

Kofax SafeCom G4 Server Administrator's Guide

Version: 10.7.0.1

Date: 2023-10-17

KOFAX

© 1995-2023 Kofax. All rights reserved.

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

Table of Contents

Preface	21
Related documentation.....	21
Training.....	21
Getting help with Kofax products.....	21
Chapter 1: Introduction	23
SafeCom Smart Printing.....	23
Components overview.....	24
Database component.....	24
SafeCom components.....	24
SafeCom Pay components.....	25
SafeCom APIs.....	26
SafeCom service and other services.....	26
Pull Printing explained.....	26
Terms and definitions.....	27
Requirements.....	31
Server requirements.....	31
Client requirements.....	32
Printers.....	33
Network ports.....	33
SafeCom ID devices.....	33
About this guide.....	34
Chapter 2: Planning your SafeCom solution	36
Checklist – to help you on the way.....	36
User authentication by card or ID code.....	37
User creation and management.....	38
Import user data from other systems.....	38
Create users at first print.....	38
Let users register cards themselves.....	39
Let users register an ID code themselves.....	39
Let administrator register cards to users.....	40
Let administrator register ID code with users.....	40
Allow users to change their PIN code.....	40
Determine user’s home server.....	40
Overview of software installation.....	41

Server installation.....	41
Multiserver installation.....	41
Disk space considerations.....	41
Shared SafeCom Pull Printer.....	42
Local SafeCom Pull Printer.....	42
SafeCom printers can reference multiple servers.....	42
Printer driver and document fidelity considerations.....	42
High Speed Print considerations.....	43
Device Server failover considerations.....	44
Print from other systems.....	45
Print from Apple Mac.....	45
Print from UNIX.....	46
Print from Novell.....	46
Print from Host systems (mainframe).....	46
Rollout considerations.....	46
Test solution prior to rollout.....	47
Inform and prepare your users.....	47
Clearly define responsibilities and procedures.....	47
Preemptive support and diagnostic tools.....	47
Event log and e-mail notification.....	48
scping.....	48
SafeCom services and processes.....	48
TCP and UDP port numbers used by SafeCom.....	51
SafeCom SQL databases.....	58
SafeCom database update log.....	59
Windows registry settings.....	59
Backup and restore.....	59
Standby computer equipment.....	59
SafeCom Windows registry settings.....	60
Customized SafeCom files.....	60
Printer configurations.....	61
SafeCom database - backup and restore.....	61
scBackup.....	62
SafeCom database - maintenance.....	63
SafeCom server trace facility.....	63
Enable trace.....	63
Trace files.....	64
TELNET interface.....	65

SafeCom device trace facility.....	66
Chapter 3: Installation.....	67
Installation methods.....	67
Server installation (Basic).....	67
Server installation (Advanced).....	69
Client installation.....	71
Tool installation.....	71
SafeCom G4 Server installer command line options.....	72
Windows Firewall – Ports that must be opened.....	77
Windows Firewall – Make SQL use fixed port.....	77
Security checkup after installation.....	79
Scripts to manually create the databases.....	79
SQL collation.....	80
Create intermediate SQL user: safecominstall.....	80
Delete intermediate SQL user: safecominstall.....	83
Do not modify SQL user: safecom.....	83
Add Windows service account to the SQL server.....	84
Enable TCP/IP protocol on the SQL server.....	84
Determine physical and virtual memory on the server.....	84
Store print files on an external file share.....	85
Change location of SafeCom print files.....	85
Configure encryption between SafeCom components.....	86
Using a custom certificate for TLS communication.....	87
Update SafeCom software – single server.....	87
Uninstall SafeCom software.....	88
Uninstall Microsoft SQL Express 2019.....	88
SafeCom Print Client.....	89
Installation.....	90
Windows Firewall.....	90
Print test page.....	91
Printing protocol.....	91
Direct print if SafeCom server is offline.....	91
Deployment to computers.....	92
scPrintClient.ini file.....	93
Use trace facility.....	94
Command line parameters.....	95
Uninstallation.....	96
Upgrade from Express to Microsoft SQL Server.....	97

Stop the SafeCom Service.....	97
Change Windows registry to refer to the SQL server.....	98
Change the dependencies on the SafeCom Service.....	98
Multiserver installation.....	98
Prerequisites.....	99
Overview.....	100
Set SQL Server Agent to automatic startup.....	102
Add the other servers to the primary server's group.....	102
Check that the replication is working.....	102
Repair replication.....	104
What happens if servers or network connections are down?.....	105
Reinitialize the subscription.....	105
Prevent the subscription from expiring.....	106
Using Group Management Service Account for services.....	106
Change SafeCom configuration from SQL to Windows authentication.....	106
Update multiserver installation.....	107
Pre-requisites.....	107
Update SafeCom software.....	107
Install the SafeCom license key code.....	109
Determine the computer name.....	109
Determine the cluster name.....	109
Understanding the license key code.....	109
Device license and user settings dependencies.....	110
User rights required when adding printers.....	111
First steps if the SafeCom server is clustered.....	111
On node 1 and 2 grant permissions in Local Security.....	112
On node 1, grant permission in cluster.....	112
On node 1, grant permission in registry.....	112
Restart the print spooler.....	112
Add a SafeCom Pull Printer on Windows 10 and 2016.....	112
Check the printer properties.....	113
Add a SafeCom Pull Printer on client computers.....	113
Install SafeCom client.....	114
Add a local SafeCom Pull Printer on Windows 10.....	114
SafeCom Pull Port.....	115
Enable printer pooling.....	115
Configure the SafeCom Pull Port.....	115
Edit servers dialog.....	117

SafeCom Print Authentication dialog.....	117
Customizing SafeCom PopUp dialogs.....	117
Configure Use job data logon.....	117
Add a SafeCom Push Port.....	119
Check the properties of the printer.....	121
SafeCom Smart Scan.....	121
SafeCom Move – scMove.exe.....	122
Setup SafeCom Move.....	122
SafeCom Move example.....	123
SafeCom PopUp – scPopUp.exe.....	124
Setup SafeCom PopUp.....	124
SafeCom PopUp deployment on Windows computers.....	126
SafeCom PopUp examples.....	126
Control dialog timeout.....	128
Remember logon timeout.....	128
Working with languages.....	129
Printing encrypted documents.....	129
Make all printing go through SafeCom.....	130
Install a card reader on a computer.....	130
Install SafeCom Smart Printer Add-on and Driver.....	131
Install Smart Printer Add-on on SafeCom server.....	131
Install Smart Printer Add-on on SafeCom Print Client.....	132
Install SafeCom Smart Printing Driver.....	132
Configure drivers to use both 32-bit and 64-bit clients.....	132
Verification – Collect your first document.....	133
Update selected SafeCom components.....	134
Update SafeCom Administrator.....	134
Update SafeCom port monitors.....	134
Update scJobServer.exe.....	135
Update scSecureLib.dll.....	135
Update filtercard.dll.....	136
Chapter 4: SafeCom Administrator.....	137
Install SafeCom Administrator.....	137
Log in to SafeCom Administrator.....	137
SafeCom Assistant.....	138
Change password.....	139
Test server.....	139
Menus and commands.....	139

Server group and server icons.....	142
User icons.....	142
Device icons.....	143
Document icons.....	144
Other icons.....	145
Built-in user accounts.....	146
System overview.....	146
Guides.....	147
Users.....	147
Devices.....	148
Servers.....	148
Device Servers.....	148
Collect system info.....	148
Check for updates.....	148
Save-O-Meter.....	149
License.....	149
Check server group properties.....	149
Server properties.....	149
Server.....	150
Users.....	151
Devices.....	153
E-mail.....	154
Configure NTLM SMTP authentication.....	155
Configure Microsoft 365 OAuth2 SMTP authentication.....	156
Configure Google OAuth2 SMTP authentication.....	157
Tracking.....	158
Billing.....	159
Encryption.....	160
User properties.....	161
Identification.....	162
Settings.....	163
ID code.....	165
Rights.....	167
Member of.....	169
Aliases.....	169
Delegates.....	170
Account.....	172
Billing.....	173

Device properties.....	174
Settings.....	175
Charging scheme.....	177
License.....	177
Statistics.....	178
Configure.....	179
Options dialog.....	181
General.....	181
Card reader.....	182
Network.....	184
Maintenance.....	185
Server group info.....	185
Branches.....	186
Administrator rights.....	187
Add a branch.....	187
Delete a branch.....	187
Add a device to a branch.....	187
Remove a device from a branch.....	188
Computer properties.....	188
Add a computer to the SafeCom solution.....	189
Add a computer to a branch at first print.....	189
Add a computer to a branch manually.....	189
Import computers.....	189
Remove a computer from a branch.....	189
Delete a computer from the SafeCom solution.....	190
Organizational units.....	190
Add an organizational unit.....	190
Delete an organizational unit.....	191
Devices with restricted access.....	191
Groups.....	192
Add groups manually.....	192
Group properties dialog.....	193
Delete groups.....	193
Add members to a group.....	194
Remove users from a group.....	195
Select rules to be used in a group.....	195
Select favorite billing codes for a group.....	195
Group print.....	195

Device servers.....	196
Add device server.....	197
View device server properties.....	197
Delete device server.....	197
Group device servers.....	198
Delete device server group.....	198
Statistics.....	198
Event log.....	199
View SafeCom event log.....	199
View SafeCom event messages in Windows event log.....	200
Event severity.....	201
Export data.....	201
Export users.....	201
Export servers.....	202
Export devices.....	203
Export billing codes.....	204
Export 2-level billing codes.....	204
Chapter 5: Manage servers.....	206
Add a single server group.....	206
Create a multiserver group.....	207
Prerequisites.....	207
Add server.....	207
Troubleshooting.....	208
Remove single or multiserver group.....	208
Delete a secondary server from a multiserver group.....	209
Failover servers.....	209
Set up user replication on failover servers.....	210
Chapter 6: Manage users.....	212
Default user.....	212
Create a default user.....	214
Delete a default user.....	214
Import users.....	214
Overview.....	215
Server.....	215
Import source.....	216
File source (CSV file and XML file).....	216
Properties (Active Directory).....	217
Properties (Novell eDirectory).....	217

Properties (LDAP server).....	218
Configuration (CSV).....	218
Configuration (XML).....	219
Configuration (Active Directory).....	220
Configuration (Novell eDirectory).....	222
Configuration (LDAP server).....	223
Rules.....	224
Extra.....	227
Schedule.....	227
User import log file.....	228
Search filter.....	230
Install certificate.....	230
Conversion of magnetic ID codes.....	231
Create users at first print.....	231
Add users manually.....	232
Find users.....	232
Customize the user list view.....	232
Hide ID codes.....	233
Hide document names.....	234
Edit the properties of multiple users.....	234
Delete users.....	235
User redaction.....	235
How to use this feature.....	235
Important notes about user redaction.....	236
List of aliases.....	238
Save aliases to file.....	238
List of ID codes.....	238
Save ID codes to file.....	239
Customize the format of ID codes.....	239
User has lost ID card.....	240
User has forgotten ID code.....	241
User has forgotten PIN code.....	241
Delete a user's print jobs (documents).....	241
Customize and translate e-mail messages.....	242
E-mail templates.....	242
Chapter 7: Manage devices.....	245
Device license.....	245
Add device.....	245

Resend configuration.....	246
Add a device to a SafeCom Device Server.....	247
Add device server and device server device.....	247
Add device server device.....	247
Print QR code for Mobile Pull Print.....	248
Find devices.....	248
Simple search.....	249
Advanced search - Device licenses.....	249
Broadcast for devices.....	249
Customize the device list view.....	249
Edit the properties of multiple devices.....	250
Delete devices.....	250
Import Ethernet Card Readers.....	251
Update software.....	251
Location of device software.....	253
Single device software update.....	253
Multiple device software update.....	253
Monitor device.....	254
Start the device monitor.....	254
Enable monitoring on selected devices.....	254
Look at device statistics.....	255
Restart devices.....	255
Open in web browser.....	255
Restrict user access to devices.....	255
DHCP server.....	255
Shorten job names in document list.....	256
Chapter 8: SafeCom Tracking.....	257
Pull print tracking.....	257
Push print tracking.....	257
Printing directly.....	258
Printing through a second printer.....	258
Add a secondary printer (output service).....	259
Add the first printer (SafeCom Push Port).....	259
Set TCP port to a custom value.....	261
Allow printing at all times.....	261
SafeCom Port Configurator.....	262
Install SafeCom Port Configurator.....	262
Start SafeCom Port Configurator.....	263

Add server.....	263
Convert to Push.....	264
Restore to TCP/IP.....	266
List printers in the domain.....	267
Repair push printer.....	267
Read servers from file.....	267
scPortConfigurator.ini.....	268
scPortUtility.....	271
Troubleshooting.....	273
Copy tracking.....	274
Fax, Scan, and E-mail tracking.....	274
Post track.....	275
Push Print Post Tracking.....	275
Planning your SafeCom Tracking solution.....	275
Print price calculation.....	275
Track deleted jobs.....	278
Backup and restore.....	278
Using tracking data.....	278
Multiple servers: Online or offline tracking.....	279
Configure SafeCom primary server.....	279
Configure SafeCom secondary servers.....	279
Configuration overview.....	279
Charging schemes.....	280
Add charging scheme.....	280
Sample charging calculation.....	280
View charging scheme properties.....	281
Associate charging scheme with device.....	281
Configure default charging scheme for new devices.....	281
Delete a charging scheme.....	281
Change cost control to tracking.....	282
SafeCom Reports.....	282
Install SafeCom Reports.....	282
Start SafeCom Reports.....	282
Make a report.....	282
Work with tracking data.....	283
Export tracking data.....	283
Hide job names in tracking data.....	284
Delete tracking data.....	284

SafeCom Data Mining.....	285
Main tracking.....	285
User statistics.....	286
Device statistics.....	288
Billing statistics.....	290
Job list.....	292
Tracking record dialog.....	292
Update scParser.dll.....	295
Chapter 9: SafeCom Rule Based Printing (RBP).....	296
Planning your SafeCom RBP solution.....	296
Create the rules.....	297
Select rules to be used on group.....	299
What if the rule does not work?.....	299
How to determine the application.....	300
Update scRuleExecuter.dll.....	300
Chapter 10: SafeCom Client Billing.....	301
Manage billing codes.....	301
Plan your SafeCom Client Billing solution.....	302
Configuration overview.....	302
Configure SafeCom Client Billing.....	303
Import billing codes.....	304
Run a billing report.....	306
View billing codes in the Manage billing codes dialog.....	306
Billing code import log file.....	307
Set up users to use billing codes.....	308
Considerations when using Tracking and Pay.....	308
Change the Bill clients for cost property of multiple users.....	308
Add favorite billing codes for a user.....	309
Select favorite billing codes for a group.....	309
Edit the template for billing reminder.....	310
Use the e-mail template for billing reminder.....	310
Manage 1-level billing code.....	310
Add billing code.....	311
Find billing codes.....	311
Delete billing codes.....	311
Modify billing codes.....	311
Manage 2-level billing code.....	312
Add primary or secondary code.....	312

Find primary or secondary codes.....	312
Delete primary or secondary codes.....	313
Modify primary or secondary codes.....	313
Add billing code.....	313
Delete billing codes.....	313
Modify billing codes.....	314
Work with Tracking data.....	314
Chapter 11: SafeCom Pay.....	315
Planning your SafeCom Pay solution.....	315
Accounting policy.....	315
Ensure that users pay.....	316
Cashless solution.....	316
Change cost control to Pay.....	316
Credit schedule.....	317
Cashier.....	318
Log in to SafeCom Administrator in Cashier mode.....	318
Find user with search string.....	319
Find user through Advanced search.....	319
User properties dialog.....	320
View user transactions.....	322
Issue a new PIN code.....	322
Unlock user.....	323
Deposit credits.....	323
Withdraw credits.....	323
Set low limit.....	323
Free reserved credits.....	323
Reset cash cards.....	324
Detect attempt to avoid paying.....	324
Print reports.....	324
Account status.....	324
Cash flow report.....	325
User transactions dialog.....	325
Prevent cheating.....	326
E-mail template for an unfinished job.....	326
Difference between print and copy.....	326
Job name pricing.....	327
JobNamePricing.txt.....	327
Chapter 12: SafeCom Device Utility.....	329

Start SafeCom Device Utility.....	329
Menus and commands.....	329
Populate list of devices.....	330
Edit configuration.....	330
Set configuration.....	331
Manage devices in batch.....	331
Command line parameters.....	332
Structure of the parameter file.....	333
Properties of the [Defaults] section.....	333
Structure of the [Devices] section for bundle installation.....	334
Structure of the [Devices] section for configuration handling.....	334
Chapter 13: Format of tracking data.....	336
Format history.....	336
Format.....	336
Chapter 14: SafeCom ID devices.....	341
SafeCom AWID Reader.....	342
SafeCom Barcode Reader.....	342
SafeCom Casi-Rusco Reader.....	342
SafeCom EM Reader.....	342
SafeCom HID Prox Reader.....	343
SafeCom iCLASS Reader.....	343
SafeCom Indala Reader.....	343
SafeCom Keypad.....	343
SafeCom Legic Reader.....	344
SafeCom Magnetic Card Reader.....	344
SafeCom Magnetic Card Reader DD.....	344
SafeCom Mifare Reader.....	345
Chapter 15: SQL Always On.....	346
SQL Always On deployments.....	346
Single-server SafeCom solution with AG.....	346
Multiserver SafeCom solution with AG.....	347
Limitations.....	348
Prerequisites for SafeCom in Availability Group.....	349
Checklist for HA.....	351
Building single-server SafeCom solution with databases in AG.....	352
Prepare SQL Server instances.....	353
Install SafeCom to an external SQL Server.....	353
Create and configure AG.....	353

Create AG Listener.....	354
Redirect SafeCom Application Server to AG Listener.....	354
Building multi-server SafeCom solution with primary databases in AG.....	354
Set up remote distributor SQL Server instance.....	355
Set up replication snapshot share.....	355
SafeCom Primary Application Server.....	355
Install secondary SafeCom servers.....	355
Add Secondary SafeCom servers to a multiserver solution.....	356
Moving multi-server SafeCom solution into AG.....	357
Set up remote distributor SQL Server instance.....	357
Set up replication snapshot share.....	357
Drop local distributor.....	358
Create and configure AG.....	358
Create AG Listener.....	358
Redirect SafeCom Application Server to AG Listener.....	359
Configure SafeCom Primary Application Server.....	359
Repair replication for secondary SafeCom servers.....	359
Troubleshoot multiserver HA.....	360
Replication is not working.....	360
Verify availability replica nodes of the publisher.....	360
Verify distributor SQL Server instance.....	361
Chapter 16: Troubleshooting.....	362
SafeCom Help Desk Assistant.....	362
SafeCom Administrator: Login failed.....	362
SafeCom Administrator: Unable to locate all SafeCom servers.....	362
SafeCom Administrator: Unable to locate all SafeCom devices.....	363
SafeCom Administrator: Users are missing.....	363
SafeCom Administrator: Add user failed and Add alias failed.....	363
SafeCom Administrator: License does not take effect.....	363
SafeCom Administrator: Controls in dialog are not visible.....	364
SafeCom Administrator: Device is recognized as SafeCom Controller.....	364
SafeCom Administrator: Device cannot be added as a Push printer.....	364
SafeCom Administrator: Device is not responding when the community name has been changed from "public".....	364
User is not created at first print.....	364
Device web interface: Displayed incorrectly or settings not saved.....	365
At the printer: Out of order.....	365
At the printer: User unknown.....	365

At the printer: Login denied.....	365
At the printer: Restricted access.....	366
At the printer: Error printing document.....	366
At the printer: Question mark before the document name.....	366
At the printer: Printer busy, retry later.....	366
At the printer: Printer keeps rebooting.....	366
At the printer: Copy not allowed.....	366
At the printer: Login error <number>.....	366
At the printer: Error printing: General Failure.....	367
At the printer: Card reader not working.....	367
Document not printed.....	367
Some documents are missing.....	367
Document printed incorrectly.....	368
Nothing is copied.....	368
Driver names are missing.....	368
Add Printer Wizard: Specified port cannot be added.....	368
Local SafeCom Pull Printer is unable to print.....	368
Start and stop the SafeCom service.....	369
How to start and stop the Print Spooler.....	369
User computer: Unable to connect to SafeCom server.....	369
User computer: Please contact your administrator!.....	369
Import users: No users imported.....	370
Import billing codes: No codes imported.....	370
Multiserver installation: Replication issues.....	370
scPopUp: The publisher could not be verified.....	371
Smart Printer Driver: Reduced performance.....	371
Smart Printer Driver: Error codes at the device.....	371
Remote SQL server cannot login.....	372
SafeCom server can not login using the safecominstall user.....	372
Spooler failure when the Print System Asynchronous Notification message is not handled by the user.....	372
Certificate of the SafeCom G4 primary server is lost.....	373
Communication failure between SafeCom components.....	373
User Import from Unix that does not contain Domain Info.....	373
SafeCom secondary server is not reachable from the SafeCom primary server.....	373
Replication subscription for the old SQL primary server appears under the SafeCom secondary server's SQL Express instance.....	374
Services using GMSA accounts do not start automatically after reboot.....	374

Chapter 17: Error codes.....	375
SafeCom Server error codes.....	375
Chapter 18: Administrator's installation notes.....	381
Servers.....	381
SafeCom primary server.....	382
SQL primary server.....	382
SafeCom secondary server.....	383
Failover servers.....	384
User authentication.....	384
Devices.....	385
Printer drivers.....	386
Chapter 19: scPortUtility operations and exit codes.....	387
Push Port Creation.....	387
Command Line usage.....	387
Options and parameters.....	387
Exit codes.....	389
Remarks.....	390
Attach Port.....	391
Command Line usage.....	391
Options and parameters.....	391
Exit codes.....	391
Queue Migration – Push Print.....	392
Command Line usage.....	392
Parameters.....	393
Exit codes.....	394
Remarks.....	395
List print queues.....	396
Command Line usage.....	396
Options and parameters.....	397
Exit codes.....	397
Appendix A: Frequently asked questions.....	398
What are the benefits of Pull Printing?.....	398
Is Copy Control supported?.....	399
Is it possible to charge for print costs?.....	399
Is it necessary to install software on the users' computers?.....	399
How are users authenticated?.....	399
How are users managed?.....	400
How are users with the same name handled?.....	400

- How many users, printers, and documents can a server handle?.....400
- Can access to devices be restricted?..... 400
- Are SafeCom solutions scalable?..... 400
- How does a solution with multiple servers work?..... 401
- Can documents be printed securely?..... 401
- What happens to uncollected documents?.....401
- Is it always possible to print?..... 402
- Can print usage be tracked without hardware?.....402
- Can a Pull Printer be used for Push tracking?.....402
- What happens if the SafeCom solution stops working?..... 402
- What is the administrative overhead?..... 403
- What about integration with other systems?..... 403
- Does it pay to apply a SafeCom solution?..... 403

Preface

This guide provides an overview and instructions for the administrator who is responsible for installing, configuring, and maintaining the Kofax SafeCom G4 Server.

Related documentation

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

https://docshield.kofax.com/Portal/Products/en_US/SafeCom/10.6.0-0jhve8olil/SafeCom.htm

Training


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

Getting help with Kofax products

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

To access the Kofax Knowledge Base:

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

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

The Kofax Knowledge Base provides:

- Powerful search capabilities to help you quickly locate the information you need.
Type your search terms or phrase into the **Search** box, and then click the search icon.
- Product information, configuration details, and documentation, including release news.

Scroll through the Kofax Knowledge Base home page to locate a product family. Then click a product family name to view a list of related articles. Please note that some product families require a valid Kofax Portal login to view related articles.

From the Knowledge Base home page, you can:

- Access the Kofax Community (for all customers).
Click the **Community** link at the top of the page.
- Access the Kofax Customer Portal (for eligible customers).
Click the **Support** link at the top of the page. When the Customer & Partner Portals Overview appears, click **Log in to the Customer Portal**.
- Access the Kofax Partner Portal (for eligible partners).
Click the **Support** link at the top of the page. When the Customer & Partner Portals Overview appears, click **Log in to the Partner Portal**.
- Access Kofax support commitments, lifecycle policies, electronic fulfillment details, and self-service tools.
Go to the **General Support** section, click **Support Details**, and then select the appropriate tab.

Chapter 1

Introduction

SafeCom Smart Printing

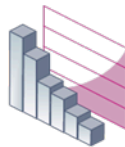
SafeCom Smart Printing offers intelligent solutions designed to help companies and organizations gain control over their printing costs and document security. SafeCom is a modular system that can be enhanced with add-on modules to build customer-specific and scalable solutions.



Cost Control

Reduce cost by 40%

- ✓ Central administration
- ✓ Consolidate print infrastructure



Efficiency

Supports the way you work

- ✓ Print anytime, anywhere
- ✓ Free up IT resources



Security

Protect your output

- ✓ Confidential printing
- ✓ Avoid unauthorized use

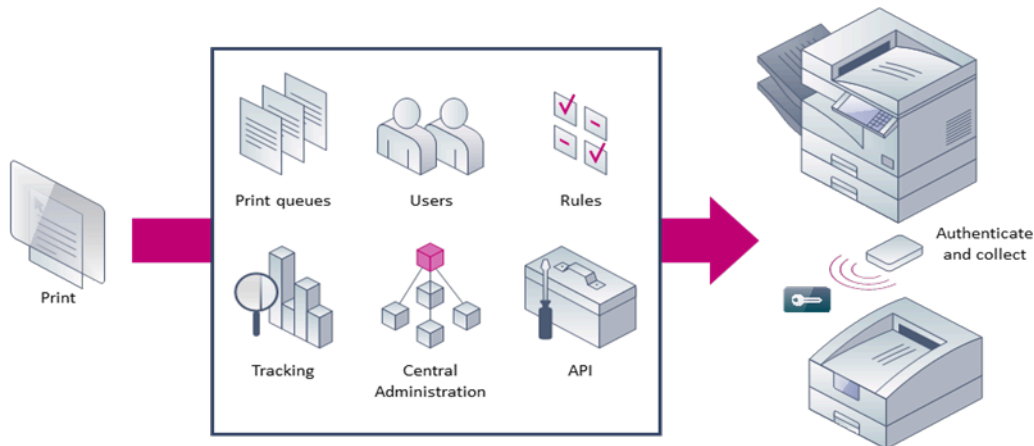


Environment

Solutions for a better world

- ✓ Reduce waste
- ✓ Sustainable print environment

Components overview



Database component

Database. A SafeCom server depends on the availability of its database. In most cases the provided database can be used. See [Server requirements](#) for details.

SafeCom components

SafeCom Go offers user authentication at the device and integrates with the touch-screen control panel on selected multifunction printers (MFPs) from Canon, Fuji Xerox, HP, Konica Minolta, Kyocera, Lexmark, Ricoh, Sharp, and Xerox. Authentication by card is possible by connecting a SafeCom ID device (card reader).

- **SafeCom P:Go** offers user authentication at single function printers and is typically used to print all documents at login.
- **SafeCom Controller / SafeCom Color Front-end** (combined touch-screen and card reader) is the printer manufacturer independent and external solution that is used to support devices not supported by SafeCom Go/SafeCom P:Go.
- **SafeCom ID Controller** allows user authentication by ID card on select MFPs and printers that are SafeCom-enabled through the SafeCom Device Server and do not support direct connection of a SafeCom USB ID device card reader.
- **SafeCom Device Server** is a web server based component that is used to offer SafeCom Go functionality on selected devices from Fuji Xerox, HP, Konica Minolta, Sharp, Xerox, and other vendors. It uses SOAP and XML to communicate with the device. No SafeCom software is installed on the device.
- **SafeCom G4** is the server software that comes with a database for storing user and tracking information. Users are added to the database the first time they print, but they can also be

imported from for example Active Directory. It can also work with an external Microsoft SQL Server, see [Server requirements](#) for details.

- **SafeCom Administrator** is the application that is used to configure and administer the SafeCom solution, including remotely updating SafeCom software on devices.
- **SafeCom Reports** is used to generate reports based on tracking data collected for printer, copied and deleted documents. Use it to report cost and environmental savings.
- **SafeCom Web Interface** offers users self service through a web browser. Users can delete or retain documents etc. Runs on Microsoft Internet Information Server (IIS).
- **SafeCom Port Configurator** is used to conveniently convert direct TCP/IP printers on print server to Push printers and thus allow tracking of documents sent directly to devices. The printers can be reverted back to TCP/IP printers if required.
- **SafeCom Push Port** is the port monitor that tracks directly printed documents.
- **SafeCom Pull Port** is a port monitor that tracks and stores the user's documents. Documents are stored on the SafeCom server. With **SafeCom Print Client** documents can optionally be stored on the hard disk drive of the user's computer or a print server.
- **SafeCom Print Client** allows documents to be stored on the hard disk drive of the computer that it is installed onto.
- **SafeCom PopUp** displays the pop-up dialogs on the user's screen that allow the user to interact with SafeCom.
 - **SafeCom Move** is a simple way for the user to manage pending print jobs or files scanned through SafeCom Smart Scan. From SafeCom Move the user can access scanned files, delete them, or download them to any location specified by the user.
 - **SafeCom Smart Scan** represents an easy way to handle scan-to-folder functionality that bypasses both Microsoft Outlook and complex password issues.
 - **Smart Printer Add-on and Driver** increases versatility across mixed MFPs from different vendors, as it ensures that users can use only one print queue, and run complex jobs on all printers without encountering driver incompatibilities. The Smart Printer Add-on and Driver create and store print data on the SafeCom server or the Print Client in Microsoft XPS format (XML Paper Specification format) until it knows which printer will be used. When the user logs onto an MFP, the system identifies the device type and only then runs the job through the correct vendor-specific printer driver.

SafeCom Pay components

These components are relevant only for solutions where users have to pay for print and copy service.

- **SafeCom Administrator** the application that is used to add (deposit) or subtract (withdraw) credits (money) from the user's account.
- **SafeCom ePay** allow users to transfer money from their bank account to their SafeCom account through the Internet.

SafeCom APIs

In addition to being a modular solution, the SafeCom Smart Printing solution also features a number of optional Application Programming Interfaces (APIs).

- **SafeCom Administrator API** is an XML-based tool that makes it possible to manipulate multiple users, automate tasks, and integrate your SafeCom Smart Printing solution with other systems.
- **SafeCom Batch Print API** is an XML-based tool used to integrate the SafeCom solution with other systems, such as document archiving systems.

SafeCom service and other services

The **SafeCom service** (scSafeComService.exe) launches the required SafeCom processes (scBroadcastServer.exe, scJobServer.exe, scMoneyServer.exe and scTrackingServer.exe). On Windows 64-bit, the files are named *64.exe. By default, the service runs under a local system account, and the databases are accessed through a safecom SQL user with SQL authentication. You can set up a dedicated service account, which requires "Logon as a service" rights and access to the SQL database with Windows authentication. The installer prompts for selecting the authentication method.

- **SafeCom Device Server:** The SafeCom Device Server (scDeviceServer.exe) launches the SafeCom Device Server.
- **SQL Agent:** The Microsoft SQL Server Agent handles the replication from the SQL primary server to the SafeCom secondary servers.
- **MSSQL:** The Microsoft SQL Server runs the database.
- **Print Spooler:** The Microsoft Print Spooler (spoolsv.exe) loads files to memory for later printing.
- **SafeCom XpsPrint Service:** Part of the Smart Printer Add-on. Handles XPS (Smart Printer Driver) job printing for SafeCom.

Pull Printing explained

From the user's point of view:


1. Print your documents from Windows.
2. Go to any SafeCom-enabled printer.
3. Log in using a card or code.
4. Select the documents you wish to print and pick them up from the printer's output bin.

From the administrator's point of view:

1. SafeCom solutions only require software to be installed on a Windows Server 2016, 2019, or 2022 or Windows 10 or 11. There is no need to install software on users' computers. It is sufficient to add or modify a shared printer on the server.

From the system's point of view:

1. The Windows print queue is using the port monitor SafeCom Pull Port to analyze the document to determine owner and job characteristics.
2. The SafeCom Pull Port transfers the formatted document and the resulting data to the SafeCom server.
3. When the user logs in at the printer, documents are released for printing. Documents that do not match the printer can be filtered from the list of documents in advance (see [Printer driver and document fidelity considerations](#) for more information).

 Different channels can be used for releasing documents. See [High Speed Print considerations](#) to read more about print channels and their configuration.

Terms and definitions

The relevance of some of the listed terms depends on the availability of SafeCom add-on modules (license key code controlled).

Billing code

A code users can select for any job that is tracked by the SafeCom solution. See [SafeCom Client Billing](#).

Charging scheme

In the charging scheme you define the cost of the different paper sizes, use of color and duplex (double-sided print). A device can be associated with two charging schemes: **Primary charging scheme**, which is used to charge users and invoice departments, and **Secondary charging scheme**, which is used to reflect the true costs. Requires SafeCom Tracking or SafeCom Pay.

Delegate print

Delegate Print is relevant for an organization that needs the advantages of SafeCom Pull Print and users who need the flexibility to entrust their print tasks to someone else. With SafeCom Delegate Print users authorize other SafeCom users to print or collect print jobs on their behalf and Delegate Print.

Domain

A group of computers that are part of a network and share a common directory database.

Driver name

In Windows, the driver name appears as **Model** on the **General** tab of the **Printer properties** dialog. The name is used to determine document fidelity (see [Printer driver and document fidelity considerations](#)).

Dual charging scheme

See [Charging scheme](#).

Encryption (option)

By means of encryption the SafeCom solution can prevent anyone from reading the documents, should they be intercepted on their way to the printer (see [Printing encrypted documents](#)). Requires SafeCom Encryption.

Group

Either a group of SafeCom servers (**Server group**) or a group of users. A user can be a member of one or more groups. Existing user grouping can be imported from Windows and used in connection with SafeCom Rule Based Printing. See [SafeCom Rule Based Printing](#).

Group print

Documents can be printed to all members of a group. With the "Print once" option, the document is deleted from all members after one member has collected it.

Home server

The SafeCom server where the list of the user's print jobs is maintained. See [Multiserver Support](#).

LDAP

Lightweight Directory Access Protocol.

License key code

The code provided by your SafeCom solution supplier.

MFP

Multifunction Printer; a device that can print, scan, and copy.

MSCS

Microsoft Cluster Service.

Multiserver Support

Enables two or more SafeCom servers to work together. Users can switch between locations to collect their documents at any SafeCom-enabled printer and at any location regardless to which SafeCom server the document was printed (see [Are SafeCom solutions scalable?](#)). See [Home server](#) and [Primary server](#).

Organizational unit (Org. unit)

An attribute that describes which part of the organizational tree users, devices, and servers belong to (see [Organizational units](#)).

PIN code

PIN (Personal Identification Number) is a personal code consisting of four (4) alphanumeric characters. To increase security, users are requested to log in by means of both the personal card (or ID code) and the PIN code. The default PIN code is 1234.

Port Configurator

See [SafeCom Port Configurator](#).

Port monitor

Port monitor is a component in the Windows print process that is responsible for the communication to the physical printer. When you do a server or client installation, you also install two special port monitors: SafeCom Pull Port and SafeCom Push Port.

Primary server

If the server group includes multiple SafeCom servers, then one is appointed the role of being the primary server. All system and user data are synchronized and distributed from the SafeCom primary server. See [Multiserver Support](#).

PUK code

PUK (Personal Unblocking Key) is an 8-digit code that associates users with their card (or ID code).

Pull Print

The process where users log in at the printer before the submitted documents are printed. See [SafeCom Pull Printer](#).

Push Print

The process where submitted documents are sent directly to the printer. See [SafeCom Push Printer](#).

RBP

Rule Based Printing.

Rule Based Printing

See [SafeCom Rule Based Printing](#).

SafeCom Administrator

The application you use to configure and administer a SafeCom solution.

SafeCom Administrator API

(option) An XML-based tool that makes it possible to manipulate multiple users, automate tasks and integrate the SafeCom solution with other systems. Available in the form of an executable and a dynamic link library (DLL).

SafeCom Batch Print API

(option) An XML-based tool used to integrate the SafeCom solution with other systems, such as document archiving systems.

SafeCom Broadcast Server

A server process that enables the various SafeCom applications to find and connect to the relevant servers.

SafeCom Client

A computer on which a local SafeCom printer is installed.

SafeCom Client Billing

(option) Allows users to select billing codes with any print, copy and possibly also fax, scan and e-mail jobs performed on MFPs. With billing codes, it is possible to get a very detailed breakdown of printer and MFP usage and possibly recover these expenses by invoicing clients. Requires SafeCom Tracking.

SafeCom Controller

Hardware that connects directly to the Ethernet network and provides network access for the SafeCom ID device.

SafeCom Devices

The SafeCom Controller, SafeCom Go and other devices that support the SafeCom protocol. Communicates with the SafeCom Job Server.

SafeCom ePay

(option) Allows users to transfer money from their bank account to their SafeCom account through the Internet.

SafeCom Front-end

Hardware that is used to authenticate users at the printer. It is a card reader with touch-screen (see [SafeCom ID devices](#)).

SafeCom Go

SafeCom device software that integrates with the touch-screen control panel of MFPs to offer authentication, access control and Pull Print (see [Printers](#)).

SafeCom ID device

Hardware that is used to authenticate users at the printer (see [SafeCom ID devices](#)).

SafeCom Job Server

A server process that stores user data, device data and print job references in the SafeCom Job database. Configuration data is also stored for the whole SafeCom solution.

SafeCom Mobile Print

Allows users to print through e-mail or to upload a print job to a web page, from a mobile device, a tablet, or computer.

SafeCom Money Server

A server process that controls access to the SafeCom Money database that stores transactions made on the users' accounts. Requires SafeCom Pay.

SafeCom Port Configurator

A wizard-based tool for converting existing TCP/IP¹ printers to SafeCom Push printers and reverting SafeCom Push printers back to their original TCP/IP settings.

SafeCom Print Client

SafeCom Print Client allows documents to be stored on the hard drive of the computer where it is installed.

SafeCom Pull Printer

(Uses SafeCom Pull Port) A printer defined in Windows that parses the printed document and transfers the printed document and tracked data to the SafeCom server. Subsequently, the user can log in at any SafeCom-enabled printer to collect the document.

SafeCom Push Printer

(Uses SafeCom Pull Port and SafeCom Push Port) A printer defined in Windows that parses the printed document, transfers the tracked data to the SafeCom server, and forwards the printed document either directly to the physical printer or to another Windows print queue. Requires SafeCom Tracking or SafeCom Pay.

SafeCom Reports

(option) SafeCom Reports enables viewing of main tracking statistics, user statistics, device statistics, client billing statistics and job list. SafeCom Reports includes a number of predefined and parameterized reports. Requires SafeCom Tracking.

¹ A TCP/IP printer is a Windows print queue that uses the Standard TCP/IP port monitor.

SafeCom Rule Based Printing

(option) Allows print cost savings by offering management a method for enforcing policies for printing. Rules can be applied to groups of users. Existing user grouping can be imported from Windows. Requires SafeCom Tracking.

SafeCom Server

The computer where the SafeCom Server software is installed.

SafeCom Tracking Server

A server process that controls access to the SafeCom Tracking database that stores information about who printed what on which printer and at what time. The tracking record includes information about paper size, number of pages and possible use of color and duplex (double-sided print). Requires SafeCom Tracking or SafeCom Pay.

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.

Server group name

A unique name used by SafeCom components to reference a group of one or more SafeCom servers. Maximum is 19 characters.

SQL Server Management Studio (SSMS)

SQL Server Management Studio (SSMS) is a tool used for handling SQL components.

Virtual server

Microsoft Cluster Service (MSCS) enables the creation of virtual servers. Unlike a physical server, a virtual server is not associated with a specific computer, and can failover from one node to another. SafeCom configurations must reference the virtual server rather than the physical servers. Requires SafeCom Cluster Server license.

Requirements

In addition to the Kofax SafeCom system requirements in the [Technical Specifications](#) document, this section lists requirements that are specific to the SafeCom G4 Server.

Server requirements

- Windows Server 2022, 2019, or 2016. For demo purposes, it can also run on Windows 10 or 11.
- Virtualization software, such as VMware and Microsoft Virtual Server, is supported as long as it supports the Operating System.
- 16 GB RAM or more.
- 120 GB or more disk space to allow for database growth and print job storage (depends on utilization).
- TCP/IP protocol installed and configured.
- Windows Installer 4.5
- Microsoft .NET Framework 4.6.

- SafeCom license key code.

Database

- Microsoft SQL Express 2019 is distributed and installed with the software, except when the primary server is installed using Microsoft SQL server.
- In a SafeCom [multiserver installation](#), the SQL primary server must run Microsoft SQL Server 2016, 2017, or 2019 Standard edition as a minimum. It must be licensed and installed (including replication option). Microsoft SQL is quite memory intensive and more memory leads to better performance. 16 GB RAM is the required minimum.
- Decide on the authentication type before installation, as you will be prompted to choose by the installer. If you select Windows authentication, the account is required during the installation and must have "Logon as service" rights. The service account credentials also need to be provided. If necessary, group managed service account can also be used for this purpose.



- These requirements are general rules for the configuration of the SafeCom servers (CPU, RAM, and disk space). The load on the system is very difficult to predict since it depends on many things, including, number, size and type of documents to be printed, printer driver, number and types of printers, number of users, and so on. See [Are SafeCom solutions scalable?](#) for information about scalability.
- The Smart Printer Driver supports both 32-bit and 64-bit versions of the operating system.
- Ensure that the computer names in the SafeCom environment are shorter than 16 characters, to avoid connection issues due to NetBIOS limitations.
- Ensure that ICMP traffic is allowed between SafeCom components (SafeCom G4 Server, Device Servers, Print Client, devices using various SafeCom Go implementations).
- Do not install your SafeCom Device Server on a computer that already has a Print Client or HP Unified Client for SafeCom installed.

Cluster

- The SafeCom server and the SafeCom printers on Windows Server 2019 and 2016 are cluster-aware (requires a SafeCom Cluster Server license). If one server in the failover cluster goes down another takes over. This increases availability of the SafeCom server installation significantly. Refer to [microsoft.com](#) for additional information on the resulting hardware and software requirements.

Client requirements

- Windows 10 or 11
- Clients running Citrix and Windows Terminal Service (WTS)
- 1 GHz CPU and 4/8 GB RAM or higher
- 1 GB free disk space (or more depending on the amount of printing)
- TCP/IP protocol installed and configured

Printing through LPD/LPR from Apple Mac, UNIX, Novell and Host systems (mainframe) is possible to a shared SafeCom Pull Printer, but may require additional software.



- For Windows 10 workstations, update 1511 is required.
- Ensure that the computer names in the SafeCom environment are shorter than 16 characters, to avoid connection issues due to NetBIOS limitations.

Printers

SafeCom Go integrates with the touch-screen control panel of the MFPs and offers user authentication by code and/or card. SafeCom P:Go is the internal solution for printers and typically offers user authentication by card. Supported printer vendors:

- Canon
- Fuji Xerox
- HP
- Konica Minolta
- Kyocera
- Lexmark
- Ricoh
- Sharp
- Xerox

If pages are to be counted, SafeCom Tracking is required and the print job must be processed by a driver that supports PCL5, PCL5c, PCL5e, PCL6, PCL XL, or PostScript level 2 or 3.

Network ports

[TCP and UDP port numbers used by SafeCom](#) has a complete list and description of the TCP and UDP port numbers used by the SafeCom solution.

SafeCom ID devices

Pull printing requires the user to log in at the printer. SafeCom offers a wide and ever expanding range of ID devices (methods), including card readers with touch-screen and stand-alone card readers. ID devices require unique ID device licenses. SafeCom ID devices come with ID device licenses, whereas ID device licenses for third-party ID devices must be purchased separately.

SafeCom Controller supported SafeCom ID devices

Authentication method	Card reader USB p/n	Card reader serial p/n	Color Front- end serial p/n
Windows authentication / ID code			672040
SafeCom AWID Reader	696020	696010	696040
SafeCom Barcode Reader	694020	694010	
SafeCom Casi-Rusco Reader	652420	652010	652040

Authentication method	Card reader USB p/n	Card reader serial p/n	Color Front-end serial p/n
SafeCom Cotag Reader	678020		67804x
SafeCom Deister Reader			65504x
SafeCom EM Reader [E] SafeCom EM Reader [R]	674120 674420	674110	674140
SafeCom Felica Reader	697420	697310	697440
SafeCom HID Prox Reader [E] SafeCom HID Prox Reader [R]	673120 673420	673110	673140
SafeCom HID Prox Reader 37 bit (custom)	671120	671110	671140
SafeCom iCLASS Reader [E] SafeCom iCLASS Reader [R]	654120 654420	654110	654140
SafeCom Indala Reader 26bit	670420	670010	670040
SafeCom Indala Reader 29bit	651020	651010	651040
SafeCom IoProx	658420	658010	658040
SafeCom Legic Reader [E] SafeCom Legic Reader [R]	679120 679420	679110	679140
SafeCom Magnetic Card Reader (Tr 1)			959040
SafeCom Magnetic Card Reader (Tr 2)			691040
SafeCom Magnetic Card Reader (Tr 3)			657040
SafeCom Magnetic Card Reader DD (Tr 1)	692010		
SafeCom Magnetic Card Reader DD (Tr 2)	691020		
SafeCom Magnetic Card Reader DD (Tr 3)	692020		
SafeCom Mifare Reader [E] SafeCom Mifare Reader [R]	970120 970420	970110	970140
SafeCom Nedap Reader	653020	978990	653040
SafeCom NexWatch Reader	698420	698010	698040

The table above shows the supported authentication methods. The ID device is either fitted or supplied with a 1.8–2.0 m cable. Additional information about the ID devices is available in [SafeCom ID devices](#).

If your method of authentication is not in the table, please contact Kofax Sales to discuss your options. Please contact your SafeCom representative if you want to have your cards verified for reading.

About this guide

This guide applies to the following product versions:

- SafeCom G4 Server version 10.7.0.1
- HP Unified Client for SafeCom version 5.10.2
- SafeCom Print Client version 10.7.0.1
- SafeCom Device Server version 9.13.0

- SafeCom Controller version S80 508.780*68
- SafeCom Controller 3 Port version S80 312.750*67
- SafeCom Controller 1 Port version S80 304.750*67
- SafeCom Go Canon version 20.25.0.28
- SafeCom Go HP version 50.32.0.114
- SafeCom Go Kyocera S96 020.060*02
- SafeCom Go Lexmark S93 nnn.030*21
- SafeCom Go Ricoh S87 nnn.030.06.3.1

Chapter 2

Planning your SafeCom solution

We want your SafeCom solution to be one that reduces print costs, is easy to administer and yields high user satisfaction. To ensure success, use the information in this chapter to plan your SafeCom solution.

Checklist – to help you on the way

Use the checklist below to plan/design the SafeCom Smart Printing solution.

Checklist for SafeCom Smart Printing solution

Topic	Notes
Responsibility	
Name of person:	
Functionality	
# Pull Print # Tracking # RBP # Client Billing	
# Pay # ePay	
Users	
Number of users:	
User authentication	
# Card, and type of card: # Import cards (conversion)	
# ID code	
# PIN code	
User creation	
Import users from # Active Directory (AD) # File # Other	
# Create users at first print	
# Create users manually	
Servers	
Enterprise server # Multiserver support # Job Data Logon	

Topic	Notes
# Cluster Support	
SQL server # SQL authentication # Windows authentication # Grant permission to the service account	
# Reports	
# Web Interface	
# Mobile Print	
Computer name / address:	
Hardware (CPU, RAM, Disk):	
Clients	
# SafeCom Print Client	
Devices	
SafeCom Go # Canon # HP # Kyocera # Lexmark # Ricoh	
SafeCom Go/Device Server # Fuji Xerox # HP # Konica Minolta # Sharp # Xerox	
SafeCom Go/Controller # Sharp # Xerox	
SafeCom Controller # SafeCom Color Front-end # SafeCom ID device	
Additional topics	

User authentication by card or ID code

Pull printing requires users to log in at the device. Authentication by card is a convenient method and the obvious choice when cards are used for existing purposes, such as building access.

There are also solutions where users authenticate themselves by entering an ID code instead of using a card. The ID code is case sensitive and can be the user's phone number, employee number, student number, social security number² or another number that is unique for the user and easy to remember.

Authentication by ID code is possible with the SafeCom Go products that integrate with the device's control panel or the external SafeCom Controller in combination with the SafeCom Color Front-end. Furthermore, you can enhance security by requesting users to enter a personal 4-digit PIN code.

If stand-alone card readers are used for authentication, card registration is manual, see [Let administrator register cards to users](#), or through import, see [Import user data from other systems](#).

² The legislation in some countries does not allow the use of social security numbers.

User creation and management

Users can be added, modified, and deleted through SafeCom Administrator. Creating and managing users are described in the following sections.

User-related data is sorted according to the following categories:

- **Personal data** includes the user's full name (John Smith), user logon (JS), domain and e-mail (JS@safecom.eu). This data can normally be imported. The user logon is a mandatory maximum of twenty (20) characters and must be unique within a domain. User logon is normally the same as the user's Windows logon.
- **Authentication data** includes the card number and an optional 4-digit PIN code. If cards are already used for existing purposes, such as building access, then it may be possible to import data from an existing database. The card number is mandatory, case sensitive, a maximum of 39 characters, and must be unique.
- **Settings data** is specific to the SafeCom solution, so it is not possible to extract and import this kind of data from other systems. However, to make administration easier, define a default user and let new users inherit settings data from the default user (see [Default user](#)).

Import user data from other systems

To make administration easier, data can be imported from other systems including those solutions with a large number of users.

SafeCom Administrator includes a user import wizard that can import personal data through Windows Active Directory (AD) and Novell eDirectory (NDS eDirectory v.8.7.3 or later). It is also possible to import both personal and authentication data via XML and CSV (see [Import users](#)).

SafeCom Administrator API (option) is an XML-based tool that makes it possible to manipulate multiple users, automate tasks and integrate your SafeCom solution with other systems.

Create users at first print

The SafeCom solution is capable of creating users automatically the first time they print through the SafeCom solution. This method keeps administrative overhead to a minimum.

How it works:

1. The user clicks **Print** in Windows and selects a SafeCom Pull Printer.
 2. The document is transferred to the SafeCom server. The server extracts the user logon and finds that the user is unknown and/or a card (or ID code) needs to be registered with the user.
 3. If the user is unknown, the server creates the user based on the default user properties. Next it sends an e-mail to the user, explaining how to collect the document. See the e-mail template example in section [Customize and translate e-mail messages](#).
- The user logon (JS) and the e-mail domain (safecom.eu) can be combined to create a valid user e-mail address (JS@safecom.eu).
 - The user must enter the e-mailed 8-digit PUK code to register their card or ID code.


For step-by-step instructions, see [Create users at first print](#).

Let users register cards themselves

Users can register cards themselves if your SafeCom solution allows users to enter a PUK code at the device, for example by having at least one MFP with SafeCom Go or a printer equipped with a SafeCom Color Front-end.

How it works:


1. Start SafeCom Administrator and then locate or add the user.
2. Provide the user with the 8-digit PUK code or let the system e-mail the PUK code to the user (see [E-mail](#)).
3. The user goes to the device and uses the card. The SafeCom solution finds that the card is not yet registered to a user. The user is asked to enter the PUK code once (and a personal PIN code twice).

 Be aware that if you login using a PUK code for a registered card that already has a PIN code, and you enter a PIN code when prompted, the system will treat this as a PIN code change, thus rendering your old PIN code invalid. You can enter your existing PIN code if you want to keep using that.

4. If the PUK code is incorrect, the registration fails and the user is asked to enter the PUK code again. The user can click **Exit** to terminate the process.
5. The card is registered with the user when the screen displays: "Operation succeeded. Please login again".

Let users register an ID code themselves

If your SafeCom solution allows users to enter a PUK code at the device, users can register an ID code themselves. The ID code is case sensitive.

 Normally, the administrator handles the registration of the user and ID code. See [Let administrator register ID code with users](#).

1. Make sure that all of the devices allow users to enter PUK codes and ID codes.
2. Start SafeCom Administrator and then locate or add the user.
3. Provide the user with the 8-digit PUK code or let the system e-mail the PUK code to the user (see [E-mail](#)).
4. The user goes to the device to log in. The user enters a unique ID code. The SafeCom solution finds that the ID code is not yet registered with a user. The user is asked to enter the PUK code once (and a personal PIN code twice).
5. If the PUK code is wrong, the registration fails and the user is asked to enter the PUK code again. The user can terminate the process.
6. The ID code is registered with the user when the screen displays: "Operation succeeded. Please login again".

Let administrator register cards to users

1. Make sure that the following prerequisites are met:
 - The computer must have a card reader installed (see [Install a card reader on a computer](#)).
 - Users must turn up in person to have their card read and a person with administrator rights must be present to operate the computer.
 - The administrator must inform the user of their PIN code.
2. Start **SafeCom Administrator** and then locate or add the user.
3. Open the **ID code** tab in the **User properties** dialog (see [ID code](#)).
4. Click **Listen** and use the card with the connected card reader.
5. If no PIN code is entered the user is assigned the default PIN code '1234'.

Let administrator register ID code with users

1. Make sure that the users are provided with an ID code and PIN code by the administrator.
2. Start **SafeCom Administrator** and then locate, or add the user.
3. Open the **ID code** tab in the **User properties** dialog (see [ID code](#)).
4. Enter the ID code (case sensitive).
5. If no PIN code is entered the user is assigned the default PIN code '1234'. The user may change the PIN code subsequently (see [Allow users to change their PIN code](#)).


Allow users to change their PIN code

If **Allow users to change PIN code** is checked on the **Users** tab in the **Server properties** dialog (see [Users](#)), then users can change their PIN code using any of the below methods:

- Using the SafeCom G4 Web Interface.
- On devices equipped with SafeCom Color Front-end.

Determine user's home server

If SafeCom multiserver support is enabled, the home server denotes the SafeCom server where the user's print jobs remain. If the server group consists of only one SafeCom server, there is no need to specify home server, since it is identical to the SafeCom server.

 If the **Store Doc on First Server** option is enabled, the user's documents are stored on the first server the Pull Port print queue contacts.

The user's home server can be specified in SafeCom Administrator (see [Identification](#)). If the user changes home server, his documents are not shown on the new home server, but the user is still able to collect his prints.

If no home server is specified, the user's home server becomes the one that is first contacted. First-time contact is when the user prints to a SafeCom device or logs in at a SafeCom device.

The home server for users that are created at first print (see [Create users at first print](#)) is by default set to the SafeCom server which the SafeCom Pull or Push port connects to.

Overview of software installation

In most cases, it is sufficient to install a SafeCom server and a shared SafeCom Pull Printer on the server.

If you have multiple Windows print servers with shared printers, you can turn these printers into SafeCom Pull Printers by making them use the SafeCom Pull Port, a special port monitor (see [Shared SafeCom Pull Printer](#)). You still need to install SafeCom hardware at the physical device to allow Pull Printing.

To administer your SafeCom solution from other computers, simply install the SafeCom Administrator on those computers (see [Install SafeCom Administrator](#)).

To delegate some of the administrative obligations, you can assign administrator rights to appointed SafeCom users.

Server installation

You need to perform the SafeCom server installation on a server computer. Download the SafeCom installer and select **Server installation** (see [Server installation \(Advanced\)](#)). This installs all the required software, including the port monitor SafeCom Pull Port and the administrative application SafeCom Administrator. See [Server requirements](#) for a description of the server requirements and SQL authentication.

The server installation allows you to specify two destination folders; one for the program files and another for the print jobs. You can locate the print jobs on a hard disk equipped with RAID or similar technology.

The default installation folder is `C:\Program Files\SafeCom\SafeComG4`.

The default folder for print jobs is `C:\Program Files\SafeCom\SafeComG4\Data`.

Multiserver installation

The SafeCom primary server must run Microsoft SQL Server. You need to make a SafeCom Server installation on each server as outlined in [Server installation](#). You use **SafeCom Administrator** to group the servers together. The steps involved are described in [Multiserver installation](#).

Disk space considerations

The amount of recommended disk space on the SafeCom server depends on a number of parameters: The number of users, number of documents, the size of these documents, and the time they are stored before they are collected by the users at the devices.

Through the SafeCom Administrator, you can specify how often uncollected documents should be deleted and whether users should be notified by e-mail in advance (see [Server](#)).

If storage prices are low, we recommend approximately 100 MB per user for printing purposes. The SafeCom software itself requires less than 25 MB.

(disk space = average number of jobs on the server per user × average size of jobs)

Shared SafeCom Pull Printer

The easiest way to make SafeCom Pull Printing available to users is to make an existing, shared Windows printer on one of the following servers:

- The SafeCom server.
- A Windows print server that uses the SafeCom Pull Port.
SafeCom Pull Port is a special port monitor that supervises the transfer of documents to the SafeCom server.

Prerequisites:

- A client installation is performed to install the SafeCom Pull Port on the Windows print server (see [Client installation](#)). The SafeCom Pull Port is installed on the SafeCom server as part of the server installation.
- The SafeCom Pull Port should be set to "Use network logon".

To avoid interfering with your users while you test your SafeCom solution, we recommend leaving shared printers as they are and adding a few new shared SafeCom Pull Printers that are dedicated to test SafeCom.

Local SafeCom Pull Printer

A local SafeCom Pull Printer (see [Add a SafeCom Pull Printer on client computers](#)) must be installed on the user's computer in order to print encrypted (see [Printing encrypted documents](#)). In all other cases, it is sufficient to use a shared SafeCom Pull Printer. However, SafeCom PopUp (see [SafeCom PopUp – scPopUp.exe](#)) must be running on the user's computer in these cases:

- If users need to print from the computer without being logged into Windows as themselves (see [SafeCom Print Authentication dialog](#)).
- If [SafeCom Rule Based Printing \(RBP\)](#) is used to ask for print confirmation.
- If [SafeCom Client Billing](#) is used and the user has to select a billing code at print submission time.

SafeCom printers can reference multiple servers

The SafeCom Pull Port (see [Edit servers dialog](#)) and SafeCom Push Port (see [Push Print Post Tracking](#)) can reference more than one SafeCom server.

This feature can be used to give additional resilience in a multiserver solution where SafeCom printers are installed on local clients or print servers.

If the first SafeCom server on the list is unavailable, it tries the next one. After 60 seconds, it attempts to revert to the first SafeCom server.

Printer driver and document fidelity considerations

When printing, the SafeCom solution takes the output from the installed Windows printer driver and stores it in the SafeCom database until the user collects the document at the device.


The question is: What happens if the document is subsequently collected at a different device model? The worst case is that the document prints incorrectly or not at all. The best case is that the document prints correctly.

However, you may also experience something in between. For example, if you request printing on both sides (duplex) in the printer driver, but it is not supported by the device. In this case, you may get a single-sided (simplex) print.

Document fidelity is determined by comparing the name of the printer driver, embedded in the print job, with the list of driver names returned by the SafeCom device. If there is no match, it is considered low fidelity and the document is labeled with a question mark ("?"). Refer to [Devices](#) on how to configure document fidelity.

Typically, document fidelity is high if you use a printer driver that generates PCL and subsequently collect the document at a printer that supports PCL. The same goes for PostScript.

If you use many different devices from different manufacturers, you may have to install multiple shared SafeCom Pull Printers, each one with their specific Windows printer driver.

 Using Internet Printing Protocol for SafeCom Pull printing does not restrict the use of printer drivers. All types of drivers can be used, including ones that produce custom binary print streams.

PDF printing


If the devices support PDF format, then PDF printer driver can be selected for the SafeCom Pull printer. It ensures that the print jobs can be pulled on devices from different vendors. It is recommended to configure the SafeCom devices to use IPP in such cases to send the documents in type safe manner.

 The Microsoft Print To PDF driver requires SafeCom Pull port with enabled v4 driver support.

High Speed Print considerations

By enabling High Speed Print on the SafeCom-enabled device, documents that are collected at the device are printed almost as fast as those that are printed directly. This is because print data is sent directly to the device from the SafeCom server (or SafeCom Print Client). The channel is selected automatically depending on the type of the stored print stream and the device configuration. The following scenarios are considered:

- If the print job was created by Smart Printer driver (its format is XPS), then the Smart Printer Add-on is used for releasing the job.

 High-Speed print must be enabled to use Smart Printer Add-on.

- If the device supports IPP, and it is enabled for the device in SafeCom Administrator, then this protocol is used for print job release.
- If IPP is not enabled for the device in SafeCom Administrator, then the regular printer port (#9100) is used.
- In an upgrade scenario, there can be devices that have no defined print channel selected. The server tries to send the job to the printer over IPP using the default IPP print URL (`http://`

[device IP address]/ipp/print). If this attempt fails, then the print job is sent over the TCP 9100 port. This approach might cause delay in starting print in the following cases:

- The device does not support IPP protocol at all.
- The device is configured to use non-default IPP URL.

In such cases, the protocol must be disabled in Device Properties dialog to eliminate the inconvenient delay at start job.

If the device supports IPPS (secure IPP), this option must be selected in the device properties. In general, the device properties should be reviewed to select the appropriate print channel.

On devices running SafeCom Go, the option of High-Speed Print can be turned off. The SafeCom device requests the print data from the SafeCom server (or SafeCom Print Client) through TCP port 7500 and sends it to the local port 9100. This communication between the device and the server is secure because it is a TLS 1.2 channel or encrypted by the SecureCom protocol.

However, because the print data is received directly by the device, it is not always possible to hold off other users' print jobs while a user is logged in at the device. Users may risk that the output bin contains other users' documents. This is not an issue if management has decided to ban all direct printing and only allow Pull Print.

Documents that are submitted through a SafeCom Push Port within the same SafeCom group can be held off, but documents that are submitted through a Standard TCP/IP port cannot be held off.

Device Server failover considerations

When planning Device Server failover groups (see [Device Servers](#), [Group device servers](#)), consider the following factors:

- Number of devices on a given single node.
- Expected level of fault tolerance (that is, maximum number of failed nodes at any give time)

Be aware that in case a failover occurs, the devices of the failed node are distributed in the failover group equally, regardless of how many devices the other nodes have individually. You must consider and plan to avoid overloading your other nodes in case of a failover. Kofax recommends assigning no more than 200 devices for a dedicated Device Server, or no more than 100 devices to a shared Device Server/G4 installation.

The following table illustrates a few examples using dedicated Device Servers.

Total amount of devices	Expected level of fault tolerance	Amount of equired nodes	Amount of devices per node
200	1	2	Node 1: 100 Node 2: 100
600	1	4	Node 1: 100 Node 2: 100 Node 3: 100 Node 4: 100

Total amount of devices	Expected level of fault tolerance	Amount of equired nodes	Amount of devices per node
600	2	5	Node 1: 120 Node 2: 120 Node 3: 120 Node 4: 120 Node 5: 120

Failover restriction of Device Server

Device Server failover from SafeCom Device Server version DS 90*10 requires SafeCom G4 Server 520*10 or newer to work.

Devices in failover state (that is, they have been distributed from their original home server due to a failover) cannot be modified, until they are reallocated to their original home server.

In case the home server becomes permanently unavailable, you have the option to delete and re-add the devices.

i Be aware that if you power on the original Device Server whose devices you redistributed, the Device Server will automatically re-acquire all devices previously assigned to it, which may result in inconsistent states.

Known limitations of Device Server failover

For SafeCom Device Server version DS 90*10 with G4 520*10 using SafeCom Device Server failover, the following limitations apply:

- New nodes should not be added if there are unavailable nodes in the group. This is prevented by the scAdministrator (520*10 or newer); older versions of scAdministrator do not prevent it.
- Nodes can be moved only one by one in scAdministrator.
- If all the nodes in a group stop at any given time simultaneously, restarting them results in the restarted nodes only managing their own devices.
- Nodes in Pending state should be not moved.

Print from other systems

Even though the SafeCom solution is a Windows-based printing solution, it is possible to print from other systems. This is described in the following sections.

Print from Apple Mac

Printing from Mac OS X Server through LPR/LPD is possible. The printing system in Mac OS X is based on the Common UNIX Printing System (CUPS).

Printing from earlier versions of Apple Mac OS is possible using the cross-platform file and printer sharing solution DAVE from Thursby Software Systems, thursby.com.

Prerequisites:

- The Windows component "Print Services for UNIX" must be installed. The Windows server must be restarted after installation.

If the user logon on Windows differs from the one on the Mac, then the user logon on the Mac must be on the user's list of aliases (see [Aliases](#)).

i If PopUp compatibility mode (see [SafeCom Pull Port](#) and [Add a SafeCom Push Port](#)) is enabled and you start a print job that uses scPopUp, ensure that you are not logged in to a Windows and a Mac computer at the same time while using the same credentials.

If you want to print from Apple Mac, ensure that you have a Microsoft v3 printer shared, because printing to v4 printers is not supported on a Mac.

Print from UNIX

On UNIX, it is possible to define an LPR/LPD printer that prints to the shared SafeCom Pull or Push Printer on the Windows server.

Prerequisites:

- The Windows component **Print Services for UNIX** must be installed. The Windows server must be restarted after installation.

If the user logon on Windows differs from the one on UNIX, then the user logon on UNIX must be on the user's list of **aliases** (see [Aliases](#)).

Print from Novell

With Novell Netware 6 and NDPS (Novell Distributed Print Services) you can use Novell iPrint to print through LPR to the shared SafeCom Pull or Push Printer on the Windows server. Refer to novell.com for additional information.

Print from Host systems (mainframe)

From the Host system, it is possible to define an LPR/LPD printer that prints to the shared SafeCom Pull or Push Printer on the Windows server.

Prerequisites:

- The Windows component **Print Services for UNIX** must be installed. The Windows server must be restarted after installation.

Rollout considerations

We want your SafeCom solution to be easy to administer and yield high user satisfaction. The following sections describe how you can make your SafeCom solution a successful one.

Test solution prior to rollout

Before you roll out your SafeCom solution, test it to make sure that everything works as expected.

Inform and prepare your users

A SafeCom solution affects the way users print. It is very important for an organization to use the channels available to them to inform users how their daily work is affected.

Even though the SafeCom solution is easy to use, we urge you to schedule a couple of short user sessions at a SafeCom-enabled device. During these sessions, demonstrate the SafeCom solution, allow users to try it hands-on, and answer any questions they may have.

You may wish to temporarily post an instruction sheet at SafeCom-enabled devices. These instructions should briefly introduce new users to how they should operate the SafeCom-enabled device.

Clearly define responsibilities and procedures

The overall responsibility for the SafeCom solution should be assigned to a single person. That way there will be no doubt as to who is responsible.

You need to decide who should have technician and administrator [rights](#).

If your organization has a help desk you should ensure that help desk staff feel comfortable with the SafeCom solution and are capable of answering questions and resolving or escalating problems relating to the SafeCom solution. We encourage you to include your help desk contact information on the Instruction sheets you can post at your devices.

You can also include help desk contact information on the "OUT OF ORDER" screen, which the SafeCom Front-end displays when communication is lost to the SafeCom server. The SafeCom Front-end returns to normal operation by itself a couple of minutes after communication is restored.

The person responsible for the SafeCom solution should ensure that administrative procedures are in place for the following:

- [Backup and restore](#)
- When you need to add new users (see [Add users manually](#))
- When users lose their ID card (see [User has lost ID card](#))
- When users forgets their ID code (see [User has forgotten ID code](#))
- When users forget their PIN code (see [User has forgotten PIN code](#))

Preemptive support and diagnostic tools

The following subsections describe the support and diagnostic tools.

Event log and e-mail notification

The SafeCom server writes information to its [event log](#). You can access the event log from the **Servers** menu in the SafeCom Administrator. Events older than one year are automatically deleted from the database.


Furthermore, the administrator can receive service and error (event log) messages through [e-mail](#).

scping

Use the supplied command line utility "scping" to search for SafeCom servers.

The syntax is as follows:

```
scping [Group|Ip|-h:Host|-b:IpMask [-c]] [-x:Host:Port] [/?]
```

 On Windows 64-bit, the program is called scping64.exe.

The variables in the syntax have the following meaning:

Group

Broadcast for server group.

Ip

Ping server on specified IP address.

-h:Host

Ping server on specified host.

-b:IpMask

Broadcast for servers on specified subnet.

-c

Try to connect server to confirm it is running.

-x:Host:Port

Try to establish a connection to Host using Port.

```
scping MyServerGroup
scping 10.0.0.10 -c
scping -h:MyServer -c
scping -b:10.255.255.255
scping -x:MyServer:7700
```

SafeCom services and processes

After SafeCom is installed, the following two services are running on the computer:

- **SafeCom Service** (scSafeComService.exe)

The service is responsible for the control and monitoring of SafeCom processes detailed in the next section. If one of the processes fails, it terminates all of them, along with the SafeCom Service itself.

- **Kofax Ethernet Card Reader controller service** (DeviceControlService.exe)

The service manages the ethernet card readers. It handles the configuration of the readers and receives card swipe events from them. It is the bridge between the readers and the local job server process.

SafeCom processes

- `scBroadcastServer.exe`

The process manages the identification requests from other external SafeCom components, such as device servers, devices, print clients, and so on. It indicates that the services are up and running and provides information about the features of the running components.

- `scJobServer.exe`

It is the central component of the server. It manages the configuration data when it runs on the primary application server. It also controls the user workflows at the devices. It communicates with the other the processes.

- `scMoneyServer.exe`

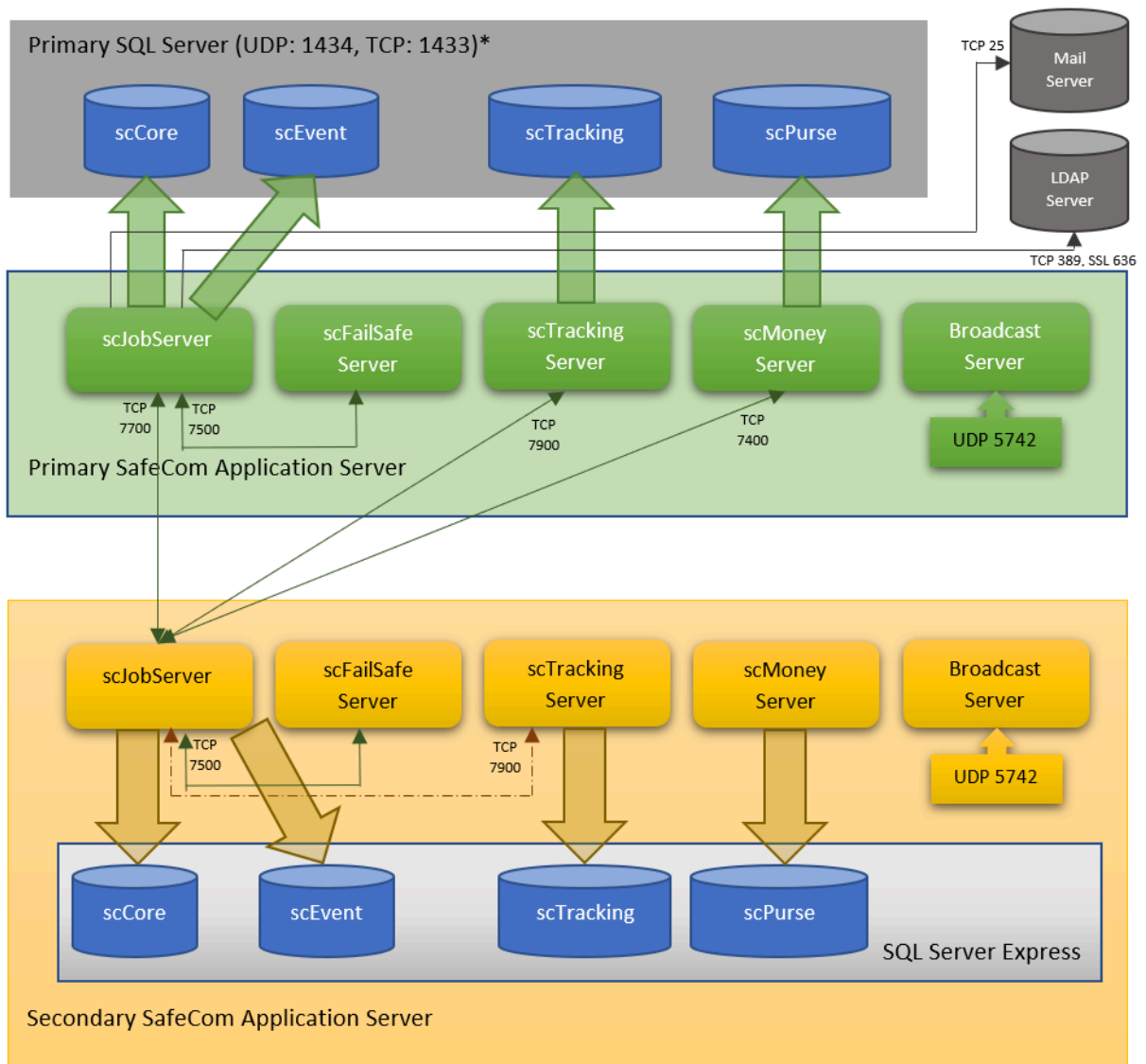
It has a role in the Pay environment when the users are charged for their jobs at the devices. It maintains the user accounts.

- `scTrackingServer.exe`

It manages the tracking data related to the MFP jobs.

- `scFailSafeServer64.exe`

It continuously monitors the members of DWS groups. It retrieves the actual configuration data from the local job server. Whenever a node fails, it reconfigures the affected devices by connecting them to a running service in the group. As the node restarts, it restores the original configuration of the devices.



The diagram above shows how the SafeCom processes cooperate with each other and their databases. Two possible ways of job tracking are shown. The tracking server of the primary application server stores the job data collected by job server from the devices. It is called online tracking. In case of offline tracking, the tracking server of the secondary application server collects the data, and the data is transferred to the primary tracking database by an offline background process controlled by the primary job server and the two tracking servers.

TCP and UDP port numbers used by SafeCom

TCP	Usage	Protocol
25	Used for sending e-mails from SafeCom Server, SafeCom Controller and device	SMTP
80	Used by SafeCom Administrator to display devices' configuration page in browser. It is also used in outbound connection by HP Unified Client to connect to a device during log off procedure.	HTTP
110	SafeCom Mobile Print - e-mail print	POP3
143	SafeCom Mobile Print - e-mail print	IMAP
389	Used for user import from Active Directory (AD)	LDAP
443	Used by Device Server to contact MFP during operation	HTTPS
465	SafeCom G4 Server e-mail and SafeCom Mobile Print - e-mail print	SMTP SSL
587	SafeCom G4 Server e-mail	SMTP STARTTLS
636	Used for user import from Active Directory (AD) if this needs to be secure via SSL/LDAPS	LDAPS
993	SafeCom Mobile Print - e-mail print	IMAP SSL
995	SafeCom Mobile Print - e-mail print	POP3 SSL
1433	Used by default for replication between Microsoft SQL servers. May be different on your server. Named instances use dynamic ports. Can be specified during advanced installation (Server installation (Advanced)).	TCP
2939	Kofax Ethernet Card Reader controller service configures the reader using this port	TCP
5420	Kofax Ethernet Card Reader controller service receives card swipe events from the reader	TCP
5740	Used by the SafeCom Pull Port and SafeCom Push Port and SafeCom PopUp dialog (in compatibility mode for scPopup.exe, when communicating with older versions of PopUp) for presenting dialogs on users' screen.	TCP
5742	Used between the SafeCom Administrator and SafeCom Go, SafeCom Device Server and SafeCom Controller.	TCP (SafeCom)
5743	Used between the SafeCom Administrator and SafeCom Go, SafeCom Device Server.	TCP (TLS 1.2)
5745	Used between from SafeCom Device Server 9.13 and HP Future Smart device	TCP
5799	Opened by SafeCom Device Server. Administrator before 10.6 uses for retrieving status devices	TCP
7290	SafeCom Mobile Print - web print	HTTP

TCP	Usage	Protocol
7400	Used between the SafeCom Job Server(s) and the SafeCom Money Server. In a multiserver solution port 7400 is used from the secondary Job Server to the primary Money server. In case of a single server solution the communication does not go onto the network, but the port still needs to be open.	TLS 1.2 / SafeCom
7500	SafeCom devices connect to SafeCom Job Server. Fail Safe Server and Kofax Ethernet Card Reader controller service also use this port to communicate with the local Job Server.	TLS 1.2 / SafeCom
7501	Kofax Ethernet Card Reader controller service opens this port to receive commands from the local Job Server. It refuses connections from external IP addresses.	
7600	Used between the SafeCom devices and SafeCom Print Client version S82 070.410 and older. SafeCom Print Client version S82 070.420 and newer use port 7700.	SafeCom
7627	SOAP Interface on HP FutureSmart devices	HTTPS
7700	SafeCom Job Server and Print Client open this port. SafeCom Job Server SafeCom applications, printer port monitors, Device Server and Device Web Server use this port to connect to Job Server. Print Client SafeCom port monitors and pull devices use this port	TLS 1.2 / SafeCom
7723	Used for TELNET connection to the SafeCom Job Server to control the SafeCom Trace Facility.	TELNET
7900	Used between the SafeCom Job Server(s) and the SafeCom Tracking Server. In a multi server solution with offline tracking outbound port 7900 is used from the primary Job Server to the secondary Tracking server(s). With online tracking port 7900 is used from the secondary Job Server to the primary Tracking server. In case of a single server solution the communication does not go onto the network, but the port still need to be open.	TLS 1.2 / SafeCom
8080	Device Server Configuration UI	HTTP
8444	Used for HP Unified Client for SafeCom (DWS) operation only.	HTTPS
9100	Used by Job Server and Print Client for sending print data to the device through TCP/IP (raw).	RAW
9443	SafeCom Mobile Print - web print	HTTPS
50001	Used between up to SafeCom Device Server 9.12 and HP Future Smart device	TCP
50002	Device Server receives connections from the devices. Device Server Configuration UI is also accessible through this port. SafeCom Administrator 10.7.0.1 uses to this port to retrieve status of devices and manage device configuration.	HTTPS
50003	Used between the SafeCom Device Server and a Konica Minolta device	HTTPS

i New versions of SafeCom print monitors use asynchronous print notification channels to communicate with SafeCom Popup. TCP port 5740 is only for backwards compatibility for Popup versions earlier than 520.10.

UDP	Usage	Protocol
5742	Used by the SafeCom Job Server, SafeCom Go, SafeCom Device Server, SafeCom Controller and SafeCom applications to find each other through the SafeCom Broadcast Server.	SafeCom
5741	Used between the SafeCom Administrator and SafeCom Go, SafeCom Device Server and SafeCom Controller.	SafeCom
1434	Applications use this port to initially talk to the SQL server to determine which TCP port (default 1433) should be used.	SQL
161	Used between the SafeCom Administrator and SafeCom devices when adding devices or retrieving status. Used by Port Monitor if SNMP status is enabled.	SNMP

The following tables contain some typical SafeCom server and client installations and list what **inbound** and **outbound ports** should be open if a firewall, such as Windows Firewall (see [Windows Firewall](#)), is installed on the computer.

SafeCom Server	TCP		UDP	
	In	Out	In	Out
SafeCom primary server with local database	7400 7500 7700	25 80 389 636 5740 5742 7700 7900 ³ 8080 9100	5742	5742
External SQL server		1433 ⁴		1434

³ With offline tracking outbound port 7900 if used to collect tracking data from the secondary servers. With online tracking inbound port 7900 on the primary server must be open.

⁴ SQL server may use another TCP port than 1433.

SafeCom primary server with external SQL server	1433 ⁵ 7400 7500 7700	25 80 389 636 5740 5742 7700 7900 ⁶ 8080 9100	1434 5742	5742
SafeCom secondary server with local database	7500 7700 7900 ⁷	80 5740 5742 7400 7700 8080 9100	5742	5742
SafeCom secondary server with connection to Device Server and Device Web Server and with Ethernet card reader connected.	5420 7500 7700 7900	80 2939 5740 5742 5743 7400 7700 8080 8444 9100 50002	5741 5742	5741 5742

SafeCom Device Server	TCP		UDP	
	In	Out	In	Out

⁵ SQL server may use another TCP port than 1433.

⁶ With offline tracking outbound port 7900 if used to collect tracking data from the secondary servers. With online tracking inbound port 7900 on the primary server must be open.

⁷ With offline tracking inbound port 7900 if used to collect tracking data from the secondary servers. With online tracking outbound port 7900 on the secondary must be open.

SafeCom Device Server	5742	80	5741	161 5742
	5743	443		
	5799	5745		
	7800	7500		
	7801	7627		
	8080	7700 ⁸		
	50002	7801		
		50001 ⁹		
		50003 ¹⁰		

SafeCom Client and other	TCP		UDP	
	In	Out	In	Out
SafeCom Print Client	7700 ¹¹	7500 ¹² 7700 9100	5742	5742
Client with local SafeCom printers (Pull and Push Ports)		5740 7500 ¹³ 7700 9100		161
Client with SafeCom PopUp	5740			
Client with SafeCom Administrator		80 5742 5743 5799 7500 7700 8080 50002		161 5741

⁸ If the job is stored on a SafeCom Print Client version S82 070.410 or older, then port 7600 is also used.

⁹ SafeCom Go HP Device Server

¹⁰ SafeCom Go Konica Minolta

¹¹ SafeCom Print Client version S82 070.420 use port 7700. Previous versions also use port 7600.

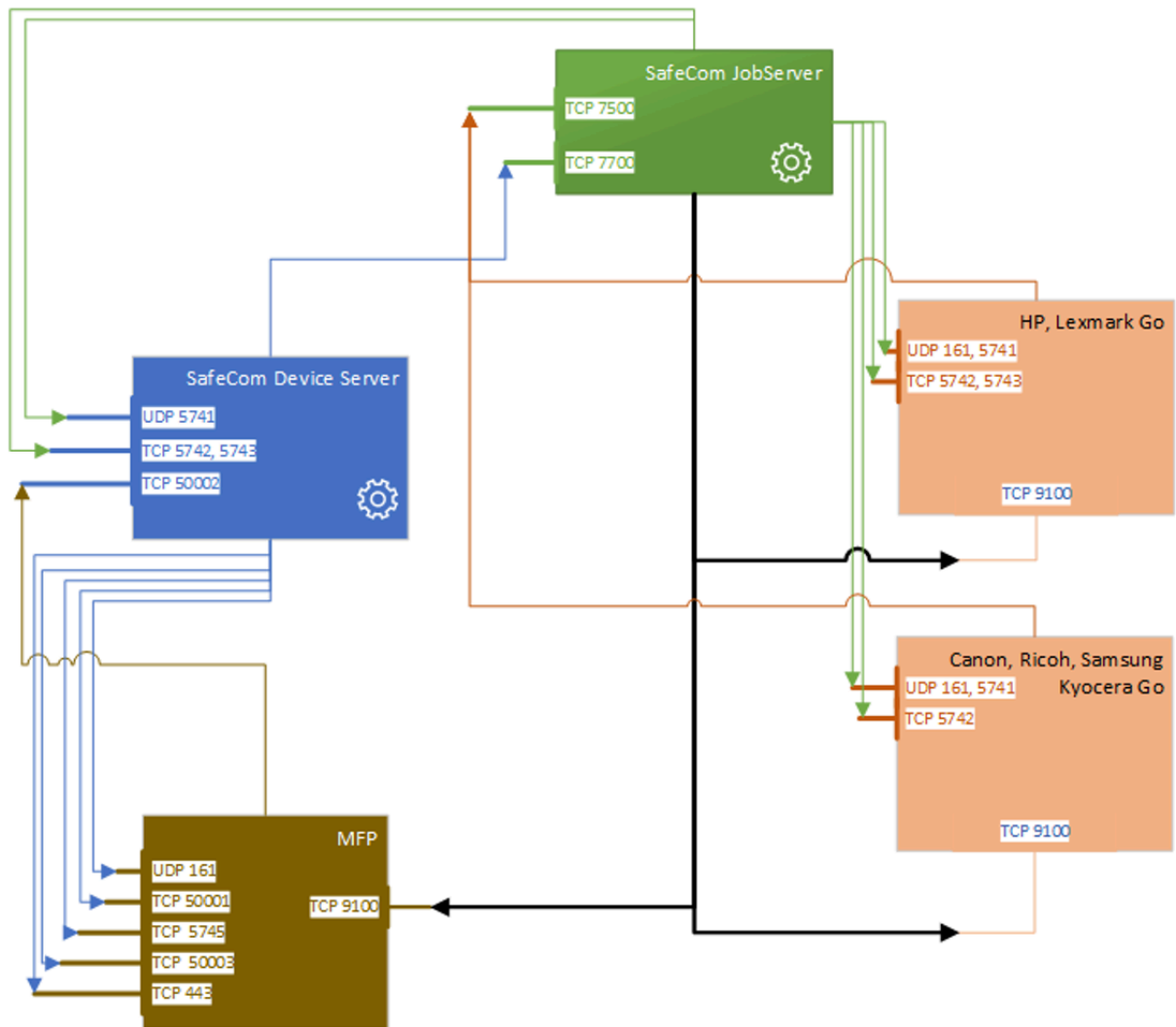
¹² SafeCom Print Client, by default, uses port 7500. However, if the SafeCom Print Client is running on a server, it is recommended to configure Default Server Port=7700 (see section [scPrintClient.ini file](#)). This means that the SafeCom Print Client keeps the connection open to the SafeCom server instead of opening and closing the connection for each job.

¹³ SafeCom Pull Port, by default, uses port 7700. However, if the SafeCom Pull Port is running on a client, it is recommended to configure Server Port=7500. This means that the SafeCom Pull Port opens and closes the connection for each document.

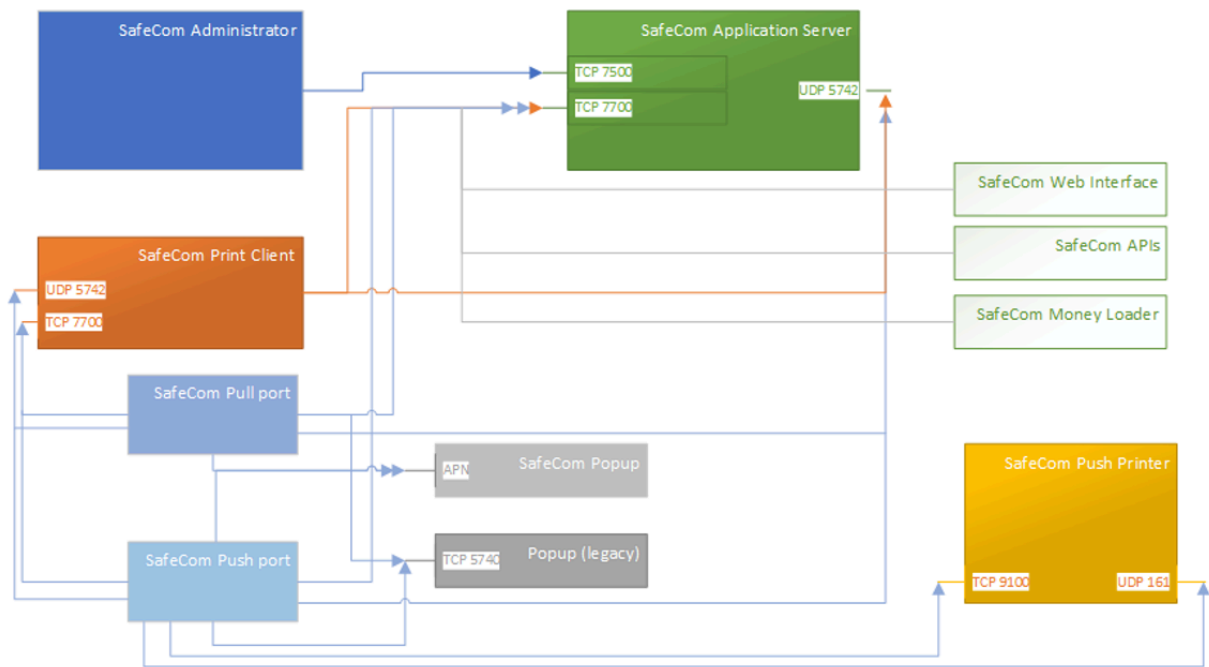
SafeCom Controller	80 5742	7500 7700 ¹⁴ 9100	161 5741	161 5742
SafeCom Web Interface	80 7700 8080	443		

SafeCom Mobile Print		TCP		UDP	
		In	Out	In	Out
SafeCom Mobile Print	Web print	7290 9443	7290 9443		
	Email print	110 143 993 995	25 465		

¹⁴ SafeCom Controller uses port 7700 to collect documents from SafeCom Print Client version S82 070.420. Port 7600 is used to collect documents from previous versions of SafeCom Print Client. Port 7500 is used to collect documents from SafeCom servers.



The diagram above shows the SafeCom components and their communication ports in device management and printing process.



The diagram above shows the SafeCom services and applications with their communication channels.

If multiple servers are used, each SafeCom secondary server will use TCP port 7900 to deliver tracking data to the SafeCom Tracking server on the SafeCom primary server, either continuously (online tracking) or scheduled (offline tracking). Refer to [Multiple servers: Online or offline tracking](#).

There is only one SafeCom Money Server and it resides on the SafeCom primary server. SafeCom secondary servers use TCP port 7400 to communicate with the SafeCom Money Server on the SafeCom primary server.

SafeCom SQL databases

The following databases are used:

- **SafeCom Job Database** Used by scJobServer.exe and scJobServer64.exe
- **SafeCom Event Log** Used by scEvent.dll
- **SafeCom Money Database** Used by scMoneyServer.exe and scMoneyServer64.exe
- **SafeCom Tracking Database** Used by scTrackingServer.exe and scTrackingServer64.exe. Also used for device logs.

Each SafeCom server in the server group has its own SafeCom Job Database and SafeCom Event Log. Events older than one year are automatically deleted from the database.

The SafeCom Tracking Database is only relevant if your solution includes the SafeCom Tracking or SafeCom Pay. The SafeCom Money Database is only relevant if your solution includes the SafeCom Pay.

A server group should only use one SafeCom Money Server. This is located on the SafeCom primary server by default.

SafeCom database update log

A number of scdbu*.log files are created in the SafeCom installation folder the first time the SafeCom Service is started after a new SafeCom server version has been installed. The files are created whether or not trace is enabled.

Windows registry settings

Use the Windows **regedit** program to view Windows registry settings. Settings for the SafeCom Server software are stored at:

- HKEY_LOCAL_MACHINE\SOFTWARE\SafeCom\SafeComG4

Settings for the SafeCom Port Monitors are stored at:

- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\ Print\Monitors\SafeCom Pull Port
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\ Print\Monitors\SafeCom Push Port


Backup and restore

We recommend you have backup and restore processes in place for your SafeCom solution. With well-defined and tested processes, it is possible to reduce downtime. With Microsoft Cluster Service (MSCS), the downtime can be reduced even further.

If a Service Level Agreement (SLA) exists, it may specify the accepted downtime. The shorter the time period specified, the more prepared you must be to restore the SafeCom solution, and the more evident is the need for a clustered SafeCom solution.

When devising the backup and restore processes, you should consider the following:

- [Standby computer](#) to replace a faulty one.
- Backup and restore [SafeCom Windows registry settings](#).
- Backup and restore any [customized SafeCom files](#).
- Backup and restore [printer configurations](#).
- Backup and restore [SafeCom databases](#).

 The described processes do not include backup and restore of users' uncollected and retained documents.

Standby computer equipment

If you have a complete standby computer, you are in a good position to immediately replace your primary computer if a serious failure occurs. If the standby computer is dedicated to the SafeCom

solution, you can reduce downtime even further by ensuring that it is pre-loaded with the right Windows operating system and SafeCom software.

The SafeCom server software must be the same version as on the computer it is to replace. This is particularly important in a multiserver solution where all the computers in the SafeCom group must be on the same SafeCom server version. See [Installation](#).

To secure a smooth transition to the new server, it should inherit the server address and the computer name of the one it is replacing. That way, all references from SafeCom-enabled devices and SafeCom ports to the SafeCom server will remain valid. You should either secure that your DHCP server will give the new server the same IP address or you should give it a static IP address.

You can further reduce downtime if the standby computer is already updated with the more static SafeCom Windows registry settings (see [SafeCom Windows registry settings](#)), customized SafeCom files (see [Customized SafeCom files](#)), and printer configurations (see [Printer configurations](#)). That way, you can reduce the restore process to restoring the backup of the SafeCom databases.

If the computer is on a SafeCom secondary server, it automatically gets its SafeCom databases restored, because the SafeCom primary server handles this as part of the replication process. It is recommended to [reinitialize the subscription](#).

SafeCom Windows registry settings

It is particularly important that the location of print files, as specified by the Windows registry setting "File Path" (see [Change location of SafeCom print files](#)), is the same on both the standby computer and the current computer. Follow the steps below to backup and restore the SafeCom Windows registry.

Backup

1. Open the Registry Editor and browse to `HKEY_LOCAL_MACHINE\SOFTWARE\SafeCom\SafeComG4`.
2. In the **File** menu, click **Export**.
3. Specify the file name and click **Save**.

Restore

Double-click the backup registry file and click **Yes** when asked to update the Windows registry.

Customized SafeCom files

The files listed below are typically customized or translated.

- EmailWelcome.txt, EmailPUK.txt, EmailWarning.txt, and EmailJobDelete.txt (see [Customize and translate e-mail messages](#))
- ExcludeJobNames.txt (see [Shorten job names in document list](#))
- JobNamePricing.txt
- EmailBilling.txt (see [Edit the template for billing reminder](#))
- EmailCode.txt (see [Customize and translate e-mail messages](#))

- EmailDelegateAccept.txt, EmailDelegateReject.txt, EmailDelegateRequest.txt (see [Customize and translate e-mail messages](#))
- IDCodeGenerating.txt (see [Customize the format of ID codes](#))
- UnfinishedJob.txt (see [E-mail template for an unfinished job](#))

Printer configurations

The Microsoft Print Migrator 3.1, available at microsoft.com/printserver, can back up and restore all print shares and user permissions.

The Print Migrator does not back up the actual SafeCom Pull Port and SafeCom Push Port monitors, only the ports' attributes. Prior to the restore operation, you must reinstall the original set of SafeCom port monitors to ensure complete functionality.

Print Migrator comes with a command line interface "printmig" that uses the following switches:

-?

Help

-b

Backup

-r

Restore

If the computer is clustered, you must backup the cluster's virtual server with the following command:

```
printmig -b \\filesrv\backup\printers.cap \\clustergroupname
```

Here, `clustergroupname` is the network name of the virtual server that contains the Print Spooler resource.

The "printmig" can be integrated into a job scheduler, such as the Scheduled Task mechanism in Microsoft Windows. Please refer to online help in Windows.

SafeCom database - backup and restore

This section explains how to back up and restore the SafeCom databases. SafeCom can work with the below two versions of the SQL databases.

- Microsoft SQL server must be purchased and licensed from Microsoft. Backup can be performed by using Microsoft SQL Server Management Studio or an SQL client tool that comes with the Microsoft SQL server. Alternatively, you can use the Transact-SQL BACKUP DATABASE statement and run the SQL command line utility, "osql.exe". Make sure to configure it to backup the transaction log files and keep them from growing endlessly.
- Microsoft SQL Express 2019 is distributed with SafeCom. No license is required from Microsoft. Database size is limited to 10 GB.

The SafeCom databases are created to use full recovery model in contrast to simple recovery model. This can lead to large transaction logs if no scheduled backup is put in place from the beginning.

i We recommend you establish a nightly scheduled full backup with a maintenance plan that minimizes the size of transaction logs. In a multiserver solution, a database backup should also be scheduled for the secondary server to keep the database transaction log files from growing. The backup itself is not really needed, as data is replicated from the SQL primary server. The provided [scBackup](#) program also backs up LDF files and prevents them from growing endlessly.

Go to microsoft.com for more information on the Microsoft SQL tools and utilities mentioned above. To back up the database, use the supplied SafeCom command line utility [scBackup](#).

All SafeCom print files are by default stored in the folder:

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

Database files are by default stored in the folder:

```
C:\Program Files\Microsoft SQL Server\MSSQL12.SAFECOMEXPRESS\MSSQL\DATA
```

scBackup

As mentioned in [SafeCom database - backup and restore](#), you can use the supplied command line utility [scBackup](#) to back up the SafeCom databases. [scBackup](#) must be run as administrator. The user running [scBackup](#) must be a local administrator on both the SafeCom server where the tool is located and on the SQL server. The user running the tool must also have the relevant permissions to perform backup and restore on the SQL database. The program works only if the database is set to use a full recovery model.

The syntax is as follows:

```
scBackup.exe -b | -r {path}
```

i On Windows 64-bit, the file is called [scBackup64.exe](#).

Here, `-b` specifies to backup data in the specified path and `-r` specifies to restore data from the path. The backup results are in the files `score.bak`, `scevent.bak`, `scpurse.bak`, and `sctracking.bak`.

i To restore successfully, the SafeCom server version must not change from the time of backup to the time of the restoration.

Example:

```
scBackup.exe -b C:\backup
```

During restoration (`-r`), [scBackup](#) attempts to stop the SafeCom service and subsequently restart the SafeCom service. This does not work in a Microsoft Cluster environment or if other services depend on the SafeCom service. In such cases, the SafeCom service must be manually stopped and started.

[scBackup](#) can be integrated into a job-scheduler, such as the Scheduled Task mechanism in Microsoft Windows. Please refer to online help in Windows.

i scbackup might fail if the backup is made from a database that is newer than the database used to restore job. Instead, use an SQL Studio manager that is capable of handling both database versions for both the backup and the restore job.

SafeCom database - maintenance

This section explains how to maintain the SafeCom databases, that is, preventing the size of the databases from growing endlessly. Backup and restore, including the process of minimizing transaction logs, is covered in (see [SafeCom database - backup and restore](#)). In tracking solutions, the tracking database (sctracking) will usually grow to a significant size, whereas the job database only grows slowly. The size of the job database depends on the number of users and devices. For each job tracked by SafeCom, there is an equivalent record in the tracking database (2 KB / tracking record).

When offline tracking is enabled, which by default it is, the tracking database on the SafeCom secondary server is automatically emptied every time the SafeCom primary server has collected the tracking data.

However, the tracking database on the SQL primary server is not emptied and continues to grow. It is recommended to establish a procedure for exporting and deleting old tracking data to keep the database size within the defined limits.

Tracking data can be exported and deleted directly using SQL tools. Alternatively, the SafeCom Administrator API's ExportTracking or DeleteTracking commands can be used.

This housekeeping process should handle the tables scMoneyLoaderTracking, scSanityTracking, and scTracking.

In Pay solutions, both the tracking database (sctracking) and the money database (scpurse) continue to grow. Even though a money database exists on each server, only the money database on the SQL primary server is used. This is because there must only be one single point to store and maintain users' credits. The housekeeping process should handle the table scTransaction.

The SafeCom event database (scevent) automatically deletes events that are more than one year old.

SafeCom server trace facility

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

Enable trace

1. Stop the SafeCom Service (see [Start and stop the SafeCom service](#)) and the Print Spooler.
2. On the SafeCom server, create the folder `C:\safecom_trace`.
3. Start the SafeCom Service and the Print Spooler.

Stopping the SafeCom Service and the Print Spooler and then deleting the folder `C:\safecom_trace` disables the trace again. The [trace files](#), by default, occupy maximum 220 MB of disk space.

Trace can also be turned on/off without disrupting the SafeCom Service through a TELNET interface (see [TELNET interface](#)). This interface can also be used to configure the trace facility, including the size and location of the trace files.

The SafeCom Service executes the supplied `scStartup.cmd` file in the installation folder before starting. By editing the `scStartup.cmd` file, it can be used to copy (and compress) the trace files before they are reset.

Trace files

Use the SafeCom Trace Facility only if SafeCom Support instructs you to do so.


Trace files are by default stored in the folder `C:\safecom_trace`.

To change the default location of the trace files, use the [TELNET interface](#) or modify these Windows registry settings:

HKEY_LOCAL_MACHINE\SOFTWARE\SafeCom\SafeComG4\Trace

For 32-bit applications (for example, `scAdministrator` or `scDevUtil`), the path is:

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\SafeCom\SafeComG4\Trace

Value name (Type)	Value data
Enabled (REG_DWORD)	0 = Disabled 1 = Enabled Default value is 0.
TracePath (REG_SZ)	Location for the trace files. The folder must be created before starting the service. <div style="background-color: #e6f2ff; padding: 5px;"> <p> If you change the location, ensure that the new path ends with a backslash (\). The location change requires restarting the SafeCom and Print Spooler services for the trace files to be created at the new location. For <code>keyManager.trc</code>, a computer restart is required for the location change.</p> </div> <p>Default location is <code>C:\safecom_trace\</code>.</p>
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.

i If any SafeCom service fails, the SAFECOM_TRACE folder is created on C: and the DMP files are created in that folder. This is the only scenario when the SAFECOM_TRACE folder is created automatically.

Contents of the trace folder can vary depending on the SafeCom installation. Below are the names of some of the typical SafeCom trace files.

The total number of trace files depends on the SafeCom installation as well as the workstation it is installed on.

The following trace file names are available:

- AdmClient<number>.trc
- AdmGui<number>.trc
- BroadcastServer<number>.trc
- DeviceControlService.txt
- DevMonServer<number>.trc
- DevUtil<number>.trc
- JobServer<number>.trc
- keyManager<number>.trc
- MoneyServer<number>.trc
- PortConfigurator<number>.trc
- PullPM2kSrv<number>.trc
- PullPM2kUI<number>.trc
- PushPM2kUI<number>.trc
- SafeComService<number>.trc
- SafeComWeb<number>.trc
- SafeComWebconfig<number>.trc
- scCoInstall<number>.trc
- scDevMonServer<number>.trc
- scPopUp<number>.trc
- scPrintClient<number>.trc
- TrackingServer<number>.trc
- SafeCom.XpsPrint.Service.trc

TELNET interface

Through the TELNET interface, it is possible to enable, disable, and configure the SafeCom server trace facility. Use of TELNET can be disabled by changing the Windows TELNET Server's Registry setting "TelnetPort" value to 0. Alternatively, create a DisableTelnet DWORD registry setting

under `HKEY_LOCAL_MACHINE\SOFTWARE\SafeCom\SafeComG4`, set its value to 1, and restart the SafeCom service.

1. From the command prompt window, issue the "telnet" command by entering `telnet <address> 7723`.

The SafeCom server prompts you for a username and a password of a SafeCom user with administrator rights.


2. Enter the username and password.

The default username is admin and the default password is nimda.

Once you are logged in, you will see the prompt `sc.tel`.

3. Enter any of the TELNET commands below.

- **help** – online help.

 You can type **help** to see additional TELNET commands, or **help <command>** to get help on a specific command.

- **logoff** – logs off from the TELNET session.
- **multiple info** – lists all open connections.
- **server info** – lists the status of servers (see [Failover servers](#)).
- **server db info** – lists database info.
- **server restart OK <servername>** – restarts the server.
- **trace info** – information about current trace setup.
- **trace off** – disables trace.
- **trace on** – enables trace.
- **trace path <path>** – specifies a new location for the trace files.
- **trace size <n>** – sets the maximum size (in kilobytes) of a trace file.
- **trace Store** – writes the trace setup into Windows registry.

4. To close the TELNET session, enter logoff.

SafeCom device trace facility

To further assist the troubleshooting process, it is also possible to obtain information from the SafeCom-enabled device.

- **SafeCom Controller:** The SafeCom Controller contains a debug interface. Instructions on how to use enable and use this is forwarded on a per-case basis.
- **SafeCom Go:** Please refer to the *Troubleshooting* chapter in the appropriate *SafeCom Go Administrator's Guide*. See the available documentation in [Related documentation](#).

Chapter 3

Installation

The installation of software and hardware is described in the appropriate *Kofax SafeCom Go Administrator's Guide*. See the available guides in [Related documentation](#).

This chapter covers SafeCom installation, including multiserver (see [Multiserver installation](#)) and cluster installation (see [Cluster installation](#)).

 Use the forms in [Administrator's installation notes](#) to record your SafeCom solution information.

Installation methods

SafeCom has two installation options.

Basic server installation


This method quickly installs the SafeCom server software and its required components to a default location. See [Server installation \(Basic\)](#).

Advanced installation

This method allows using an existing SQL server and also allows specifying the location of SafeCom program files, print files, and the database. See [Server installation \(Advanced\)](#).

This method also allows client and tool installation. See [Client installation](#) and [Tool installation](#).

Server installation (Basic)

 See [Server requirements](#) for software prerequisites and install these prior to the installation of the SafeCom G4 Server.

Basic installation is recommended for those who want to set up the following:

- A single-server system with default settings
- A secondary node for a multiserver system with default settings

Microsoft SQL Express 2019 is also installed if **Basic installation** is selected. The installed instance name is SAFECOMEXPRESS.

If you want to have one of the two configurations but with customized settings, select **Advanced installation** (see [Server installation \(Advanced\)](#)).



- Installing the Microsoft Redistributable Package (x86) may take minutes, depending on your system. During this time, the installation process may appear to be non-responsive. Wait a few minutes to ensure that the installation proceeds normally.
- Make sure that the computer has no pending installations. SafeCom G4 verifies it and prompts for computer restart if necessary.

1. Download the SafeComG4_Server_x64_build_{version_number}.exe file from the link supplied to you. The installation must be run as administrator. When the installation program is launched, click **Next**.

2. Read and accept the end-user license agreement, then click **Next**.

3. Click **Basic server installation**, then click **Next**.

4. Select the authentication method to connect to SafeCom databases.

- **SQL Authentication**

A new SQL user is created called "safecom" with system administrator (sysadmin) role granted. The SafeCom service runs under the Local System account.

- **Windows Authentication**


Create a service account in your Windows domain before installing SafeCom and enter its credentials in the installer window. System Administrator (sysadmin) role is granted for this account and for the one that runs the installer. The SafeCom service runs under this Windows account. Permission to "Log on as a service" must be granted.



- System administrator role is mandatory because the SafeCom databases are created on behalf of this user, and database table changes in an upgrade scenario are also performed with this account.
- In a multiserver system, the same Windows account must be selected on all servers at installation, and System administrator role must be granted on the primary SQL server instance you plan to use with SafeCom. For more information, see [Add Windows service account to the SQL server](#). The SafeCom service runs under this account.
- Ensure that the selected service account has proper access rights to the private key of the certificate specified in the TlsCert registry entry, which is created by SafeCom itself under HKLM\Software\SafeCom\SafeComG4. As several components of SafeCom (G4, PrintClient, Port) use this certificate/key pair, ensure that all accounts running the components have proper access rights. If you are using a service user account for SafeCom G4, ensure it has administrator access.
- Changing your SQL authentication when upgrading your existing installation is not supported. In such cases, remove your existing SafeCom installation (see [Uninstall SafeCom software](#)) and perform a clean installation where you select your SQL authentication method.
- In rare cases, the installer may display a message to remind you about creating a "safecominstall" user. Ignore this message.

The current settings are displayed.

5. Click **Install** to accept and start the installation. The Print Spooler is restarted and the SafeCom service is started at the end of this process.
6. Click **Finish** to launch the [SafeCom Administrator](#).
7. If Windows Firewall is on, open the ports as specified in [Windows Firewall](#).
8. Optionally, configure your encryption settings (see [Configure encryption between SafeCom components](#)).

 The product installer creates a log file at this location: {COMMON_APPDATA}\Temp\scInstG4Server.log. Its default path is C:\ProgramData\Temp\scInstG4Server.log.

Server installation (Advanced)

Advanced installation is used when you need to specify a specific SQL server instance (for example, primary SQL server in a SafeCom multiserver environment) or if you want to specify folder locations for print jobs or folder location for the Microsoft SQL Express 2019 instance. For prerequisites and details on multiserver installations, see [Multiserver installation](#).

1. Download the SafeComG4_Server_x64_build_{version_number}.exe file from the link supplied to you. The installation must be run as administrator. When the installation program is launched, click **Next**.
2. Read and accept the end-user license agreement, then click **Next**.
3. Click **Advanced installation**, then click **Next**.
4. Click **Server**, then click **Next**.
5. Select the authentication method to connect to the SafeCom databases.

- **SQL Authentication**

A new SQL user is created called "safecom" with system administrator (sysadmin) role granted. The SafeCom service runs under the Local System account.

- **Windows Authentication**

Create a service account in your Windows domain before installing SafeCom and enter its credentials in the installer window. System Administrator (sysadmin) role is granted for this account and for the one that runs the installer. The SafeCom service runs under this Windows account. Permission to "Log on as a service" must be granted.



- Ensure that the selected service account has proper access rights to the private key of the certificate specified in the TlsCert registry entry, which is created by SafeCom itself under HKLM\Software\SafeCom\SafeComG4. As several components of SafeCom (G4, PrintClient, Port) use this certificate/key pair, ensure that all accounts running the components have proper access rights. If you are using a service user account for SafeCom G4, ensure it has administrator access.
- Changing your SQL authentication when upgrading your existing installation is not supported. In such cases, remove your existing SafeCom installation (see [Uninstall SafeCom software](#)) and perform a clean installation where you select your SQL authentication method.

6. Select the location for the SafeCom program files, then click **Next**.

7. Select the location for print files, then click **Next**. See [Store print files on an external file share](#) if you choose to use an external file share.
8. Select the preferred SQL server and click **Next**.
 - a. Install Microsoft SQL Express 2019 using the default data location.
 - b. Install Microsoft SQL Express 2019 and specify the data location.
Select this to specify the location of the SQL database files.
 - c. Use an existing SQL server.
To use this option, you must know the instance name before the installation.
Enter the SQL server as `computername\instancename` or `computername` if there is no named instance of the SQL server. The instance name is case sensitive. The instance name SAFECOMEXPRESS is reserved for SafeCom and must not be used to name an SQL server instance.



- If Microsoft SQL Express 2019 is installed (see [8.a](#) or [8.b](#)) and SafeCom authentication is selected, the safecom SQL user is created with sysadmin role granted.
- If Microsoft SQL Express 2019 is installed (see [8.a](#) or [8.b](#)) and Windows authentication is selected, the selected service user is added as an SQL server user with sysadmin role granted. The same is true for the account that runs the installer.
- On the existing SQL server (see [8.c](#)), you must create an intermediate SQL user called "safecominstall" (see [Create intermediate SQL user: safecominstall](#)) with sysadmin role granted. This user is used for creating SafeCom databases. After the software is installed, this user can be deleted.
- On the existing SQL server (see [8.c](#)), you must add the selected service account to the SQL user with sysadmin role granted before starting the installation.
- System administrator role is mandatory for each case, because database management operations are performed on behalf of this user ("safecomuser" or the service account) at installation or during software update (see [Add Windows service account to the SQL server](#)).


The current settings are displayed.

9. Click **Install** to accept and start the installation.
The Print Spooler is restarted at the end of this process.
10. Click **Finish** to launch SafeCom Administrator (see [SafeCom Administrator](#)).
11. If Windows Firewall is on, then open both the inbound and outbound ports as specified in [Windows Firewall](#) and make the SQL server use the fixed TCP port 1433 (see [Windows Firewall – Make SQL use fixed port](#)). You can use the SafeCom-provided firewall script to open the ports.



If the SQL server is to use a fixed port other than 1433, you can edit the SafeCom-provided firewall script to include the desired port.

12. Optionally, configure your encryption settings (see [Configure encryption between SafeCom components](#)).

 The product installer creates a log file at this location: {COMMON_APPDATA}\Temp\scInstG4Server.log. Its default path is C:\ProgramData\Temp\scInstG4Server.log.

Client installation

A client installation is relevant if you intend to:


- Create a [shared SafeCom Pull Printer](#) or SafeCom Push Printer on a Windows print server.
- Create a [local SafeCom Pull Printer](#) or SafeCom Push Printer on clients.

Follow these steps to perform a client installation.

1. Download the SafeComG4_Server_x64_build_{version_number}.exe file from the link supplied to you. The installation must be run as administrator. When the installation program is launched, click **Next**.
2. Read and accept the end-user license agreement, then click **Next**.
3. Click **Advanced installation**, then click **Next**.
4. Click **Client**, then click **Next**.
5. Select the location for the SafeCom program files, then click **Next**.
The current settings are displayed.
6. Click **Install** to accept and start the installation.
The Print Spooler is restarted at the end of this process.
7. Click **Finish**.

Tool installation

You only need to perform a tool installation if you want to administer your SafeCom solution from multiple computers.


- 
- Before installing tools, ensure that your Windows operating system is fully up-to-date.
 - SafeCom Administrator requires elevated access to the computer.
 - Upgrading an already existing G4 tool installation is not recommended due to the changes in G4 functionality. Uninstall the existing one and install the new one.

Installing SafeCom Administrator also installs the files required to run the SafeCom Administrator API (AdmClient.exe) and the SafeCom Batch Print API (scClient.exe). Select the SafeCom Port Configurator to install it.

Follow these steps to perform the tool installation.


1. Download the SafeComG4_Tools_x64_build_{version_number}.exe file from the link supplied to you.
2. Run the installation file as administrator.
3. When the installation program is launched, click **Next**.
4. Read and accept the end-user license agreement, then click **Next**.
5. Click **Advanced installation**, then click **Next**.

6. Click **Tools**, then click **Next**.
7. Select the tools you wish to add, then click **Next**.
8. Select the location for the SafeCom program files, then click **Next**.
The current settings are displayed.
9. Click **Install** to accept the current settings and start the installation.
If the installation includes SafeCom Port Configurator, the Print Spooler is restarted at the end of this process.
10. Click **Finish**.

 The product installer creates a log file at this location: {COMMON_APPDATA}\Temp\scInstTools.log. The default path is C:\ProgramData\Temp\scInstTools.log.

SafeCom G4 Server installer command line options

The command-line options for the SafeCom G4 Server installer are presented in this section. The installer uses the InnoSetup technology. The section includes the standard InnoSetup switches and the custom SafeCom specific ones.

 The command line options are case insensitive.

Standard Inno setup switches

/VERYSILENT

Very silent display option.

The installer runs an installation without displaying a user interface. No prompts, messages, or dialog boxes are displayed to the user. The user cannot cancel the installation.

Use the `/NORESTART` and `/SUPPRESSMSGBOXES` standard command line options to control reboots. If no reboot options are specified, the installer restarts the computer whenever necessary without displaying any prompt or warning to the user.

Silently install the program, prevent restarting the system.

```
setup.exe /VERYSILENT /SUPPRESSMSGBOXES /NORESTART
```

/SILENT

Silent display option.

The installer displays a progress bar to the user that indicates that an installation is in progress but no prompts or error messages are displayed to the user. The user cannot cancel the installation.

Use the `/NORESTART` and `/SUPPRESSMSGBOXES` standard command line options to control reboots. If no reboot options are specified, the installer restarts the computer whenever necessary without displaying any prompt or warning to the user.


/SUPPRESSMSGBOXES

Instructs 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.

 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.

/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` or `/VERYSILENT`.

/NORESTART

Prevents Setup from restarting the system following a successful installation or after a **Preparing to Install** failure that requests a restart. Typically used along with `/SILENT` or `/VERYSILENT`.


/DIR="x:\dirname"

Overrides the default directory name displayed on the Select Destination Location wizard page. A fully qualified pathname must be specified. May include an `expand:` prefix which instructs Setup to expand any constants in the name. For example: `/DIR=expand:{autopf}\My Program`.

 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. Use quotation marks if the filename contains spaces.

 Only use a file that you previously created with the `/SAVEINF` switch.

```
Setup.exe /LOADINF="%USERPROFILE%\Desktop\srvsetup.inf" /LOG="%USERPROFILE%\Desktop\srvinstall.log" /VERYSILENT /NORESTART /SUPPRESSMSGBOXES
```

/SAVEINF="filename"

Instructs Setup to save installation settings to the specified file. Use quotation marks if the filename contains spaces.

 The installer changes the contents of the `.inf` file continuously during the entire installation. The contents of the `.inf` file are considered completed if the installation process is completed successfully.


```
Setup.exe /SAVEINF="%USERPROFILE%\Desktop\srvsetup.inf" /LOG="%USERPROFILE%\Desktop\srvinstall.log"
```

SafeCom custom command line parameters

/ICOMPONENT="component name"


In this option, you must specify which component you want to install. Only the specified components are selected, the rest are deselected. The `/ICOMPONENT` switch has the following values:

- SERVER
- CLIENT
- TOOLS

 Some switches can only be interpreted if a suitable value is specified for this switch.

/TRACE

Enables and creates the trace folder for SafeCom Server. You can enter the path to the trace folder here.

 Each of the command line switches can correspond to the input box or selectable option of the user interface, but changing the path of the trace folder can only be done on the command line.

You can also specify the `TracDest` and `TracSize` parameters: `/Trace=" [PATH] ; [DEST] ; [SIZE] "`

```
setup.exe ... /VERYSILENT /SUPPRESSMSGBOXES /NORESTART /Trace="C:\SAFECOM_TRACE;3;10240"
```

/JOBDATA

This command line option can only be interpreted in if the SERVER component is selected.

You can enter the path of the Job server folder.

/MSSQLDATA

This command line option can only be interpreted in if the SERVER component is selected.

You can enter the path of the SQL Server database.

```
setup.exe /ICOMPONENT "Server" /JobData="C:\Program Files\SafeComG4\JobData" /MSSQLDATA="C:\Program Files\SafeComG4\SQLData" /VERYSILENT /NORESTART /SUPPRESSMSGBOXES
```

/EXTMSSQL

This command line option can only be interpreted in if the SERVER component is selected.

Use this switch to use an external SQL server for the SafeCom G4 server. Enter the SQL Server as:
computername\instancename

```
setup.exe ... /VERYSILENT /SUPPRESSMSGBOXES /NORESTART /Trace="C:\SAFECOM_TRACE;3;10240" /EXTMSSQL="SRV2022\SafeComDatabase"
```

/USER

This command line option can only be interpreted in if the SERVER component is selected.

Windows authentication with service account. If this parameter is not specified, the SafeCom service runs under the Local System account.

```
setup.exe /ICOMPONENT="Server" /User="YourDomain\Username" /PWD="P@ssword" /JobData="C:\Program Files\SafeComG4\JobData" /VERYSILENT /NORESTART /SUPPRESSMSGBOXES
```

/PWD

This command line option can only be interpreted in if the SERVER component is selected.

If you have specified a user name for Windows authentication, you must use this switch to enter the password required for the user. If you specified a gMSA user (Group Managed Service Accounts) for the /USER switch, you do not need to use this option.

/ServerIP

This command line option can only be interpreted in if the CLIENT component is selected.

If the value of the /ICOMPONENT switch is client, the name or IP address of the server must be entered in the value of /ServerIP.

```
setup.exe /ICOMPONENT="Client" /ServerIP="10.0.0.1" /VERYSILENT /NORESTART /SUPPRESSMSGBOXES
```

/TOOLS

If the value of the `/ICOMPONENT` switch is `TOOLS`, you can specify which subcomponents you want to install using this switch.

Possible values are the `Admin` or `Port`. You can specify one or more subcomponents in this switch. If you want to install multiple subcomponents, the separator character between subcomponents is the semicolon (`;`).

```
setup.exe /ICOMPONENT="Tools" /TOOLS="Admin;Port" /VERYSILENT /NORESTART /
SUPPRESSMSGBOXES
```

Setup exit codes

The single step execution file (`setup.exe`) sets an error level on return that corresponds to System Error Codes.

The SafeCom setup program may return the following exit codes:

Error code	Description
0	Setup was successfully run to completion or the <code>/HELP</code> or <code>/?</code> command line parameters were used.
1	Setup failed to initialize.
2	The user clicked Cancel in the wizard before the actual installation started, or chose No on the opening This will install... message box.
3	A fatal error occurred while preparing to move to the next installation phase (for example, from displaying the pre-installation wizard pages to the actual installation process). This can only happen under the most unusual of circumstances, such as running out of memory or Windows resources.
4	A fatal error occurred during the actual installation process. <div style="background-color: #e6f2ff; padding: 5px; margin-top: 10px;"> <p>i Errors that cause an Abort, Retry, Ignore box to be displayed, are not fatal errors. If the user chooses Abort at such a message box, exit code 5 is returned.</p> </div>
5	The user clicked Cancel during the actual installation process, or chose Abort at an Abort, Retry, Ignore box.
6	The Setup process was forcefully terminated by the debugger (<code>Run Terminate</code> was used in the Compiler IDE).
7	The <i>Preparing to Install</i> stage determined that Setup cannot proceed with installation.

Error code	Description
8	The <i>Preparing to Install</i> stage determined that Setup cannot proceed with installation, and that the system needs to be restarted in order to correct the problem.

Before returning an exit code of 1, 3, 4, 7, or 8, an error message explaining the problem is normally displayed.

Future versions of Inno Setup may return additional exit codes, so applications checking the exit code should be programmed to handle unexpected exit codes gracefully. Any non-zero exit code indicates that Setup was not run to completion.

Windows Firewall – Ports that must be opened

If Windows Firewall is enabled, it may prevent the SafeCom solution from working. Disable the firewall or run the script below.

1. Browse to the SafeCom Print Client installation folder.
2. Right-click the `open_firewall_print_client.cmd` file. Click **Run as administrator**.
In the file, you can see which TCP and UDP ports will be opened.

i If users are to be imported from Active Directory (AD), you need to add TCP port 389 (or 636 if the import is to be secured via SSL/LDAPS). For a complete list of ports that must be open, see [TCP and UDP port numbers used by SafeCom](#).

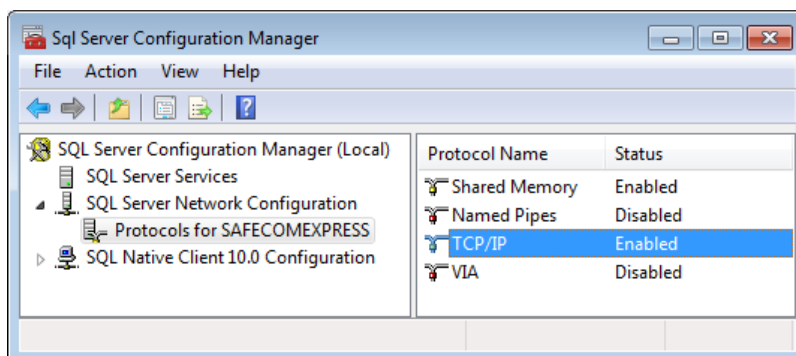
Windows Firewall – Make SQL use fixed port

The Windows Firewall is on by default and blocking remote connections. The following ports are used in connection with SQL communication:

- UDP port 1434: The SQL Server Browser Service uses the UDP port.
- TCP port 1433: Configure the SQL server to use the fixed TCP port (see below).

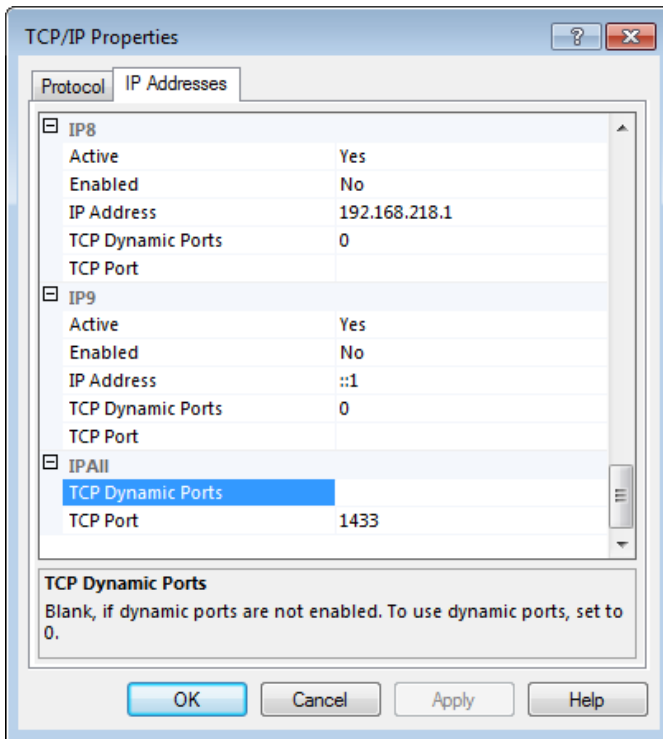
Follow the instruction below to make the SQL server use a fixed port.

1. Click **Start**, point to **All Programs, Microsoft SQL Server <version>, Configuration Tools, and SQL Server Configuration Manager**.

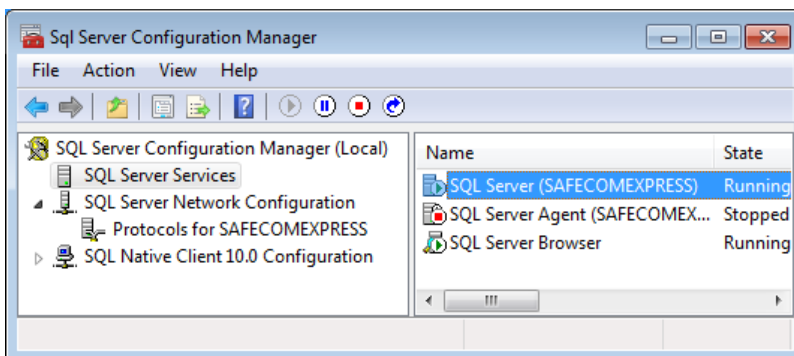


2. Double-click **TCP/IP** to open the **TCP/IP properties** dialog.

- On the **IP Addresses** tab, scroll to the **IP All** section at the bottom.



- Clear **TCP Dynamic Ports** and set **TCP Port** to **1433**.
- Click **OK**.
- Click **SQL Server Services**.



- Right-click **SQL Server (SAFECOMEXPRESS)** and click **Restart**.
- Start the SafeCom service.


Security checkup after installation

Once the SafeCom G4 Server has been installed and successfully tested, it is recommended to go through this checklist:

- Change the default password (nimda) for the built-in user account ADMIN (see [Change password](#)).
- Change the default password (hctet) for the built-in user account TECH. Check that the initial PUK code (12345678) is no longer present.
- Make sure that there is at least one user with [Administrator rights](#).
- Check that SafeCom Controllers and SafeCom Go devices are password protected.
- Delete the intermediate SQL user: safecominstall (see [Delete intermediate SQL user: safecominstall](#)).
- Put in place a scheduled backup of the database (see [SafeCom database - backup and restore](#)).

Scripts to manually create the databases

Included in the distribution of SafeCom G4 are a number of *.scs script files that can be used to manually create the databases required by SafeCom.

 Running these scripts clears the existing SafeCom databases.

The scripts are located in the SafeCom installation folder. The default installation folder is:

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

The scripts must be executed in the following order:

- sscore.scs
- sscoredef.scs
- ssevent.scs
- sseventdef.scs
- scpurse.scs
- scpursedef.scs
- sctracking.scs
- sctrackingdef.scs

If the distribution includes any of the following files, they must be executed last.

- sscoreadapt.scs
- sseventadapt.scs
- scpurseadapt.scs
- sctrackingadapt.scs

To ensure that the database ownership is correct, run the following script:

- scChangeOwner.sql

SQL collation

The databases created by the SafeCom system use the collation: SQL_Latin1_General_CP1_CI_AS.

Use of other collations has not been tested and is not supported. Using another collation may perhaps reveal situations where case sensitivity could cause problems.

To use another SQL collation, do the following, before the databases are created.

1. On the SafeCom primary server make a backup of the files:
 - sscore.scs
 - scevent.scs
 - scpurse.scs
 - sctracking.scs
2. Edit each of the above *.scs files to reference the appropriate SQL collation. Look for the following text string.

```
SQL_Latin1_General_CP1_CI_AS
```

 The corresponding *def.scs should not be edited.


If the solution is a multiserver installation the modified *.scs files must also be used on the SafeCom secondary servers. This implies that the modified *.scs files must be copied to the SafeCom secondary server before the secondary creates its database.

Create intermediate SQL user: safecominstall

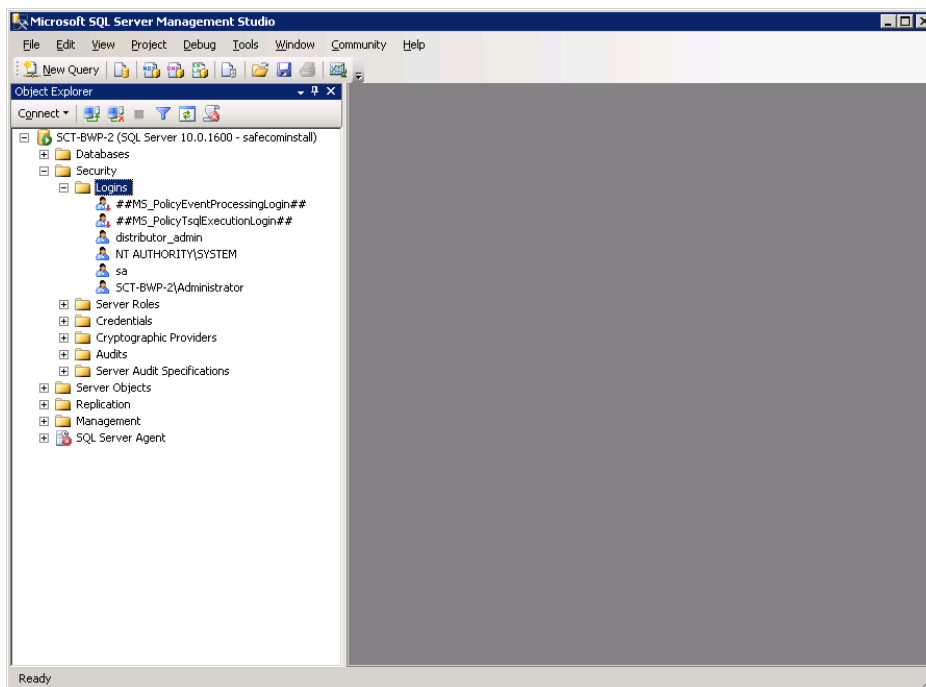
The SafeCom Service will automatically create the SafeCom databases in the Microsoft SQL Server the next time the SafeCom Service is restarted. However, before this is done you need to temporarily create an SQL user named safecominstall.

The SQL user is created using Microsoft SQL Server Management Studio. Refer to Windows online help for additional information on the Management Studio.

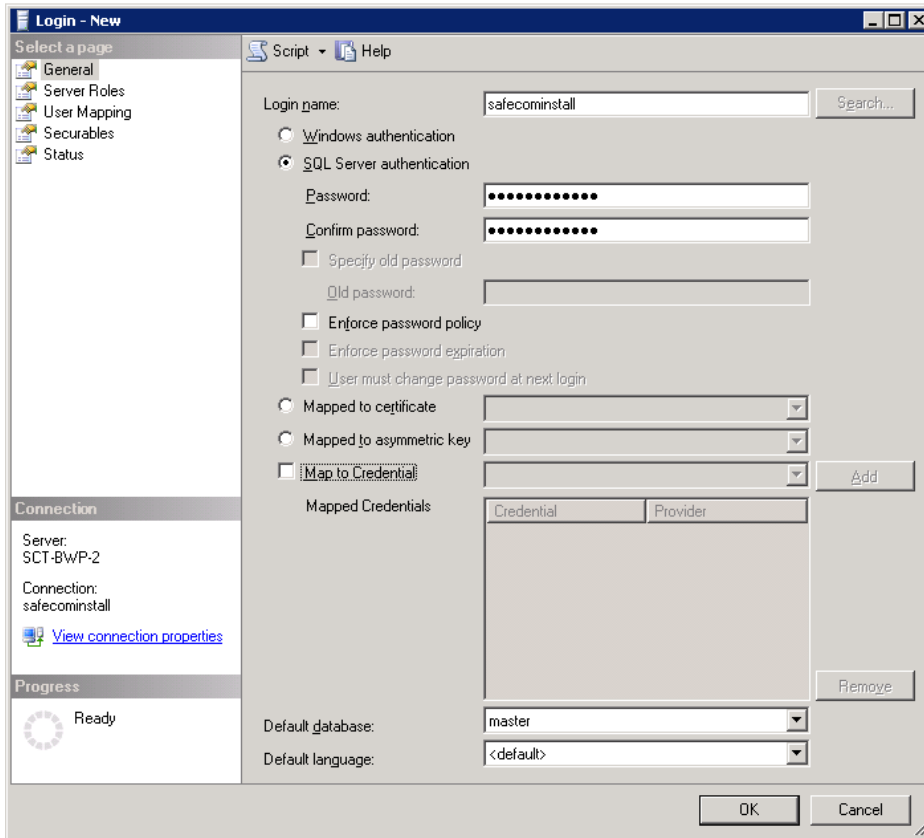
1. Click **Start**, point to **All Programs** and **Microsoft SQL Server <version>**, and click **SQL Server Management Studio**.

 The SQL Server Group must not be registered as LOCAL. The server name must be used instead (for example, SafeCom4).

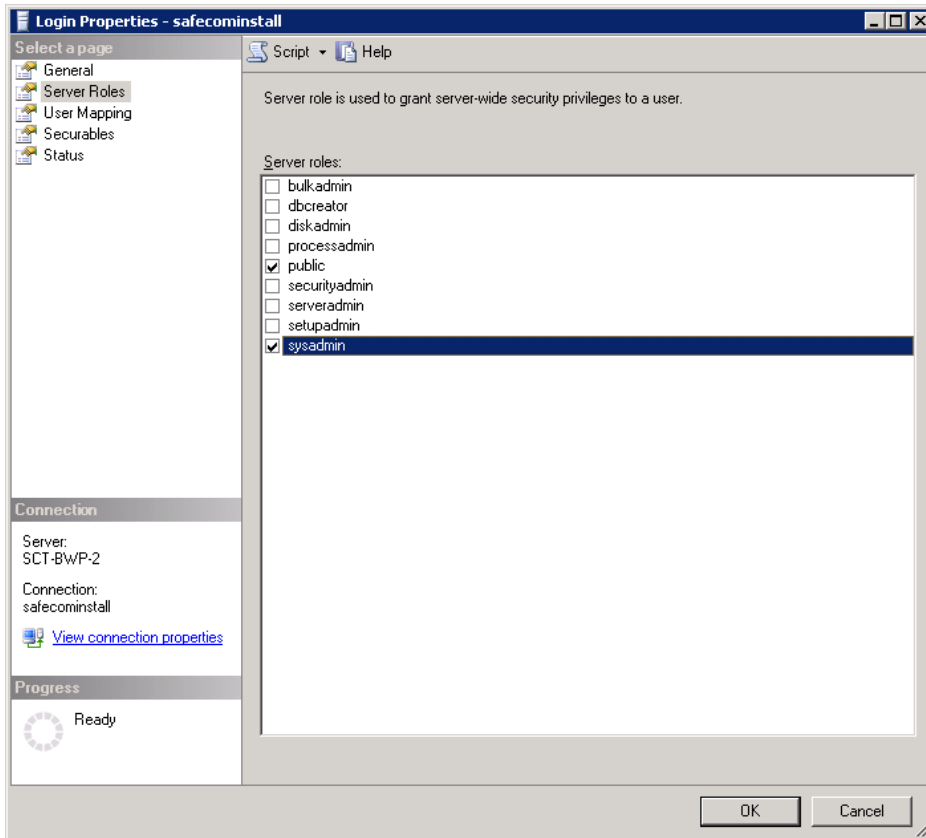
2. Expand to the **Logins** level as depicted on the figure below.



3. Right-click **Logins** and click **New Login**.



4. On the **General** page, set **Login name** to safecominstall. Select **SQL Server authentication** and set **Password** to safecom_2_DB. Clear **Enforce password policy**.
5. Click the **Server Roles** page.



6. Give the SQL user the required rights by checking **sysadmin**, then click **OK**.
Remember that the safecominstall SQL user is a temporary user that you can delete later, as described in [Delete intermediate SQL user: safecominstall](#).

Delete intermediate SQL user: safecominstall

1. Open the **SQL Server Management Studio**.
2. Browse to **Logins**.
3. Right-click the **safecominstall SQL user** and click **Delete**.

Do not modify SQL user: safecom

The first time the SafeCom Service is started, the temporary safecominstall SQL user is used to create a permanent safecom SQL user. The safecom SQL user is used to log in to the database.

i Do not modify the settings of the safecom SQL user as it may stop day-to-day operations and prevent successful future updates of the SafeCom G4 Server software. Also, do not enforce a password renewal policy to the safecom SQL user, because it may cause the safecom SQL account to be locked and prevent the solution from working.

Add Windows service account to the SQL server

1. Start the SQL Server Management Studio.
2. Connect to the SQL server instance used by SafeCom.
3. Expand the **Security** entry.
4. Right-click **Logins** and select **New login**.
5. Browse to the Windows user you want to use.
6. Under **Server Roles**, select **sysadmin**.
7. Click **OK**.

Enable TCP/IP protocol on the SQL server

1. Click **Start**, point to **All Programs, Microsoft SQL Server <version>, Configuration Tools and SQL Server Configuration Manager**.
2. Browse to **SQL Server Network Configuration** and **Protocols for MSSQLSERVER**.
3. Right-click **TCP/IP** and select **Enable**.

Determine physical and virtual memory on the server

For good performance, it is important to have sufficient physical RAM. Remember that SQL is a memory intensive application. Having 2 GB of physical memory is a good start, but more is better. To take advantage of 4 GB or more physical memory, it is necessary enable PAE X86 (Physical Address Extension) on 32-bit Windows server. Refer to microsoft.com.

The amount of physical memory can be determined by looking at the **General** tab in the **System Properties** dialog.

Determine CPU and RAM

1. Open the Control Panel on the computer where the SafeCom server software is installed.
2. Click **Administrative Tools**, then click **Computer Management**.
3. Right-click **Computer Management (Local)** and click **Properties**.
The **General** tab includes information about CPU (MHz) and RAM (MB), and it says "Physical Address Extension" if PAE is enabled.

If you see a small message in the bottom right corner of the screen announcing "Windows - Virtual Memory Minimum Too Low", Windows is increasing the virtual memory. During this process, memory requests for some applications, such as the SafeCom server, may be denied and these applications may potentially become unstable.

Adjust the virtual memory

1. Log in with administrator privileges on the server.
2. Open the Control Panel on the computer where the SafeCom server software is installed.
3. Click **Administrative Tools**, then click **Computer Management**.
4. Click the **Advanced** tab.
5. In **Performance**, click **Settings**.

6. In **Virtual memory**, click **Change**.
7. In the **Drive** list, click the drive that contains the paging file you want to change.
8. Under **Paging file size for selected drive**, type a new paging file size in megabytes in the **Initial Size (MB)** or **Maximum Size (MB)** box, then click **Set**.
If you increase the sizes, you are normally not required to restart the computer.

i The initial size is, normally, equivalent to 1.5 times the amount of physical RAM on the system. If the Task Manager (see below) indicates that the peak memory use is close to the maximum, it is recommended to change the initial size to 1.5 times the current maximum and to increase the maximum to 2 or more times the current maximum. Example: Initial size is 2 GB and maximum is 4 GB. If the peak gets close to 4 GB, increase the initial size to 6 GB and maximum to 8 GB.

Check peak memory usage

1. Right-click an empty space on the Task bar and click **Task Manager**.
2. Click the **Performance** tab.
In **Commit Charge (K)**, you can see the peak memory usage. Peak memory usage on a SafeCom server is typically reached when there is high print activity and/or when user data is imported.

Store print files on an external file share

If the print files folder you specified in [Server installation \(Advanced\)](#) is on an external file share, you must ensure that the SafeCom service runs as an account that has read and write access to the external file share.

1. Open the Control Panel on the computer where the SafeCom server software is installed.
2. Click **Administrative Tools**, then click **Services**.
3. Right-click **SafeCom Service** and click **Properties**.
4. Click the **Log on** tab.
5. Select **This account** and assign an account that has read and write access to the external file share.

Change location of SafeCom print files

Unless you specified an alternate location when you installed the SafeCom software, the SafeCom print files are by default stored in the folder `C:\Program Files\SafeCom\SafeComG4\data`.

Follow the steps below to change the location of SafeCom print files.

1. Click **Start**, type "service.msc" into the **Search** box, then press Enter.
2. Right-click **SafeCom Service** and click **Stop**.
3. Right-click **Print Spooler** and click **Stop**.
4. Create the folder that should hold the print files from now on.
5. Copy the existing print files to the new folder.
6. Open the Registry Editor and browse to:

`HKEY_LOCAL_MACHINE\SOFTWARE\SafeCom\SafeComG4`

7. Change **FilePath** to the new location.
8. Close the Registry Editor.
9. Start the SafeCom service and the Print Spooler.

Configure encryption between SafeCom components

By default, the SafeCom components use TLS encryption.

i For S82 70.520*10 or later, scPopUp does not work without TLS. Switching TLS off disables the scPopUp as well.

1. Open the Registry Editor and browse to `HKEY_LOCAL_MACHINE\SOFTWARE\SafeCom\SafeComG4`.
2. Create a DWORD named ChannelEncryption.
3. Set one of the following values:
 - 1: Only Legacy is enabled.
 - 2: Only TLS is enabled.
 - 3: Both Legacy and TLS are enabled (default).

Configure encryption between G4 Server and SQL Server

To configure encryption between the G4 Server and an SQL Server:

1. Install the latest Microsoft Visual C++ Redistributable x86 and x64 versions from [Microsoft Visual C++ Redistributable latest supported downloads](#)
2. Install the Microsoft OLE DB Driver 19 for SQL Server x64 version (or above) from [Download Microsoft OLE DB Driver for SQL Server](#)
3. Open the Registry Editor and browse to `[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MSSQLServer\Client\SNI19.0\GeneralFlags\Flag2]`
4. Set DWORD named Value to 1.
5. Browse to `HKEY_LOCAL_MACHINE\SOFTWARE\SafeCom\SafeComG4\Database`
6. Create a new DWORD named Provider and set to 2.
7. Create a new String named ConnectionProperties and set it to: the following:

```
Provider=MSOLEDBSQL19;Use Encryption for Data=True;Trust Server Certificate=True
```

For secure connectivity, ensure that the SQL Server requires encryption (for server-side configuration, see [Configure encryption settings in SQL Server](#)). Also ensure that the server has a verifiable certificate, and change the setting to `Trust Server Certificate=False` in ConnectionProperties.


8. Restart the SafeCom Service.

Using a custom certificate for TLS communication

To use custom certificates for TLS communication, follow the steps below:


1. On the SafeCom G4 Server machine, import your custom certificate to the local computer's **Computer** account > **Personal** certificate store.
 - a. On the server, press Windows key + R to open the **Run** dialog, then execute the **certlm.msc** command.
 - b. Under **Certificates (Local Computer)**, expand the **Personal** node, then click the **Certificates** folder.
 - c. Right-click the background of the right pane, point to **All Tasks**, then click **Import**.
 - d. Follow the instructions of the wizard to import your certificate in the **Personal** certificate store.
2. Make sure the account running SafeCom has permissions to use the private keys of the imported certificate.
 - a. Right-click your certificate in the certificate store, point to **All Tasks**, and click **Manage Private Keys**.
 - b. On the **Security** tab, confirm that the account running SafeCom has Full Control permissions.
3. On the server, run the following PowerShell command to retrieve the certificate thumbprint:

```
Get-ChildItem -path cert:\LocalMachine\My
```
4. Run the regedit command to open the Registry Editor, and browse to the following key:
Computer > HKEY_LOCAL_MACHINE > SOFTWARE > SafeCom > SafeComG4
5. If it does not exist, create a REG_SZ value with the name "TlsCert".
6. Paste the certificate thumbprint retrieved in step 3 to the "TlsCert" value.

 The certificate thumbprint should only contain upper-case letters. In some cases, the thumbprint query may be case-sensitive, and lower-case letters may cause problems.
7. Restart the SafeCom service.

After completing the steps above, the SafeCom G4 Server will use the specified certificate for TLS communication.

Update SafeCom software – single server

 If you have a SafeCom G2 version S82 070.380*09 (32 bit) installation, you first need to upgrade to SafeCom G3 version S82 070.440*04 (32 bit) before upgrading to SafeCom G4.

The SafeCom license must be valid (not expired) in order to perform an update.

If you launch the installation to update or reinstall the SafeCom G4 software, the installation gives a different response based on what is currently installed on the computer:

- **Server is already installed:** The installer prompts you to update your existing SafeCom server installation.
- **Client is already installed:** The installer prompts you to update your existing SafeCom [client installation](#) and offers you to add whatever tools you have not installed at previous occasions.
- **SafeCom Administrator is installed alone:** The installer prompts you to update the SafeCom Administrator. To subsequently install a client, you must first uninstall the SafeCom Administrator as described in [Uninstall SafeCom software](#) and then perform a [client installation](#) and then a [tool installation](#).

i After the update, SafeCom solutions originally based on SafeCom G2 or G3 continue to use the original SafeCom installation folder (SafeCom G2 or SafeCom G3 instead of SafeCom G4) and also continue to use the SQL server. The update does not replace the SQL server already in use.

The product installer stops the following services before the upgrade procedure:

- SafeCom Service
- Kofax Ethernet Card Reader service
- Print Spooler

When the installer finishes the product update, it may prompt for computer restart in order to apply all the changes. It is recommended to select **Yes** or restart the computer later before using services of the software. The software might malfunction if it is used without a computer restart.

i If you upgrade your G4 server from version 10.530.0, you can safely remove SQL Express instance SAFECOMRMO after restarting the computer, as the G4 server does not use it anymore.

The update procedure for multiserver installation is covered in [Using Group Management Service Account for services](#).

Uninstall SafeCom software

1. Stop the SafeCom Service (see [Start and stop the SafeCom service](#)) and the Print Spooler (see [How to start and stop the Print Spooler](#)). If other services depend on the Print Spooler, they must also be stopped.
2. If SafeCom PopUp (scPopUp.exe) is running, stop it.
3. Open the Control Panel.
4. Click **Programs and Features** (or **Add or Remove Programs**).
5. Right-click **SafeCom G4** and click **Uninstall**.
6. Proceed to section [Uninstall Microsoft SQL Express 2019](#) to uninstall the SafeCom-specific instance of the SQL server.
7. Restart your computer after uninstalling Microsoft SQL Express 2019.

Uninstall Microsoft SQL Express 2019

1. Open the Control Panel.
2. Click **Programs and Features** (or **Add or Remove Programs**).

3. Right-click **Microsoft SQL Server [version]** and click **Uninstall**.
4. Uninstall the DATA folder that contains SafeCom SQL database files (sc*.mdf and sc*.ldf). These files must be deleted manually.

The default location for the database files:

```
C:\Program Files\Microsoft SQL Server\MSSQL[version].SAFECOMEXPRESS\MSSQL
\DATA
```

If you chose a different location during installation (see [Server installation \(Advanced\)](#)), find the files and delete them manually. If you reinstall the SafeCom software, these files are suffixed with *.old before a new set of SafeCom SQL database files is installed.

5. Restart the computer.

SafeCom Print Client

Network bandwidth is often a barrier to the central administration of printers at remote sites. With SafeCom Print Client, you can minimize the need for network capacity locally since only control data travels over the corporate network. Pending documents are stored locally on the user's computer until the user authenticates and collects the print job at any network printer. Only login and tracking information is sent to the SafeCom server.

Separate installers are delivered for the 32-bit and 64-bit versions of the software. Though the 32-bit version can be installed on 64-bit version of Windows platform, it is recommended to install the appropriate version according to the type of operating system.

Default storage of print jobs

For the 64-bit version, print jobs are stored by default at C:\Program Files\SafeCom\SafeComPrintClient\JobFiles.

For the 32-bit version, the default folder is dependant on the operating system version. The print jobs are stored by default at the following:

Windows 32-bit version

```
C:\Program Files\SafeCom\SafeComPrintClient\JobFiles
```

Windows 64-bit version

```
C:\Program Files (x86)\SafeCom\SafeComPrintClient\JobFiles
```

The location of print jobs is specified in the `scPrintClient.ini` file. It can be a local folder or the one shared by a network. The software can be installed on computers that conform to the specified system requirements. For more information, see [Client requirements](#).

i The description of Print Client computers cannot exceed 100 characters. Only the first 100 characters of the computer description are saved in the database.

Upgrade of an existing 32-bit Print Client running on 64-bit version of Windows operating system is supported. Software configuration and the stored print jobs are managed and kept during update.

Installation

1. Download the `SafeCom_print_client_xxx.exe` file from the link supplied to you. The installation must be **Run as administrator**.
2. Accept the **License agreement**.
3. **Select components**. Full installation is the default option. SafeCom Popup is an optional component. Print Client service is also optional; you can deploy only the SafeCom Pull and Push ports without the service. Installing the service without ports is not possible. The next screen of the installer depends on the selected components.
4. When **Full install** is selected:
 - a. **SafeCom server**. The home server of the Print Client must be specified. The address can be specified as the hostname or the IP address. Use semicolon as a separator if multiple servers are entered.
 - b. **Location of the configuration file**. If you leave the SafeCom server address field empty, then the location of the configuration file - `scPrintClient.ini` - must be specified on the next screen. The configuration file can be located on a network share. The SafeCom server address is defined in this file. It is mandatory to specify the SafeCom server address either manually or through this configuration file.
5. When **Ports only install** is selected:
 - a. **Print engine**. The Print engine - a SafeCom server or a Print Client - must be specified. This server is used for transferring print jobs and tracking data captured by SafeCom ports.
6. Click **Install** to copy the files to the installation folder. Default installation folder is: `c:\Program Files\SafeCom\SafeComPrintClient`.
7. Click **Finish** to apply the following changes to the system:
 - New service named: **SafeCom Print Client**.
 - New port (**scPull**) that uses the **SafeCom Pull Port** (see [Configure the SafeCom Pull Port](#)).

The **SafeCom PopUp** (see [SafeCom PopUp deployment on Windows computers](#)) is also installed and started if selected in the installation wizard.



- If a non-default `JobStoragePath` is used either during installation or later, the specified folder must exist, and the account running the SafeCom Print Client must have the necessary access rights to that folder.
- In a SafeCom multiserver solution, the SafeCom Print Client and the SafeCom Pull Port (see [Configure the SafeCom Pull Port](#)) will failover to the first server in the failover server list.

Windows Firewall

If Windows Firewall is enabled, it may prevent the SafeCom solution from working. Disable the firewall or run the script below.

1. Browse to the `SafeComPrintClient` installation folder.

2. Right-click `open_firewall_print_client.cmd`. The command file must be **Run as administrator**. In the file you can see what TCP and UDP ports will be opened.

Print test page

1. Use one of these methods to make a printer use the SafeCom Print Client.
 - Modify an existing local printer to use the new port. In the **Print properties** dialog, click the **Ports** tab and select the **scPull** port.
 - Add a new local printer and make it use the new port. Please see [Add a local SafeCom Pull Printer on Windows 10](#) for instructions.
2. Print a test page and collect it at one of the SafeCom-enabled devices.

Printing protocol

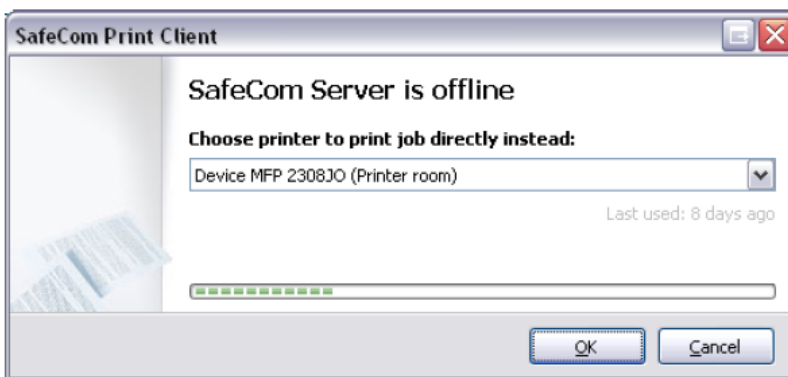
SafeCom Print Client takes the IPP settings of devices into consideration and selects the printing protocol accordingly. The device settings are always queried from the G4 server when it is online, and a pull print request arrives. If the server is offline, then the device settings are used from local cache. See [High Speed Print considerations](#) for more information.

Direct print if SafeCom server is offline

If the connection to the SafeCom server fails, it is still possible for a user to print with SafeCom Print Client installed.

SafeCom Print Client keeps a record of the devices that have been used for printing so if the connection to the SafeCom server is lost, SafeCom Print Client prompts the user to print directly to one of the last used devices.

When a user submits a print job and the SafeCom server is offline, the SafeCom Print Client dialog opens, prompting the user to send the print job directly to a printer on a list.



The user selects a printer from the drop-down menu, clicks **OK**, and the print job is sent directly to the selected printer. Printers that are driven by SafeCom Device Server version S82 060.050 or earlier are excluded from the list.

i Even when the connection to the SafeCom server is lost, the tracking data is still collected and then sent to the server once the connection is re-established.

Deployment to computers

1. Create a folder and copy `SafeCom_print_client_xxx.exe` and `scPrintClient.ini` (see [scPrintClient.ini file](#)) into the folder.
2. Edit the `DefaultServerAddress=` entry in the `scPrintClient.ini` [scPrintClient.ini file](#) to include the address (hostname or IP address) of the SafeCom servers.
`DefaultServerAddress=slave1;slave2`
 Use semicolon (;) as separator. It might be relevant to reference a couple of SafeCom secondary servers, similar to what you might do for the purpose of failover (see [Failover servers](#)). To control the location of print job files edit the `JobStoragePath` parameter.
3. Save the `scPrintClient.ini`.
4. To suppress dialogs invoke the `SafeCom_print_client_xxx.exe` file with the command line parameters (see [Command line parameters](#)): `/VERYSILENT /NORESTART /SUPPRESSMSGBOXES`
 To install in a specific folder use the `/DIR="x:\pathname"` command line parameter. A fully qualified *pathname* must be specified.
5. Optionally, the administrator could specify the components to be installed with the `/COMPONENTS` switch. The available component combinations are as follows:
 - `/COMPONENTS="Print Client Service,Ports,PopUp"`
 - `/COMPONENTS="Print Client Service,Ports"`
 - `/COMPONENTS="Ports,PopUp"`
 - `/COMPONENTS="Ports"`
 - `/COMPONENTS="PopUp"`

The INI file can be saved from an existing installation to a network location that can be read by all Print Client computers. Print Clients can be configured to read the INI file from this shared location both during and after installation.

During installation, use the `/CONFIGFILE` command line parameter to specify the location of the shared ini file. This will automatically create the required registry entry for the shared configuration file.

- `/CONFIGFILE="Full path and file name of the ini file"`

For an existing Print Client installation to use a shared INI file, the following registry value must be created manually, and the SafeCom Print Client service must be restarted. The value must contain the full path and file name of `scPrintClient.ini`.

Value name:

`ConfigFile` (String value)

Key name (on 64-bit operating systems):

`HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\SafeCom\scPrintClient`

Key name (on 32-bit operating systems):

```
HKEY_LOCAL_MACHINE\SOFTWARE\SafeCom\scPrintClient
```

i The settings in a shared INI file are used by all configured Print Clients. Make sure that all settings are valid for all clients (for example, `DefaultServerAddress` and `JobStoragePath` settings are valid for all).

scPrintClient.ini file

The configuration file is loaded by the service at startup. The service resolves the location of the configuration file using methods in the following order:

1. Path specified in the registry as defined in the previous section.
2. `{ProgramData folder}\SafeCom\PrintClient` (default in case of the standard installation procedure).
3. `{Program installation folder}`.

i If this file is present next to the Print Client installer, it is automatically copied to the Print Client installation directory, and the Print Client Service uses the information and settings presented in this file (especially the server information). If the server IP address is specified in `scPrintClient.ini`, the installer does not display the relevant dialog and takes the information from the `scPrintClient.ini` itself.

```
[scPrintClient]
```

```
JobStoragePath=C:\Program Files\SafeCom\SafeComPrintClient\JobFiles\
```

```
ScReconnectRetryWaitMs=120000
```

```
DefaultServerAddress=xxx.yyy.zzz.nnn; aaa.bbb.ccc.ddd
```

```
DefaultServerPort=7500
```

```
DefaultServerPortPS=7700
```

```
JobServerConnTimeOutMS=30000
```

```
JobServerPingTimeOutMS=1000
```

```
OfflineTrackingTaskInterval=1200000
```

```
OfflineTrackingTaskIntervalRnd=1200000
```

```
CleanUpTaskInterval=72000
```

```
CleanUpTaskIntervalRnd=36000
```

- **JobStoragePath=C:\Program Files\SafeCom\SafeComPrintClient\JobFiles**: States the path where the print client saves the job files.

i If a non-default `JobStoragePath` is used either during installation or later, the specified folder must exist, and the account running the SafeCom Print Client must have the necessary access rights to that folder.

- **ScReconnectRetryWaitMs=1200000**: States the time that must pass in between retries to connect to the SafeCom server.
- **DefaultServerAddress=xxx.yyy.zzz.nnn; aaa.bbb.ccc.ddd**: Semicolon separated list of server addresses to which the print client connects.
- **DefaultServerPort=7500**: Port used when computer is running in workstation mode (default is 7500).
- **DefaultServerPortPS=7700**: This is the port that the print client will use for connecting to the job server if the computer is running in PrintServer mode (default is 7700).
- **JobServerConnTimeOutMS=30000**: Time in milliseconds to wait in between tries to reconnect to a server if the current server is not responding. If no server responds to the print client, the print client will go into offline mode. The default is 30000. The print client will also respond in an offline manner if user's home server is offline.
- **JobServerPingTimeOutMS=1000**: Timeout in milliseconds used when pinging servers.
- **OfflineTrackingTaskInterval=1200000**: Time in milliseconds between performing offline tracking.
- **OfflineTrackingTaskIntervalRnd=1200000**: Value used to calculate random offset added to the `OfflineTrackingTaskInterval` parameter to prevent all print clients from performing offline tracking at the exact same time.
- **CleanUpTaskInterval=72000**: Time in milliseconds between performing cleanup (removing old jobs, and so on).
- **CleanUpTaskIntervalRnd=36000**: Value used to calculate random offset added to the `CleanUpTaskInterval` parameter to prevent all print clients from performing cleanup at the exact same time.

i The servers listed in parameter **DefaultServerAddress** are not prioritized. The print client only connects to the first server in the list at service restart.

Use trace facility

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

On the computer, create the folder `C:\safecom_trace`.

The trace file `scPrintClient{number}.trc` contains a number as part of the filename. When a trace file reaches the maximum size (10 MB), a new one is created and the number is incremented with one. The trace folder holds the current and previous version of the trace file. Older files are automatically deleted.

Restarting the SafeCom Print Client Service resets the trace files by default.

Command line parameters

Use the following command line parameters as applicable to your deployment:

/SILENT, /VERYSILENT

Instructs the setup process to be silent or very silent. When the setup is silent, the wizard and the background window are not displayed while the installation progress window is shown. When a setup is very silent, the installation progress window is not displayed. Everything else is normal. During installation, error messages and the start-up prompt are displayed (if it has not been disabled by DisableStartupPrompt).

If a restart is necessary and Setup is silent, the application displays a "Reboot now?" message box.

If it is very silent, it reboots automatically without a prompt.

/SUPPRESSMSGBOXES

Instructs Setup process to suppress all message boxes. This parameter can only be used when combined with **/SILENT** and **/VERYSILENT**.

The default responses are as follows:

- **Yes** in response to a "Keep newer file?" message.
- **No** in response to a "File exists, confirm overwrite" message.
- **Abort** in response to Abort/Retry messages.
- **Cancel** in response to Retry/Cancel messages.
- **Yes** (=continue) in response to diskSpaceWarning / DirExists / DirDoesntExist / NoUninstallWarning / ExitSetupMessage / ConfirmUninstall messages.
- **Yes** (=restart) in response to FinishedRestartMessage / UninstalledAndNeedsRestart messages.

The following message boxes are not suppressible:

- The About Setup message box.
- The Exit Setup? message box.
- The FileNotInDir2 message box displayed when Setup requires a new disk to be inserted and the disk was not found.
- Any (error) message box displayed before Setup (or Uninstall) could read the command line parameters.
- Any message box displayed by the [Code] support function MsgBox.

/LOG

Causes the Setup process 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 is not being replaced when you believe it should be (or vice versa), the log file tells 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.

i 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"

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

i 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.

/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** or **/VERYSILENT**.

/LOADINF="filename"

Instructs Setup process 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.

/SAVEINF="filename"

Instructs Setup process to save installation settings to the specified file.

Don't forget to use quotes if the filename contains spaces.

/DIR="x:\dirname"

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

/SERVER="IP_ADDRESS"

Allows you to specify the G4 server address during silent installation.

i If you have an scPrintClient.ini file next to the Print Client installer, and the ini file specifies a server IP address, the settings in scPrintClient.ini overwrite the /SERVER parameter.

Uninstallation

You can uninstall the Print Client in either of the following ways:

- Go to **Programs and Features**, select the Print Client application, then click **Remove**.

- Alternatively, locate and run `unins000.exe` in your Print Client installation directory.

You can use the following command line parameters when running the uninstallation:

/KEEPSETTINGS=YES|NO

Keeps or discards your Print Client settings.

i If you uninstall the Print Client through **Programs and Features**, you have the option to keep your settings through selecting the relevant UI option when prompted.

/SILENT, /VERYSILENT

See [Command line parameters](#) for more details.

/SUPPRESSMSGBOXES

See [Command line parameters](#) for more details.

/LOG

See [Command line parameters](#) for more details.

/NORESTART

Upgrade from Express to Microsoft SQL Server

You can use the supplied **scBackup** (see [scBackup](#)) to backup the Microsoft SQL Express 2019 database and use it to restore the backup once you have changed to Microsoft SQL Server as described below:

1. Create intermediate SQL user: `safecominstall` (see [Create intermediate SQL user: safecominstall](#)).
2. Stop the SafeCom Service (see [Stop the SafeCom Service](#)).
3. Change Windows Registry to reference SQL Server (see [Change Windows registry to refer to the SQL server](#)).
4. Change the dependencies on the SafeCom Service (see [Change the dependencies on the SafeCom Service](#)).
5. Delete intermediate SQL user: `safecominstall` (see [Delete intermediate SQL user: safecominstall](#)).

i For this to take effect, you must restart the computer.

Once you have performed the above successfully, you may uninstall the Microsoft SQL Express 2019 database as described in [Uninstall Microsoft SQL Express 2019](#).

Stop the SafeCom Service

1. Click **Start**, type **services.msc** into the Search box and press ENTER.

2. Right-click the **SafeCom Service** and click **Stop**.

Change Windows registry to refer to the SQL server

1. Open the Registry Editor and browse to `HKEY_LOCAL_MACHINE\SOFTWARE\SafeCom\SafeComG4\Database`.
2. Find the following registry settings:
 - DBServerNameCore
 - DBServerNameEvent
 - DBServerNamePurse
 - DBServerNameTracking
3. Change the value from `computername\SAFECOMEXPRESS` to one of the following values. It is not possible to specify the IP address instead of the `computername`.
 - `computername`: You only need to specify the `computername` if there is no named instance of the SQL Server. There is no named instance of the SQL Server if **Services** only lists MSSQLSERVER.
 - `computername\instancename`: You need to specify both `computername` and `instancename` if there is a named instance of the SQL server. The instance name can be seen in **Services**. The named service appears in **Services** as `MSSQL$instancename`. The instance name is case sensitive.
4. Click **OK** to save the settings.
5. Repeat steps 3-4 for the remaining registry settings.
6. Exit the Registry Editor.

Change the dependencies on the SafeCom Service

1. Open the Registry Editor and browse to `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SafeCom Service`.
2. Double-click **DependOnService** and replace `MSSQL$SAFECOMEXPRESS` with the instance name of the SQL server (`MSSQL$instancename`). Use `MSSQLSERVER` if there is no named instance. See also step 3 in [Change Windows registry to refer to the SQL server](#). The instance name is case sensitive. If the SQL server is installed on another computer, you should right-click **DependOnService** and click **Delete**.

 For these changes to take effect, you must restart the computer.

Multiserver installation

The nodes of a standard multiserver installation communicate to their own SQL server databases. The primary server is connected to a local or external SQL server (Standard Edition is the minimum requirement), and the secondary servers are connected to their own SQL server instances (SAFECOMEXPRESS). The configuration data of servers, Print Clients, devices, users etc. is shared among databases. Whenever configuration data is created or modified, it is recorded in the `scCore` database of the primary SQL server. The secondary databases are updated using transactional replication. The primary SQL server acts as publisher and distributor in a standard setup. The

secondary SQL servers are the subscribers. Adding and removing servers to such installation is done by the primary SafeCom server automatically.

This chapter describes the required manual SQL server configuration steps and decisions about the SafeCom server to get the replication to work properly and keep each server node up to date.

i SafeCom also supports SQL Always On configuration. It is described in a separate document.

See the [Server requirements](#) chapter for server versions required for the SQL primary server. It must be licensed and installed (including replication option). Microsoft SQL is quite memory intensive and more memory leads to better performance. 16 GB RAM is the required minimum.

Prerequisites

SafeCom-specific requirements

- A **SafeCom license key** that includes SafeCom Enterprise Server. The license key code is based on the computer name (see [Determine the computer name](#)) of the SafeCom primary server.
- You can install primary and secondary SafeCom servers having access to their database with **SQL authentication** (loginby 'safecom' SQL user) or **Windows authentication**. Your choice must be common for primary and all secondary servers and this decision must be made in before the system setup. If Windows authentication for SQL server is selected then the same Windows account is going to be used for running the SafeCom service. For the SafeCom service account, ensure that the following criteria are met:
 - The selected user has local administrator rights on all SafeCom servers.
 - The selected user has "Log on as a service" right on all SafeCom servers.
 - Ensure that the selected user account is added to the sysadmin server role at the primary SQL server instance. For more information, see [SQL server](#).

i If you install a secondary SafeCom G4 server with Windows account, then the selected account has system administrator role granted on the local SQL server Express instance just like the account that runs the installer.

- Ensure that all SafeCom service accounts have full access to the replication snapshot folder on the primary SQL server (see the next section).
- The same version of primary and secondary SafeCom servers must be installed.

Primary SQL server requirements

- The SQL primary server must be defined as an SQL publisher and distributor. SQL server Standard edition is required as minimum.
- If the product is used with 'safecom' authentication then the SQL server must be configured to use the SQL server and Windows authentication method, otherwise the Windows authentication method should be selected.
- To get the one-way replication from the primary to the secondary work, the SQL primary server must have the following three services running:
 - SQL service
 - SQL browser
 - SQL agent

Make sure that the startup type of the service is set to Automatic

- The name resolution must be able to locate servers by name and IP address, including primary and secondary application servers and SQL servers.
- The folder for the replication snapshots must be created on the primary SQL server computer. If not specified, the default local path is `C:\Program Files\Microsoft SQL server\MSSQL<version>.<instance name>\MSSQL\ReplData`.
 - Although the folder is created when the replication is set up, it is better to create it manually and supply with user permissions as follows.
 - If a non default folder is used, then the path must be added to the registry of the primary application server. Use `REG_SZ` value of `DBReplicationSnapshotShare` under key `Computer\HKEY_LOCAL_MACHINE\SOFTWARE\SafeCom\SafeComG4\Database`. The use of UNC path is recommended, but the local path is also accepted by SafeCom. The local path is relative to the distributor.
- Grant permission for the replication snapshot folder
 - If SafeCom uses SQL authentication, then grant the SQL Agent service account full access to the replication snapshot data folder.
 - If SafeCom uses Windows authentication, then grant the SafeCom service account full access to the replication snapshot data folder.

Common requirements for primary and secondary SQL servers

- The SQL primary server, SafeCom primary server and SafeCom secondary servers must be part of the same domain or workgroup.
- The firewall for both the primary server and the secondary servers must ensure that the SQL port is open. If you set a SQL port (see [Windows Firewall – Make SQL use fixed port](#)), make sure the SQL browser service is running if the SQL server is using a named instance or it is configured to a non-default port.



- It is recommended to have the SafeCom secondary servers use their own bundled SQL Express instances.
- Be aware that Microsoft only supports replication between SQL servers that are no further than two versions apart, so older SafeCom secondary servers may need to be upgraded to use Microsoft SQL Express instances.
- When you add a SafeCom server to a SafeCom primary server's group, the SafeCom secondary server loses its existing data, including devices, users, and print jobs.
- See [SQL server](#) if you are upgrading from a running SafeCom server with Microsoft SQL Express to Microsoft SQL server.

Overview

1. Install the SafeCom server on the primary server. Select **Advanced installation** and use an existing SQL server (see [Server installation \(Advanced\)](#)).
2. Run SafeCom Administrator to install the license key code on the primary server (See [Install the SafeCom license key code](#) and its subsections).

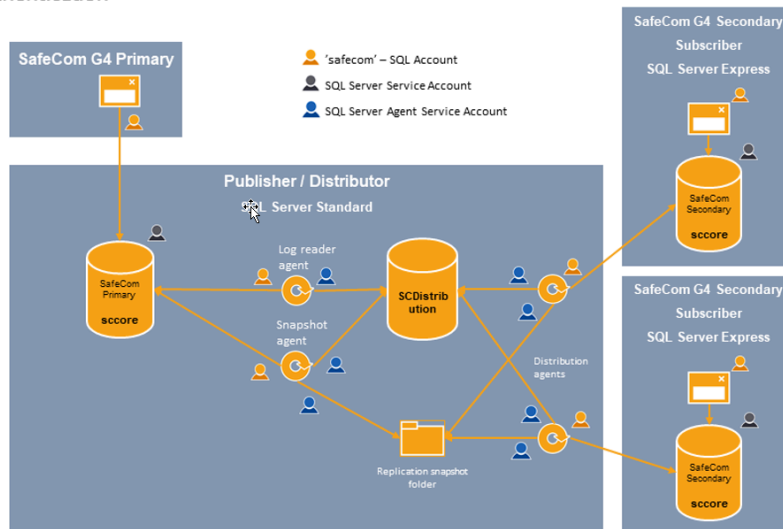
i Secondary servers use the license key on the primary server.

3. Create a replication snapshot folder and the requested permissions. Add the replication UNC network share or local path in the registry of the primary SafeCom server.
4. Delete intermediate SQL user: safecominstall (see [Delete intermediate SQL user: safecominstall](#)) in case of SQL authentication selected for SafeCom servers.
5. Install SafeCom Server on each secondary server (see [Server installation \(Basic\)](#) or [Server installation \(Advanced\)](#)).
6. Add the secondary servers to the primary server's group (see [Add the other servers to the primary server's group](#)).
7. Check that replication is working (see [Check that the replication is working](#)).
8. Schedule a database backup for the secondary server to shrink the database transaction log files. The backup itself is not needed, as data is replicated from the SQL primary server (see [SafeCom database - backup and restore](#)).

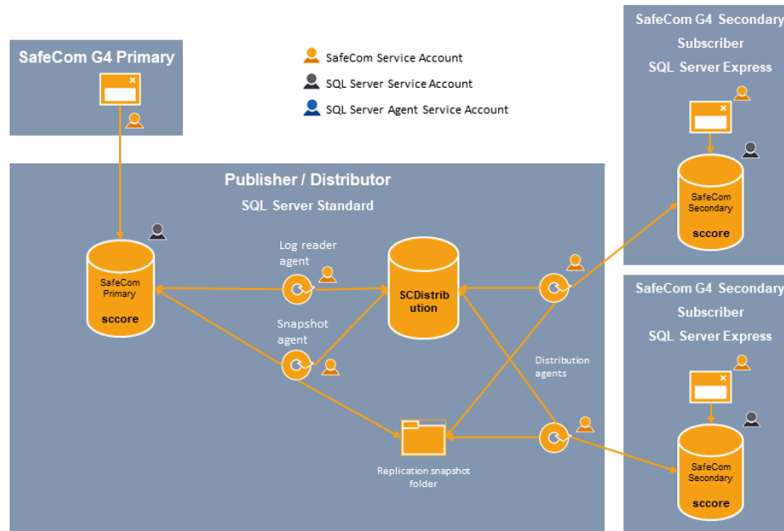
i Replication is configured when the first secondary server is added to the primary server.

The following diagrams show the configuration of replication in case of the two types of authentication.

G4 Server 10.6 Multi-server Architecture safecom authentication



G4 Server 10.6 Multi-server Architecture Windows authentication



Set SQL Server Agent to automatic startup

The SQL Server Agent (*instancename*) on the SQL server must be set to **Automatic** startup in **Services**. Its service account depends on the type of the SafeCom installation (SQL or Windows authentication).

Add the other servers to the primary server's group

Use **SafeCom Administrator** to add the secondary servers to the primary server's group. The server you add must be running. Refer to [Create a multiserver group](#).

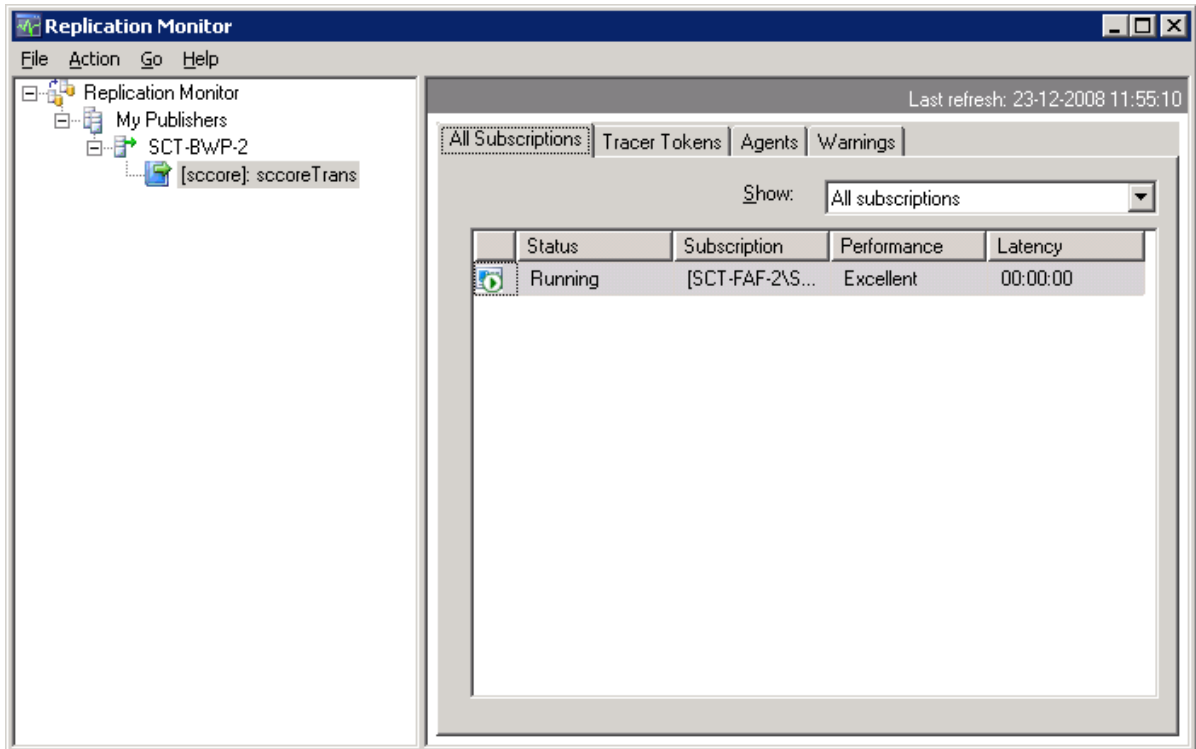
Check that the replication is working

You can also check the replication status in SafeCom Administrator. The server icon in the **Server groups** pane shows a yellow warning triangle if the replication status is **Retrying** or **Failed**. More detailed status is listed in the **Replication** column in the **Servers** list. The status can be **Started**, **Succeeded**, **In progress**, **Idle**, **Retrying**, or **Failed**.

On the primary SQL Server:

1. Open SQL Server Management Studio.
2. Verify that the SQL Server Agent is running. Right-click **SQL Server Agent** and click **Properties** and verify that **Service** state is **Running**.
3. Monitor the replication. Browse to **Replication** and **Local Publications** and right-click **[score]:scoreTrans** and click **Launch Replication Monitor**.

The following window appears:



If the replication is working, status symbols should be colored green only and not red.

4. To check any latency click the **Tracer Tokens** tab and click **Insert Tracer**.
5. Click the **Agents** tab and check that agents are running.

! SQL replication must always be working and must not be set to expire. It is highly recommended to use the SQL server alerting capabilities to send notifications when the replication stops. For preventive steps, see [Prevent the subscription from expiring](#).

The tables containing SafeCom configuration data of are replicated. The tables that store temporary data related to the users' daily work - job and scan file properties - are not part of the replication. The following tables are replicated:

- scAliases
- scBillingCodes
- scBillingComb
- scBillingConfig
- scBillingFavorites
- scBillingUserInfo
- scBOPCInfo
- scBranchInfo
- scCardInfo
- scCardReaderInfo
- scClientConfig

- scDelegates
- scDeviceInfo
- scDeviceServerInfo
- scDeviceServerGroup
- scDeviceServerGroupMembers
- scDomainInfo
- scGroupInfo
- scGroupMembers
- scGroupRbpRule
- scMainSettings
- scMasterServerVersion
- scPriceScheme
- scRbpAction
- scRbpCondition
- scRbpRuleInfo
- scScheduleInfo
- scServerInfo
- scServerSettings
- scTreeView
- scTrustedIssuers
- scUserInfo

Repair replication

If a replication fails or is interrupted, it can be repaired from SafeCom Administrator.



- Use Microsoft SQL Management Studio to back up your replication configuration, using the **Generate Script** button.
- This feature can only be used if **Setup replication** was checked when the secondary server was added ([Add server](#)).

The icon of each server in SafeCom indicates the state of the server from replication point of view. The replication can be repaired as described in the following steps:

1. Right-click the secondary server and select **Repair replication**.

2. Click **OK**.

The replication repair begins. The secondary server's subscription is deleted and created again. When the replication is repaired successfully, a confirmation message appears.

3. Click **OK**.

What happens if servers or network connections are down?

To answer this question, we first explain the concept behind the SafeCom multiserver solution.

The SafeCom primary server uses SQL replication to propagate the entire configuration to the SafeCom secondary servers. Initially, it does a snapshot replication and subsequently, it only replicates the changes (transactional replication).

This way, all SafeCom servers have the configuration, including the network details for each other. This allows the servers to communicate directly, rather than having to rely on the SafeCom primary server. In other words, the SafeCom servers become autonomous.

The replication from the SQL server to the SafeCom secondary servers is one-way. Changes to the configuration are possible only when the SafeCom primary server and the SQL primary server are running. This is secured by the system as users with special rights always have the SafeCom primary server as their home server.

- If the primary server is down, it is not possible to make any configuration changes (administrators cannot log in to SafeCom Administrator).
- If a SafeCom server is down, users who have this SafeCom server as their home server cannot log in. However, push printers configured to allow printing at all times can still be used on the servers running. SafeCom servers still running will continue to serve the users who have those servers as their home server. Pull print or Smart scan jobs stored on the server are not accessible from devices.

Additional resilience can be achieved by specifying a prioritized list of [failover servers](#) that users should be moved to if their home server becomes unavailable.

- If the network is partially down, it is still possible to print and switch between the servers as long as they can still reach each other (they are not affected by the part of the network that is down). If the network is completely down, nothing is possible until the network is up again.

Reinitialize the subscription

If a SafeCom secondary server has been restored, you may wish to reinitialize the replication from the SQL server to the SafeCom secondary server.

1. Click **Start**, point to **All Programs > Microsoft SQL Server {version}**, and click **SQL Server Management Studio**.
2. Log in to the SQL server and browse to **Replication > Local Publications > [score]:scoreTrans**.
3. Right-click the subscription of the SafeCom secondary server and select **Reinitialize All Subscriptions**.
4. Select **Generate the new snapshot now**, then click **Mark For Reinitialization**.

For more information, see [Check that the replication is working](#).

Prevent the subscription from expiring

The replication from the SQL server to the secondary server may get dropped if the subscription is not synchronized within 72 hours.

1. Click **Start**, point to **All Programs > Microsoft SQL Server {version}**, and click **SQL Server Management Studio**.
2. Log in to the SQL server and browse to **Replication > Local Publication**.
3. Right-click **[score]:scoreTrans** and select **Properties**.
4. On the **General** page, select **Subscription never expire, but they can be deactivated until they are reinitialized**, then click **OK**.

Using Group Management Service Account for services

The SafeCom service can be configured to use a group managed service account (gMSA) instead of a standard Windows service account. This account type is managed by the operating system, including password management, according to the actual password policy. More information can be found in Microsoft documentation.

You can use the gMSA in your SafeCom configuration the same way as a standard Windows service account. When SafeCom prompts you for account credentials, use the account name with a "\$" suffix and leave the password field blank. The requirements for a gMSA are the same as for a Windows service account. These requirements are listed below.

- sysadmin server role granted on the primary and all secondary servers
- Group membership in the local administrator group on the primary and all secondary servers
- Permission of "Log on as a service"
- Full access to the replication snapshot folder on the primary SQL server in multiserver environment

Change SafeCom configuration from SQL to Windows authentication

To migrate the SafeCom multiserver installation from SQL to Windows authentication, perform the steps below.



- The requirements for the service account are detailed in [Prerequisites](#).
- The steps described below must be performed on the primary and each secondary server. To get the multiserver environment operational, each node must be changed accordingly.
- The reconfiguration is recommended to be done outside working hours.


1. Stop the SafeCom service.
2. Change the service account in the **Log On** tab in the Service Manager.

The service uses the Local System.

- A group-managed service account can be set by entering the account name with a "\$" suffix and without password.


- A dedicated Windows service account can also be used. Both the account name and password are required.
- 3. Open the Registry Editor and browse to `HKEY_LOCAL_MACHINE\SOFTWARE\SafeCom\SafecomG4\Database`.
- 4. Change the `REG_DWORD` value from 0 to 1 for each of the following registry settings:
 - `DBUseWindowsAuthenticationCore`
 - `DBUseWindowsAuthenticationEvent`
 - `DBUseWindowsAuthenticationPurse`
 - `DBUseWindowsAuthenticationTracking`
- 5. Restart SafeCom and all reconfigured services.
- 6. Verify the configuration change through the following steps:
 - a. Run SafeCom Administrator and check that the connection to the primary server works properly.
 - b. Confirm that replication is working properly by adding some users to one of the SafeCom secondary servers. If the user properties are displayed correctly, then the replication works properly.

Update multiserver installation

 If you want to perform an upgrade scenario outside the process documented in this guide, contact your Kofax sales representative for a Professional Services engagement.

Pre-requisites

- The SafeCom license must be valid (not expired).
- If you are updating from SafeCom G2 version S82 070.360 or S82 070.370, you must install `sclicenseManager.dll` version 8.38.1.1 on all secondary servers prior to the update.
- If you have a SafeCom G2 version S82 070.380*09 (32 bit) installation, you first need to upgrade to SafeCom G3 version S82 070.440*04 (32 bit) before upgrading to SafeCom G4.

 After the update, SafeCom solutions originally based on SafeCom G2 or G3 continue to use the original SafeCom installation folder (SafeCom G2 or SafeCom G3 instead of SafeCom G4) and also continue to use the SQL server. The update does not replace the SQL server already in use.

Update SafeCom software

All the SafeCom secondary servers must be updated before the SafeCom primary server. The installation does not function properly before all servers are updated to the same version.

i It is best practice to use change management during the update process. The update process should occur outside normal working hours, as it requires a restart of the computers after the update.

The Microsoft SQL server continues to replicate the SafeCom databases to the secondary servers during the update. Every 10 seconds, each secondary server checks if the primary server is on the correct version. Once they are on the same version, the secondary servers start automatically.

The update process on each server is as follows:

1. Stop the SafeCom service (see [Start and stop the SafeCom service](#)) and the Print Spooler (see [How to start and stop the Print Spooler](#)). If other services depend on the Print Spooler, these must be stopped too.
2. Update with the SafeCom server software.
3. Select **Yes, I want to restart my computer now.**

i It is recommended to restart the computer, but in most cases, it is sufficient to restart the SafeCom Service and Print Spooler.

4. Click **Finish.**

This will restart the computer (and the **SafeCom Service** and **Print Spooler**).

The update should be completed outside normal working hours, as printing will be unavailable during the update process. You may want to use the table below to help you through the update process.

No	Secondary server address	1. Stop services	2. Update software	3. Start services	Version
1					
2					
3					
4					
...					
No	Primary server address	1. Stop services	2. Update software	3. Start services	Version
M					

After the update has been completed, you should [check that the replication from the primary server is still working](#).

You may also want to view the [scdbu*.log files](#) that were created during the update process.

Install the SafeCom license key code

All SafeCom licenses require the installation of a license key code that is linked to the server via the computer name (see [Determine the computer name](#)). On a cluster server, the license is based on the cluster name (see [Cluster installation](#)).

i If your SafeCom solution is a multiserver solution, the license is based on the name of the SafeCom primary server and only needs to be installed on the SafeCom primary server. The license applies to all servers within the group.

The supplier of your SafeCom solution provides you with your license key code.

1. On the server, click **Start**, point to **All Programs > SafeCom G4**, right-click **SafeCom Administrator**, and select **Run as administrator**.
2. Log in to the server by double-clicking the group name listed to the left.
3. Enter the user logon (default is ADMIN) and the password (default is nimda).
4. In the **Servers** menu, click **License** to open the **License** dialog.
5. Enter the license key code and click **Apply**, then click **Close**.

The license key code takes immediate effect and there is no need to restart the server.

Determine the computer name

1. Open the Control Panel, and click **System**.
2. Click the **Computer Name** tab and note the **Full computer name**.

Only the first part of the computer name (up to the first dot ".") is used. The first part of the license key code corresponds to the computer name, with uppercase letters and the removal of all dashes. Spaces and underscores remain.

Computer name	Sample license keys
prn-srv1.acme	PRNSRV1-2923rS-254zMhqGTH-5B62ZZ
Prn_Srv F16	PRN_SRV F16-29233Xa-2s4A2ZCfDG-5BkJdy

Determine the cluster name

On a cluster server, the license is based on the cluster name instead of the computer name.

Windows Server 2016:

1. Open **Failover Cluster Management**.
2. Browse to the cluster and select **Properties**.
Name contains the cluster name.

Understanding the license key code

A new license key code is only accepted if the current configuration does not conflict with the new license key code. The [event log](#) contains information about possible license issues.

A new license key code overrides the old license key code. This means that the new license key code should embed the features allowed by the previous license key plus the new ones. It is therefore necessary to supply the existing license key code to get a new license key code.

- **Maintenance license:** If SafeCom maintenance is bought (for a period of 1, 2, 3, 4, or 5 years), the license key includes the maintenance expiry date. Update is only possible to a version that has a version date that is earlier than the expiry date of the maintenance license. If no SafeCom maintenance is bought, update is possible for a period of 90 days after the license is issued.
- **Trial license:** A standard trial license expires 30 days after it is issued and allows testing all functionality. It allows 3 servers, 5 SafeCom Go, 5 SafeCom Go High-end, and 5 SafeCom Controllers. Customized trial licenses are available upon request.
- **Embedded license:** The embedded license expires 30 days after installation. It allows 1 server, 1 SafeCom Go, 1 SafeCom Go High-end, 1 SafeCom Controller, 10 tracking devices, and all device features. This allows loading the software and getting started while waiting for a trial license or the purchased permanent license.

Device license and user settings dependencies

The dependencies between device licenses and user settings are covered in the following tables for Encryption, Tracking, Pay, Rule Based Printing, and Client Billing.

- **Encryption:** The prerequisites for printing encrypted documents is listed in [Printing encrypted documents](#). The following table describes the relation between device licenses and user encryption settings.

Device license and user encryption settings

Device \ User	No encryption of user's documents	Encryption of user's documents
No encryption by device	No encryption	No encryption.
Encryption by device	No encryption	Encrypt and ignore High Speed Print if enabled.

- **Tracking and Pay:** Tracking data is recorded if the device has a SafeCom Tracking license and the user's cost control is set to Tracking or Pay. If the user is set to No cost control, tracking data is not recorded. A Pay user (cost control is Pay) can log in to a device with a SafeCom Pay license and to a device with a Tracking license if **Allow Pay user** is checked on the device. When **Allow Pay user** is checked, the Pay user is not charged.

Device license and user cost control settings

Device \ User	No cost user	Tracking User	Pay User
No cost device	No tracking	No tracking	No tracking and reject login unless Allow Pay user is checked
Tracking device	No tracking	Tracking	Tracking and reject login unless Allow Pay user is checked

Device \ User	No cost user	Tracking User	Pay User
Pay device	No tracking	Tracking	Pay

- **Rule Based Printing:** Tracking and Pay users are subjected to Rule Based Printing on devices with a SafeCom Rule Based Printing license.
- **Client Billing:** A Billing user (set to Bill clients for costs) can select billing codes with jobs that are tracked on devices with a SafeCom Client Billing license. If the Billing user uses a device with no SafeCom Client Billing license, the job is tracked without the possibility to select a billing code.

Device license and user billing settings

Device \ User	No bill clients for cost	Bill clients for cost
No billing device	No billing	No billing
Billing device	No billing	Billing

User rights required when adding printers

The policy of some corporations may prohibit granting Windows administrator rights to the user who needs to add SafeCom printers and configure the SafeCom Pull Port and SafeCom Push Port.

In most cases, there are no policy restrictions and the user who adds SafeCom printers has Windows administrator rights on the computer in question, and therefore, there is no need to make any changes.

In cases with policy restrictions AND if the adding of printers is done remotely by typing \\server in the Explorer, then special steps must be followed. If the printers are added using Remote Desktop, these steps are not required.

Special steps: The user in question must be a member of a group with sufficient rights. Permissions must be granted and the Print Spooler must be restarted. Additional configuration changes are required if the SafeCom server is clustered.

One way to go about this would be to add the user to the Domain Print Operators group and then add the Domain Print Operators group to the local Power Users group on the print servers. This way, you do not need to add the individual users to the local Power Users group on the print servers.

The steps are as follows:

First steps if the SafeCom server is clustered

1. Make sure the user is a member of the local Power Users group on both nodes.
2. Make sure the SafeCom Port Monitors are installed on the computer and the version of these is across the solution.

On node 1 and 2 grant permissions in Local Security

1. Open the Control Panel.
2. Click **Administrative Tools** and **Local Security Policy**.
3. Browse to **Local Policies > User Rights Assignment** and double-click **Load and unload device drivers**.
4. Click **Add User or Group** and add the local Power Users group.
5. Repeat steps 1-4 on the other node.

On node 1, grant permission in cluster

Windows Server 2016:

1. Open Failover Cluster Management.
2. Right-click **[Cluster]** and click **Properties**.
3. On the **Cluster permissions** tab, add the local Power Users group and grant **Full Control**.

On node 1, grant permission in registry

1. Open the Registry Editor and browse to `HKEY_LOCAL_MACHINE\SYSTEM\Cluster\Resources`.
2. Right-click **Resources** and click **Permissions**.
3. Add the local Power Users group and grant **Full Control**.

Restart the print spooler

For the changes to take effect, the print spooler must be restarted.

1. Open the Cluster Administrator to restart the Print Spooler.
2. Locate the Print Spooler service, right-click and choose **Take Offline**.
3. Wait for the status to change to Offline.
4. Right-click **Print Spooler** again and choose **Bring Online** to start the service.

Add a SafeCom Pull Printer on Windows 10 and 2016

This section describes how to add a shared SafeCom Pull Printer on Windows 10 and 2016.

1. In a modern Windows interface, navigate to the **Charms** bar and press the **Search** button.
2. Under the appearing apps, select the Control Panel in the **Windows System** section.
3. In the Control Panel, click **Hardware and sound**.
4. In the **Devices and printers** section, click **Advanced Printer Setup**.
5. In the **Add printer** window, click **The printer that I am looking for is not on the list**.
6. Select **Add a local printer or a network printer with manual settings** and click **Next**.
Ensure that the **User Account Control (UAC)** settings is turned off, otherwise you will not be able to add the printer, as there are no sufficient rights to add the SafeCom Pull Port.

i If you have already created a printer that uses the SafeCom Pull Port, you should use this port instead of creating a new one (as described in steps 4, 5, and 6).

7. Choose **Create a new port** and select **SafeCom Pull Port** from the drop-down list, then click **Next**.
8. Enter a unique name of your choice for the port in **Port Name**, then click **OK**.
9. The **Configure Pull Port** dialog allows you to enter the hostname or IP address of the SafeCom server. Select **Use network logon** as method of **User authentication**. Click **OK**.
The **Authorize port configuration** dialog appears.
10. Enter **User logon** and **Password** of a user that has SafeCom Administrator or Technician rights, then click **OK**.
11. Click **Have Disk** to install the files from the printer manufacturer's installation disk (or downloaded the files from the manufacturer's web site). Click **Next**.
12. Enter a **Printer name** and choose whether or not this printer should be your default Windows printer, then click **Next**.
13. Select **Share this printer** and enter **Share name**, then click **Next**.
14. Click **Print a test page** to verify the system, then click **OK** when prompted to confirm that the test page printed correctly, then click **Finish**.

i In SafeCom Administrator, the test page appears as a pending print job under the user you are logged in (as administrator).

Check the printer properties

1. Right-click the printer and click **Printer properties**.
2. On the **Device Settings** tab, check the settings, such as paper size in the trays and installable options.
3. On the **Advanced** tab, select **Start printing after last page is spooled**.
This is required for the tracking and billing information to be correct. Also, it allows for faster spooling.
4. Click **OK**.

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 adding multiple identically configured SafeCom Pull Ports. In our experience, 1-4 ports are sufficient and no more than 12 ports should be added.

Add a SafeCom Pull Printer on client computers

As discussed in [Local SafeCom Pull Printer](#), you may wish to add a local SafeCom Pull Printer on a client computer. To do this, you need to do two things on the client computer:

1. [Install the SafeCom client](#) on the computer.

2. Add a local SafeCom Pull Printer on Windows 10 (see [Add a local SafeCom Pull Printer on Windows 10](#)).

Install SafeCom client

To add a local SafeCom Pull Printer, you need to install the SafeCom Pull Port on the client computer. You only need to do this once.

1. Download the SafeComG4_Server_x64_build_{version_number}.exe file from the link supplied to you. The installation must be run as administrator. When the installation program is launched, click **Next**.
2. Click **Advanced installation**, then click **Next**.
3. Click **Client** and follow the instructions on the screen (see [Client installation](#)).

The SafeCom Pull Port is now installed on the client computer. Next, you need to either modify an existing local printer or add a new local printer. When you do this, you should make sure that:

- The printer is not shared.
- The printer uses the SafeCom Pull Port, which sees to the transfer of documents to the SafeCom server from the SafeCom Pull Printer.
- The SafeCom Pull Port is configured correctly (see [Configure the SafeCom Pull Port](#)).

Add a local SafeCom Pull Printer on Windows 10

1. Click **Start > Control Panel > Devices and Printers**.
2. In the **File** menu, select **Run as administrator** and click **Add a printer**. Select the **The printer that I want isn't listed** option.
3. Click **Add a local printer or network printer with manual settings**.
4. Select **Create a new port** and select **SafeCom Pull Port** from the drop-down list, then click **Next**.



- If **Run as administrator** was not chosen in step 2, Windows reports "Specified port cannot be added. Access is denied".
- If you have installed the SafeCom Print Client (see [Installation](#)), you can select **Use an existing port** and select **scPull** from the list, then click **Next** and continue to step 8.

5. Enter a unique name of your choice for the port in **Port Name**, then click **OK**.
6. The **Configure Pull Port** dialog (see [Configure the SafeCom Pull Port](#)) prompts you to enter the hostname or IP address of the SafeCom server and select the method of user authentication. See step 5 in [Configure the SafeCom Pull Port](#).
7. Click **OK**.
The **Authorize port configuration** dialog appears.
8. Enter the **User logon** and **Password** of a user that has SafeCom Administrator or Technician rights, then click **OK**.
9. Click **OK** and select the manufacturer and printer model, then click **Next**.
10. State whether you want to keep the existing driver or use the new one, then click **Next**.

11. Enter a printer name and select whether this printer should be your default Windows printer, then click **Next**.
12. Select **Do not share this printer**, then click **Next**.
13. Click **Print a test page** to print a test page to verify the system.
You are prompted to confirm that the test page was printed correctly, but the test page is only printed when you log in at the device.
14. For now, click **Close** and **Finish**.

SafeCom Pull Port

The SafeCom Pull Port is a special port monitor that transfers documents to the SafeCom server from the SafeCom Pull Printer. The SafeCom Pull Port is installed when you perform a server installation, a client installation (see [Add a SafeCom Pull Printer on client computers](#)), and when installing the SafeCom Print Client (see [SafeCom Print Client](#)).

i If you have multiple devices you want to use with the "Hide job names" feature, ensure that all devices are properly set to take advantage of the additional value provided by the feature.

If connecting to a shared printer, ensure that the user attempting to connect does have the relevant access rights and credentials for accessing the shared printer, and that the appropriate network logon port settings are employed when connecting to the shared printer.

In workgroup environments, ensure that users who want to access the shared printer have an account on the server the printer is connected to, and that the account uses the exact same credentials as their workstation, and that the printer has been connected using that account.

Enable printer pooling

You can enable Windows printer pooling to minimize the wait for documents to be processed and transferred to the SafeCom server if users are dissatisfied with the time it takes before the SafeCom Print Authentication dialog appears.

1. Click **Start**, point to **Settings**, and click **Printers**.
2. Right-click the SafeCom Pull Printer and click **Properties**.
3. Click the **Ports** tab.
4. Select **Enable printer pooling**.
5. Click **Add Port** to create multiple instances of the SafeCom Pull Port.
You should not use more than 12 ports per queue.


i If you are using the "Hide document name" feature, ensure that all ports attached to the same print queue have the same "Hide document name" setting.

Configure the SafeCom Pull Port


The SafeCom Pull Port is configured when you add a SafeCom Pull Printer.

To configure the SafeCom Pull Port after you have added the SafeCom Pull Printer:

1. Click **Start** and then click **Devices and Printers**.
2. Right-click the SafeCom Pull Printer and click **Printer Properties**.
3. Click the **Ports** tab. Select the SafeCom Pull Port and click **Configure Port**.

 The Default Print Engine setting of the registry is used as the default server. If the registry setting does not exist, localhost is offered as the default.

4. Click **Edit servers** to add, remove, change, or test the connection to the SafeCom server (see [Edit servers dialog](#)).
5. Select the method of user authentication, then click **OK**.
 - **Use network logon**: Select to use your Windows logon as your SafeCom user logon when printing.
 - **Use specified logon**: Select and enter the SafeCom user logon of the user who is to receive all future jobs sent to the print queues that use this Pull Port. This can be combined with [Group print](#) by specifying the name of the group instead of the name of a user.
 - **Show authentication dialog at every print**: Select if the user should be prompted every time they print. SafeCom PopUp must be running on the user's computers to display the prompts for the login (see [SafeCom Print Authentication dialog](#)). Up to 10 minutes may elapse before the choice takes effect. The time is configured by the Windows registry setting CacheExpireSuccess.

 The **User logon** field is limited to 20 characters. If you plan to log in using Windows credentials, including the domain, you must select **Windows authentication** in the SafeCom PopUp.

- **Show authentication dialog on first print only**: Select if the user should only be prompted the first time they print. SafeCom PopUp must be running on the user's computer to show the dialog that prompts for the login (see [SafeCom Print Authentication dialog](#)). Up to 10 minutes may elapse before the choice takes effect. The time is configured by the Windows registry setting CacheExpireSuccess.
- **Use job data logon**: Select to extract the logon from the job data (see [Configure Use job data logon](#)).
- **Default domain**: Use the dropdown menu to select the default domain.
- **V4 printer driver support**: Select if you want to use Microsoft v4 printer drivers through this port. The option is backwards compatible, so your Microsoft v3 drivers continue working on this port.
- **Warning messages if PopUp is not running**: Select this check box to display a warning message when a user attempts to use Delegate Print or Billing Codes when printing while the SafeCom PopUp is not running. This function is only available for printers using Microsoft v3 drivers.
- **PopUp compatibility mode**: Select this option if you want to enable legacy encryption on this port.
- **Hide document name**: Select this option to enable hiding document names in the print queue. This allows for more secure printing, as it eliminates the chance of unauthorized people seeing the original document names. These names appear encrypted.

i If printer pooling is enabled, all printers of the same print queue must have the same value for this setting. The document appears with its original name at the device.

- **Override driver name:** Select and enter the driver name. The specified driver name overrides the driver name supplied by the printer driver

The **Authorize port configuration** dialog appears.

Edit servers dialog

1. In the **Edit servers** dialog, click **Test connection** to test the communication with the SafeCom server, then click **Close**.
2. It is not possible to edit an entry on the server list. Instead, select the server and click **Remove**. Then click **Add**.
3. In the **Add server** dialog, enter the SafeCom server address (IP address or hostname), then click **OK**.

SafeCom Print Authentication dialog

If the SafeCom Pull Port is configured to show authentication dialog at every print, the SafeCom Print Authentication - User logon dialog will appear every time you print.

Select **Stay logged in** to make the dialog appear with the last used ID the next time you print. Restarting the computer or the Print Spooler clears the check box.

i If any **Show authentication dialog** options are enabled and the printer is shared, then SafeCom PopUp (see [SafeCom PopUp - scPopUp.exe](#)) must be running on the users' computer.

Customizing SafeCom PopUp dialogs

Modifying the UI strings of SafeCom PopUp requires modifying the scPopUp.ini file. The language can be selected on the **Settings** window of SafeCom PopUp, or set through the /U command line parameter (see [Setup SafeCom PopUp](#)).

An example of scPopUp.ini can be found in the \template subdirectory of your SafeCom G4 installation directory.

The **General information** section must always be present in your scPopUp.ini file, in the same format as in the template.

Configure Use job data logon

The SafeCom Pull Port (see [Configure the SafeCom Pull Port](#)) can be configured to **use job data logon** instead of the network logon.



- This requires a SafeCom Enterprise Server (Multiserver license).
- This function is not compatible with Microsoft v4 printer drivers.

When printing from SAP and similar applications, the print job is normally associated with a generic user logon rather than the logon of the real user. This is quite unfortunate in a Pull Print scenario, as it causes all jobs to be stored under the name of this generic user.

However, for SAP, it is possible to configure it such that the logon of the real user can be embedded in the job data stream as a PJI command. Please refer to the documentation that came with your application (SAP).

With the user authentication option **Use job data logon**, the SafeCom Pull Port can be configured to extract the logon from the job data.

1. Open the **Configure Pull Port** dialog (see [Configure the SafeCom Pull Port](#)).
2. Select **Use job data logon**.
3. Click **Configure** to open the **Job data properties dialog**.
 - **Job data string** is the string that precedes the logon. The logon (maximum characters) is extracted as the string that is between the **Job data string** (with the potential succession of any skip characters and a start character) and the **Stop character**.
 - **Max search length** is the number of bytes to search into the job data stream. Typically, the job data string is within the first 1000 bytes.
 - **Characters to skip** can be **<None>**, **<Tab>**, **<Space>**, or any entered printable character. It defines that any occurrence of this character should be skipped after the **Job data string** and before the **Start character**.
 - **Start character** can be **<None>**, **<Tab>**, **<Space>**, or any entered printable character. It defines the character in front of the logon.
 - **Stop character** can be **<None>**, **<Tab>**, **<Space>**, or any entered printable character. It defines the character after the logon. A carriage return or new line always terminates the logon string.
 - **Use alternative logon** can be **<None>** or **Network logon**. It defines the fallback logon to use in case the logon cannot be extracted from the job data.

Example:

Extract from file	Date="2007.01.01"Name="JS",File="letter.txt"	Time: 12:15:32 User: JS Doc: letter.txt
Job data string	Name=	User:
Characters to skip	<None>	<Space>
Start character	"	<None>
Stop character	"	<None>
Extracted logon	JS	JS

Add a SafeCom Push Port

When connecting to a shared printer, ensure that the user attempting to connect has the relevant access rights and credentials for accessing the shared printer, and that the appropriate network logon port settings are employed when connecting to the shared printer.

In workgroup environments, ensure that users who want to access the shared printer have an account on the server the printer is connected to, and that account uses the exact same credentials as their workstation, and that the printer has been connected using that account.

If you are printing directly via TCP/IP port 9100, follow these steps to add the SafeCom Push port to a printer.

1. Open the Windows Control Panel and browse to Printers.
2. Open the Add Printer Wizard.
3. Click **Add a local printer**.
4. Choose **Create a new port**, select **SafeCom Push Port** from the drop-down list, and click **Next**.
5. Enter a unique name of your choice for the port in **Port Name**, then click **Next**.

The **Configure Push Port** dialog appears.

i The default print engine setting of the registry is used for the default server. If the registry setting does not exist, localhost is offered as the default.

6. In **Servers**, click **Edit servers** to add, remove, change, or test the connection to the SafeCom server.

i It is not possible to edit an entry on the SafeCom server list in the **Edit servers** dialog. Instead, you have to remove the server and add a new one.

7. Set up the user authentication as required based on the following descriptions.
 - Select **Use network logon** to use your Windows logon as your SafeCom user logon when printing.
 - Select **Use specified logon** and enter the SafeCom user logon of the user who is to receive all future prints sent to the print queues that uses this push port. This can be combined with [Group print](#) by specifying the name of the group instead of the name of a user.
 - Select **Show authentication dialog at every print** if you want to enter your credentials at every print job. SafeCom PopUp must be running on the user's computer to show the dialog that prompts for the login (see [SafeCom Print Authentication dialog](#)). Up to 10 minutes may elapse before the choice takes effect. The time is configured by the Windows registry setting CacheExpireSuccess.

i The **User logon** field is limited to 20 characters. If you plan to log in using Windows credentials, including the domain, you must select **Windows authentication** in SafeCom PopUp.

- Select **Show authentication dialog on first print only** if the user should only be prompted the first time they print. SafeCom PopUp must be running on the user's computer to show

the dialog that prompts for the login (see [SafeCom Print Authentication dialog](#)). Up to 10 minutes may elapse before the choice takes effect. The time is configured by the Windows registry setting `CacheExpireSuccess`.

i The **User logon** field is limited to 20 characters. If you plan to log in using Windows credentials, including the domain, you must select **Windows authentication** in SafeCom PopUp.


- Select **Use job data logon** to extract the logon from the job data (see [Configure Use job data logon](#)).
 - Select a default domain to save the user from entering a domain.
8. In **Output device**, select **Use printer IP address or hostname** and specify the IP address if you are printing directly. Then click **Test connection** to display the **Printer Properties** dialog and to test the connection to the printer.

The printer must be online and allow SNMPv1 access via UDP port 161. Otherwise, you get the message: "Not able to connect to printer".

i If you are printing with a second printer, you need to select **Select the printer that this port will use as output device** and select one of the output devices.

9. Select **SNMP status enabled** if you want SNMP status to be reported.
10. In **Select printer for tracking**, you can select **Select printer from list** and choose a tracking device. Alternatively, select **Auto-create printer** and enter a **Printer name** and an optional **Printer location**.
11. In the **Miscellaneous** section, select the options you need based on the following descriptions:
- **V4 printer driver support**: This option is backwards compatible, so your Microsoft v3 drivers continue working on this port.
 - **Warning messages if PopUp is not running**: Select this checkbox to display a warning message when a user attempts to use Delegate Print or Billing Codes when printing while the SafeCom PopUp is not running. This function is only available for printers using Microsoft v3 drivers.
 - **PopUp compatibility mode**: Select this option if you want to enable legacy encryption on this port.
 - **Show job price before printing**: Select this if users are to unconditionally see a dialog with the cost of the document before they print. If the printer is a shared, printer users must have SafeCom PopUp (see [SafeCom PopUp - scPopUp.exe](#)) set up and running on their computer to confirm that they wish to print the document.
 - **Override user cost code**: The specified cost code overrides the cost code of the user who prints.
Example: If John Smith has the cost code 2949 and prints to a Push Port where a cost code of 1009 is specified, the resulting `UserCostCode` parameter in the tracking record shows 1009 and not 2949.
 - **Override driver name**: The specified driver name overrides the driver name supplied by the printer driver. This is particularly useful to differentiate printers using the HP Universal Print Driver.

- **Hide document name:** Select this option to enable hiding document names in the print queue. This allows for more secure printing, as it eliminates the chance of unauthorized people seeing the original document names. These names appear encrypted.

 If printer pooling is enabled, all printers of the same print queue must have the same value for this setting.

12. Click **OK**.
The **Authorize port configuration** dialog opens.
13. Enter the **User logon** and the **Password** of a user with SafeCom Administrator or Technician rights, then click **OK**.
14. Click the **Have Disk** button, and in the **Install From Disk** dialog, browse to the files from the printer manufacturer's installation disk (or download the files from the manufacturer's web site). Click **Next**.
15. Enter a **Printer Name**, then click **Next**.
16. Select **Share this printer**, enter a **Share name** (P101), then click **Next**.
17. Set up whether this printer should be your default Windows printer, then click **Print a test page** to verify the system.
18. Click **OK** when prompted to confirm that the test page printed correctly, then click **Finish**.

Check the properties of the printer

1. In the Control Panel, right-click the printer, then click **Printer Properties**.
2. On the **Device Settings** tab, check the settings, such as paper size in the trays and installable options.
3. On the **Advanced** tab, select **Start printing after last page is spooled**.
This is required for the tracking and billing information to be correct. It also allows for faster spooling.
4. Click **OK**.

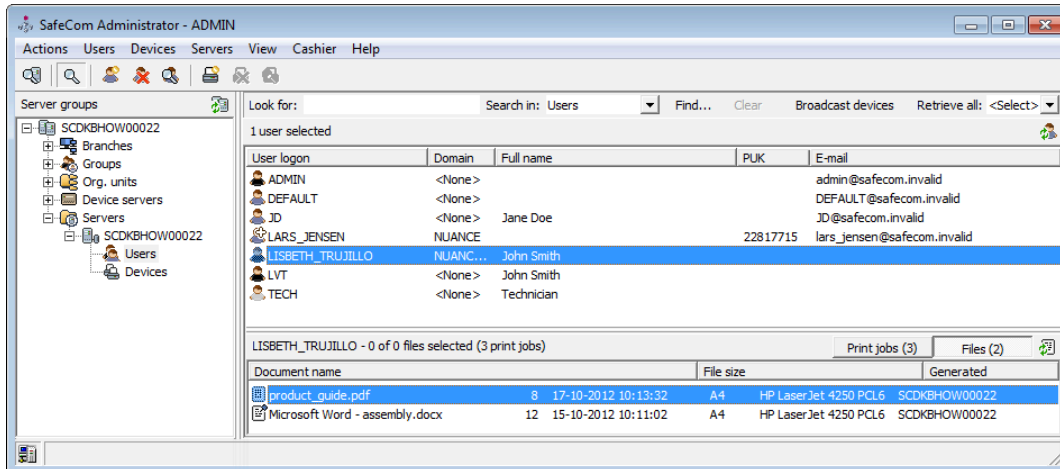
SafeCom Smart Scan

Smart Scan represents an easy way to handle scan-to-folder functionality that bypasses both Microsoft Outlook and complex password issues.

Users start by logging in to the MFP and tapping the **Smart Scan** icon. Scans on the MFP are sent to the SafeCom server that handles administration of the scan job and stores the document file in a private scan folder reserved for the user. This means that scanned files are also subject for deletion based on the specified time in the server properties in SafeCom Administrator.

Users then access and download their files to any chosen location through SafeCom Move – an application running on their local system tray – or through the SafeCom Web Interface. The solution adds increased security, because scan files on the server are encrypted until they are retrieved by the user.

SafeCom Administrator has been updated to also display the user's scanned files. In the document list for each user, toggle between the print jobs and files to view all pending print jobs or scanned files.



i Smart scan is supported on Ricoh devices and HP Future Smart devices. Refer to *SafeCom Go HP Administrator's Guide* or *SafeCom Go Ricoh Administrator's Guide* for detailed information about setup and configuration.

SafeCom Move – scMove.exe

SafeCom Move is a simple way for the user to manage pending print jobs or files scanned through SafeCom Smart Scan.

From SafeCom Move the user can access scanned files, delete them, or download them to any location specified by the user. Furthermore, the user can retain, unretain, or delete regular print jobs.

The scMove.exe is located in the SafeCom installation folder:

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

i SafeCom Move (scMove.exe) must be installed in a folder that also includes the following DLL files: scScum.dll, scIntrLib.dll, scSecureLib.dll, and scUtilLib.dll.

We recommend that you run scMove.exe from a file share, in which case, you need to ensure that Internet Properties on the computer allows local (Intranet) sites and includes the specified share. Otherwise, Windows may present a security warning stating "The publisher could not be verified".

If [Windows Firewall](#) is installed on the computer, TCP port 5740 must be open.

Setup SafeCom Move

1. To start scMove.exe, use the scMove.exe command.

i By default, SafeCom Move is set up to run against the SafeCom server on the localhost and with login type "U" (User logon and PIN code).

2. Change the SafeCom server and the login method by using the following commands:

```
scMove /H [hostname]
scMove /L [login type]
```

Login types:

- **U** – Userlogon and PIN code (default)
- **I** – ID code and PIN code
- **W** – Windows authentication

Example: To change to Windows authentication, enter:

```
scMove /L W
```

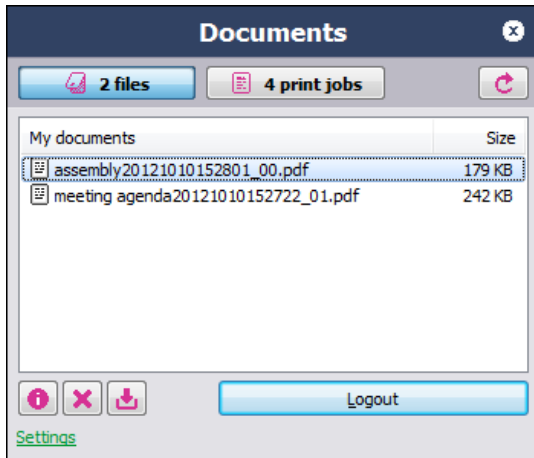
3. To view scMove help, use the following command:

```
scMove.exe /?
```

SafeCom Move example

Below is an example of how SafeCom Move looks to the users.

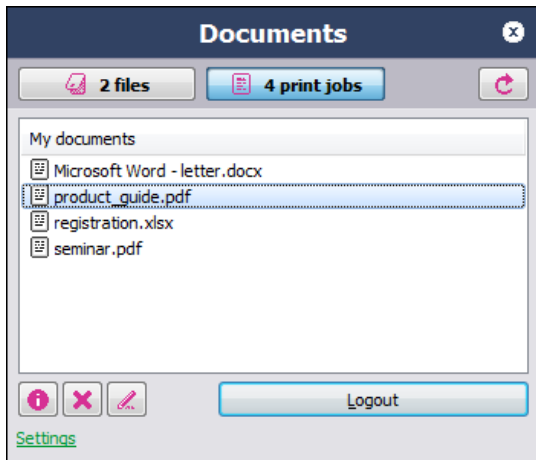
Files:



When selecting a file, the user can choose to delete it, download it, or view the detailed information of the file.

Under **Settings**, the user can set a default directory location for downloaded files.

Print jobs:



When selecting a print job, the user can choose to delete it, retain/unretain it, or view the detailed information of the job.

SafeCom PopUp – scPopUp.exe

SafeCom PopUp displays the following pop-up dialogs on the user's screen:

- **Print authentication:** The user is authenticated during print submission if the user is not logged onto the network. This can be configured for both the [SafeCom Pull Port](#) and the SafeCom Push Port (see [Push print tracking](#)). The Print Authentication dialog can be customized (see [Customizing SafeCom PopUp dialogs](#)). Authentication by card during print submission is possible by specifying the /AU and /LC startup parameters to scPopUp (see [Setup SafeCom PopUp](#)).
- **Delegate print:** With SafeCom Delegate Print, users grant permission to other users to print or collect print jobs on their behalf (see [Delegates](#)).
- **Client billing:** With [SafeCom Client Billing](#), it is possible to ask users to select a billing code during print submission.
- **Print confirmation:** With SafeCom Rule Based Printing (see [Create the rules](#)), it is possible to increase cost awareness among users by asking them to confirm that the document should be printed.
- **Show job price before printing:** With SafeCom Push Print (see [SafeCom Print Authentication dialog](#)), it is possible to show the job price to the user during print submission.
- **SafeCom Print Client offline printing:** When a user submits a print job and the SafeCom server is offline, the SafeCom Print Client dialog opens (see [Direct print if SafeCom server is offline](#)), offering the user to select a printer to send the print job to directly.

Setup SafeCom PopUp

scPopUp.exe is installed as part of the [server installation](#) or the [client installation](#). The PopUp is also installed and started automatically as part of the [Print Client](#) installation, although with Print Client, the PopUp installation can be optionally deselected. The scPopUp.exe is located in the SafeCom installation folder:

C:\Program Files\SafeCom\SafeComG4



- scPopUp.exe must be the same version as the SafeCom G4 Server software. From S82 070.520*10 onwards, scPopUp does not work with earlier versions of SafeCom Pull Port or SafeCom Push Port.
- From S82 070.520*10 onwards, SafeCom Pull and Push ports work with older versions of SafeCom PopUp if the **PopUp compatibility mode** option is checked for the Pull (see [SafeCom Pull Port](#)) or Push (see [Add a SafeCom Push Port](#)) port.
- In case of using Microsoft v3 printers, when the pop-up is not running but would be needed for certain operations (for example, authentication), a notification is displayed with the Windows Print System Asynchronous Notification. The user can start scPopUp and click **OK** on the message tab to continue printing without interrupting the job in question.
- In case of shared network printer queues, restarting the Print Spooler on the server due to any modifications may be only detected after a couple of minutes of delay on the SafeCom PopUp running on your workstations.
- If the computer running SafeCom PopUp is connected to a new shared SafeCom queue, you must restart SafeCom PopUp to detect and work with the new queue.

If you intend to run scPopUp.exe from a file share, you should ensure that the internet properties of the computer allow local (Intranet) sites and include the specified share. Otherwise, Windows may present a security warning stating "The publisher could not be verified".

Start scPopUp

1. Start scPopUp64.exe.

We recommend setting up scPopUp64.exe to start each session, either by making a shortcut in the Windows Startup folder or by starting it in a logon script. To view PopUp help, use the following command:

```
ScPopUp64.exe /?
```

Help:

```
scPopUp64.exe [/AU [r:][<yy>|<yy:uu>]] [/CA <path>] [/G] [/K] [/R] [/S] [/U] [/WT  
[p:]<title>[:zz]]
```

- /G — Run in guest mode, prohibits the user to exit the application.
- /K — Timeout on a dialog selects **OK** button as default.
- /R — Reset saved scPopUp settings to the defaults.
- /U — Specify the LCID of your preferred language (for example, 1033)
- /S — Show splash screen on startup.
- /CA <path> — Specifies the path of the language captions file.
- /AU [r:][<yy>|<yy:uu>] — Show/hide authentication status dialog.
 - r — Indicates that authentication status timer is reset on every print job (default: no).
 - yy — The authentication status dialog timeout warning. Default: 60 seconds.
 - uu — The duration of how long the dialog is displayed (default: 5 seconds, always shown: 0)

- /WT [p:]<title>[:zz] — Force logout based on Window Title
 - p — Indicates that we logout when window title appears instead of disappears.
 - zz — The check interval in seconds (default: 5 seconds)

Example:

```
scPopUp64 /AU R:300 /WT "Clinical Management System":5
```

i The <title> parameter only looks for text matches in window titles and is unable to differentiate files containing the defined text from real applications. For example: If you define "Clinical Management System" in the window title parameter and open a document containing the phrase "Clinical Management System", the pop-up does not react to closing the Clinical Management System application since the document is still open.

If no arguments are supplied, the Pop-Up starts only with TCP connection.

2. Double-click the scPopUp icon in the Windows system tray to see status and version.

SafeCom PopUp deployment on Windows computers

The following SafeCom Popup dialog software must be deployed to client computers:

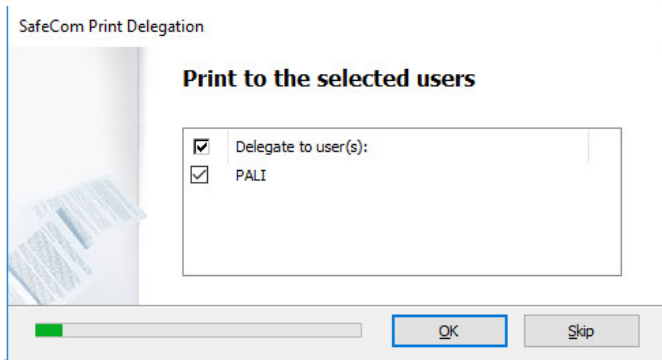
- scPopup.exe
- scPopup.ini (optional; for modifying or localizing the strings of the application)

SafeCom PopUp examples

Below are some examples of how the SafeCom PopUp appears on the user's computer screen.

- **Print authentication:** The following screens can appear if one of the **Show authentication dialog** options is enabled on the SafeCom Pull Port (see [Configure the SafeCom Pull Port](#)) or SafeCom Push Port (see [Push print tracking](#)):

With card swipe:



Control dialog timeout

Timeout for scPopUp is controlled from the Windows Registry settings of the SafeCom Pull Port and SafeCom Push Port.

1. Open the Registry Editor and browse to the following:
 - For Pull Port, browse to: `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Print\Monitors\SafeCom Pull Port\Ports`
 - For Push Port, browse to: `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Print\Monitors\SafeCom Push Port\Ports`

The location of registry settings is the same in a cluster.

2. Create a new DWORD named DialogTimeout.
It can have any value between 3 and 600 seconds. The default is 60 seconds.

Remember logon timeout

This setting shows the logon validity time in seconds if the **Authentication** dialog had the **Stay logged in** check box selected and there was a successful authentication.

This setting is optional.

1. Open the Registry Editor and browse to `HKEY_LOCAL_MACHINE\SOFTWARE\SafeCom\SafeComG4\SafeCom Notifier`.

The location of registry settings is the same in a cluster.

2. Create a new DWORD named RememberLogonTimeout.
The default is 300 seconds.



- When a user is logged on, the system tray tooltip of scPopUp changes to show the name of the logged in user.
- The command line option /AU is related to this function, as it displays if a user is logged on in a format of a status dialog (Authentication Status Dialog). If /AU *x* is used, every subsequent printing resets the timer to the value of RememberLoginTimeout (or 300 seconds, if the setting is not created).

Working with languages

Adding a language, localizing or modifying the UI strings of SafeCom PopUp requires modifying the scPopUp.ini file. The language can be selected on the **Settings** window of SafeCom PopUp, or it can be set with the /U command line parameter (see [Setup SafeCom PopUp](#)).

An example of scPopUp.ini can be found in the `\template` subdirectory of your SafeCom G4 installation directory.

The **General information** section must always be present in your scPopUp.ini, in the same format as in the template.

New languages are defined by their LCID.

Printing encrypted documents

With SafeCom encryption, documents can be encrypted on the network. Encryption applies from the moment the user clicks print on their computer and until the document is collected at the device. This prevents anyone from reading the documents, should they be intercepted on the network. Documents are always encrypted when traveling from the SafeCom Pull Port to the SafeCom server and when they are stored for later printing.

Prerequisites:

- Encryption is included in the [SafeCom license key code](#).
- The user has encryption enabled, that is, **Encrypt documents** is checked on the **Settings** tab in the **User properties** dialog (see [Settings](#)).
- The device has encryption enabled, that is, **Encryption** is checked on the **License** tab in the **Device properties** dialog (see [License](#)).
- A local SafeCom Pull Printer is installed on the computer of the user requiring encryption (see [Add a SafeCom Pull Printer on client computers](#)).
- The device is connected to the SafeCom Controller's 2-port switch. On devices with an internal SafeCom Go solution, decryption is done inside the device.

Make all printing go through SafeCom

This section describes how to ensure that all printing is done solely through SafeCom.

You only need to take special precautions for devices with a built-in and connected network interface. The first precaution is to ensure that only the SafeCom servers are allowed to connect to the device's network interface.

Some network interfaces, such as the HP JetDirect print servers and Ricoh Network Interface Cards, feature an IP host access list. Only the hosts on the list are allowed to access the network interface. In this case, it means that the IP address of the SafeCom server and/or SafeCom Controller should be the only ones on the list. The SafeCom Controller should have a fixed IP address.


You may also need to disable selected network printing protocols, such as the Internet Printing Protocol (IPP). Some network devices also offer the possibility to disable their parallel and/or USB port. For additional information, please refer to the documentation that came with your device / network interface or contact your printer vendor.

Install a card reader on a computer

If the administrator wants to register cards to users (see [Let administrator register cards to users](#)), a card reader must be connected and configured on the computer.

The stand-alone card readers (see [SafeCom ID devices](#)) can be used with the SafeCom Administrator. Most USB card readers can be connected to the computer through the USB port and used directly. Connecting a SafeCom ID device needs to be connected to a USB port if you want to enable SafeCom Print Authentication by card. The serial card readers can be connected to the computer through a SafeCom Serial PC Cable (p/n 660010). The cable connects to the computer's RS-232 DB9 connector for communication and 5 Volt power must be supplied through the PS2 keyboard pass-thru connector.

1. Connect the USB card reader to the USB port.
The serial card reader should be connected to the computer's serial port (COM1, COM2, or COM3).
2. Start the SafeCom Administrator.
3. In the **Actions** menu, click **Options**.
4. Click the **Card reader** tab in the **Options** dialog and make your selections.

 SafeCom ID devices come with ID device licenses, whereas ID device licenses for third-party ID devices must be purchased separately.

Install SafeCom Smart Printer Add-on and Driver

The Smart Printer Add-on and Driver increases versatility across mixed MFPs from different vendors, as it ensures that users can use only one print queue, and run complex jobs on all printers without encountering driver incompatibilities.

The Smart Printer Add-on and Driver creates and stores print data on the SafeCom server or on the Print Client in Microsoft XPS format (XML Paper Specification format) until it knows which printer will be used. When the user logs onto an MFP, the system identifies the device type and only then runs the job through the correct vendor-specific printer driver.

The Add-on and Driver software is distributed in two separate installation packages:

- **SafeCom Smart Printing Driver:** A printer driver that converts the print data to XPS.
- **SafeCom Smart Printer Add-on:** A service that is installed either on the SafeCom server or on the computer running the SafeCom Print Client. The service directs the print job to the best suitable printer driver from a specific printer vendor.

Follow the steps below to enable printing using the concept of SafeCom Smart Printer Driver.

1. Install the SafeCom Smart Printer Add-on.
 - SafeCom server (see [Install Smart Printer Add-on on SafeCom server](#)).
 - SafeCom Print Client (see [Install Smart Printer Add-on on SafeCom Print Client](#)).
2. Install the SafeCom Smart Printing Driver (see [Install SafeCom Smart Printing Driver](#)) and add a SafeCom Pull Printer that uses the Smart Printing Driver.
3. Verify the installation by collecting your first document (see [Verification – Collect your first document](#)).


i It is recommended to install the vendor-specific printer driver in advance. For HP Universal and similar print drivers, this is best accomplished by downloading the latest version and subsequently extracting the files and using the "add driver" function in the Windows Print Server Properties to add the printer driver.

Install Smart Printer Add-on on SafeCom server

1. Make sure the server meets the following requirements:
 - SafeCom G4 Server version S82 070.510*01 or newer
 - Windows Server as described in [Server requirements](#)
 - Microsoft .NET Framework 3.5
2. Download the `safecom_smart_printer_addon_xxx.exe` file from the link supplied to you. The installation must be run as administrator.
3. Follow the instructions and click **Finish** when done.
4. Install the SafeCom Smart Printing Driver as described in [Install SafeCom Smart Printing Driver](#).

Install Smart Printer Add-on on SafeCom Print Client

1. Make sure the client meets the following requirements:
 - SafeCom Print Client version S82 070.510*03 or newer
 - Windows 10 or later
 - Microsoft .NET Framework 3.5
2. Download the SafeCom_print_client_smart_printer_addon_xxx.exe file from the link supplied to you. The installation must be run as administrator.
3. Follow the instructions and click **Finish** when done.
4. Install the [SafeCom Smart Printing Driver](#).

 Similar to the SafeCom Print Client software, the Add-on can also be deployed silently using the /VERYSILENT option (see [Command line parameters](#)).

Install SafeCom Smart Printing Driver

To install the Smart Printing Driver on Windows 10 or on a Windows Server 2016 system, follow the steps below.

1. Download the SafeCom_smart_printing_driver_xxx.zip file from the link supplied to you.
2. Extract the printer driver files to a folder.
You can refer to this folder later as you proceed to [Add a SafeCom Pull Printer on Windows 10 and 2016](#).
3. Remember to print a test page that you will use for verification in [Verification – Collect your first document](#).

Configure drivers to use both 32-bit and 64-bit clients

To support client computers that use different processor architectures than the print server, you must install additional drivers. For example, if your print server is running a 64-bit version of Windows and you want to support client computers running 32-bit versions of Windows, you must add x86-based drivers for each printer.

1. Open Print Management on the print server.
2. In the left pane, click **Print Servers**, click the applicable print server, and click **Printers**.
3. In the center pane, right-click the printer to which you want to add additional printer drivers, then click **Manage Sharing**.
4. Click **Additional Drivers**.
The **Additional Drivers** dialog appears.
5. Select the check box of the processor architecture for which you want to add drivers.
For example, if the print server is running an x64-based edition of Windows, select the **x86** check box to install 32-bit version printer drivers for client computers running 32-bit versions of Windows.

If the print server does not already have the appropriate printer drivers in its driver store, Windows prompts you for the location of the driver files.

6. Download and extract the appropriate driver files, and then in the dialog that appears, specify the path to the .inf file of the driver.

i For more information on handling driver configuration under various Windows operating systems, check the relevant Microsoft article about printer drivers.

Verification – Collect your first document

1. While you installed the SafeCom Smart Printer Driver and added the SafeCom Pull Printer that uses the driver (see [Install SafeCom Smart Printing Driver](#)), you should have printed a test page. If not, then please print a test page before proceeding.
2. Open the SafeCom Administrator and verify that the test page is listed as a pending document for you and that the SafeCom Smart Printer Driver is listed as the **Driver**.
3. Verify that the SafeCom-enabled device you intend to collect the document at is configured for High-speed printing (default).
4. Go to the device and log in, then print the test page.

i You will experience a first-time delay of 10-30 seconds as the system is creating the print queue the first time.

The automatically created print queue is named "SafeCom-{Device ID}". Depending on your setup, you can verify the existence of the print queue on either the SafeCom server, referred by the SafeCom-enabled device, or your computer running the SafeCom Print Client.

- i**
- The {Device ID} can be seen in SafeCom Administrator in the upper right corner (ID: {xx}) in the **Settings** tab in the **Device properties** dialog. The ID can also be added as a separate column to the list of devices in SafeCom Administrator. In the list of devices, right-click the column header and select **ID** in the menu.
 - If the SNMP community name of the device is not public, you have to set it manually through **Control Panel > Devices and Printers > Safecom-{Device ID} > Printer properties > Ports > Configure Port > SNMP Status Enabled > Community Name**.

5. Optionally, print and collect a second test page to verify the absence of the delay you experienced when collecting the first document in step 4 above.

If the print fails

If the service fails to locate a compatible driver for the device, the queue generation fails and the print is canceled. The trace will contain the error (example):

```
"Mon Jun 03 15:45:52.773, tid:03708> Result: [0x80131500]: Failed to register device "2". Failed to locate driver for Hewlett-Packard - HP LaserJet flow MFP M525."
```

Installing a compatible driver and repeating the printing process fixes the issue.

Update selected SafeCom components

To update to a completely new SafeCom G4 Server version, please refer to the sections: Single server (see [Update SafeCom software – single server](#)), Multiserver installation (see [Using Group Management Service Account for services](#)), and Cluster installation (see [Cluster installation](#)).

Kofax may release updates for some of the components. Always review the ReadMe file for the update, as it may contain additional and important information.

The update of each SafeCom component is covered below:

- [SafeCom Administrator](#), scAdministrator.exe
- [SafeCom port monitors](#), scPullPM2k.dll and scPushPM2k.dll
- [SafeCom job server](#), scJobServer.exe
- [SafeCom secure library](#), scSecureLib.dll
- SafeCom ID code conversion, [filtercard.dll](#)
- [SafeCom parser](#), scParser.dll
- [SafeCom rule executer](#), scRuleExecuter.dll

Update SafeCom Administrator

1. Close the SafeCom Administrator.
2. Replace the scAdministrator.exe in the SafeCom installation folder with the new one.



- If the server is clustered, use the Cluster Administrator to move the virtual server as you update scAdministrator.exe on the nodes.
- To determine the version, right-click the scAdministrator.exe file, click **Properties** and click the **Version** tab.

Update SafeCom port monitors

1. Stop the Print Spooler (see [How to start and stop the Print Spooler](#)) on the computer.
2. Replace the scPullPM2k.dll and scPushPM2k.dll files in the C:\Windows\system32 folder. In case of a Windows 32-bit system, skip to step 4. In case of a Windows 64-bit system, proceed to the next step.
3. Replace the scPullPM2k.dll and scPushPM2k.dll files in the C:\Windows\syswow64 folder.
4. Start the Print Spooler.




- If any of the servers are clustered, use the Cluster Administrator to move the virtual server as you update the files on the nodes.
- To determine the version, right-click the file, click **Properties** and click the **Version** tab.

Update scJobServer.exe

1. Perform the following steps on all SafeCom servers.
 - a. Stop the SafeCom service (see [Start and stop the SafeCom service](#)).
 - b. Replace the scJobServer.exe file in the SafeCom installation folder with the new one.
 - c. Restart the SafeCom service.

 On Windows 64-bit, the file is named scJobServer64.exe.

2. If you are using the SafeCom G4 Web Interface, restart the following services for the update to take effect:
 - IIS Admin Service
 - HTTP SSL
 - World Wide Web publishing service



- If any of the servers are clustered, use the Cluster Administrator to move the virtual server as you update the scJobServer.exe on the nodes.
- To determine the version, right-click the scJobServer.exe file, click **Properties** and click the **Version** tab.

Update scSecureLib.dll

1. Perform the following steps on all SafeCom servers.
 - a. Stop the SafeCom service (see [Start and stop the SafeCom service](#)) and the Print Spooler (see [How to start and stop the Print Spooler](#)).
 - b. Replace the scSecureLib.dll file in the SafeCom installation folder with the new one.
 - c. Restart the SafeCom Service and the Print Spooler.

 On Windows 64-bit, the file is named scSecureLib64.dll.

2. If you are using the SafeCom G4 Web Interface, restart the following services for the update to take effect:
 - IIS Admin Service
 - HTTP SSL
 - World Wide Web publishing service



- If any of the servers are clustered, use the Cluster Administrator to move the virtual server as you update the scSecureLib64.dll on the nodes.
- To determine the version, right-click the scSecureLib64.dll file, click **Properties** and click the **Version** tab.

Update filtercard.dll

This section is relevant only for customers who have been supplied with a filtercard.dll to accomplish on-the-fly ID code conversion. This method can be used in installations where SafeCom ID devices return ID codes differently.

1. Unzip the received file.
2. If the received DLL file is not called filtercard.dll, rename it.
3. Copy the filtercard.dll file to the SafeCom installation folder.

The default folder is `C:\Program Files\SafeCom\SafeComG4\`.

4. Restart the SafeCom service.

The above steps should be performed on all SafeCom servers. They should also be performed on all the computers that have SafeCom Administrator installed and a card reader connected (see [Install a card reader on a computer](#)).

Chapter 4

SafeCom Administrator

SafeCom Administrator is the application you use to configure and administer your SafeCom solution. SafeCom Administrator can be installed on any Windows computer to administer all the SafeCom servers within TCP/IP range of the computer.

When you log in to SafeCom Administrator, the [SafeCom Assistant](#) guides you through the steps needed to make your devices part of the SafeCom solution.

Install SafeCom Administrator

To administer your SafeCom solution from other computers, simply install the SafeCom Administrator on those computers. If you also want to install a local SafeCom Pull Printer or SafeCom Push Printer, you must install the SafeCom Client first (see [Add a SafeCom Pull Printer on client computers](#)).

1. Download the `SafeComG4_Server_x64_build_{version_number}.exe` file from the link supplied to you. The installation must be run as administrator. When the installation program is launched, click **Next**.
2. Click **Advanced installation**, then click **Next**.
3. Click **Tools**.
4. Select **SafeCom Administrator**. Follow the instructions on the screen or see [Log in to SafeCom Administrator](#) for more details.

Log in to SafeCom Administrator

1. Click **Start**, point to **All Programs > SafeCom G4**, and click **SafeCom Administrator**.

i If you want to restart SafeCom Administrator right after closing it, either wait for a few seconds or check and ensure that the previous instance is no longer running in the background.

2. In SafeCom Administrator, click the server to log in and enter the user logon and password.
 - a. To log in normally, enter the user logon (default ADMIN) and password (default nimda). Once you are logged in, you can change the user logon and password.

i If the user belongs to a domain, it must be specified in front of the user's logon followed by a slash (/) or a backslash (\). Example: MYDOMAIN\JS. Alternatively, you can specify the user logon followed by the symbol "@" and the domain, like this: JS@MYDOMAIN.

- b. To log in with Windows credentials, enter your Windows logon followed by the symbol "@" and the domain in the **User logon** field, then enter the password.

SafeCom Assistant

When you log in to SafeCom Administrator, the SafeCom Assistant appears. The SafeCom Assistant is not present in multiserver solutions.

The SafeCom Assistant guides you through a 3-step process to make your devices part of the SafeCom solution. You can jump between the steps by clicking on the title (for example, *2 Add SafeCom Pull Printer*).

Clear **Show the screen at login** if you do not want the SafeCom Assistant to open at login.

1. Manage devices.

- **Select the device type:** Click the type of SafeCom device: **SafeCom Go** (Canon, Fuji Xerox, HP, Konica Minolta, Kyocera, Lexmark, Ricoh, Sharp, Xerox) or **SafeCom Controller** (Other).
- **Download device manuals and software:** Download the required files if the manuals and the device_software (see [Location of device software](#)) subfolders do not contain them, then click **Next**.¹⁵
- **Open the device manual** (and install device hardware): The relevant device manual appears. You may need to open and consult this manual to install the device hardware and/or send software to the device. The manual is in PDF format and requires Adobe Reader. Then click **Next**.¹⁶

2. Add a SafeCom Pull Printer.

- **Add a SafeCom Pull printer:** Click **Windows Add Printer Wizard** to open this and add a shared printer to be used for Pull printing. Follow the instructions in the device manual. If a SafeCom Pull Printer is already added, you do not need to do this.
- **Add device:** Click **Add device** to add the physical device to the SafeCom solution. On SafeCom Go HP, SafeCom Go Lexmark, and SafeCom Go Ricoh, the steps include sending software to the device. Complete the steps according to the device manual or as documented in [Add device](#).

3. Add a SafeCom Push Printer.

- **Open SafeCom Port Configurator:** If you have an existing TCP/IP printer and wish to convert this to a SafeCom Push printer, and thus also be able to track documents that are printed directly, then click **Close** and complete the steps in [SafeCom Port Configurator](#).

¹⁵ To get future updates, select **Check for updates** in [System overview](#).

¹⁶ The manual is also added to the list of manuals in [System overview](#).

Change password

1. In the **Users** menu, click **Change password**.

i Passwords can be maximum 16 characters.

2. Enter your **Old password** and **New password**, then confirm your new password.
3. Click **OK**.

The password can also be changed in the **User properties** dialog (see [Rights](#)).

Test server

1. In the **Actions** menu, click **Test server**.
2. Enter the **Server address** (IP address or hostname) and click **Test**.

The connection can also be tested in the **Server properties** dialog (see [Server](#)) or by right-clicking a SafeCom server and clicking **Test server**.

The **Loop** check box and the **Server address** field are only present when the **Test server** dialog is opened from the **Actions** menu.

Menus and commands

This section lists the menus and commands of the SafeCom Administrator, their shortcut keys, and a reference to relevant sections in this guide. Additional commands may appear if your solution includes any add-on modules, such as Tracking and Pay.

Actions	Login	Enter	Log in to SafeCom Administrator
	Logout	Ctrl + Q	
	Test server...		Test server
	Reports...	Ctrl + R	SafeCom Reports
	Export...	Ctrl + E	Export data
	Server group Add server group... Remove server group... Server group properties... Locate server groups	Ctrl + L	
	Options...		Options dialog
	Exit	Alt + F4	
	Users	Refresh	F5








Add user...	Insert	Add users manually
Delete user	Delete	Delete users
Import users...		Import users
Aliases...		
ID codes...		List of ID codes
Domains...		
User groups Add group... Delete group Group properties...	Insert Delete Alt + Enter	Groups
Jobs Refresh... Auto-retrieve Delete job	F5 Delete	Delete a user's print jobs (documents)
Change password...		Change password
User properties...	Alt + Enter	User properties

Devices	Refresh	F5	
	Add device...	Insert	Add device
	Delete device	Delete	Delete devices
	Import Ethernet Card Reader		Import Ethernet Card Readers
	Send Go Loader...		Update software
	Update software...		Update software
	Restart...		Restart devices
	Open in web browser		Open in web browser
	Monitor setup...		Monitor device
	Charging schemes Refresh Add charging scheme Delete charging scheme Charging scheme properties		Charging schemes
	Device properties...	Alt + Enter	Device properties



Servers	Refresh		
	Add server...		Add server
	Delete server...		Delete a secondary server from a multiserver group
	License...		License
	Branches Add branch... Delete branch... Branch properties...	Insert Delete	
	Organizational units Add org. unit... Delete org. unit Org. unit properties...	Insert Delete	Organizational units
	Device servers Add device server... Delete device server Device server properties... Device server failover		Device Servers
	Rule Based Printing...		SafeCom Rule Based Printing (RBP)
	Client Billing Manage billing codes... Import billing codes... Schedule billing code import...		SafeCom Client Billing
	Tracking data Export tracking data... Import tracking data codes...		Export tracking data Hide job names in tracking data
	Statistics...		Statistics
	Event log...		Event log
	Server properties...	Ctrl + Enter	Server properties
	View	SafeCom Assistant...	
Toolbars Users Devices Servers Charging schemes Search Tools			
View server group info...			Server group info








	Expand server view at login All Branches Groups Servers		
Cashier	Account status...		Account status
	Cash flow report...		Cash flow report
Help	Support...		
	SafeCom online...		
	About...		

Server group and server icons






	Server group
	Primary server
	Secondary server
	Offline server
	Unsupported server group (old version)
	Server group is unavailable (unable to connect)
	Replication problems











User icons

	Standard user
	Default user



	Locked user (login prevented)
	User with no defined home server
	User has been moved to a failover server
	Technician
	Cashier user (requires SafeCom Pay)
	Administrator
	Administrator with limited rights

Device icons

	MFP or printer with SafeCom Controller
	MFP with SafeCom Go/SafeCom Controller
	MFP with SafeCom Go/SafeCom Device Server
	MFP with SafeCom Go Canon
	MFP with SafeCom Go HP
	Printer with SafeCom P:Go HP










	MFP with SafeCom Go High-end HP
	MFP with SafeCom Go Lexmark
	Printer with SafeCom P:Go Lexmark
	MFP with SafeCom Go Ricoh
	Printer with SafeCom P:Go Ricoh
	Push Printer
	Ethernet Card Reader
	Device with no defined home server
	Device registration not completed
	Device not registered in the SafeCom solution



Document icons

	Document
	Retained document
	Group printed document

	Delegated document
	Branch office document
	Branch office document retained
	Document delegated and retained
	Job deleted after first print
	Group retained print job

Other icons

	Branches (top level)
	Branch
	Computer in branch
	Groups (top level)
	Group
	Organizational units (top level)
	Org. unit
	Servers (top level)
	Device server group

	Standard charging scheme (requires SafeCom Tracking)
	Default charging scheme (requires SafeCom Tracking)

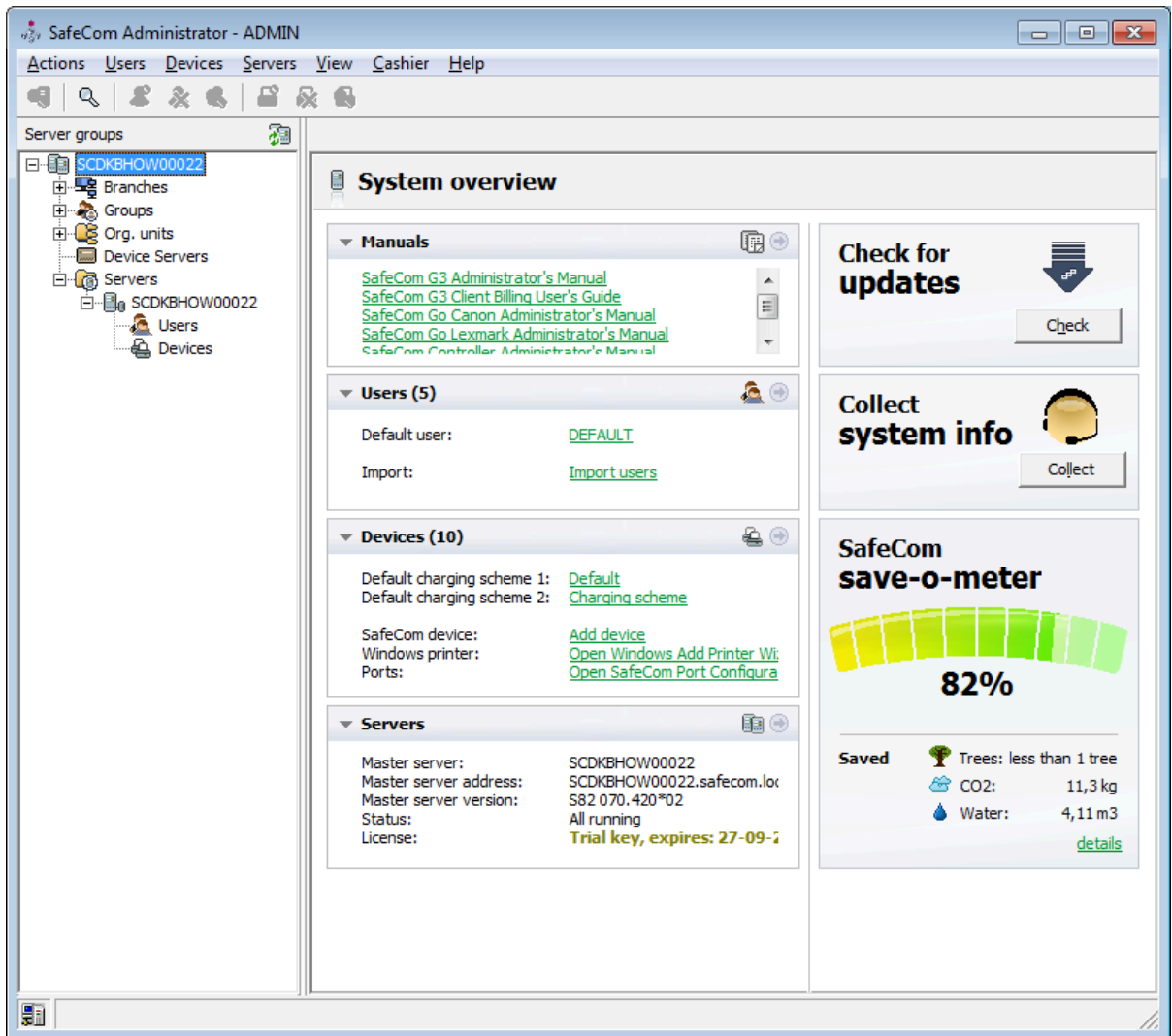
Built-in user accounts

The SafeCom solution features two built-in user accounts:

- **ADMIN:** Administrator account with the default password nimda.
- **TECH:** Technician account with the default password hcet, initial PUK code 12345678, and default PIN code 1234.

System overview

Click the server group to open the **System overview**. This provides easy access to system information, manuals, updates, and common tasks.



Guides

- *SafeComG4 Administrator's Guide* (this guide) is the initially listed manual. Relevant SafeCom Go Administrator's Guides and others are added to the list as you use the [SafeCom Assistant](#).

Users

This menu shows the total number of users (initially two). Click the **Users** arrow icon to open the list of users on the primary server.

- **Default user** shows the user logon of the [default user](#). Click the user logon to open the **User properties** dialog.
- Click **User import** to open the **Scheduled user import** dialog (see [Import users](#)). The date and time of the next scheduled user import is shown.

Devices

This menu shows the total number of devices. Click the **Devices** arrow icon to open the list of devices on the primary server.

- Click **Default charging scheme 1** and **Default charging scheme 2**, then click the respective names to open the **Charging scheme** dialog (see [Charging schemes](#)).
- Click to configure and register the device on the SafeCom primary server. This function is not available in a multiserver solution, as you would normally have devices registered on the secondary servers.
- Click **Windows Add Printer Wizard** to open this.
- Click **SafeCom Port Configurator** to open this.

Servers

The **Servers** menu shows information about the primary and secondary servers. Click the **Servers** arrow icon to open the list of servers.


Click the **License** arrow icon to open the dialog.

Device Servers

The **Device Servers** menu shows information about the device servers. Click the **Device Servers** arrow icon to open the list of device servers and device server groups.

Right-click a device server in the list to access the grouping feature (see [Group device servers](#)).

Each device has a specific device server as its home server (the device server to which the device was added to), and by default, all information and data of a device is handled by the home server of that device. In case of a device failover or a device server fallback, the members of the device group distribute the incoming load evenly.

 If device failover occurs while a user is logged in, the fallback to the device's home server does not occur until the user logs out and the device goes into idle state. This prevents user session interruptions.

Collect system info

In the **Collect System Info** menu, click **Collect**.

Check for updates

1. Click **Check** in the **Check for updates** menu.
A connection is established to the SafeCom Update Server to check for new updates of manuals, device software, and release notes.
2. Click **Run in background** to have the files downloaded while you continue your work.
If access to the internet requires a proxy server, this can be specified in the **Network** tab in the **Options** dialog (see [Network](#)).

i If the **Check for updates** function is used on a cluster, you are advised to update both nodes.

Save-O-Meter

For the SafeCom Save-O-Meter to work, the **Track deleted print jobs** option in the **Tracking** tab in the **Server properties** dialog must be checked (see [Tracking](#)).

i The widget in the Save-O-Meter requires .NET Framework 4.0 or later to function properly.

License

The **License** dialog can be accessed from the **Servers** menu. The **License** dialog shows the number of licensed server features, devices, and device features, and it allows you to install license upgrades in the form of a key code. More information about license key codes is available in [Install the SafeCom license key code](#).

1. Enter your key code in the **Enter key code** field.
2. Click **Apply**.
 - **Current key** displays the license key code currently used by the SafeCom server.
 - **Listing features** displays the features activated by the current license key code.

See section [Advanced search – Device licenses](#) to see how the **Find devices** function can show which device is using which device license.

Check server group properties

The **Server group properties** dialog can be accessed from the **Servers** menu by right-clicking the group in the **Server groups** pane.

1. Click **Search** to search for server groups.
The search results appear in a dialog.
2. Click **Test** to test the connection.

Server properties

The **Server properties** dialog can be accessed from the **Servers** menu, the **Server** button, and by right-clicking the server in the **Server groups** pane.

The dialog comprises the tabs:

- **Server**
- **Users**
- **Devices**

- **E-mail**
- **Failover** (see [Failover servers](#))
- **Tracking** (see [Tracking](#) and [Configure SafeCom primary server](#))
- **Billing** (see [Billing](#) and [Configure SafeCom Client Billing](#))
- **Encryption**

Server

Server | Users | Devices | E-mail | Tracking | Billing | Encryption

Server

Server group: 2012SRV01

Computer name: 2012SRV01

Org. unit: <None>

Server address: 2012SRV01 Test server...

Events

Write event to Windows event log Audit log

Database integrity check


Occurs once at: 00:00 on days: Monday Tuesday Wednesday Thursday Friday Saturday Sunday

Occurs every: 2 hours Starting at: 00:00

Delete print jobs after: 1 day(s) 0 hour(s) 0 min(s)

ID: 1 OK Cancel Apply

Server group is the name of the server group. **Computer name** must match the computer name of the SafeCom server. Refer to [Determine the computer name](#).

i If using SafeCom Administrator version 9.41.6.2, the server group name can be changed. If clicking the **Refresh servers** icon  in the **Server groups** pane within a minute after changing the name, the old server group name appears again in the **Server groups** pane. Click the **Refresh servers** icon again after another minute, and the new name appears in the **Server groups** pane.

Org. unit is the organizational unit the SafeCom server belongs to (see [Organizational units](#)). **Server address** is the address of the SafeCom server. Click **Test server** to test the connection (see [Test server](#)).

Select **Write event to Windows event log** (see [Event log](#)) if you wish to use the Window Event Viewer to view event log messages from the SafeCom solution.

Select **Audit log** if you wish to use the Window Event Viewer to view log messages related to user login/logouts from the SafeCom solution.

Database integrity check verifies the consistency between document references in the SafeCom database and executes the document deleting functionality. The check can take place on selected weekdays (Monday, Tuesday, ... , Sunday) at a specific time or at regular predefined intervals starting at a specific time. The available intervals are every 10, 20, or 30 minutes, or every 1, 2, 3, 4, 6, 8, and 12 hours. Every 2 hours on all weekdays is the default setting.

Select **Delete print jobs after** to keep the print in the SafeCom solution for the specified number of days, hours, and minutes. The default is 1 day.

Users

Server properties - BP-REC-S339

Server | **Users** | Devices | E-mail | Tracking | Billing | Encryption

Automation

- Create users at first print
 - Same ID code as User logon
- Generate PUK on Pull print
- Auto-create e-mail addresses with domain:
- Release credits reserved on error

Security

- Max login attempts:
- Allow users to change PIN code Deny multi delete
- Hide: ID codes Document names
- Allow delegates

IDs

- Max number of IDs per user: Register by Windows auth.
- User registered ID number and beyond
- expires by the end of:

Default settings

- Default user: NEWUSER
- Keep and use settings from default user when creating new users
- Initial Account 2:

ID: 1


Under **Automation**, you can select . This means that a new user account is created in the database the first time the new user prints with the SafeCom solution. Select **Same ID code as User logon** if newly created users log in at the device with their user logon (JS).

Select **Generate PUK on Pull print** if the PUK code should be generated during Pull print. The PUK code can be e-mailed (see [E-mail](#)).

Select **Create e-mail addresses with domain** to combine the user logon (JS) and the E-mail domain (safecom.eu) into the user's valid e-mail address.

Select **Release credits reserved on error** to give back reserved credits to the user if an error occurs. This is only relevant if SafeCom Pay (see [Ensure that users pay](#)) is used.

Under **Security**, you can specify **Max login attempts** to control the number of times the user can try to log on with an invalid PIN code before the account is locked. The default is 3 times. The administrator can unlock a locked user account by clearing **Prevent login** on the **Identification** tab in the **User properties** dialog (see [Identification](#)).

 The max login attempts do not apply to users with administrator rights on the device. However, the setting does affect scAdmin, so administrators can lock themselves out if the max login attempts are exceeded. Ensure that you set up your system carefully, use multiple administrator accounts to be able to unlock locked administrator accounts.

Select **Allow users to change PIN code** to allow users to change their PIN code through the SafeCom G4 Web Interface and SafeCom-enabled devices (restrictions may apply). Do not select this if you wish to manage PIN codes centrally.

Select **Deny multi delete** to prevent deleting multiple devices and users. This option is only editable for administrators with full rights for users.

Select **ID codes** to hide user codes and card numbers in SafeCom Administrator to all users except the users with administrator rights (see [Hide ID codes](#)). The administrators are still able to see and export ID codes.

Select **Document names** to hide document names in SafeCom Administrator. When this is checked, the **Document name** column in the list of a user's pending jobs is not visible for users that do not have administrator rights (see [Hide document names](#)).

Select **Allow delegates** to permit users to delegate or accept delegation of print jobs. **Allow delegates** is not selected by default.

Under **IDs**, you can specify **Max IDs per user**. By default, there is one ID per user. The **IDs** section is not present in the **Server properties** dialog of SafeCom secondary servers. You can also specify an expiration date for the user ID through the **expires by the end of** list.

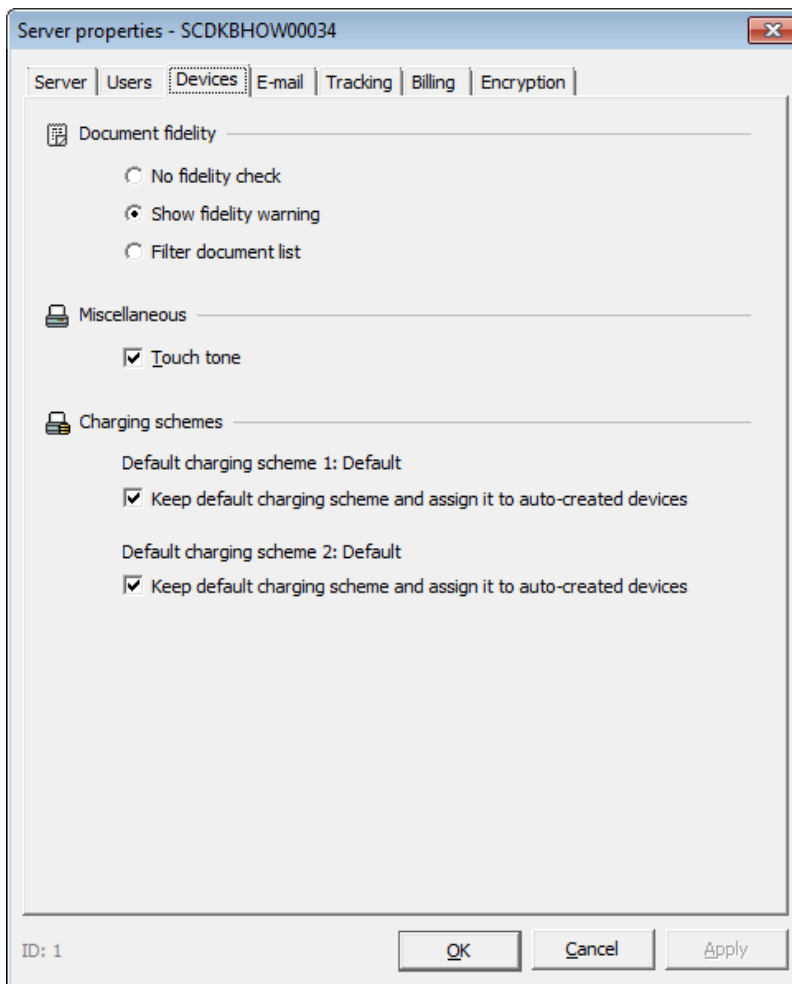
The **Register by Windows authentication** option allows users to register their card at the device using their Windows credentials. This feature is only available on HP Unified Client.

Under **Default settings**, it shows if a [default user](#) is defined. If there is a default user, you can select **Keep default user and use settings when creating new users**. You can select the default user by right-clicking a user with standard rights in the list of users.

In the list of users, the default user is indicated with a plus  sign.

Initial account 2 is only relevant if SafeCom Pay (see [Ensure that users pay](#)) is used.

Devices



As discussed in [Printer driver and document fidelity considerations](#), document fidelity is determined by comparing the name of the printer driver embedded in the print job with the list of driver names returned by the SafeCom Controller or SafeCom Go. You may select from the following options:

- **No fidelity check:** All the user's documents can be collected at the device.
- **Show fidelity warning:** All the user's documents can be collected at the device. If SafeCom Front-end is used, a warning dialog appears whenever the user attempts to print a document that was generated with a driver that is not included on the SafeCom Controller's list of driver names.
- **Filter document list:** Only those documents with a matching driver name can be collected at the device.

Touch tone controls if touching the touch-screen should cause a beep sound. The change takes effect the next time someone logs in at the specified SafeCom ID devices.

E-mail

Server properties - WSLEJ3

Server | Users | Devices | **E-mail** | Tracking | Billing | Encryption

E-mail options

SMTP server address: Port:

Reply e-mail address:

Connection security: None STARTTLS SSL/TLS

Authentication:

Administrator

E-mail address:

E-mail messages: Event Credits reserved notification

Users

E-mail PUK code when generated

E-mail welcome message to new users

E-mail job deletion note to author of job

E-mail delete warning to: Author of job Recipients of job

Send warning ahead: day(s) hour(s) min(s)

OK Cancel Apply

SMTP server address shows the hostname or the IP address of the mail server that is used to send outgoing mails. **Port** is 25 by default.

Reply e-mail address is used by the SafeCom auto-mailer when sending e-mails.

Connection security settings determine if the connection to the mail server is encrypted:

- **None:** The connection is not encrypted (default port 25).
- **STARTTLS:** The connection starts as unencrypted but attempts to make a secure connection if the mail server supports it (default port 587).
- **SSL/TLS:** (Recommended when possible) The connection is encrypted (default port 465).

i STARTTLS or SSL/TLS connection security requires that the SafeCom Mail Service log on account has Read access to the private key of the certificate specified in the TlsCert registry entry, which is created by SafeCom itself under `HKLM\Software\SafeCom\SafeComG4`.

Authentication methods used to verify that you are the owner of the account you are trying to access. The following options are available:

- **None:** No need for authentication to connect to the mail server.
- **Password:** Username and password are required for the connection.
- **NTLM:** NT LAN Manager authentication. See [Configure NTLM SMTP authentication](#) for more information.
- **Microsoft 365 OAuth2:** OAuth2 protocol is used to connect to the Microsoft mail server. See [Configure Microsoft 365 OAuth2 SMTP authentication](#) for more information.
- **Google OAuth2:** OAuth2 protocol is used to connect to the Google mail server. See [Configure Google OAuth2 SMTP authentication](#) for more information.

E-mail address: Type in the e-mail address where SafeCom should send "Event" and "Credits reserved notification" messages. These messages help administrators address potential problems proactively. For example, these e-mails may inform the administrator that a trial license is about to expire in a couple of days. The administrator can also look at the [Event log](#).

If you select **E-mail PUK code when generated**, the PUK code is automatically sent to the user through e-mail using the template EmailPUK.txt (see [Customize and translate e-mail messages](#)). A PUK code is generated in the following ways:

- If **Generate PUK on Pull print** is checked in the **Users** tab in the **Server properties** dialog (see [Users](#)).
- When generating a PUK code in the **ID code** tab in the **User properties** dialog (see [ID code](#)).
- When importing users while **Generate PUK** is checked (see [Import users](#)).

i No e-mail is sent if the PUK is generated from the SafeCom G4 Web Interface.

If you select **E-mail welcome message to new users**, a welcome message is automatically sent to the user through e-mail using the template EmailWelcome.txt (see [Customize and translate e-mail messages](#)).

If you select **E-mail job deletion note to author of job**, the author receives an e-mail when a document is deleted. See EmailJobDelete.txt in [Customize and translate e-mail messages](#).

In **E-mail delete warning to**, you can select **Author of job** and/or **Recipients of job**. If checked, an e-mail warning is sent that specifies the remaining time before deletion. See EmailWarning.txt in [Customize and translate e-mail messages](#).

Configure NTLM SMTP authentication

To use NT LAN Manager (NTLM) authentication, execute the following steps on the primary and all secondary SafeCom G4 servers:

1. Modify the SafeCom Mail Service property: set **Log on account** to the mail sender user

2. Create the local or domain **SafeComMailSender** group and add the following accounts to it:
 - Mail sender user account
 - SafeCom Service log on account

If the SafeCom Service runs under the Local System account, change the account to `NT AUTHORITY\SYSTEM`.

The SafeCom Service and the mail sender user accounts must be in the same given local or domain group for security reasons. The software checks the group membership and refuses sending email if the verification fails.

3. Restart the SafeCom Mail Service and SafeCom Service.
4. Specify connection settings in SafeCom Administrator, on the **Server properties > E-mail** page:
 - **Port:** 587
 - **Reply e-mail address:** the e-mail address of the mail sender user
 - **Connection security:** STARTTLS
 - **Authentication:** NTLM



- In case of later modification of the settings above, restart the SafeCom Service and SafeCom Mail Service.
- To send e-mails successfully during user import, increasing the message processing rates of the SMTP server may be needed. In case of Exchange Server, run the following command in the Exchange Management Shell to set the rates to unlimited:

```
Get-ReceiveConnector | Set-ReceiveConnector -MessageRateLimit Unlimited
```

For more information, search for *Message rate limits and throttling* in Microsoft documentation.

Configure Microsoft 365 OAuth2 SMTP authentication

To use OAuth2 authentication to connect to the Microsoft mail server, an application must be registered with Azure Active Directory. During the registration select Mobile and desktop applications platform.

For more information, search for *Quickstart: Register an application with the Microsoft identity platform* in Microsoft documentation.

The following steps must be executed on the primary and all secondary SafeCom G4 servers to grant access to the registered application to be able to send e-mails:

1. Specify connection settings in SafeCom Administrator, on the **Server properties > E-mail** page:
 - **SMTP server address:** `smtp.office365.com`
 - **Port:** 587
 - **Reply e-mail address:** the Microsoft 365 e-mail address of the mail sender user
 - **Connection security:** STARTTLS
 - **Authentication:** Microsoft 365 OAuth2
 - **Client ID:** Application (client) ID of the registered application
 - **Tenant ID:** Directory (tenant) ID of the registered application

2. Click on **Authorize...** to authenticate the registered application and get an access token for the mail server.

This opens a login screen in a browser for the mail sender user and ask for permission for the registered application to send e-mails.

i If the mail sender user's password is changed, the registered application needs to be authenticated again.

3. Enable SMTP AUTH on the mail sender user's mailbox.

i For more information, search for *Enable or disable authenticated client SMTP submission (SMTP AUTH)* in *Exchange Online* in Microsoft documentation.

Configure Google OAuth2 SMTP authentication

To use OAuth2 authentication to connect to the Google mail server, an application must be registered with Google Cloud Platform. During the registration enable Gmail API service and create OAuth client ID and select Desktop app application type.

For more information, search for *Enable and disable APIs* and *Setting up OAuth 2.0* in Google documentation, in API Console Help.

The following steps must be executed on the primary and all secondary SafeCom G4 servers to grant access to the registered application to be able to send e-mails:

1. Specify connection settings in SafeCom Administrator, on the **Server properties > E-mail** page:

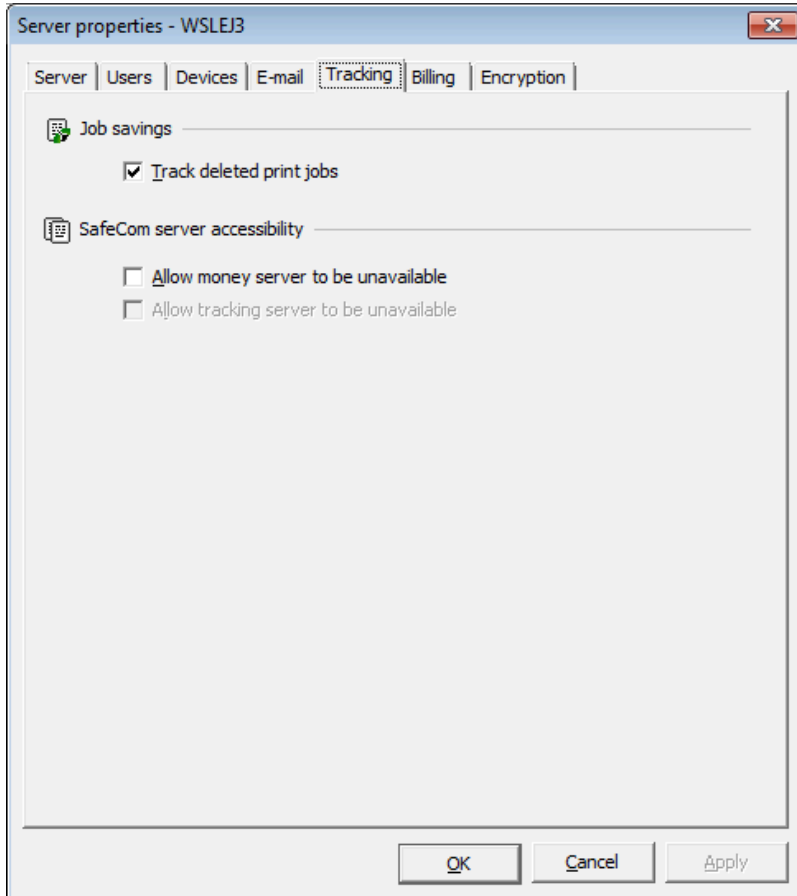
- **SMTP server address:** `smtp.gmail.com`
- **Port:** 587
- **Reply e-mail address:** the Google e-mail address of the mail sender user
- **Connection security:** STARTTLS
- **Authentication:** Google OAuth2
- **Client ID:** Client ID of the registered application
- **Client secret:** Client secret of the registered application

2. Click on **Authorize...** to authenticate the registered application and get an access token for the mail server.

This opens a login screen in a browser for the mail sender user and ask for permission for the registered application to send e-mails.

i If the mail sender user's password is changed, the registered application needs to be authenticated again.

Tracking



Select **Track deleted print jobs** to have the SafeCom solution track deleted jobs and to see the effect in the [Save-O-Meter](#).

Select **Allow money server to be unavailable** if you want Pay users to be able to print and log in to devices even if it is not possible to charge the user for the jobs produced by the user. This setting has no effect without a Pay license.

Select **Allow tracking server to be unavailable** if you want tracking users to be able to print and log in to devices even if it is not possible to track the jobs produced by the user. The tracking server can only be allowed to be unavailable if the money server is allowed to be unavailable. This setting has no effect without a Pay license.

How it works:

- A severity 2 event (error) is created in the SafeCom [event log](#) when the first Pay user logs in while the money server is unavailable. The user is treated as a tracking user. If the tracking server is unavailable, the user is treated as a no cost user.

A severity 5 event (information) is created in the SafeCom [event log](#) when the first user logs in and the servers are available again.

In a multiserver solution, the **Tracking** tab looks different on the primary server (see [Configure SafeCom primary server](#)) and the secondary server (see [Configure SafeCom secondary servers](#)).

Billing

The screenshot shows the 'Server properties - WSLEJ3' dialog box with the 'Billing' tab selected. The dialog has several sections:

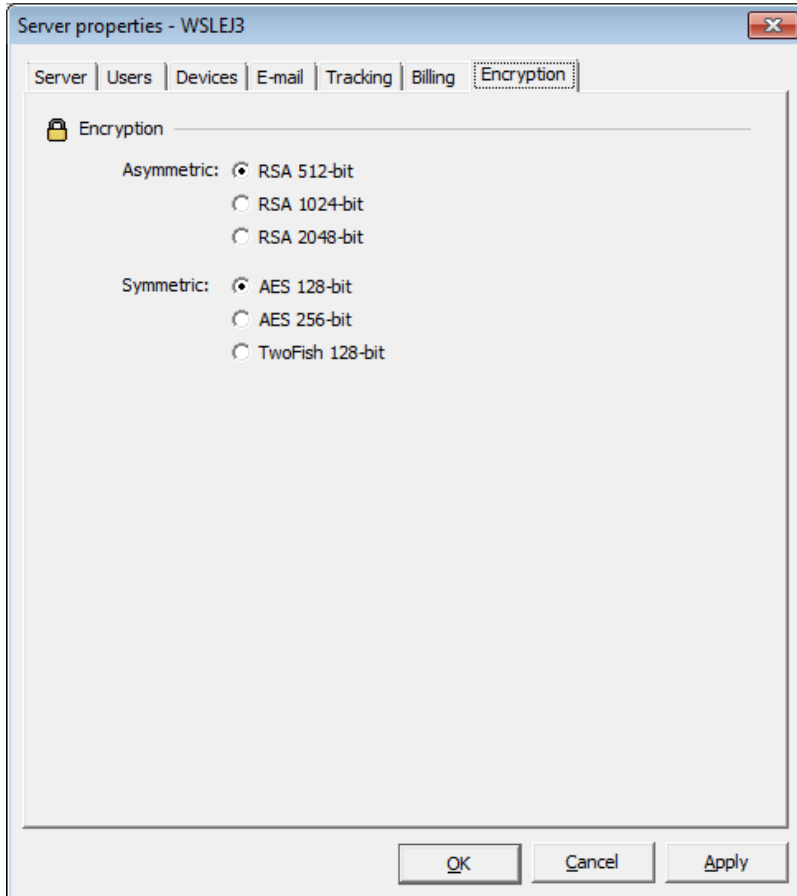
- Billing codes:** Includes a 'Primary code' field with 'Client code' entered, a 'Secondary code' checkbox (unchecked), a 'Display format' dropdown with 'Primary code' selected, and a 'Size' spinner set to '0'.
- Billing window:** Includes a checkbox 'Store tracking data temporarily to allow users commit billing after:' (unchecked), followed by spinners for '0' days, '0' hours, and '0' minutes.
- Commit billing records:** Includes radio buttons for 'Move once at:' (selected) and 'Move every:', with a 'Starting at:' spinner set to '00:00'. To the right, a list of days (Monday through Sunday) is shown with all checkboxes selected.

Buttons for 'OK', 'Cancel', and 'Apply' are at the bottom.

Select **Store tracking data temporarily to allow users to apply billing codes**. State the time to elapse before the billing data is committed and when the billing data should be moved to the tracking data.

See [Configure SafeCom Client Billing](#) for additional information.

Encryption



All control data that is exchanged using the SafeCom protocol is encrypted according to the choice of cipher. This includes login requests with user details, such as user logon, card numbers, PIN codes, and passwords. Other encrypted data include List of documents, tracking data, event log information, and more.

Asymmetric: RSA is used for asymmetric encryption and for the exchange of the symmetric keys. RSA is a very slow encryption algorithm and is not suited to encrypt and decrypt bulk data efficiently. The default is **RSA 512-bit** encryption.

Symmetric: Encryption of bulk data is done using more efficient algorithms, either AES (Rijndael algorithm) or TwoFish, a proposal by NIST (National Institute of Standards and Technology) for an Advanced Encryption Standard. The default is **AES 128-bit** encryption.

Pending documents are always encrypted using 128-bit encryption. Pull print data is always encrypted on the network while traveling to the server. Pull print data traveling to a device is encrypted if:

Encrypt documents is enabled for the user (see [Settings](#)).

Encryption is enabled for the device (see [License](#)).

By default, clients have settings that are adjusted to the encryption method and size that has been specified on the server. Clients include the SafeCom Print Client, SafeCom Pull Port, SafeCom Push Port, SafeCom Administrator, SafeCom Reports, SafeCom Web Interface, and SafeCom Go devices.

The SafeCom Go devices take the processing power and memory of the device into consideration. This means that in most cases, no additional configuration steps are required on the device. Refer to the relevant *SafeCom Go Administrator's Guide* for additional information.

The selected encryption method on the server takes effect once the SafeCom service has been restarted on the server. When a secondary server is added, it by default gets the same encryption settings as the primary server's.

User properties

The **User properties** dialog is accessed from the **Users** menu, the **User** button, and by right-clicking a user in the **Users list**.

The dialog tabs are:

- **Identification**
- **Settings**
- **ID code**
- **Rights**
- **Member of**
- **Aliases**
- **Delegates**
- **Account**
- **Billing**

Identification

The screenshot shows the 'Add User - JOHN_SMITH' dialog box with the following fields and values:

- Domain: <None>
- User logon: JOHN_SMITH
- Full name: John Smit
- Home server: (empty)
- Org. unit: <None>
- E-mail: john_smith@safecom.eu
- Description: (empty)
- Cost code: (empty)
- Home folder: (empty)

Credits section:

- Account 1: 0.00
- Account 2: 300.00
- Low limit: 0.00
- Credits reserved: 0.00


Login section:


- Login without PIN code

Buttons: Create user, Cancel

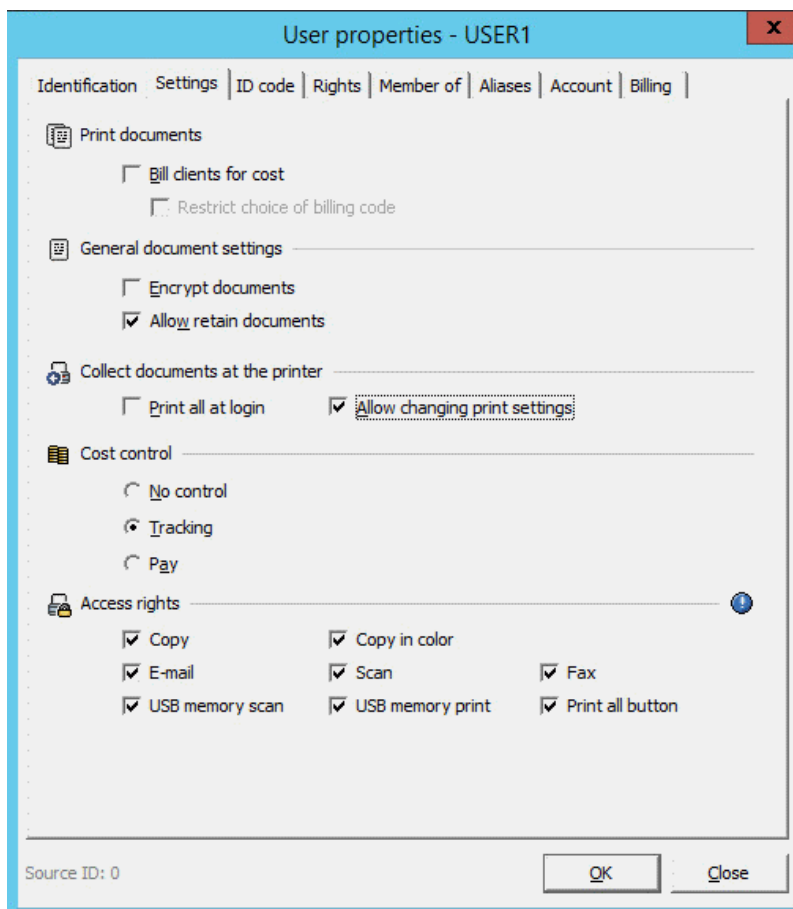
- **Domain:** The domain the user belongs to.
- **User logon:** This is identical to the user's Windows logon. The user logon is mandatory, maximum 20 characters, and must be unique in regards to other user logons, user aliases, and group names. **ID** is the database ID.
- **Full name:** The user's name.
- **Home server:** The SafeCom server the user belongs to. Only present if you have a SafeCom License Key.
- **Org. unit:** The [organizational unit](#) the user belongs to.
- **E-mail:** The user's e-mail address. The SafeCom solution can use the e-mail address to send welcome messages and PUK code messages.
- **Description:** An optional description of the user.
- **Cost code:** The cost code of the user.

- **Home folder:** The personal network folder of the user.

 This option is only available for HP FutureSmart devices. For more information, refer to *SafeCom Go HP Administrator's Guide*.

- **Credits section:** Only relevant if the **Cost control** is set to **Pay** in the **Settings** tab.
- **Logins failed:** The number of consecutive, failed login attempts for the user. Click **Clear** to set the number to zero. If this number reaches the **Max login attempts** specified in the **Users** tab of the **Server properties** dialog, the user is prevented from printing (**Prevent login** is checked).
- **Prevent login:** Checking this makes the user unable to log in at the device. A user that is prevented from printing is indicated with an image  in the **User list**.
- **Login without PIN code:** Check if the user should **not** be required to enter a 4-digit PIN code at the device (restrictions may apply).
- **Source ID:** This indicates from which source the user was imported. A value of zero indicates that the user was manually created.

Settings



For more information about the **Bill clients for cost** setting, see [SafeCom Client Billing](#).

Encrypt documents is only relevant if encryption of documents is possible (see [Printing encrypted documents](#)).

Allow retain documents shows if the user is allowed to keep documents on the server so they can be printed multiple times.

Print all at login shows if all the user's documents should be printed as soon as the user logs in at the device. Documents are printed in chronological order (oldest first).

Allow changing print settings shows if the user can force B/W and Duplex printing on the device. Checking the option displays the relevant Forced Mono-Duplex (FMD) control buttons on the device screen, allowing the users to force monochrome (by pressing **B/W** or **Clear B/W** as appropriate) and/or duplex (by pressing **Duplex** or **Clear Duplex** as appropriate) printing. The setting can be managed for a group of users if the **Property** dialog is open when multiple users are selected from the user list.



- If this setting is applied to the default user correctly, all new users inherit this value of the setting.
- This option requires a Rule-Based Printing (RBP) license.
- This option is only available for HP FutureSmart devices.

For additional information about cost control, see [SafeCom Tracking](#) and [SafeCom Pay](#).


Access rights shows what users are allowed to do at the devices in your print environment. By default, users have access to all device functions.

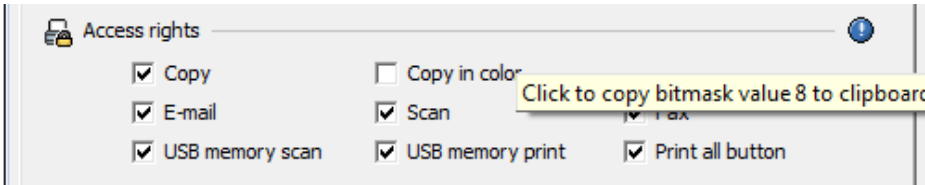
- **Copy**
- **Copy in color**
- **E-mail**
- **Scan**
- **Fax**
- **USB memory scan:** It allows users to scan from a flash memory or mass storage device.
- **USB memory print:** It allows users to print from a flash memory or mass storage device.



USB memory print workflows are tracked and priced as copy workflows.

- **Print all button**

The concept is based on a bitmask. The bitmask can be imported as part of the user import (see [Import users](#)). To see the current value, position the mouse pointer on the blue icon , then click the icon to copy the value to the clipboard.

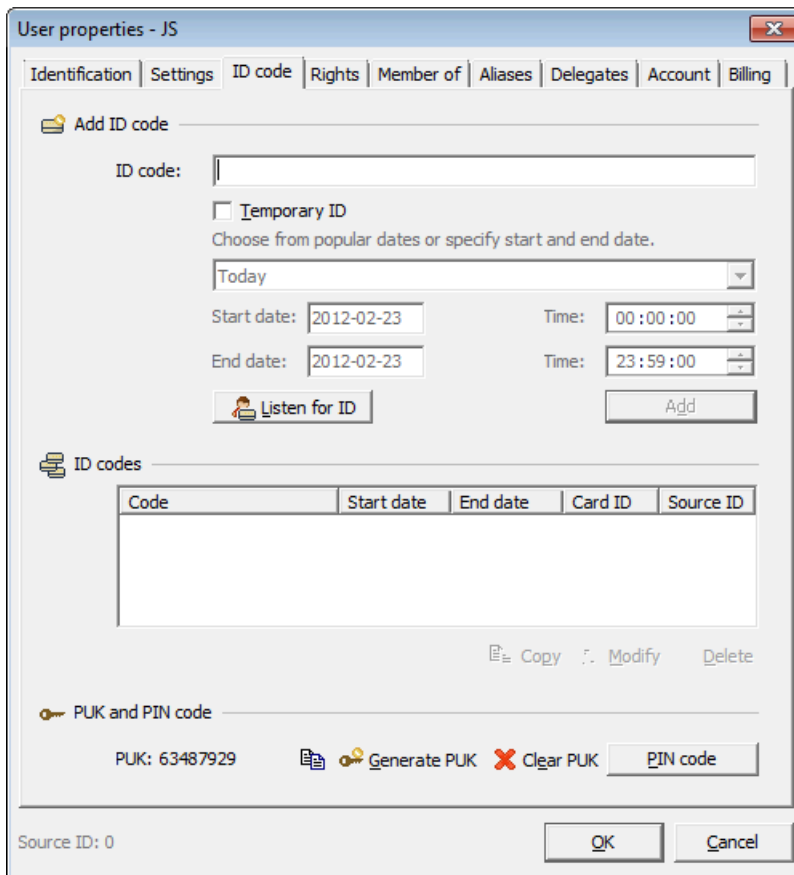


i When importing users, select the **Modify users** check box in the **Rules** step of the user import wizard and run the import twice immediately. This allows users with access rights to all functions to keep their access rights.

In the database, the bitmask is stored as an Integer (32 bits). A bit value of 0 (zero) means that access is allowed. A value of 1 (one) means that access is denied.

i The restrictions are device-dependent.

ID code



By default, there is one ID (card or code) per user. The maximum IDs per user can be specified in the **Users** tab in the **Server properties** dialog (see [Users](#)) of the SafeCom primary server.

1. Enter the **ID code** and click **Add**.

A warning appears when the maximum number of IDs per user is reached.

2. Select **Temporary ID** if the ID code is only to be valid for a restricted period.

Expired IDs are deleted from the SafeCom solution automatically within 10 minutes.

i If **Temporary ID** is checked an e-mail reminder can be set up to be sent to the user specified days before the ID code expires. This way the user is reminded to either generate a new ID code themselves (if the user is allowed) or to make sure a new ID code is generated for them.

3. Select from the popular dates or specify a date.

The following popular dates can be selected:

- **Today**
- **Today and tomorrow**
- **This week** (End date is the upcoming Sunday at midnight)
- **This month** (End date is the last day of the month at midnight)

If you select **Specify dates**, specify the **Start date**, **End date**, and **Time**.

4. Click the calendar icon to open the **Choose date** dialog for easy date selection.
5. Click **Listen for ID** if a card reader is installed on the computer (see [Install a card reader on a computer](#)).




i If you are using Micro Multi-Card Reader, ensure that it is set to **Keyboard emulated** mode. Use the Reader Maintainer tool to set this option.

In **ID codes**, the available codes are listed. **Start date** and **End date** appear only if **Temporary ID** was checked when the ID was added. The **Source ID** indicates from which source the ID was imported. A value of zero indicates that the ID was manually added.

6. Select an ID code and click one of the buttons:

 Copy	 Modify	 Delete
Copy ID code	Modify ID code	Delete ID code

7. In **PUK and PIN code**, use these buttons:

 Copy	 Generate PUK	 Clear PUK
Copy PUK code	Generate PUK code	Clear PUK code

The user can have one PUK code open at a time.

i The PUK code is generated irrespectively if you subsequently click **Cancel** to exit the **User properties** dialog.

The behavior of the **Generate PUK** button depends on the following:

- **Single ID per user** (default): Generating a new PUK code deletes the PIN code and removes any current registration with an ID.
- **Multiple IDs per user**: Generating new PUK codes is possible until the maximum number of IDs has been reached. Otherwise, one of the existing IDs must be deleted before a new PUK code can be generated.

8. Click **PIN code** to open the **PIN code** dialog.

A **PIN code** contains the 4-digit PIN code. If a PIN code is assigned when the dialog is opened, the field contains "****".

9. Click **Random** to assign and display a randomly generated PIN code.

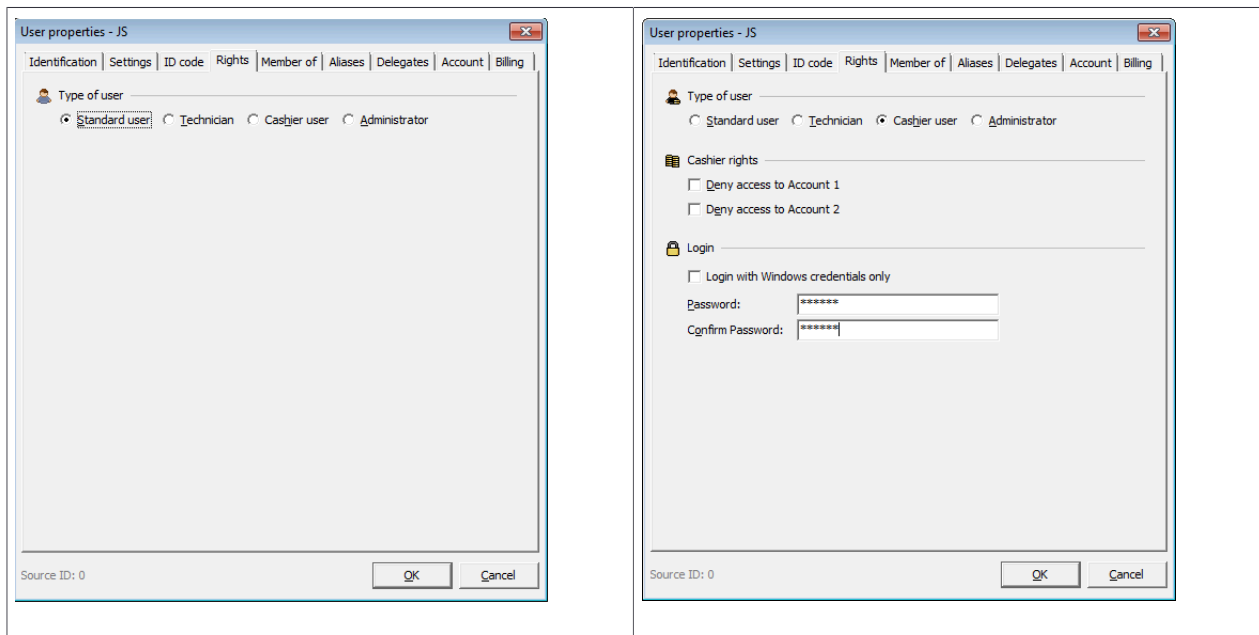
10. Click **Default** to assign and display the default PIN code "1234".

Changing the PIN code automatically clears **Prevent login** and resets **Logins failed** to zero in the **Identification** tab in the **User properties** dialog. The user can have only one PIN code.

If no PIN code is specified, the user is assigned the default PIN code when **OK** is clicked in the **User properties** dialog.

If allowed, the user may subsequently change the PIN code and ID code at the SafeCom G4 Web Interface or at the SafeCom-enabled device (restrictions may apply) (see [Users](#)).

Rights



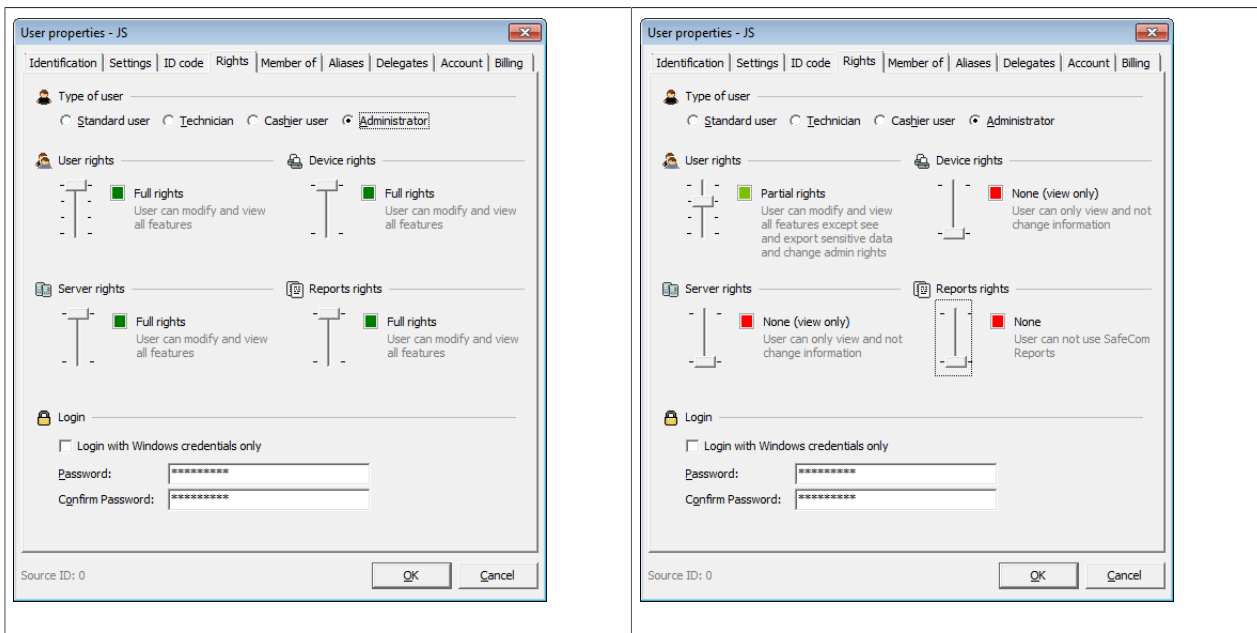
A standard user can have any server as their home server, while users with other rights must have the primary server as their home server.

Selecting technician rights allows users to install SafeCom devices. Devices are operable and can be used for Pull Printing once a user with technician or administrator rights has logged in at the device. In a SafeCom Pay solution, the technician's (or administrator's) **Cost control** setting should be set to **No control** or **Tracking**, because selecting **Pay** prevents the user from registering SafeCom devices.

Selecting **Cashier user** rights (requires SafeCom Pay) allows the user to use SafeCom Administrator in Cashier mode.

When **Administrator**, **Technician**, or **Cashier user** is selected, two additional password fields and a check box to set up login with Windows credentials are displayed in the dialog:

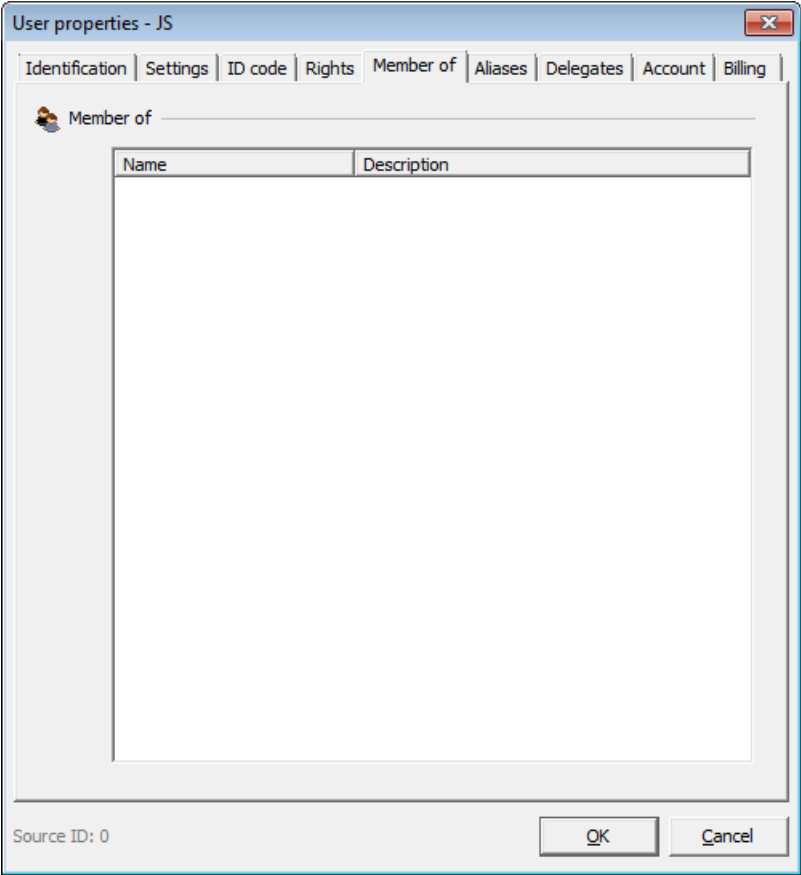
- **Login with Windows credentials only:** Restricts login to Windows credentials only.
- **Password:** Enter a password of your choice to password-protect login or to change your existing password.
- **Confirm Password:** Re-enter the new password.



If you select **Administrator**, the user is given administrator rights, allowing the user to modify users, devices, groups, and the server.

- **User rights Full rights** allows you to add, modify, and delete users. With **Partial rights**, it is possible to do everything except modify user rights and export ID codes and PUK codes. **Limited rights** only allows assigning a new **Code**, **PIN code**, and **PUK code**, as well as clear **Logins failed** and **Prevent login**. It is not possible to add, modify, and delete users. Typically, Help Desk personnel are issued this type of limited administrative rights.
- **Device rights Full rights** allows you to add, modify, and delete devices.
- **Server rights Full rights** allows you to add, modify, and delete servers.
- **Report rights Full rights** allows you to log in to [SafeCom Reports](#).

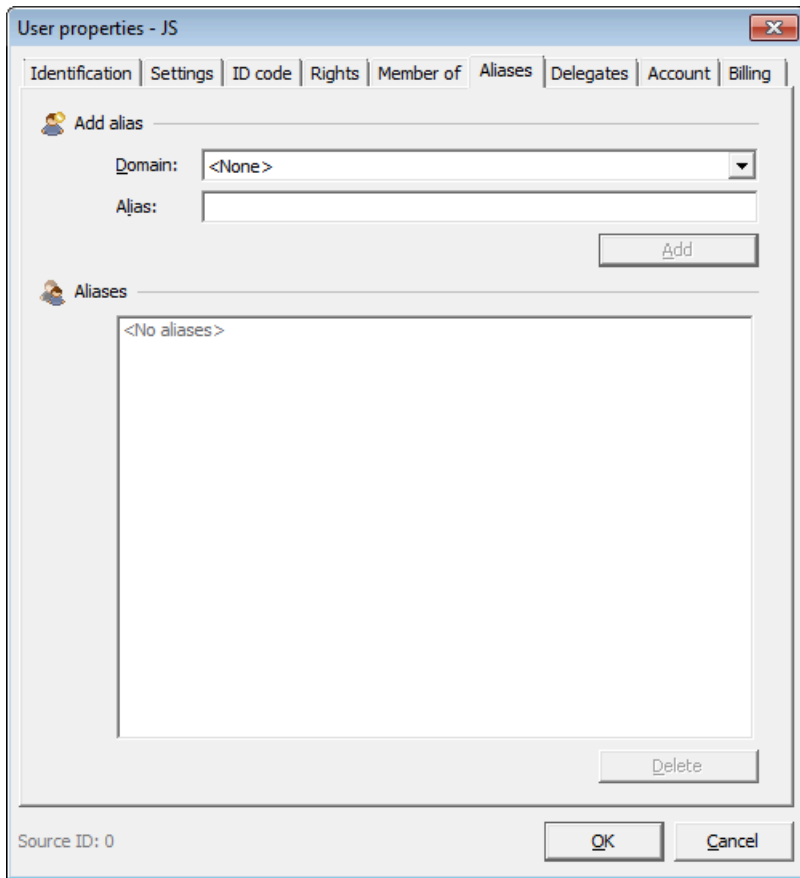
Member of



Member of contains a list of the groups the user belongs to.

Aliases

The SafeCom solution supports printing from multiple client operating systems. Since users often do not use the same user logon for all systems, the SafeCom solution's alias-mapping feature allows users to access their documents from all systems using the same SafeCom account.



To add an alias, enter the **Alias** and click **Add**.

To delete an alias, select the alias and click **Delete**.

The alias must be unique in regards to other user aliases, user logons, and group names. 20 characters is the maximum length of an alias. Any number of aliases can be entered.

In the **Aliases overview** dialog (see [List of aliases](#)), it is possible to see which alias is mapped to which user.

Delegates

With SafeCom Delegate Print, users can grant permission to other users to print or collect print jobs on their behalf. Setup is centrally controlled under **Delegates**, while users themselves can also manage who is allowed to carry out print tasks for them.

i The **Delegates** tab is only visible if **Allow Delegates** is selected in the **Users** tab in the **Server Properties** dialog (see [Users](#)).

Select a user to collect documents on behalf of another user

1. Under **Submit delegated documents to these users**, click **Add**.

If you know the name of the user:

2. In the **Add user** dialog, enter the name in the **Find users** field and click **Find**.
 - a. If SafeCom recognizes the user, the name is listed under **Users**. Select their name in the list and click **Add** to confirm.
 - b. If SafeCom does not recognize the user, you get the "No matches found!" message.

If you are unsure of the user's name or want to select more than one user:

3. Under **Find users**, click **Find**.
4. In the **Confirm** dialog, click **Yes** for SafeCom to retrieve all users listed in the database.
5. In the **Users** list, select the names of the users for delegate print or click **Select all** and **Finish**.
You can select up to 10 delegates.

Select a user who can delegate the collection of their documents to another user

1. Under **Collect delegated documents from these users**, click **Add**.
2. Select users.
You can select up to 10 delegates.
3. For users in the list to always be delegated all submitted documents, select **Always delegate to the listed users**.

With this option enabled, the user who submits documents for delegation does not need to confirm delegation through SafeCom PopUp.


Set a time limit on print delegation


1. Under **Delegates** in the **User Properties** dialog, select the name of the user and click **Modify**.
2. Select **End date**, enter the date when print delegation should end, then click **OK**.
3. If there is a delegate print relationship with a time limit that should be permanent, deselect **End date**.


Users who have a submit/collect relationship in delegate printing always have user properties that correlate. When you change, for example, the expiration date for a user who submits a print job for the other user to collect, the date is automatically updated in the user properties of the other user.

Account

The screenshot shows the 'User properties - JS' dialog box with the 'Account' tab selected. The 'Information' section displays: Full name: John Smith, User logon: JS, PIN code: *****, and Prevent login: Not locked. The 'Account info' section shows: Account 1: 0,00, Account 2: 0,00, Low limit: 0,00 (with an edit icon), and Reserved: 0,00. The 'Disposible' amount is 0,00. The 'Transaction' section has an 'Amount' field with '0', a 'do' dropdown set to 'add amount', and an 'on' dropdown set to 'Account 1'. There is a 'Comment' field and 'Transactions' and 'Record' buttons. At the bottom, there are 'OK' and 'Cancel' buttons, and 'Source ID: 0' is displayed.

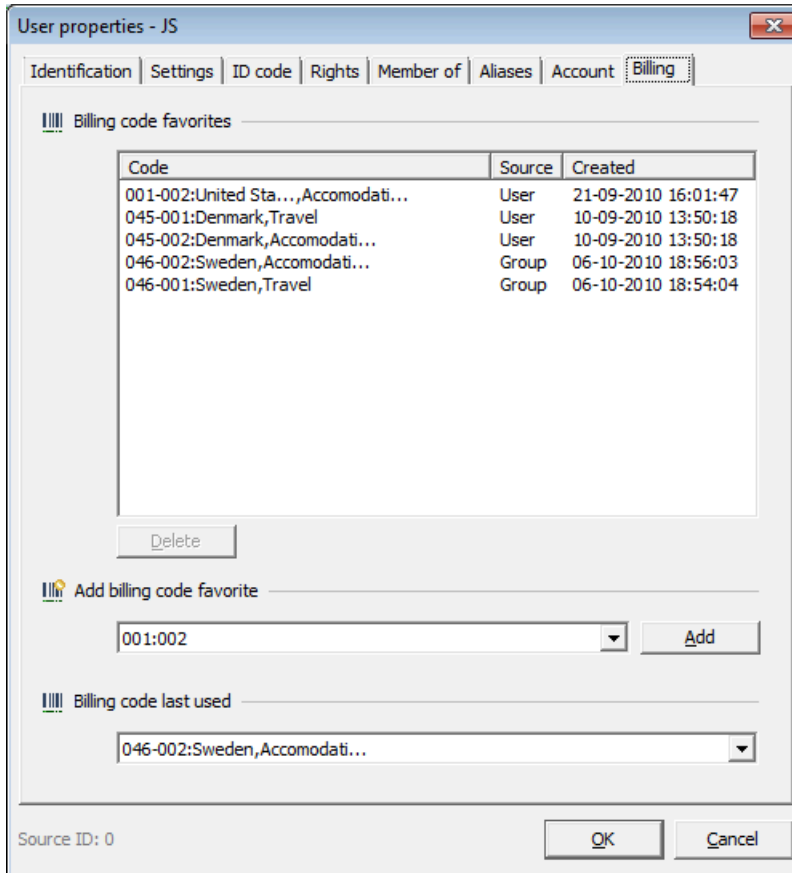
- **Account 1:** Shows the current amount of money available for the user.
- **Account 2:** Shows the current available quota for the user.
- **Low limit:** This is the lowest amount that must be available to print (allows negative figures). Click the icon  to edit the low limit.

 In some cases, the user may not be able to print or copy, even if the account balance exceeds the lower limit by more than the expected printing or copying cost. The user estimate may be lower than the preliminary calculation, which may include not only the price per page, but the job start-up cost also, and considers using at least one color impression. In copy job pre-calculations, the size of the document is not yet known, so SafeCom takes the "Other" paper size into account, which may not have the required balance.

- **Reserved:** This is the amount of credits reserved due to a print or copy job that finished in error. It should be 0.00 (zero) normally. If the system has reserved any credits, you will see a positive amount printed in red. Click the icon  to edit the **Reserved** field. The new amount must be greater than 0.00 (zero) and less than or equal to the currently reserved amount of credits.
- **Disposible:** This amount is equal to **Balance** minus **Low limit** and **Reserved**.

- **Amount:** Type in an amount to add to, subtract from, or set the amount – select the appropriate action from the drop-down list. Select the appropriate account and click **Record** to carry out the transaction.
- **Comment:** Add any description (optional).
- **Transactions:** View a list of user account transactions.

Billing



Click **Add** to add the selected billing code to the **Billing code favorites** list. It will be listed in the **Source** column as "User". The user billing code can be removed from the list by clicking **Delete**. Billing code favorites that are listed in the **Source** column as "Group" are billing codes that are associated to the groups where the user is a member. In this dialog, it is not possible to remove group billing codes from the list. This must be done through the **Billing** menu in the **Group properties** dialog (see [Select favorite billing codes for a group](#)).



- If a Tracking user only has one billing code favorite, then this code is automatically applied to all of his print jobs. To change this, the user should tap the **Account** icon and select **No billing**.
- If a Tracking or Pay user sets **NONE** as his default billing code on the SafeCom Web Interface, any jobs where no billing code is specified in the workflow are billed as **NONE**, and are charged to the user if applicable.
- A user's billing code favorites are replicated to all secondary servers, which means that a user is still able to view and use the favorite billing codes, even if the home server is changed. This does not apply to **Last used** billing codes. (To see what elements are replicated between secondary servers, see [Check that the replication is working.](#))

Device properties

The **Device properties** dialog can be accessed from the **Devices** menu, the **Device** button, and by right-clicking a device in the **Devices** list.

The dialog comprises the tabs: **Settings**, **Charging scheme**, and **License**. Each tab is described subsequently.

Settings

Add Device - NPIEA338A

Settings | Charging scheme | License | Configure

SafeCom Go HP
 Version: MAC: 24be05ea338a
 Serial: CN20D8X0M4

General

Name: NPIEA338A

Model: hp laserjet 700 color mfp m775

Home server: WIN-ECSQK788239

Location:

Device address: 10.144.200.201

Community name: public

IPP enabled:

Printer URI: ipp://10.144.200.201:631/ipp/print

Capabilities

Duplex supported Restricted access

Color supported Push print

Large format print Allow Pay user

Open in browser Add Cancel

ID, specified in the upper right corner, is the device ID that, for example, is used when setting up SafeCom Smart Printer Driver. Refer to *SafeCom Tech Note Smart Printer Driver*, then click the ID to copy it to the clipboard.

Name is a field for specifying a name for the device (mandatory).

Model is a field for specifying the model and/or manufacturer of the device (optional).

Home server is the SafeCom server the device belongs to. Only present if you have a SafeCom Multiserver license key.

Device server is the SafeCom Device Server that the device belongs to.

Community name is the SNMP community name of the device. The default value when adding a device is "public". If the SNMP community name is different, you have to perform additional steps (see [Add device](#)).

IPP enabled 3-state checkbox indicates whether the Internet Printing Protocol can be used to release the print job. IPP and SafeCom high-speed printing must be enabled on the device. If


you have upgraded your server and there were devices registered, the state of this check box is undefined (grayed out). When users use these devices for pull printing, the system first attempts to print through the IPP channel. If the operation is unsuccessful, it uses the normal 9100 printer port. If IPP is not supported or not enabled on the device, a delay may occur before printing can start. It is recommended to manage the checkbox status of such devices to avoid this inconvenience. For more information, see [High Speed Print considerations](#).

Printer URI specifies the URL where the device is receives the print requests. It can be different per device or per vendor. Refer to the device documentation to get the appropriate URL. The default URLs are the following:

- `ipp://[device IP address]/ipp/print`
- `ipps://[device IP address]/ipp/print`

Make sure the correct communication port is used. The default IPP port is 631 and for IPPS it is 443. For some devices, port 631 can be used for both IPP and IPPS. If the default port is supported, the supported URIs are retrieved from the device and the IPPS URI is automatically selected if available.

Make sure that IPP authentication is disabled at the device. The protocol with authentication enabled is not supported.

 If device printer URI port is not the default 631, the corresponding setting is empty in the Device properties dialogue. In this case, the administrator must specify the URI manually.

The list of available printer URIs is automatically queried and populated in the dropdown list. If the device's IPP configuration is customized and the default URI is not enabled, the URIs are not automatically listed. In this case, the administrator must enter the proper URI manually. For example, the default IPP port is 443 in many Canon devices.

Org. unit is the organizational unit the device belongs to (see [Organizational units](#)). Only present if there are any defined organizational units.

Branch is the branch the device belongs to (see [Branches](#)). Only present if there are any defined branches.

Location is a field for indicating the place where the device is physically located (optional).

Device address is the host name or IP address of the device. Click the IP address to copy it to the clipboard.

Capabilities shows a number of check boxes depending on the device and the SafeCom license key code. Select **Duplex supported**, **Color supported**, **Large format print**, **Restricted access**, **Allow Pay user** (only available if the server key license allows one or more Pay devices), and **Push print** if the device supports it.

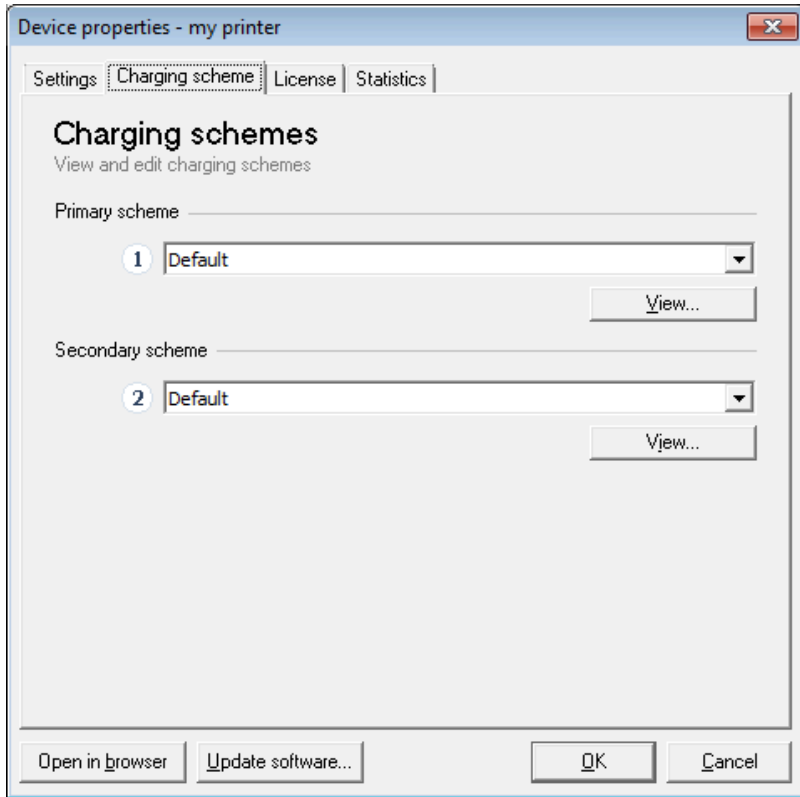
Restricted access can be used to control users' access to the device based on the organizational relationship (see [Organizational units](#)).

Click **Open in browser** if you want to access the device's web interface (see [Open in web browser](#)).

Click **Update software** to update the software of the device (see [Import Ethernet Card Readers](#)).

Charging scheme

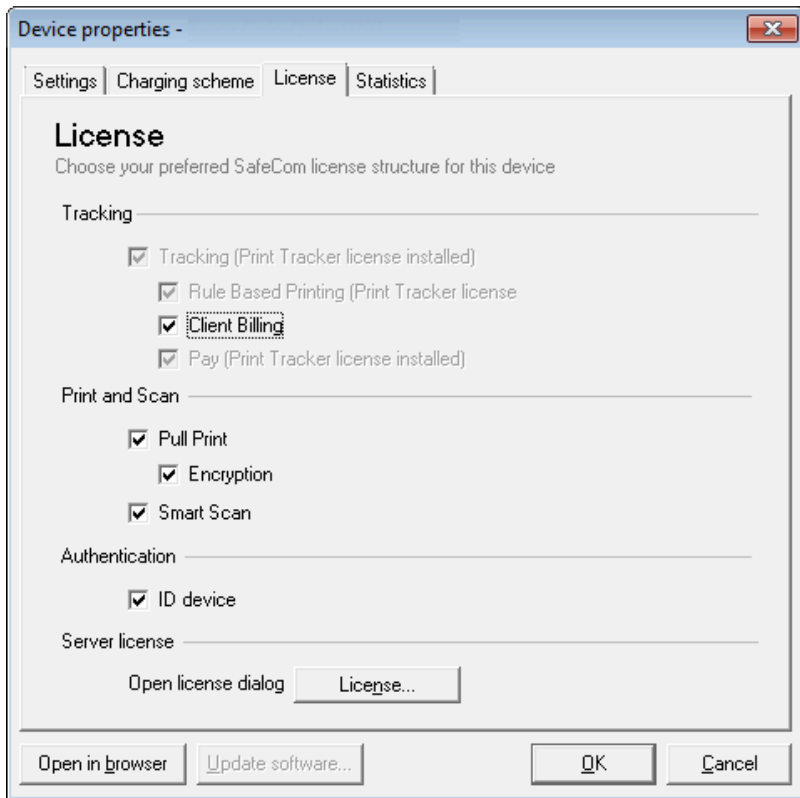
In the **Charging scheme** tab in the **Device properties** dialog, it is possible to select which charging schemes should be used on the device.



Click **View** to see the charging scheme (see [Charging schemes](#)).

License

On the **License** tab in the **Device properties** dialog, it is possible to select which SafeCom features should be enabled on the device in question.

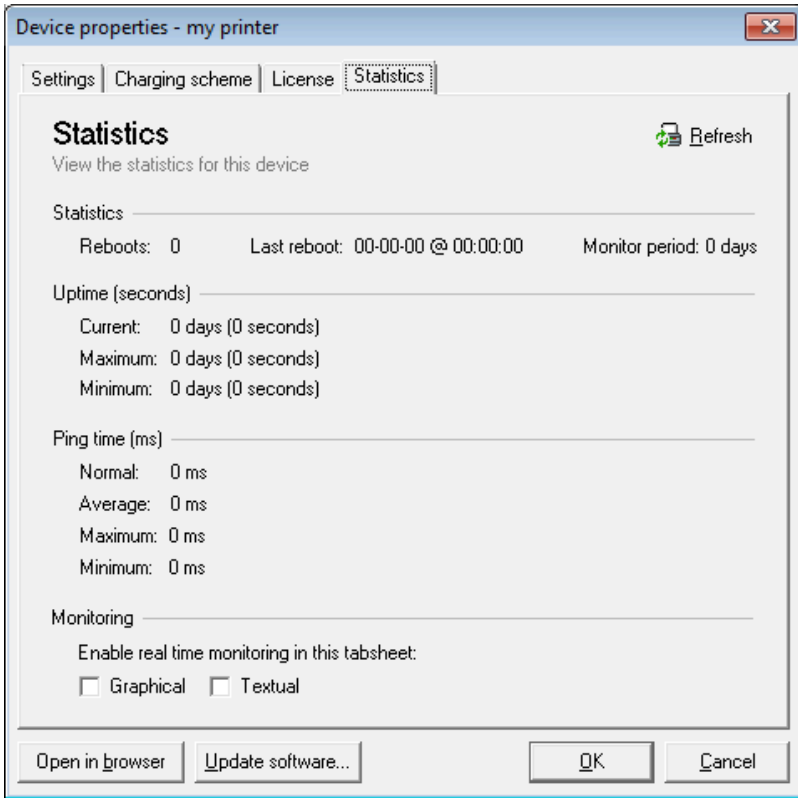


The checked features are only accepted if the license key code allows the device features. Click **License** to open the **License** dialog (see [License](#)) to see if the license key code allows the additional features to be enabled for this device.

i When using an Ethernet card reader, ensure that the ID device option is cleared for the device assigned to the Ethernet card reader, because the Ethernet card reader uses a license by itself.

Statistics

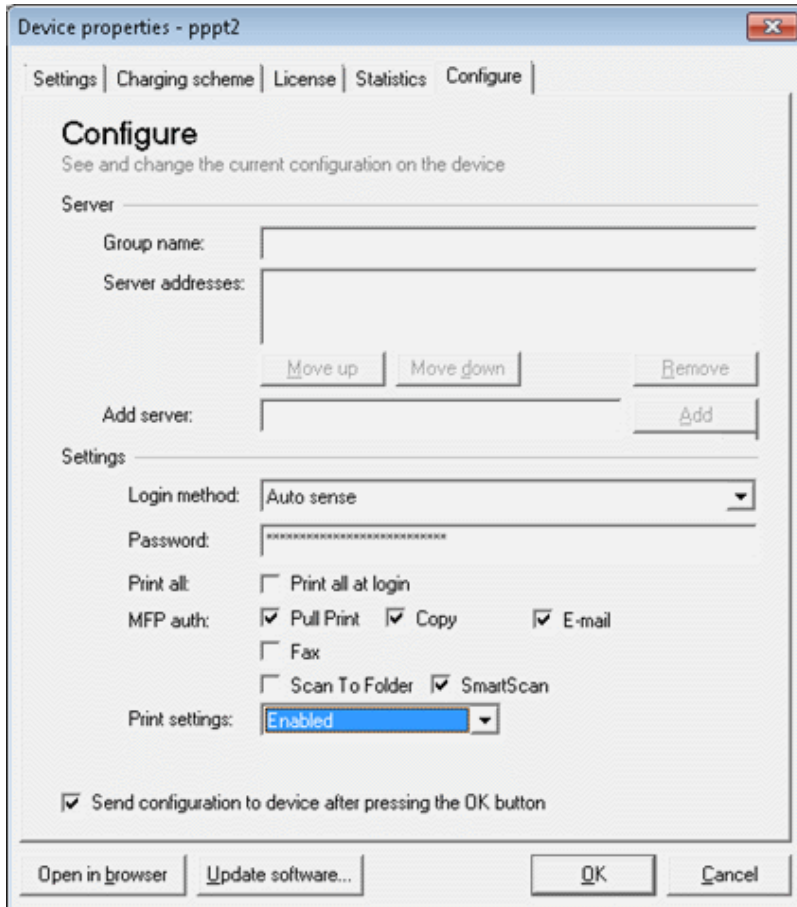
On the **Statistics** tab in the **Device properties** dialog, it is possible to see a textual and graphical representation of the statistics. The **Statistics** tab is not presented if you have opened multiple devices.



How to monitor device status is covered in section [Monitor device](#).

Configure

On the **Configure** tab in the **Device properties** dialog, you can modify settings that are stored with the device. The **Configure** tab is not presented if you have opened multiple devices.



The **Details** section is used to specify the SafeCom server. You can directly enter a **Group name** and the SafeCom server IP address in **Add server**. Use the **Move up** and **Move down** button to prioritize the order in which the servers are contacted in case the first one on the list becomes unavailable.

Login method: Specifies how users must identify themselves to log in to the device.

Print all at login: Check if all the user's documents should be printed as soon as the user logs in. This setting applies to the device. If checked, this overrules the equivalent user property on the SafeCom G4 Server.

MFP auth: The SafeCom product on the device controls access to the selected functions. Additional options may be available on the device's SafeCom Configuration web page.

Print settings: regulates whether users are allowed to control their print jobs. When set to **Enabled**, this control is independent from the user-specific settings. When set to **Disabled**, the device hides the options from all users and the job settings cannot be changed. When set to **User Setting**, the device enables or disables the features according to the currently logged on user's settings.

i 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.

Select **Send configuration to device on OK** if you want to save the configuration changes when you click **OK**.

Click **Open in browser** if you want to access the device's web interface (see [Open in web browser](#)).

Click **Update software** to update the software of the device (see [Import Ethernet Card Readers](#)).

Options dialog

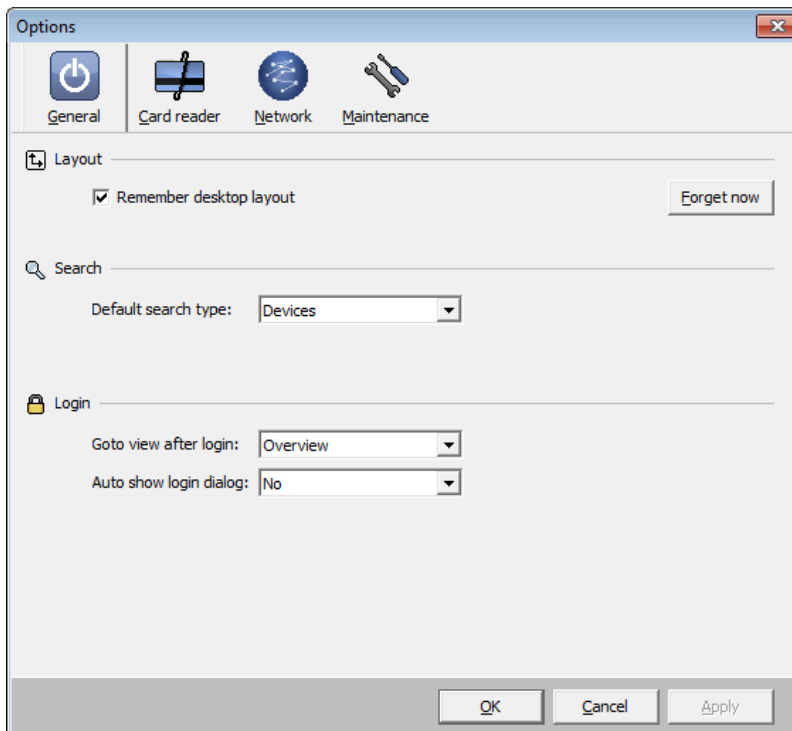
The **Options** dialog can be accessed from the **Actions** menu.

The dialog comprises the tabs: **General**, **Card reader**, **Network**, and **Maintenance**. Each tab is described subsequently.

General

Select **Remember desktop layout** if you want to remember the position and size of the SafeCom Administrator when you exit. The next time you start SafeCom Administrator, it appears as when you exited.

Click **Forget now** to reset the desktop layout.

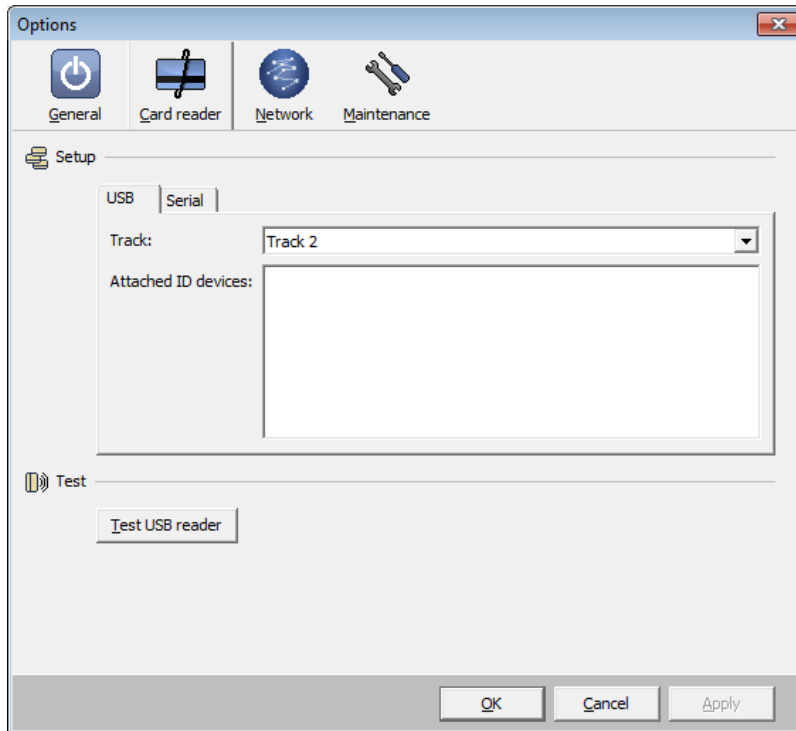


Card reader

[Install a card reader on a computer](#) describes how to connect the card reader.

USB card reader

1. Select **USB** if a USB card reader is connected.
2. Click **Test USB reader** and present the card.



i If you are using Micro Multi-Card Reader, ensure that it is set to **Keyboard emulated** mode. Use the Reader Maintainer tool to set this option.

Serial card reader

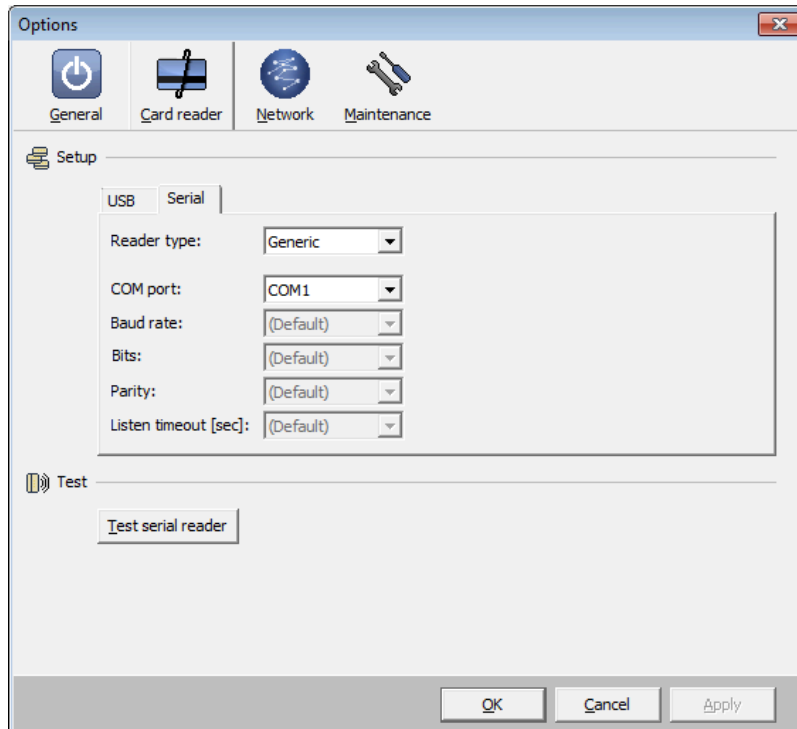
1. Choose a **Reader type** from the list.
 - **None**
 - **Generic**
 - **Magnetic**
 - **Adazzi**
 - **HID Prox**
 - **Legic**
 - **Mifare**

Click **Support** to see the latest list of supported card readers on our web site.

2. Choose a **COM port** from the list.

- **COM1**
- **COM2**
- **COM3**

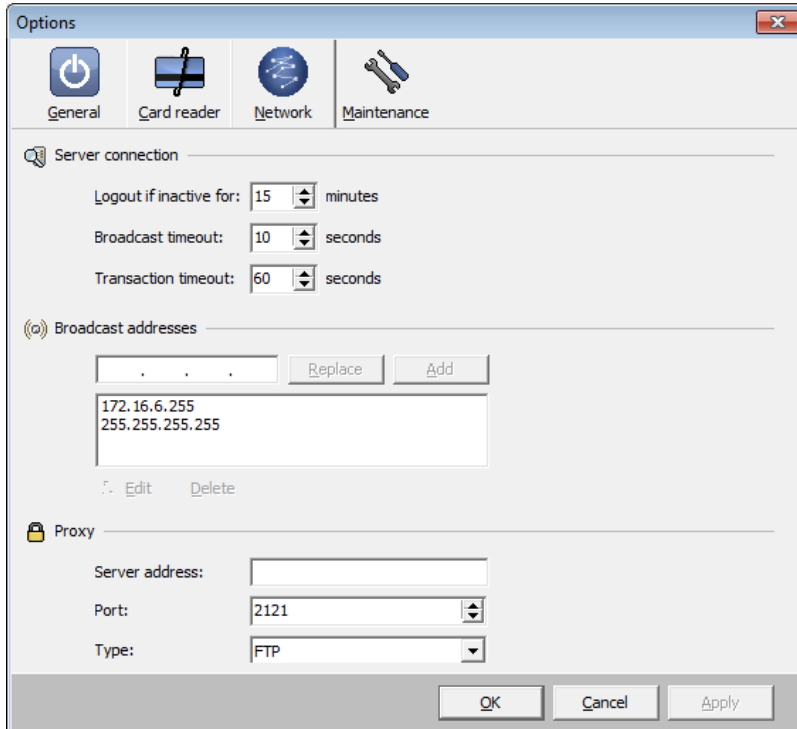
3. Click **Test** and use the card to test if reading is possible. If it fails, you may need to move the card reader to another **COM port**.



If your card reader does not match any of the listed reader types, you should select **Generic** and find the correct combination of **Baud rate** (4800, 9600, 14400, 19200, 28800, 38400), **Bits** (7 or 8), and **Parity** (No, Even, or Odd).

Listen timeout can be 10, 20, 30, 40, 50, or 60 seconds. **Listen timeout** determines the maximum number of seconds that may pass from the moment you click **Listen for ID** on the **ID code** tab in the **Users properties** dialog (see [ID code](#)) until you use the card with the card reader.

Network



In **Logout if inactive for**, you can change the automatic logout time. If no activity has been registered in the SafeCom Administrator for the number of minutes shown, all open connections are closed. The default is 15 minutes and the maximum value is 99 minutes.

Broadcast timeout is the time in seconds the SafeCom Administrator will search for SafeCom servers and devices on the network. Default is 10 seconds.

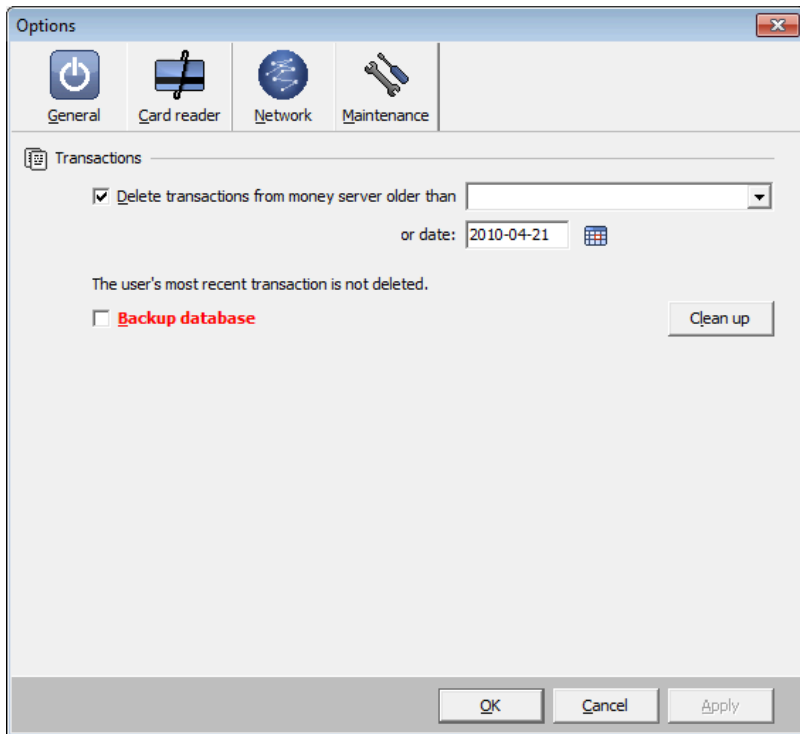
Transaction timeout is the maximum time in seconds the SafeCom Administrator will wait for a SafeCom server to respond. We recommend that this is only increased for large installations with thousands of users. Default is 60 seconds.

Broadcast addresses shows the list of network masks for all TCP/IP networks containing SafeCom servers and devices. You must configure this list correctly for the SafeCom Administrator to be able to locate all SafeCom servers and broadcast for SafeCom devices.

i It is recommended to replace 255.255.255.255 with a list of individual masks, as broadcasting may otherwise not work.

If access to the Internet requires use of a **Proxy**, the **Check for updates** feature cannot connect to the SafeCom Update Server to check for updates of manuals, device software, and release notes. Specify the **IP address**, **Port** (default 2121), and **Type** (default FTP) of connection the proxy server is using.

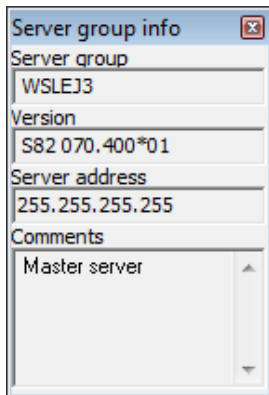
Maintenance



In a Pay solution, you may wish to delete transaction records older than a certain date. Specify the exact date or select a date from the list, which includes the selections: **1 month, 2 months, ..., 11 months, 1 year, 2 years, ..., 5 years**.

Select **Backup database** to have a backup created of the scpurse database before deletion, then click **Clean up**. The user's most recent transaction is not deleted.

Server group info



In the **View** menu, select **View server group info** to display the **Server group info** dialog.

The **Server group info** dialog updates its content whenever you select another server, even if you do not log in to the server. You can anchor the **Server group info** dialog to the bottom of the **Server groups** pane by dragging it to the bottom left corner of the SafeCom Administrator.

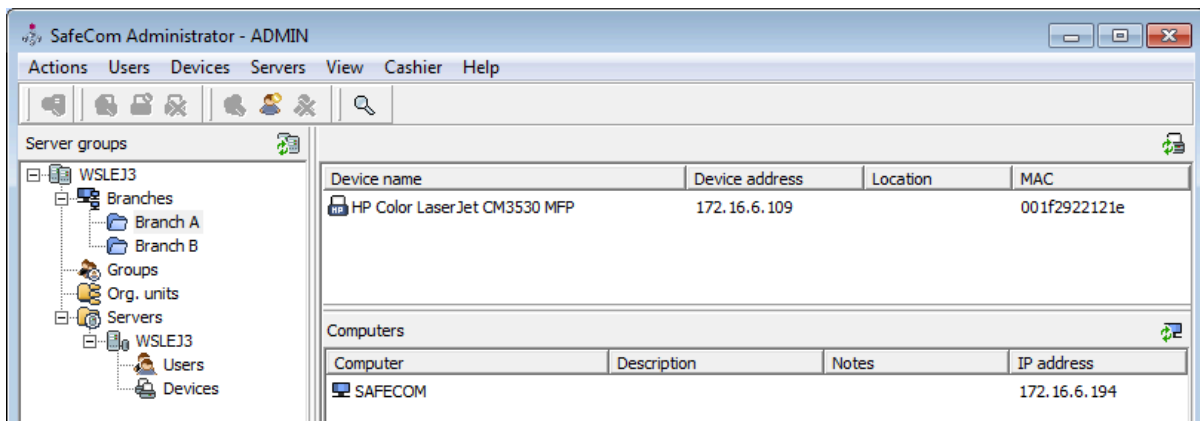
Branches

In SafeCom Administrator, it is possible to define branches and associate devices and computers to these branches. This is used to ensure that devices within the branch allow collection of only those documents that reside on computers that belong to the same branch. The table below reflects when printing is possible.

	Computer belongs to No branch	Computer belongs to Branch A	Computer belongs to Branch B
Device belongs to No branch	Yes	Yes	Yes
Device belongs to Branch A	Yes. Computer is added to Branch A	Yes	No
Device belongs to Branch B	Yes. Computer is added to Branch B	No	Yes

In this context, the term "computer" denotes a computer that is running the SafeCom Client Print software where documents reside on the computer's local hard disk drive, rather than on a SafeCom server.

The maximum number of branches, computers, users, and devices is virtually unlimited, but of course, is subject to the limitations imposed by the size of the database.



1. Click the **Branches** icon in the **Server groups** pane to expand the list of defined branches (in alphabetic order).
Two panes appear to the right. The top pane is the **Devices** pane. The bottom pane is the **Computers** pane.

2. In the **Devices** pane, click **Refresh** to retrieve an updated list from the database of all the devices that have not been added to a branch.
3. Right-click the device and click **Properties** to open the **Device properties** dialog (see [Settings](#)).
4. In the **Computers** pane, click **Refresh** to retrieve an updated list from the database of all the computers that have not been added to a branch.
5. Right-click the computer and click **Properties** to open the **Computer properties** dialog (see [Computer properties](#)).

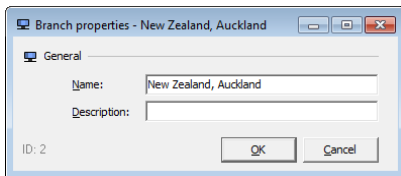
Administrator rights

Within the SafeCom solution, the administrator must have full server rights to modify branches, computers, and the branch property in devices.

Add a branch

Branches can be added in the **Branches** dialog. The **Branches** dialog can be accessed from the **Servers** menu.

1. Click the **Branches** icon in the **Server groups** pane.
2. In the **Servers** menu, click **Branches** and click **Add branch**.
3. Right-click the **Branches** icon in the **Server groups** pane and click **Add Branch**.



4. Enter the **Name** of the branch and an optional **Description**, then click **OK**.
ID is the database ID of the branch.

To associate devices and computers to a branch, you can drag and drop these between the branches. Alternatively, you can select the branch from the **Branch** list in the **Device properties** dialog (see [Device properties](#)) or the **Computer properties** dialog (see [Computer properties](#)).

Delete a branch

Right-click the branch in the **Server groups** pane and click **Delete Branch**.

i A branch can only be deleted if no device or computers reference it.

Add a device to a branch

Perform one of the following steps:

- In the **Devices** pane, select the device and drag it onto the branch in the **Server group** pane.
- In the **Device properties** dialog, select the **Branch**.

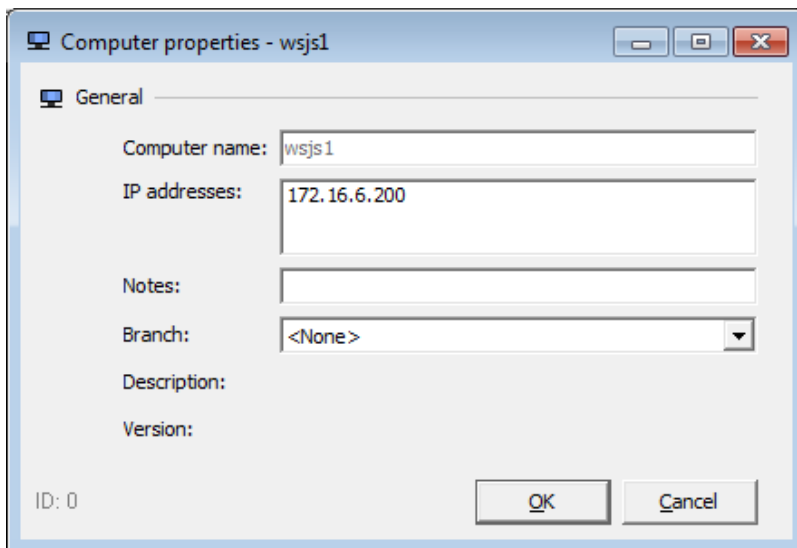
Remove a device from a branch

Perform one of the following steps:

- In the **Branch devices** pane, select the device and drag and drop it onto the **Branches** icon in the **Server group** pane.
- In the **Branch devices** pane, right-click the device and click **Remove device from branch**.
- In the **Device properties** dialog, change **Branch** to "<None>".

Computer properties

Right-click a computer in the **Computers** pane to open the "Computer properties" dialog.



"Computer name" is the hostname (FQDN) of the computer.

"IP address" holds the IP address the computer had the last time it was started.

"Notes" hold optional notes that have been entered by the administrator.

"Branch" is the branch the device belongs to. Only present if there are any defined branches.

"Description" holds the description of the computer.

"Version" is the version of the SafeCom Branch software running on the computer.

"ID" is the database ID of the computer.



- The computer is listed in the SafeCom database by its GUID (globally unique identifier). The "Computer name", "IP address", and "Description" fields are not editable once the computer has been added. These properties are automatically updated when the SafeCom Branch software is started on the computer.
- Tracking data is reported to the Home Server of the user printing. The computer has no Home Server itself.

Add a computer to the SafeCom solution

A computer is, by default, added to the SafeCom solution the first time the installed SafeCom Branch software is started. Information about the computer is stored in the SafeCom Job Database (score) on the SafeCom primary server.

Add a computer to a branch at first print

A computer that has not been added to a branch will have the branch determined at first print. When the first document is pulled from the local hard disk drive of the computer, the computer is added to the same branch as the device pulling the document.

Add a computer to a branch manually

Perform one of the following steps:

- In the **Computers** pane, select the computer and drag and drop it onto the branch in the **Server group** pane.
- In the **Computer properties** dialog, select the **Branch**.

Import computers

Right-click a branch and click **Import computers**.

The imported source file can be in CSV format and can contain the following columns:

- Computer name (mandatory)
- IP address (optional)
- Description (optional)

Remove a computer from a branch

Perform one of the following steps:

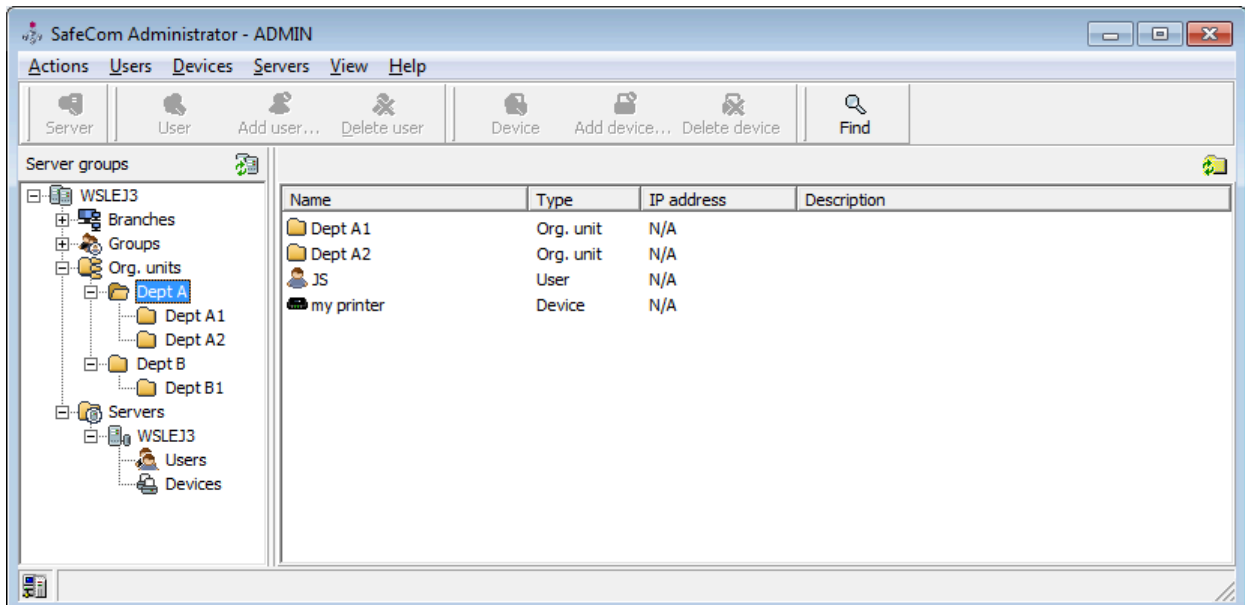
- In the **Computers** pane, select the computer and drag it onto the **Branches** icon in the **Server group** pane.
- In the **Computers** pane, right-click the computer and click **Remove computer from branch**.
- In the **Computer properties** dialog, change **Branch** to "<None>".

Delete a computer from the SafeCom solution

1. Right-click the computer in the **Computers** pane.
2. Click **Delete computer**.

Organizational units

With the concept of organizational units, you can use SafeCom Administrator to visualize the organizational/departmental relations between users, devices, and servers in your SafeCom solution.



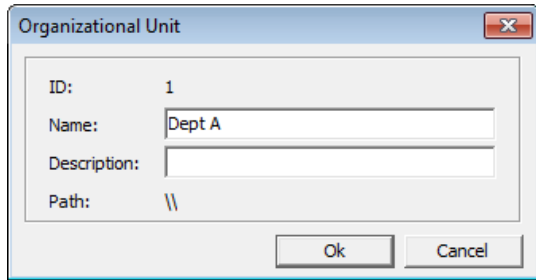
There is a strong resemblance between the organizational unit concept and the folder structure on a computer, and many of the same rules apply. The organizational path can be up to 255 characters long.

The organizational relationship can be used to restrict users' access to devices. See [Devices with restricted access](#).

Add an organizational unit

Organizational units can be added in the **Organization Unit** dialog. The **Organization Unit** dialog can be accessed from the **Servers** menu. To add an organizational unit, perform the following steps.

1. Click the **Org. units** icon in the **Server groups** pane. In the **Servers** menu, click **Organizational units** and click **Add org. unit**.
2. Right-click the **Org. units** icon in the **Server groups** pane and click **Add org. unit**.



3. Enter the **Name** of the organizational unit and an optional **Description**, then click **OK**.

ID is the database ID of the organizational unit. This corresponds to UserNodeID in tracking records.

To associate resources (users, devices, and servers) to an organizational unit, you can drag them between the organizational units. Alternatively, you can select the organizational unit from the **Org. unit** list in the resource's properties dialog.

New users, devices, and servers are always created at the root. The relationship to an organizational unit must be done manually using drag and drop. Users, devices, and servers can be assigned to one and only one organizational unit.

i Restricted access does not work until a device is added to the organizational unit.

Delete an organizational unit

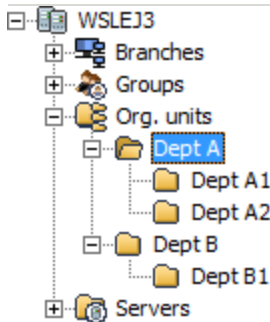
Right-click the organizational unit in the **Server groups** pane and click **Delete org. unit**.

i Organizational units can only be deleted if they are not referenced by any user, device, server, and organizational unit.

Devices with restricted access

The following rules apply to restricted access:

- A device with restricted access can only be used by users who have the device in their organizational path.
- A device without restricted access can be used by any user regardless of the user's and device's organizational path.
- Restricted access does not apply to users with SafeCom Technician or Administrator rights.



- Devices with restricted access in Dept A1 can be used by all users in Dept A1.
- Devices with restricted access in Dept A can be used by all users in Dept A, Dept A1, and Dept A2.
- Devices without restricted access in Dept A1 can be used by all users.
- Devices without restricted access in Dept A can be used by all users.

How it works:

The user cannot log in to the device if "Restricted access" is checked on the "Device properties" dialog (see [Settings](#)) and the device is not part of the user's organizational path.

The user may see the message "Restricted Access" on the device's control panel if a SafeCom Go product is used or on the SafeCom Front-End.

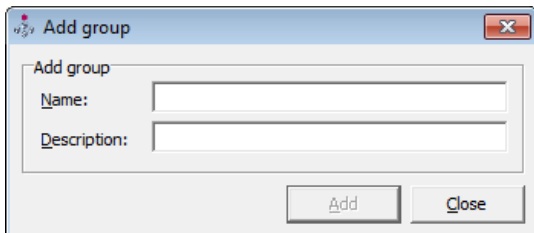
Groups

With the concept of groups, you can use SafeCom Administrator to organize users into groups. Information about groups can be imported from and synchronized with Active Directory (see [Rules](#)). However, it is also possible to manually add groups (see [Add groups manually](#)), delete groups (see [Delete groups](#)), and add members to groups (see [Add members to a group](#)). It is even possible to print to groups (see [Group print](#)).

Add groups manually

Groups can be added in the **Add group** dialog.

1. Click the **Groups**  icon in the **Server groups** pane.
2. In the **Users** menu, click **User groups** and **Add group**.




3. Enter a **Name** and an optional **Description**, then click **Add**.

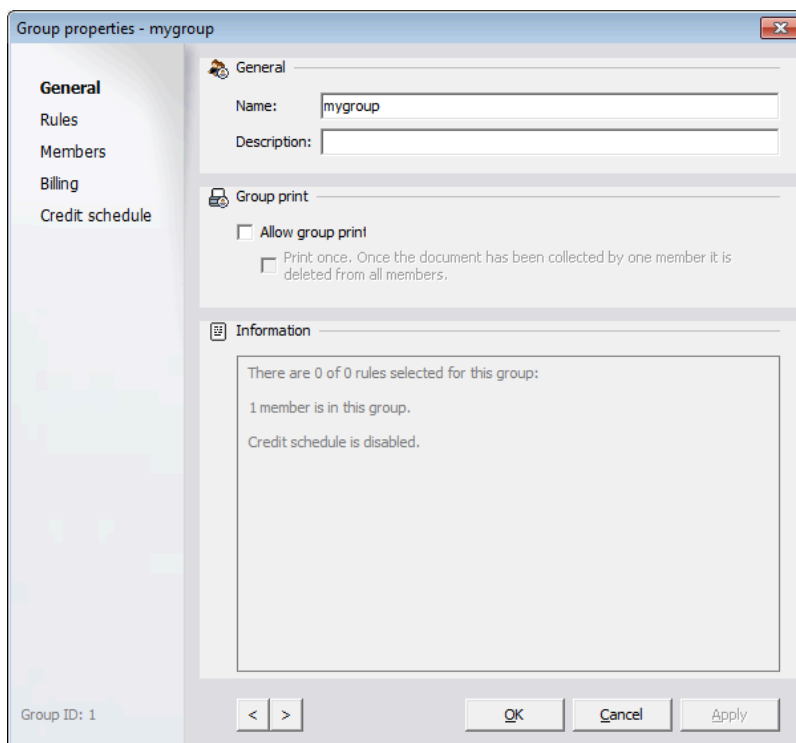
The name must be unique in regards to other groups, user logons, and user aliases.

i The group name cannot be more than 20 characters if group print should be allowed (see [Group properties dialog](#)). Group name cannot contain slash (/) or backslash (\).

4. Click **Close**.

Group properties dialog

1. Click the **Groups**  icon in the **Server groups** pane.
2. Double-click a group in the **Group list** to open the **Group properties** dialog.



The **Group properties** dialog includes these menus:

- **General:** In the **General** menu, you can change the **Name** and **Description** of the group and allow **Group print** (see [Group print](#)).
- **Rules:** In the **Rules** menu, you can select the rules to be used by the group. For additional information about rules, see [SafeCom Rule Based Printing \(RBP\)](#).
- **Members:** In the **Members** menu, you select which users are a member of the group (see [Add members to a group](#)).
- **Credit schedule:** In the **Credit schedule** menu, you can add and subtract credits on a scheduled basis (see [Credit schedule](#)).

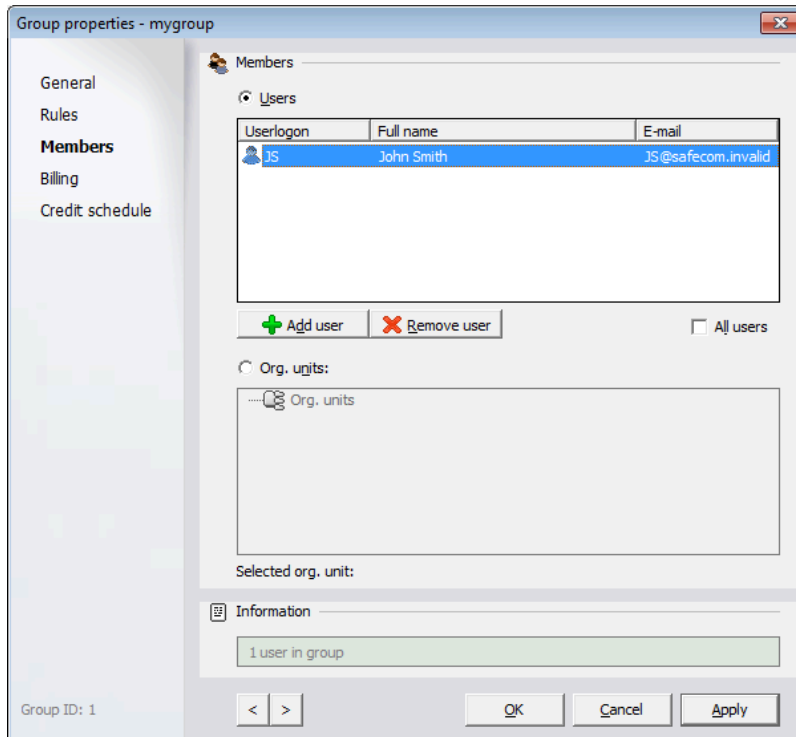
Delete groups

1. In the **Groups** list, select the groups you wish to delete.

2. Perform one of the following steps:
 - Select the group and press the Delete key.
 - Right-click the group and select **Delete group**.

Add members to a group

1. Open the **Group properties** dialog.
2. Click the **Members** menu.



3. Select a method to add users from the following options.
 - [Add users individually](#).
 - [Add users by organizational unit](#).

Add users individually

1. In **Group properties dialog** > **Members menu**, select **Users**.
2. Select **All users** to include all users as members.
3. Click **Add user** to open the **Add user** dialog.
4. Enter your search criteria and click **Find**.
The **Find** button uses field-based, case insensitive, free-text search.
5. Click **Select all** or press and hold Ctrl, then click each user.
6. Select **Differences** to filter away the users who are already member of the group.
7. Click **Add**.
8. Click **Finish** when you are done selecting and adding users to the group.

9. In the **Group properties** dialog, click **Apply** and **OK**.

Add users by organizational unit

In **Group properties dialog** > **Members menu**, select **Org. units**.

Selecting an org. unit also includes the users in the sub units.



- The root Org. unit cannot be selected in the **Members** section.
- Any subsequent import of users and groups (see [Import users](#)) may override your selections.

Remove users from a group

1. Open the **Group properties dialog**.
2. Click the **Members** menu.
3. Press and hold down Ctrl, and click each user.
4. Click **Remove user**.

Select rules to be used in a group

1. Open the **Group properties dialog**.
2. Click the **Rules** menu.
3. Select the rules you want to be used on the group.
4. Click **OK**.

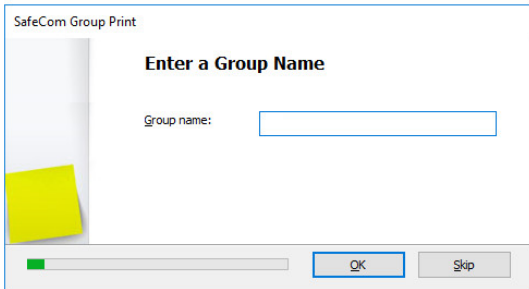
Select favorite billing codes for a group

1. Open the **Group properties dialog**.
2. Click the **Billing** menu.
3. Click **Add** to add the selected billing code to the **Billing code favorites** list.
The group billing code can be removed from the list by clicking **Delete**.
4. Click **OK**.

Group print

By allowing group print for a group, the members of that group can collect the documents sent to the group.

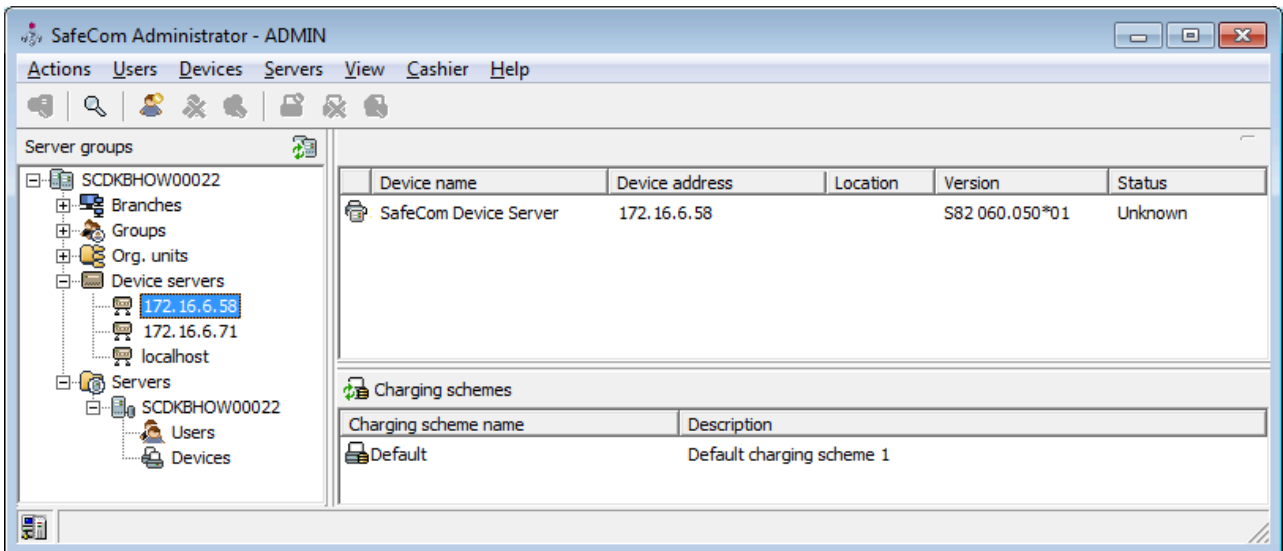
To use group printing, ensure that the **Group Print** window is enabled through the scPopUp settings, then when the screen below is displayed, enter the relevant **Group Name**:




1. Open the **Group properties** dialog.
2. Click the **General** tab.
3. Select **Allow group print**.
4. Select **Print once** to delete the document from all members once one member has collected it.
5. Click **OK**.

Device servers

Under **Device Servers** in SafeCom Administrator, you get a great overview of the SafeCom Device Servers, including the specific devices that are added to each device server.



Furthermore, it is indicated with the icon  next to the device server if the connection to a device server is lost, in which case you benefit from having a quick overview of which devices no longer work as a result of the lost connection.

i If your device fleet includes HP Pro devices, ensure that the HP Pro devices are using a dedicated device server.


The following sections cover how to:

- Add a device server in the SafeCom Administrator (see [Add device server](#))
- View and change the device server properties (see [View device server properties](#))
- Delete a device server (see [Delete device server](#)) or a device server group (see [Delete device server group](#))
- Configure a device server for failover (see [Group device servers](#))

Add device server

To add a device server to SafeCom Administrator:

1. Open a web browser on the device server and log in to the device server.
2. Click **Device Server** on the left pane.
3. Under **SafeCom Servers**, click the **[+]** icon to add a SafeCom server.
4. Enter the server address and click **OK**.
 - a. To add localhost as the server, leave the **Address** field blank and click **OK**.
5. Click **Save**.

If the connection to the device server is down, an icon  is next to the device server and the status is "Down".

Once a device server is added, the devices added to that specific device server (through the Add Device functionality) are automatically added to the device server in the Device Servers menu. To add a new device to the device server, go to [Add a device to a SafeCom Device Server](#).

View device server properties

If the device server has a changed IP address, it can be changed under the **Device server properties**. Furthermore, you can edit the note to the device server if necessary, and if the device server has multiple IP addresses, they are also listed in the device server properties.

To view the device server properties, perform the following steps.

1. Double-click the **Device servers** container in the **Server groups** pane.
2. Right-click the device server and click **Device server properties**.
3. Make the necessary changes to the device server properties.
4. Click **OK**.

Delete device server

To delete a device server, perform the following steps:

1. Right-click the device server.
2. Click **Delete device server**.
3. Click **OK**.

Group device servers

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

1. Open the **Device Server** list.
2. Click **Add device server group**.
3. Enter a **Name** and optionally a **Description** for the device server group.
4. Click **OK**.
5. Drag the device servers to incorporate them into the newly created group.
6. Restart the device servers incorporated to the group.



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

Delete device server group

To delete a device server group, perform the following steps:

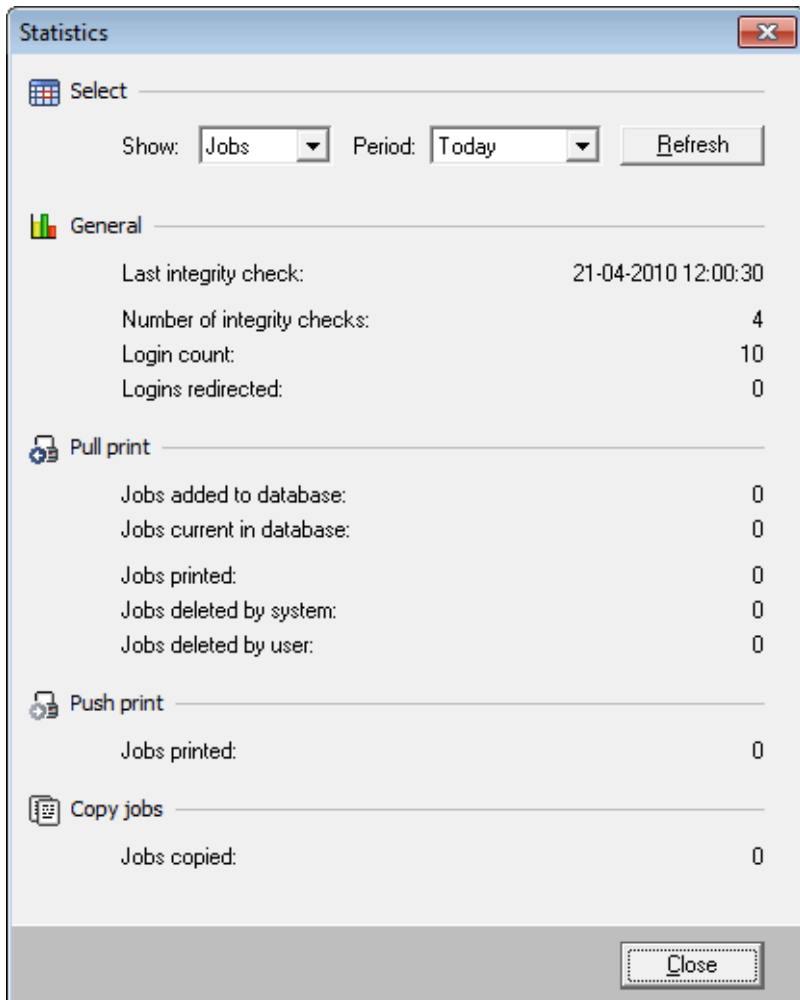
1. Remove all device servers from the group.
2. Right-click the device server group.
3. Click **Delete device server group**.
4. Click **OK**.

Statistics

The SafeCom solution collects statistics every time an integrity check is performed (see [Server](#)). The **Statistics** dialog can be accessed from the **Servers** menu.

The **Statistics** dialog, by default, shows the number of jobs handled today. **Period** can be **Today**, **One week**, or **One month**. **Show** can be **Jobs**, **Pages**, or **Size**. Click **Refresh** to update the statistics.

Jobs that are deleted by users with administrator rights are tracked as **Jobs deleted by system** and not as **Jobs deleted by user**.



Event log

Event log messages are written to the SafeCom event log database, and optionally, to the Windows event log if this is enabled in the **Server properties** dialog (see [Server](#)).

View SafeCom event log

The **Event log** dialog can be accessed from the **Servers** menu by right-clicking a SafeCom server. If your SafeCom solution does not behave the way you expect it to, you should always look at the event log for a possible explanation. In the event log, you can, for example, find information about license issues.

The event log records which user with special rights (Administrator, Technician, or Cashier) logs in and performs such tasks as: adding, modifying, or deleting users, devices, servers, and charging


schemes. These events all get severity 6 (Information) and are **not** forwarded to the administrator by e-mail.

1. Open the **Event log** dialog.
2. Select the period.
A number of predefined periods are available ranging from **Today** to **7 days back**. Choose **Specify period** to freely specify the beginning (from) and finish (to) of the period.
3. Click **Refresh** to view the events for the selected period.
4. Click **Save to file** to save the events as a CSV file with the fields: EventId, UserId, DateTime, Abstract, Module, Severity, and Description.




View SafeCom event messages in Windows event log

If writing events to the Windows event log is enabled (see [Server](#)), it is possible to use the Windows Event Viewer to see these and also to use Microsoft Operations Manager (MOM) to monitor SafeCom event alert messages.

1. Open the Control Panel on the computer where the SafeCom server software is installed.
2. Click **Administrative Tools**, then click **Event Viewer**.
3. Click **SafeCom**.

 Messages are stored on a per server basis (and per node basis in a clustered environment). This implies that Microsoft Operations Manager (MOM) should be set up to monitor all SafeCom servers within the solution and not just the primary server.

The table below describes how SafeCom event log messages are mapped to the Windows event log.

SafeCom field	Windows field	Comment
EventDateTime	Date	Date in dd-mm-yyyy format
	Time	Time in hh:mm:ss format
Severity	Type	 Error - SafeCom Severity 1 and 2  Warning - SafeCom Severity 3 and 4  Information - SafeCom Severity 5 and 6
	Event ID	SafeCom Severity 1 → Windows Event ID 10001 2 → Windows Event ID 10002 3 → Windows Event ID 10003 4 → Windows Event ID 10004 5 → Windows Event ID 10005 6 → Windows Event ID 10006
Abstract / EventSubject	Description	Description of the event
Description / EventText		
Module / CodeModule		

SafeCom field	Windows field	Comment
	Source	Always SafeCom EventLog
	Category	Always None
	User	Always N/A
	Computer	Computer
UserId / CreatorId		N/A
Viewed		N/A
EventId		N/A

Event severity

Events are sorted in six levels on three categories.

- Level 1 and level 2 events are categorized as errors.
- Level 3 and level 4 events are categorized as warnings.
- Level 5 and level 6 events are categorized as information.

Export data

Users who are administrators in the SafeCom solution and have Full user rights can export data about users, devices, and servers in XML or CSV format.

Export users

1. On the **Actions** menu, click **Export**.
2. Select **Users**.
3. Click **Next**.
4. Select **Save as type** and enter **File name**, then click **Save**.
5. Click **Close**.

i When exporting to a CSV file, only the first AliasName, CardNo, and GroupID are exported for each user. When exporting to an XML file all Aliases, Cards, and Groups with additional details are exported.

The XML tags are covered in the tables below. The CSV column header is the same as the XML tag.

Parameter	Description
UserID	Database ID of the user
UserLogon	Logon name
FullName	Full name
HomeServer	Home server

Parameter	Description
EMail	E-mail address
Description	Description
UserNodeID	Database ID of the organizational unit the user belongs to
CostCode	Cost code
LoginsFailed	Number of failed login attempts
UserLocked	Prevent login. Values: Yes No
AvoidPINCode	Login without PIN code. Values: Yes No
AllowRetainDocuments	Allow retain documents. Values: Yes No
EnableBillingDialog	Bill client for costs. Values: Yes No Yes_Restrict
PrintAll	Print all at login. Values: Yes No
AccountingModel	Cost control. Values: NONE PRINT_AND_PAY PAY_AND_PRINT
PUKCode	PUK code

Parameter	Description
GroupID	Database ID of the group
GroupName	Group name
GroupDescription	Group description

Parameter	Description
CardID	Database ID of the card
CardNo	Card number
SourceID	Source ID of the card
TemporaryCard	Temporary card. Values: Yes No
StartDate	Start date, yyyy-mm-dd
StartTime	Start time, hh:mm:ss
EndDate	End date, yyyy-mm-dd
EndTime	End time, hh:mm:ss

Parameter	Description
AliasID	Database ID of the alias
AliasName	Alias name

Export servers

1. In the **Actions** menu, click **Export**.
2. Select **Servers**.
3. Click **Next**.

4. Select **Save as type** and enter **File name**, then click **Save**.
5. Click **Close**.

The XML tags are covered in the table below. The CSV column header is the same as the XML tag.

Parameter	Description
ServerID	Database ID of the server
ComputerName	Computer name
IPAddress	IP address
MasterServer	Primary server. Values: Yes No

Export devices

1. In the **Actions** menu, click **Export**.
2. Select **Devices**.
3. Click **Next**.
4. Select **Save as type** and enter **File name**, then click **Save**.
5. Click **Close**.

The XML tags are covered in the table below. The CSV column header is the same as the XML tag.

Parameter	Description
DeviceID	Database ID of the device
Name	Device name
Model	Device model
Type	Device type. Values: SafeCom Controller SafeCom Go {vendor} SafeCom P:Go {vendor} SafeCom Go High-end HP
Version	Version
HomeServer	Home server
Location	Location
IPAddress	IP address
DuplexSupport	Duplex support. Values: Yes No
RestrictedAccess	Restricted access. Values: Yes No
ColorSupport	Color support. Values: Yes No
PushPrint	Push print. Values: Yes No
PullPrint	Pull print. Values: Yes No
LicenseTracking	Tracking license. Values: Yes No
LicenseClientBilling	Client Billing license. Values: Yes No
LicenseRuleBasedPrinting	Rule Based Printing license. Values: Yes No
LicensePay	Pay license. Values: Yes No
LicensePullPrint	Pull Print license. Values: Yes No

Parameter	Description
LicenseEncryption	Encryption license. Values: Yes No
DeviceMac	MAC address
ChargingSchemeID	Database ID of charging scheme
ChargingSchemeType	Type of charging scheme. Values: Primary (1) Secondary (2)
ChargingSchemeName	Charging scheme name
ChargingSchemeDescription	Description of charging scheme

Export billing codes

1. In the **Actions** menu, click **Export**.
2. Select **Billing codes**.
3. Click **Next**.
4. Select **Save as type** and enter **File name**, then click **Save**.
5. Click **Close**.

The XML tags are covered in the table below. The CSV column header is the same as the XML tag.

Parameter	Description
BillingCodeID	Database ID of the billing code.
BillingCode	The billing code.
BillingDescription	The description of the billing code.
Level	Level 1 is for primary code and 2 is for secondary code.
SourceID	Source ID of the combined billing code.
Billable	The value is 1 if the billing code is billable and 0 if it is not billable.

Export 2-level billing codes

1. In the **Actions** menu, click **Export**.
2. Select **Billing, primary and secondary codes**.
3. Click **Next**.
4. Select **Save as type** and enter **File name**, then click **Save**.
5. Click **Close**.

The XML tags are covered in the table below. The CSV column header is the same as the XML tag.

Parameter	Description
CombCodeID	Database ID of the combined billing code
BillingCodeID1	Database ID of the primary code
BillingCodeID2	Database ID of the secondary code
PrimaryBillingCode	The primary code

Parameter	Description
PrimaryBillingDescription	The description of the primary code
SecondaryBillingCode	The secondary code
SecondaryBillingDescription	The description of the secondary code
SourceID	Source ID of the billing code
Billable	The value is 1 if the billing code is billable and 0 if it is not billable







Chapter 5

Manage servers

SafeCom servers can be organized into two types of server groups in the SafeCom Administrator.

- **Single server group:** This is a group consisting of only a primary server.
- **Multiserver group:** This is a group with multiple servers – one primary server and one or more secondary servers. This requires SafeCom multiserver support.

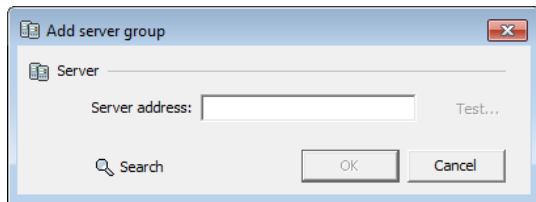
Below, the different icons for server groups and servers in the SafeCom Administrator are listed.

	Server group
	Primary server
	Secondary server
	Offline server
	Unsupported server group (old version)
	Server group is unavailable (unable to connect)

Add a single server group

To add single server groups in the SafeCom Administrator, perform the following steps.

1. Open and log in to the SafeCom Administrator.
2. Click the **Actions** menu, browse to **Server group**, and then click **Add server group**.
You can also right-click in the **Server groups** pane and then select **Add server group**.



3. Specify the **Server address** of the SafeCom server you want to have as primary server. If you do not know the name of the server, click **Search** to search for the appropriate primary server.
4. Click **Test** to verify that you can connect to the server.
5. When the green play button appears the server is running properly and you can click **Close**.
6. Click **OK** to add server group.

The new single server group is now available in the **Server groups** pane in the **SafeCom Administrator**. To log in, double-click the server group and enter login credentials.

Create a multiserver group

To create a multiserver group, you need to have SafeCom installed on at least two different servers (see [Multiserver installation](#)). One server is the primary and another one is to be added to the primary server and turned into the secondary server in the multiserver group.

i The installed SafeCom G4 version must be the same for all servers.

Prerequisites

- i**
- Before creating a Multiserver group, make sure to go through the prerequisites in [Multiserver installation](#).
 - Create a back-up of the primary server in case restoration is necessary.

Add server

i When you add a server to a primary server group, secondary servers lose their existing data including devices, users, and print jobs.

1. In the SafeCom Administrator, log in to the primary server.
2. Browse to the **Servers** container in the left menu, right-click it, then click **Add server**.
3. Enter the server address of the secondary server (IP address or hostname).
4. Clear **Setup replication** if replication is not necessary.
5. Click **Next**, then wait a few minutes.

The server is added successfully when a green check mark appears next to **Server added**.

6. Once the server is added, select **Open Server properties after wizard is completed** if needed.
7. Click **Finish**.



- If you want to add the secondary server immediately after deleting it, you may have to restart SafeCom Administrator before you can add the same secondary server.
- If you are using an external SQL server, the newly-added secondary server may display a yellow triangle to show the ongoing replication process. This icon is removed once the replication finishes running. If the triangle vanishes from the list view but is still present in the tree view, restart SafeCom Administrator.
- If the SQL Server of the primary SafeCom server is in an availability group, the workflow described above changes. The Add Server Wizard prompts for the password of distributor_admin to set up the replication. See *Kofax SafeCom G4 Server SQL Always On Support Guide* for more details.

Troubleshooting

If the attempt to create a multiserver fails, review the list of prerequisites in [Multiserver installation](#). For troubleshooting tips, go through the lists below.

On the primary server:

- Check that publication and subscription are set up. See [Check that the replication is working](#).
- Reinitialize the subscription (see [Reinitialize the subscription](#)) or repair the replication from SafeCom Administrator (see [Repair replication](#)).
- Use the SQL management studio tool for troubleshooting the SQL.

On the secondary server:

- If the secondary server does not start up, enable SafeCom Trace to view the job server trace log file.
- Restart the SafeCom service on the secondary server.
- Restart the SQL service (SafeComExpress) on the secondary server.
- Toggle online/offline tracking on the secondary server.

Fixes:

- If there is no backup, the primary server may be fixed by removing excess rows from the SafeCom Database table: SCServerInfo, SCServerSettings.

Remove single or multiserver group

Perform one of the following steps:

1. Select the server group that must be deleted in the **Server groups** pane, then click the **Actions** menu, browse to **Server group**, and click **Remove server group**.
2. Right-click the server group in the **Server groups** pane and select **Remove server group**.

Removing a server group only prevents it from appearing in the **Server groups** pane. It is not deleted.

Delete a secondary server from a multiserver group

If the server group contains multiple servers, you can delete any of the non-primary servers by performing the following steps:

1. Make sure the prerequisites are met:
 - You must be logged in to the server group to delete a server.
 - **Secondary server must be running:** The secondary server must be running during deletion, otherwise, its reference to the primary server cannot be removed from its database.
 - **No users must have the server as home server:** Verify this in SafeCom Administrator by clicking on the server in question and verify that the **Users** folder is empty.
 - **No devices must have the server as home server:** Verify this in SafeCom Administrator by clicking on the server in question and verify that the **Devices** folder is empty.
2. In the **Servers** menu, click **Delete server**.

i All Windows print queues that use a SafeCom Pull Port to connect to the deleted server will stop working until they are configured to use another server in the group.

To remove the SafeCom server software from the deleted server, you must log in to the server and uninstall the SafeCom software (see [Uninstall SafeCom software](#)).

Failover servers

In a SafeCom multiserver solution, additional resilience can be achieved by specifying a prioritized list of servers that users should be moved to if their home server becomes unavailable. The home server is where the user's documents remain until they are either collected or deleted.

i If the **Store Doc on First Server** option is enabled, the user's documents are stored on the first server the Pull Port print queue contacts.

The user's home server will automatically be reset to the original once the original home server is available again. To avoid excess network load, pending documents are not moved when the user's home server changes. Therefore, users may have to submit their documents for printing again.


At the end of the [Servers](#) section, there is a table that can be used to plan how servers should failover.

How it works:

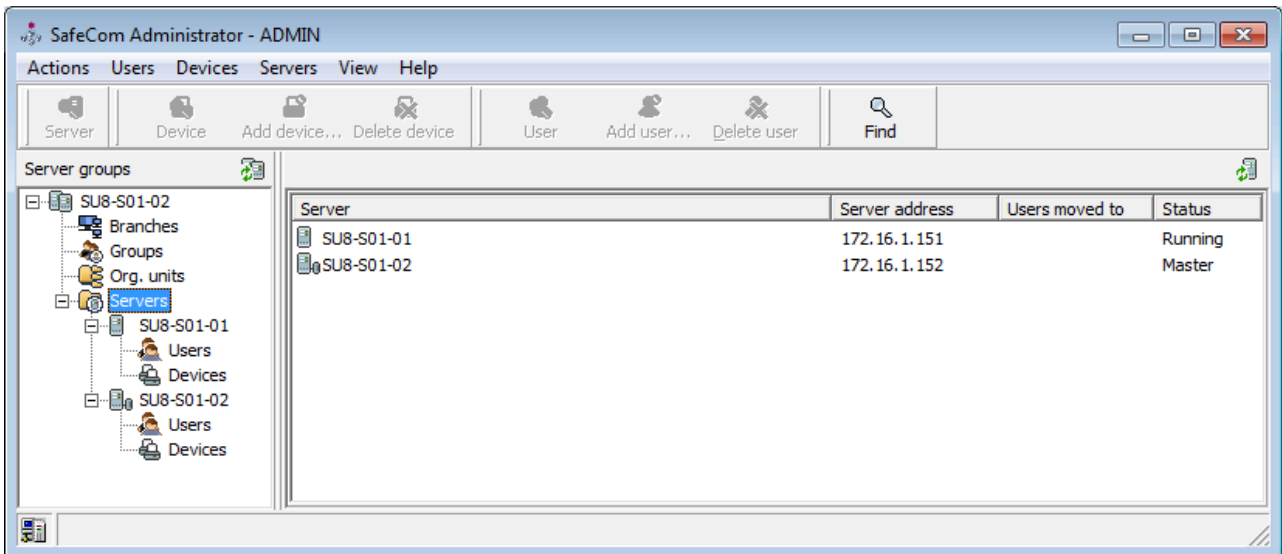
- When a server goes down, the failover process is initiated after approx. 2 minutes and the users' home server reference is changed to the failover server with the highest priority. The change sets in on the affected secondary servers as soon as the changed home server reference has

been replicated from the SQL primary server to the databases used by the secondary servers. The failover triggers a severity 2 event (error) in the [SafeCom event log](#). The event includes the name of the server that went down and the name of the failover server.

- When the server comes back, the users that originally belonged to it are moved back. The fallback triggers a severity 5 event (information) in the [SafeCom event log](#). The event includes the name of the server that came back up and the name of the failover server that temporarily acted as the home server.

The status of servers can be viewed by clicking the **Servers**  icon in the **Server groups** pane.

Status can be Running, Down, or Master.



The [TELNET interface](#) can also be used to view the status of the servers. Once logged in, use the TELNET command: "server info". Below is an example of the server status.

```
ServerId ComputerName Ip Status UserMovedTo
1 SafeCom4 172.16.6.164 MASTER -
2 SafeCom5 172.16.6.165 UP -
3 SafeCom6 172.16.6.166 DOWN 4
4 SafeCom7 172.16.6.167 UP -
```

In the above example, the secondary server SafeCom6 is unavailable and all the users have been moved to SafeCom7 (ID 4).

Set up user replication on failover servers

1. Make sure the prerequisites are met:
 - The SafeCom primary server and the SQL primary server are available.
 - Users with special rights are not moved as they always have the SafeCom primary server as their home server.
2. Open the **Server properties** dialog.
3. Click on the **Failover** tab (only available on secondary servers).

4. Select a server and use the left arrow and right arrow buttons to add and remove server to and from the list of failover servers.
5. Use the up arrow and down arrow buttons on control the priority of the failover servers.
The primary server will always have lowest priority.
6. Click **Apply** to accept the changes.


Chapter 6

Manage users

User management was introduced in section [User creation and management](#), and the interface dialogs described in chapter [SafeCom Administrator](#). This chapter covers how to manage users in more detail.

Default user

When you define a default user, new users inherit default user properties. Typically, one default user resides on the SafeCom primary server.

 For ease of use, we recommend using the logon: "DEFAULT".

User properties inherited from the default user

Tab	User Property	Factory default
Identification	Low limit	0,00
	Login without PIN code	No
Settings	Print documents	
	Bill clients for cost	No
	Restrict choice of billing code	No
	General document settings	
	Encrypt documents	No
	Allow retain documents	Yes
	Collect documents at the printer	
	Print all at login	No
	Cost control	
	No control	Yes – if no license key
	Tracking	Yes – if part of license key
	Pay	Yes – if part of license key
	Access Rights	
	Copy	Yes
	E-mail	Yes

Tab	User Property	Factory default
	USB memory scan	Yes
	Copy in color	Yes
	Scan	Yes
	USB memory print	Yes
	Fax	Yes
	Print all button	Yes

The **Prevent login** functionality and the account credit balance are not inherited from the default user.

User properties inherited from other sources

Tab	User Property	Factory default
Identification	Initial account 2	0,00
ID code	PIN code	1234
Rights	Standard user	Standard user

Initial Account 2 is specified on the **Users** tab in the **Server properties** dialog (see [Users](#)). This setting is only relevant if **Cost control** is set to "Pay".

In a multiserver solution, there can be one default user per server. Please read the following list to understand how the concept of default user comes into play in different situations:

- **Manually added users:** When users are added manually through the SafeCom Administrator, the **User properties** dialog is pre-filled according to the settings of the default user defined on the SafeCom server they are added to. If there is no default user, factory defaults are used. The home server becomes the one they are added to. Users that are added while the **Find users** list is open will have the **User properties** dialog pre-filled according to the default user on the primary server.
- **Created users at first print:** Users that are created at first print inherit the settings of the default user defined on the SafeCom primary server. If there is no default, user factory defaults are used. The home server is set to the SafeCom primary server.
- **Imported users:** Users that are imported inherit the settings of the default user defined on the SafeCom primary server or the settings of a particular user if this is specified for the scheduled import. If there is no default user, factory defaults are used. The home server remains undefined until they get in contact with the SafeCom solution in any of the following ways:
 - **Printing:** If their first action is to print, their home server will be the one referenced by the SafeCom Pull Port.
 - **Log in at device:** If their first action is to log in at a SafeCom-enabled device, their home server will be the one that is referenced by the SafeCom-enabled device.
 - **SafeCom G4 Web Interface:** If their first action is to log in to the SafeCom G4 Web Interface, their home server will be the one referenced by the SafeCom G4 Web Interface (typically, the SafeCom primary server).

Create a default user

1. In the **Users** menu, click **Add user** and enter "DEFAULT" in **User logon**.
2. On the **Identification** tab (see [Identification](#)) and **Settings** tab (see [Settings](#)), check the desired settings.
3. Click **Add**, then click **Finish**.
4. Right-click the "DEFAULT" user and click **Set as default user**.

Delete a default user

1. Open the **Server properties** dialog and click the **Users** tab.
2. Clear **Keep default user and use settings when creating new users** and click **OK**.
3. Right-click the default user and click **Delete user**.

Import users

It is possible to create multiple user import schedules. This gives great flexibility as exemplified in the following bullets.

- **Run now:** Click **Run now** to instantly run any user import. This way, user import is performed immediately during initial configuration.
- **Import from multiple sources:** Import users from different sources, for example, the Active Directory, a file, or even a different part of the same Active Directory. The SafeCom Administrator supports infinite possibilities.
- **Default user per import schedule:** Select **Apply settings from default user** or select which settings should be applied from a specific user.

For example: An educational institution imports staff from one part¹⁷ of the Active Directory and sets them to **Tracking**. It then imports students from another part of the Active Directory and has them inherit the settings of a manually¹⁸ created user (DEFAULT_STUDENT), which is set to Pay.

- **User handling:** There is only one way that users created at first print or added manually in SafeCom Administrator can be deleted during a scheduled import. These users are only deleted if they had, at any time, also been part of a scheduled import and are subsequently missing from a later scheduled import. The SafeCom solution notices their absence and deletes them. Whenever a user is imported, the ID of the import schedule is recorded in the database together with the user. A manually added user initially has the source ID 0. The user logon is unique regardless of the source ID. The function **Find user** allows selecting source ID as criteria.
- **ID handling:** There is only one way that IDs (or cards) registered at the device or added manually in SafeCom Administrator can be deleted during a scheduled import. These IDs are only deleted if their card numbers had, at any time, also been part of a scheduled import and are subsequently missing from a later scheduled import. The SafeCom solution notices their absence and deletes them. Whenever an ID code is imported, the ID of the import schedule is recorded in the

¹⁷ See search root and search filter in section [Properties \(Active Directory\)](#).

¹⁸ A user logon that starts with DEFAULT_ makes it easier to find the user and keep the user out of any scheduled import to prevent unintentional deletion.

database together with the ID code. A manually added ID codes initially has the source ID 0. In the **ID codes overview** dialog (see [List of ID codes](#)), the source ID can be seen for each ID code. ID code must be unique regardless of the source ID. If **Max IDs per user** (see [Users](#)) is greater than 1, you can add an ID as long as the user has not reached the maximum number of IDs. If a user is listed with another ID code in the same and subsequent import, the original ID code is replaced with the newer one.

- **Secondary and primary source:** A secondary source is only meant to modify the settings of existing users, typically, the ID code or cost code. A primary source is usually used to add, modify, and delete users and contains the user logon. The secondary source must include the user logon as the unique identifier.

For example: Users and most of their settings are imported from the Active Directory (primary source), and card numbers are imported from a CSV file (secondary source). In the CSV file, the user's logon is listed together with the ID code.

Overview

1. In the **Users** menu, click **Import users**.
The **User import schedules** dialog appears.
2. Click **Add** and proceed to the **Server** page.
3. If at least one scheduled import is defined, select it, and to test it, click **Run now**.
 - Click **Edit** to proceed to the **Server** page.
 - Click **Delete** to delete the scheduled import.
When a schedule is deleted, the source ID of the affected users and the ID codes are reset to 0.

In the **User import** dialog, there is both a progress bar and status list.

4. Select **Show log** to see a [user import log](#).

Server

Perform the following steps in the **SafeCom server properties** dialog.

1. Enter the **Server address** (hostname or IP address), a **User logon** with administrator rights, and the **Password**.
2. Click **Next** and proceed to the **Import source** page.
 - If you are editing an existing schedule, click **8. Schedule** to jump directly to the **Schedule information dialog**, and change the name of the schedule or the actual schedule.



- In a multiserver installation, you should specify the primary server for best performance.
- In a multiserver installation, you can use the PerformanceWaitTime registry key under `HKEY_LOCAL_MACHINE\SOFTWARE\SafeCom\SafeComG4` to set up performance data collection from the secondary servers to the primary server on a regular basis. The default value of the registry setting is 3600 seconds (1 hour). After modifying the value, you must restart SafeCom for the changes to take effect.

Import source

Perform the following steps in the **Select import source** dialog.

1. Select the source of the user import.
2. Click **Next** and proceed to the relevant, bolded sections:

	CSV file	XML file	Active Dir	Novell eDir	LDAP
1. Overview	Overview				
2. Server	Server				
3. Import source	Import source				
4. File source	File source (CSV file and XML file)	File source (CSV file and XML file)			
4. Properties			Properties (Active Directory)	Properties (Novell eDirectory)	Properties (LDAP server)
5. Configuration	Configuration (CSV)	Configuration (XML)	Configuration (Active Directory)	Configuration (Novell eDirectory)	Configuration (LDAP server)
6. Rules	Rules				
7. Extra	Extra				
8. Schedule	Schedule				

Source type can be **Primary** (standard) or **Secondary**. Only select **Secondary** if the import is meant to modify only the settings of existing users, typically card number or cost code. The secondary source must include the user logon as the unique identifier.

File source (CSV file and XML file)

Perform the following steps in the **Select source of file** dialog.

1. Browse to the import file and specify the name of the file to import from (with full path) as seen from the SafeCom server.

The account that runs the SafeCom service (normally, the Local System account) must have read access to the file.

i If you intend to click **Run now** in the **User import schedules** dialog to run the import momentarily, the file to import from (with full path) should be specified as seen locally from the computer where you are running SafeCom Administrator.

2. Click **Next** and proceed to **Configuration** for CSV (see [Configuration \(CSV\)](#)) or XML (see [Configuration \(XML\)](#)).

Properties (Active Directory)

Perform the following steps in the **Active Directory properties** dialog.

1. Enter the **AD server** (hostname or IP address).
2. Enter the **User account** and **Password**.
Specify the user logon followed by (@) and the domain, such as ADMIN@MYDOMAIN.
Alternatively, you can specify: MYDOMAIN\ADMIN .
3. Click **Next** and proceed to **Configuration** (see [Configuration \(Active Directory\)](#)).
The import can be secured and done through SSL (LDAPS) and port 636 by preceding the **AD server** with LDAPS://. If another port is used, it must be specified after the hostname or IP address.

Example:

For the secure import to function, the AD server must have **Certificates Services** installed (see [Install certificate](#)) and running, and the SafeCom server must trust the certificate from the AD server.

4. Select **Search root** to import all users from the specified organizational unit and below.

Example:

```
OU=MyDept,OU=MyCompany,DC=MyDomain,DC=com
```

5. Select **Search filter** to import user objects matching the specified filter.

Example:

```
(&(objectClass=user)(sAMAccountName=*))
```

Properties (Novell eDirectory)

Perform the following steps in the **Novell eDirectory properties** dialog.

1. Enter the **eDir server** (hostname or IP address).
2. Enter the **User account** and **Password**.
 - Specify the user logon in the following way:
cn=Administrator, o=Admins

If using LDAPS, use the server name from the certificate. Typically, the DNS name is LDAPS:// dns name.

3. Click **Next** and proceed to **Configuration** (see [Configuration \(Novell eDirectory\)](#)).
4. Select **Search root** to import users or enter the specific organizational unit where you want **Search root** to look for users.

Example:

```
ou=MyDept, o=MyOrg
```

5. Select **Search filter** to import user objects matching the specified filter.

Example:

```
(&(objectClass=user)(Uid=*))
```

Properties (LDAP server)

The **LDAP server properties** dialog appears.

1. Enter the **LDAP server** (hostname or IP address), the **User account**, and the **Password**.
 - If the LDAP server is an **AD server**, specify the user logon followed by (@) and the domain like this: ADMIN@MYDOMAIN. Alternatively, you can specify: MYDOMAIN\ADMIN.
 - If the LDAP server is an **eDir server**, specify the user logon like this: cn=Administrator, o=Admins.
 - If the LDAP server is on Linux/Unix, specify the user logon like this: The DN distinguished name must be cn=xxxx, ou=xxxx, dc=xxxx, dc=com, or a Uid=xxxx, ou=xxxx, dc=xxxx, dc=com.

If using LDAPS, use the server name from the certificate. Typically, the DNS name is LDAPS:// dns name.

2. Click **Next** and proceed to **Configuration** (see [Configuration \(LDAP server\)](#))

See [Properties \(Active Directory\)](#) if the import needs to be secure. Select **Search root** to import users from that organizational unit, for example:

- Search root example **AD server**:

```
OU=MyDept,OU=MyCompany,DC=MyDomain,DC=com
```

- Search root example **eDir server**:

```
ou=MyDept,o=MyOrg
```

Select **Search filter** to import user objects matching the specified filter.

Configuration (CSV)

Perform the following steps in the **Specify fields in CSV file** dialog.

1. Check the configuration options as required (see below).
2. Click **Next** and proceed to **Rules**.

Specify from which field in the CSV file the values should be retrieved. Enter 0 to avoid import.

Example CSV file with header and two entries:

```
UserLogon;FullName;Email;IDCode
JS;John Smith;JS@safecom.eu;1232
JD;Jane Doe;JD@safecom.eu;9856
```

Microsoft Excel files with the extension *.csv cannot be used directly. Open the file in Notepad, for example, to ensure that it is a plain text file like the example and to determine what separator character is used (semicolon is default).

If you select **First line in file is a header**, you need to specify the name of the field rather than the number. The field name is not case-sensitive.

If a code is being imported and the import consists of magnetic card ID codes, select the appropriate conversion method (see [Conversion of magnetic ID codes](#)).

In **Alias**, you can specify multiple fields by separating them by semicolons.

Example:

```
Alias1; Alias2; Alias3
```

In **Access rights mask**, specify the access rights mask (see [Settings](#)).

Configuration (XML)

There is no **XML configuration** dialog. Proceed to **Rules**. The syntax of the XML file is illustrated in this example:

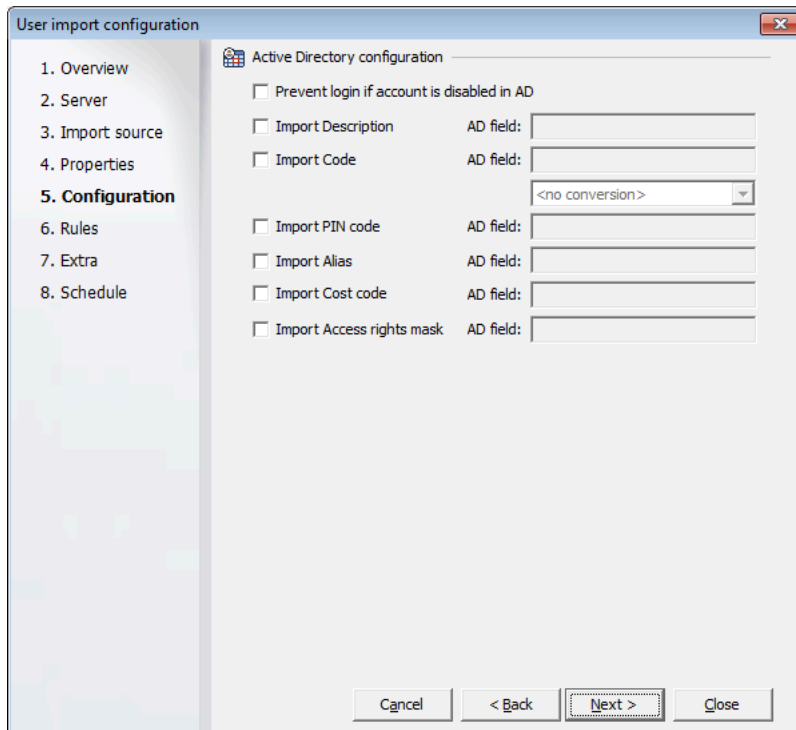
```
<?xml version="1.0" ?>
<UserList>
  <User>
    <UserLogon>JS</UserLogon>
    <FullName>John Smith</FullName>
    <Description>location 1</Description>
    <EMail>JS@safecom.eu</EMail>
    <CardNo>1232</CardNo>
    <PINCode>2222</PINCode>
    <OrgUnit>\MyCompany\MyDepartment</OrgUnit>
    <Alias>JSmith</Alias>
    <CostCode>90678</CostCode>
  </User>
</UserList>
```

Parameter	Description	Remark	Default value
UserLogon	The user's logon name. Maximum 20 characters.	Mandatory	None
FullName	The user's full name. Maximum 80 characters.	Optional	None
Description	Description field. Maximum 80 characters.	Optional	None
Email	The user's E-mail address. Maximum 80 characters.	Optional	None
CardNo	The ID code. Maximum 39 characters. See User authentication by card or ID code .	Optional	None
PINCode	The 4-digit PIN code.	Optional	<u>1234</u>
OrgUnit	The organization unit.	Optional	None
Alias	Alias. Maximum 20 characters. Maximum 10 Alias tags.	Optional	None
CostCode	Cost code. Maximum 50 characters.	Optional	None
AccessRightsMask	Access rights mask. Integer. See Settings .	Optional	0

Configuration (Active Directory)

Perform the following steps in the **Active Directory configuration** dialog.

1. Check the configuration options as required (see below).
2. Click **Next** and proceed to **Rules**.



3. Select **Prevent login if account is disabled in AD** if users who are disabled¹⁹ in Active Directory should be prevented from logging in to the SafeCom solution (Login denied). In SafeCom Administrator, this is reflected by the status of the **Prevent login** check box on the **Identification** tab of the **User properties** dialog (see [Identification](#)).
4. Select **Import Description** and specify the **AD field** that holds the description.
5. Select **Import Code** and specify the **AD field** that holds the ID code.
 - If the import consists of magnetic card ID codes, select the appropriate conversion method (see [Conversion of magnetic ID codes](#)).
6. Select **Import PIN code** and specify the **AD field** that holds the PIN code.
7. Select **Import Alias** and specify the **AD field** that holds the alias. You can specify multiple alias fields, by separating them by semicolon.
Example: Alias1; Alias2; Alias3.
8. Select **Import Cost code** and specify the **AD field** that holds the cost code.
9. Select **Import Access rights mask** and specify the **AD field** that holds the access rights mask (see [Settings](#)).

i The options listed above are in addition to the automatically used options listed in the table below.

These standard AD attributes are used during the import:

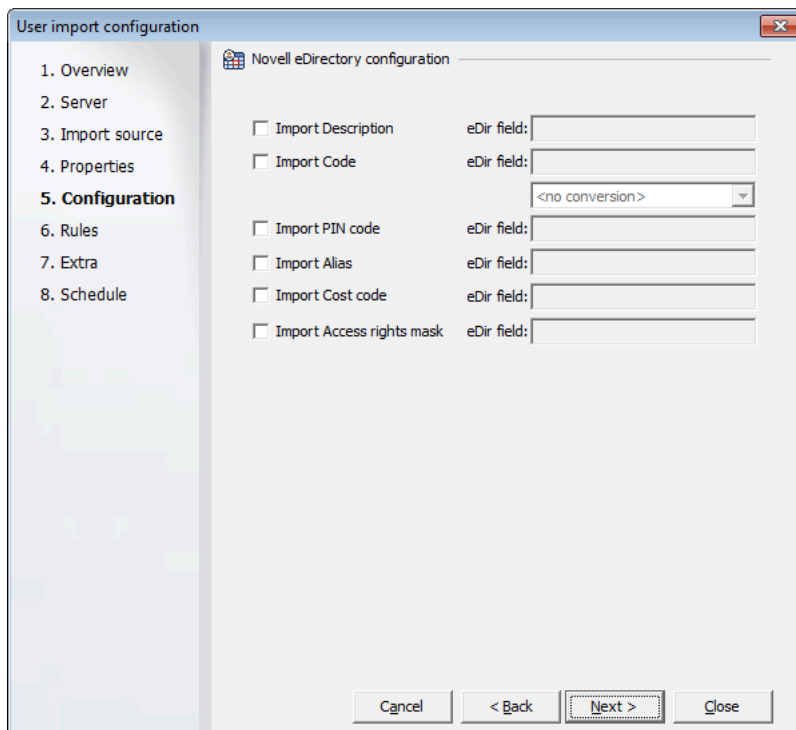
¹⁹ The user is considered disabled in Active Directory if the UF_ACCOUNTDISABLE bit is set in the userAccountControl attribute.

Microsoft Management Console	AD Field name	SafeCom	Examples
User logon name	sAMAccountName	User logon	JS
Display name	DisplayName	Full name	John Smith
Description	Description	Description	location 1
E-mail	Mail	E-mail	JS@safecom.eu
Account is locked out	userAccountControl	Prevent login	
Org. unit	distinguishedName	Org. unit	ou=MyDept, ou=MyCompany
		Alias	Jsmith
		Cost code	
		Access rights mask	

Configuration (Novell eDirectory)


Perform the following steps in the **Novell eDirectory configuration** dialog.

1. Check the configuration options as required (see below).
2. Click **Next** and proceed to **Rules**.



3. Select **Import Description** and specify the **eDir field** that holds the description.

4. Select **Import Code** and specify the **eDir field** that holds the ID code.
 - If the import consists of magnetic card ID codes, select the appropriate conversion method (see [Conversion of magnetic ID codes](#)).
5. Select **Import PIN code** and specify the **eDir field** that holds PIN code.
6. Select **Import Alias** and specify the **eDir field** that holds alias.
You can specify multiple alias fields, by separating them by semicolon.
Example: Alias1; Alias2; Alias3
7. Select **Import Cost code** and specify the **eDir field** that holds the cost code.
8. Select **Import Access rights mask** and specify the **eDir field** that holds the access rights mask (see [Settings](#)).

 The options listed above are in addition to the automatically used options listed in the table below.

These Novell eDirectory attributes are used during the import:

Novell ConsoleOne	eDir Field name	SafeCom	Examples
Unique ID	Uid	User logon	JS
Full name	FullName	Full name	John Smith
Department	Ou	Description	location 1
E-mail address	Mail	E-mail	JS@safecom.eu
dn ²⁰	Dn	Org. unit	ou=MyDept, o=MyOrg
		Alias	Jsmith
		Cost code	
		Access rights	

Configuration (LDAP server)

Perform the following steps in the **LDAP server configuration** dialog.

1. Check the configuration options as required (see below).
2. Click **Next** and proceed to **Rules**.

²⁰ The organizational unit is extracted from the distinguished name in the Novell eDirectory and is not held in one particular field.

The screenshot shows the 'User import configuration' dialog box. On the left, a sidebar lists steps from 1 to 8, with '5. Configuration' highlighted. The main area is titled 'LDAP server configuration' and contains a list of attributes with checkboxes and 'LDAP field:' text boxes. The 'User logon' checkbox is checked. The 'Code' attribute has a dropdown menu set to '<no conversion>'. At the bottom, there are four buttons: 'Cancel', '< Back', 'Next >', and 'Close'.

3. Select **User logon** and specify the **LDAP field** that holds the user logon.
4. Select **Full name** and specify the **LDAP field** that holds the full name.
5. Select **Description** and specify the **LDAP field** that holds the description.
6. Select **E-mail** and specify the **LDAP field** that holds the e-mail address.
7. Select **Code** and specify the **LDAP field** that holds the ID code.
 - If the import consists of magnetic card ID codes, select the appropriate conversion method (see [Conversion of magnetic ID codes](#)).
8. Select **PIN code** and specify the **LDAP field** that holds PIN code.
9. Select **Org. unit** and specify the **LDAP field** that holds organizational unit information.
10. Select **Alias** and specify the **LDAP field** that holds alias.

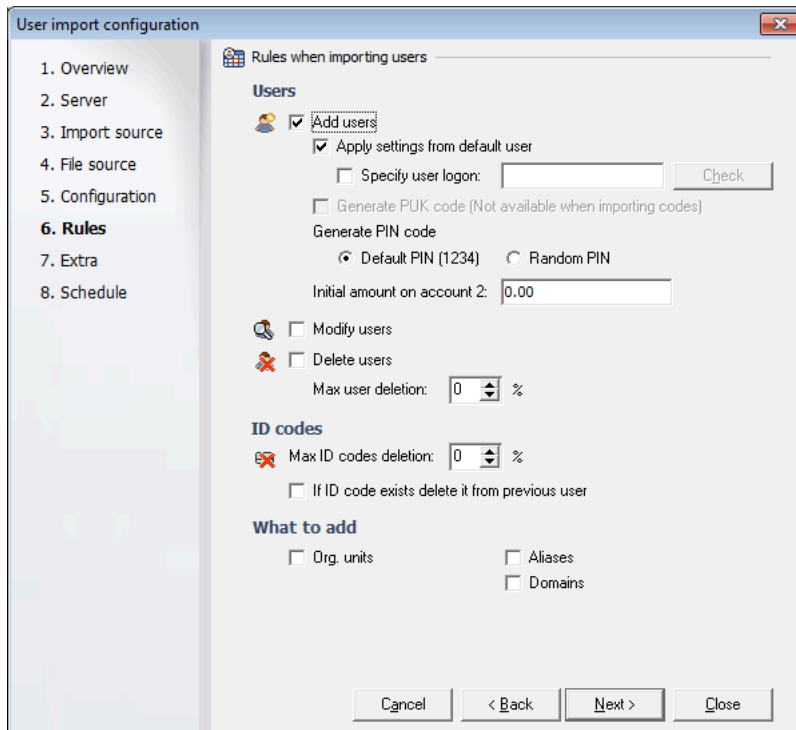
In **Alias**, you can specify multiple fields, by separating them by semicolon.

Example: Alias1; Alias2; Alias3
11. Select **Cost code** and specify the **LDAP field** that holds the cost code.
12. Select **Access rights mask** and specify the **LDAP field** that holds the access rights mask (see [Settings](#)).

Rules

Perform the following steps in the **Rules when importing users** dialog.

1. Select the rules as required (see below).
2. Click **Next** and proceed to [Extra](#).



3. Select **Add users** to have all users imported.

- Select **Apply settings from default user** if you want the newly imported users to inherit the settings of the default user.

i The following settings are not inherited, even though **Apply settings from default user** is checked: **Prevent login**, **Account Credit Balance**, and **User Access Rights**.

4. Select **Specify user logon** and enter the user logon of the user from which you wish the new users to inherit settings.

In a multiserver installation, the default user must have the primary server as home server.

5. Select **Generate PUK code** if you want a PUK code to generated.

The PUK code can be e-mailed to users (see [E-mail](#)). **Generate PUK code** is dim if ID codes are part of the import.

- Select **Generate PIN code** to generate PIN codes for AD users missing PIN codes in AD (already existing PINs in AD will not be overwritten).
- Select **Default PIN (1234)** or **Random PIN**.
- Change **Initial amount on account 2** to another value than 0.00 only if the solution involves Pay, and the initial amount on the account should have the specified value. See [Credit schedule](#).

6. Select **Modify users** to modify the settings of any user that were previously imported through this schedule.

In that case, the schedule ID of the user matches that of the schedule.

Running the import twice ensures that users with access rights to all functions keep these access rights.

7. Select **Delete users** to delete any existing users that are now missing from the import but were previously imported through this schedule.

In that case, the schedule ID of the user matches that of the schedule.

The default user and users with [special rights](#) are not deleted.

8. Use **Max user deletion** as a safety measure to prevent unintentional deletion of users.

A value of 0% causes the import to take place anyway. A value of 20% cancels the import if it would delete every fifth or more users that were previously imported through this same, scheduled import. The import of a user fails if the user's ID code is already registered with another user in the SafeCom solution. To resolve this, perform step 9.

9. Select **If ID code exists, delete it from previous user**.

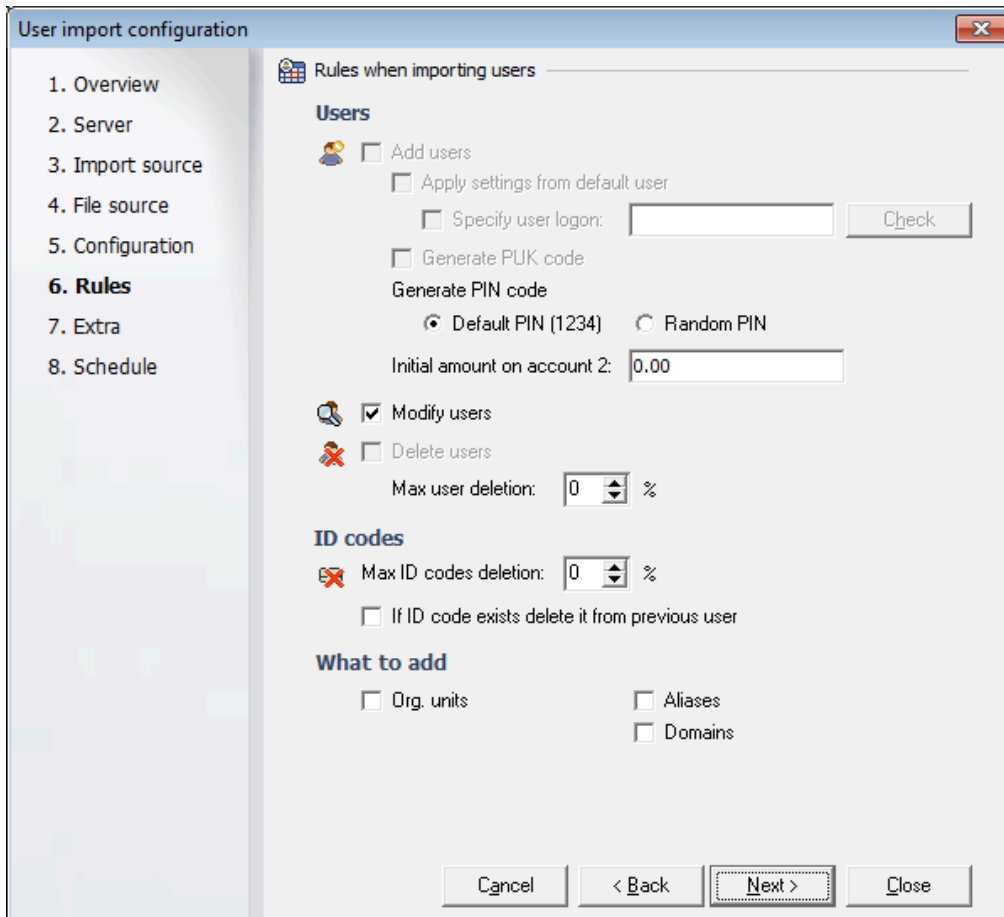
For this to work, you are advised to select **Modify users** and/or **Delete users**. During the import, users are sorted alphabetically based on their user logon and ID codes are being reused in that order. Details are recorded in the log file.

Select **Org. units** to extract [organizational units](#). Select **Aliases** to import the aliases from the list of fields specified in the **Alias** field.

The following two check boxes are only present when importing from Active Directory:

- Select **Groups** to import [group information](#) from Active Directory and include it in the import.
- Select **Synchronize groups** if you want the information in Active Directory to completely control which groups a user is member of, and any local changes made within the SafeCom solution are lost at the subsequent import from Active Directory.

Most of the controls are dim when **Source type** is set to **Secondary** in the **Select import source** dialog (see [Import source](#)).



Extra

Perform the following steps in the **Advanced extra configuration** dialog.

1. If a special user import module has been supplied, select **Use extra configuration** and enter the configuration according to the supplied instructions.
2. Click **Next** and proceed to **Schedule**.

Schedule

Perform the following steps in the **Schedule information** dialog:

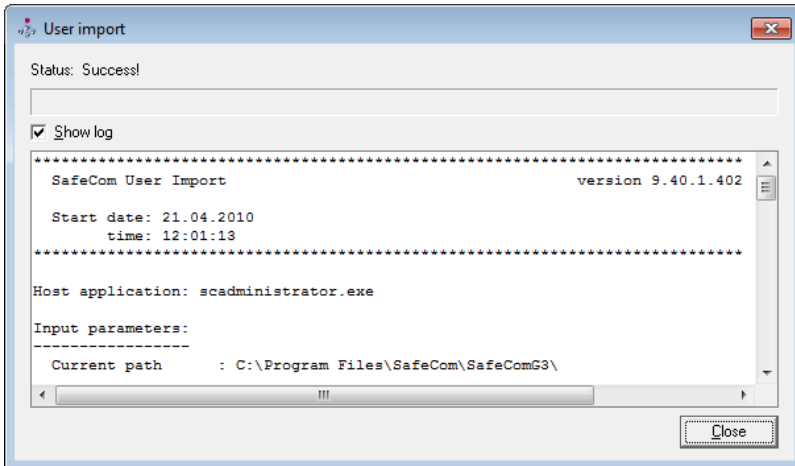
1. Select the schedule options as required (see below).
2. Click **Finish** to save the changes and return to **Overview**, where the scheduled import, including its source ID, is listed and can be run now.

The screenshot shows the 'User import configuration' dialog box with the 'Schedule information' tab selected. The sidebar on the left lists steps 1 through 8, with '8. Schedule' highlighted. The main content area includes a 'Name' text field, radio buttons for scheduling options (Manual, One time only, Daily, Weekly, Monthly), and sections for selecting start and end dates and frequencies. The 'Daily' option is selected, and the start time is set to 00:00. The 'Every 24 hours' frequency is also selected. At the bottom, there are buttons for 'Cancel', '< Back', 'Finish', and 'Close'.

3. Enter a meaningful **Name**.
If you leave the field empty, it gets populated with the text "User schedule (date time)".
4. Choose from the following options to schedule the import:
 - **One time only**
 - **Daily**
 - **Weekly**
 - **Monthly**
5. Select **End date** and specify a date for when the scheduled import should end.
Ensure that the end date does not conflict with the selected frequency options. Otherwise, scheduled imports might not run.

User import log file

During the import, a log file is created.



The log file is called <Lyyyymmddhhmmss.log>.

- yyyy is the year
- mm is the month
- dd is the day
- hh is the hour
- mm is the minutes
- ss is the seconds

The log file is stored in the logfiles folder below the SafeCom G4 installation folder. The default folder is:

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

During import, you may encounter conflicts because either the UserLogon (cc = 58) or the Card number (cc = 60) already exists. Examples:

- Not able to add new user. Logon <UserLogon>, cc = 58
- Not able to add new user. Logon <UserLogon>, cc = 60
- Not able to modify user (modify). Logon <UserLogon>, cc = 58
- Not able to modify user (modify). Logon <UserLogon>, cc = 60

If the import includes aliases, you may also get these messages because either the specified user does not exist (cc = 54) or the specified alias already exists (cc = 73). Examples:

- Not able to add new alias. User <UserLogon> Alias <Alias>. cc = 54
- Not able to add new alias. User <UserLogon> Alias <Alias>. cc = 73

If **If ID code exists, delete it from previous user** (see [Rules](#)) was checked during import, there will be an entry in the log file for each reused ID code. Example:

```
27.11.2008 10:16:15: Duplicate card Card3 removed from user USERC 27.11.2008 10:16:15:
Duplicate card Card3 given to user USERD
```


3. Complete the steps presented by the Certificate Import Wizard.

i If a one-time import is to be done, the certificate must be installed on the computer from where the SafeCom Administrator is used.

Conversion of magnetic ID codes

When importing magnetic ID codes, you must select which track you want to use (Track1, Track 2, or Track 3). Normally, you should use Track 2.

If you are using SafeCom magnetic cards, the ID code is stored on Track 2 and is printed on the card. However, further steps are necessary before importing the ID code.

First, register the card at the device and check what it looks like in when it appears in SafeCom Administrator. If the ID code contains any of the letters C, D, or E within the number (not at the end or the start), then the letter must be replaced with another character at the same location. In the example below, the = character is inserted to get a resulting D.

Example:

- 6032170000002954890103000

This is how the ID code is printed on the card.

- B603217000000295489D0103000F1

This is how the ID code appears in SafeCom Administrator if it has been registered at a device or in SafeCom Administrator using a connected card reader.

- 603217000000295489=0103000

This is how the ID code must look like before importing. The = character is inserted to get a resulting D.

For the letter C to appear, insert <.

For the letter D to appear, insert =.

For the letter E to appear, insert >.

Create users at first print

As discussed in [Create users at first print](#), this method keeps administrative overhead to a minimum.

1. In the **Servers** menu, click **Properties**.
In a multiserver solution, these changes are only required on the SafeCom primary server.
2. Click the **Users** tab.
3. Select **Create users at first print**.
4. Select **Create e-mail addresses** and enter the **E-mail domain**.
5. Select **Keep default user and use settings when creating new users** and select the **Default user**.
6. Click the **E-mail** tab.
7. Verify that a valid **SMTP mail server** has been specified.

8. Select **E-mail PUK code to new users** and any of the messages you may wish to enable.
9. [Customize the e-mail messages](#) if required.

Add users manually

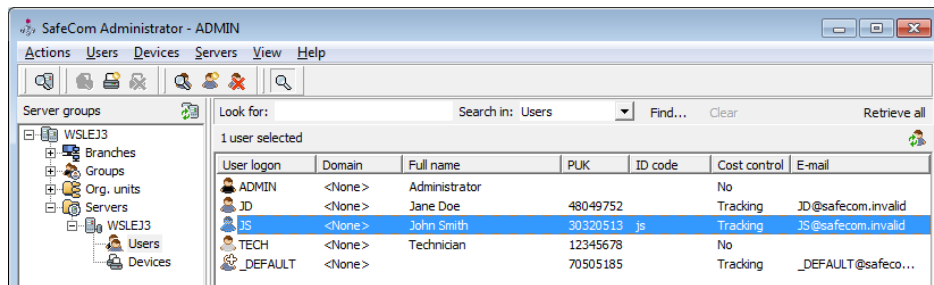
Perform one of the following steps:

- Right-click in the **Users list** and select **Add user**.
- In the **Users** menu, click **Add user**.
- Click the **Add user** button.

Refer to the **User properties** dialog in [User properties](#) for a description of the fields.

Find users

1. Click the **Find** button.
2. Change **Search in** to "Users".



3. Find users with one of the following methods:
 - Enter a search string in **Look for** and click **Find now**.
The Find function uses case insensitive, free-text search.
 - Click **Retrieve all** to display all users regardless of their home server.
 - Click **Clear** to reset the Find function.
 - Click **Find** to open the **Find users** dialog.
 - Enter your find criteria and click **Find**.
The Find function uses field-based, case insensitive, free-text search, with the exception of ID codes.
 - To find a particular ID code, enter the complete **ID code** to the right or click **Listen for card** if a card reader is installed on the computer.

Customize the user list view

1. In the user list, right-click one of the column headers, such as **User logon**.
2. Select the properties that should appear as columns in the user list.

Hide ID codes

For security reasons, viewing ID codes (user codes and card numbers) and PUK codes in SafeCom Administrator can be restricted for users with no administrator rights.

To hide ID codes for users, perform the following steps:

1. Start SafeCom Administrator and log in.
2. Select **Hide ID codes** on the **Users** tab in the **Server properties** dialog.
3. Identify the users with administrator rights who are not allowed to see ID codes and make sure to change their user rights to **Partial rights** or lower.

Based on the level of administrator rights, a user may be allowed to display and perform various operations with ID codes and PUK codes. Permissions for each right level are described below. For reference, please see the image below.

User rights	ID code									PUK code						Users > ID codes... menu visible	
	Server properties	Masking	User pane	User properties				Export Wizard	Server properties	Masking	User pane	User properties			Export Wizard		
	Hide ID codes	Visible	Column visible	Add	Copy	Modify	Delete	Export	Hide ID codes	Visible	Column visible	Generate	Copy	Clear	Export		
Full rights User can modify and view all features	<input type="checkbox"/>	1234	✓	✓	✓	✓	✓	✓	<input type="checkbox"/>	1234	✓	✓	✓	✓	✓	✓	✓
	<input checked="" type="checkbox"/>	1234	✓	✓	✓	✓	✓	✓	<input checked="" type="checkbox"/>	1234	✓	✓	✓	✓	✓	✓	
Partial rights User can modify and view all features except sensitive data and export sensitive data and change admin rights	<input type="checkbox"/>	1234	✓	✓	✓	✓	✓	✗	<input type="checkbox"/>	1234	✓	✓	✓	✓	✗	✗	✗
	<input checked="" type="checkbox"/>	****	✓	✓	✗	✗	✓	✗	<input checked="" type="checkbox"/>	****	✓	✓	✗	✓	✗	✗	
Limited rights User can add information but have no permission to add or remove information	<input type="checkbox"/>	1234	✓	✓	✓	✓	✓	✗	<input type="checkbox"/>	1234	✓	✓	✓	✓	✗	✗	✗
	<input checked="" type="checkbox"/>	****	✓	✓	✗	✗	✓	✗	<input checked="" type="checkbox"/>	****	✓	✓	✗	✓	✗	✗	
None (view only) User can only view and not change information	<input type="checkbox"/>	1234	✓	✗	✓	✗	✗	✗	<input type="checkbox"/>	1234	✓	✗	✓	✗	✗	✗	✗
	<input checked="" type="checkbox"/>	****	✓	✗	✗	✗	✗	✗	<input checked="" type="checkbox"/>	****	✓	✗	✗	✗	✗	✗	

Administrators with full rights can see ID and PUK codes and perform all related operations with them, regardless of the **Hide ID codes** setting.

Only administrators with full rights can access the **Users > ID codes** menu.

When the **Hide ID codes** setting is checked, the following permissions apply:

Administrators with partial or limited rights:

- can only see masked ID and PUK codes.
- cannot copy or modify ID codes.
- cannot copy PUK codes.
- cannot export ID or PUK codes.

Administrators with no rights ("None (view only)"):

- see only masked ID and PUK codes.
- cannot perform any operation with ID or PUK codes.

When the **Hide ID codes** setting is unchecked, the following permissions apply:

Administrators with partial or limited rights:

- can see ID and PUK codes.
- cannot export ID or PUK codes.

Administrators with no rights ("None (view only)":

- can see ID and PUK codes.
- can only perform Copy operations with ID and PUK codes.



- To learn more about administrator permissions, see [Rights](#).
- Checking **Hide ID codes** does not affect the user's view in the SafeCom Web Interface. Hiding ID codes in the Web Interface must be set up in scWebConfigurator.exe. For more information, refer to *SafeCom G4 Web Interface Administrator's Manual* in the downloadable [SafeCom G4 legacy documentation zip file](#).

Hide document names

1. Start SafeCom Administrator and log in.
2. Select **Hide Document names** on the **Users** tab in the **Server properties** dialog.
3. Identify the users with administrator rights who are not allowed to see ID codes and make sure to change their rights to **Full rights** or lower.

A user with no administrator rights can no longer see document titles in the list of print jobs under any user, including in the user's own list of documents. It is also possible to hide document names in the print queue (see [Configure the SafeCom Pull Port](#)).



Checking **Hide Document names** does not affect the users view in the SafeCom Web Interface.

Edit the properties of multiple users

1. Use [Find users](#) to get a list of relevant users.
2. Perform one of the following steps:
 - To select consecutive users, click the first user, press and hold down Shift, then click the last user.
 - To select non-consecutive users, press and hold down Ctrl, then click each user.
 - To select all users in the window, press Ctrl + A.
3. Press Alt + Enter or right-click the selected users, then select **User properties**.
4. Make the required changes on the **Identification** and **Settings** tabs.
 - On the **Identification** tab, it is possible to edit the following properties:
 - **Domain**
 - **Home server**

- **Org. unit**
- **Description**
- **Cost code**

The following actions are also possible:

- Click **Clear** to set the number of failed login attempts to zero.
- Select or clear **Prevent login**.
- Select or clear **Login without PIN code**.
- On the **Settings** tab, it is possible to edit all properties.
- On the **ID code** tab, the following actions are possible:
 - Click **PUK** to generate a new PUK code
 - Click **PIN code** to assign a default PIN code.

The PUK code can be e-mailed to users (see [E-mail](#)).

5. Click **OK.**

When editing multiple properties, the following legend applies:

- Check boxes can have three states: Checked, clear, and dim. If it is dim, it is because the selected users have different properties.
- Fields are shown with a light gray background and the text N/A in black if the selected users have different properties.
- Drop-down lists are shown with a light gray background and the first element in the list.

Delete users

In the user list, select the users you wish to delete, then perform one of the following steps:

- Right-click the selected user and select **Delete user**.
- In the **Users** menu, click **Delete user**.
- Select the user and press the Delete key.

User redaction

User redaction is a feature in SafeCom G4 Server available from version 10.530. This feature enables administrators to redact certain user-specific data, including personally identifiable information in the database for deleted users.

How to use this feature

This feature is available through SafeCom Administrator.

Redacting upon deletion

The user deletion dialog provides a check box for redacting data for the user being deleted. When this check box is selected, user redaction takes place immediately upon deletion. If you select not to redact user data at deletion, you will still have a way to redact user data for previously deleted users, see below.

To redact data for a user upon deletion:

1. In SafeCom Administrator, select the users you would like to delete.
2. Press the Delete key, or right-click and click **Delete user**, or click **Delete user** in the **Users** menu.
The confirmation dialog appears.
3. Select the check box with the **Permanently redact personal data** label.
4. Click **OK**.

Redacting a previously deleted user

The administrator can decide to redact data for users that have been deleted earlier in SafeCom.

To redact data for a previously deleted user, perform the following steps:

1. In SafeCom Administrator, click **Users** in the menu bar and click **Redact user data**.
The **Redact user data** dialog appears.
2. Under **Find users**, enter the search criteria for the deleted user you would like to redact.
3. Click **Find** to have a list of deleted users whose user logon, full name, or email address contain the search criteria.
An unfiltered list of deleted users can also be retrieved using a blank value for search.
The operation may result in a large number of search results, so only the first 100 users are listed.
4. In the **Users** list, select one or more users to redact, then click **Redact**.

Important notes about user redaction

Redacting is irreversible

User data redaction cannot be undone. This process results in unrecoverable data loss in the database in the records related to the redacted user.

Data in logs or previously exported data is not redacted

SafeCom does not redact any data already written to software logs, including the SafeCom event database, the event log, or trace logs. Personal user data can be found in previously exported tracking records, transactional data, user lists, or database backups. The administrator should make sure that these previously exported files are cleaned up as needed.

Email warnings about the upcoming deletion of print jobs may contain personally identifiable data like the name of the print job.

Data in other tracking fields

Depending on usage, there are other fields in the database that may hold personally identifiable data, such as the names of devices, billing code fields, port names, and user cost code fields. These fields are not redacted by this feature.

Print job data may temporarily remain on servers or Print Clients after user deletion

When users are deleted from the system, their print jobs are not immediately deleted from the database. Print job lifetime is dependent on periodic job synchronization between servers, the schedule of database integrity checks, and other job length configurations.

In group print and delegated print scenarios, retained jobs may remain in the system.

Data stored on secondary servers and Print Clients is not redacted

The primary database may receive tracking records for an already deleted user from various sources.


Secondary servers or Print Clients can work in offline mode. Tracking data including users' personal data is stored locally in this case. The administrator should make sure that the proper amount of time has passed between a user's last action and the time of redaction to make sure all data from secondary servers and Print Clients is synchronized with the primary server. Redaction only takes place on the primary server, and then changes in the database are propagated to secondary servers.

If the redaction was performed before data synchronization, then the operation must be repeated in order to have data redacted completely.

If tracking data arrives to the primary database after redaction and a new redaction is repeated by administrators later, the newly redacted records are not associated with the earlier redacted tracking records by any of the relevant database fields.

Billing data may not be redacted if a user is deleted and redacted before the billing window closes

If a billing window is enabled and all tracking records for a deleted user are waiting for user review, thus, no final committed records are in the tracking database yet, then this user cannot be found by the search operation in the **Redact user data** dialog. In general, it is recommended to wait for the billing window to pass after redacting a deleted user.

 The tracking records for user review are also in scope of the data redaction procedure.

Information in jobs owned by non-redacted users is not redacted

In some scenarios, there may be information about redacted users in the metadata of print jobs belonging to different, non-redacted users, even after the redaction takes place. For example, when a redacted user delegated a job to another user, the delegated print job contains a reference for the redacted user as the delegator. This is a temporary situation. When these print jobs are printed or purged, this data is expected to disappear from the system.

Users with the same user logon in different domains

In tracking and transactional data, SafeCom does not differentiate between users with the same **User logon** property in different domains. Although, these user logons can be used to log in with

different user credentials, they are treated as one user during redaction, and data for all these users are redacted.

The "Redact user data" dialog only finds users having jobs

User search in the **Redact user data** dialog uses the core and tracking databases to find users. Those deleted users who have no released jobs are not found by this dialog. This may affect Pay and Administrator users.

Redacting users in an upgraded SafeCom G4 Server environment

Data redaction works without any further limitation in an upgraded SafeCom environment. The upgrade mechanism guarantees that the database tables are upgraded according to the requirements of the feature.

List of aliases

1. In the **Users** menu, click **Aliases**.
The **Aliases overview** dialog appears.
2. Click **Copy** to copy the selected aliases to the clipboard.
3. Click **Save** to [save the list of aliases to a file](#).

Save aliases to file


1. Open the **Aliases overview** dialog (see [List of aliases](#)).
2. Click **Save**.
3. Select **Save as type** (XML or CSV) and enter a **File name**, then click **Save**.

The XML tags are covered in the table below. The CSV column header is the same as the XML tag.

Parameter	Description
UserLogon	Logon name
FullName	Full name
Alias	Alias

List of ID codes

1. Open the SafeCom Administrator and log in.

 Only users with administrator rights have the option to open the ID codes overview if **Hide ID codes** is checked in **Server properties** on the **Users** tab.

2. In the **Users** menu, click **ID codes**.
The **ID codes overview** dialog appears. The list of temporary IDs is displayed by default.
3. Select **Permanent cards** to see the list of permanent cards.
 - Click **Make permanent** to change the selected temporary IDs to permanent IDs.

- Click **Copy** to copy the selected ID codes to the clipboard.
- Click **Delete** to delete the selected IDs from the users.
- Click **Save** to [save the list of ID codes to a file](#).

Save ID codes to file

1. Open the **ID codes overview** dialog (see [List of ID codes](#)).
2. Click the **Save** button.

Either **Temporary IDs** or **Permanent IDs** are saved. The saved information includes User Logon, Full name, and ID code (decrypted). If **Temporary IDs** are saved, the **Start date** and **End date** are not included.

The **Save list of ID codes** dialog appears.

3. Select **Save as type** (CSV, XML, or TXT). Enter a **File name** and click **Save**.

The XML tags are covered in the table below. The CSV column header is the same as the XML tag.

Parameter	Description
UserLogon	Logon name
FullName	Full name
CardNo	ID code

Customize the format of ID codes

When a user generates an ID code through the SafeCom Web Interface, the ID code is set by default to the following:

- Six characters in length – with a minimum two digits and two letters (lower case only).
- Temporary – ID codes expire six months after they are created.

Also, by default, the SafeCom solution sends three e-mail warnings to the user that their ID code is going to expire. The first e-mail is a three week warning, the second is a two week warning, and the last one is a seven day warning.

To customize ID code settings, perform the following steps:

1. Open the IDCodeGenerating.txt file.

The file is located in the %SafeCom%\Templates folder, whose default location is C:\Program Files\SafeCom\SafeComG4\Templates.

The content of **IDCodeGenerating.txt** is as follows:

```

;-----
; This file specifies the configuration
; of generation of ID codes in SafeCom.
;; (c) 2011 SafeCom
;-----
[Params]
Version="1"
CodePattern="11xx**"

```

```
ExpireWarning1="21"  
ExpireWarning2="14"  
ExpireWarning3="7"
```

2. Change the file according to the following information:

i When selecting the number of characters in the ID code, make sure there are a sufficient number of permutations possible, considering the number of ID codes needed in your organization.

- **CodePattern:** This string specifies the minimum number of digits, minimum number of lowercase letters, and the total length.
 - The string "11xx**" indicates a 6 character string, with minimum 2 digits (11) and 2 letters (xx).
 - The string "11111" indicates a 5 digit string.

i Only numbers 0-9 and letters a-z (lower case only) can be used. No special characters are allowed.

- **ExpireWarning1:** The ID code expires in the amount of days this string specifies. The first email that warns about this contains this string.
- **ExpireWarning2:** The ID code expires in the amount of days this string specifies. The second email that warns about this contains this string.
- **ExpireWarning3:** The ID code expires in the amount of days this string specifies. The final email that warns about this contains this string.

i An automatic e-mail reminder can be set up to notify the user about their ID code expiring soon (see [Customize and translate e-mail messages](#)). The generated ID codes follow the settings configured under the **Users** tab of **Server properties** (see [Users](#)).

3. Save the changes to the file.
4. Copy the file from the Templates folder to the SafeCom install folder on the SafeCom primary server.

The new template takes effect immediately after restarting the SafeCom service.

User has lost ID card

If a user loses their ID card, the user needs to register a new card.

1. [Find the user](#).
2. Open the **User properties** dialog, then click the **ID code** tab.
3. Click **PUK** to generate a new PUK code or enter the ID code.

User has forgotten ID code

If the user forgets their ID code, you can retrieve it.

1. [Find the user.](#)
2. Open the **User properties** dialog, then click the **ID code** tab.
Code contains the ID code.

User has forgotten PIN code

If the user forgets their PIN code, you can generate a new PIN code.

1. [Find the user.](#)
2. Open the **User properties** dialog, then click the **ID code** tab.
3. Click **PIN code**.
4. Click **Random** to assign and display a randomly generated PIN code, or click **Default** to assign and display the default PIN code (1234).
See [Allow users to change their PIN code](#) on how users can subsequently change their PIN code.

Delete a user's print jobs (documents)

1. Select the user whose print jobs (documents) you wish to delete.
2. In the Job list, select the print jobs, and delete them by performing one of the following steps:
 - In the **Jobs** menu, click **Delete job**.
 - Right-click the selected job and select **Delete job**.
 - Press the Delete key.

The job list may contain these columns:

- **Document name:** The name of the print job.
- **Pages:** The number of pages in the print job.
- **Generated:** The date and time when the job was stored.
- **Paper size:** The paper size (A4, Letter).
- **Driver name:** The name of the print driver.
- **File location:** The computer where the print job is stored. The computer is running the SafeCom server software or the SafeCom Print Client.
- **Job distributor:** The SafeCom server the SafeCom Pull Port or SafeCom Print Client was referencing at the time of printing.

Customize and translate e-mail messages

E-mail messages can be customized and translated to give the users the highest user satisfaction. Dates are written according to the server's short format.

To use a specific e-mail template, copy the template file from the templates folder to the SafeCom installation folder on the SafeCom primary server. The new template automatically takes effect. The files are located in the %SafeCom%\Templates folder:

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

The e-mail templates are listed in the next section.

E-mail templates

- **EmailWelcome.txt:** Send a welcome message to new users if **E-mail welcome message to new users** is checked on the **E-mail** tab in the **Server properties** dialog (see [E-mail](#)).
- **EmailPUK.txt:** Send PUK code to the user if **E-mail PUK code when generated** is checked on the **E-mail** tab in the **Server properties** dialog (see [E-mail](#)).
- **EmailCode.txt:** Send code to the user if the EmailCode.txt file is located in the SafeCom installation folder. The E-mail is sent if the code is added in SafeCom Administrator through APIs or through an import. If the user gets, for example, two codes during an import, then the user receives two e-mails, one with each code.
- **EmailJobDelete.txt:** Send a note to the author about a document that has been deleted if **E-mail job deletion note to author of job** is checked on the **E-mail** tab in the **Server properties** dialog (see [E-mail](#)).
- **EmailWarning.txt:** Send a warning to the author and/or recipients about a document to be deleted if **E-mail delete warning** is checked on the **E-mail** tab in the **Server properties** dialog (see [E-mail](#)).
- **EmailIDCodeExpireWarning.txt:** Send an e-mail reminder to users, warning them that they have an ID code that is about to expire.
- **Email DelegateRequest.txt:** Send an e-mail notification to a potential user of SafeCom Delegate Print.
- **EmailDelegateRequestAccept.txt:** Send an e-mail where a user accepts the use of SafeCom Delegate Print.
- **EmailDelegateRequestReject.txt:** Send an e-mail where a user rejects the use of SafeCom Delegate Print.

In the **EmailWelcome.txt** and **EmailPUK.txt** files, it is possible to use the tags:

- <%ACCOUNTINGMODEL="No|Tracking|Pay For Print"%>
- <%CREDITS%>
- <%ENCRYPTION="No|Yes"%>
- <%GROUPNAME%>
- <%LOGINWITHOUTPIN="No|Yes"%>
- <%PIN%>
- <%PRINTALL="No|Yes"%> <%PUK%>

EmailWelcome.txt

```
<%SUBJECT="Welcome to SafeCom"%>
Dear <%USER%>,
You have been added as a user to the SafeCom solution.
You are about to experience the patented SafeCom Pull Print
technology. It gives you the freedom to collect your documents
at any SafeCom-enabled printer when it suites you.
When you print through SafeCom uncollected documents are deleted
after <%JOBDELETEDAYS%> days, <%JOBDELETEHOURS%> hours
and <%JOBDELETEMINUTES%> minutes.
www.safecom.eu
```

EmailPUK.txt

```
<%SUBJECT="SafeCom PUK code"%>
Dear <%USER%>,Your PUK code is: <%PUK%>
When you present the card at a SafeCom-enabled printer you
will be prompted for the above PUK code.
Write down the PUK code and bring it with you so you can
enter it when you are at the printer.
Once you have entered the PUK code, you do not need the PUK
code any longer.
www.safecom.eu
```

EmailCode.txt

```
<%SUBJECT="SafeCom ID code"%>
Dear <%USER%>,
You have been granted the following ID code:
<%CardNo%>
To login at the SafeCom-enable printer you can enter the
above code.
www.safecom.eu
```

EmailWarning.txt

```
<%SUBJECT="[SafeCom] Delete warning"%>
This mail is to inform you that
your document: <%DOCUMENTNAME%>
submitted on <%SUBMITDATE%><%SUBMITTIME%>
will be deleted on <%DELETEDATE%><%DELETETIME%>
<%USERLIST TEXT="Document has not yet been collected by:"%>
www.safecom.eu
```

EmailJobDelete.txt

```
<%SUBJECT="[SafeCom] Document deleted"%>
This mail is to inform you that
your document: <%DOCUMENTNAME%>
submitted on <%SUBMITDATE%><%SUBMITTIME%>
has been deleted.
<%USERLIST TEXT="Document was not collected by:"%>
www.safecom.eu
```

EmailIDCodeExpireyWarning.txt

```
<%SUBJECT="[SafeCom] ID code is about to expire"%>
This mail is to inform you that you have an ID code that
will expire on: <%DELETEDATE%><%DELETETIME%>
Please click the link below to generate a new ID code or
contact your administrator.
www.safecom.eu
```

EmailDelegateRequest.txt

```
<%SUBJECT="[SafeCom] Print delegate request"%>
Dear <%USER%>,
<%DELEGATEUSER%> has requested print delegation, then click the
link below to open a web browser and respond to the request.
http://server/safecom/<%DELEGATELINK%>
Print delegation enables you to submit delegated documents
to selected users and/or accept delegated documents from
selected users.
www.safecom.eu
```

EmailDelegateRequestAccept.txt

```
<%SUBJECT="[SafeCom] Print delegate request accepted"%>
Dear <%USER%>,
<%DELEGATEUSER%> has accepted your print delegate request.
www.safecom.eu
```

EmailDelegateRequestReject.txt

```
<%SUBJECT="[SafeCom] Print delegate request rejected"%>
Dear <%USER%>,
<%DELEGATEUSER%> has rejected your print delegate request.
www.safecom.eu
```

Chapter 7

Manage devices

From within SafeCom Administrator, it is possible to manage SafeCom devices and perform the following steps:

- **Device license:** Select licenses for the device.
- **Add device :** Register a device in the database.
- **Add device to a SafeCom Device Server:** Register a device to a device server.
- **Find devices:** Search the database for devices.
- **Broadcast for devices:** Broadcast on the network to find SafeCom Controllers and devices with SafeCom Go.
- **Customize the device list view**
- **Edit the properties of multiple devices**
- **Delete devices:** Remove one or multiple devices from the database.
- **Update software:** Load new software to one or multiple devices.
- **Monitor device status:** See the online status of devices. Enable device status logging for troubleshooting purposes.
- **Restart devices:** Restart one or multiple devices.
- **Open the device's web interface:** The web interface that can be used for configuration.

Device license

On the **License** tab in the **Device properties** dialog, it is possible to select which SafeCom features should be enabled on the device in question.

The checked features are only accepted if the license key code allows the device features.

Click **License** to open the **License** dialog to see if the license key code allows the additional features to be enabled for this device.

Add device

1. Begin the process of adding devices by performing one of the following steps:
 - Right-click in the device list and select **Add device**.
 - In the **Devices** menu, click **Add device**.
 - Click the **Add device** button.
 - In **System overview**, click **Add device** (only present on single servers).

You need to know the IP address of the device. Alternatively, you may try to [broadcast for the device](#).

The Add Device Wizard appears.

2. Enter the device address (hostname or IP address) and SNMP community name, then click **Next**.

Information is retrieved from the device to establish the type of device.

3. Click **More information** to see additional details.
4. If you agree with the type of device, click **Next**. Otherwise, click **[change]** to change the SafeCom type.
 - **SafeCom Go in the device**
 - **SafeCom Go/SafeCom Device Server**
 - **SafeCom Go/SafeCom Controller**
 - **SafeCom Tracking device** (see [SafeCom Tracking](#))

i If you select any device under **SafeCom Go/SafeCom Device Server** or **SafeCom Go/SafeCom Controller**, you are prompted for the IP address or hostname of the MFP. You are also prompted for the user name and password needed to log in to the MFP.

5. Click **Next**.
6. On the **Settings** tab, specify the properties of the device.
 - **Duplex supported**
 - **Color supported**
7. Click **Add** to register the device and save it in the database.

If the SNMP community name is public, no further steps are required. In any other case, proceed to step 8.
8. Locate the scDevMonSettings.ini file in your SafeCom installation directory.
9. Create the [SNMPCommunityNames] heading, and add the SNMP community name of the device in the following format:

```
<device IP address>=<SNMP community name>
```

Resend configuration

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

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

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

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

Add a device to a SafeCom Device Server


Before adding a device server device in SafeCom Administrator, a SafeCom Device Server must be added to the **Device server** container in the left menu.

If the relevant device server is already added in the SafeCom Administrator, go to [Add device server device](#).

Add device server and device server device

If the SafeCom Device Server is installed on the same machine where the SafeCom server is installed, it is automatically added to the Device Server section of SafeCom Administrator.

If the SafeCom Device Server is installed on a separate workstation, you must log in to the Device Server web page, and specify the SafeCom server there.

 To delete the device server again, right-click the device server and select **Delete device server**.

The SafeCom Device Server is now added to SafeCom Administrator and you can now add a device (see [Add device server device](#)).

Add device server device

1. Click the **Devices** container.
2. Right-click the content area and click **Add device**.
The **Add Device Wizard** is launched.
3. From the **Device server** drop down menu, select the relevant SafeCom Device Server and click **Next**.
Information is retrieved from the device server to establish the status of the device server.
4. Click **Next**.
5. Enter the **Printer address** (the device IP address or host name) and click **Next**.
Information is retrieved from the device.
6. Click **Next**.
7. Select the type of device and click **Next**.
8. Enter the username and password as specified on the device web page and click **Next**.
The device properties dialog opens.
9. Make sure to specify on the **Settings** tab the device server and the properties of the device (duplex and color supported), and ensure that the **SNMP community name** is correct.
10. Click **Add** to register the device and save it in the database.
After approximately 2 minutes, the device is added to the device server and is available to be configured in the SafeCom Device Server.

The device server device is now added and listed both under **Devices** in SafeCom Administrator and on the Device Server webpage.

Print QR code for Mobile Pull Print


Allow users to Pull Print documents through their smart phone by printing a QR code for each device. Users can scan the QR code label at the device with their phone, thus identifying themselves and declaring their presence at the specific device.

The users must have a smart phone with the SafeCom Mobile Pull Print app for Android or iOS installed (you can download the app from the relevant app store). For more information about the Mobile Pull Print, refer to *SafeCom Mobile Print Administrator's Guide*.

 SafeCom Mobile Pull Print requires SafeCom G4 and SafeCom Device Server.

Generate a QR code for a device:

1. In SafeCom Administrator, browse to the specific device.
2. Right-click the device and select **Generate QR code**.
3. In the **QR code for device** dialog, specify the print size and edit the text as appropriate.
4. Click **Print QR code**.
5. Make the QR label available at the device for users to scan.

 Make sure the default domain is specified for the device on the device server web page, as the users are not prompted for domain when logging into a device using a smart phone. If the default domain is not specified, but the users are required to use domains, they can enter the domain with their username (domain\username).

For more information about using pull print, refer to *SafeCom Mobile Print Administrator's Guide*.

Find devices

Once a device has been registered, you can use the Find function in SafeCom Administrator to find it.

1. Click the **Find** button.
2. Change **Search in** to **Devices**.
3. Enter text in **Look for** and click **Find now**.

The Find function uses case insensitive, free-text search.

- Click **Retrieve all** to display all registered devices.
- Click **Broadcast** to broadcast for devices.

Alternatively, you can click **Find** to open the **Find devices** dialog.

The **Find devices** dialog can be used with simple (see [Simple search](#)) or advanced (see [Advanced search – Device licenses](#)) search settings. The latter is very useful if you want to search for devices based on their use of device licenses.

Simple search

The **Find devices** dialog opens in **Simple search** mode by default.

1. Enter your search criteria and click **Find**.

The Find function uses field-based, case insensitive, free-text search.

The search result appears with information about version and online status.

2. Click the column label to sort the result.

- If you would rather see what license is in use by the different devices, you can right-click in the device list and select **Show device license**.

Advanced search – Device licenses

The **Advanced** option in the **Find devices** dialog makes it possible to search for devices based on their use of device licenses.

The following steps show an example of an advanced search:

1. Choose from the following options:

- To find all devices that use a Pull Print license, change **Pull Print** to **Yes**.
- To find all devices that do not use a Client Billing license, change **Billing** to **No**.

2. Enter your search criteria and click **Find**.

The **Find** button uses field-based, case insensitive, free-text search.

The search result appears with information about what license is in use by the different devices.

3. Click the column label to sort the results.

- If you would rather see the version and online status of the devices, you can right-click in the device list and clear **Show device license**.

Broadcast for devices

1. Click the **Find** button and select **Devices**.

2. Click **Broadcast**.

If a device does not appear, it can be because it is powered off, not connected, or not reachable, because the network setup is not reflected by the list of broadcast addresses (see [Network](#)). If the device does not appear, see [SafeCom Administrator: Unable to locate all SafeCom devices](#).

Customize the device list view

1. In the device list, right-click one of the column headers, such as **Device name**.
2. Select the properties that you want to appear as columns.

Edit the properties of multiple devices

1. Use **Find devices** to get a list of relevant devices.
2. Perform one of the following steps:
 - To select consecutive devices, click the first device, press and hold down Shift, then click the last device.
 - To select non-consecutive devices, press and hold down Ctrl, then click each device.
 - To select all devices in the window, press Ctrl + A.
3. Press Alt + Enter or right-click the selected devices, then select **Device properties**.
4. Make the required changes on the **Settings** and **Charging scheme** tabs.
 - On the **Settings** tab, it is possible to edit the following properties:
 - **Model**
 - **Home server**
 - **Org. unit**
 - **Location**
 - **Duplex supported**
 - **Color supported**
 - **Restricted access**
 - **Disable Pay for Print**
 - On the **Charging scheme** tab, it is possible to edit all properties.
 - On the **License** tab, it is also possible to edit all properties.
5. Click **OK**.

When editing multiple properties, the following legend applies:

- Check boxes can have three states: Checked, clear, and dim. If it is dim, it is because the selected devices have different properties.
- Fields are shown with a light gray background and the text N/A in black if the selected devices have different properties.
- Drop-down lists are shown with a light gray background with the first element in the list.

Delete devices

1. In the device list, select the devices you wish to delete.
2. Perform one of the following steps:
 - Right-click the selected devices and select **Delete device**.
 - On the **Devices** menu, click **Delete device**.
 - Press the Delete key.

Import Ethernet Card Readers

You can import multiple Ethernet Readers through a comma-separated CSV file. The first column is the IP address of the card reader, the second is the **Home Server**, the third is the **Secondary Server** (optional), and the fourth is the network address of the controlled device.

i For **Home Server** and **Secondary Server**, use the values you set when adding those to SafeCom Administrator. You can check these under **Server properties** (see [Server](#)).

Update software

- In the device list, select the devices you wish to update.
The settings of the device are preserved during the software update.
- Perform one of the following steps:
 - Right-click the selected devices and select **Update software**.
 - In the **Devices** menu, click **Device properties**, then in the **Device properties** dialog, click **Update software**.
 - Update the SafeCom Controller through FTP.
- Select **Online status** (see [Monitor device](#)) in SafeCom Administrator to ensure the device is powered on and ready to receive updated software.


SafeCom Controller	Software (*.b80)
SafeCom Controller Sharp OSA-enabled MFP, Xerox EIP-enabled MFP	508xxx
SafeCom Controller 3 Port	312xxx
SafeCom Controller 1 Port	304xxx

SafeCom Device Server	Software
Fuji Xerox ApeosPort III-IV MFP, HP LaserJet device with OXP and FutureSmart, Konica Minolta OpenAPI-enabled MFP, Sharp OSA-enabled MFP, Xerox EIP-enabled MFP	No software on the device

Canon MFPs	Software (*.lic, *.jar)
Canon MEAP-enabled MFP	010xxx

HP MFPs and printers	SafeCom Go HP (*.b49, *.b89, *.uin)
CP4025, CP4525	151xxx
P3015	150xxx
CP3525	141xxx
CM3530 MFP	140xxx

HP MFPs and printers	SafeCom Go HP (*b49, *.b89, *.uin)
CM6030 MFP, CM6040 MFP, CM6049 MFP	132xxx
CP6015	131xxx
P4014, P4015, P4515	130xxx
CP3505	121xxx
CM8050 MFP, CM8060 MFP	120xxx
P3005	111xxx
M3035 MFP, M4345 MFP, M4349, MFP CM4730 MFP, M5035 MFP, M5039 MFP, M9040 MFP, M9050 MFP, M9059 MFP, 9250C Digital Sender	110xxx
3000, 3800	102xxx
4730mfp	101xxx
4700	100xxx
4345mfp, 9040mfp, 9050mfp, 9500mfp	090xxx
2410, 2420, 2430, 4250, 4350	081xxx
9040, 9050	080xxx
4650, 5550	075xxx

 SafeCom Go HP software can only be updated if a password is set for the admin account.

Lexmark MFPs and printers	SafeCom Go Lexmark (*.fls)
X463de, X464de, X466de, X466dte, X466dwe, X651de, X652de, X654de, X656de, X658de X734de, X736de, X738de, X738dte, X860e, X862e, X864e	021xxx
X642e, X644e, X646e, X646ef, X646dte, X782e, X782e XL, X850e, X854e, X940e, X945e	012xxx
T656dne	121xxx

Ricoh MFPs and printers	SafeCom Go Ricoh (*b87, *.uin)
SP C320DN, SP C430DN, SP C431DN	150xxx
MP C300, MP C400, MP C2051,MP C2551, MP C3001SP, MP C3501SP, MP C4501SP, MP C5501SP, MP C6501SP, MP C7501SP	147xxx
SP 4210N, SP C820DN, SP C821DN	110xxx
MP 6001, MP 7001, MP 8001, MP 9001, Pro 907EX, Pro 1107EX, Pro 1357EX	100xxx
MP 2851, MP 3351, MP 4001, MP 5001, MP C2050, MP C2550, MP C2800, MP C3300, MP C4000, MP C5000	090xxx

Ricoh MFPs and printers	SafeCom Go Ricoh (*.b87, *.uin)
SP C420DN	080xxx
MP 2550, MP 3550, MP 4000, MP 5000, MP C6000, MP C7500	060xxx
MP 1100, MP 1350, MP 5500, MP 6000, MP 6500, MP 7000, MP 7500, MP 8000, MP 9000, MP C2000, MP C2500, MP C3000, MP C3500, MP C4500 Pro906EX, Pro1106EX, Pro1356E	030xxx
MP 2510, MP 3010, MP 3500, MP 4500, 2051 (DSm651), 2060 (DSm660), 2075 (DSm675), 3025 (DSm725), 3030 (DSm730), 3035 (DSm735), 3224C (DSc424), 3228C (DSc428), 3232C (DSc432), 3235C (DSc435), 3245C (DSc445), 3260C (DSc460), 5560C (CS555)	020xxx

Location of device software

SafeCom Administrator automatically picks the latest software version for updating if the files are located in the `device_software` subfolder to where you installed the SafeCom G4 Server software. Normally:

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

Single device software update

1. Open the **Device control** dialog as described in [Import Ethernet Card Readers](#).
2. Specify the **Software file** or **Browse** to it.
3. Click **Start** to begin the software update process.
If you are updating a SafeCom Go HP software, the **Device Authorization** dialog appears.
4. Enter **User name** admin and the **Password**.
5. Click **Close** when the software update processes is completed.
 - After the process completes, you can click **View log** to see the details.
 - If the update process fails, try again.

If you are updating a SafeCom Go product, you should refer to the relevant *SafeCom Go Administrator's Guide* (see the list in [Related documentation](#)) for troubleshooting hints.

Multiple device software update

1. Select multiple devices, then open the **Device control** dialog as described in [Import Ethernet Card Readers](#).
 2. Specify the **Software files** for each type.
 - a. Select **<specify software file>** and click the browse button ([...]) to launch the **Open** dialog.
 - b. Browse to and select the software update file that matches the selected type. Repeat this step for each device type.
- Max connections** specifies the maximum allowed devices that can be updated simultaneously. When you open the dialog, the maximum connections is set to 10. You can specify a maximum


of 1, 5, 10, 20, 50, or 100 connections. This limit is to ensure that the software update process does not occupy all the network bandwidth.

3. Click **Start** to begin the software update process.
If you are updating a SafeCom Go HP software, the **Device Authorization** dialog appears.
4. Enter **User name** admin and the **Password**.
5. Click **Close** when the software update processes has been completed for the selected devices.
 - If the update process fails, try again or refer to the *Troubleshooting* chapter in the appropriate *SafeCom Go Administrator's Guide* (see the list in [Related documentation](#)).

Monitor device

Monitor the status of the SafeCom devices from within the SafeCom Administrator using one of the following methods:

- **Online status** (simple): In the **Devices** pane, right-click any of the headers (**Device name**, **IP address**, or other) and select **Online** to enable status for all devices. Press F5 to retrieve device status.
- **Device status logging** (troubleshooting): Device status logging allows monitoring reboots, uptime, and response time of selected SafeCom devices. It can be very useful for troubleshooting. Follow the steps below to start device status logging.

 Device monitoring requires a full SafeCom G4 installation to work. If only a tool installation is used, the required service is not included, thus the Device Monitoring feature cannot be taken into use.

Start the device monitor

1. In the **Devices** menu, click **Monitor setup**.
The **Device Monitor** dialog appears.
2. Set the **Poll interval**.
The default value is 5 minutes.
3. Click **Start** to launch the scDevMonServer.exe process.

Enable monitoring on selected devices

1. Use **Find devices** to get a list of relevant devices.
2. In the **Devices** pane, right-click any of the headers (**Device name**, **IP address**, or other) and select one of the following:
 - **Monitored status**: Makes the **Monitored** column appear. An "x" indicates that the device is monitored and a dash ("-") indicates that the device is not monitored.
 - **Monitoring**: Allows you to control what details should be presented in the columns. Select from **Reboots**, **Uptime**, **Avg. ping**, and **Normal ping**. Select **All** to select all of the above.
3. Right-click a device and click **Monitor device**.

Look at device statistics

1. Open the **Device properties** dialog.
2. Click the **Statistics** tab.
The statistics tab does not appear if multiple devices are open.
A textual representation of the statistics is shown.
3. Select **Graphical** to see a graphical representation of the statistics.

Restart devices

Restart devices from within SafeCom Administrator by performing one of the following steps:

- Right-click in the device list and select **Restart**.
- In the **Device** menu, click **Restart**.

Open in web browser

The SafeCom devices have a web interface that can be used for configuration.

Open the web interface by performing one of the following steps:

- Right-click in the device list and select **Open in web browser**.
- In the **Device properties** dialog (see [Settings](#)), click **Open in browser**.

Restrict user access to devices

1. Build an organizational tree by adding org. units as required (see [Organizational units](#)).
2. Associate users and devices to the org. units.
3. Select **Restricted access** in the **Device properties** dialog of the intended devices (see [Settings](#)).

DHCP server

You can assign a fixed IP address in the DHCP server. If you know the MAC address, you can log in to the DHCP server to determine which IP address has been assigned. The MAC address of the SafeCom Controller is printed on the white label on the bottom of the SafeCom Controller. The MAC address is a 12-digit hexadecimal number.

Example: Example

```
00C076FF00F2
```


Shorten job names in document list

Redundant text, such as Microsoft Word, Microsoft Excel, and http:// can be excluded from the job name that appears in the **Document list** in the SafeCom Front-end (available as the first action after you click **MORE**) and in the device's control panel if SafeCom Go is used.

The text to exclude is controlled by the ExcludeJobNames.txt file located in the %SafeCom%\Templates folder. The %SafeCom% indicates the SafeCom installation folder, normally:

C:\Program Files\SafeCom\SafeComG4

1. Copy the ExcludeJobNames.txt file from the %SafeCom%\Templates folder to the %SafeCom% folder.
2. Modify the ExcludeJobNames.txt file in the %SafeCom% folder to match your requirements.
3. Restart the SafeCom service (see [Start and stop the SafeCom service](#)).

 Subsequent modifications to the file in the %SafeCom% folder take immediate effect.

ExcludeJobNames.txt

```
-----  
; This file specifies text to be excluded from  
; job names in the SafeCom Front-end.  
;  
; Text is excluded if appearing as the first part  
; of the job name.  
;  
; (c) 2003 SafeCom  
-----  
Version="1"  
Item="Microsoft Word - "  
Item="Microsoft Excel - "  
Item="http://"
```


Chapter 8

SafeCom Tracking

The SafeCom Tracking makes it possible to track print and MFP usage and costs on a per device and user basis.

You can use [SafeCom Reports](#) to view tracking data and generate reports.

Pull print tracking

Pull print tracking makes it possible to track print costs on SafeCom Pull printers. Tracking is performed by the special port monitor SafeCom Pull Port.

The Pull print tracking process is as follows:

1. The SafeCom Pull Port analyzes the document in regards to number of pages, paper size, and possible use of color and duplex.
2. The SafeCom Pull Port transfers the document and the resulting tracking data to the SafeCom server. The document remains on the SafeCom server until the user collects it. Documents that are not collected are automatically deleted after a configurable time.
3. When the user collects the document, the price is calculated based on the charging scheme of the selected device. If **Post track** is enabled, the tracking data can be adjusted according to the information that is available from the device at print time.

Push print tracking

Push print tracking makes it possible to track print costs without installing dedicated SafeCom hardware. Push print tracking requires the use of the special port monitor SafeCom Push Port.

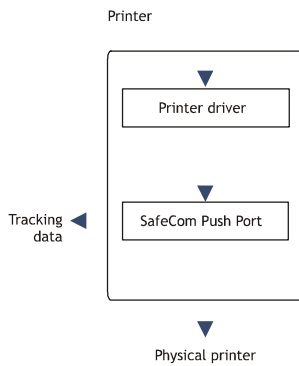
The Push print tracking process is as follows:

1. The SafeCom Push Port analyzes the document with regards to number of pages, paper size, and the use of color and duplex.
2. The SafeCom Push Port transfers the resulting tracking data to the SafeCom server where the data is registered under the appointed tracking device, and the price is calculated based on the charging scheme.
3. The SafeCom Push Port can be configured as follows:
 - **Print directly:** The document output is moved directly to the physical device's TCP (port 9100). See [Printing directly](#).

- **Print through a second printer:** The document is forwarded to the port monitor of a second printer, which, in turn, moves the document output directly to the physical device. The second printer is also called the output device. See [Printing through a second printer](#).

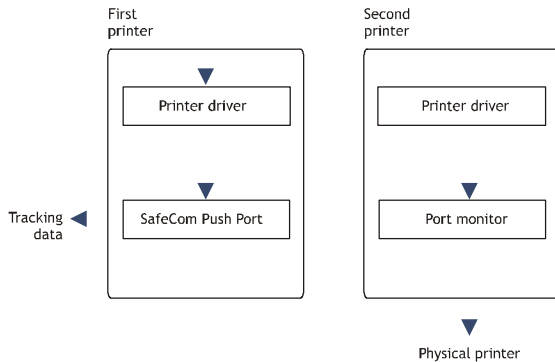
Printing directly

The method of printing directly is illustrated below.



Printing through a second printer

The method of printing documents through a second printer (output device) is illustrated below:



When printing through a second printer, the printer driver of the first printer formats the document, whereas the printer driver of the second printer (the output device) is not used.

The port monitor on the second printer communicates directly with the physical printer. This concept gives you the freedom to use your printer vendor supplied port monitor. Port monitors may support such protocols as: LPR, TCP (port 9100), DLC, PjL, AppleTalk, or SCSI.

Only the first printer should be shared. Sharing the secondary printer would enable users to bypass tracking.


i There must be one instance of the SafeCom Push Port per physical printer on each machine.

Add a secondary printer (output service)

As explained above, the SafeCom Push print concept involves two print queues: printing directly or printing through a secondary printer.

In the following part, it is described how to add a secondary printer (output service).

1. Open the Windows Control Panel and browse to Printers.
2. Open the Add Printer Wizard.
3. Click **Add a local printer**.
4. Choose an existing port that is used to connect to the printer, then click **Next**.
5. Click **Have Disk**, browse to install the files from the printer manufacturer's installation disk (or download the files from the manufacturer's web site), then click **OK**.
6. Click **Next**.
7. Enter a **Printer Name**, then click **Next**.
8. Select **Do not share this printer**, then click **Next**.


 Do not make this printer your default Windows printer.

9. Click **Print a test page** to verify the system.
10. Click **OK** when prompted to confirm that the test page printed correctly, then click **Finish**.

Add the first printer (SafeCom Push Port)

If you are printing directly via TCP/IP port 9100, follow these steps to add the first printer (SafeCom Push port).

1. Open the Windows Control Panel and browse to Printers.
2. Open the Add Printer Wizard.
3. Click **Add a local printer**.
4. Choose **Create a new port** and select **SafeCom Push Port** from the drop-down list. Click **Next**.
5. Enter a unique name of your choice for the port in **Port Name**, then click **Next**.
The **Configure Push Port** dialog appears.
6. In **Servers**, click **Edit servers** to add, remove, change, or test the connection to the SafeCom server.

 It is not possible to edit an entry on the SafeCom server list in the **Edit servers** dialog. Instead, you have to remove the server and then add a new one.

7. Set up the user authentication as required according to the following descriptions:
 - Select **Use network logon** to use your Windows logon as your SafeCom user logon when printing.
 - Select **Use specified logon** and enter the SafeCom user logon of the user who is to receive all future prints sent to the print queues that use this push port. This can be combined with **Group print** by specifying the name of the group instead of the name of a user.

- Select **Show authentication dialog at every print** if the user should be prompted every time they print. SafeCom PopUp must be running on the user's computer to show the dialog that prompts for the login (see [SafeCom Print Authentication dialog](#)). Up to 10 minutes may elapse before the choice takes effect. The time is configured by the Windows registry setting CacheExpireSuccess.
 - Select **Show authentication dialog on first print only** if the user should only be prompted the first time they print. SafeCom PopUp must be running on the user's computer to show the dialog that prompts for the login (see [SafeCom Print Authentication dialog](#)). Up to 10 minutes may elapse before the choice takes effect. The time is configured by the Windows registry setting CacheExpireSuccess.
 - Select **Use job data logon** to extract the logon from the job data (see [Configure Use job data logon](#)).
 - Select a default domain to save the user from entering a domain.
8. In **Output device**, select **Use printer IP address or hostname** and specify the IP address if you are printing directly.
 9. Click **Test connection** to display the **Printer Properties** dialog and to test the connection to the printer.

The printer must be online and allow SNMPv1 access via UDP port 161. Otherwise, you get the message: "Not able to connect to printer".

i If you are printing through a second printer, you need to select **Select the printer that this port will use as output device** and select one of the output devices.

10. Select **SNMP status enabled** if you want SNMP status to be reported.
11. In **Select printer for tracking**, select **Select printer from list** and choose a tracking device.
 - Alternatively, select **Auto-create printer** and enter a **Printer name** and an optional **Printer location**.
12. In the **Miscellaneous** section, select according to the following descriptions:
 - **Show job price before printing:** Check if users are to unconditionally see a dialog with the cost of the document before they print. If the printer is a shared, printer users must have SafeCom PopUp (see [Setup SafeCom PopUp](#)) set up and running on their computer to confirm that they wish to print the document.
 - **Override user cost code:** The specified cost code overrides the cost code of the user who prints. Example: If John Smith has the cost code 2949 and prints to a Push Port where a cost code of 1009 is specified, the resulting UserCostCode parameter in the tracking record shows 1009 and not 2949.
 - **Override driver name:** The specified driver name overrides the driver name supplied by the printer driver. This is particular useful to differentiate printers using the HP Universal Print Driver.
 - **Hide document name:** Select this option to enable hiding document names in the print queue. This allows for more secure printing, as it eliminates the chance of unauthorized people seeing the original document names. These names appear encrypted.

i If printer pooling is enabled, all printers of the same print queue must have the same value for this setting.

13. Click **OK**.

The **Authorize port configuration** dialog opens.

14. Enter **User logon** and **Password** for a user with SafeCom Administrator or Technician rights, then click **OK**.
15. Click **Have Disk**, and in the **Install From Disk** dialog, browse to the files from the printer manufacturer's installation disk (or download the files from the manufacturer's web site), then click **Next**.
16. Enter a **Printer Name** and click **Next**.
17. Select **Share this printer** and enter **Share name** (P101), then click **Next**.
18. Set up whether this printer should be your default Windows printer.
19. Click **Print a test page** to verify the system.
20. Click **OK** when prompted to confirm that the test page printed correctly.
21. Click **Finish**.
22. Check the properties of the printer:
 - a. Back in the Control Panel, right-click the printer, then click **Printer Properties**.
 - b. On the **Device Settings** tab, check the settings, such as paper size in the trays and installable options.
 - c. On the **Advanced** tab, select **Start printing after last page is spooled**. This is required for the tracking and billing information to be correct, while it also allows faster spooling.
 - d. Click **OK**.

Set TCP port to a custom value

The SafeCom Push Port, by default, prints directly to port 9100. However, this can be changed by performing the following steps:

1. Stop the SafeCom service and the Print Spooler.
2. Open the Registry Editor and browse to:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Print\Monitors\SafeCom Push Port\Ports
```
3. Browse to the relevant instance of the port.
4. Right-click **Output Ip Port** and select **Edit**.
5. Change the value from 9100 to the TCP port value to be used, then click **OK**.
6. Exit the Registry Editor.
7. Start the SafeCom service and the Print Spooler.

Allow printing at all times

The port monitors allows printing during server errors by default. The behavior can be controlled through the Registry Editor.

It is possible to create and specify an overall AllowPrintOnServerError setting for the SafeCom Push Port. A setting like this also prevents dropping print jobs in case the SafeCom Push Port refers to a nonexistent tracking device.

1. Stop the SafeCom service and the Print Spooler.

2. Open the Registry Editor and browse to:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Print\Monitors\SafeCom Push Port\Ports
```

3. Create a new DWORD called AllowPrintOnServerError.

It can take the following values:

- 0: Do not print during a server error.
- 1: Allow printing during a server error (default).

4. Exit the Registry Editor.
5. Start the SafeCom service and the Print Spooler.

The overall AllowPrintOnServerError setting takes effect when local PrintOnJdbError for the SafeCom Push Port has a value of 2.

Change the port-specific PrintOnJdbError setting

1. Stop the SafeCom service and the Print Spooler.
2. Open the Registry Editor and browse to:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Print\Monitors\SafeCom Push Port\Ports\{port}
```

3. Choose from one of the following values:
 - 0: Do not print during a server error.
 - 1: Allow printing during a server error.
 - 2: Use the overall setting AllowPrintOnServerError (Default).
4. Browse to the relevant instance of the port.
5. Right-click **PrintOnJdbError** and select **Edit**.
6. Change the value, then click **OK**.
7. Exit the Registry Editor.
8. Start the SafeCom service and the Print Spooler.

SafeCom Port Configurator

SafeCom Port Configurator is a wizard-based tool for converting existing TCP/IP printers²¹ to SafeCom Push printers and revert SafeCom Push printers back to their original TCP/IP settings. The tool allows viewing printers in the domain and easily launching the Port configuration dialog for TCP/IP, Push, and Pull printers. The selected settings in the [scPortConfigurator.ini](#) file can be customized to match the behavior of the SafeCom Port Configurator.

Install SafeCom Port Configurator

SafeCom Port Configurator can be installed in the following ways:

- **Server installation:** It is always installed during a server installation.

²¹ A TCP/IP printer is a Windows print queue that uses the standard TCP/IP port monitor.

- **Tool installation:** Optionally, when doing a tool installation, check **SafeCom Port Configurator**. If you intend to perform a client and a tool installation on the same computer, you should do the [client installation](#) first.

The SafeCom installation files are copied to the SafeCom installation folder.

The default is:

C:\Program Files\SafeCom\SafeComG4

Start SafeCom Port Configurator

The SafeCom Port Configurator enables you to:

- **Convert to Push:** Convert existing TCP/IP printers to SafeCom Push, allowing SafeCom Tracking and SafeCom Rule Based Printing.
- **Restore to TCP/IP:** Restore printers converted to SafeCom Push back to their original TCP/IP settings.
- **List and repair printers** (see [List printers in the domain](#) and [Repair push printer](#)): List printers in the domain and reconfigure them.

To start the SafeCom Port Configurator, perform the following steps:

1. Click **Start** and point to **All Programs**.
2. Click **SafeCom G4** and **SafeCom Port Configurator**.
 - Alternatively, click `scPortConfigurator.exe` if a separate installation (see [Install SafeCom Port Configurator](#)) was performed.


The SafeCom Port Configurator Wizard appears.

3. Choose the task you want to perform.

Add server

The SafeCom Port Configurator, by default, lists printers on the local server only. To use it to convert, restore, and list printers on other servers, you must add these servers to the list of servers. The list of servers is saved to and read from a file (see [Read servers from file](#)).

1. Start SafeCom Port Configurator (see [Start SafeCom Port Configurator](#)) and select one from the following actions:
 - **Convert to Push**
 - **Restore to TCP/IP**
 - **List and Repair Printers**
2. Once you are logged in, click **Add server**. The **Add server** dialog appears.
3. To add only one server, select **Single**, enter the server host name or IP address, then click **OK**.

 If the server is clustered, you must refer to the virtual server.

4. To add multiple servers, select **Multiple**, select the domain, then click **OK**.

Once a server has been added, it is stored in a file. In section [scPortConfigurator.ini](#), it is covered how to customize behavioral settings of the SafeCom Port Configurator.

If you wish to remove a server, open the file and remove the row containing the appropriate servers (see [Read servers from file](#)).

Convert to Push


To convert existing TCP/IP printers to SafeCom Push:

1. [Start the SafeCom Port Configurator](#).
2. Select **Convert to Push**, then click **Next**.
3. Enter the **SafeCom Server**, the **SafeCom User name**, and the **Password** in the **SafeCom Login** dialog, then click **Next**.

 The SafeCom user needs to have SafeCom Administrator or Technician rights.

The **Convert to Push** dialog appears with one or more servers, including **Local Machine**.

4. Log in by using one of the following methods:
 - Press Shift + Click on a listed server. This prompts you to log in to the server with your **Windows user name** and **Password**.
 - Click a print server to log in as the user you are already logged in with.²² If the server is part of a domain and you are already logged into the domain, then you are logged in directly. Otherwise, you are asked to log in with your **Windows user name** and **Password**.


 If the Windows user running the application has administrative rights on the clicked print server (or its domain), then both shared and non-shared (local) printers will be listed. However, if the user has no elevated rights in the machine (or domain), then only public (local) TCP/IP printers will be listed.

A public printer is a print queue that has been made shared, and at the same time has **Allow** checked for **Print for Everyone** on the **Security** tab in the **Properties** dialog.

- Log in as a domain user by specifying the domain followed by a backslash (\) and the **Windows user name**. Example: MYDOMAIN\JS. Alternatively, you can specify user logon followed by (@) and the domain, like this JS@MYDOMAIN.

If the server does not appear in the list, then add a new server by clicking [Add server](#).

5. Check the printers to be converted from TCP/IP to Push, then click **Next**.
The **Push Port Configuration** dialog appears.
6. Make changes to the Push Port Configuration according to the descriptions below or leave the default settings.

 Ensure that your printer name is shorter than 50 characters to avoid possible configuration issues.

²² There are no specific error messages for failed logons: The program does not distinguish between a misspelled username/password and a successful logon of a user with no rights to "see" (server-enumerate) the printers.

User authentication

- Select **Use network logon** to use the Windows logon as the SafeCom user logon when printing.
- Select **Use specified logon** and enter the SafeCom user logon of the user who is to receive all future prints sent to the print queues that uses this push port. This can be combined with **Group print** by specifying the name of the group instead of the name of a user.
- Select **Show authentication dialog at every print** if the user should be prompted every time they print. SafeCom PopUp must be running on the user's computer to show dialog that prompts for the login (see [SafeCom Print Authentication dialog](#)). Up to 10 minutes may elapse before the choice takes effect. The time is configured by the Windows registry setting CacheExpireSuccess.
- Select **Show authentication dialog on first print only** if the user should only be prompted the first time they print. SafeCom PopUp must be running on the user's computer to show the dialog that prompts for the login (see [SafeCom Print Authentication dialog](#)). Up to 10 minutes may elapse before the choice takes effect. The time is configured by the Windows registry setting CacheExpireSuccess.
- Select **Use job data logon** to extract the logon from the job data (see [Configure Use job data logon](#)).
- Select a default domain to save the user from entering a domain.

Select **Show job price before printing** if users are to unconditionally see a dialog with the cost of the document before they print. If the printer is a shared printer, users must have SafeCom PopUp (see [SafeCom PopUp – scPopUp.exe](#)) set up and running on their computer in order to be able to confirm that they wish to print the document.

Select **Override user cost code** and enter the cost code to have the specified cost code override the cost code of the user who prints. Example: If John Smith has the cost code 2949 and prints to a Push Port where a cost code of 1009 is specified, the resulting UserCostCode parameter in the tracking record shows 1009 and not 2949.

Select **Override driver name** and enter the driver name to have the specified driver name override the driver name supplied by the printer driver. This is particularly useful to differentiate printers using the HP Universal Print Driver.

In **Sharing**, you can select **Make sure printer is shared** (default) or select **Do not change share** to leave it as is.

7. Click Next.

One of the following dialogs opens:

- **Printer not registered in SafeCom server** (default): Create a tracking device in the SafeCom server. If this dialog appears, perform step [8](#).
- **Printer already registered in SafeCom server**: A tracking device with a matching MAC address is already registered in the SafeCom server and it is suggested to use that. If this dialog appears, perform step [9](#).

8. Select one of the radio buttons in the dialog.

- **Create in SafeCom, a new device to track this printer** if your SafeCom solution is Push Print solution only.
- **Skip reconfiguring the print queue for this printer** if your SafeCom solution includes Pull Print and you wish to add the printer as a Pull Printer to the SafeCom solution first. This way, both Pull and Push print activity get associated with the same tracking device in the SafeCom solution.

Skip to step 10.

9. Select one of the radio buttons in the dialog.
 - **Merge print tracking with already existing SafeCom device** if you wish to have all tracking registered under the same tracking device. The match is done based on the physical printer's MAC address.
 - **Create in SafeCom, a new device dedicated to track only Push jobs sent to this printer** if you want jobs coming from this particular print queue with a dedicated tracking device.
10. Select **Do not ask again** if the choices are to apply in conversions made during this session.
11. Click **Next**, then click **OK** in the dialog that appears with information about the number of converted printers.


The **Continue** dialog appears.
12. Select one of the radio buttons in the dialog.
 - **No, I have finished setting up printers** if you have finished, then click **Next** to close the SafeCom Port Configurator.
 - **Yes, I'd like to reconfigure more printers for Push printing** if you wish to convert additional printers. Click **Next** to go to the **SafeCom Tracking** dialog described in step 4.

Restore to TCP/IP

To restore printers converted to SafeCom Push back to their original TCP/IP settings, perform the following steps:

1. [Start the SafeCom Port Configurator](#), then click **Next**.
2. Select **Restore to TCP/IP**, then click **Next**.


The **TCP/IP Printer Restore** dialog appears with one or more servers, including **Local Machine**.
3. Double-click a server to expand and to show the list of Push printers. Other types of printers (TCP/IP, Pull) do not appear in the list.

 SafeCom Port Configurator does not work with printers using Microsoft v4 Printer Drivers.

4. To see all printers on the server, press Shift + Click.

You are prompted to supply a **Windows User Name** and **Password**.

 - **Server NOT part of domain:** If the server is NOT part of the domain, you must supply **Windows User Name** and **Password** of a local administrator on the server.
 - **Server part of domain:** If the server is part of a domain and you are already logged into the domain, then you are logged in directly. Otherwise, you are asked to log in. Enter **Windows user name** and **Password**, then click **Login**.

 If the Windows user running the application has administrative rights on the clicked print server (or its domain), then both shared and non-shared (local) printers are listed. However, if the user has no elevated rights in the machine (or domain), then only public (local) Push printers are listed.

5. If the server does not appear in the list, click [Add server](#).
6. Select the printers to be restored to TCP/IP, then click **Next**.

Restoration is possible only if the printer has a **Yes** in the **Restorable** column.

A dialog appears with information about the number of reverted printers.

7. Click **OK** to go to the **TCP/IP Printer Restore** dialog in step 2.

List printers in the domain

The **List Printers** dialog lists the printers in the domain and enables you to reconfigure them.

1. Start the [SafeCom Port Configurator](#), then click **Next**.

2. Select **List Printers**, then click **Next**.

The **List Printers** dialog appears.

3. Click on a server to expand it to show the list of shared TCP/IP, Push, and Pull printers.

The **List Printers** dialog can also be used to identify Push Printers that are not referring to a valid tracking device (unknown device ID).

Repair push printer

The **List Printers** dialog can be used to identify Push Printers that are not referencing a valid tracking device (unknown device ID).

To Repair Push Printer, perform the following steps.


1. Start the [SafeCom Port Configurator](#) and click **Next**.

2. Select **List Printers**. Click **Next**.

3. Click **Repair Push** to repair the push printer.

A dialog appears with information about the number of push printers fixed.

4. Click **OK**.

 The new device has the Tracking license checked. If the SafeCom license key code is a permanent one, the Rule Based Printing, Client Billing, and Pay licenses are checked if there are any spare licenses. To control the use of licenses, open the **License** tab in the **Device properties** dialog.

Read servers from file

SafeCom Port Configurator can read servers from files. This may prove useful in installations where browsing the domain takes too long due to the number of servers or where the possibility to browse the domain is limited.

By default, the servers are read from the `svlist.csv` file located in the SafeCom Port Configuration installation folder. It is the same file that is used to record the servers that are added by clicking **Add server**.

Example `svlist.csv` file, where the first line (Host) is the header:

```
Host
server1
server2
```

In the `scPortConfigurator.ini` file, it is possible to control the name of the file.

```
[GENERAL]
ExternalServerList_FileName=srvlist.csv
```

If you wish to remove a server, open the `srvlist.csv` file and remove the row containing the servers to be removed.

scPortConfigurator.ini

An `scPortConfigurator.ini` file is produced to record information from the previous SafeCom Port Configurator session, including last used server, window sizes, and column widths.

Settings in the file are added as dialogs are used. Edit selected settings to customize the behavior of SafeCom Port Configurator. These settings are covered below:

- Push port name
- Tracking device name
- Tracking device settings
- Tracking device licenses
- Convert to Push dialog
- Restore to TCP/IP dialog
- List Printers dialog
- Smart Printer Driver dialog

Push port name

The default convention for naming Push ports is similar to the one used by the Standard TCP/IP port, except that `IP_` is replaced by `Push_`.

For example, if the IP address is `172.16.6.123`, the default TCP/IP port is named `IP_172.16.6.123` and the Push port is named `Push_172.16.6.123`.

In the `scPortConfigurator.ini` file, this is controlled as follows:

```
[PortReconfiguration]
NameForNewPort_use_PortType=1
NameForNewPort_use_QueueName=0
NameForNewPort_use_PrinterIP=1
```

The Push port inherits the print queue name if the settings are changed to:

```
[PortReconfiguration]
NameForNewPort_use_PortType=0
NameForNewPort_use_QueueName=1
NameForNewPort_use_PrinterIP=0
```

Tracking device name

The tracking device in the SafeCom solution, by default, inherits the name of the print queue. For example, if the print queue name is "myprinter", the tracking device is named "myprinter". To include additional information, change one or more of the below settings from 0 to 1.

```
[PortReconfiguration]
NameForNewTrackingDevice_use_QHostName=0
NameForNewTrackingDevice_use_QueueName=1
NameForNewTrackingDevice_use_PrtModel=0
```

```
NameForNewTrackingDevice_use_PrtIP=0
NameForNewTrackingDevice_use_PrtLocation=0
NameForNewTrackingDevice_TokenSeparator=' '
```

Tracking device settings

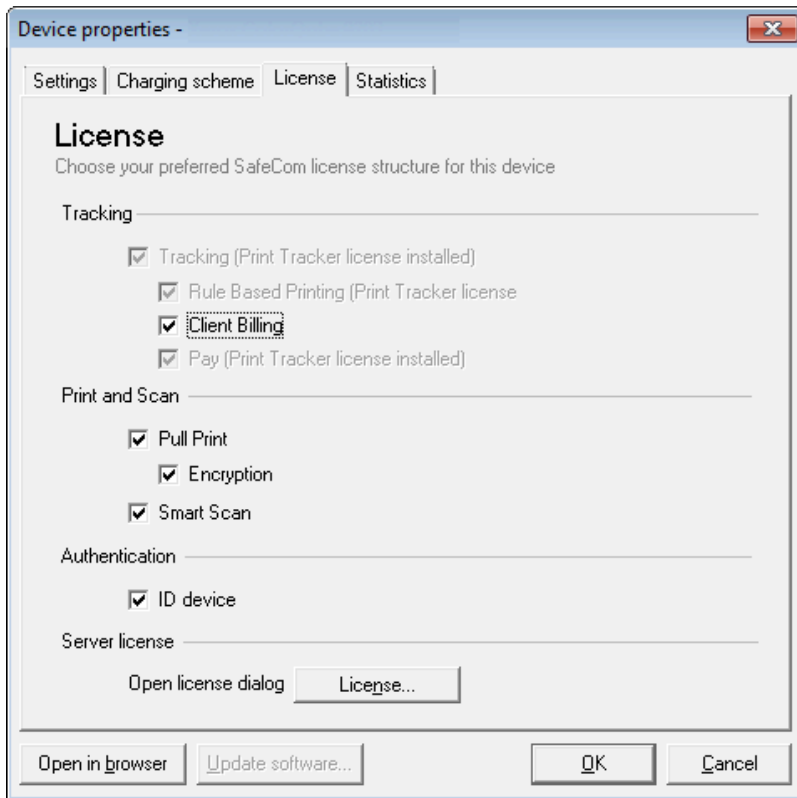
In the following part, it is described how the selected settings from the [CoScum] section map to the controls in the **Settings tab** in the **Device properties** dialog.

```
CoScum]
NewTrackingDevice_Default_DeviceIPAddress=127.0.0.1
NewTrackingDevice_Default_AllowPay=1
NewTrackingDevice_Default_AllowBilling=1
NewTrackingDevice_Default_RBP=1
NewTrackingDevice_Default_AllowPull=1
NewTrackingDevice_Default_AllowEncryption=1
NewTrackingDevice_Default_Duplex=0
NewTrackingDevice_Default_Color=0
NewTrackingDevice_Default_TreeNodeId=0
NewTrackingDevice_Default_DeviceTypeBitmask=2
NewTrackingDevice_Default_ServerId=-1
NewTrackingDevice_Default_DisablePayAndPrint=0
NewTrackingDevice_Default_RestrictedAccess=0
```

- **MAC** is pre-filled if the physical printer is online at the time of creation. Otherwise, it will read 00000000.
- **ID** is the database ID of the tracking device.
- **Name** is for specifying a name for the device (mandatory). This is, by default, the name of the print queue, but it can be customized to be composed of, for example, the **IP address** and **Model** (tracking device name).
- **Model** is for specifying the model and/or manufacturer of the device (optional). If the physical printer was online at the time of conversion, it is pre-filled. Otherwise, it is left blank.
- **Home server** is present only if SafeCom multiserver support is enabled. This can be controlled at the time of creation by setting `NewTrackingDevice_Default_ServerId`. The default is -1.
- **Org. unit** is the organizational unit the device belongs to. The default is 0. The setting `NewTrackingDevice_Default_TreeNodeId` does not control the ID of the org. unit.
- **IP address** is pre-filled if the physical printer was online at the time of creation. Otherwise, it defaults to the value specified by `NewTrackingDevice_Default_DeviceIPAddress`.
- **Capabilities** shows a number of check boxes depending on the device and the SafeCom license key code.
- **Duplex supported** is checked if the printer driver that is associated with the device supports duplex. The `NewTrackingDevice_Default_Duplex` is not used.
- **Color supported** is checked if the printer driver that is associated with the device supports color. The `NewTrackingDevice_Default_Color` setting is not used.
- **Restricted access**: The `NewTrackingDevice_Default_RestrictedAccess` setting is not used.
- **Allow Pay user** is only available if the server key license allows one or more Pay devices. The `NewTrackingDevice_Default_DisablePayAndPrint` is not used.
- **Push print** is checked by default.

Tracking device licenses

This image shows the **License** tab in the **Device properties** dialog in SafeCom Administrator.



When a tracking device is added, it always occupies at least a Tracking license. If the SafeCom license key code is permanent and Rule Based Printing is available, Client Billing and Pay licenses are also taken.

Convert to Push dialog

In the following part, it is described how the settings from the [PortReconfiguration] section affect the **Convert to Push** dialog and the subsequent conversion process.

```
[PortReconfiguration]
Default_Print_if_SafeCom_offline=2
GUIShowOption_Print_if_SafeCom_offline=0
Calculate_needed_tracking_licenses_before_converting_any_printer=1
Match_SCDevice_by_IP_if_TCPIP_MAC_unavailable=1
```

Default_Print_if_SafeCom_offline maps directly to the SafeCom Push Port's Windows registry setting **PrintOnJdbError**. It is recommended to leave it at the default 2 to use the overall setting **AllowPrintOnServerError**.

GUIShowOption_Print_if_SafeCom_offline can be set to 1 to include an additional check box in the **Push Port Configuration** dialog. The check box maps directly to the SafeCom Push Port's Windows registry setting **PrintOnJdbError**. The check box can have three labels and states:

- **If SafeCom offline: Use common registry setting.** This maps to `PrintOnJdbError=2`.
- **If SafeCom offline: Don't print.** This maps to `PrintOnJdbError=0`.
- **If SafeCom offline: Allow print.** This maps to `PrintOnJdbError=1`.

Calculate needed tracking licenses before converting any printer is 1 by default. By setting it to 0, there is no check to ensure that the SafeCom license key code includes the required device tracking licenses. The lack of device tracking licenses causes print jobs to be cancelled.

Match_SCDevice_by_IP_if_TCPIP_MAC_unavailable is used to control whether the device IP address can be used to determine if the device is already registered and if the **Printer already registered in SafeCom server** dialog should appear.

Restore to TCP/IP dialog

In the following part, it is described how the settings from the [RestoreTCPDialog] section affect the **Restore to TCP/IP** dialog and the subsequent restoration process.

```
MachinePingTimeOutMS=1000
CtrlClick_opens_remote_queue=1
SNMPWaitTimeoutMS_when_clicking_next=5000
Deserialize_remote_TCP_port_on_restore=0
```

List Printers dialog

In the following part, it is described how the settings from the [PrinterViewDialog] section affect the **List Printers** dialog (see [List printers in the domain](#)).

```
Update_scDevices_IP=1
Update_scDevices_MAC=1
Update_scDevices_Location=1
Update_scDevices_Model=1
MachinePingTimeOutMS=1000
```

Smart Printer Driver dialog

The setting **SmartPrintingReservedQueueNamePrefix=SafeCom-** regulates which TCP/IP queues are ignored. These queues are ignored and not converted when SafeCom Port Configurator is running.

i If the **SmartPrintingReservedQueueNamePrefix=** setting is empty, the Port Configurator ignores all queues.

scPortUtility

The SafeCom Port Configuration Utility (scPortUtility) is a command line tool that can be used to create SafeCom Push Ports or migrate existing Windows print queues to use SafeCom Push Port.

- Push Port creation
- Attach port
- Queue migration
- List print queues

The operations are specified on the command line as parameters.

Command line options can use quotation marks (") for option strings that include spaces.

The SafeCom Port Utility returns an exit code, indicating a success or failure of the operation. Exit codes are in the range 0-255.

For a detailed list of command line parameters and exit codes, see [scPortUtility operations and exit codes](#).

Simple Push Port creation

The following example creates a new push port called PRN-U134-PRT for the device with IP address 10.42.58.134. The port connects to the SafeCom server at 10.42.57.8.

A tracking device is automatically created. The tracking device's name is PRN-U134-PRT, the same as the port's. The IP address for the tracking device is the same as the output device (10.42.58.134).

To create this port, an administrator user called "admin" is used, where the password for that user is "nimda" (without the quotes).

```
scPortUtility --create-push-port -sc-server-addresses
10.42.57.8 --port PRN-U134-PRT --output-address 10.42.58.134
--sc-user admin --sc-password "nimda"
```

Attaching queue to port

The following example will, on the print server named prnsvr02, attach the PRN-U134 queue to the PRN-U134PRT port.

```
scPortUtility --attach-port --port PRN-U134PRT --queue
PRN-U134 -target-machine prnsvr02
```

Queue migration

The following example creates a new push port called PRN-U134-PRT based on the settings from the standard TCP/IP port attached to the PRN-U134 queue. The port connects to the SafeCom server at 10.42.57.8. The queue PRN-U134 will be connected to the newly created port PRN-U134-PRT.

A tracking device is automatically created. The tracking device name is PRN-U134, the same as the queue. The IP address for the tracking device is the same as the previous standard TCP/IP port address.

An administrator user called "admin" is used, where the password for that user is "nimda" (without the quotes).

```
scPortUtility --migrate -sc-server-addresses 10.42.57.8 -queue
PRN-U134 --port PRN-U134-PRT --sc-user admin
--sc-password "nimda"
```

List printing

Print all

The following example will output all queues, including queues with print pooling enabled (PRN-U135).

```
scPortUtility --list-print-queues
```

The output is similar to:

```
"PRN-U134";"PRN-U134-PRT";"SafeCom Push Port";"SafeCom Push Port";
"PRN-U135";"IP_10.0.0.45";"TCPMON.DLL";"Standard TCP/IP Port";
"PRN-U135";"IP_10.0.0.46";"TCPMON.DLL";"Standard TCP/IP Port";
```



```
"PRN-U135";"IP_10.0.0.47";"TCPMON.DLL";"Standard TCP/IP Port";  
"PRN-U136";"IP_10.0.0.48";"TCPMON.DLL";"Standard TCP/IP Port";  
"PRN-U137";"IP_10.0.0.49";"IPP Provider";"IPP Port";
```

List print queues eligible for migration

The following example will output only queues eligible for migration.

```
scPortUtility --list-print-queues --only-migratable
```

The output on the same machine as the previous example would be:

```
"PRN-U136";"IP_10.0.0.48";"TCPMON.DLL";"Standard TCP/IP Port";
```

Troubleshooting

SafeCom Administrator: Unable to locate all SafeCom servers

The SafeCom Administrator uses broadcasts to locate the SafeCom servers. If your network is a VLAN (Virtual Local Area Network), then it may prevent the SafeCom Administrator from locating the SafeCom servers.

To solve the problem, you should enter the SafeCom servers' IP addresses directly in the list of individual **Broadcast addresses** on the **Network** tab in the **Options** dialog.

Document is not printed

Check this if the document leaves the print queue as printed:

- Is the printer powered on and connected?
- Is the printer online?
- Is intervention required? Check for:
 - wrong paper size
 - manual feed
 - out of paper
 - paper jam
 - toner low
- Does the printer driver work with the printer? Test this by using the standard TCP/IP port instead of the SafeCom Push Port. If it still fails, try to use a more appropriate printer driver. Another possibility is to test if the problem is related to a specific application or perhaps version of an application.

Check this if the document remains in the print queue:

- Is the print queue paused?

Check this if the document is deleted from the print queue:

- Does the SafeCom Event Log contain any event of the type Push print failed? The event will contain additional details indicating that perhaps the tracking device is missing. Open the Configure Push Port dialog and verify that a SafeCom printer is selected for tracking. SafeCom Port Configurator can be used to repair the Push printer (see [Repair push printer](#)).
- Does the SafeCom Event Log contain any event of the type Push print failed? The event will contain additional details indicating that perhaps the cost control of user does not match device, that is, a Pay user is trying to print on a device that does not have a Pay license.

- Does the SafeCom Event Log contain any event of the type Push print failed? The event will contain additional details indicating perhaps user credits shortage, that is, the Pay user did not have enough credits.
- Is the user subject to SafeCom Rule Based Printing and the rule is causing the deletion of the document?
- Is the user unknown to SafeCom? If SafeCom trace is enabled, the PullPM2kSrv.trc will contain a line with the text: ExecuteTransaction: Status error [SC_USER_NOT_FOUND].

Document is not tracked

- Did the document print?
- Is the user set to Cost control Tracking?
- Does the device include a Tracking license?
- If Client Billing is enabled, there is a delay before you can see the tracking record.

User's computer: "... Please contact your administrator!"

If there are problems that prevent users from printing documents through SafeCom, the **Messenger Service** dialog appears on the screen.

Typical messages:

- Unable to connect to SafeCom server.
- There is not enough disk space on the SafeCom server.
- Unable to logon to the SafeCom database.
- SafeCom license violation.
- You are unknown to SafeCom.

The above SafeCom-generated messages appear after any print notification messages are sent by the Windows print subsystem. For this reason, we recommend that you disable notification messages from the Windows print subsystem. On the Windows server, open the **Printers** folder. On the **File** menu, click **Server Properties** and click the **Advanced** tab. Refer to online Windows help.

Copy tracking

Copy tracking makes it possible to track copy costs on MFPs. Your SafeCom license key code must include Copy Control and the MFP must be networked, and in most cases, you need a special SafeCom MFP cable.

Fax, Scan, and E-mail tracking

Fax, Scan, and E-mail tracking is possible on most MFPs equipped with SafeCom Go.


Post track

Post tracking affects the following tracking data for Pull print jobs:

- **Tracking pages** (TrackingPageCount) is adjusted to reflect the actual number of pull printed pages. If a 100 page document is cancelled after 10 pages, the job is only tracked (and priced) as 10 pages.
- **Color pages** (TrackingColorPageCount) is adjusted to reflect the actual number of pull printed pages with color.
- **Price 1** (JobPrice) and **Price 2** (JobPrice2) are adjusted to reflect the adjustment of Tracking pages and Color pages. See [Accounting policy](#).
- **Toner** (TonerCyan, TonerMagenta, TonerYellow, and TonerBlack) is tracked. The values are not shown in the **Tracking record** dialog.

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.

 Push Print Post Tracking is supported on HP FutureSmart devices. Refer to *SafeCom Go HP Administrator's Guide* for detailed information on setup and configuration.

Planning your SafeCom Tracking solution

When planning your SafeCom Tracking solution, you need to:

- Define the cost of printing. This is accomplished through a [charging scheme](#). Print costs default to 0.00 if no charging scheme is defined.
- Set up the server properties to [track deleted jobs](#).
- Plan how you will secure the recorded tracking data (see [Backup and restore](#)).
- Decide if you wish to [use the recorded tracking data](#) for invoicing and/or auditing.
- Control what happens if the [tracking server](#) is unavailable.
- If your SafeCom solution is a multiserver solution, you need to configure if tracking data should be collected online or offline (see [Multiple servers: Online or offline tracking](#)).

Print price calculation

The price calculation is defined in a charging scheme. The price calculation is based on paper size, number of sheets and impressions, and possible use of color. Multiple charging schemes can be created to reflect the varying print costs of different printer models.

SafeCom supports dual charging schemes. Each printer can be associated with two charging schemes:

- **Primary charging scheme:** The primary charging scheme (Cost 1) is used to charge users and invoice departments.
- **Secondary charging scheme:** The secondary charging scheme (Cost 2) is used to reflect the true print costs.

It is recommended to have the **Name** and/or **Description** of the charging scheme reflect if it is a primary or secondary charging scheme. Sample charging scheme:

Print				
Price per job (start-up cost)				0.20
Price per page	Paper size	Sheet	Impressions	
			Mono	Color
	A3	0.10	0.20	0.60
	A4	0.05	0.10	0.30
	Executive	0.05	0.10	0.30
	Letter	0.05	0.10	0.30
	Ledger	0.05	0.10	0.30
	Other	0.05	0.10	0.30

Copy				
Price per job (start-up cost)				0.20
Price per page	Paper size	Sheet	Impressions	
			Mono	Color
	A3	0.10	0.20	0.60
	A4	0.05	0.10	0.30
	Executive	0.05	0.10	0.30
	Letter	0.05	0.10	0.30
	Ledger	0.05	0.10	0.30
	Other	0.05	0.10	0.30

Fax	
Price per job (start-up cost)	0.10
Price per page	0.10

Scan	
Price per job (start-up cost)	0.10
Price per page	0.10

E-mail	
Price per job (start-up cost)	0.10
Price per page	0.10

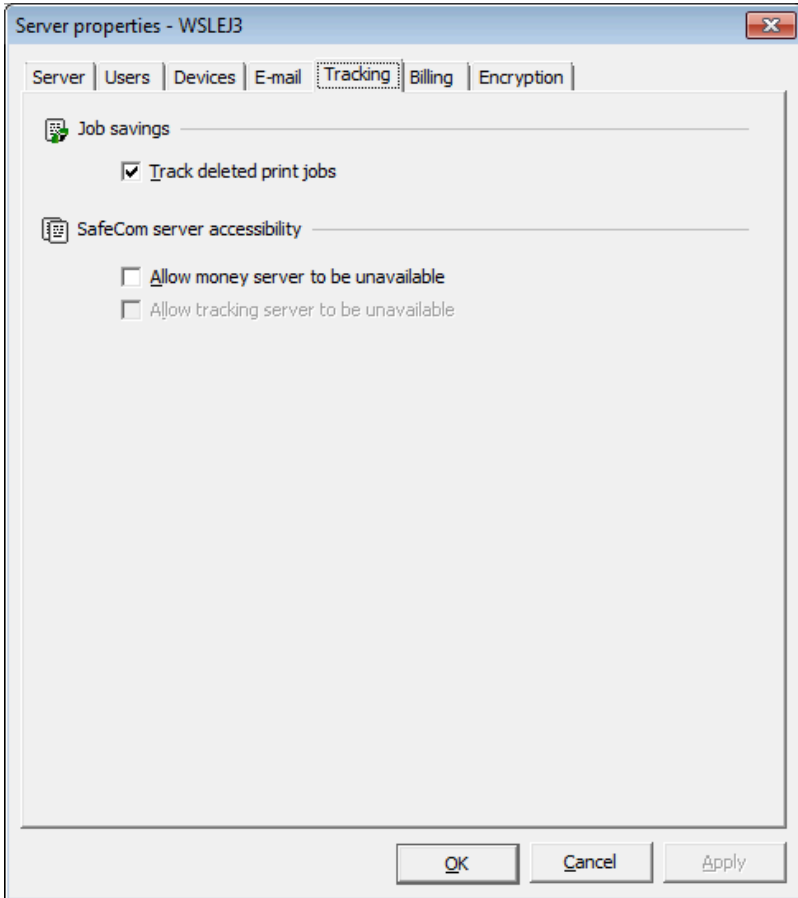
Define print costs through charging schemes

1. Make a list of all the relevant printer models in your solution.
2. Calculate the costs for each printer model.
3. Make a proposal for the charging schemes. The charging schemes may require approval from higher management.
4. Use SafeCom Administrator to define the [charging schemes](#).



- Some Windows printer drivers set paper size to "Default". The SafeCom solution will map this to "Other". For this reason, you should set the price of "Other" to the same price as the most commonly used paper size, typically "A4" or "Letter".
- Some MFPs can only report the number of copied pages and do not provide information about paper size or use of color and duplex. In such cases, the copy page price is based on the price of "A4".

Track deleted jobs



Backup and restore

This topic is covered in [Backup and restore](#), where you can also find information about the Tracking database.

Using tracking data

Tracking data can be exported for further analysis (see [Work with tracking data](#)) and analyzed by the supplied Data Mining tool (see [SafeCom Data Mining](#)).

As the amount of tracking data continues to grow, it is advisable to delete tracking data (see [Hide job names in tracking data](#)) once it has been exported, perhaps on a monthly or quarterly basis. During the exporting or deletion of large amount of tracking data, the server may become slow. It is therefore recommended to perform this outside working hours, or at least not during peak hours.

The tracking data can also be used to invoice users based on what they have printed. If you want users to pay up front, you should use the SafeCom Pay module described in [SafeCom Pay](#).

You can utilize the **Organizational Unit** and/or **Description** properties of users to specify which cost center, division, or department they belong to. That way, you can invoice the user's organizational unit.

With the **SafeCom Administrator API** (option), you can extract tracking data automatically. This XML-based tool is ideal for system integration with financial applications.

Multiple servers: Online or offline tracking

SafeCom Tracking solutions with multiple servers can be configured to use the following tracking options:

- **Offline tracking** (recommended and set by default): Tracking data is stored locally on the SafeCom secondary server to allow subsequent, scheduled collection by the SafeCom primary server. Scheduling data collection to run at night saves network bandwidth during daytime.
- **Online tracking**: SafeCom secondary servers continuously report tracking data to the SafeCom primary server.

To configure offline tracking, perform the following steps:

1. On the SafeCom primary server, enable and configure the scheduled collection of tracking data (see [Configure SafeCom primary server](#)).
2. Configure each SafeCom secondary server to use offline tracking (see [Configure SafeCom secondary servers](#)).

Configure SafeCom primary server

The scheduled collection of tracking data by the primary server can take place on selected weekdays (Monday, Tuesday, ... , Sunday) at a specific time or at a regular, predefined interval starting at a specific time. The available intervals are every 10, 20, or 30 minutes, or every 1, 2, 3, 4, 6, 8, and 12 hours.

1. In the **Servers** menu, click **Server properties**.
2. Click the **Tracking** tab.
3. Configure the scheduled collection of tracking data, then click **OK**.

Configure SafeCom secondary servers

1. In the **Servers** menu, click **Server properties**.
2. Click the **Tracking** tab.
3. Select **Offline**, then click **OK**.

Configuration overview

The steps involved in configuring your SafeCom Tracking solution are as follows:

1. **Install license key code**: Use SafeCom Administrator to install your license key code with tracking enabled.

- 2. Create charging schemes:** Use SafeCom Administrator to create multiple charging schemes to reflect the varying print costs of the different printer models (see [Charging schemes](#)).
- 3. Associate charging scheme with device:** Use SafeCom Administrator to associate a charging scheme with the device (see [Associate charging scheme with device](#)).
- 4. Change cost control to tracking:** Use SafeCom Administrator to change the user property Cost control to Tracking (see [Change cost control to tracking](#)).
- 5. Work with the tracking data:** Use the Data Mining tool to view the tracking data (see [Work with tracking data](#)).

Charging schemes

In section [Charging scheme](#), we describe the concept of charging schemes, dual charging schemes, and how to set them up. The following subsections describe how to work with charging schemes in SafeCom Administrator.

Add charging scheme

1. In the **Devices** menu, point to **Charging schemes** and click **Add charging scheme**. The **New Charging Scheme** dialog appears.
2. Enter prices.
3. Click **Add** and then **Finish**.
 - **Name** is the unique name of the charging scheme (mandatory).
 - **Description** is an optional description of the charging scheme
 - Enter price per job to charge a **Start-up cost per job**. Select **Enable job name pricing** if you wish to enable pricing based on job name (see [Job name pricing](#)).
 - Enter **Price per page** in the form of the price for **Sheet** (paper), **Mono Impression**, and **Color Impression** for the paper sizes: A3, A4, Executive, Letter, and Legal. Click **Set all** to quickly enter a price for all paper sizes. The price specified in **Other** is used when the paper size is unknown (or default).
4. Click the **Copy** tab to specify the prices for copy jobs.

i Some MFPs, which are unable to provide information about paper size or the use of duplex and color, try to compensate for this lack of detail by reporting a higher number of copied pages. For example, one monochrome A3 page or one color A4 page is reported as two pages. Or one color A3 page is reported as 4 pages.

5. For selected MFPs, it is also possible to charge for fax, scan, and e-mail. Click the **Fax+Scan+E-mail** tab to specify these prices.

Sample charging calculation

Job properties:

5 color pages in paper size A4 and duplex

Price per job = 0.20

Price per sheet A4 = 0.05

Price per color impression A4 = 0.30

Price calculation:

= price per job + price per sheet × number of sheets + price per impression × number of impressions

= 0.20 + 0.05 × 3 + 0.30 × 5

= 0.20 + 0.15 + 1.50

= 1.85

View charging scheme properties

Perform one of the following steps:

- Double-click the charging scheme in the **Charging scheme list**.
- In the **Devices** menu, point to **Charging schemes** and click **Charging scheme properties**.
- Open the **Device properties** dialog and click the **Charging scheme** tab, then click **View**.

See [Add charging scheme](#) for a description of the **Charging scheme properties** dialog.

Associate charging scheme with device

1. Double-click the device in the **Devices list**.
The **Device properties** dialog appears.
2. Click the **Charging scheme** tab.
3. Select a charging scheme as **Charging scheme 1 (primary)**.
This is used to charge users and invoice departments.
 - Optionally, select a charging scheme as **Charging scheme 2 (secondary)**.
This is used to reflect the true print costs.
4. Click **OK**.

Configure default charging scheme for new devices

A charging scheme can be marked as default. All new devices will use this charging scheme by default.

1. In SafeCom Administrator, open the **Server properties** dialog and click the **Devices** tab.
2. Select **Keep default charging scheme 1 and assign it to auto-created devices**, and optionally, select **Keep default charging scheme 2 and assign it to auto-created devices**.
3. Click **OK**.

Delete a charging scheme

Deleting a charging scheme removes the charging scheme from all devices that used it. No charging is done on these devices until you select another charging scheme.

In the **Charging scheme list**, right-click the charging scheme and select **Delete charging scheme**.

Change cost control to tracking

Tracking must be enabled for each existing user.

Select **Tracking** on the **Settings** tab in the **User properties** dialog of the SafeCom Administrator.

It is possible to change the property of multiple users. See [Hide ID codes](#).

By selecting a Tracking user as the default user, you can make any user imported in the future (users who are created at first print or are added manually) a Tracking user.

SafeCom Reports

SafeCom Reports is an optional program that enables viewing main tracking statistics, user statistics, device statistics, Client Billing statistics, and the job list. For additional information, refer to *SafeCom Reports Administrator's Guide*.


Install SafeCom Reports

1. Download the software from the link supplied to you.
2. When the SafeCom Reports Setup Wizard appears, click **Next**.
3. Select the destination folder for the SafeCom Report files. Optionally, click **Disk Cost** to check the available disk drives for required disk space. Select **Everyone** to install SafeCom Reports so everyone who uses the computer can use it, then click **Next**.
4. Click **Next** to start the installation.
A progress bar appears.
5. Click **Close** when the installation has completed.

The default installation folder is C:\Program Files\SafeCom\SafeCom Reports.

Start SafeCom Reports

1. Click the SafeCom Reports icon on the desktop.
2. Enter the **SafeCom Server** (IP address or hostname) or click the SafeCom server button to broadcast for available SafeCom servers.
3. Enter **User** (default is ADMIN) and **Password** (default is nimda).

 If the user belongs to a domain, the domain followed by a backslash (\) must be specified in front of the user's logon. Example: MYDOMAIN\JS.

4. You must have [SafeCom Report rights](#) to log in. Click **Login**.

Make a report

Once you are logged into SafeCom Reports, you are able to generate a report.

1. Select what you want to create a report of in the **Report** column.

For example: **Application Usage** or **Largest Print Users**.

2. Click **Extract New Data for Report.**

In most reports, you need to specify the **Date of first record** and the **Date of last record**.

3. Click **OK to generate the report.**

In the **Exporting Records** dialog, you can monitor the progress while records are being exported.

It is possible to schedule one or more reports using the supplied SafeCom Reports command line interface. Refer to *SafeCom Reports Administrator's Guide*.

Work with tracking data

You can interact with tracking data in the following ways:

- [Export tracking data](#)
- [Hide job names in tracking data](#)
- [Delete tracking data](#)

Export tracking data

1. In the **Servers menu, click **Tracking data** and **Export tracking data**.**

2. Select the period.

A number of predefined periods are available ranging from **Today** to **1 year back**. Choose **Specify period** to freely specify the beginning (from) and the end (to) of the period.

3. Enter the path and **File name of the export file.**

4. Click **Browse to specify the location of the export file.**

5. Select a **File format (XML, TXT, or CSV).**

6. Select a **Separator (not needed when using XML).**

The default value for separator is taken as the **List separator** setting on the **Numbers** tab of the **Regional settings** dialog.

- Use the default setting if you intend to use Microsoft Excel, since Excel takes its default separator from the same place and the separators need to match.

7. Select **Launch Datamining if you want to analyze the data right away.**


8. Click **OK.**

i When you export to txt format, two files are created. One is a *.txt (or *.csv) file, the other is a *.sch file. They are automatically placed in the same directory when they are created. The *.sch file is used by the administrator's data mining function as a reference file. It tells the administrator how to interpret each field in the *.txt file. For this reason, you must keep them together in the same directory when using the files for data mining.

Hide job names in tracking data

You have the option to mask job names with asterisks (*) in the tracking database for users on specified home servers, while leaving the rest of the job names readable. The option is available for both online and offline tracking, and in multiserver environments, you can designate if a given server uses this function or not.

To use the function, you need to create a list of servers by either creating a list in the registry or with a text file.

 For each server, only one of the options should exist in your SafeCom installation.

Create a list of servers in registry

1. Log in to the SafeCom Administrator on the primary server.
2. Use the **Server properties** to locate the IDs of the servers you want to use with this function.
3. Create a registry key named **Tracking** under `HKEY_LOCAL_MACHINE\SOFTWARE\SafeCom\SafeComG4`.
4. Create a String (REG_SZ) registry value named **ServerIds**.
5. Enter the IDs of all servers into the value field using comma (",") or semicolon (";") as the separator characters.
6. Ensure that the total length of the value does not exceed 255 characters.

Create a list of servers in a text file

1. Log in to the SafeCom Administrator on the primary server.
2. Use the **Server properties** to locate the IDs of the servers you want to use with this function.
3. Create an Unicode text file listing all server IDs.
The first line of the file must be "Servers" without quotation marks. The server IDs must be added starting from line 2, with each ID in a separate line.
4. Create a registry key named **Tracking** under `HKEY_LOCAL_MACHINE\SOFTWARE\SafeCom\SafeComG4`.
5. Create a String (REG_SZ) registry value named **ServerIdsFile**.
6. Enter the full path of the text file created in step 3.

Delete tracking data

You can delete data prior to a given date from the Tracking database. This can be used to increase the speed of your SafeCom solution. Too much data can slow it down.

1. In the **Servers** menu, click **Tracking data** and **Delete tracking data**.
All data before **Last date** is exported to a file and is deleted from the tracking database.
2. Enter the path and **File name** of the file.
3. Click **Browse** to specify the location of the export file.
4. Select a **File format** (XML, TXT, or CSV). Do not select CSV if you intend to **Launch Datamining**.
5. Select a **Separator** (not needed when using XML).

The default value for separator is taken from the **List separator** setting in the **Numbers** tab of the **Regional settings** dialog.

- Use the default setting if you intend to use Microsoft Excel, since Excel takes its default separator from the same place and the separators need to match. In chapter [Format of tracking data](#), there is a complete description of the exported tracking data.

6. Click **OK**.

SafeCom Data Mining

SafeCom Data Mining enables you to see main tracking statistics, user statistics, device statistics, billing statistics, and the job list.

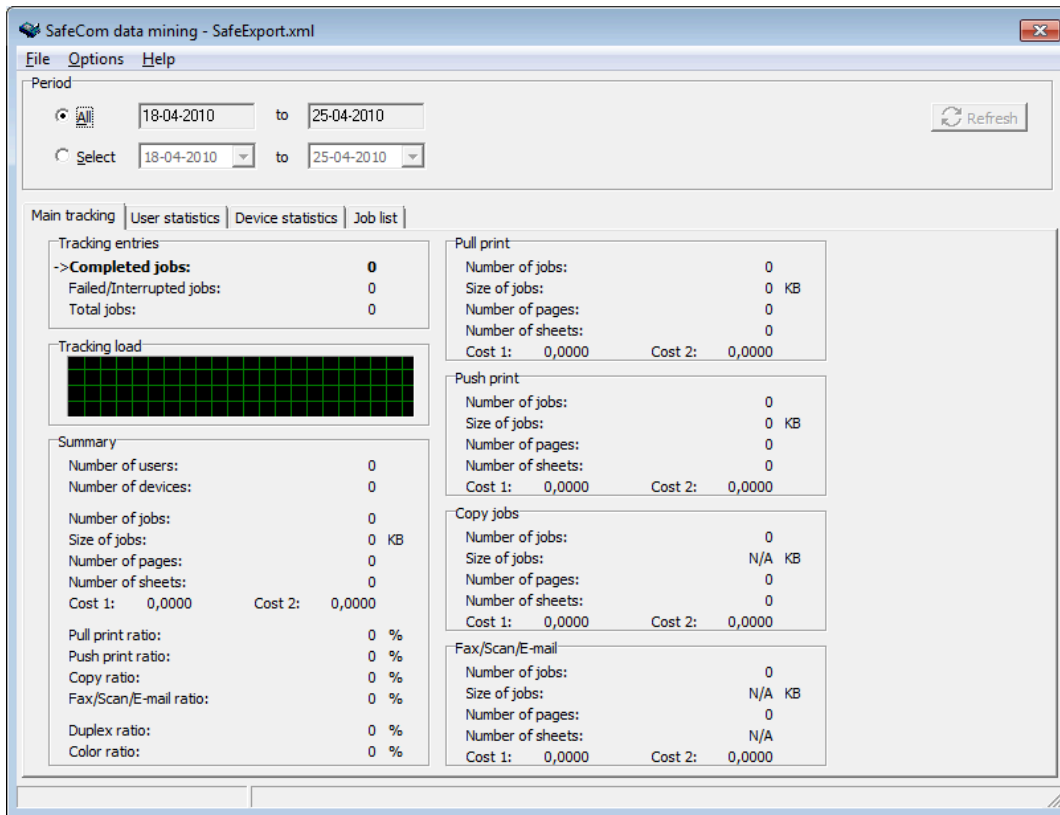
i SafeCom Data Mining is designed to handle up to 50,000 tracking records. Use [SafeCom Reports](#) to work with more tracking records. The optional SafeCom Administrator API can be used to export selected fields from the tracking records. This allows optimized data post-processing by third-party applications that can work on the CSV or XML file exported from the SafeCom solution.

Use SafeCom Data Mining as described in the following steps:

1. Select **Launch Datamining** when you [export tracking data](#) or [delete tracking data](#).
The SafeCom Datamining window is displayed (see [Main tracking](#)).
2. In the **File** menu, click **Open**.
3. Find the SafeCom Data Mining file (*.xml or *.txt) containing the data you want to view. Click **Open**.
4. Choose either to view **All** data or **Select a Period**.
 - Click **Refresh** if you change the period.
5. Click the **User Statistics**, the **Device Statistics**, or the **Billing statistics** tab according to the data you want to view.
6. Click **Options** and select **Setup** to change the job types to be included in the statistics.
 - Completed jobs only
 - Failed/Interrupted jobs only
 - All jobs
7. Click **Refresh** to update the view of the exported statistics according to the changed options.

Main tracking

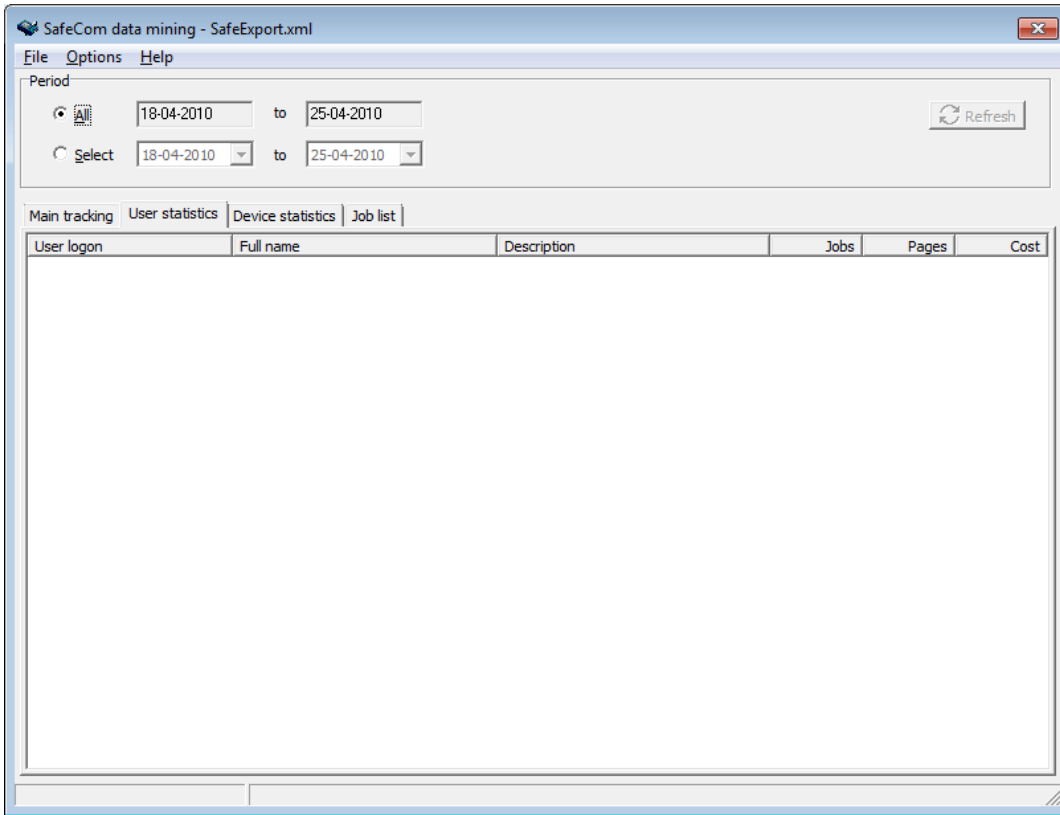
The **Main tracking** tab gives an overview of the tracking data, including the ratio between the different job types and the use of color and duplex.



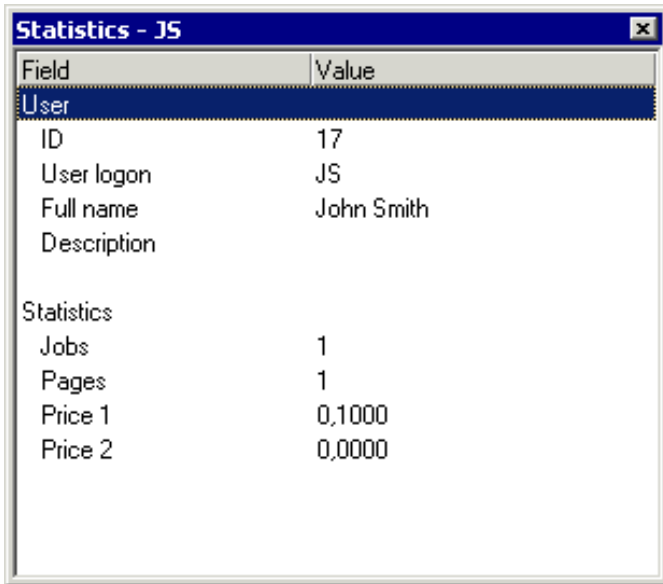
- **Tracking entries** shows the number of **Completed jobs**, **Failed/Interrupted jobs**, and **Total jobs**.
- **Tracking load** shows a graphic representation of the number of tracking jobs as a function of time (the selected period).
- **Summary** lists the **Number of jobs**, **Size of jobs**, **Number of pages**, and the resulting costs as calculated using the primary and secondary charging scheme. The **Pull print ratio**, **Push print ratio**, **Copy ratio**, **Fax/Send/E-mail ratio**, **Duplex ratio**, and **Color ratio** are also shown.
- **Pull print** lists the **Number of jobs**, **Size of jobs**, **Number of pages**, and the resulting costs as calculated using the primary and secondary charging scheme.
- **Push print** lists the **Number of jobs**, **Size of jobs**, **Number of pages**, and the resulting costs as calculated using the primary and secondary charging scheme.
- **Copy jobs** lists the **Number of jobs**, **Size of jobs**, **Number of pages**, and the resulting costs as calculated using the primary and secondary charging scheme.
- **Fax/Scan/E-mail** lists the **Number of jobs**, **Size of jobs**, **Number of pages**, and the resulting costs as calculated using the primary and secondary charging scheme. You can track fax, scan, and e-mail on devices with SafeCom Go installed.

User statistics

The **User statistics** tab lists the recorded tracking data summarized on a per-user basis. The following columns are available: **User logon**, **Full name**, **Description**, **Jobs**, **Pages**, and **Cost**.



- Click the **Pages** header to sort and find who has been producing most pages using the printers and MFPs for the specified period.
- Click the **Cost** header to sort and find who has been spending most credits using the printers and MFPs for the specified period. The listed cost is calculated using the primary charging scheme.
- Click the selected user to open the **Statistics** dialog with more detailed statistics, including costs calculated using the secondary charging scheme.

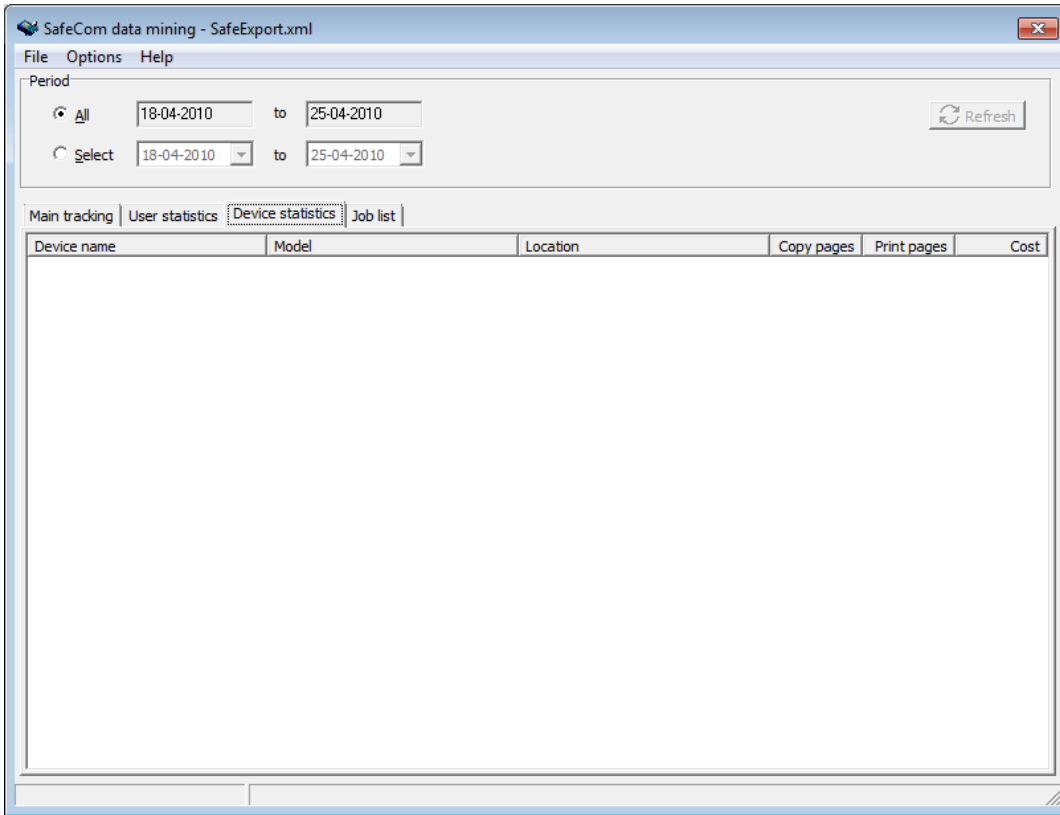


The screenshot shows a window titled "Statistics - JS" with a table of data. The table has two columns: "Field" and "Value". The data is organized into two sections: "User" and "Statistics".

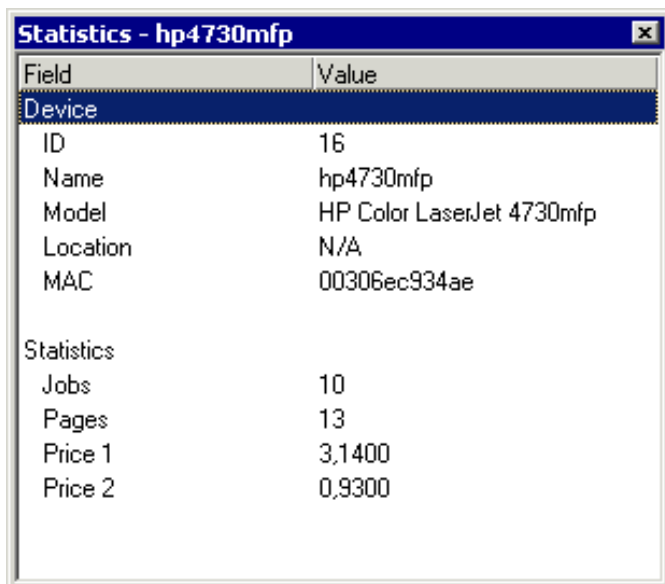
Field	Value
User	
ID	17
User logon	JS
Full name	John Smith
Description	
Statistics	
Jobs	1
Pages	1
Price 1	0,1000
Price 2	0,0000

Device statistics

The **Devices statistics** tab lists the recorded tracking data summarized on a per-device basis. The following columns are available: **Device name**, **Model**, **Location**, **Copy pages**, **Print pages**, and **Cost**.



- Click the **Print pages** header to sort and find which device has been printing most pages for the specified period.
- Click the **Copy pages** header to sort and find which device has been copying most pages for the specified period.
- Click the **Cost** header to sort and find which device has been producing most for the specified period. The listed cost is calculated using the primary charging scheme.
- Click the selected device to open the **Statistics** dialog with more detailed statistics, including costs calculated using the secondary charging scheme.

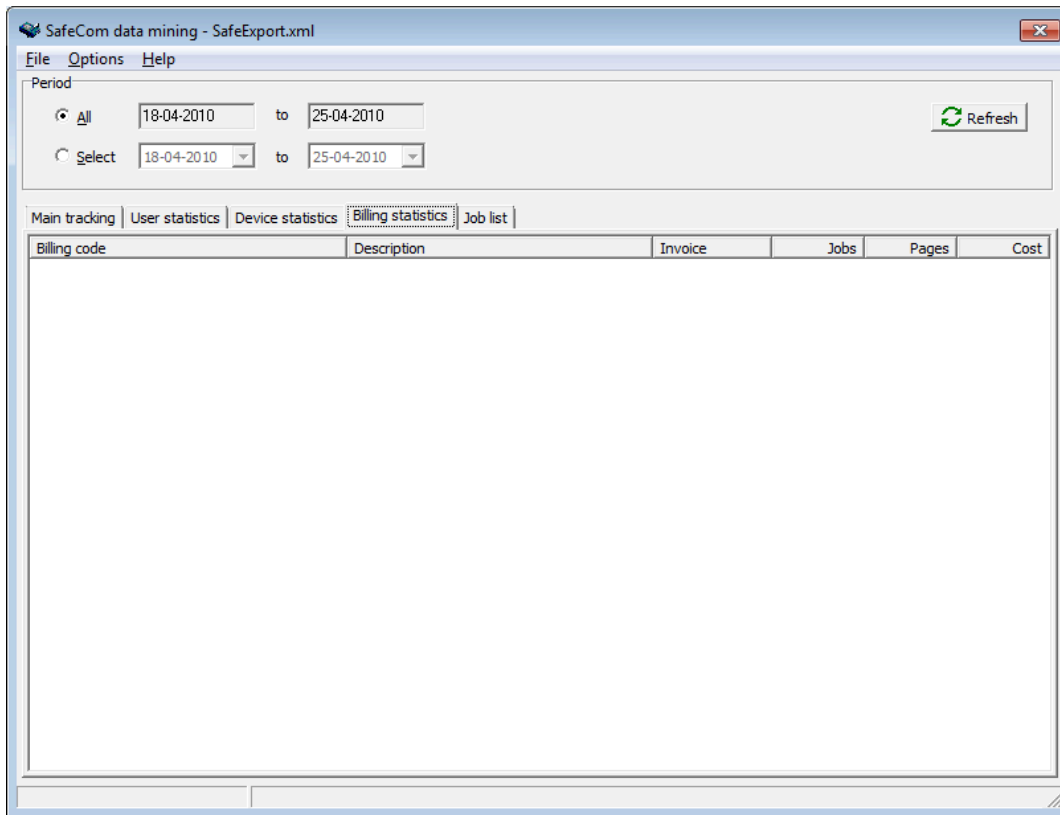


The screenshot shows a window titled "Statistics - hp4730mfp" with a close button in the top right corner. The window contains a table with two columns: "Field" and "Value". The table is divided into two sections: "Device" and "Statistics".

Field	Value
Device	
ID	16
Name	hp4730mfp
Model	HP Color LaserJet 4730mfp
Location	N/A
MAC	00306ec934ae
Statistics	
Jobs	10
Pages	13
Price 1	3,1400
Price 2	0,9300

Billing statistics

The **Billing statistics** tab lists the recorded tracking data summarized on a per-billing code basis. The following columns are available: **Billing code**, **Description**, **Invoice**, **Jobs**, **Pages**, and **Cost**.

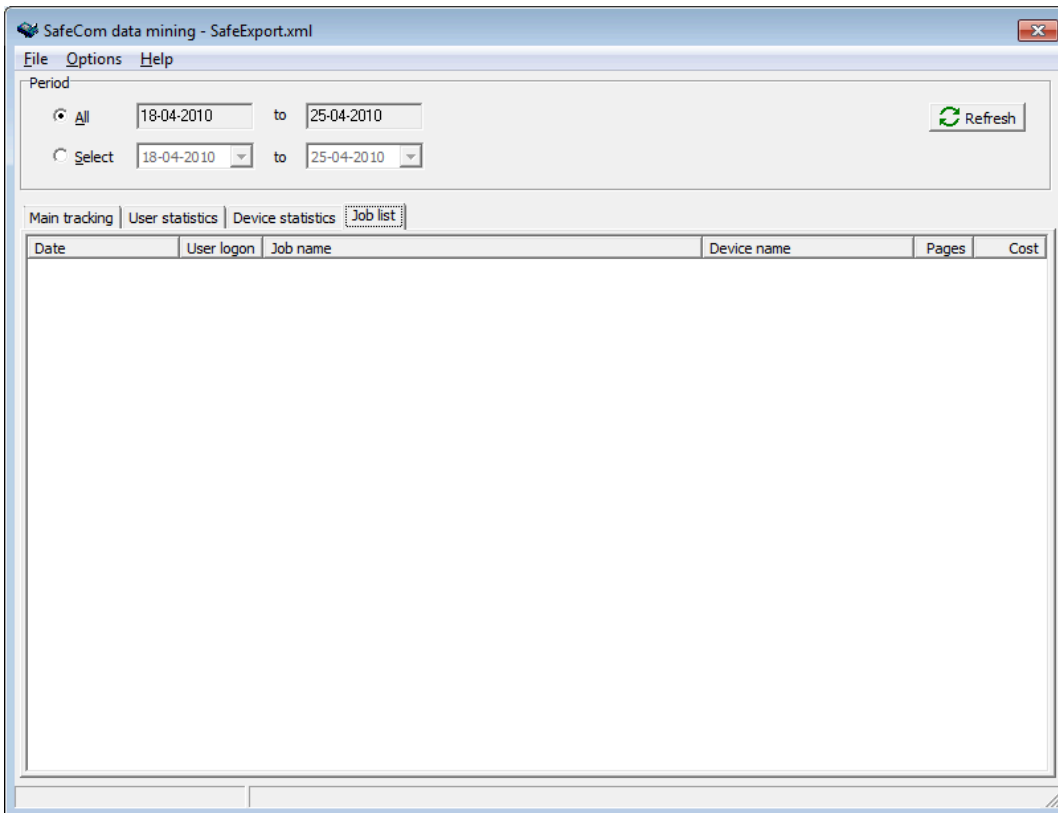


- Click the **Pages** header to sort and find who has been producing most pages using the printers and MFPs for the specified period.
- Click the **Cost** header to sort and find who has been spending most credits using the printers and MFPs for the specified period. The listed cost is calculated using the primary charging scheme.
- Click the selected billing code to open the **Statistics** dialog with more detailed statistics, including costs calculated using the secondary charging scheme.

Field	Value
Billing code	
Name	45
Description	Denmark
Invoice	NO
Statistics	
Jobs	1
Pages	1
Price 1	0,1000
Price 2	0,0500

Job list

The **Job list** tab lists the recorded tracking data on a per-job basis. The following columns are available: **Date**, **User logon**, **Job name**, **Device name**, **Pages**, and **Cost**.



- Click the **User logon** header to sort and find the jobs produced by user for the specified period.
- Click the **Device name** header to sort and find the jobs produced by device for the specified period.
- Click the **Cost** header to sort and find which job is the most expensive for the specified period. The listed cost is calculated using the primary charging scheme.
- Click the selected job to open the **Tracking record dialog** with more detailed information, including costs calculated using the secondary charging scheme.

Tracking record dialog

The Tracking record dialog appears when you click a job in the [job list](#).

Tracking record



Field	Value
Job	
Name	Wordpad-Duplex
Generated	5/18/2017 9:17:04 AM
Size	41 KB
Paper	A4
Duplex	Yes
Color	Yes
Driver	HP Universal Printing PCL 6 (v6.3
Type	PULL
Destination	
User	
ID	3
User logon	SP
Full name	
Description	
Cost code	N/A
Device	
ID	1
Name	HPDF0047
Model	HP PageWide Pro 552 Printer
Location	N/A
Duplex	Yes
Color	Yes
MAC	5820b1df0047
Page count	
Tracking state	COMPLETED
Tracking pages	8
Driver pages	0
Parser pages	8
Color pages	8
Sheets	4
Cost	
Price 1	0.0000
Price 2	0.0000
Billing	
Primary code	N/A
Primary description	N/A
Secondary code	N/A
Secondary description	N/A
Invoice	NO
Miscellaneous	
Start time	5/18/2017 9:34:08 AM
End time	5/18/2017 9:34:08 AM
Print queue	HP Universal Printing PCL 6 (v6.3
Print computer	WIN2016-SP
RBP force duplex	No
RBP force mono	No
RBP force toner save	No

The tables below list the tracking record fields displayed in the **Tracking record** dialog. The records are grouped as follows:

- Job
- User
- Device
- Page count
- Cost
- Miscellaneous

The corresponding XML tag is also listed and can be used to reference the tracking format as described with all fields in section [Format](#). A plus sign ("+") indicates the field is relevant for the listed job. A minus sign ("-") indicates the field is not relevant for the listed job.

Job	PUSH	PULL	COPY	SCAN	EMAIL	FAX
Name <JobName>	+	+	+	+	+	+
Generated <JobDate>	+	+	+	+	+	+
Size <JobSize>	+	+	-	+	+	+
Paper <JobPageFormat>	+	+	+	+	+	+
Duplex <JobIsDuplex>	+	+	+	+	+	+
Color <JobIsColor>	+	+	+	+	+	+
Driver <DriverName>	+	+	-	-	-	-
Type <JobType>	+	+	+	+	+	+
Destination <JobDestination>	-	-	-	+	+	+

User	PUSH	PULL	COPY	SCAN	EMAIL	FAX
ID <UserID>	+	+	+	+	+	+
User logon <UserLogon>	+	+	+	+	+	+
Full name <FullName>	+	+	+	+	+	+
Description <Description>	+	+	+	+	+	+
Cost code <UserCostCode>	+	+	+	+	+	+

Device	PUSH	PULL	COPY	SCAN	EMAIL	FAX
ID <DeviceID>	+	+	+	+	+	+
Name <DeviceName>	+	+	+	+	+	+
Model <DeviceModel>	+	+	+	+	+	+
Location <DeviceLocation>	+	+	+	+	+	+
Duplex <DeviceSupportsDuplex>	+	+	+	+	+	+
Color <DeviceSupportsColor>	+	+	+	+	+	+
MAC <DeviceMac>	+	+	+	+	+	+


Page count	PUSH	PULL	COPY	SCAN	EMAIL	FAX
Tracking state <TrackingState>	+	+	+	+	+	+
Tracking pages <TrackingPageCount>	+	+	+	+	+	+
Driver pages <DriverPageCount>	+	+	-	-	-	-
Parser pages <ParserPageCount>	+	+	-	-	-	-
Color pages <TrackingColorPageCount>	+	+	+	+	+	+
Sheets <JobSheetCount>	+	+	+	-	-	-

Cost	PUSH	PULL	COPY	SCAN	EMAIL	FAX
Price 1 <JobPrice>	+	+	+	+	+	+
Price 2 <JobPrice2>	+	+	+	+	+	+

Miscellaneous	PUSH	PULL	COPY	SCAN	EMAIL	FAX
Start time <StartDate>	+	+	+	+	+	+
End time <StopDate>	+	+	+	+	+	+
Print queue <PMQueueName>	+	+	-	-	-	-
Print computer <PMComputerName>	+	+	-	-	-	-

Update scParser.dll

The component scParser.dll is responsible for parsing the print data stream. If a new version is made available to you, you should follow the steps below to update it.

 On Windows 64-bit, the file is named scParser64.dll.

1. Backup the existing file scParser.dll from the SafeCom installation folder.
The default folder is C:\Program Files\SafeCom\SafeComG4\.
2. Stop the SafeCom service and the Print Spooler.
3. Copy scParser.dll to the SafeCom installation folder.
4. Start the SafeCom service and the Print Spooler.

Chapter 9

SafeCom Rule Based Printing (RBP)

The Rule Based Printing module makes it possible to gain cost savings by offering management a method of enforcing printing policies.

The policies are formulated as one or more rules. Rules are assigned to groups of users. It is possible to construct rules as follows:

- Only color jobs can be printed on color devices.
- Print e-mail as black/white and with toner save.
- Color print is not allowed.
- Allow color print, but warn that color print is more expensive.

Disclaimer:

- SafeCom Rule Based Printing needs to modify the print data stream to control the rules "Duplex on/off", "Toner save on/off", and "Force job to black/white". SafeCom does not guarantee that these modifications will work and cannot be held responsible if they do not work as expected. SafeCom Rule Based Printing has been tested with PCL5, PCL5c, PCL5e, PCL6, PCL XL, and PostScript level 2 and 3 printer drivers from HP using a broad range of HP LaserJets.

Planning your SafeCom RBP solution

When planning your SafeCom Rule Based Printing solution you need to:

- Organize users into groups, as rules apply to groups rather than individual users. A user can be a member of multiple groups and is subject to all rules of the groups he is a member of.
- Create the rules enforcing the policies (see [Create the rules](#)).
- Run the scPopUp.exe program on the user's computer if the rule to notify the user runs on the user's computer (see [Add a SafeCom Push Port](#)).
- Test all new rules using the available printer drivers and printers to ensure that the outcome is as expected before applying the rules on a large scale. Section [What if the rule does not work?](#) includes some troubleshooting hints.
- Select the rules to use on the different groups (see [Select rules to be used on group](#)).
- Make sure your license covers tracking (see [Device license and user settings dependencies](#)) and that relevant users' cost control is set to either Tracking or Pay (see [Settings](#)).

Create the rules

Select the conditions, actions, and notifications to make up and create a rule.

1. In the **Servers** menu, click **Rule Based Printing** to open the **Rule Based Printing** dialog.
2. Click **Add** to create a new rule.
3. On the **Conditions** tab, double-click a condition to apply it.

Rules without conditions always apply (unconditionally). Multiple conditions can be applied. Remove an applied condition by selecting it and clicking the left arrow.

Available Conditions:

- **Device [does | does not] support color:** Allows you to select if the rule should apply when printing on a device with color capabilities.
- **Device location contains "specific text" Device location does not contain "specific text":** Allows you to specify a text that will be used for case insensitive matching based on the device location.
- **Device model contains "specific text" Device model does not contain "specific text":** Allows you to specify a text that will be used for case insensitive matching based on the device model.
- **Device name contains "specific text" Device name does not contain "specific text":** Allows you to specify a text that will be used for case insensitive matching based on the device name.
- **Job color mode is [b/w | color]:** Allows you to select if the rule should apply to a b/w or a color job.
- **Job driver name contains "specific text" Job driver name does not contain "specific text":** Allows you to specify a text that will be used for case insensitive matching based on the job driver name.
- **Job name contains "specific text" Job name does not contain "specific text":** Allows you to specify a text that will be used for case insensitive matching based on the job name. Jobs printed from Internet Explorer and other browsers typically include the text string "http". Section [How to determine the application](#) gives more examples on how the job name can be used to determine the application.
- **Job page count larger than "number":** Allows you to specify a larger page count than specified.
- **Job page count less than "number":** Allows you to specify a smaller page count than specified.
- **Job size larger than "number" KB:** Allows you to specify a larger job size than specified in kilobytes.
- **Job size less than "number" KB:** Allows you to specify a smaller job size than specified in kilobytes.



- The “specific text” is used for case insensitive matching. There is no support for wildcard syntax, such as the use of "*" and "?".
- The “specific text” can take multiple strings delimited by a separator symbol ("|") as the filter character. This acts as an OR operator. The filter characters can be escaped by a preceding backslash ("\\"), so they may also be present in the condition texts.

4. On the **Actions** tab, double-click an action to apply it.

If no actions are applied, there is no action to the rule. Multiple actions can be applied. Remove an applied action by selecting it and clicking the left arrow.

Available actions:

- **Confirm pull job. Message: “text”:** When Pull Printing, a pop-up dialog appears with the configured message text (max 100 characters). The user can click **OK** to print or **Cancel**. One <%pages%> and one <%price%> tag can be included in the text. These tags are replaced with the number of pages and the price of the job. Requires the use of SafeCom PopUp (see [Setup SafeCom PopUp](#)). Details about the calculation of the price based on the charging scheme are in section [Define print costs through charging schemes](#).
- **Confirm push job. Message: “text”:** When Push Printing, a pop-up dialog appears with the configured message text (max 100 characters). The user can click **OK** to print or **Cancel**. One <%pages%> and one <%price%> tag can be included in the text. These tags are replaced with the number of pages and the price of the job. Requires the use of SafeCom PopUp (see [Setup SafeCom PopUp](#)).
- **Delete job:** The job is deleted.
- **Duplex on/off:** The print data is modified to get double-sided print. To avoid 1-page documents from using the duplexer, it is recommended to combine this with the condition: Job page count larger than 1.
- **Force job to b/w:** The print data is modified to force the job to b/w.
- **Hide pull print job:** The job does not appear on the Pull Print list of documents. Typically, combined with the conditions "Device supports color" and "Job color mode is color" to ensure that only color jobs can be Pull printed on color devices. If the job is Push Print, it is deleted.
- **Redirect to queue “name”:** This action applies to Push Print only. The print job is redirected to the specified destination. Normally, the destination is in the form of a printer’s **IP address** or **hostname**. However, it is also possible to redirect to another print queue by, for example, entering the share name: **\\SERVER\Printer**. If you redirect to a print queue that uses the SafeCom Push Port, the print job is tracked again.
- **Redirect to user “logon”:** This action applies to Pull Print only. The print job is redirected and stored under the specified user logon. Redirecting to a Group name is not supported.
- **Toner save on/off:** The print data stream is modified to enable toner save (Economode on b/w HP LaserJets).

5. On the **Notification** tab, select the notification method you want to use and enter the notification message.

It is possible to refrain from selecting any of the notification methods to have the rule execute behind the scenes (silently).


The notification message text does not support the use of tags like <%pages%> and <%price %>. If you require use of these tags, then please use the Action: "Confirm Pull job" or "Confirm Push job".

The notification only occurs if a notification message text is specified.

Notify by:

- **PopUp:** A pop-up dialog with a configurable message appears on the user's computer explaining that the rule has been executed. No client installation is required (see [Add a SafeCom Push Port](#)).
 - **E-mail:** The user receives an e-mail with a configurable message explaining that the rule has been executed.
 - **Log file:** This should only be used during testing. The SafeCom event log lists that the rule was applied. For more information about the event log, see [Event log and e-mail notification](#).
6. On the **Rule description** tab, enter a meaningful **Rule name** to identify the rule, then click **OK**.

Select rules to be used on group

1. Click the **Groups** icon  in the **Server groups** pane.
2. Click a group in the **Group list** to open the **Group properties** dialog.
3. Click the **Rules** tab.
4. Select the rules you want to be used on the group.
5. Click **Apply** and then **Close**.

What if the rule does not work?

Go through the troubleshooting hints below if the rule does not work:

- **Identify the rules:** Verify that the rule is indeed to be executed. You can do this by looking at the **Member of** tab in the **User properties** dialog to determine which groups the user is a member of. Next, you should look at the **Rules** tab in the respective **Group properties** dialog to see which rules are selected.
- **Print data stream compatibility:** If the rule requires customization of the print data stream, it may be that the print data stream is not PCL5, PCL5c, PCL5e, PCL6, PCL XL, or PostScript level 2 or 3.
- **Printer driver compatibility:** Even if the print data stream is supported, it may be driver/printer-specific to a level that is not supported by the current SafeCom Rule Based Printing. In this case, you should refrain from using the rule.
- **IPP compability:** Forcing black and white or duplex printing may not work if this protocol is used for releasing pull print jobs. Though the protocol allows managing such rules, they are not applied on certain device models. Consider changing the print protocol to the legacy port 9100 based method. The print stream is changed directly at the server side according to the selected rule.

How to determine the application

Many customers want to define rules based on the application. The application can, in most cases, be determined by using the condition: **Job name contains "specific text"**.

The table below contains suggested texts to use for popular applications.

Application	Specific text
Adobe	.pdf
Microsoft Excel	.xls
Microsoft Outlook	Microsoft Outlook
	outbind://
Microsoft PowerPoint	Microsoft PowerPoint
Microsoft Word	Microsoft Word
Notepad	Notepad
Plain text files	.txt
Windows Internet Explorer	http
Windows Test Page	Test Page

i E-mails printed from Lotus Notes have the same job name as the subject of the e-mail. It is not possible to use the job name to determine that it's the Lotus Notes application.

Update scRuleExecuter.dll

The component scRuleExecuter.dll is responsible for modifying the print data stream. If a new version is made available to you, follow the steps below to perform the update:

i On Windows 64-bit, the file is called `scRuleExecuter64.dll`.

1. Back up the existing file scRuleExecuter.dll from the SafeCom installation folder.
The default folder is `C:\Program Files\SafeCom\SafeComG4\`.
2. Stop the SafeCom service and the Print Spooler.
3. Copy scRuleExecuter.dll to the SafeCom installation folder.
4. Start the SafeCom service and the Print Spooler.


Chapter 10

SafeCom Client Billing

The Client Billing module makes it possible to register billing codes with any job that is tracked by the SafeCom solution. The billing data can be exported and used for further analysis.

Users can specify billing codes in the following three ways:

- **At print submission:** A billing code can be specified when submitting a job for either Pull or Push print. When a billing code is added during print submission for a Pull print, it is preserved and cannot be overridden by, for example, a new billing code selected at the device.

 For billing codes to be selectable during print submission, SafeCom PopUp ([SafeCom PopUp - scPopUp.exe](#)) must be running on the user's computer.

- **At the device:** On selected SafeCom-enabled MFPs, a billing code can be selected with any job that is tracked by SafeCom. The user can select from a list of specified, favorite billing codes and the last used 10 billing codes.
- **Via web interface:** On the SafeCom G4 Web Interface, users can specify billing codes on their print jobs if this is done before the elapsed time. Also, the users can change the specified billing codes earlier.

Manage billing codes

Managing billing codes involves these administrator tasks:

- **Import billing codes into the SafeCom solution:** Billing codes can be imported either on a scheduled basis or added manually through the SafeCom Administrator or SafeCom API.
- **Assign favorite billing codes to users and/or user groups:** To control which billing codes a user can select from on print jobs, the administrator can create a predefined list of favorite billing codes for each user.

The administrator can create these predefined lists of billing codes through the SafeCom Administrator or the SafeCom API. Using the SafeCom API enables system integration and limits the manual labor involved in managing billing codes.

By utilizing the SafeCom G4 Web Interface, users can be allowed to build and manage their own list of favorite billing codes. This reduces the administrative overhead, but it requires that the administrator can rely on the users' honesty and ability to select the appropriate billing code for the jobs they perform.

Plan your SafeCom Client Billing solution

When planning your SafeCom Client Billing, you need to:

- Plan and configure SafeCom Tracking as SafeCom Client Billing relies on that. Consult chapter [SafeCom Tracking](#) on how to plan (see [Planning your SafeCom Tracking solution](#)) and configure (see [Configuration overview](#)) SafeCom Tracking.
- Decide where to install the SafeCom G4 Web Interface and how users should authenticate themselves to see the SafeCom Client Billing web page.
- Decide if Client Billing should be done using one- or two-level codes. For two-level codes, the billing code consists of a primary (Client) code and a secondary (Matter) code.
- Decide if billing codes should be imported on a scheduled basis.
- Decide the elapsed time before billing codes are committed to tracking data. During this period, users can select and change billing codes on the SafeCom Client Billing web page.
- Schedule and prepare a training for users about how to select billing codes for jobs.

Configuration overview

1. Configure SafeCom Tracking.

See [Planning your SafeCom Tracking solution](#), [Multiple servers: Online or offline tracking](#), and [Configuration overview](#).

2. Install the SafeCom G4 Web Interface.

3. Configure SafeCom Client Billing.

See [Configure SafeCom Client Billing](#).

4. Add the billing codes into the SafeCom solution.

- a. Import billing codes automatically (see [Import billing codes](#)).
- b. Add one-level billing codes (see [Manage 1-level billing code](#)) and two-level billing codes (see [Manage 2-level billing code](#)) manually.

5. Assign favorite billing codes to users and/or user groups.

- a. Select favorite billing codes for a user (see [Billing](#)).
- b. Select favorite billing codes for a group (see [Select favorite billing codes for a group](#)).

6. Allow users to select billing codes on print jobs.

See [Set up users to use billing codes](#).

7. Edit the reminder template so it refers to the SafeCom G4 Web Interface, that is, the Billing web page.

See [Edit the template for billing reminder](#).

8. Work with the tracking data.

Use the Data Mining tool to view the tracking data (see [SafeCom Data Mining](#)).

Configure SafeCom Client Billing

Perform the following steps to:

- Configure the billing codes and how they are displayed for the users.
 - Set the elapse time before billing codes are committed to tracking.
1. In the SafeCom Administrator, click on the **Servers** menu and choose **Server properties**.
 2. Click on the **Billing** tab.
 3. Depending on whether you are working with one-level or two-level billing codes, perform the following steps:
 - If you are working with one-level billing codes, enter a primary code that coincides with terms used within your organization.
 - Select **Secondary code** to use 2-level billing codes, composed of a primary (Client) code and secondary (Matter) code. Enter the codes (Client code and Matter code) to match the terms used within your organization.
 4. Configure how the codes should be displayed to the user at the printer or on the SafeCom Web Interface.
 - a. Under **Display format**, specify the field order of the primary code, the primary description, the secondary code, and the secondary description.

You can choose not to display all by selecting **<None>**. For example, select **Primary code** in the first drop-down and **Secondary code** in the second drop-down. In the third drop-down, if you select **<None>**, nothing else is displayed.
 - b. Under **Size**, set the field abbreviation value to a number between 0 and 50.

The number indicates the number of characters (including the separators) the displayed text has. 0 indicates that the text should not be abbreviated.
 - c. Specify the type of separator you want to use.

Three periods (...) are added to the displayed text to indicate that it is abbreviated. See the following examples:
- Example:**
- Two-level code with default order of fields, comma as separator, and an abbreviation of descriptions to 12 characters.
`0123, Ajax Interna..., 4567, Project Mana...`
 - Two-level without separator and without abbreviation, but with primary code and secondary code first followed by the corresponding descriptions.
`01234567Ajax InternationalProject Management`
5. Select **Store tracking data temporarily to allow users to apply billing codes**.
 6. Specify the period where the users can still modify billing codes to a job already sent.

After this period of time has passed, the billing data is committed and moved to the tracking data.

i In a multiserver environment, tracking data within the billing window is not collected by the primary server.

7. Specify under **Commit billing records** how often you want to move billing records to tracking data.
8. Click **OK**.
Once this is done, you can see the tracking records and selected billing codes when you export tracking data (see [Work with tracking data](#)).

Import billing codes

This chapter is about the import of billing codes. The import is completed through a wizard that takes you through the necessary steps.

The import file with billing codes must be a CSV file, saved as a *.txt file.

The following are examples of a one-level and two-level CSV file, where the first line is a header. The billable field can be 0 (not billable) or 1 (billable). The billing code and the billing code description can each consist of maximum 50 characters.

i You do not get a notification if the billing code or description exceeds the allowed number of characters.

One-level billing code example

```
Code;Description;Billable
10102;Human Resources;0
10103;Acme Project;1
```

Two-level billing code example

```
Code1;Description1;Code2;Description2;Billable
1;United States;002;Athletics;1
1;United States;004;Basketball;1
1;United States;011;Modern pentathlon;0
44;United Kingdom;002;Athletics;1
44;United Kingdom;008;Football;1
44;United Kingdom;011;Modern pentathlon;0
45;Denmark;008;Football;1
45;Denmark;011;Modern pentathlon;0
46;Sweden;002;Athletics;1
46;Sweden;008;Football;1
```

1. In the **Servers** menu, click **Client Billing** and **Import billing codes**.
2. To schedule a new import of billing codes, click **Add**.
3. Enter the **Server address** (hostname or IP address), the **User logon** with administrator rights, and the **Password**.
 - In a multiserver installation, you should specify the primary server for best performance, then click **Next**.
4. Click **Next** to select the CSV file you want to import billing codes from.
The content of the file has to be structured as a CSV file. (See examples in [Import billing codes](#).)
 - **When run by SafeCom server:** Specify the path to the file to import billing codes from in a scheduled import. The file name must be specified with full path as seen from the SafeCom

server and the account that runs the SafeCom service (normally the **Local System** account) must have read access to the CSV file.

- **Same as server filename:** Clear if you want to use a different CSV file for an immediate billing code import (**Run now** functionality). Specify the path to the file to import billing codes from in the **When run locally from SafeCom Administrator** dialog.

i The CSV file must be a *.txt file. When browsing, remember to select **All files** to make *.txt files visible.

5. Click **Next** to specify the format of the CSV file that you want to import from.

Indicate with numbers from which location in the CSV file the values should be retrieved. Leave a field value of 0 to avoid import from the specific location.

If you are working with two-level billing codes, you need to specify the location of the primary code, the primary description, the secondary code, and the secondary description.

If the first line in the CSV file is a header, you need to select **First line in file is a header**. Then the specific name of the location, rather than the number, needs to be specified.

If two-level billing codes are used, the dialog looks like as follows:

The screenshot shows the 'Billing Import' dialog box with the 'Specify CSV fields' tab active. On the left, a sidebar lists steps: 1. Overview, 2. Server, 3. File source, 4. Configuration (selected), 5. Extra, and 6. Schedule. The main area contains the following fields and options:

- Separator character: ;
- First line in file is a header
- Primary code field: Code1
- Primary description field: Description1
- Secondary code field: Code2
- Secondary description field: Description2
- Billable field: Billable

At the bottom, there are four buttons: Cancel, < Back, Next >, and Close.

i The field names are case insensitive.

6. Specify in the field **Separator character** the separator used in the CSV file (default is semicolon). Click **Next**.
7. Select the options as required according to the descriptions below.
 - **Add billing codes:** This imports all billing codes in the file.
 - **Modify billing codes:** This modifies any existing billing codes according to the imported values.
 - **Delete billing codes:** This deletes existing billing codes that do not appear in the import file.
 - **Max difference:** Use this to control if an import should be cancelled if the difference between the imported file and the existing billing codes are too big. A value of 0 (zero percent) will cause the import to take place regardless to the difference in percentage.
 - **Use extra configuration:** If a special billing code import module has been supplied, you should select this check box and enter the configuration according to the supplied instructions.
8. Click **Next**.

9. In the **Scheduled billing code import** dialog, select the schedule option according to descriptions below.
- **Name:** Specify a name for the import.
 - **Manual:** The import must be run manually.
 - **One time only:** Specify the **Start date** and **Time** for the import, and that it is run only once at that specific time.
 - **Daily:** Specify the **Start date** and **Time** for the import and how often you want to perform this task.
 - **Every 1, 2, 4, 6, 12, or 24 hour:** The import starts running from the specified start time.
 - **Weekdays:** The import runs once a day, Monday through Friday, at the specified time.
 - **Every 1, 2, 3, etc. day:** The import starts running at the specified time.
 - If needed, specify the **End date** as well.
 - **Weekly:** Specify the **Start date** and **Time** for the import and how often you want to perform this task on a weekly basis. Also select the days of the week when you want the import to run, and if needed, specify the **End date**.
 - **Monthly:** Specify the **Start date** and **Time** for the import and how often you want to perform this task on a monthly basis. Also select the specific months of the year when you want the import to run, and if needed, specify the **End date**.

i If an **End date** is specified, the import task will be deactivated by midnight on the date specified.

10. Click **Finish**.

The billing schedule appears in the **Billing Import** dialog, from where you can edit, delete, or run the billing code schedule.

Run a billing report

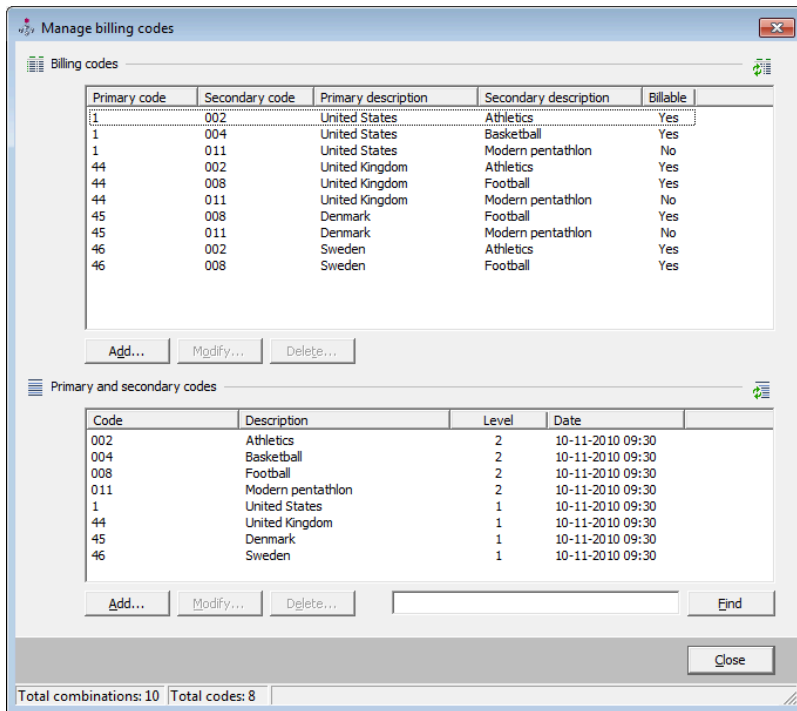
1. Select the billing code schedule in the list.
2. Click **Run now**.
When the import has finished successfully, the **Billing import** dialog opens.
3. Click **Show log** to see the import log.

Once the import is run and the billing codes are imported, they can be viewed in the **Manage billing codes** dialog (see [Manage 1-level billing code](#)), and also be added as favorites for specific users in the **User properties** (see [Billing](#)).

View billing codes in the Manage billing codes dialog

1. Click **Servers, Client Billing**, and **Manage billing codes**.
2. To refresh the dialog, click the green refresh button in the top right corner or click **Find** and then **Yes** to retrieve all billing codes.

The following screenshot shows the **Manage billing codes** dialog, when working with two-level billing codes:



Billing code import log file

During the import, a log file is created with information about the input parameters, RunTime messages, and the statistics for the import of billing codes. The statistics include the number of billing codes added, modified, and deleted during the import.

The log file is named **<Billingyyyymmddhhmmss.log>**.

- yyyy specifies the year
- mm specifies the month
- dd specifies the day
- hh specifies the hour
- mm specifies the minutes
- ss specifies the seconds

The log file is stored in the logfiles folder below the SafeCom G4 installation folder. The default folder is:

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

On **Windows 64-bit**:

```
C:\Program Files (x86)\SafeCom\SafeComG4\logfiles
```

If the same billing code exists twice in the same import file, the following RunTime message appears:


```
Not able to add Billing code <BillingCode>. cc = 131
```

This means that the billing code is added, but only once.

Set up users to use billing codes

For users to be able to use billing codes, this must be set up in the **User properties**.

1. Open the **User properties** by double-click a specific user in SafeCom Administrator.
2. Click the **Settings** tab.
3. Make sure that either **Tracking** or **Pay**²³ is selected under **Cost control**.
4. Select **Bill clients for cost** under **Print documents**.
5. Select **Restrict choice of billing codes** if the user should only be able to select from the billing codes on the predefined list of favorite billing codes.
If **Restrict choice of billing codes** is not checked, the user can use the SafeCom G4 Web Interface to add and delete billing codes to the list of favorite billing codes.
6. Click **OK**.

 When importing users, you can specify that the settings from the default user should be applied to the imported users. This could be, for example, the **Bill clients for cost** parameter if this is set up for the default user.

Considerations when using Tracking and Pay

This section describes how **Tracking** and **Pay** affect billing.

- If the user is set to **Tracking** and **Bill clients for cost** and only has one **Favorite** billing code, then that one billing code will be used when printing. In order not to use that billing code, the user must access the **Account** icon on the printer and press **No billing**.
- If the user is set to **Tracking** and **Bill clients for cost**, and if the user has more than one **Favorite** billing codes, then the user must select the specific billing code by pressing the **Account** icon on the printer. Otherwise, the print job is not billed.
- If the user is set to **Pay** and **Bill clients for cost**, then the user must select a billing code at the printer by pressing the **Account** icon. Otherwise, the print job is not billed and the user is charged for the job.
- If a billing code is added during print submission, it is preserved and not overridden by, for example, a billing code selected at the device.

Change the Bill clients for cost property of multiple users

1. Use **Find users** to get a list of relevant users.
2. Perform one of the following steps:
 - To select consecutive users, click the first user, press and hold down Shift, then click the last user.
 - To select non-consecutive users, press and hold down Ctrl, then click each user.

²³ A Pay user is not charged for the job if a billing code is selected.

- To select all users in the window, press Ctrl + A.
3. Open the **User properties** by pressing Alt + Enter or by right-clicking the selected users and selecting **User properties**.
 4. Click the **Settings** tab and make the changes as described above.

Add favorite billing codes for a user

When a user selects a billing code to a print job, the user can select a billing code from a list of 10 last used billing codes or from the favorite billing codes list.

The list of favorite billing codes is a list of the billing codes that are relevant to a specific user or group. This is set up in the SafeCom Administrator, but in some cases, users can select the favorite billing codes themselves through the SafeCom Web Interface.

In the SafeCom Administrator, favorite billing codes can be applied to a specific user or user group.

1. Open the **User properties** for on a specific user in SafeCom Administrator.
2. Click the **Billing** tab.
3. In the menu under **Add billing code favorite**, select the billing code that you want to add and click **Add**.

The billing code is now listed under **Billing code favorites** with the **Source** column specified as **User**. The list also shows the billing code favorites that are added to groups that the user is a member of. These are specified with **Group** in the **Source** column.

A favorite billing code can be removed again from the list if you select it and click **Delete**.



- On the **User properties** dialog, it is not possible to delete group-favorite billing codes. This must be done from the **Group properties** dialog (see [Select favorite billing codes for a group](#)).
- A user's billing code favorites are replicated to all secondary servers, which means that a user is still able to view and use the favorite billing codes even if the home server is changed. This does not apply to **Last used** billing codes. (To see what elements are replicated between secondary servers, see [Check that the replication is working](#).)

Select favorite billing codes for a group

1. Open the **Group properties** dialog.
2. Click the **Billing** menu.
3. Click **Add** to add the selected billing code to the **Billing code favorites** list.
The group billing code can be removed from the list by clicking **Delete**.
4. Click **OK**.

Edit the template for billing reminder

If the user has enabled the **Reminder** on the SafeCom web interface, an e-mail is sent to remind the user about selected billing codes to the print job. The user can set up the e-mail to be sent either:

- As soon as a job completes.
- When the specified number of jobs have been completed.

This is set up in the SafeCom web interface as well.

The e-mail is based on the EmailBilling.txt template which is located in the %SafeCom%\Templates folder. The %SafeCom% indicates the SafeCom installation folder, normally:

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

On Windows 64-bit:

```
C:\Program Files (x86)\SafeCom\SafeComG4
```

The e-mail template looks as follows:

EmailBilling.txt

```
<%SUBJECT="[SafeCom] Billing notification"%>
This mail is to inform you that
you now have <%BILLINGJOBS%> jobs that require
your choice of billing code.
Click the link below to go to the billing web page:
<%BILLINGLINK HOST="http://safecomserver/safecom/"%>
www.safecom.eu.
```

Use the e-mail template for billing reminder

1. Open the EmailBilling.txt file in an editor such as Notepad.
2. Replace the `http://safecomserver/safecom/` link with the link to the server that hosts the SafeCom G4 web interface.
3. Customize or translate the message to accommodate the users.
4. Save the file into the %SafeCom% folder. If you leave it in the %SafeCom%\Templates folder, it does not take effect.

Manage 1-level billing code

In the following sections, it is covered how to manage one-level billing codes. In the **Manage billing codes** dialog, it is possible to:

- Add billing codes
- Find billing codes
- Delete billing codes
- Modify billing codes

i To manage one-level billing codes, it must be configured in **Server properties > Billing tab**. The **Secondary code** check box must be cleared.

Add billing code

To add billing codes manually from SafeCom Administrator, perform the following steps:

1. Click the **Servers** menu, click **Client Billing**, then open the **Manage billing codes** dialog.
2. Under **Billing codes**, click **Add** to add a new billing code.
3. Enter a **Code** and a **Description** in the **New billing code** dialog.
4. The new billing code is billable by default, so clear **Billable** if you do not want it to be billable. Click **OK**.

The billing code can now be viewed in the **Manage billing codes** dialog.

Find billing codes

1. Open the **Manage billing codes** dialog.
2. Enter your search criteria in the search box and click **Find**.
If the search box is left empty, all billing codes are retrieved.

i The Find button uses case insensitive, free-text search across the Code and Description columns.

Delete billing codes

1. Open the **Manage billing codes** dialog.
2. Use the **Find** button to retrieve all relevant billing codes.
3. Select the billing codes and click **Delete**.
4. Click **Yes** in the **Confirm** dialog to delete the billing codes.

i If a user selects a billing code for a print job at the computer, and if then the billing code is deleted from SafeCom before the user collects the print job the printer, the billing code for the print job is not remembered. The billing information is then replaced by N/A.

Modify billing codes

1. Open the **Manage billing codes** dialog.
2. Use the **Find** button to retrieve all relevant billing codes.
3. Select a billing code and click **Modify**.
4. Modify **Description** and **Billable** as required, then click **OK**.

i You cannot modify the code for the billing code, only the description and whether it needs to be billable. This applies to both imported and manually created billing codes.

Manage 2-level billing code

In the following sections, it is covered how to manage two-level billing codes. In the **Manage billing codes** dialog, it is possible to manage both billing codes, primary codes, and secondary codes.

Under **Primary and secondary codes**, the available primary and secondary codes are listed. In the **Level** column, it is specified if the code is level 1 or level 2.

Under **Billing codes**, the available combinations of the primary and secondary codes are listed. Primary codes, secondary codes, and descriptions are both specified, and also whether the code is billable.

i Because the billing codes are combinations of the primary and secondary codes, it is advised to add the primary and secondary codes first and then the billing codes.

Here is an overview of the following sections:

Primary and secondary codes:

- Add primary or secondary codes
- Find primary or secondary codes
- Delete primary or secondary codes
- Modify primary or secondary codes

Billing codes:

- Add billing codes
- Delete billing codes
- Modify billing codes


i To manage two-level billing codes, it must be configured in **Server properties > Billing tab**. The **Secondary code** check box must be selected.

Add primary or secondary code

1. Click the **Servers** menu, click **Client Billing**, then open the **Manage billing codes** dialog.
2. Under **Primary and secondary codes**, click **Add**.
3. Enter a **Code** and a **Description**.
4. Select the **Level** (Primary 1 or Secondary 2) and click **OK**.


Find primary or secondary codes

1. Open the **Manage billing codes** dialog.
2. Enter your search criteria in the search box and click **Find**.
If the search box is left empty, all codes are retrieved.

 The Find button uses case insensitive, free-text search across the Code and Description columns.

Delete primary or secondary codes


1. Open the **Manage billing codes** dialog.
2. Use the **Find** button to retrieve all relevant codes.
3. Select the codes and click **Delete**.
4. Click **Yes** in the **Confirm** dialog to delete the codes.

 When you delete primary or secondary codes, the billing codes that contain the specific primary or secondary codes are also deleted.

- If a user selects a billing code for a print job at the computer, and if then the billing code is deleted from SafeCom before the user collects the print job at the printer, the billing code for the print job is not remembered. The billing information is then replaced with N/A.


Modify primary or secondary codes

1. Open the **Manage billing codes** dialog.
2. Use the **Find** button to retrieve the relevant codes.
3. Select a code and click **Modify**.
4. Modify **Description** and **Billable** as required, then click **OK**.

 You can only modify the description of a primary or secondary code.

Add billing code

1. Make sure that at least one primary and one secondary code is already added.
2. Open the **Manage billing codes** dialog.
3. Under **Billing codes**, click **Add**.
4. Select a **Primary code** and a **Secondary code**.
5. Clear **Billable** if you do not want the billing code to be billable, then click **OK**.

 Click **Add new primary code** or **Add new secondary code** to add codes that are not already available from the menus.

Delete billing codes


1. Open the **Manage billing codes** dialog.
2. Under **Billing codes**, find and select the billing codes you want to delete and click **Delete**.
3. Click **Yes** in the **Confirm** dialog to delete the billing code.

Modify billing codes

1. Open the **Manage billing codes** dialog.
2. Use the **Find** button to retrieve all relevant billing codes.
3. Select a billing code and click **Modify**.
4. Change the choice of **Primary code** and/or **Secondary code**.
5. Click **Modify**.

Work with Tracking data

Use the Data Mining tool to view and work with the tracking data created with relations to billing codes. See more at [SafeCom Data Mining](#).

 If a print job is sent to the printer with an assigned billing code, and before printing the job, the billing code is deleted from the server, then once the job is printed, it is tracked without a billing code.

Chapter 11

SafeCom Pay

The SafeCom Pay module provides total print cost management. In addition to the [SafeCom Tracking module](#), the module can be used to prevent a user from printing if the account balance falls below a specified limit (default zero credits).

The SafeCom Administrator (see [Cashier](#)) can be used to add (deposit) or subtract (withdraw) credits from the user's account. Credits are equivalent to money.

Planning your SafeCom Pay solution

When planning your SafeCom Pay solution, you need to:

- Define what the cost of printing should be. This is accomplished through a [charging scheme](#).
- Plan how you will secure the data stored in the tracking server and money server databases (see [Backup and restore](#)).
- Control what happens if the money server is unavailable (see [Tracking](#)).
- Select an [accounting policy](#).
- [Ensure that users pay](#).
- Investigate if a [cashless solution](#) is required.
- [Change the cost control property to Pay](#).

Accounting policy

There are three different accounting policies:

- **Full cost recovery:** The user has to pay for all prints (and copies). This policy is popular in libraries. Involves account 1 only.
- **Partial cost recovery:** The user is given a certain amount of credits on their account 2. When the credits run out, the user can choose to add money to their account 1. This policy is popular at universities.
- **Quota control:** The user is given a certain amount of credits and can print until they run out (quota is used). This policy is popular in schools that do not allow fee-based printing. Involves using account 2 only.

In addition, you need to decide if [Post track](#) should be enabled, in which case, Pay users may be charged a different (lower) price compared to the price they were given when they collected their document.

Ensure that users pay

The introduction of a fee-based printing solution may tempt users to try to avoid paying for their prints (and copies). To suppress these attempts, you can apply a number of counter-measures:

- **Make all printing go through SafeCom**
- **View the list of unfinished jobs:** The SafeCom Tracking database records information about unfinished print (and copy) jobs. An unfinished job may be caused by legitimate network or printer failure. However, the cause may also be purposely tampering with the printer and SafeCom hardware. The list of unfinished (failed/interrupted) jobs can be viewed in [SafeCom Data Mining](#).
- **Notify administrator by e-mail:** You can configure your SafeCom solution to send an e-mail to the administrator whenever a job does not finish. By looking at (and perhaps sorting) the list of received e-mails, the administrator can quickly spot if someone is trying to avoid having to pay. If required, the administrator can prevent the user from logging into the SafeCom solution.
- **Do not release reserved credits in case of an error:** When the user prints anything, the SafeCom solution reserves credits corresponding to the cost of the print job. When the user copies anything, the SafeCom solution reserves all the user's credits. On the **Users** tab in the **Server properties** dialog (see [Users](#)), you can request that the reserved credits are not released in case of error. The reserved credits can be released manually from SafeCom Administrator (see [Free reserved credits](#)).
- **Awareness through information:** Making users aware that the SafeCom Pay solution includes counter measures to prevent repeated attempts to avoid paying can reduce the number of attempts.

Educational institutions in particular should inform their users about these counter measures. This helps them limit the number of unfinished jobs that are likely to happen at the start of semester when new students enroll.

Cashless solution

Your SafeCom solution can be enhanced to support methods where users can make deposits to their account through the internet using SafeCom ePay.

SafeCom Pay solutions also support the use of smart cards. If the user's SafeCom account is empty, the user can use Smart Pay to finance their print activity.

Change cost control to Pay

You must enable Pay for each existing user. This is achieved by selecting **Pay** on the **Settings** tab in the **User properties** dialog.

It is possible to change the property of multiple users (see [Hide ID codes](#)).

By selecting a Pay user as the default user, you can make any user imported in the future (users who are created at first print or are added manually) a Pay user.

Credit schedule

1. Open the **Group properties** dialog.
 2. Click the **Credit schedule** tab.
 3. Enter a meaningful **Description**.
 4. In **Transaction**, select if the member's **Account 1** or **Account 2** should be **Set** to the specified **Amount** or changed with the specified amount (**Add** or **Subtract**).
 - An optional **Comment** can be entered.
 5. If the schedule is **Enabled**, it is possible to schedule credits **One time only**, **Daily**, **Weekly**, or **Monthly**.
 - Select **End date** and specify a date for when the periodic schedule should end. Ensure that the end date does not conflict with the selected frequency options. Otherwise, the credit schedule might not run.
- In the following example, members of the STUDENTS group are having their account 2 set to 100 credits on the first Monday at midnight of each month, except for the three months in summer:

Group properties - students

General
Rules
Members
Billing
Credit schedule
Disable

Schedule
Description: Monthly credits to students

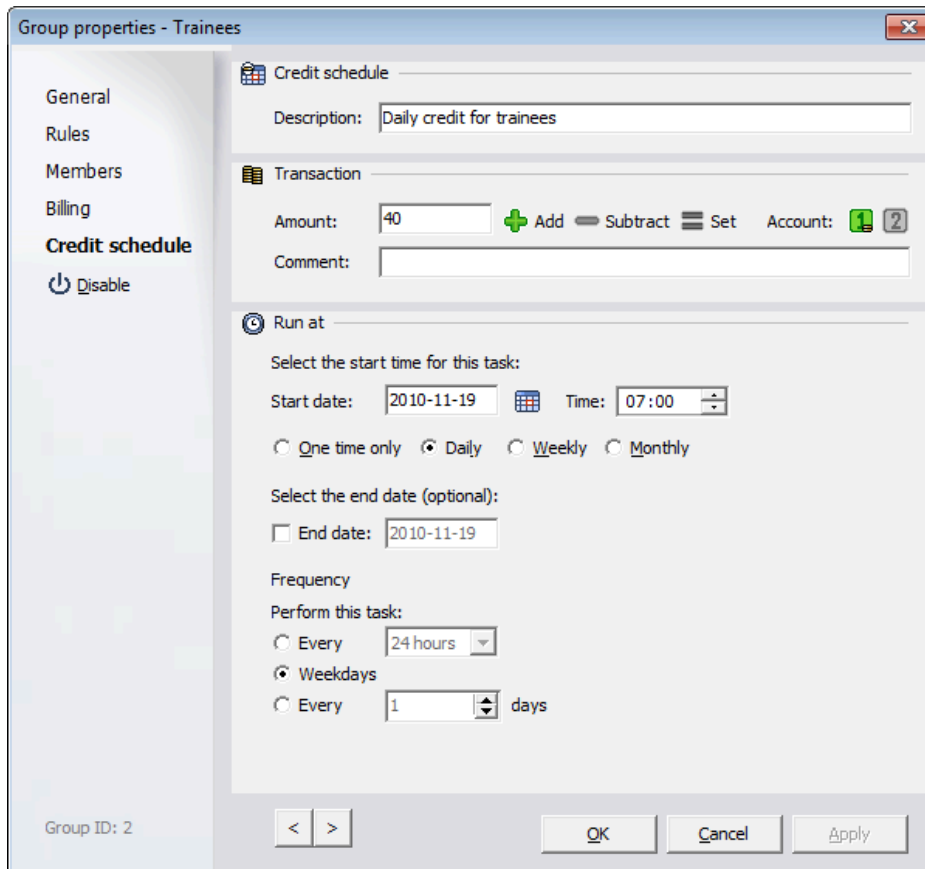
Transaction
Amount: 100 + Add - Subtract = Set Account: 1 2
Comment:

Run at
Select the start time for this task:
Start date: 2010-10-06 Time: 19:10
 One time only Daily Weekly Monthly
Select the end date (optional):
 End date: 2010-10-06
Frequency
 Day 1
 The first Monday
Of the month(s):
 Jan Feb Mar Apr May Jun
 Jul Aug Sep Oct Nov Dec

Group ID: 2

< > OK Cancel Apply

- In the following example, members of the TRAINEES group have their account 1 set to 40 credits each weekday at 07:00 am:



Cashier

The following subsections assume that you are logged into SafeCom Administrator as a user with [cashier rights](#).

Log in to SafeCom Administrator in Cashier mode




1. Click **Start**, point to **All Programs > SafeCom G4**, and click **SafeCom Administrator**.
2. In the SafeCom Administrator, click the server to log in.
3. Enter **User logon** and **Password**, then click **Login**.

i If you belong to a domain, the domain followed by a slash (/) or a backslash (\) must be specified in front of the user's logon. Example: MYDOMAIN\JS. Alternatively, you can specify the user logon followed by (@) and the domain, like this: JS@MYDOMAIN.

Find user with search string

1. Enter the search string in **Look for** and press Enter. If a card reader is installed on the computer (see [Install a card reader on a computer](#)), then present the card.

The following icons represent the outcome of the search:

		
<p>No users match the search string (red icon)</p>	<p>Multiple users match the search string (green icon)</p>	<p>No search string entered (blue icon)</p>

2. If only one user is found, the **User properties dialog** appears. Otherwise, double-click a user on the appearing list of users.




Find user through Advanced search

1. Click **Advanced search** to open the **Find users dialog**.
2. Enter your search criteria and click **Find**.

The Find function uses field-based, case insensitive, free-text search, with the exception of ID codes.

- To find a particular ID code, enter the complete **ID code** in the right case or click **Listen for card** if a card reader is installed on the computer (see [Install a card reader on a computer](#)).

The following icons represent the outcome of the search:

		
<p>No users match the search string (red icon)</p>	<p>Multiple users match the search string (green icon)</p>	<p>No search string entered (blue icon)</p>

3. If only one user is found, the **User properties dialog** appears. Otherwise, double-click a user on the appearing list of users.

User properties dialog

User properties - JS

Identification | Settings | ID code | Rights | Member of | Aliases | **Account** | Billing

Information

Full name: John Smith
 User logon: JS
 PIN code: ***** Generate random PIN
 Prevent login: Not locked

Account info

Account 1:	0,00
Account 2:	0,00
Low limit:	0,00
Reserved:	0,00
Disposable:	0,00

Transaction


Amount: do add amount on Account 1
 Comment:

Transactions Record

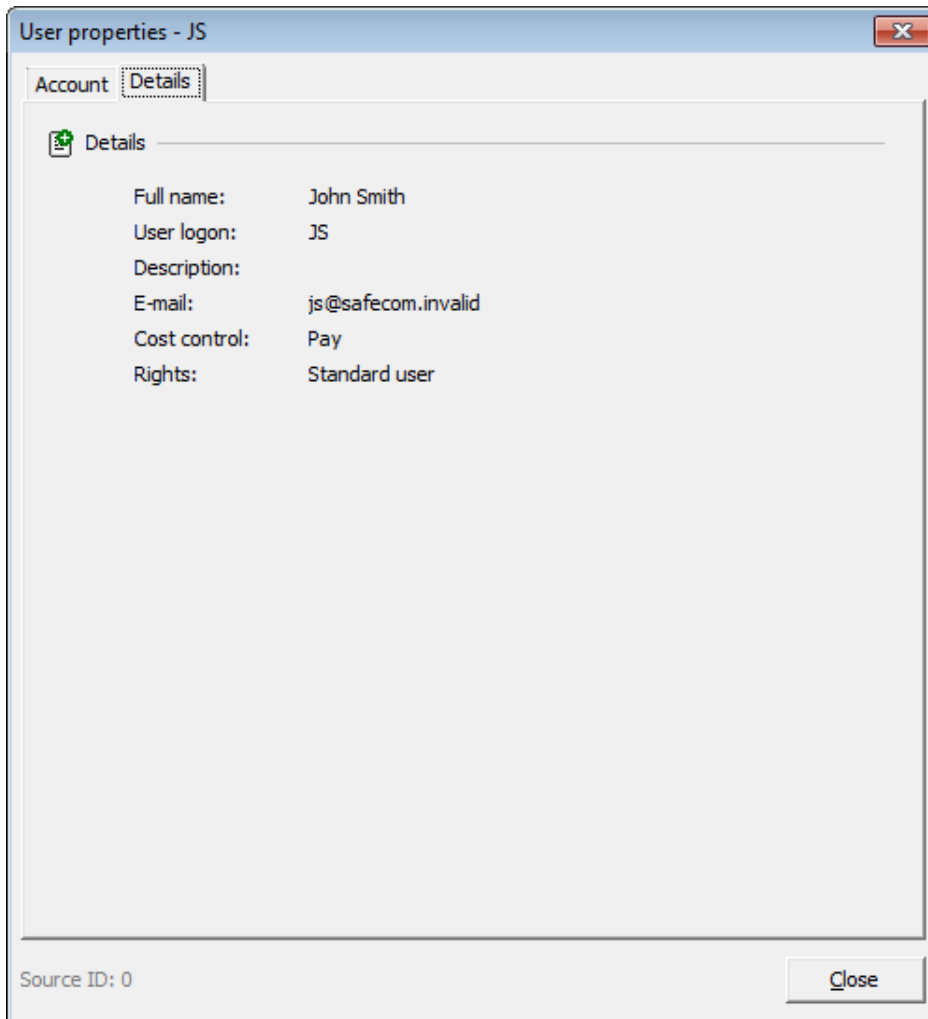
Source ID: 0 OK Cancel

- **Account 1** shows the current amount of money available to the user. **Account 2** shows the current available quota available to the user.
- **Low limit** is the lowest amount that should be available in order to print (Allows negative figures). Click to edit the Low limit.



- The user account balance needs to exceed the Low limit value to successfully log in to the device.
 - In some cases, the user may not be able to print or copy, even if the account balance exceeds the lower limit by more than the expected printing or copying cost. The user estimate may be lower than the preliminary calculation, which may include not only the price per page, but the job start-up cost too, and considers using at least one color impression. In copy job pre-calculations, the size of the document is not yet known, so SafeCom takes the Other paper size into account, which may not have the required balance.
-
- **Reserved** is the amount of credits reserved due to a print or copy job that finished in error. It should be 0.00 (zero) most of the time. If the system has reserved any credits, you see a positive amount printed in red. Click  to edit the reserved amount. The amount must be between 0.00 (zero) and the currently reserved amount of credits.
 - **Disposable** is equal to **Balance** minus **Low limit** and **Reserved**.
 - **Amount:** Type in an amount to **add** to, **subtract** from, or **set** account to. Select the appropriate action from the drop-down list. Select the appropriate account and click **Record** to carry out the transaction.
 - **Comment** allows you to add any description (optional).
 - **Transactions:** View a list of user account transactions.

Select the **Details** tab to see additional information about the user.



View user transactions

1. Open the **User properties** dialog.
2. On the **Account** tab, click **Transactions** to open the **User transactions** dialog.
3. To look at a transaction from a different period, make your **Selection** and click **Refresh**.
4. Click **Print** to make a printout of the transactions.
5. When done, click **Close**.

Issue a new PIN code

1. Open the **User properties** dialog.
2. On the **Account** tab, click **Generate random PIN**.
A new, random 4-digit PIN code is displayed.
3. Click **Close**.

Unlock user

1. Open the **User properties** dialog.
2. On the **Account** tab, click **Unlock user**.
3. Click **Close**.

Deposit credits


1. Open the **User properties** dialog.
2. On the **Account** tab, select **Account 1** (money) or **Account 2** (quota).
3. Enter an **Amount** and select **add amount** from the drop-down list.
4. Enter an optional **Comment** and click **Record**.
5. Click **Close**.

Withdraw credits

1. Open the **User properties** dialog.
2. On the **Account** tab, select **Account 1** (money) or **Account 2** (quota).
3. Enter an **Amount** and select **subtract amount** from the drop-down list.
4. Enter an optional **Comment** and click **Record**.
5. Click **Close**.

Set low limit

Low limit is the amount of credits that must be available in order to print (and copy).

1. Open the **User properties** dialog.
2. On the **Account** tab, click  and enter a **Low limit**, then click **OK**.


The amount is normally 0.00, but it can be both positive and negative.

3. Press **Enter**.

Free reserved credits

If the system has reserved any credits, you can see a positive amount printed in red in the **User account** dialog. See [Prevent cheating](#) for a discussion about reserved credits.

To free the reserved credits, perform the following steps:

1. Open the **User properties** dialog.
2. On the **Account** tab, click  next to the reserved amount and enter the amount that must be released.
3. Press **Enter**.

Reset cash cards

This section is only relevant if the SafeCom Pay solution stores money on a Smart Card. The dialog displays **Temporary card: <amount>** in red when the user had the specified amount transferred from the cash card to the SafeCom account on the SafeCom server.

i If you click **Reset**, the money is not transferred back to the user's cash card the next time the cash card is used at one of the SafeCom-enabled printers.

1. Open the **User properties** dialog.
2. On the **Account** tab, click **Reset**.
3. Click **Close**.

Detect attempt to avoid paying

The SafeCom Pay solution can be configured to send an e-mail to the administrator whenever a SafeCom session does not terminate appropriately.

1. Log in to SafeCom Administrator as an administrator.
2. Log in and open the **Server properties** dialog.
3. Click on the **E-mail** tab.
4. Select **E-mail notification on credits reserved**.

For additional information, see [Prevent cheating](#).

Print reports

It is possible to print a number of reports, including:

- [Account status](#)
- [Cash flow report](#)
- [Transactions](#)

See the relevant sections for additional information.

Account status

1. In the **Cashier** menu, click **Account status** to view and print the credit status, which includes the following information:
 - Total credits in the system
 - Total reserved in the system
 - Total temporary cash cards²⁴

²⁴ SafeCom Pay solutions with money stored on a Smart Card.

The **Cash card** tab is only available if the SafeCom Pay solution stores money on a Smart Card. On the **Cash card** tab, it is possible to see a list of the users who temporarily has had money transferred from their cash card to their SafeCom account on the SafeCom server. This money will be transferred back to the user's cash card the next time the cash card is used at one of the SafeCom-enabled printers.

2. Click **Print** to print a hard copy of the reports.

Cash flow report

1. In the **Cashier** menu, click **Cash flow report** to view and print a cash flow report for a specified period.

The cash flow report can be of the following types:

- Cashier, Account 1
- Cashier, Account 2
- ePay

2. Select the period.

A number of predefined periods are available ranging from today to 1 year back.

- Select **Specify period** to freely specify the beginning (from) and finish (to) of the period.

3. Click **Refresh** to view the transactions for the selected period.

4. Click **Print** to print the cash flow report.

The cash flow report contains a list of transactions, detailing the **ID**, **Date/Time**, **Type** (Cashier or ePay), **Account**, **Value**, and **Comment**. In case of ePay, the **Comment** column contains the ePay order number.

- Select **Personalize** if the report should only include transactions conducted by the user that is currently logged into SafeCom Administrator.

User transactions dialog

1. In the **User properties dialog** on the **Account** tab, click **Transactions**.

2. Select to see the last 20, 50, or 100 transactions, then select among the predefined periods. Select **Specify period** to freely specify the beginning (from) and end (to) of the period.

3. Click **Refresh** to view the transactions for the selected period.

4. Click **Print** to print the report.

- **Current values** shows the **Balance**, **Low limit**, **Reserved**, and **Disposable** values.
- **GID** is an identification number for the transactions.
- **Date/Time** indicates the date and time of the transaction.
- **Author** is the user logon of the user who did the transaction.
- **Type** indicates the type of the transaction.
- **Description** shows the description (if any) of the transaction.
- **Value** indicates the amount that has been added/subtracted from the account.

- **Account 1** shows the balance on the account with real money. **Account 2** shows the balance on the account with quota.
- **Card** is only present if the SafeCom Pay solution stores money on a Smart Card. It shows the amount that has been transferred from the cash card to the SafeCom account on the SafeCom server. Select **Merge Cash Card** to see the transactions that involve the cash card.
- Select **Show reservations** if you want to see the reservations.

Prevent cheating

To ensure user payment and prevent cheating, the SafeCom solution can reserve all or some user credits whenever a Pay user logs in to SafeCom to copy or print.

E-mail template for an unfinished job

If the SafeCom session does not terminate correctly, an e-mail is sent to the administrator based on the **UnfinishedJob.txt** e-mail template. The reserved credits are freed as soon as the e-mail has been sent.

This functionality is controlled through the **Server properties** dialog:

- Select **E-mail notification on credits reserved** on the **E-mail** tab in the **Server properties** dialog.
- Select **Release credits reserved on error** on the **Users** tab in the **Server properties** dialog.

UnfinishedJob.txt

```
<%SUBJECT="[SafeCom Unfinished Job] <%USERLOGON%>"%>
This mail is to inform you about an unfinished job.
Credits
-----
Reserved: <%RESERVEDCREDITS%>
Job properties
-----
Job name: <%DOCUMENTNAME%>
Pages: <%PAGES%>
Date: <%STARTDATE%>
Device properties
-----
Device name: <%DEVICENAME%>
IP address: <%DEVICEIPADDR%>
MAC address: <%DEVICEMAC%>
Model: <%DEVICEMODEL%>
Location: <%DEVICELOCATION%>
User properties
-----
User logon: <%USERLOGON%>
Full name: <%FULLNAME%>
E-mail: <%EMAIL%>
```

Difference between print and copy

When a user prints, the SafeCom solution reserves credits corresponding to the cost of the print job or document. When a user copies, the SafeCom solution reserves all their credits.

The table below describes how the print and copy values differ in an unfinished job e-mail.

Tag	Pull print	Copy
<%RESERVEDCREDITS%>	Cost of the document.	Calculated sum of user credits, from start of copy job minus cost of pages copied and tracked.
<%DOCUMENTNAME%>	Name of the document.	Always "Copy job".
<%PAGES%>	Number of document pages. Number of pages actually printed not possible to calculate.	Number of tracked copy pages. Additional pages may have been copied.

Job name pricing

Job name pricing allows you to impose print charges based on the print job name. This was originally developed for libraries to allow borrowers to print search results and electronic articles for free or for a fixed amount.

The name of the print job is compared against a list of conditions (filters). If one of the conditions is met, the document is priced according to the specified price. If none of the conditions are met, the document's price is calculated according to the defined charging scheme.

To enable job name pricing for a printer, perform the following steps:

1. Select **Enable job name pricing** on the charging scheme that is used by the printer (see [View charging scheme properties](#)).
2. Modify the `JobNamePricing.txt` file to match your requirements.
3. [Restart the SafeCom service](#).

JobNamePricing.txt

The pricing based on job names is controlled from the text file `JobNamePricing.txt` located in the SafeCom Templates folder located in the SafeCom installation folder. The default path is `C:\Program Files\SafeCom\SafeComG4`.

1. Copy the `JobNamePricing.txt` file from the Templates folder to the SafeCom installation folder.
2. Modify the `JobNamePricing.txt` file in the SafeCom installation folder to match your requirements.
3. [Restart the SafeCom service](#).



- Subsequent modifications to the file in the SafeCom installation folder take immediate effect.
- In multiserver environments, ensure that you have the modified `JobNamePricing.txt` file present on all primary and secondary servers in the correct location.

You can add as many filters and prices as you want. You can use a maximum of 4 wildcards ("*") in a filter. The filters are case sensitive. The price must be specified with a decimal point (".").

```
-----  
; This file specifies print jobs to be given a  
; special price if job name is matching a  
; certain filter.  
;  
; The '*' character is used as wild card.  
; Maximum 4 '*' (wild cards) is allowed per filter.  
;  
; (c) 2003 SafeCom A/S  
-----  
Version="1"  
Price1="0.00"  
Filter1="Test Page"  
Price2="0.10"  
Filter2="http*safecom.eu*"  
Filter2="safecom*.PDF*"
```


Chapter 12

SafeCom Device Utility

SafeCom Device Utility is an application used to load SafeCom device software onto devices in preparation for a staged rollout. It requires logging in to SafeCom server as an administrator or a technician. It is possible to load and save lists of device addresses as *.dip.

SafeCom Device Utility can also be used to upload, edit, save, and download configuration files from SafeCom controllers and devices that have SafeCom software inside. It does not register devices to the SafeCom system.

SafeCom Device Utility is part of the SafeCom G4 software and is started by clicking scDevUtil.exe. It is installed by the server and tool installers. It requires the presence of the files: scDevUtilLib.dll, scSNMPLib.dll, scSecureLib.dll, and scUtilib.dll.

Start SafeCom Device Utility

1. Double-click scDevUtil.exe in the SafeCom installation folder.
Details on how to populate the list of devices are in section [Populate list of devices](#). **Edit configuration** is covered in section [Edit configuration](#).
2. Login as Administrator or Technician to SafeCom.
3. Click **Status** to enable status updates from the listed devices every 30 seconds.
4. Click **Refresh** to update the list of devices and their status.

Menus and commands

This table lists the menus and commands for the SafeCom Device Utility.

Menu	Action	Description
File	Load device list from file...	Load the devices from a plain text file.
	Save device list to file...	Save the list of devices as a *.dip file.
	Options	Specify a default configuration file for the devices.
	Exit	Exit the SafeCom Device Utility.
Action	Send Go Loader...	Send the Go Loader software to the selected devices.
	Update software...	Send the SafeCom Go file to the selected devices.

Menu	Action	Description
	Configuration	Modify and work with the device configuration options, including editing, saving, loading, and loading from a default configuration file.
	Get serial number	Display the serial number of the selected device.
	Restart device...	Restart the device.
	Remove device from list	Remove the device from the list.
	Open in web browser...	Open the device in a web browser.
Help	About...	View the version number for SafeCom Device Utility.

Populate list of devices

With SafeCom Device Utility, there are three ways to add devices to the list of devices:

- **Load from file:** Create a plain text file with one address (IP address or hostname) per line and save it with the extension dip (Device IP file). In the **File** menu, click **Load device list from file**.
- **Add device:** Enter the **Device address**, click the > button next to the **Broadcast** button, enter the SNMP community name into the **Community** field, and click **Add**.
- **Broadcast for devices:** Click the > button next to the **Broadcast** button, enter the SNMP community name into the **Community** field, and click **Broadcast** to broadcast for devices.


Edit configuration

1. Select a device and click **Edit configuration** to retrieve the configuration from the selected device and open the editor.

Configuration files are human readable.

- Configuration files from SafeCom Go devices are in XML format.
- Configuration files from SafeCom Controllers are in a special format with BEGIN_CONFIGURATION and END constructions.

2. Click **Update** when done editing (or viewing) or click **Cancel** if you do not want to modify the configuration file.
3. In the **Action > Configuration** menu, click **Save configuration to folder** to optionally save the file for subsequent use.

 All activities performed by the SafeCom Device Utility are logged in the DevUtilNNN.trc file in the specified folder if SafeCom logging is enabled on your computer.

Set configuration

The configuration that is currently uploaded can be loaded to one or more selected devices if the devices are of the same type. This can be used to clone entire configurations from one device to other devices.

1. Click **Edit configuration** and **Update** to load the current configuration to the selected devices of the same type.
2. Enter the **User name** and the **Password** of the device.
 - Select **Same for all devices** if you are updating multiple devices that are configured with the same user name and password.

For SafeCom Controller, the default user name and password is "adm".

A dialog appears saying either "Set configuration succeeded" or "Set configuration failed".

3. Click **OK**.



- To change the SNMP Get community name on HP Go embedded devices, the following XML content has to be sent:

```
<?xml version="1.0" encoding="utf-16"?>
<CONFIGURATION>
  <DEVICE>
    <COMMUNITY_NAME_RAW>newcommunityname</COMMUNITY_NAME_RAW>
  </DEVICE>
</CONFIGURATION>
```

- To enable the installation of SafeCom Go software on HP devices, please make sure that the check box Allow firmware upgrades sent as print jobs (port 9100) at **EWS > Security > General security** is set.
- All activities performed by the SafeCom Device Utility are logged in the DevUtilNNN.trc file in the specified folder if SafeCom logging is enabled on your computer.

Manage devices in batch

The command line utility scDevUtilConsole64.exe (64-bit application) provides functionality similar to the SafeCom Device Utility. It is part of the server and tool installers. It can install SafeCom Go software on target devices and retrieve and send the configuration parameters of them. It can work with a single device or manage multiple devices to ensure the appropriate data files are passed in the command line argument. The utility supports the following device vendors:

- Canon
- HP
- Ricoh

i Although the utility does not register devices to SafeCom, it still requires a SafeCom Administrator or Technician username and password for security reasons.

Use the `-h` or `--help` parameter for a detailed description of how to use this utility.


Command line parameters

Operations	Description
<code>-i</code> or <code>--install</code>	Install or upgrade a bundle. i This may restart the device.
<code>-g</code> or <code>--getconfig</code>	Download the configuration XML file from a device.
<code>-s</code> or <code>--setconfig</code>	Upload the configuration XML file to a device.

Parameters	Description
<code>-d</code> or <code>--device</code>	Device type (HP, CANON, RICOH) Use the listed tokens to specify the vendor.
<code>-a</code> or <code>--address</code>	Device IP address
<code>-u</code> or <code>--user</code>	Device administrator username
<code>-p</code> or <code>--password</code>	Device administrator password
<code>-c</code> or <code>--community</code>	SNMP community name of device
<code>-f</code> or <code>--file</code>	File name <ul style="list-style-type: none"> File name of a Go software for operation <code>-i</code> Name of an XML configuration file for a specific vendor for operations <code>-g</code> and <code>-s</code>
<code>-v</code> or <code>--serveraddress</code>	SafeCom G4 Server address (default is 127.0.0.1)
<code>-w</code> or <code>--adminuser</code>	SafeCom Administrator logon name (mandatory)
<code>-x</code> or <code>--adminpassword</code>	SafeCom Administrator password (mandatory)
<code>-r</code> or <code>--restart</code>	Switch to restart the device after bundle installation for operation <code>-i</code>

Parameters for batch mode	Description
<code>-o</code> or <code>--optionfile</code>	Use an option file instead of the direct parameters (mandatory); applicable for multiple devices from the same vendor. The structure of the file is described later.
<code>-e</code> or <code>--stopaterror</code>	Stop at the first error when executing an option file. i In case of parallel execution, the application stops after completing all running tasks. New operations do not start after detecting an error.

Parameters for batch mode	Description
-t or --threads	How many threads will be used for batch execution (default is 1). Please consider the capabilities of the running computer.
-w or --adminuser	SafeCom Administrator logon name (mandatory)
-x or --adminpassword	SafeCom Administrator password (mandatory)

 The -r and -e commands have boolean values. To set the value to true, use "1", "y", "yes", or "true". All other values are considered false.

Structure of the parameter file

The purpose of the INI file is to specify a group of target devices and the necessary parameters of the performed operation.

The file has a [Defaults] section optionally. It specifies the common properties of devices or the operation. Any parameter in this section can be omitted as there is no common value for each device.

Properties of the [Defaults] section

address

Device address

device

Device type

user

Admin user's logon name

password

Admin user's password

community

SNMP put community name

file

Go bundle or configuration XML with full path according to the operation specified as command line parameter

restart

Restarts the device after installation of the bundle

The [Devices] section contains device-specific parameters that are unique for the target devices. The keys of INI records have no specific purpose, they just distinguish the devices. The content of the records varies depending on the requested operation.

The parameters are separated by comma. If a parameter is missing, the default value is used. The separator must be used even if the default value must be applied.

Structure of the [Devices] section for bundle installation

```
Device1=address,devicetype,user,password,community,bundlefile,restart
```

Structure of the [Devices] section for configuration handling

```
Device1=address,device,configfile
```

i The parameter file can contain different types of devices, but the performed operation is specified independently with using the special command line parameter. In other words, only one operation can be performed in a batch.

Example 1

For the command line `scDevUtilConsole.exe -i -o optionfile.ini -t 2 -w admin -v password123`, the content of `optionfile.ini` is as follows:

```
[Defaults]
address=192.168.18.75
device=hp
user=admin
password="my""hp""password"
community=mycommunity
file="c:\my_bundles\bundle.bdl"
restart=true
[Devices]
FirstDevice=,,,test,,
SecondDevice=192.168.18.76,,,,,
```

This command installs the same SafeCom Go software on two HP devices having common admin username and password and both are restarted after the operation completed. The IP address of the first device is specified in the Defaults section and the other is in the Devices section. The first device has community name property of "test" and the second one uses the default community name, "mycommunity". The operation is performed parallel because two working threads are requested in command line.

- i** The password in this sample has special characters ("my""hp""password").
- The bundle path is between quotation marks because of the space character in it.

Example 2

For the command line `scDevUtilConsole.exe -s -o optionfile.ini -t 3 -w admin -v password123`, the content of `optionfile.ini` is as follows:

```
[Defaults]
device=hp
file="c:\configurations\hpconfig.xml"
[Devices]
Device1=192.168.18.75,,
Device2=192.168.18.77,,
Device3=192.168.18.78,canon,c:\configurations\canonconfig.xml
```

This command sends configuration files to three devices. Two of them are HP devices and receive the `hpconfig.xml`. For the third one, the type of the device and the device specific configuration is provided in the Devices section, because it is a Canon device. The three devices are configured parallel to each other.

Chapter 13

Format of tracking data

This chapter describes the format of the tracking data.

Format history

SafeCom G3 S82 070.410*01

- New Client Billing, with primary and secondary code.

SafeCom G3 S82 070.400*01

- Introduced Unicode support.

Format

Parameter	Description	Default value
TrackingID	A unique ID for this tracking record.	
ComputerName	Name of the computer.	
ExportTrackingID	Contains the value of the ApplyExportTrackingID that was supplied the first time this tracking record was exported. Otherwise, it is blank. Maximum 20 characters.	
TransactionID	A unique ID that can be used to link to corresponding transaction (change of credits).	
AccountingModelUsed	The type of cost control the user was set to when copies were made or the document was printed (collected at the printer).	<u>NONE</u> PAY_AND_PRINT PRINT_AND_PAY
StartDate	The date when the user started collecting the document at the printer.	
StopDate	The date when the user's document was printed.	

Parameter	Description	Default value
TrackingState	The state of the tracking. If the state is interrupted it could indicate that an attempt was made to disconnect or otherwise tamper with the SafeCom equipment to bypass tracking.	TRACKING_STATE_COMPLETED TRACKING_STATE_INTERRUPTED
TrackingPageCount	Number of pages to use for tracking purpose of both print and copy jobs. In case of a print job (see JobType) the number of pages is normally the same as reported by ParserPageCount. However, if TrackingState is INTERRUPTED then TrackingPageCount can be less than ParserPageCount.	
ParserPageCount	Number of pages as counted by the used SafeCom Pull Port and SafeCom Push Port. This is 0 in case of a copy job (see JobType). The status of the parsing can be seen from PageCountStatus.	
DriverPageCount	Number of pages as reported by the Windows printer driver (see DriverName). This is 0 in case of a copy job (see JobType).	
JobSubmitLogon	The UserLogon of the user who submitted the document for printing. In case of distribution (P-mail) this will differ from UserLogon.	
JobName	Name of the document. Always 'Copy job' in case of copies.	
JobDate	The date when the document was submitted for printing, that is when it arrived in the SafeCom job database.	
JobSize	Number of bytes.	
UserID	The ID (internal) of the user.	
UserDomainID	The ID (internal) of the domain.	
UserLogon	The user's logon name.	
Domain	The user's domain.	
FullName	The user's full name.	
Description	Description field.	
Email	The user's e-mail.	

Parameter	Description	Default value
DeviceMac	The MAC address of the device.	
DeviceID	The ID (internal) of the device.	
DeviceName	The name of the device.	
DeviceLocation	The location of the device.	
DeviceIpAddr	The IP address of the device.	
DeviceSupportsDuplex	Whether or not double-sided print is supported.	
DeviceSupportsColor	Whether or not color is supported.	
DeviceModel	The Model name listed in the SafeCom Administrator's Device properties dialog.	
DriverName	This is the driver name. It is identical to the Model name listed in the Windows printer properties dialog.	
JobPageFormat	The paper size. Typically, A4, A3 or Letter.	
JobIsDuplex	Is the job set up for double-sided print?	YES NO
JobIsColor	Is the job a color job?	YES NO
BillingCode	The primary billing code. Maximum of 50 characters.	
BillingDescription	The primary code description. Maximum of 50 characters.	
BillingInvoice	If YES the billing code can be used to invoice clients.	<u>NO</u> YES
JobPrice	The cost of the job. Calculated based on charging scheme and job/device attributes.	
JobType	The type of job: Pull print, Push print, Copy, Fax, Scan, or E-mail.	JOB_TYPE_PULL JOB_TYPE_PUSH JOB_TYPE_COPY JOB_TYPE_FAX JOB_TYPE_SCAN JOB_TYPE_EMAIL
PageCountStatus	Indicates the status of the parsing done with the SafeCom Pull Port and SafeCom Push Port.	PAGECOUNT_STATUS_OK PAGECOUNT_STATUS_UNDEFINED PAGECOUNT_STATUS_FAILURE
UserNodeID	The internal ID of the Organizational unit the user belongs to. The ID can be seen in the Org. unit properties dialog in SafeCom Administrator.	0

Parameter	Description	Default value
DeviceNodeID	The internal ID of the Organizational unit the device belongs to. The ID can be seen in the Org. unit properties dialog in SafeCom Administrator.	0
PageCountModel	If pages were counted by software(0) or hardware(1). Pull and Push print jobs are always counted using software method.	0
TrackingColorPageCount	Number of pages with color.	
JobDestination	Empty in case of a print or copy job. If a Fax job this is the phone number of the receiver. In a Scan job this is the name of the folder. If an E-mail job this is the e-mail address of the receiver.	
TonerSave	Whether or not toner save was invoked. Reserved for future use.	YES NO
JobPrice2	The cost of the job. Calculated based on the secondary charging scheme and job/device attributes.	
PMQueueName	The name of the Windows print queue that was used to print the document through the SafeCom Push Port or SafeCom Pull Port.	
PMPortName	The name of the SafeCom Push Port or SafeCom Pull Port that was used to print.	
PMComputerName	The computer name of the computer with the Windows print queue using either the SafeCom Push Port or SafeCom Pull Port.	
DocComputerName	The computer name of the client from where the document was formatted.	
TonerCyan	The toner coverage is recorded as 100 times the coverage in percent. Example: A toner coverage of 2.5% is recorded as the 250. A toner coverage of 10000 is equal to 100%. Toner coverage is tracked for Copy, Scan, E-mail and Fax jobs on selected HP LaserJet MFPs with SafeCom Go.	0
TonerMagenta	See TonerCyan.	0
TonerYellow	See TonerCyan.	0

Parameter	Description	Default value
TonerBlack	See TonerCyan.	0
UserCostCode	User's cost code.	
JobSheetCount	Number of sheets.	
BillingCode2	The secondary code. Maximum of 50 characters.	
BillingDescription2	The secondary code description. Maximum of 50 characters.	

Chapter 14

SafeCom ID devices

SafeCom ID devices come with ID device licenses, whereas ID device licenses for third-party ID devices must be purchased separately. SafeCom offers the following stand-alone card readers:

ID devices	USB	Serial	Section
SafeCom AWID Reader	USB	Serial	SafeCom AWID Reader
SafeCom Barcode Reader	USB	Serial	SafeCom Barcode Reader
SafeCom Casi-Rusco Reader	USB	Serial	SafeCom Casi-Rusco Reader
SafeCom EM Reader	USB	Serial	SafeCom EM Reader
SafeCom HID Prox Reader	USB	Serial	SafeCom HID Prox Reader
SafeCom HID Prox Reader 37 bit (custom)	USB	Serial	SafeCom HID Prox Reader
SafeCom iCLASS Reader	USB	Serial	SafeCom iCLASS Reader
SafeCom Indala Reader 26bit	USB	Serial	SafeCom Indala Reader
SafeCom Indala Reader 29bit	USB	Serial	SafeCom Indala Reader
SafeCom Keypad	USB	Serial	SafeCom Keypad
SafeCom Legic Reader	USB	Serial	SafeCom Legic Reader
SafeCom Magnetic Card Reader (Tr 1)		Serial	SafeCom Magnetic Card Reader
SafeCom Magnetic Card Reader (Tr 2)		Serial	SafeCom Indala Reader
SafeCom Magnetic Card Reader (Tr 3)		Serial	SafeCom Indala Reader

ID devices	USB	Serial	Section
SafeCom Magnetic Card Reader DD (Tr 1)	USB		SafeCom Magnetic Card Reader DD
SafeCom Magnetic Card Reader DD (Tr 2)	USB		SafeCom Magnetic Card Reader DD
SafeCom Magnetic Card Reader DD (Tr 3)	USB		SafeCom Magnetic Card Reader DD
SafeCom Mifare Reader	USB	Serial	SafeCom Mifare Reader
SafeCom Nedap Reader	USB	Serial	

SafeCom AWID Reader

Dimensions: 6.4 x 10.6 x 2.2 cm. Color is black. Cable length: 1.8 m. When a proximity card is presented to the reader, the red light flashes green.

SafeCom Barcode Reader

Dimensions: 5.2 x 12.7 x 3.5 cm. Color is black. Cable length: 1.8 m.

Barcode centerline length: 1.25 cm from bottom of slot to reading window center. Supported barcode formats: UPC-A, UPC-E, EAN-8, EAN-13, Code 39, Telepen, Interleaved 2 of 5, Industrial 2 of 5, Code 128, MSI/Plessey, Codabar.

SafeCom Casi-Rusco Reader

Dimensions: 6.4 x 10.6 x 2.2 cm. Color is black. Cable length: 1.8 m. When a proximity card is presented to the reader, the red light flashes green.

SafeCom EM Reader

Dimensions: 5.5 x 9.0 x 2.0 cm. Color is black. Cable length: 2.0 m. Supports the following card technologies: EM41xx, UNIQUE, TITAN, Hitag 1/2/S and Paxton. The card reader can signal status through lights and beeps when used with SafeCom Go:

Status	Lights	Beeps
Nobody is logged in	Solid red	Off
Card is presented	Flashing green	One
User is logged in	Solid green	Off

SafeCom HID Prox Reader

Dimensions: 5.5 x 9.0 x 2.0 cm. Color is black. Cable length: 2.0 m. The reader is available in a 35 bit (most common) and a 37 bit version. The card reader can signal status through lights and beeps when used with SafeCom Go:

Status	Lights	Beeps
Nobody is logged in	Solid red	Off
Card is presented	Flashing green	One
User is logged in	Solid green	Off

SafeCom iCLASS Reader

Dimensions: 5.5 x 9.0 x 2.0 cm. Color is black. Cable length: 2.0 m. The card reader can signal status through lights and beeps when used with SafeCom Go:

Status	Lights	Beeps
Nobody is logged in	Solid red	Off
Card is presented	Flashing green	One
User is logged in	Solid green	Off

SafeCom Indala Reader

Dimensions: 6.4 x 10.6 x 2.2 cm. Color is black. Cable length: 1.8 m. The card reader is available in a 26 bit version (most common) and a 29 bit version. When a proximity card is presented to the reader, the red light flashes green.

SafeCom Keypad

The SafeCom Keypad USB (p/n 699010) can be used with SafeCom Go HP on the HP Color LaserJet 3000, 3800 and 4700. The SafeCom Keypad is powered from the printer's USB port. Dimension: 10.7 x 15.8 x 3.8 cm. Color is black. Cable length: 1.5 m.

The SafeCom Keypad Serial (p/n 974010) can be used with SafeCom Go HP on the HP LaserJet 4250, 4350, 4650 and 5550. The SafeCom Keypad is powered from the supplied switch mode power supply (Input: 230V~, 50Hz/145mA, Output: 12V, 1.3A). Dimension: 10.7 x 15.8 x 3.8 cm. Color is black. Cable length: 1.5 m.

SafeCom Legic Reader

Dimensions: 5.5 x 9.0 x 2.0 cm. Color is black. Cable length: 2.0 m. The card reader can signal status through lights and beeps when used with SafeCom Go:

Status	Lights	Beeps
Nobody is logged in	Solid red	Off
Card is presented	Flashing green	One
User is logged in	Solid green	Off

SafeCom Magnetic Card Reader

Dimensions: 3.0 x 9.0 x 2.8 cm. Color is black. Cable length: 2.0 m. The card reader should be mounted on a plain clean surface. The card reader can signal status through its two lights and beeper when used with SafeCom Controller:

Status	Lights	Beeps
Standby	Off	Off
Card is read	Green is on	One
Documents	Green and red are flashing once	One
No documents	Green and red are flashing twice	Two
Prevent login	Off	Off
Card read failed	Green and red are flashing six times	Six
Unknown card	Green and red are flashing six times	Six
Other errors	Green and red are flashing six times	Six

SafeCom Magnetic Card Reader DD

Dimensions: 3.13 x 10.0 x 3.25 cm. Color is black. Cable length: 1.8 m. Connector USB Type A plug. The card reader should be mounted on a plain clean surface.

SafeCom Mifare Reader

Dimensions: 5.5 x 9.0 x 2.0 cm. Color is black. Cable length: 2.0 m. The card reader can signal status through lights and beeps when used with SafeCom Go:

Status	Lights	Beeps
Nobody is logged in	Solid red	Off
Card is presented	Flashing green	One
User is logged in	Solid green	Off

Chapter 15

SQL Always On

Always On is a high availability (HA) and disaster recovery technology of the SQL server. SafeCom support of the Always On technology requires additional configuration in both single application server and multiserver solutions. For a general overview of Always On availability groups (AGs), refer to the relevant Microsoft documentation²⁵.

SafeCom had its own failover mechanism in previous releases. This failover feature took over the role of a secondary SafeCom server in a multiserver solution. The SafeCom failover feature is included in the SafeCom G4 Server 10.6 release, and the Always On support makes this feature even more robust. This section describes high availability for the primary SafeCom databases. In this section, "failover" refers to Windows Server Failover Clustering.

This section introduces AG support for SafeCom single-server and multiserver deployments. It describes supported use-cases, prerequisites, limitations, and other changes compared to earlier SafeCom releases.

SQL Always On deployments

SafeCom databases in a single-server solution or primary databases in a multiserver solution can be subject to HA considerations.

Single-server SafeCom solution with AG

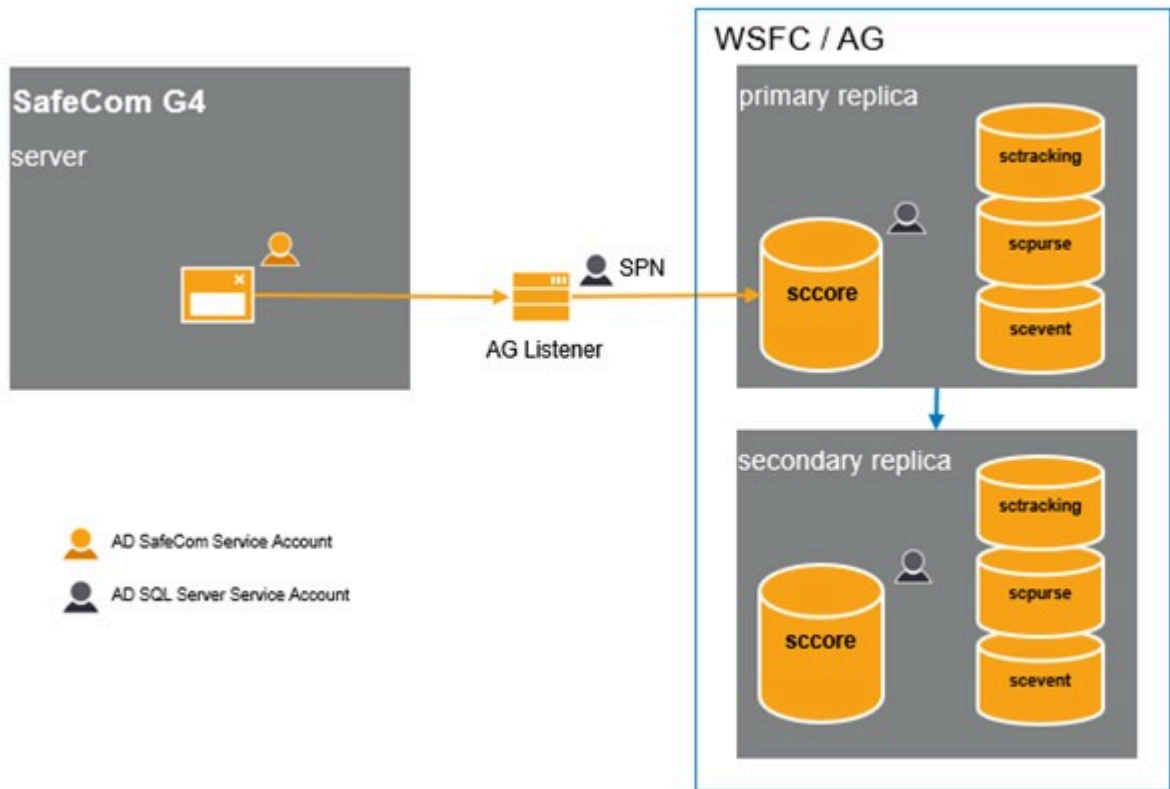
The SafeCom G4 Server advanced installer can configure SafeCom to use an external SQL Server in a single server setup. In this case, the standalone SQL server can be part of an AG. When AGs are configured, all four SafeCom databases (*sccore*, *scevent*, *scpurse*, *sctracking*) must be part of the same AG.

The AG must be created and configured on the four existing SafeCom databases by IT.

The authentication mode between SafeCom and SQL servers must be Windows Authentication, if an AG is involved.

To achieve HA, the SafeCom G4 Server must connect to the external SQL server cluster through AG Listener. When failover occurs between database servers, the database transaction in progress fails and all SafeCom components have to reconnect to their databases. AG Listener redirects the connection to the newly assigned primary replica.

²⁵ <https://docs.microsoft.com/en-us/sql/database-engine/availability-groups/windows/overview-of-always-on-availability-groups-sql-server?view=sql-server-ver15>



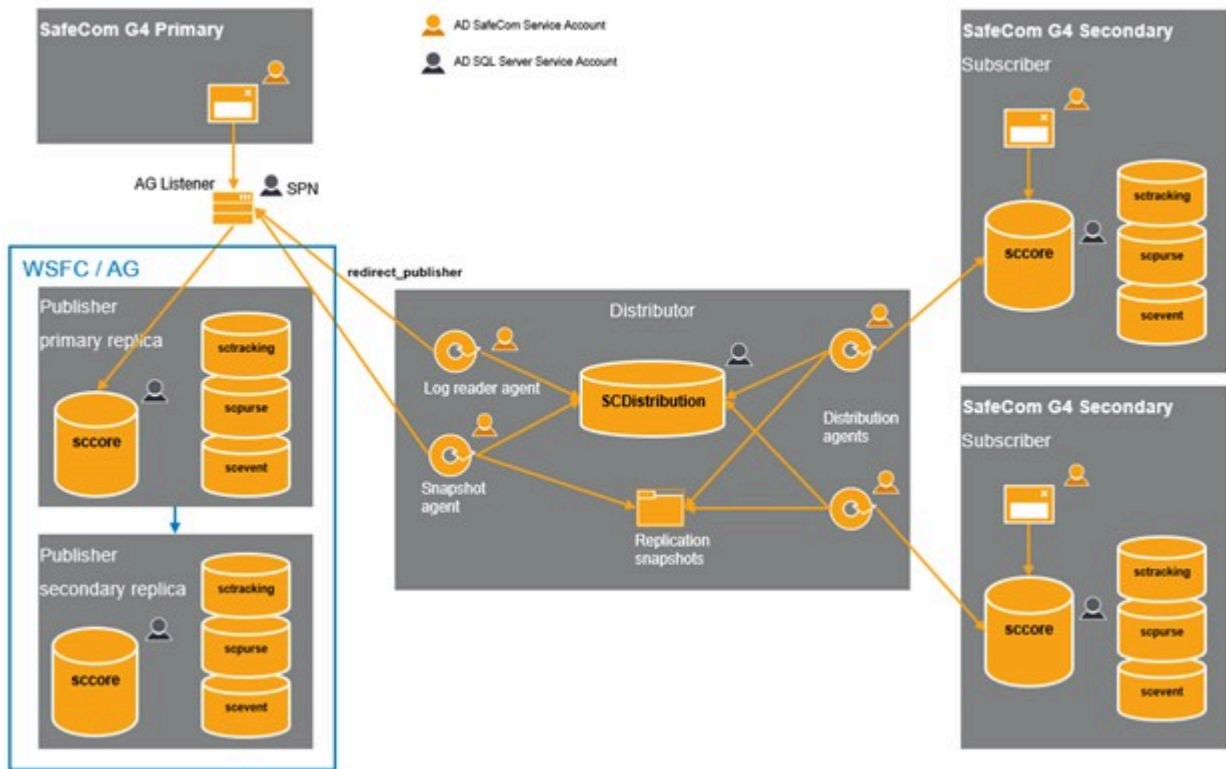
Grey boxes indicate server computers and SQL server instances.

For a SafeCom single-server solution, AG is supported for a new installation or a previous deployment that is already upgraded to the latest version.

Multiserver SafeCom solution with AG

In a multiserver solution, the primary SafeCom G4 Server is connected to the primary SQL server cluster. Secondary SafeCom G4 Servers are connected to their local SQL Express servers and can be connected to external SQL servers.

The configuration tables in the `score` database are transported from the primary SQL server to secondary SafeCom databases by transactional replication. Replication agents in previous SafeCom releases run on the primary SQL Server. When the primary SafeCom database is part of an AG, the replication publisher and distributor must be separated at the SQL Server Instance level. All replication agents (snapshot, log reader, distributor) run on the remote distributor.



To achieve a multiserver SafeCom solution with the primary databases in AG, start from a single-server HA solution, then convert it to multiserver.

The currently supported way of configuring SafeCom to HA databases goes through the HA first approach. A single-server SafeCom solution must be configured for HA. Replication to secondary SafeCom servers can be added to primary databases that are already in HA. SafeCom G4 Server implements automated configuration steps to support this scenario.

Limitations

Upgrading SafeCom multiserver deployments from 530.00 or 520.12 to 10.6 requires updating the distributor from the publisher to a remote distributor. The remote distributor supports the primary databases in AG. Although it can be configured manually, it is not supported.

In SafeCom 10.6, only the primary SQL databases can be involved in AG; the remote distributor and secondary SafeCom databases cannot.

SafeCom server	Primary		Secondary
Replication	Publisher	Distributor	Subscriber
AG	Yes	No	No

Prerequisites for SafeCom in Availability Group

Authentication

The SafeCom G4 Server installer prompts for the authentication method to access SQL servers. The installer provides the following options:

SafeCom authentication

The SafeCom service runs under the Local System account, and SQL authentication is used to access the SQL server.

Windows authentication

The SafeCom service is set up to a selected service account which is also used to access the databases.

For a SafeCom G4 Server connecting to an AG, the authentication method must be Windows authentication. SafeCom authentication is not supported²⁶. In a multiserver SafeCom solution where the primary server is configured to Windows authentication, all secondary servers must be configured to Windows authentication as well.

SafeCom solution \ Authentication	SafeCom	Windows
Single-server	Yes	Yes
Single-server with databases in AG	No	Yes
Multiserver	Yes	Yes
Multiserver with databases in AG	No	Yes

To extend existing deployments to AG, you must reconfigure SafeCom to use Windows authentication.

SafeCom service account

When Windows authentication is configured, the account type for SafeCom G4 Server Service Account must be the Domain Account or group Managed Service Account.

SafeCom solution / SafeCom service account type	Local	Virtual	sMSA	Domain Account	gMSA
Single-server	No	No	Yes	Yes	Yes
Multiserver	No	No	No	Yes	Yes

²⁶ <https://docs.microsoft.com/en-us/archive/blogs/sqlserverfaq/orphaned-users-with-database-mirroring-and-log-shipping>

Standalone Managed Service Account is not sufficient because the replication agent jobs run at a different server in multiserver solutions. Local and Virtual accounts are not supported either, because local accounts and network resource access must be configured manually at each server.

Databases

SafeCom has four databases to be involved in AG: `score`, `scpulse`, `scevent`, and `stracking`.

All SafeCom databases must have a full backup and a transaction log backup, and they must be configured to full recovery model before adding them to AG.²⁷

SQL server editions and versions

The external SQL servers of the primary SafeCom application server must be Enterprise edition because Basic AGs of the Standard edition support only a single user database.²⁸

The same version of SQL server and the same SQL server collation must be used for AG replica nodes.²⁹

The following SQL server versions are supported in SafeCom 10.6:

- SQL Server 2016 SP2
- SQL Server 2017
- SQL Server 2019

Multiserver SafeCom solution in AG

In a multiserver solution, log reader and snapshot agents connect to the primary SafeCom database or database cluster, Distribution database and snapshot folder. Distributor agents connect to secondary SafeCom databases, the Distribution database and the snapshot folder.

SafeCom Service account in multiserver solution:

- When Windows authentication is used, the SafeCom Administrator requests only a single SafeCom service account in its Add server and Repair replication dialogs. Therefore, the primary and secondary SQL servers must use the same SafeCom service account for Windows authentication.

Publisher and distributor SQL Server instances:

- The same version of SQL Server must be used for publisher AG replica nodes. The distributor SQL server version must be the same as, or later than the publisher version.³⁰
- The replication feature must be installed on all SQL server instances.

²⁷ <https://docs.microsoft.com/en-us/sql/database-engine/availability-groups/windows/prereqs-restrictions-recommendations-always-on-availability?view=sql-server-ver15>

²⁸ <https://docs.microsoft.com/en-us/sql/sql-server/editions-and-components-of-sql-server-version-15?view=sql-server-ver15#RDBMSHA>

²⁹ <https://docs.microsoft.com/en-us/sql/database-engine/availability-groups/windows/prereqs-restrictions-recommendations-always-on-availability?view=sql-server-ver15>

³⁰ <https://docs.microsoft.com/en-us/sql/database-engine/install-windows/upgrade-replicated-databases?redirectedfrom=MSDN&view=sql-server-ver15>

Publisher availability replica nodes:

- The publisher in an AG cannot be part of a Distributed AG.³¹

Remote distributor:

- If the primary SafeCom databases are included in an AG, then the transactional replication distributor must be a standalone SQL server instance.
- The remote distributor SQL server must be Standard edition or Enterprise edition to be able to run SQL Agent jobs for transactional replication.
- If the SafeCom Service account is a group Managed Service Account (gMSA), the SQL Server Agent service at the distributor must be configured to be run by this service account.

Secondary SafeCom servers:

- Transactional replication between the primary and secondary SQL servers must not be more than two versions apart, so older SQL servers at SafeCom secondary servers may need to be upgraded.³²

Checklist for HA

Make sure the following points are met to set up a HA environment.

Windows service user account for SafeCom:

- The service account is Domain Service Account or gMSA.
- The same service account is configured at Primary and Secondary SafeCom G4 Servers.

SQL Server availability replica nodes:

- The failover cluster feature is installed in the server OS.
- HADR is enabled on SQL server instances.³³

WSFC cluster and AG configuration:

- WSFC cluster is created.
 - The cluster has a virtual network name.
 - Quorum is configured.
- Mirroring endpoints on all replica nodes:
 - The SQL Server service account has connect permission granted to the mirroring endpoint.^{34 35}
 - `SSMS: Security/Logins/SQL Server service account properties/Securables/MirroringEndpoint connect permission is granted.`

³¹ <https://docs.microsoft.com/en-us/sql/database-engine/availability-groups/windows/replicate-track-change-data-capture-always-on-availability?view=sql-server-ver15>

³² <https://docs.microsoft.com/en-us/sql/database-engine/install-windows/upgrade-replicated-databases?redirectedfrom=MSDN&view=sql-server-ver15>

³³ <https://docs.microsoft.com/en-us/sql/database-engine/availability-groups/windows/enable-and-disable-always-on-availability-groups-sql-server?view=sql-server-ver15>

³⁴ <https://docs.microsoft.com/en-us/sql/database-engine/database-mirroring/set-up-login-accounts-database-mirroring-always-on-availability?view=sql-server-ver15>

³⁵ <https://docs.microsoft.com/en-us/sql/database-engine/database-mirroring/troubleshoot-database-mirroring-configuration-sql-server?view=sql-server-ver15>

- Firewall allows inbound connections to the mirroring endpoint.
- At least one full backup and a transaction log backup exist for all SafeCom databases.
 - The databases are configured to full recovery model.
- UNC network share is configured if full database and log backup for initial data synchronization is used.³⁶
 - The SQL server service account has full control ACL and share permissions.
- AG^{37 38}:
 - The AG has "create any database" permission if auto seeding is used.³⁹
 - Databases are in synchronized state.
 - AG state is healthy.
- AG Listener:
 - DNS Host Name is configured for the AG Listener⁴⁰.
- The SafeCom service account is in the sysadmin server role on all availability replica nodes.

SafeCom G4 Servers:

- The SafeCom service account has "Log on as a service" right.
- The SafeCom service account is a member of the local Administrators group.
- The SafeCom is redirected to the AG Listener in the registry.

 This setting requires the SafeCom service restart to take effect

Building single-server SafeCom solution with databases in AG

AG can be built on existing user databases. For a clean installation, SafeCom is installed first, then databases are copied to secondary AG replicas based on how the initial data synchronization is configured.

It is also possible to install SafeCom to existing databases, but that requires creating databases manually before installing SafeCom.

³⁶ <https://docs.microsoft.com/en-us/sql/database-engine/availability-groups/windows/select-initial-data-synchronization-page-always-on-availability-group-wizards?view=sql-server-ver15>:

³⁷ <https://docs.microsoft.com/en-us/sql/database-engine/availability-groups/windows/prereqs-restrictions-recommendations-always-on-availability?view=sql-server-ver15>

³⁸ <https://docs.microsoft.com/en-us/sql/database-engine/availability-groups/windows/troubleshoot-always-on-availability-groups-configuration-sql-server?view=sql-server-ver15>

³⁹ <https://docs.microsoft.com/en-us/sql/database-engine/availability-groups/windows/automatic-seeding-secondary-replicas?view=sql-server-ver15>

⁴⁰ <https://docs.microsoft.com/en-us/sql/database-engine/availability-groups/windows/create-or-configure-an-availability-group-listener-sql-server?view=sql-server-ver15>

Prepare SQL Server instances

1. Open firewall ports.
 - a. Create inbound rules for the SQL Server and SQL Server Browser when necessary.
 - b. Create an inbound rule for the database mirroring endpoint.
2. Configure the SafeCom service account as an SQL Server login.
 - a. Add the SafeCom service account to all SQL Server instances that are planned to host an availability replica.
 - b. Add the SafeCom service account to the sysadmin server role.

Install SafeCom to an external SQL Server

1. Prepare the SafeCom G4 Server installation.

Make sure the following conditions are met:

 - The SafeCom service account has "Log on as a service" rights.
 - The account is a member of the Local Administrators group.
2. Install the SafeCom G4 Server.
 - a. Select the SQL Server instances that are planned to serve as the primary replica.
 - b. Configure Windows authentication and the SafeCom service account during the installation.
3. Open a firewall for the SafeCom G4 Server.

The `Open_firewall_safecom.cmd` script contains the ports necessary for SafeCom features.

Create and configure AG

1. Install the FailoverCluster Windows feature on SQL server nodes of the AG.
2. Install the FailoverCluster.
 - a. Install the WSFC cluster and specify the cluster nodes.
 - b. Configure cluster quorum.
3. Initialize HADR on the SQL Servers hosting availability replicas.
 - a. Enable the AGs feature on the SQL Server instances.
 - b. Create an SQL login for the SQL Server service account.
 - c. Create a Mirroring Endpoint and grant "connect" permission for the SQL Server service account.
4. Create the AG.
 - a. Create a full backup and a transaction log backup of SafeCom databases.
 - b. Configure the full recovery model.
 - c. Create the availability replicas.
 - d. Create the Availability Group.

- e. Join the availability replicas to the AG.⁴¹
- f. Define the primary replica to the with the having SafeCom databases.
- g. Grant "create any database" permission to the AG if automatic seeding is used.⁴²

Create AG Listener

Create the AG Listener at the Primary replica by specifying its name, port, and optionally its IP address.⁴³

Redirect SafeCom Application Server to AG Listener

Redirect SafeCom Service to AG Listener.

If primary SafeCom databases are involved in AG, SafeCom G4 Server can connect to the primary database cluster through AG Listener. The name of the AG Listener must be specified for each database connection. The port must be added when a different port than default is used.⁴⁴

HKLM\SOFTWARE\SafeCom\SafeComG4\Database

- DBServerNameCore="<AG Listener>, <port>"
- DBServerNameEvent="<AG Listener>, <port>"
- DBServerNameTracking="<AG Listener>, <port>"
- DBServerNamePurse="<AG Listener>, <port>"

The SafeCom G4 Server must be restarted for these changes to take effect.

i You can connect SafeCom G4 Server directly to the primary replica at the cost of losing the benefits of the AG Listener and HA.⁴⁵

Building multi-server SafeCom solution with primary databases in AG

A multiserver SafeCom solution can be built from a single-server SafeCom solution that is already configured for HA. This section describes the steps starting from an already operational single-server HA solution, discussed in [Building single-server SafeCom solution with databases in AG](#).

⁴¹ <https://docs.microsoft.com/en-us/sql/database-engine/availability-groups/windows/join-a-secondary-replica-to-an-availability-group-sql-server?view=sql-server-ver15>

⁴² <https://docs.microsoft.com/en-us/sql/database-engine/availability-groups/windows/automatically-initialize-always-on-availability-group?view=sql-server-ver15>

⁴³ <https://docs.microsoft.com/en-us/sql/database-engine/availability-groups/windows/create-or-configure-an-availability-group-listener-sql-server?view=sql-server-ver15>

⁴⁴ <https://docs.microsoft.com/en-us/sql/database-engine/availability-groups/windows/listeners-client-connectivity-application-failover?view=sql-server-ver15>

⁴⁵ <https://docs.microsoft.com/en-us/sql/database-engine/availability-groups/windows/listeners-client-connectivity-application-failover?view=sql-server-ver15#BypassAGI>

Set up remote distributor SQL Server instance

1. Set up a distributor SQL Server instance.
Start the SQL Server Agent service.
2. Open firewall ports.
Create inbound rules for the SQL Server and SQL Server Browser when necessary.
3. Configure the SafeCom service account as SQL Server login.
Add the SafeCom service account as a member of sysadmin server role.
4. Configure the SQL Server Agent service.
 - a. If the SafeCom service account is a gMSA, configure the SQL Server Agent service to be run by this service account.
 - b. The SafeCom service account must have "Log on as a service" rights.

Set up replication snapshot share

Create and configure network share.

- a. Create UNC network share for replication snapshots.⁴⁶
- b. The SafeCom service account that runs the replication snapshot and distribution agent jobs must have full control ACL and share permissions.

SafeCom Primary Application Server

1. Configure the SafeCom G4 Server for remote distributor.
 - a. Set the following registry values at the primary SafeCom G4 Server:
HKLM\SOFTWARE\SafeCom\SafeComG4\Database
 - The distributor SQL server instance name:
DBDistServerName = <SQL server>\<instance>
If the port needs to be specified: <SQL server>\<instance>,<port>
 - The network share for replication snapshots:
DBReplicationSnapshotShare = <UNC network share>
2. Restart the SafeCom Administrator.
Although SafeCom G4 Server reads the remote distributor and snapshot share parameters from the registry on demand, SafeCom Administrator must be restarted for these changes to take effect.

Install secondary SafeCom servers

1. Prepare the SafeCom G4 Server installation.
Make sure the following conditions are met:
 - The same SafeCom service account was used to install the primary SafeCom G4 Server.

⁴⁶ <https://docs.microsoft.com/en-us/sql/relational-databases/replication/security/secure-the-snapshot-folder?view=sql-server-ver15>

- The SafeCom service account has "Log on as a service" rights.
 - The account is a member of the Local Administrators group.
2. Install SafeCom G4 Server.
 - a. Use SQL Server Express or an external SQL server instance.
It serves as the replication subscriber.
 - b. Configure Windows authentication and SafeCom service account during the installation.

i If you choose the built-in SQL Server Express 2019 (SAFECOMEXPRESS) instance, the installer gives sysadmin server role to:

- The SafeCom service account
- The account running the installer

3. Open a firewall for SafeCom G4 Server.

`Open_firewall_safecom.cmd` script contains the ports necessary for SafeCom features.

i Review the script and make sure that the appropriate port is opened considering the actual configuration of SQL Server Express.

Add Secondary SafeCom servers to a multiserver solution

Add a secondary SafeCom server in SafeCom Administrator

SafeCom Administrator verifies if the primary database is involved in an AG, and if a remote distributor is required based on the information received from the primary SafeCom G4 Server. The Add Server wizard workflow changes accordingly.

1. Enter the SafeCom service account and password when prompted.
For gMSA account, the name ends with \$. In this case, leave the password blank.
2. Enter the distributor_admin password when prompted.

The SafeCom G4 Server performs automated configuration for replication in AG.

The following steps are performed automatically when the first secondary SafeCom server is added to the multiserver solution.

1. Set up publication and articles.
2. Create distribution database.
3. Create and configure replication agent jobs.
4. Configure the secondary SafeCom database as replication subscriber.⁴⁷
5. Configure all availability replicas for replication.
 - Even if SafeCom is not connecting through AG Listener.

⁴⁷ <https://docs.microsoft.com/en-us/sql/database-engine/availability-groups/windows/replication-subscribers-and-always-on-availability-groups-sql-server?view=sql-server-ver15>

- If any secondary replica configuration fails, the process continues.
6. Redirect replication agents, Log reader, and Snapshot agents to use the first available AG Listener associated with the publisher.

While adding a secondary server to the multiserver solution or repairing replication in the SafeCom Administrator, the SafeCom Administrator checks if any part of the replication topology is missing, and tries to resolve the missing configurations.⁴⁸

Moving multi-server SafeCom solution into AG

A multi-server SafeCom solution can be configured for HA.

If the SafeCom multi-server solution was upgraded from an earlier version of SafeCom, the transactional replication distributor is the same server as the publisher. Local distributor may be used by SafeCom 10.7 if multi-server was created before introducing AG to the primary SQL server.

This section covers how to move from a local distributor to a remote distributor and how to configure AG in an existing SafeCom multi-server solution.

Set up remote distributor SQL Server instance

1. Set up a distributor SQL Server instance.
Start the SQL Server Agent service.
2. Open firewall ports.
Create inbound rules for the SQL Server and SQL Server Browser when necessary.
3. Configure the SafeCom service account as SQL Server login.
Add the SafeCom service account as a member of sysadmin server role.
4. Configure the SQL Server Agent service.
 - a. If the SafeCom service account is a gMSA, configure the SQL Server Agent service to be run by this service account.
 - b. The SafeCom service account must have "Log on as a service" rights.

Set up replication snapshot share

Create and configure network share.

- a. Create UNC network share for replication snapshots.⁴⁹
- b. The SafeCom service account that runs the replication snapshot and distribution agent jobs must have full control ACL and share permissions.

⁴⁸ <https://docs.microsoft.com/en-us/sql/database-engine/availability-groups/windows/always-on-availability-groups-interopability-sql-server?view=sql-server-ver15>

⁴⁹ <https://docs.microsoft.com/en-us/sql/relational-databases/replication/security/secure-the-snapshot-folder?view=sql-server-ver15>

Drop local distributor

1. Stop SafeCom service on the primary SafeCom application server.
2. Drop local distributor and SCDistribution database.
 - a. Connect to the local distributor, which is the SQL server of the primary SafeCom.
 - b. In SSMS right click on Replication and start "Disable Publishing and Distribution Wizard".
 - c. Choose "Yes, disable publishing on this server".
3. Start SafeCom service on the primary application server.

Create and configure AG

1. Install the FailoverCluster Windows feature on SQL server nodes of the AG.
2. Install the FailoverCluster.
 - a. Install the WSFC cluster and specify the cluster nodes.
 - b. Configure cluster quorum.
3. Initialize HADR on the SQL Servers hosting availability replicas.
 - a. Enable the AGs feature on the SQL Server instances.
 - b. Create an SQL login for the SQL Server service account.
 - c. Create a Mirroring Endpoint and grant "connect" permission for the SQL Server service account.
4. Create the AG.
 - a. Create a full backup and a transaction log backup of SafeCom databases.
 - b. Configure the full recovery model.
 - c. Create the availability replicas.
 - d. Create the Availability Group.
 - e. Join the availability replicas to the AG.⁵⁰
 - f. Define the primary replica to the with the having SafeCom databases.
 - g. Grant "create any database" permission to the AG if automatic seeding is used.⁵¹

Create AG Listener

Create the AG Listener at the Primary replica by specifying its name, port, and optionally its IP address.⁵²

⁵⁰ <https://docs.microsoft.com/en-us/sql/database-engine/availability-groups/windows/join-a-secondary-replica-to-an-availability-group-sql-server?view=sql-server-ver15>

⁵¹ <https://docs.microsoft.com/en-us/sql/database-engine/availability-groups/windows/automatically-initialize-always-on-availability-group?view=sql-server-ver15>

⁵² <https://docs.microsoft.com/en-us/sql/database-engine/availability-groups/windows/create-or-configure-an-availability-group-listener-sql-server?view=sql-server-ver15>

Redirect SafeCom Application Server to AG Listener


Redirect SafeCom Service to AG Listener.

If primary SafeCom databases are involved in AG, SafeCom G4 Server can connect to the primary database cluster through AG Listener. The name of the AG Listener must be specified for each database connection. The port must be added when a different port than default is used.⁵³

HKLM\SOFTWARE\SafeCom\SafeComG4\Database

- DBServerNameCore="<AG Listener>, <port>"
- DBServerNameEvent="<AG Listener>, <port>"
- DBServerNameTracking="<AG Listener>, <port>"
- DBServerNamePurse="<AG Listener>, <port>"

The SafeCom G4 Server must be restarted for these changes to take effect.

 You can connect SafeCom G4 Server directly to the primary replica at the cost of losing the benefits of the AG Listener and HA.⁵⁴

Configure SafeCom Primary Application Server

1. Configure SafeCom G4 Server for remote distributor.

Set the following registry values at the primary SafeCom G4 Server:

HKLM\SOFTWARE\SafeCom\SafeComG4\Database

- The distributor SQL server instance name:
DBDistServerName = <SQL server>\<instance>
 If the port needs to be specified: <SQL server>\<instance>,<port>
- The network share for replication snapshots:
DBReplicationSnapshotShare = <UNC network share>

2. Restart the SafeCom Administrator.

Although SafeCom G4 Server server reads the remote distributor and snapshot share parameters from the registry on demand, SafeCom Administrator must be restarted for these changes to take effect.

Repair replication for secondary SafeCom servers

Repair replication for secondary SafeCom servers in SafeCom Administrator.

If the primary database is involved in AG, remote distributor is required.

- a. Add server wizard in SafeCom Administrator prompts for SafeCom service account.
- b. For gMSA account, leave the password blank.

⁵³ <https://docs.microsoft.com/en-us/sql/database-engine/availability-groups/windows/listeners-client-connectivity-application-failover?view=sql-server-ver15>

⁵⁴ <https://docs.microsoft.com/en-us/sql/database-engine/availability-groups/windows/listeners-client-connectivity-application-failover?view=sql-server-ver15#BypassAGI>

- c. Add server wizard also prompts for the **distributor_admin** password.

SafeCom G4 Server performs automated configuration for replication in AG.

Repair replication performs the following steps:

1. Create distribution database and register distribution publishers.
2. Set up publication and articles.
3. Create and configure replication agent jobs.
4. Configure the secondary SafeCom database as replication subscriber.
5. Configure all availability replicas for replication.
This happens even if SafeCom is not connected through AG listener.
If any of the secondary replicas fail to configure, repair replication continues with the next replica.
6. Redirect replication agents, Log reader and Snapshot agents to use the first available AG Listener associated with the publisher.

Repairing replication in SafeCom Administrator checks if any part of the replication topology is missing, and tries to resolve the missing configuration.

Troubleshoot multiserver HA

Replication is not working

All AG replicas must cache (harden) transaction log records for the replication log reader to proceed. If a failed replica cannot be repaired, it must be removed from the AG.⁵⁵

Verify availability replica nodes of the publisher

Check the following points:

- Linked servers exist for:
 - Repl_distributor
 - All subscribers (Secondary SafeCom SQL servers)
- Check that local publication by the name "scoreTrans" is configured.
- Check if the remote distributor is registered at all publisher nodes:
 - EXEC sp_helpdistributor
- Check if the score database is enabled for transactional replication:
 - EXEC sp_helpreplicationdboption

⁵⁵ <https://docs.microsoft.com/en-us/sql/database-engine/availability-groups/windows/replicate-track-change-data-capture-always-on-availability?view=sql-server-ver15>

- Get the name of the original publisher⁵⁶
 - `SELECT PUBLISHINGSERVERNAME()`

Verify distributor SQL Server instance

Check the following points:

- The server is marked as a Distributor:
 - Check table `sys.servers` for `srvname=repl_distributor, dist=1`
- SCDistribution database exists:
 - `SSMS:Databases/System Databases/SCDistribution`
- Distributor_admin SQL account:
 - `distributor_admin` SQL login exists and has `sysadmin` server role.
- Linked servers exist for:
 - `Repl_distributor`
 - All publisher server instances (availability replica nodes)
 - All subscribers (Secondary SafeCom SQL servers)
- SQL Server Agent jobs exist for transactional replication:
 - Replication Log reader, snapshot and distribution agents are run by the SafeCom service account.
 - Verify agent history.
- All remote publishers use the distribution database:
 - `EXEC sp_helpdistpublisher`
 - Verify name, `distribution_db` and `working_directory`.
- The distributor is redirected to the AG Listener:
 - Get the name of the original publisher at one of the publishers.
 - ```
USE SCDistribution
EXEC sys.sp_get_redirected_publisher @original_publisher='<original publisher>',
@publisher_db='sccore'
```
- Validate that all availability replica hosts are configured as publishers:<sup>57</sup>
  - `sp_validate_replica_hosts_as_publishers`

---

<sup>56</sup> <https://docs.microsoft.com/en-us/sql/database-engine/availability-groups/windows/maintaining-an-always-on-publication-database-sql-server?view=sql-server-ver15>

<sup>57</sup> <https://docs.microsoft.com/en-us/sql/relational-databases/system-stored-procedures/sp-validate-replica-hosts-as-publishers-transact-sql?view=sql-server-ver15>

## Chapter 16

# Troubleshooting

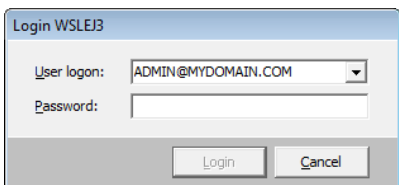
## SafeCom Help Desk Assistant

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

## SafeCom Administrator: Login failed

When you try to log in to a group with SafeCom Administrator, it reports "Login failed". Check your user logon, password, and that you have [administrator rights](#). Remember that if you belong to a domain (see [Identification](#)), you must specify the domain followed by a backslash (\) in front of the user logon. For example: <MYDOMAIN>\ADMIN.


Alternatively, you can specify user logon followed by @ and the domain. For example: ADMIN@<MYDOMAIN>.



## SafeCom Administrator: Unable to locate all SafeCom servers

The SafeCom Administrator uses broadcasts to locate the SafeCom servers. If your network is a VLAN (Virtual Local Area Network), then it may prevent the SafeCom Administrator from locating SafeCom servers.

Enter the SafeCom servers' IP addresses manually, directly in the list of individual **Broadcast addresses** on the **Network** tab in the **Options** dialog (see [Network](#)).

If the server group appears with a question mark , it is either because the SafeCom server is not running or because it is not referring to the IP addresses of the SafeCom server.

1. Start SafeCom Administrator (see [Log in to SafeCom Administrator](#)) and right-click the group in the **Server groups** pane and click **Server group properties** (see [License](#)).
2. In **IP address of entry point**, enter the IP address of the SafeCom server. Click **OK**.
3. Log in to the group and open the **Server properties** dialog (see [Server](#)). In **IP address**, enter the IP address of the SafeCom server, then click **OK**.

The IP address of the SafeCom server can be obtained by logging into the SafeCom server, starting a **Command Prompt**, and typing `ipconfig -all`.

## SafeCom Administrator: Unable to locate all SafeCom devices

A device only appears in the SafeCom Administrator after it was added through the SafeCom Administrator or after a user with [technician or administrator rights](#) has logged in.

If you are attempting to [broadcast for SafeCom Controllers](#), perform the following steps:

1. In SafeCom Administrator, go to **Actions menu** > **Options** and verify that the list of broadcast addresses on the **Network** tab is correct.
2. Contact a network administrator who has access to the DHCP server.  
The network administrator can log in to the DHCP server and see the IP address that is assigned to the device.

## SafeCom Administrator: Users are missing

Users are either not associated to a server or they belong to a different server than the one you are looking at.

Click the **Find** button and click **Retrieve all** (see [Find users](#)).

## SafeCom Administrator: Add user failed and Add alias failed

This is because either a user with the specified user logon or alias (see [Aliases](#)) exists already. Consult the SafeCom server [event log](#) to see which user is causing the conflict.

## SafeCom Administrator: License does not take effect

If nothing happens when you try to [apply a new license key code](#), close SafeCom Administrator and start it again by right-clicking **SafeCom Administrator** and selecting **Run as administrator**.

## SafeCom Administrator: Controls in dialog are not visible

The menus and controls in SafeCom Administrator adapt to reflect the SafeCom license key code and the rights with which you are logged into SafeCom Administrator. However, if a certain control in the dialog displayed by the SafeCom Administrator is not completely visible, it may be because the resolution of the screen is configured for a different value than 96 dpi. Change the resolution to 96 dpi.

## SafeCom Administrator: Device is recognized as SafeCom Controller

When adding a new device, if "SafeCom type: SafeCom Controller" is displayed on the Add Device Wizard, it may have an incorrect SNMP community name. Check that the SNMP community name on the device matches the SNMP community name you entered when adding the device to SafeCom Administrator. Also, if the SNMP community name is not public, you have to edit the `scDevMonSettings.ini` file. For more information, see [Add device](#).

## SafeCom Administrator: Device cannot be added as a Push printer

Devices that do not have "public" as their SNMP community name cannot be added to SafeCom Administrator as Push printers.

## SafeCom Administrator: Device is not responding when the community name has been changed from "public"

Ensure that you are running SafeCom Administrator as an administrator or as an equivalent role.

## User is not created at first print

First, verify that **Create users at first print** is checked (see [Users](#)). If the user is printing from a workgroup computer to a shared SafeCom Pull Printer, the user must be known on the server with the exact same logon and password as on the client. If this is not the case, the print job is stored under the server account that owns the printer, typically, the Administrator or Guest account. If the server and the client belong to the same domain, there is no problem.

## Device web interface: Displayed incorrectly or settings not saved

Your web browser must allow the use of JavaScript (Active Scripting). The steps below apply to Internet Explorer.

1. Start Internet Explorer.
2. In the **Tools** menu, click **Internet Options**.
3. Click the **Security** tab in the **Internet Options** dialog.
4. Click **Custom Level** to open the **Security Settings** dialog.
5. Scroll down to **Scripting, Active scripting** and click **Enable**. Click **OK** twice.

## At the printer: Out of order

This message is displayed when communication with the SafeCom server is lost. Check the following:

- Does the web page of the SafeCom device refer to a SafeCom server and are the IP address and group name correct?
- Is the SafeCom service running on the SafeCom server (see [Start and stop the SafeCom service](#))?
- Is the network down?
- Is a firewall blocking communication (see [Windows Firewall – Ports that must be opened](#))?
- Is the SafeCom Controller connected to the network through the MDI/MDI-X port? If the network is up and running, the port's green light should be on and its yellow light should be flashing.
- Is the printer connected to the network?

The message is cleared and the device returns to normal operation a couple of minutes after communication has been restored.

## At the printer: User unknown

The used card (or entered ID code) is unknown. The user needs a PUK code from the administrator. See [Add users manually](#) and [Customize the format of ID codes](#).

## At the printer: Login denied

- Wrong PIN code.
- The device is not registered. For SafeCom Go, refer to the *How to* chapter in the appropriate *SafeCom Go Administrator's Manual* (see [Related documentation](#)).
- Too many consecutive, failed login attempts has caused **Prevent login** to be checked on the **Identification** tab in the **User properties** dialog (see [Identification](#)).

If none of the above apply, it is possible that the Windows system on the SafeCom server does not allow any more connections. If you also get a "Connection error. Login failed" message when you try to log in to SafeCom Administrator, then you should restart the computer.

## At the printer: Restricted access

- The user is not allowed to use the device.
- A Pay user is trying to log in and **Pay** is not selected on the **License** tab in the **Device properties** dialog.

## At the printer: Error printing document

- **Pull Print** is cleared on the **License** tab in the **Device properties** dialog (see [License](#)).
- **Pull Print** is cleared on the **Settings** tab in the **Device properties** dialog (see [Settings](#)).

## At the printer: Question mark before the document name

The list of supported printer drivers does not include an entry matching the driver you used. Use the web browser to add the driver name to the list (see [Devices](#)).

## At the printer: Printer busy, retry later

The "Printer busy, retry later" message on the device's control panel indicates that SafeCom does not have exclusive access control of the device. Exclusive SafeCom access control ensures that it is only the user currently logged in can print or copy documents. If there is no apparent reason for this message, check whether SNMP is disabled on the printer and enable it.

## At the printer: Printer keeps rebooting

Please check that the printer's formatter board is properly in place.

## At the printer: Copy not allowed

Please check that **MFP** is selected in the **Device properties** dialog (see [Settings](#)).

## At the printer: Login error <number>

- Is the SafeCom service running on the SafeCom server?

- Is the SafeCom device registered at the SafeCom server?

## At the printer: Error printing: General Failure

The document you are trying to print is no longer on the SafeCom server. This may happen if you log in at two or more devices and try to print simultaneously on all of them.

## At the printer: Card reader not working

- Is the card reader powered and firmly connected?
- Is the card compatible with the reader?
- Try to move the card reader away from the printer to check if electrical interference is what prevents the reader from working.

## Document not printed

- Is the print queue paused?
- Is the printer powered on and connected?
- Is the printer online?
- Is intervention required? Check for:
  - Wrong paper size
  - Manual feed
  - Out of paper
  - Paper jam
  - Toner low

## Some documents are missing

- The user may be trying to collect documents that have not yet been transferred to the SafeCom solution. Allow sufficient time for the document to be processed and spooled. Try to log in again.
- The user may previously have attempted to print the documents on another device but did not collect all of the documents. (Perhaps because the printer required intervention or needed to warm up.) Consult SafeCom Tracking data (if available) to confirm whether this is the case.
- The **Filter document list** (see [Devices](#)) should be enabled to control that only documents generated by certain drivers are available for printing on a particular printer.
- The printer may have discarded the document due to driver compatibility problems. Try to print the same document directly to the printer to verify that this has nothing to do with SafeCom.

## Document printed incorrectly

- Is there a paper jam?
- Is the toner low?
- Does the driver support the printer? If PostScript or PCL data is sent to a printer that does not support it, the result may be garbage print. Change to a printer driver that supports the printer.

## Nothing is copied

- Is the MFP powered on and is the SafeCom MFP Cable connected?
- Is the MFP online?
- Is the MFP out of paper, low on toner, or is there a paper jam?

## Driver names are missing

During the installation of the SafeCom Front-end, you are presented with a list of driver names. The list of driver names is provided and maintained by the SafeCom server.

New driver names are automatically added to the list when a document is printed from a printer that uses the SafeCom Pull Port. If there are driver names missing from the list, it is because you have not printed a document with that driver.

## Add Printer Wizard: Specified port cannot be added

When you try to configure a Windows printer to use the SafeCom Pull Port or Push Port, you might receive the message:

"Specified port cannot be added. The request is not supported."

It is because you tried to create a shared SafeCom printer on a clustered server computer other than the two nodes.

## Local SafeCom Pull Printer is unable to print

Use the SafeCom Administrator to check if the document is on the user's job list. If this is the case, then it could be because the SafeCom Pull Port used by the local SafeCom Pull Printer cannot connect to the SafeCom server.

Open the **Configure Pull Port** dialog and enter the **Address** of the SafeCom server.




## Start and stop the SafeCom service

1. Click **Start**, type **services.msc** into the search box, and press Enter.
2. Locate the SafeCom service. Select the **Status** field, then click **Start/Stop SafeCom Service** as needed.
3. To restart, right-click the **SafeCom Service** and click **Restart**.

## How to start and stop the Print Spooler

1. Click **Start**, type **services.msc** into the search box, and press Enter.
2. Locate the **Print Spooler**. Select the **Status** field, then click **Start** or **Stop** as needed.
3. To restart, right-click the **Print Spooler** and click **Restart**.

 If other services, such as Fax, depend on the Print Spooler, these must also be stopped.

## User computer: Unable to connect to SafeCom server

Either the SafeCom server is not running or the SafeCom Pull Port cannot broadcast to the SafeCom server.

1. Open the **Configure Pull Port** dialog (see [Configure the SafeCom Pull Port](#)).
2. Test the connection to the configured SafeCom servers.

## User computer: Please contact your administrator!

If a user can not print documents through SafeCom, the **Messenger Service** dialog displays one of the following error messages:

- Unable to connect to SafeCom server (see [User computer: Unable to connect to SafeCom server](#)).
- There is not enough disk space on the SafeCom server.
- Unable to logon to the SafeCom database.
- SafeCom license violation.
- You are unknown to the SafeCom solution.

These SafeCom-generated messages appear after print notification messages are sent by the Windows print subsystem. For this reason, we recommend that you disable notification messages from the Windows print subsystem. On the Windows server, open the Printers folder. In the **File** menu, click **Server Properties** and click the **Advanced** tab. Refer to online Windows help.

## Import users: No users imported

If the **Import user** function fails or yields only incomplete results, check whether:

- The separator specified in the CSV import (see [Configuration \(CSV\)](#)) matches the actual separator used in the CSV file. Use Notepad or another editor to verify the separator in the CSV file.
- The specified field name is the correct one or if it was typed incorrectly.
- The specified import file exists, is empty, or is formatted incorrectly. Make sure to specify the name of the file to import from (with full path) as seen from the SafeCom server. The account that runs the SafeCom service (normally, the Local System account) must have read access to the file.
- The difference between the existing users and the users in the import file exceeds the percentage specified in **Max user deletion**.
- In a multiserver installation, the users have a home server assigned. Use **Find users** to see the imported users. If users are not assigned to a home server, they do not appear in the import list.

For additional troubleshooting, consult the log file produced during the attempted import (see [User import log file](#)).

## Import billing codes: No codes imported

If the **Import billing codes** function fails or yields incomplete results, check whether:

- The separator specified in the CSV import matches the actual separator used in the CSV file. Use Notepad or another editor to verify the separator in the CSV file.
- The specified field name is the correct one or if it was typed incorrectly.
- The specified import file is nonexistent, empty, or formatted incorrectly. Make sure to specify the name of the file to import from (with full path) as seen from the SafeCom server. The account that runs the SafeCom service (normally, the Local System account) must have read access to the file.
- The difference between the existing billing codes and the billing codes in the import file exceeds the percentage specified in the **Max difference [%]** field.

For additional troubleshooting, consult the log file produced during the attempted import (see [User import log file](#)).

## Multiserver installation: Replication issues

- **User is unknown when logging in on some devices:** Occurs if the replication from the primary server to the secondary servers does not work. See [Check that the replication is working](#) and verify that the replication is working. Remember to [set SQLSERVERAGENT to automatic startup](#).
- **Unknown state:** Occurs if the SQL agent does not have proper access rights to the DATA folder. Ensure that the relevant rights are set as outlined in [Multiserver installation](#).
- **Failed state:** Occurs if the user does not have the explicit **Connect SQL** rights. Check the user properties on the SQL server, and ensure that **Connect SQL** is checked under the **Logon properties > Securables > Permissions > Explicit** tab. Check if the user is listed

under **Replication Monitor > My Publishers > {server\instance} > [score]:scoreTrans > Properties > Publication Access List**. If the user is not listed, add the user.

**i** If you performed any of the above instructions, wait for a few minutes to the replication to restart. If the replication does not restart automatically, force a refresh from SafeCom Administrator.

## scPopUp: The publisher could not be verified

If you run scPopUp.exe (see [Setup SafeCom PopUp](#)) from a file share and Windows presents a security warning stating "The publisher could not be verified", perform the following steps:

1. Click **Start**, type **inetcpl.cpl** into the search box, and press Enter.  
The **Internet Properties** dialog appears.
2. Click the **Security** tab.
3. Select **Local intranet** as the **Zone**, then click **Sites**.
4. Ensure that **Include all local (intranet) sites not listed in other zones** is selected, then click **Advanced**.
5. Enter the website (`\\share`) and click **Add**, then click **Close**. Click **OK** twice.

## Smart Printer Driver: Reduced performance

If performance suffers, it might be because one or more printer drivers are leaking resources. One solution is to restart of the SafeCom XPS Print Service. Another solution is to find and use another printer driver that does not have this problem.

## Smart Printer Driver: Error codes at the device

If error codes in the 400-499 range appear on the device, it is related to the SafeCom XPS Print Service.

### Example:

- "Cannot print to printer queue "SafeCom-<DeviceID>". Printing is not supported when EMF spooling is enabled."  
This relates to the setting **Print directly to printer** under **Printer properties**.
- "Could not open printer queue " SafeCom-<DeviceID>."
- "Failed to lookup Windows Queue name for Device ID "3000". Failed to open Windows Queue "SafeCom-<DeviceID>."  
This relates to the Windows queue that does not work properly or it may not exist at all.

For details on error logs, open **Event viewer > Applications Services Logs > SafeCom > SafeCom XPS Print Service** .

## Remote SQL server cannot login

If your SafeCom primary server cannot log in to your external SQL server and you cannot detect any connection issues, the external server instance may be hidden. In such cases, check the following:

1. In **SQL Server Configuration Manager**, expand **SQL Server Network Configuration**, right-click **Protocols for <server instance>**, and select **Properties**.
2. On the **Flags** tab, select the **Hide Instance** box and ensure that it is set to **No**.

## SafeCom server can not login using the safecominstall user

If the SafeCom server cannot login with the safecominstall user to an SQL server instance named <servername>\<SQLINSTANCE>, perform the following steps:

1. Verify that the safecominstall user is created correctly (use Microsoft SQL Server Management Studio to remotely connect to the server instance). If you cannot connect, proceed with the steps below.
2. Verify that the SQL server instance is set up to run in mixed authentication mode.
3. Verify if the SQL browser service is running on the SQL server. In a multiserver environment, verify that the SQL agent is also running.
4. Use the SQL Server Configuration Manager to enable the TCP protocol for the SQL server instance.
5. Ensure that the firewall exceptions for the SQL server are set up properly or stop and disable the firewall. If using Microsoft firewall, you can use the SafeCom firewall script.
6. Ensure that the network discovery policy is enabled on both the SQL server and the SafeCom server.

If you can ping the SQL server by servername from the primary server and vice versa, then it is working properly.

7. Restart the SafeCom service on the primary server.
8. Verify that all four SafeCom databases are created.

## Spooler failure when the Print System Asynchronous Notification message is not handled by the user

In such cases, a message is displayed that notifies the user about the SafeCom PopUp not running, and provides a prompt for starting the SafeCom PopUp. If the user does not take action in 4 minutes, on some operating systems, the print spooler may stop working, requiring a restart.


## Certificate of the SafeCom G4 primary server is lost

In such cases, ensure that you perform a factory reset on the Ethernet Card Readers. After that, you can re-add the readers to your SafeCom G4 installation.

## Communication failure between SafeCom components

SafeCom G4 uses TLS 1.2 by default for encryption. If your system is not set to use TLS 1.2 or uses older versions of TLS, ensure that the following registry entries are created and set:

- [HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2]
- [HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Client]
- "DisabledByDefault"=dword:00000000
- [HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Server]
- "DisabledByDefault"=dword:00000000

 Be aware that modifying the TLS version may cause issues for any other applications you are using with an older TLS version.

## User Import from Unix that does not contain Domain Info

If you are planning to import users from Unix, but your Unix system does not have domain information, perform the following steps:

1. Under **User import configuration** > **Extra**, select the **Use extra configuration** check box.
2. Add the following lines:

```
[SPECIAL_IMPORT_SETTINGS]
ExDomainField=DoNotUse
```

## SafeCom secondary server is not reachable from the SafeCom primary server

This symptom can be confirmed by running the `netstat -an` command from the command line on an unreachable SafeCom secondary server. If the port 7700 is not in the list of open ports, but the SafeCom service is running, the following procedure can be used to recover the SafeCom secondary server:

**i** This process should only be used as a last measure. In some cases (for example, when offline tracking is enabled), this process could result in loss of data that has not been propagated to the SafeCom primary server yet.

A last emergency repair measure for this symptom is to delete all local databases on affected secondary servers, so they can be recreated by SafeCom, and valid data from the primary SQL database can be replicated. To do this, perform the following steps:

1. Stop the SafeCom service on the affected SafeCom secondary server.
2. Delete all four SafeCom databases from the SafeCom secondary server's SQL Express database instance.
3. Delete any replication subscriptions from the SafeCom secondary server's SQL Express database.
4. Restart the SafeCom secondary computer.
5. Repair replication from SafeCom Administrator on the affected SafeCom secondary server.

## Replication subscription for the old SQL primary server appears under the SafeCom secondary server's SQL Express instance

In cases when the old and the new SQL primary servers are online at the same time, replication subscriptions may appear for both servers at the SafeCom secondary server's SQL Express instance. As long as SafeCom databases on the old SQL primary server are offline, this symptom should not cause any functional problems, as no replication will take place from the old SQL primary server. To clean up this setup, follow these steps:

1. On the old SQL primary server, delete any replication publications for SafeCom.
2. On the affected SafeCom secondary servers, delete replication subscriptions pointing to the old SQL primary server.

## Services using GMSA accounts do not start automatically after reboot

Services that run under a GMSA account may not be able to start up after a computer reboot if the following registry value is not configured properly:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\<>service_name>\ServiceAccountManaged
```

If you experience startup problems after reboot for any service run by a GMSA account, confirm that this registry value is set to 01 00 00 00.

## Chapter 17

# Error codes

This chapter contains SafeCom G4 error codes and their meaning. These codes may appear as supplementary information in end-user messages as well as event logs and trace files.

## SafeCom Server error codes

The following table contains the error codes for the SafeCom G4 Server:

|    |                                                        |
|----|--------------------------------------------------------|
| -1 | [Internal] Action failed                               |
| 0  | Action completed successfully                          |
| 1  | General failure.                                       |
| 2  | General database failure.                              |
| 3  | A handle was not valid.                                |
| 4  | By default, all status fields are initialized to this  |
| 5  | A connection was lost                                  |
| 6  | Received request is known but version is not supported |
| 7  | Received request is unknown                            |
| 8  | When a session gets different versions                 |
| 9  | User cancelled a print job                             |
| 10 | Plug-in failure                                        |
| 11 | General Money Server failure                           |
| 12 | Server is busy                                         |
| 14 | Name is not valid                                      |
| 15 | Unknown user name or bad password                      |
| 16 | User did not respond to dialog                         |
| 17 | Database connection down or in error                   |
| 20 | Receive operation completed successfully               |
| 21 | Send operation completed successfully                  |
| 22 | Connection lost during transfer                        |
| 23 | Connection never opened or wrong type                  |

|    |                                                                      |
|----|----------------------------------------------------------------------|
| 24 | Connection is in error                                               |
| 25 | The cryptation method can't be used                                  |
| 26 | The cryptation couldn't be performed                                 |
| 27 | UDP receive time out                                                 |
| 28 | Connection time out                                                  |
| 31 | General replication failure                                          |
| 32 | Replication is slow or may be down                                   |
| 45 | Job is locked. Fx. because of Print Once                             |
| 46 | User is not allowed access to object                                 |
| 47 | Specified user properties are not unique                             |
| 48 | Redirection to server failed.                                        |
| 49 | [Internal] Special error code to signal redir                        |
| 50 | General access violation. Bad password etc.                          |
| 51 | Account is locked                                                    |
| 52 | Job could not be found                                               |
| 53 | User is not logged in                                                |
| 54 | Specified user could not be found                                    |
| 55 | Job marked for deletion. Will be automatically deleted when released |
| 56 | Card number does not exists                                          |
| 57 | User already exists                                                  |
| 58 | User logon already exists                                            |
| 59 | PUK code already exists                                              |
| 60 | Card number already exists                                           |
| 61 | Device is locked. Push print must wait.                              |
| 63 | Billing code ID not valid                                            |
| 64 | Distribution group already exists                                    |
| 65 | Device type is not allowed operation                                 |
| 66 | Device ID not valid                                                  |
| 67 | Device not able to control copy sessions                             |
| 69 | Device is not allowed copy                                           |
| 70 | Specified name already exists                                        |
| 71 | Specified export label already exists                                |
| 72 | Specified home server is invalid                                     |
| 73 | Specified alias already exists                                       |
| 80 | Credits too low                                                      |



|      |                                                        |
|------|--------------------------------------------------------|
| 81   | Device could not be found                              |
| 82   | Server could not be found                              |
| 83   | Server contains working objects                        |
| 84   | Primary Server cannot be deleted                       |
| 85   | Multi server not supported when running WIN auth in DB |
| 86   | Server already exists                                  |
| 90   | Domain could not be found                              |
| 91   | Domain already exists                                  |
| 92   | Domain contains working objects                        |
| 95   | User has too many cards                                |
| 101  | File not found                                         |
| 102  | Could not open file                                    |
| 103  | Could not read file                                    |
| 104  | Could not write to file                                |
| 105  | Reading file not finish                                |
| 106  | Error reading file                                     |
| 107  | No more disk space                                     |
| 108  | Invalid file handle                                    |
| 109  | File path could not be found                           |
| 110  | File already exists                                    |
| 111  | File is empty                                          |
| 112  | Error reading file                                     |
| 113  | Error reading registry                                 |
| -101 | Registry access violation                              |
| 120  | OU could not be found                                  |
| 121  | OU already exists                                      |
| 122  | Specified OU parent is invalid                         |
| 123  | OU contains other OU's                                 |
| 124  | OU contains users                                      |
| 125  | OU contains devices                                    |
| 126  | OU contains servers                                    |
| 130  | Billing code not found                                 |
| 131  | Billing code already exists                            |
| 132  | Billing is not enabled                                 |
| 140  | Group could not be found                               |

|     |                                                |
|-----|------------------------------------------------|
| 141 | Group already exists                           |
| 142 | Group print is disabled                        |
| 150 | General license error                          |
| 152 | License violation, Encryption not allowed      |
| 157 | License violation, Tracking                    |
| 158 | License violation, Pay                         |
| 159 | License violation, license is expired          |
| 160 | No license installed                           |
| 161 | License is valid                               |
| 162 | License violation, license is expired          |
| 163 | License is not valid                           |
| 165 | License could not be verified                  |
| 170 | [Internal] License library error code          |
| 171 | [Internal] License library error code          |
| 172 | [Internal] License library error code          |
| 173 | [Internal] License library error code          |
| 174 | [Internal] License library error code          |
| 175 | [Internal] License library error code          |
| 176 | [Internal] License library error code          |
| 177 | [Internal] License library error code          |
| 178 | [Internal] License library error code          |
| 179 | [Internal] License library error code          |
| 180 | [Internal] License library error code          |
| 186 | License violation, too many Devices            |
| 187 | License violation, SCClient                    |
| 188 | License violation, AdmClient                   |
| 189 | License violation, Multi Server                |
| 191 | License violation, Billing                     |
| 192 | License violation, ePay                        |
| 193 | License violation, RBP                         |
| 194 | License violation, PULL                        |
| 195 | License violation, ID device                   |
| 196 | License violation, Smart scan                  |
| 200 | Cannot connect to specified IpAddr, PortNumber |
| 201 | Invalid socket handle                          |

|     |                                                  |
|-----|--------------------------------------------------|
| 202 | Invalid memory handle                            |
| 203 | An error occurred while transmitting/receiving   |
| 204 | Data export failure                              |
| 205 | Data Field not found                             |
| 206 | Result too big                                   |
| 220 | Cannot find user account                         |
| 221 | Default error code                               |
| 222 | General database failure in the Money Server     |
| 223 | No data to export                                |
| 224 | Reservation failure                              |
| 225 | User is not pay user                             |
| 230 | Schedule not found                               |
| 240 | Charging scheme not found                        |
| 250 | RBP rule not found                               |
| 260 | BOPC could not be found                          |
| 261 | BOPC already exists                              |
| 270 | Branch could not be found                        |
| 271 | Branch already exists                            |
| 280 | Configuration could not be found                 |
| 281 | Configuration already exists                     |
| 282 | Configuration data too large                     |
| 290 | Version of database not supported                |
| 300 | Connection to secondary server is in error       |
| 301 | Login to secondary server is in error            |
| 310 | User has too many delegates                      |
| 311 | Such a delegate relation already exists          |
| 312 | DelegateID does not exist in DB                  |
| 313 | Delegate is not enabled on the primary server    |
| 314 | Delegate relation has end date/time before       |
| 320 | Device Server Group name already exists in DB    |
| 321 | Device Server Group ID does not exist in DB      |
| 323 | Trying to delete a group that is not empty in DB |
| 400 | General XpsPrint failure                         |
| 401 | Failed to create XpsPrint job                    |
| 402 | Failed to write data to XpsPrint service         |

|      |                                                      |
|------|------------------------------------------------------|
| 403  | Failed to commit XpsPrint job                        |
| 410  | HighSpeed printing must be enabled for XpsPrint jobs |
| 420  | Failed to register device with XpsPrint service      |
| 421  | Failed to unregister device with XpsPrint service    |
| 422  | No driver available to serve device                  |
| 423  | Device is not available                              |
| 9999 | [Internal] Special error code to signal restart      |

## Chapter 18

# Administrator's installation notes

This chapter contains forms that allow you to record relevant information about the SafeCom solution. The information is relevant when multiple people are involved in the solution over time in connection with, for example, maintenance and support.

## Servers

If the solution is a multiserver solution, we recommend creating an overview diagram (using Microsoft Visio or a similar tool). The diagram should visually illustrate the different servers and ports used in your solution.

This section contains several types of tables:

- SafeCom primary server
- SQL primary server
- SafeCom secondary server
- Failover servers

The rightmost column in the tables contains one or more letters. Use the letters with the legend below:

Legend:

|   |                                                                                                                                                                                                                              |
|---|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| A | If the SafeCom server is clustered, all other SafeCom components (devices, port monitors, and so on) must refer to the <b>Virtual Server</b> and not the nodes. Otherwise, failover will not function properly.              |
| B | The <b>SafeCom license key code</b> is based on the <b>Computer Name</b> (see <a href="#">Determine the computer name</a> ), unless the primary server is clustered, in which case, it is based on the <b>Cluster Name</b> . |
| C | A SafeCom multiserver solution requires the SafeCom primary server to use Microsoft SQL Server. If the SQL server resides on another server, then add the word "Remote" and fill in the SQL primary server table.            |
| D | Enter the SafeCom G4 version.<br>Example: S82 070.410*07.                                                                                                                                                                    |
| E | Enter the Windows OS information.<br>Example: Windows Server 2016.                                                                                                                                                           |
| F | Normally, a cluster has two nodes. Add more rows if required.                                                                                                                                                                |
| G | If the SQL server is clustered, the reference to the SQL server should be {NetworkName}\{instancename}. Otherwise, it should be {computername}\{instancename}.<br>The instance name is case sensitive.                       |

|   |                                                                                                |
|---|------------------------------------------------------------------------------------------------|
| H | Normal practice is to install and use Microsoft SQL Express 2019 on SafeCom secondary servers. |
|---|------------------------------------------------------------------------------------------------|

## SafeCom primary server

| SafeCom primary server |                            |          |   |
|------------------------|----------------------------|----------|---|
|                        | <b>Server address</b>      |          | A |
|                        | <b>Computer Name</b>       |          | B |
|                        | <b>SQL Server</b>          |          | C |
|                        | <b>SafeCom G4 version</b>  | S82 070. | D |
|                        | <b>Windows OS</b>          |          | E |
| Cluster information    |                            |          |   |
| Cluster Group          | <b>Server address</b>      |          | B |
|                        | <b>Cluster Name</b>        |          |   |
|                        | <b>Disk Resource (Q)</b>   |          |   |
| Virtual Server 1       | <b>Server address</b>      |          | A |
|                        | <b>Network Name</b>        |          | A |
|                        | <b>Disk Resource</b>       |          |   |
|                        | <b>Spool folder</b>        |          |   |
|                        | <b>SC print job folder</b> |          |   |
| Virtual Server 2       | <b>Server address</b>      |          | A |
|                        | <b>Network Name</b>        |          | A |
|                        | <b>Disk Resource</b>       |          |   |
|                        | <b>Spool folder</b>        |          |   |
| Node 1                 | <b>Server address</b>      |          | F |
|                        | <b>Heartbeat address</b>   |          | F |
|                        | <b>Network Name</b>        |          | F |
| Node 2                 | <b>Server address</b>      |          | F |
|                        | <b>Heartbeat address</b>   |          | F |
|                        | <b>Network Name</b>        |          | F |

## SQL primary server

| SQL primary server |                       |  |   |
|--------------------|-----------------------|--|---|
|                    | <b>Server address</b> |  |   |
|                    | <b>Port</b>           |  |   |
|                    | <b>Computer Name</b>  |  | G |

|                     |                          |  |   |
|---------------------|--------------------------|--|---|
|                     | <b>SQL</b>               |  |   |
|                     | <b>SQL instancename</b>  |  |   |
|                     | <b>Windows OS</b>        |  |   |
| Cluster information |                          |  |   |
| Cluster Group       | <b>Server address</b>    |  |   |
|                     | <b>Cluster Name</b>      |  |   |
|                     | <b>Disk Resource (Q)</b> |  |   |
| Virtual Server      | <b>Server address</b>    |  |   |
|                     | <b>Network Name</b>      |  | G |
|                     | <b>Disk Resource</b>     |  |   |
| Node 1              | <b>Server address</b>    |  | F |
|                     | <b>Heartbeat address</b> |  | F |
|                     | <b>Network Name</b>      |  | F |
| Node 2              | <b>Server address</b>    |  | F |
|                     | <b>Heartbeat address</b> |  | F |
|                     | <b>Network Name</b>      |  | F |
| Folder              | <b>SQL</b>               |  |   |

## SafeCom secondary server

|                          |                            |          |   |
|--------------------------|----------------------------|----------|---|
| SafeCom secondary server |                            |          |   |
|                          | <b>Server address</b>      |          | A |
|                          | <b>Computer Name</b>       |          | B |
|                          | <b>SQL / Express</b>       |          |   |
|                          | <b>SafeCom G4 version</b>  | S82 070. | D |
|                          | <b>Windows OS</b>          |          | E |
| Cluster information      |                            |          |   |
| Cluster Group            | <b>Server address</b>      |          |   |
|                          | <b>Cluster Name</b>        |          |   |
|                          | <b>Disk Resource (Q)</b>   |          |   |
| Virtual Server 1         | <b>Server address</b>      |          | A |
|                          | <b>Network Name</b>        |          | A |
|                          | <b>Disk Resource</b>       |          |   |
|                          | <b>Spool folder</b>        |          |   |
|                          | <b>SC print job folder</b> |          |   |
|                          | <b>SQL folder</b>          |          |   |

|                  |                          |  |   |
|------------------|--------------------------|--|---|
| Virtual Server 2 | <b>Server address</b>    |  | A |
|                  | <b>Network Name</b>      |  | A |
|                  | <b>Disk Resource</b>     |  |   |
|                  | <b>Spool folder</b>      |  |   |
| Node 1           | <b>Server address</b>    |  | F |
|                  | <b>Heartbeat address</b> |  | F |
|                  | <b>Network Name</b>      |  | F |
| Node 2           | <b>Server address</b>    |  | F |
|                  | <b>Heartbeat address</b> |  | F |
|                  | <b>Network Name</b>      |  | F |

## Failover servers

In case you intend to increase resilience by specifying [failover servers](#), you can use the table below to record the priorities.

| Failover servers |                              |
|------------------|------------------------------|
| Server address   | Prioritized failover servers |
| 1                |                              |
| 2                |                              |
| 3                |                              |
| 4                |                              |
| 5                |                              |
| 6                |                              |
| 7                |                              |
| 8                |                              |
| ...              |                              |

## User authentication

How are users identified at the devices?

|  | Authentication Method     |  |
|--|---------------------------|--|
|  | ID code                   |  |
|  | SafeCom Casi-Rusco Reader |  |
|  | SafeCom Cotag Reader      |  |
|  | SafeCom Deister Reader    |  |



|  | Authentication Method                 |  |
|--|---------------------------------------|--|
|  | SafeCom EM Reader                     |  |
|  | SafeCom Felica Reader                 |  |
|  | SafeCom HID Reader 35 bit             |  |
|  | SafeCom HID Reader 37 bit             |  |
|  | SafeCom iCLASS Reader                 |  |
|  | SafeCom Indala Reader 26bit           |  |
|  | SafeCom Indala Reader 29bit           |  |
|  | SafeCom IoProx                        |  |
|  | SafeCom Legic Reader                  |  |
|  | SafeCom Magnetic Card Reader, Track 1 |  |
|  | SafeCom Magnetic Card Reader, Track 2 |  |
|  | SafeCom Magnetic Card Reader, Track 3 |  |
|  | SafeCom Magnetic Card Reader DD, Tr 1 |  |
|  | SafeCom Magnetic Card Reader DD, Tr 2 |  |
|  | SafeCom Magnetic Card Reader DD, Tr 3 |  |
|  | SafeCom Mifare Reader                 |  |
|  | SafeCom NEDAP Reader                  |  |
|  | SafeCom NexWatch Reader               |  |

## Devices

Devices can be SafeCom-enabled by means of:

- **SafeCom Controller**(Type = EC): Involves the SafeCom Controller and a SafeCom ID device (normally, the SafeCom Front-end). This solution is independent of the printer firmware version.
- **SafeCom Go in the device**(Type = GO): SafeCom software is installed on the device's hard disk or on a memory module. Attaching a SafeCom ID device (card reader) may require a SafeCom ID kit. Always check if there are any dependencies of the printer firmware version.
- **SafeCom Go / SafeCom Device Server**(Type = GS): User interaction is through the device's touch-screen control panel, but SafeCom communication happens through the SafeCom Device Server. Always check if there are any dependencies of the printer firmware version.
- **SafeCom Go / SafeCom Controller**(Type = GC): User interaction is through the device's touch-screen control panel, but SafeCom communication happens through the SafeCom Controller. Always check if there are any dependencies of the printer firmware version.

Use the table below to record the SafeCom device and printer firmware level.

| Device |          | SafeCom |         |
|--------|----------|---------|---------|
| Model  | Firmware | Type    | Version |
|        |          |         |         |

|                              |              |    |                |
|------------------------------|--------------|----|----------------|
| HP Color LaserJet CM4730 MFP | 50.011.6     | GO | S89 110.030*42 |
| Xerox WorkCentre Pro 255     | 14.60.22.000 | GC | S80 508.770*42 |
| ...                          |              |    |                |
| ...                          |              |    |                |
| ...                          |              |    |                |
| ...                          |              |    |                |
| ...                          |              |    |                |
| ...                          |              |    |                |
| ...                          |              |    |                |
| ...                          |              |    |                |
| ...                          |              |    |                |

### Printer drivers

| Printer driver               | Version      |
|------------------------------|--------------|
| HP Color LaserJet 4730mfp PS | 60.52.262.32 |
| ...                          |              |
| ...                          |              |
| ...                          |              |
| ...                          |              |

## Chapter 19

# scPortUtility operations and exit codes

## Push Port Creation

Push Port Creation creates a new SafeCom Push Port and a related tracking device on the target machine if the port does not already exist.

### Command Line usage

```
scPortUtility --create-push-
port
--port <port
name>
--output-address <output device
address>
--sc-server-addresses <SafeCom server address
list>
--sc-user <SafeCom Administrator
username>
--sc-password <SafeCom Administrator password>
--target-machine <target machine address>
--output-port <output device port>
--tracking-address <tracking device>
--tracking-name <tracking device name>
--tracking-location <tracking device location>
--snmp
--show-price
--driver-name <driver name>
--model <model name>
--duplex
--color
--charging-scheme-id1 <numerical scheme id>
--charging-scheme-id2 <numerical scheme id>
--hide-jobs
```

### Options and parameters

--create-push-port

#### Required

This switch specifies that the Push Port Creation command should be executed.

--port <port name>

#### Required

The parameter specifies the name of the port to be created.

```
--output-address <output device address>
```

**Required**

This is the address or name of the device the print output is forwarded to.

```
--sc-server-addresses <SafeCom server address list>
```

**Required**

The parameter provides a semicolon-separated list of SafeCom servers to which the new port should connect, in order of priority. They can be specified either as IP or fully qualified hostnames.

The SafeCom Port Utility also uses this list.

```
--sc-user <SafeCom Administrator user name>
```

**Required**

This is the SafeCom Administrator user name.

```
--sc-password <SafeCom Administrator password>
```

**Required**

This is the SafeCom Administrator user password.

```
--target-machine <target machine address>
```

Hostname or address of the machine on which to create the new port. Default is the local machine.

```
--output-port <output device port>
```

TCP/IP port of the target device. The default is 9100, which is the standard RAW / JetDirect port.

```
--tracking-address <tracking device>
```

This is the address of the SafeCom server tracking device.

If this option is not specified, the specified output device is used instead.

```
--tracking-name <tracking device name>
```

This is the name of the tracking device.

If this is not specified, the tracking device is named the same as the SafeCom Push port.

```
--tracking-location <tracking device location>
```

This option specifies the location of the tracking device as it appears in scAdministrator.

If this is not specified, the location field in scAdministrator is empty.

```
--snmp
```

This switch enables SNMP for the newly created port. If the option is not specified, the default value is OFF.

`--show-price`

Show job prize before printing. If the option is not specified, the default value is OFF.

`--driver-name <driver name>`

Override the driver name with the specified name when committing jobs to the SafeCom server.

`--model <model name>`

Tracking device model. The model name is displayed in the SafeCom Administrator Console.

`--duplex`

Specifies that this is a duplex-capable tracking device.

`--color`

Specifies that this is a color tracking device.

`--charging-scheme-id1 <numerical scheme id>`

Primary charging scheme used for price calculation.


`--charging-scheme-id2 <numerical scheme id>`

Secondary charging scheme used for price calculation.

`--hide-jobs`

This switch enables the hide jobs feature, which hides the job names in the print queue. If the option is not specified, the default value is OFF.

If the switch is specified and the SafeCom Push Port monitor does not support the feature, port creation fails.

 The option works with G4-520 (or later) SafeCom Push Port monitors.

## Exit codes

0—SCPORTUTIL\_ERROR\_SUCCESS

The operation completed successfully.

1—SCPORTUTIL\_ERROR\_GENERAL\_FAILURE

The operation could not be completed due to a general failure.

2—SCPORTUTIL\_ERROR\_ACCESS\_DENIED

Access is denied by target machine (Windows Print Spooler) or the SafeCom server.

3—SCPORTUTIL\_ERROR\_INVALID\_PARAMETER

One of the command line parameters is incorrect.

4—SCPORTUTIL\_ERROR\_CAN\_NOT\_CONNECT\_TO\_SC

A connection attempt to a SafeCom server failed.

5—SCPORTUTIL\_ERROR\_SC\_MONITORS\_NOT\_INSTALLED

The SafeCom print monitor is not installed on the target machine.

6—SCPORTUTIL\_ERROR\_INVALID\_PORT\_NAME

The specified port name is invalid.

9—SCPORTUTIL\_ERROR\_CAN\_NOT\_CREATE\_TRACKING\_DEVICE

The tracking device cannot be created.

12—SCPORTUTIL\_ERROR\_PORT\_ALREADY\_EXISTS

The specified port already exists.

13—SCPORTUTIL\_ERROR\_SPOOLER\_CALL\_FAILED

A call to the Windows Print Spooler failed.

15—SCPORTUTIL\_ERROR\_INVALID\_QUEUE\_NAME

The queue name or target machine is invalid.

## Remarks

### SafeCom user authentication

The newly created port uses the default user authentication scheme, which is "Use network logon".

### SafeCom server performance considerations

When running the tool during user logon or rollout scenarios, take into consideration that this command contacts the SafeCom server and might create new tracking devices.

You might want to limit the number of concurrent calls.

### Tracking devices

If a tracking device with the same name already exists, the existing tracking device is used and no new tracking device is created.

If more than one tracking device with the same name already exists, an arbitrary device with the same name is selected.

Existing tracking devices are not updated with any settings provided to this command.

The automatically created tracking device has the same name as the port if no other name is specified.

## Attach Port

The `Attach Port` command attaches an already existing port to an already existing queue.

### Command Line usage

```
scPortUtility --attach-
port
--port <port
name>
--queue <queue name>
--target-machine <target machine address>
```

### Options and parameters

`--attach-port`

#### Required

This switch specifies that the Attach Port command should be executed.

`--port <port name>`

#### Required

The parameter specifies the name of the port to be created.

`--queue <queue name>`

#### Required

The name of the Windows Spooler print queue that is to be attached to the specified port.

`--target-machine <target machine address>`

Hostname or address of the machine on which the queue and port are located. Default is the local machine.

### Exit codes

0—SCPORTUTIL\_ERROR\_SUCCESS

The operation completed successfully.

1—SCPORTUTIL\_ERROR\_GENERAL\_FAILURE

The operation could not be completed due to a general failure.

3—SCPORTUTIL\_ERROR\_INVALID\_PARAMETER

One of the command line parameters is incorrect.

6—SCPORTUTIL\_ERROR\_INVALID\_PORT\_NAME

The specified port name is invalid.

13—SCPORTUTIL\_ERROR\_SPOOLER\_CALL\_FAILED

A call to the Windows Print Spooler failed.

15—SCPORTUTIL\_ERROR\_INVALID\_QUEUE\_NAME

The queue name or target machine is invalid.

16—SCPORTUTIL\_ERROR\_QUEUE\_NOT\_SUPPORTED

The specified queue is not supported.

- RDP queue
- remote queue / share

17—SCPORTUTIL\_ERROR\_WIN32\_FAILURE

A call to the Windows API failed.

## Queue Migration – Push Print

Migration of Windows printer queue from using Standard TCP/IP Monitor ports to SafeCom Push Port Monitor ports.

It uses the available information from the attached Standard TCP/IP port to create a new SafeCom Push Port, and changes the queue to use this new port.

### Command Line usage

```
scPortUtility --migrate-to-
push
--queue <queue
name>
--port <port
name>
--sc-server-addresses <SafeCom Server address
list>
--sc-user <SafeCom Administrator
username>
--sc-password <SafeCom Administrator password>
--target-machine <target machine address>
--tracking-address <tracking device>
--tracking-name <tracking device name>
--tracking-location <tracking device location>
--driver-name <driver name>
--model <model name>
--show-price
--duplex
--color
--charging-scheme-id1 <numerical scheme id>
```



```
--charging-scheme-id2 <numerical scheme id>
```

## Parameters

```
--migrate-to-push
```

### **Required**

This switch specifies that the Migrate command should be executed.

```
--queue <queue name>
```

### **Required**

The name of the Windows Spooler print queue which should be migrated.

```
--port <port name>
```

### **Required**

The parameter specifies the name of the port to be created.

```
--sc-server-addresses <SafeCom server address list>
```

### **Required**

The parameter provides a semicolon-separated list of SafeCom servers to which the new port should connect, in order of priority. They can be specified either as IP or fully qualified hostnames.

The SafeCom Port Utility also uses this list.

```
--sc-user <SafeCom Administrator user name>
```

### **Required**

This is the SafeCom Administrator user name.

```
--sc-password <SafeCom Administrator password>
```

### **Required**

This is the SafeCom Administrator user password.

```
--target-machine <target machine address>
```

Hostname or address of the machine on which to create the new port. Default is the local machine.

```
--tracking-address <tracking device>
```

This is the address of the SafeCom server tracking device.

If this option is not specified, the specified output device is used instead.

```
--tracking-name <tracking device name>
```

This is the name of the tracking device.

If this is not specified, the tracking device is named the same as the SafeCom Push port.

`--tracking-location <tracking device location>`

This option specifies the location of the tracking device as it appears in scAdministrator.

If this is not specified, the location field in scAdministrator is empty.

`--driver-name <driver name>`

Override the driver name with the specified name when committing jobs to the SafeCom server.

`--model <model name>`

Tracking device model. It is displayed in the SafeCom Administrator Console.

`--show-price`

Show job prize before printing.

`--duplex`

Specifies that this is a duplex-capable tracking device.

`--color`

Specifies that this is a color tracking device.

`--charging-scheme-id1 <numerical scheme id>`

Primary charging scheme used for price calculation.

`--charging-scheme-id2 <numerical scheme id>`

Secondary charging scheme used for price calculation.

## Exit codes

0—SCPORTUTIL\_ERROR\_SUCCESS

The operation completed successfully.

1—SCPORTUTIL\_ERROR\_GENERAL\_FAILURE

The operation could not be completed due to a general failure.

2—SCPORTUTIL\_ERROR\_ACCESS\_DENIED

Access is denied.

3—SCPORTUTIL\_ERROR\_INVALID\_PARAMETER

The command line parameter is incorrect.

4—SCPORTUTIL\_ERROR\_CAN\_NOT\_CONNECT\_TO\_SC

A connection attempt to a SafeCom server failed.

5—SCPORTUTIL\_ERROR\_SC\_MONITORS\_NOT\_INSTALLED

The SafeCom print monitor is not installed.

6—SCPORTUTIL\_ERROR\_INVALID\_PORT\_NAME

The specified port name is invalid.

9—SCPORTUTIL\_ERROR\_CAN\_NOT\_CREATE\_TRACKING\_DEVICE

The tracking device cannot be created.

12—SCPORTUTIL\_ERROR\_PORT\_ALREADY\_EXISTS

The specified port already exists.

13—SCPORTUTIL\_ERROR\_SPOOLER\_CALL\_FAILED

A call to the Windows Print Spooler failed.

15—SCPORTUTIL\_ERROR\_INVALID\_QUEUE\_NAME

The queue name or target machine is invalid.

16—SCPORTUTIL\_ERROR\_QUEUE\_NOT\_SUPPORTED

The queue name is invalid. The specified queue is not supported, could be due to:

- Port pooling
- No port attached
- RDP queue
- Remote queue / share

17—SCPORTUTIL\_ERROR\_WIN32\_FAILURE

A call to the Windows API failed.

## Remarks

### Supported queue types

Only queues that use any of the supported port types are supported for migration.

### Unsupported queue types

The tool does not support migration of the following queue types:

- Remote queues not local to the target machine. Queues that are attached using shares.
- Queues with no port attached
- Remote Desktop queues
- Queues that have Printer Pooling enabled

## Supported port types

Only queues that are attached to Standard TCP/IP ports using the RAW protocol are supported for migration. The LPR protocol is not supported.

## Existing ports and queues

The existing Standard TCP/IP port is not deleted or altered in any way.

Other queues attached to the same Standard TCP/IP port are not affected.

## SafeCom user authentication

The newly created port uses the default user authentication scheme, which is "Use network logon".

## SafeCom server performance considerations

When running the tool during user logon or rollout scenarios, take into consideration that this command contacts the SafeCom server and might create new tracking devices.

You might want to limit the number of concurrent calls.

## Tracking devices

If a tracking device with the same name already exists, the existing tracking device is used and no new tracking device is created.

If more than one tracking device with the same name already exists, an arbitrary device with the same name is selected.

Existing tracking devices are not updated with any settings provided to this command.

The automatically created tracking device has the same name as the port if no other name is specified.

## List print queues

This operation outputs a list of print queues, their attached port, port types, and port descriptions.

It can be restricted to only output queues that are eligible for migration by the SafeCom Port Utility.

## Command Line usage

```
scPortUtility --list-print-queues
--only-migratable
--target-machine <target machine address>
```

## Options and parameters

`--list-print-queues`

### **Required**

This switch specifies that the List Print Queues command should be executed.

`--only-migratable`

List only queues that are eligible for migration by the SafeCom Port Utility.

`--target-machine <target machine address>`

Hostname or address of the machine on which the queue and port are located. Default is the local machine.

## Exit codes

0—SCPORTUTIL\_ERROR\_SUCCESS

The operation completed successfully.

1—SCPORTUTIL\_ERROR\_GENERAL\_FAILURE

The operation could not be completed due to a general failure.

3—SCPORTUTIL\_ERROR\_INVALID\_PARAMETER

The command line parameter is incorrect.

13—SCPORTUTIL\_ERROR\_SPOOLER\_CALL\_FAILED

A call to the Windows Print Spooler failed.

15—SCPORTUTIL\_ERROR\_INVALID\_QUEUE\_NAME

The target machine is invalid.

17—SCPORTUTIL\_ERROR\_WIN32\_FAILURE

A call to the Windows API failed.

## Appendix A

# Frequently asked questions

In the following subsections, you can find answers to some of the questions frequently asked by administrators.

## What are the benefits of Pull Printing?

- Using cost-effective workgroup devices as personal devices without jeopardizing document security. This means fewer devices to provide service to, because all smaller personal devices can be taken out of service. With fewer devices, office space is freed up to accommodate user-friendly and efficient floor plans.
- Documents follow users to their choice of device. If one device is out of order, users can collect their documents at another SafeCom-enabled device.
- Depending on your printing environment, users may need access to only one shared SafeCom Pull Printer on a server to print on any SafeCom-enabled device (see [Printer driver and document fidelity considerations](#)). This allows a much less complex printing environment and little to no print queue setup on the users' computers.
- When the users are logged in at the device, they have full control and time to load stationery, transparencies, labels, or other media that may require manual feed.
- Users who print many small documents do not need to rush to the device every time they print. They can collect their documents when it suits them.
- The time spent at the device waiting for the documents to print is limited because workgroup devices can output 40 or more pages per minute. Workgroup devices typically support double-sided print (duplex), printing multiple pages on the same page (N-up printing), and booklet printing. With booklet printing, an 8-page document can be printed on 2 sheets of paper (paper use is reduced by 75%).

In addition to these benefits, you can gain additional benefits by installing any of the following SafeCom add-on modules.

- [SafeCom Tracking](#)
- [SafeCom Rule Based Printing \(RBP\)](#)
- [SafeCom Client Billing](#)
- [SafeCom Pay](#)

## Is Copy Control supported?

Yes, on selected Multifunction Printers (MFPs) the SafeCom solution can control access to the copy function. The user has to log in before copying is allowed.

**i** Such control may restrict access to several MFP functions, depending on the specific configuration.

## Is it possible to charge for print costs?

Yes. With SafeCom Tracking, you can monitor print and copy usage and use the recorded data for subsequent departmental invoicing. Tracking applies to the following:

- Documents printed directly to the device (Push Print)<sup>58</sup>
- Documents requiring user login at the device (Pull Print)
- Copies made after user login at the MFP (Copy Control)

With [SafeCom Pay](#) (an add-on to [SafeCom Tracking](#)), users can be required to pay up front for printing and copying. With SafeCom ePay, users can revalue their account.

## Is it necessary to install software on the users' computers?

No, it is normally not necessary to install software on the users' computers. However, there are a few exceptions where it is necessary to install a [local SafeCom Pull Printer](#) on users' computers.

## How are users authenticated?

Users can log in by card or ID code. See [User authentication by card or ID code](#). A complete list of supported ID devices can be found in [SafeCom ID devices](#). There are basically two types of ID devices to select from:

- **Card Reader:** All the user's documents are printed as the user's personal card is used.
- **Card Reader and touch-screen:** Document security can be enhanced by requesting the user to enter a personal PIN code when using their card. Or the user can enter an ID code instead of using a card. Once logged in, the user can print all documents with a single touch or browse through the list of documents to print, delete, retain, or request multiple copies of individual documents.

---

<sup>58</sup> Tracking of Push Print does not require SafeCom device software or hardware.

## How are users managed?

Users can be created in advance, either manually, or through a user import wizard (see [Import users](#)), or they can be created the first time they print.

## How are users with the same name handled?


Users with the same name from multiple domains can be added to the SafeCom solution. User logon does not have to be unique across domains. The user John Smith (JS) within domain A is different from the user John Smith (JS) within domain B and is different from John Smith (JS) with no domain info.

## How many users, printers, and documents can a server handle?

The bottleneck is the number of concurrent documents (print jobs) that can go to and from the SafeCom server. The performance of a SafeCom server is comparable to that of a Windows print server. This means that a SafeCom server is capable of supporting approximately as many devices as you would normally install on an equivalent Windows print server.

## Can access to devices be restricted?

Yes, it is possible to control users' access to devices (printers and MFPs) based on the organizational relationship between the user and device (see [Organizational units](#)) or with [SafeCom Rule Based Printing \(RBP\)](#).

 Access to specific functions can also be restricted on the same basis.

## Are SafeCom solutions scalable?

Yes. With a SafeCom Enterprise Server license, it is possible to use multiple servers to scale the SafeCom solution to match the demanding requirements of large organizations with thousands of users and hundreds of devices.

Scalability is achieved by adding the required number of SafeCom servers. Users can switch between locations to collect their documents at any SafeCom-enabled device and at any location regardless of the server where the document was printed.

Large companies and organizations that use multiple Windows print servers to handle printing today are likely to need a SafeCom Enterprise Server license.



## How does a solution with multiple servers work?

A SafeCom multiserver solution consists of one SafeCom primary server and one or more SafeCom secondary servers.

The SafeCom primary server uses the replication capabilities of its Microsoft SQL server to ensure that all SafeCom secondary servers' databases are up-to-date at all times. The SafeCom secondary servers can use the provided Microsoft SQL server for free and are not required to run a licensed Microsoft SQL server.

A user's home server denotes the SafeCom server. Because data about users and devices is known on all servers, only the users and devices belonging to a particular secondary server (home server) are affected if that server goes down.

Enterprise customers, whose printing is mission-critical, often use the Microsoft cluster service (see [Cluster installation](#)) to further ensure the availability of SafeCom servers. SafeCom print queues can be installed on any of the SafeCom servers, but most enterprise customers select to install print queues on the SafeCom secondary servers only and keep the primary server free from print processing tasks so it only needs to replicate data (and collect tracking data from the secondary servers).

It is possible to distribute the print processing task to ordinary Windows print servers by doing a SafeCom [Client installation](#) on these. However, this can increase the network load, because Pull Print jobs must go onto the network for a longer time (to get transferred from the Windows print server to the user's home server, if the **Store Doc on First Server** option is disabled). This can slow performance if the file size of the resulting print jobs is big. File size and document length do not always correlate. For example, a two-page PDF file can grow to 500 MB. This heavily depends on the printer driver.

## Can documents be printed securely?

Yes. With SafeCom encryption, documents can be encrypted on the network from the moment the user clicks Print on the computer until the document is collected at the device. This prevents anyone from reading the documents, should they be intercepted on the network. Documents are always encrypted when they are stored for later printing (see [Printing encrypted documents](#)).

Basic document security is achieved by requesting users to log in by means of both a personal ID card (or ID code) and a PIN code when they collect their documents at the device.

## What happens to uncollected documents?

Documents remain on the SafeCom server until the user logs in at the device to collect the documents. Documents that are not collected by users are automatically deleted after a configurable time.

## Is it always possible to print?

Printing may not always be possible. The SafeCom solution is dependent on the stability of your network, devices, and computers, especially the hard disks. However, with the SafeCom Pull Print solution, if a device fails, users can collect their documents at another device.

In general, you should apply the same measures to ensure that Windows print servers and Windows domain controllers are up and running at all times. The following technologies reduce the risk of failure:

- Hard disks with RAID or similar technology
- Microsoft cluster service (see [Cluster installation](#))
- Duplicated network connections
- Backup of databases, so you can re-create the SafeCom solution in case of computer failure (see [Backup and restore](#))

## Can print usage be tracked without hardware?

Yes. With the Push Print tracking concept in SafeCom Tracking, users can print directly to the device and still have their print usage tracked. It is not necessary to install dedicated SafeCom hardware. The device can be networked or locally attached to a Windows computer through a parallel, USB, or SCSI port.

## Can a Pull Printer be used for Push tracking?

Yes, a SafeCom-enabled device can also be used to track documents that are sent directly. In other words, users are offered the choice of Push or Pull Printing, while maintaining total print cost management. To prevent documents from being mixed, incoming Push Printed documents are put on hold as long as someone is logged in at the printer or MFP.

## What happens if the SafeCom solution stops working?

In case of any problems, the SafeCom solution has three methods to communicate the issues.

- **On the user's computer:** A message appears on the user's computer screen when trying to print through the SafeCom solution. The message can read: "Unable to connect to SafeCom server. Document is not printed. Please contact your administrator!" See [User computer: Please contact your administrator!](#) for additional messages.
- **At the device:** An "OUT OF ORDER" screen is displayed on the SafeCom-enabled device while the problem persists (see [Device web interface: Displayed incorrectly or settings not saved](#)).
- **E-mail to administrator:** The administrator can receive service and error (event log) messages through [E-mail](#).

## What is the administrative overhead?

Under the right circumstances, your SafeCom solution is capable of creating users automatically the first time they print through the SafeCom solution. The system can send a welcome e-mail with instructions to new users the first time they print. This method reduces the administrative overhead to a minimum (see [Create users at first print](#)).

In the [Planning your SafeCom solution](#) chapter, you learn how your SafeCom solution can become one that reduces print costs, is easy to administer, and yields high user satisfaction. Chapter [Planning your SafeCom solution](#) features a checklist for planning your SafeCom solution (see [Checklist – to help you on the way](#)), a section on [rollout considerations](#), and input to the administrative procedures you need to have in place (see [Clearly define responsibilities and procedures](#)).

Chapter [Troubleshooting](#) is a comprehensive troubleshooting guide. You can even configure the SafeCom solution to e-mail you service and error (event log) messages.

## What about integration with other systems?

In addition to being a modular solution, the SafeCom solution also features a number of Application Programming Interfaces (APIs). The SafeCom Administrator API allows you to automate tasks and integrate the SafeCom solution with other systems. It is an XML-based tool available as an executable and DLL. The SafeCom Batch Print API can be used for integration with document archiving systems.

Kofax is always ready to discuss customized development, if this is required to optimize your print and copy solution. For details, contact your Kofax sales representative.

## Does it pay to apply a SafeCom solution?

It is a common (and costly) mistake to compare the price of a SafeCom solution with the purchase price of today's devices. The purchase price of the device constitutes only a small fraction compared to the lifetime costs of consumables (paper, toner, and moving parts).

Calculations should be based on the amount of money saved due to reduced print costs and administrative and organizational benefits.