your accounts and the different deposits:

### **Cash card**

Available amount on a Cash Card.

### **Account 1. and Account 2.**

The balance of the two accounts.

### **Low limit**

The minimum amount of credits that must be available in order to print or copy. Displayed only if the user has a **Low limit** value set.

### **Reserved**

The amount of credits reserved due to a print or copy job that finished in error. Displayed only if the user has a **Reserved value** set.

### **Disposable**

The actual available credits (the **Balance** minus **Low limit** and **Reserved**).

### **Time interval**

Allows you to set a time range to filter transactions.

### **Show details**

Check to get a detailed information about the transactions. The following additional fields appear:

- Device name
- Pages
- Color
- Duplex
- Size


You can filter the document list by clicking **Find** and typing.

## Transfer money through ePay

1. Log into the **SafeCom G4 Web Interface** in a web browser.
2. Click the **ePay** tile or select ePay in the menu.
3. Enter the amount to be transferred in the Online money transfer window.  
The email address is retrieved from the SafeCom server and pre-filled but it can be changed. Upon successful completion of the transaction, an email is sent to the specified email address. See [Customize and translate ePay email message](#) to see how the notification message can be configured.



4. Select the payment option by clicking the corresponding icon. The following payment options are available:
  - PayPal
  - Debit or Credit Card
5. Enter the payment information in the payment processing gateway.
6. The user is informed on the message bar about the result of the transaction.

 The screen to manage the payment is generated by the ePay provider. The application only hosts the user interface.

## Managing PayPal transactions

### Transaction status

The user interface for payment processing is provided by PayPal. The SafeCom Web Interface only hosts the PayPal web application. The payment process is controlled by the provider. Web Interface follows the process and status of each transaction is recorded by the SafeCom server. The recorded transactions can have following status values:

#### **Created (1)**

The order request is sent to PayPal.

#### **Approved (2)**

Confirmation of order received from PayPal.

#### **Completed (4)**

Confirmation of the completed transfer.

#### **Cancelled (8)**

The payment process cancelled by the user.

#### **Failed (16)**

The transaction failed due to a technical reason.

The normal flow of the transaction status is **Created**, **Approved**, and **Completed**.

The identifiers of the orders and the transactions are stored in database **scPurse** to follow the result of the transactions even in exceptional cases, such as hardware or software failures. The PayPal transaction status reports are managed by the server side component of Web Interface, so the communication remains under control even if the initiating browser session terminates on client side.

### Cancelled transaction

PayPal transactions can be cancelled at different points of the UI workflow. The user can leave the PayPal page, click the **X** to close the dialogue window, or close the browser to cancel the transaction. A warning can appear to confirm the cancellation of the transaction. Software or

hardware issues can also lead to cancellation of transactions. In such cases, the initiated transaction is marked with status of **Cancelled** in the SafeCom database.

Web Interface can detect that the workflow was cancelled in an unexpected manner and the next time when the user logs in and navigates to the ePay page, such transactions are cancelled automatically. The notification is shown at the top bar of Web Interface ePay page to let the user know the result of the background operation.

```
[timestamp] Payment successfully cancelled. (Amount: NNN, Create date: ..., Order ID: XXX)
```

### Approved but not completed transactions

Users must approve the transaction first and then the PayPal system confirms the transactions. If the transaction is accepted and the user's PayPal account is charged, then the amount is credited to the SafeCom account. The transaction is completed even in case of unsecured transactions, but the SafeCom account is not changed.

During this process, the network connection can break or other unexpected failures can happen. The transaction may or may not complete, but the result is unknown. The following error message is shown on the screen of Web Interface to notify the user about the failure:

```
[timestamp] Payment failed
```

The transaction state in the SafeCom database indicates that the operation was not completed. The next time the user logs in and navigates to the ePay page, the following notification is displayed:

```
Approved unfinished payment: [the date and time of the transaction] [Amount]: Order ID: [PayPal order ID]
```

Next to the notification **Complete** and **Cancel** buttons are displayed. Using the buttons the user can continue and finish the transaction or cancel it.

If the user completes the transaction and it is successful, the following notification appears:

```
[timestamp] Payment successfully recovered (Amount, Transaction creation date, PayPal order ID)
```

If the user cancels the operation, the following notification is shown:

```
[timestamp] Payment successfully cancelled (Amount, Transaction creation date, PayPal order ID)
```

### Completed but not accounted payments

If the user approved the transaction but the PayPal confirmation did not arrive due to network problems, the amount cannot be credited to the SafeCom account. The transaction history is maintained by PayPal for a limited period. Such transactions can be recovered automatically.

If this failure occurs, the following error message appears in the notification bar:

```
[timestamp] Payment failed. Connection error. Please try again later.
```

In this case, the payment status remains **Approved**.

The next time the user navigates to the ePay page, the system detects the inappropriate transaction status. If the transaction can be found in PayPal transaction history, then the amount is credited to

SafeCom account and the record status is set to **Completed**. The automatic recovery is indicated in the notification bar by the following message:

```
[timestamp] Payment successfully recovered. [amount] was transferred to your account  
(Create date: [timestamp], Order ID: [value], Transaction ID: [value]).
```

If the transaction cannot be found in the PayPal transaction history, the transaction status in scPurse database is set to Failed (16) and the amount is not credited on the SafeCom account.

In this case, the following message appears in the notification bar:

```
[timestamp] Failed to recover payment. (Amount: [amount], Create date: [timestamp],  
Order ID: value).
```


The amount can be credited to the SafeCom account if PayPal can confirm that the transaction identified by the Order ID succeeded and the users PayPal account is charged.

## Manage client billing

The **Client Billing** web page offers users an overview of their finished jobs and gives them the opportunity to add or modify billing codes (for as long as the specified elapse time allows, refer to the [SafeCom G4 Administrator's Manual](#)) and manage their list of favorite codes.

In this section the following areas are covered:

- [Client billing settings](#)
- [Assigning billing codes to completed jobs](#)

 For Client billing to be available to the user, the user needs to be a tracking user. This is set up on the **User properties** in the SafeCom Administrator.

### Client billing settings

Through SafeCom Web Interface, the user can set up the following default values for Client Billing:

#### **Email reminder**

The user can specify if and when they want a reminder to add billing codes to jobs before they are committed to tracking.

#### **Default billing code**

The user can specify the default billing code. This code will be used if no other billing code was added to the job.

#### **Favorite billing code**

The user can specify the list of favorite billing codes. Only those codes can be used on the devices or in the ScPopup.

To configure the default client billing settings:

1. Log into the **SafeCom G4 Web Interface** in a web browser.
2. Click the **Billing settings** icon or select Client Billing > Settings in the menu.

3. Under **Reminder**, select the preferred email reminder. The following options are available:

**Never remind me**

An email reminder is never sent.

**Remind me as soon as a job completes**


An email reminder is sent after each print job is completed.

**Remind me when job completes and there are more than X unbilled jobs**

A reminder is sent when there more than a specified number of print jobs are completed and ready for billing.

4. Under **Manage billing codes** select the favorite billing codes and the default billing code. The current default billing code is displayed in the top of the section.


If the user is a billing user and choice of billing code is not restricted, then all available billing codes are listed on the page and the user can add or remove codes from the list of favorites. User's billing codes can be restricted through the SafeCom Administrator User properties dialog > Settings tab.

 The default billing code can also be specified as **Personal**, which means that it is not billed. If the user is set up as pay user, the job will be billed to the user.

The list of billing codes can be filtered.

## Assigning billing codes to completed jobs

After a user has finished a job at an MFP, the user can add or modify billing codes of the job through SafeCom Web Interface.

 The time when jobs are available for change of billing codes in the SafeCom Web Interface depends on the settings of the **Server properties** in the SafeCom Administrator. After this time frame, the unbilled jobs are billed with the user's default billing code.

To assign or modify billing codes in the SafeCom Web Interface:

1. Log into the **SafeCom G4 Web Interface** in a web browser.
2. Click the **Set billing** icon or select Client billing > Set billing in the menu.
3. Choose the billing code you want to add from your favorites drop-down list.  
The user's available jobs are listed under the following tabs depending on the billing status of the job:

**Unbilled jobs**

Print jobs that do not have a billing code added yet.


**Billed jobs**

Print jobs with billing codes assigned already but still available for change.

**Personal jobs**

Print jobs that do not need a billing code. If the user is a pay user, every job is billed to the user.

4. On the **Unbilled jobs** or the **Personal** tab select the jobs that you want to add the billing code to. Alternatively, select a job on the **Billed jobs** tab to modify the current billing code.
5. Click one of the following buttons to add the code:
  - **Not billable**. Click if you want to add the billing code to the job, but not bill for the job. The job is moved to the **Billed jobs** list.
  - **Billable**. Click if you want to add the billing code to the job and make sure that the job is billed. The job is moved to the **Billed jobs** list.
  - **Personal**. Click if the job is personal. The billing code and whether the job is billable is not specified or tracked. The job is moved to the **Personal** list.

 If the billing code is set to not billable, the billing code is added to the job and **Billable** is set to **No** for the specific job. If the billing code is set to be billable, the billing code is added to the job and **Billable** is set to **YES** for the specific job.

## Manage delegates

With delegated print, you can let other users collect your print once they have been assigned as your delegate within the SafeCom system. You can use the SafeCom Web Interface to manage delegates, if you have been granted these rights by your administrator.

In this section the following areas are covered:

- [Send request](#)
- [Pending requests](#)
- [Collect my documents](#)
- [Submit documents to me](#)

### Send request

1. Log into the **SafeCom G4 Web Interface** in a web browser.
2. Click the **Delegates** tile or select **Setup > Delegates** in the menu.
3. Select a user from the list and select whether they can collect from and submit documents to you.
4. Click the **Add user** icon when ready.

The request is displayed on the selected user's Web Interface under the **Pending Request** menu. You can have a maximum of ten users collecting your print. However, you can collect prints from any number of users.

### Pending requests

A delegate request can be cancelled in the **Pending request** page by the sender before it is accepted.

Incoming delegate requests accepted or rejected in the **Pending request** page.

## Collect my documents

The **Collect my documents** list contains all the users who were delegated to collect the current user's documents.

The following operations are available:

- If the **Always delegate to the listed users** checkbox is checked, all of the user's print jobs are automatically delegated to the listed users.
- By clicking the **Calendar** icon, the user can set an expiration date. By default all delegating rights are permanent.
- Any non-permanent delegate can be converted to a permanent one by clicking the **Stopwatch** icon.
- Any delegation rights can be removed by clicking the **Trashcan** icon.

## Submit documents to me

The **Submit documents to me** list contains all the users who can send print jobs to the current user.

If the delegated user does not want to collect any more print jobs from the delegating user, the delegation can be removed by clicking the **Trashcan** icon.

## Manage codes and set up language

The **Setup** menu allows you to change PIN, see and change PUK and ID code (if this is enabled on the server), as well as change the default language.

In this section the following areas are covered:

- [Change PIN](#)
- [Manage PUK and ID codes](#)
- [Change default language](#)

## Change PIN

Users can only change their PIN if **Allow user to change PIN code** is checked on the **Users** tab in the **Server properties** dialog in **SafeCom Administrator**.

To change the PIN:

1. Log into the **SafeCom G4 Web Interface** in a web browser.
2. Click the **Change PIN** icon or select Setup > Change PIN in the menu.
3. Enter the old and new PIN codes.
4. Click **Change PIN**.

## Manage PUK and ID codes

On the **Codes** page users can view the ID codes assigned to them, as well as the start and end dates if the code is a temporary code.

**i** Support for multiple cards is controlled on the **Users** tab in the **Server properties** dialog in **SafeCom Administrator**.

Depending on the setup on **SafeCom Web Interface Configurator**, users can generate a new PUK codes if they have lost their card and need to associate themselves to another card. Users can also generate or delete an ID code, make a temporary ID code permanent, or change the expiry date.

Before managing PUK or ID codes, log into the Web Interface:

1. Log into the **SafeCom G4 Web Interface** in a web browser.
2. Click the **Codes** icon or select Setup > Codes in the menu.

### Generate a new PUK code

1. On the **PUK** section, click **Generate new PUK**.
2. The new PUK code is now shown in the **PUK section**, and the old PUK code no longer works.

### Generate a new ID code

1. On the **Codes** tab, click **Generate new ID code**.
2. If **Hide ID codes** is not checked in **SafeCom Web Interface Configurator**, the generated ID code is listed in the list of ID codes.
3. If **Hide ID codes** is checked in **SafeCom Web Interface Configurator**, the generated ID code is hidden in the list. The new ID code appears on the notification bar.

**i** The structure of the ID code is determined in the file `IDCodeGenerating.txt` but can be changed. The settings in the SafeCom Administrator are used as a default, unless customized by editing `IDCodeGenerating.txt`. For more information, see the SafeCom G4 Administrator's Manual.

### Delete an ID code

Users can delete ID codes that were generated manually, through the SafeCom Administrator or the SafeCom Web Interface.

1. On the **Codes** tab, click the **Trashcan** icon next to the ID code that needs to be deleted.
2. Click **Yes** to confirm deleting the ID code.

### Edit an ID code

Temporary ID codes can be edited.


1. On the **Codes** tab, click the **Calendar** icon next to the ID code that needs to be edited.

2. To change the expiry date of the ID code, choose a new date.
3. Alternatively, click the **Stopwatch** icon to make the temporary ID code permanent.

## Change default language

On the **Language** page (**Setup > Language** in the menu) users can choose the language that they prefer to use on the SafeCom Web Interface.

Select your preferred language by clicking the relevant flag icon.

 The Default language is set by the administrator through the Configurator.

## Select appearance

The user can change the appearance of the Web Interface. The following themes are available:

### **Default**

The default theme selected by the administrator through Web Interface Configurator.

### **Light**

Light mode with white background.

### **Dark**

Dark mode with black background.

### **Light accessible**

Light mode with support for visually impaired persons.

### **Dark accessible**

Dark mode with support for visually impaired persons.

To change the Web Interface appearance:

1. Log into the **SafeCom G4 Web Interface** in a web browser.
2. Select **Themes** in the menu and select the desired UI theme.