

Kofax SafeCom Mobile Print Administrator's Guide

Version: 4.3.0

Date: 2023-05-03

KOFAX

© 1995-2023 Kofax. All rights reserved.

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

Table of Contents

Preface	8
Related documentation.....	8
Training.....	8
Getting help with Kofax products.....	8
Chapter 1: Introduction	10
Requirements.....	11
Mobile Print Gateway requirements.....	11
Performance considerations.....	12
Supported documents.....	13
Supported languages.....	13
Chapter 2: Prerequisites	15
Microsoft Office.....	15
Install Microsoft Office.....	15
Configure Microsoft Office.....	15
Install Microsoft Office add-in.....	16
OpenOffice.....	16
Install OpenOffice.....	16
Set up OpenOffice Writer.....	16
SafeCom Pull Port.....	17
Install SafeCom G4 client.....	17
Add a local SafeCom Pull Port.....	17
Enable printer pooling.....	18
Chapter 3: SafeCom Mobile Print installation	19
Install SafeCom Mobile Print.....	19
Mobile Gateway installation.....	19
Mobile Gateway configuration.....	20
Windows Firewall – ports that must be opened.....	22
Chapter 4: Configure SafeCom Mobile Print	24
Log in to the SafeCom Mobile Print web interface.....	24
Add devices to SafeCom Mobile Print.....	24
Add all devices from the server.....	24
Add devices manually.....	25
General settings.....	26
Check for updates.....	26

Debug logging.....	26
Document support.....	26
Application settings.....	27
Language and location.....	27
Printing and security.....	28
User authentication.....	30
LDAP authentication.....	31
Email and Google Cloud Print authentication.....	31
SafeCom authentication.....	32
SafeCom Guest Users Self-Signup.....	32
User web portal configuration.....	33
Web Portal single sign-on.....	34
Modify language text strings.....	35
Change default Web ports from 7290 and 9443.....	36
Web print configuration.....	36
Driver print configuration.....	37
Advanced Driver Print.....	38
LPD server.....	38
Email print configuration.....	38
Enable Email Print.....	39
Configure incoming mail.....	39
Email print settings.....	39
Email print permissions.....	40
Configure outgoing mail.....	40
Configure HTML zoom rendering.....	41
Printing HTML emails with inline images.....	41
Wide Area Mobile Print.....	41
Configuration overview.....	42
Create Wide Area Mobile Print sub domains.....	43
Configure SafeCom Mobile Print Gateway.....	43
Configure DNS server.....	44
Verify DNS configuration.....	47
Set search domains on mobile devices.....	48
One Wide Area Mobile Print sub domain.....	48
Multiple Wide Area Mobile Print sub domains.....	50
Configure Google Cloud print.....	52
Enable Google API access.....	52
Register printers.....	52

Enable Public Link sharing.....	53
Print with AirPrint on iOS.....	53
Authenticated print.....	53
Print with Android.....	54
Native print on Android.....	54
Card server.....	55
Card Reader Profile.....	56
Direct E-mail Print to Printer Email Alias.....	56
Configure mail forwarding account on Microsoft Exchange.....	57
Mobile Print configuration.....	57
Using SSL with SafeCom Mobile Print.....	58
Generate a test certificate.....	58
Configure SafeCom Mobile Print with the test certificate.....	59
Verify the test certificate.....	59
Obtain a trusted certificate.....	60
Chapter 5: Administer SafeCom Mobile Print.....	61
Log in to the SafeCom Mobile Print web interface.....	61
Access SafeCom Mobile Print web interface remotely.....	61
Dashboard with statistics.....	61
See the reporting data for a specific period.....	62
See all activity from a specific user in a date range.....	62
SafeCom Mobile Print monitor.....	62
Hide user and document information in Monitor.....	62
Hide the Monitor completely.....	63
Manage existing printers.....	63
Associate network card reader with device.....	63
Manage user email addresses.....	64
Delete an email address from a user.....	64
Associate a new email address to a user.....	64
Import User Email Addresses from a CSV file.....	64
Change Administrator Login.....	65
Back up SafeCom Mobile Print data.....	65
Upgrade SafeCom Mobile Print.....	65
Licensing.....	66
Uninstall SafeCom Mobile Print.....	66
Chapter 6: Use SafeCom Mobile Print.....	67
Log in to User Web Portal.....	67
Send a print job through AirPrint.....	67

Using AirPrint.....	67
Send a print job through email.....	67
Send email print.....	68
Send email printer and control choice of printer.....	68
Register a new email address.....	69
Send a print job through web.....	69
Upload document for print.....	69
Driver Print.....	70
Guest printing.....	71
Private Print Clouds.....	71
Pull print essentials.....	71
Create Private Print Cloud.....	72
Print to Private Print Cloud.....	72
Using the SafeCom Mobile Print iOS app.....	72
Configuration.....	72
Account.....	73
Releasing available print jobs.....	73
Print using Open in or the Print with Mobile Print action.....	74
Setting custom output options.....	74
Output printer selection.....	74
AirPrint vs. Open in vs. Print with Mobile Print action.....	75
Chapter 7: Troubleshooting.....	76
Common LDAP authentication error codes.....	76
Using an LDAP browser.....	76
Log files.....	76
LDAP errors.....	76
Active Directory Specific Errors.....	78
Chapter 8: Clustering for high availability and scalability.....	80
Cluster servers overview.....	81
Server types.....	82
Configuration types.....	83
Prerequisites for a cluster configuration.....	83
Configure a primary server.....	84
Open firewall on primary server.....	84
Configure shared spool in primary server.....	84
Configure additional secondary servers.....	85
Configure shared spool in secondary server.....	85
Modify secondary server's cluster configuration.....	85

Replicate printers from primary server.....	86
Install SafeCom Mobile Print in a Windows failover cluster.....	86
Validate cluster.....	87
Install SafeCom Mobile Print on first active node.....	88
Change service logon accounts.....	88
Move database to shared storage.....	88
Modify primary cluster nodes configuration.....	90
Change the primary server's spool folder.....	90
Add external load balancer for high front-end scalability.....	91
Replicate printers across all servers.....	92
Windows Print Migration Printbrm.exe command-line tool.....	92
Licensing in clustered configurations.....	93
SafeCom Mobile Print clustering in high-availability virtual configurations.....	93

Preface

This guide includes instructions for installing, configuring, and using Kofax SafeCom Mobile Print.

Related documentation

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

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

Training


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

Getting help with Kofax products

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

To access the Kofax Knowledge Base:

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

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

The Kofax Knowledge Base provides:

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

From the Knowledge Base home page, you can:

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

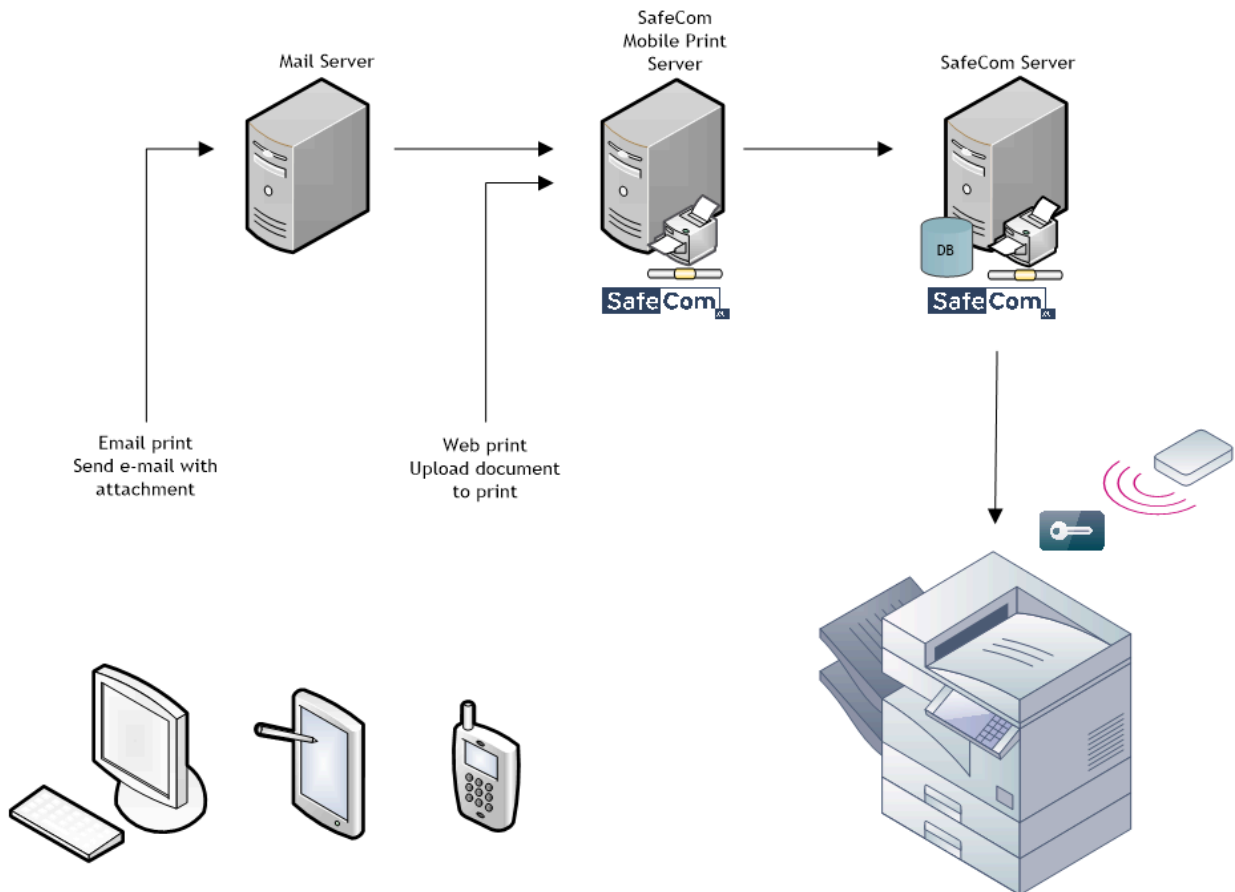
Chapter 1

Introduction

SafeCom Mobile Print enables users to print from their workstation computers, laptops and notebooks, mobile devices and tablets through email or web. Users upload the print job to a website or send the job as an email attachment to a defined email address. The print job is then made available for the user to collect at any SafeCom-enabled network printer.

SafeCom Mobile Print is very flexible. Users can submit a print job from any computer or device at hand, collect the print job at a company network printer, and still be guaranteed the same security and flexibility that characterize a SafeCom Smart Printing solution.

The following is an overview of the SafeCom Mobile Print setup.



Requirements

For a successful SafeCom Mobile Print installation, you need:

- One server with SafeCom G4 Server version S82 070.520*07 or higher installed.
- One server, where SafeCom Mobile Print must be installed, with the following minimum specifications:
 - Supported servers include: Windows Server 2008 SP1 (32 or 64-bit), Windows Server 2008 R2 (32 or 64-bit), Windows Server 2012 (64-bit), Windows Server 2012 and 2012 R2 (64-bit), Windows Server 2016.
 - Recent generation server CPU processor, such as Intel Xeon 64 or equivalent (see note below on performance). Desktop CPUs are NOT recommended for production use.
 - Minimum 1 GB free RAM memory (minimum 4 GB free RAM memory recommended for higher volume processing).
 - Minimum 5 GB free hard disk space for print job spooling and processing (10 GB free disk space recommended for higher volume processing).
 - No antivirus program monitoring or interrupting the SafeCom Mobile Print directories.
 - No proxy server interrupting local communication on the server (localhost/127.0.0.1).
 - A local administrative user.
 - Internet Explorer Enhanced Security must be disabled to print Web addresses.



- SafeCom Mobile Print can be a resource demanding application, which requires sufficient CPU and memory. If SafeCom Mobile Print is expected to handle significant print volume, make sure that the server, on which the application is installed, has enough CPU and memory. Alternatively, multiple SafeCom Mobile Print servers should be set up.
- Ensure that MS Visual C++ 2008 Redistributable Package (x86) is installed.

Mobile Print Gateway requirements

By default, SafeCom recommends installing the Mobile Print Gateway on the same server as the SafeCom Mobile Print server. Also, Kofax recommends that iOS and Android devices should belong to the same local subnet.

If you are installing it on a separate server, it must meet the following minimum requirements:

- Windows Server 2008 SP1 (64-bit) or Windows Server 2008 R2 (64-bit) or newer
- Recent generation server CPU processor, such as Intel Core, Xeon or equivalent
- Minimum 1 GB free RAM memory
- Minimum 5GB free hard disk space
- No antivirus program monitoring or interrupting the SafeCom Mobile Print Gateway directories
- iOS 4.3 or later (excluding iOS 5.1.1)
- Android version 2.3.4 or newer

Performance considerations

SafeCom Mobile Print can be a resource demanding application, as the SafeCom Mobile Print typically handles many of the tasks done by a normal workstation.

In a normal client/server environment, when a user prints a Word document, Office on the client computer renders the document to print. With SafeCom Mobile Print, if a user uploads a Word document, that conversion and rendering now takes place on the server, and effectively SafeCom Mobile Print assumes the workload of numerous clients.

Thus it is essential that the SafeCom Mobile Print server is fitted with a sufficiently powerful CPU and memory to handle the print volume.

SafeCom Mobile Print allows multiple ways to print: Web upload, Driver Print, Email Print and Mobile/App print. Each of these perform differently, and performance further depends on the document type and complexity of the document.

- **Web Print:**
Upload of Microsoft Office or OpenOffice documents is most resource demanding, with each job processing taking from 1-2 seconds for simple jobs to 15-20 seconds for more complex documents. PDF documents and images require very little server processing, and are processed typically in less than 2 seconds.
- **Email Print:**
Office, PDF and images attached to emails are processed similar to Web Print jobs, and take the same time and resources to process.
- **Driver Print:**
With Driver Print there are two different core methods: "Simple" which uses a generic driver the user have already got on their machine, meaning no need to download and install a driver for the user; and "Advanced" where the user uses a manufacturer Postscript or PCL driver, for example, to use finishing options like stapling and binding. Driver Print fundamentally is very efficient. With "Simple" driver print, users print with a generic Postscript driver, and this data is converted and ultimately sent to the final destination printer using the driver installed on the SafeCom Mobile Print server.
- **Mobile Print:**
Print jobs from native app printing from mobile devices is typically very efficient, as little processing is required.

In case of excessive print job volume within a short time, the server will simply let jobs it cannot handle expire.

The following numbers are based on load testing with mixed Office and PDF documents, various number of pages and complexity, to simulate a typical customer environment.

The server was an Intel i7-level server CPU with 4 GB ram on Windows 2008 R2 only running SafeCom Mobile Print and Microsoft Office. This server could process and print:

Web/Email print:	800 Jobs per hour
Simple Driver Print:	1500 Jobs per hour
Advanced Driver Print:	12000 Jobs per hour

Mobile Print:	1500 Jobs per hour
---------------	--------------------

So the usage pattern, volume of jobs, features used and the documents printed fully determines how many servers are needed. Target the number of servers for the peak load. If using a high-end server and the expected print volume is less than above test results, a single server should be sufficient.

Supported documents

The following document formats are supported through Web and Email Print. All document formats are supported under Driver Print.

File format	Requirements
PDF, HTML, HTM, GIF, PNG, JPEG, TIFF	None
DOC, DOCX, XLS, XLSX, PPT, PPTX, RTF, TXT	Microsoft Office
ODT, ODS, ODP	OpenOffice

Supported languages

The SafeCom Mobile Print Administrator interface is available in English, French, and German.

In addition, the following table lists the languages and their postfixes supported by Kofax SafeCom Mobile Print for the user web interface and default email language.

Postfix	Language
_cy	Cymraeg
_da	Danish
_de	German
_en	English
_es	Spanish
_et	Estonian
_fr	French
_it	Italian
_nl	Dutch
_no	Norwegian
_pl	Polish
_pt	Portuguese
_fi	Finnish
_se	Swedish

Postfix	Language
_tr	Turkish
_cz	Czech
_ru	Russian
_jp	Japanese
_cn	Chinese
_kr	Korean

Chapter 2


Prerequisites

For the SafeCom Mobile Print solution to be successful, the following must be installed and configured on each SafeCom Mobile Print server in the SafeCom solution:

- [Microsoft Office](#)
- [OpenOffice 3.3.0](#) or newer
- [SafeCom Pull Port](#)

Microsoft Office


For SafeCom Mobile Print to be able to convert Word, Excel, and PowerPoint documents to print format, Office 2013 with at least Word, Excel and PowerPoint, must be installed on the SafeCom Mobile Print server. Microsoft Office must be activated.

 Microsoft Office 64-bit is supported for Microsoft Office versions 2013 and newer.

Install Microsoft Office


The standard installation installs all programs by default, but the installation can be customized to only install the necessary programs (Word, Excel, and PowerPoint). There is no need to install any other Office suite program, such as OneNote, Access, or similar.

Ensure that the Visual Basic for applications component is included in components to install. This is necessary when uploading PPT & PPTX for print through web.

 If you customize the installation, make sure that Fonts and Additional TrueType Fonts under Office Shared Features are installed, for broadest font support.

Configure Microsoft Office

After the installation, it is necessary to open Microsoft Word, as it shows the Privacy Options dialog box, where all options must be cleared as it otherwise prevents printing.

 If Microsoft Office was already installed on the server make sure to disable the privacy options, by opening Word options, then clicking **Trust Center > Trust Center Settings > Privacy option**.

To avoid Microsoft Office restarting and doing server reboots automatically, check I don't want to use Microsoft Update to disable the automatic update service.

After performing these changes, exit and reopen Microsoft Word. If a blank page is displayed, the installation and configuration is completed successfully.

Install Microsoft Office add-in

If the installed version of Microsoft Office is a version earlier than SP2, it is necessary to install the Microsoft Office add-in "Microsoft Save as PDF or XPS" in addition to the basic Microsoft Office installation.

This add-in can be downloaded and installed directly from the Microsoft website.


OpenOffice

Installing OpenOffice on the SafeCom Mobile Print server is optional, and only needed if OpenOffice document support is required in SafeCom Mobile Print.

Microsoft Office has basic support for OpenOffice documents (odt, ods, and odp), but for an accurate conversion of OpenOffice documents, it is highly recommended to install OpenOffice 3.3.0 or later.

Install OpenOffice

It is recommended to install the standard version of OpenOffice which includes JRE (Java Runtime Engine). For example, the filename of a downloaded installer file can be OOo_3.3.0_Win_x86_install-wjRE_en-US.exe.

 Make sure the installation is done as a local administrator user.

1. During the installation, select **Custom** setup type. Click **Next**.
2. In the dialog box **OpenOffice.org Program Modules**, select to install only **Writer, Calc, and Impress**.
3. Under **Optional Components**, scroll to the component **Quickstarter** at the bottom and select **This feature will not be available**.
4. Continue the rest of the installation with default settings.

Set up OpenOffice Writer

After installation, it is necessary to open OpenOffice Writer, as the setup wizard opens on first launch.

1. During the setup in the wizard, make sure to clear the option **Check for updates automatically** under **3. Online Update**.
2. Under **Registration**, select **I do not want to register**.
Selecting this option prevents printing.
3. Close and open OpenOffice Writer again, and in the **Improvement Program** dialog box, select **No, I do not wish to participate**.
4. Click **OK**.

The installation of OpenOffice is now complete.

SafeCom Pull Port

A local SafeCom Pull Port must be added on the SafeCom Mobile Print server in order to connect to the SafeCom Server.

To add a local SafeCom Pull Printer on the SafeCom Mobile Print server, the following three steps must be performed:

- [Install SafeCom G4 client](#).
- [Add a local SafeCom Pull Port](#).
- [Enable printer pooling](#) and add additional SafeCom Pull Ports.

Install SafeCom G4 client

To add a local SafeCom Pull Printer you need to make a SafeCom G4 client installation on the SafeCom Mobile Print server.

1. Download the safecom_G4_xxx.exe file from the link supplied to you.
The installation must be run as administrator.
2. When the installation program is launched, click **Next**.
3. Click **Advanced installation**. Click **Next**.
4. Click **Client** and follow the instructions on the monitor.
The SafeCom Pull Port is now installed on the SafeCom Mobile Print server.
5. Next you need to either modify an existing local printer or add a new local printer.
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.

Add a local SafeCom Pull Port

1. Click **Start** and then **Printers**.
2. Click **Add a Printer**.
The Add Printer Wizard appears.
3. Click **Next**.
4. Select **Local printer** and click **Next**.
5. Select **Create a new port** and select **SafeCom Pull Port** from the list. Click **Next**.
6. Enter a unique name of your choice for the port in **Port Name**. Click **OK**.
The **Configure SafeCom Pull Port** dialog box prompts you to enter the hostname or IP address of the SafeCom Server.
7. If the SafeCom Mobile Print Server is the same as the SafeCom Server, you can enter 'localhost'.

8. As method of authentication, select **Use network logon**. Select **Default domain** from the menu if needed.
 9. Click **OK**.
The **SafeCom User Logon** dialog box appears.
 10. Enter the user logon and the password of a user that has SafeCom Administrator or Technician rights. Click **OK**.
 11. Select the manufacturer and printer model. Click **Next**.
 12. State if you want to keep the existing driver or use the new one. Click **Next**.
 13. Enter a **Printer Name** and select if this printer should be your default Windows printer. Click **Next**.
 14. Select **Do not share this printer**. Click **Next**.
 15. Select **Yes** to print a test page to verify the system. Click **Next**, and then **Finish**.
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.
 16. For now, click **OK**.
- Then you need to set up the necessary rights for the administrator on the Pull Port:
17. Open the **Printers** dialog box again, and right-click the SafeCom Pull Port you just added.
 18. Click **Properties** and then the **Security** tab.
 19. Under **Permissions for Administrators**, make sure that **Print, Manage this printer**, and **Manage documents** are checked (**Allow**).

Enable printer pooling

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

To enable printer pooling:


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. Check **Enable printer pooling**.
5. Click **Add Port** to create multiple instances of the SafeCom Pull Port.

Chapter 3

SafeCom Mobile Print installation

The following section describes how to install SafeCom Mobile Print and lists the ports that must be opened in Windows Firewall.


Install SafeCom Mobile Print

 The installation must be performed by a local administrator.

1. To install SafeCom Mobile Print, log in to the SafeCom Mobile Print server as local administrator.
2. Run the installer SafeCom Mobile Print Setup xxx.exe.
3. Follow the installation wizard and select the destination directory, start menu name, and other similar basic settings.

The default installation folder is `C:\Program Files\SafeCom\SafeCom Mobile Print`.
On Windows 64-bit, it is `C:\Program Files (x86)\SafeCom\SafeCom Mobile Print`.

4. Before finishing the setup wizard, make sure to check **Go to Services to configure SafeCom Mobile Print Web service logon account**.
5. Click **Finish**.
The **Services** dialog box opens.
6. Browse to the SafeCom Mobile Print Web service, right-click, and select **Properties**.
7. Click the **Log On** tab.
8. Select **This account** and enter the login credentials for a user with local administrative rights.

 Do not set up the Print and Data services with **This account**, because that would cause SafeCom Mobile Print to not work.

9. Click **Apply** and **OK**.
10. Now restart the SafeCom Mobile Print service and then continue with [opening the necessary ports in Windows Firewall](#).

Mobile Gateway installation

The SafeCom Mobile Print Gateway must be installed on a server which is on the same subnet as the iOS mobile devices, and is required to fully utilize SafeCom Mobile Print on such devices.

The Mobile Gateway installer is downloaded along with the SafeCom Mobile Print application. To install it, simply start SafeCom Mobile Print Gateway 4.2.0.exe, and click through the installation wizard.

If you want to install the Mobile Gateway to a different server than the one you are using for SafeCom Mobile Print, simply copy the installer to the target server, and run it from there.


 Use **Run as administrator** to run the installer.

Mobile Gateway configuration

To configure the SafeCom Mobile Print Gateway, double-click the AdminWebpage icon in Program Files or browse to <https://127.0.0.1:9444/admin/>.

The following settings can be adjusted:

- **Server host/IP:** The hostname or IP address of the Mobile Print Gateway server. If the Gateway is installed on a host different from the SafeCom Mobile Print server, this setting must be changed to reflect the SafeCom Mobile Print server's IP or hostname.
- **Server port:** The port of the SafeCom Mobile Print server. By default, this is 7290.
- **SSL port:** The secure (SSL) port of the SafeCom Mobile Print server. By default, this is 9443.
- **IPP server port:** The IPP server port. IPP server is a component of SafeCom Mobile Print server. By default, this port is 631.
- **Use SSL encrypted connection to SafeCom Mobile Print:** If enabled, all communication of the Gateway with the SafeCom Mobile Print server is encrypted.
- **Enable debug logging:** If enabled, additional information is logged to the log file. This is useful for SafeCom support in case of an issue.
- **How long to authenticate window:** This setting configures how long pending jobs which were not yet authenticated are stored on the Gateway.
- **Publish services on NICs:** If multiple network cards are installed, select the network interface on which to announce printers. Multiple interfaces can be selected/deselected using the common selection keyboard shortcuts. Changing NICs requires restart of the gateway service.

 Due to a bug in the JVM (Java virtual machine), the announcement on multiple NICs only works properly if the IPv6 option was enabled in the NIC configuration (system network configuration).

- **Enable AirPrint printer announcements:** If enabled printers retrieved from SafeCom Mobile Print server are announced for AirPrint using Apple Bonjour protocol.
- **Do Service Announcements on this IP address:** When an IP address is set here all announcements (AirPrint and gateway service) are being made for the given IP address instead of the host's local IP address. This is relevant if using multiple gateways behind a load balancer or failover cluster, where the announced IP should be the cluster or load balancers IP address.
- **Support for MDM AirPrint:** This option allows the gateway to support AirPrint printers deployed via MDM (Mobile Device Management) providers. This requires the gateway to occupy port 443 as encrypted endpoint for IPP communication, thus port 443 must not be taken already on the host system. Restart the gateway after toggling this setting.

- Wide-Area-Mobile-Print printer time-to-live settings: This option allows to change the TTL value that is used for printer announcements made through DNS-SD. Default value is 60 seconds. This setting is picked up on the next refresh of the DNS zones which happens every 2 minutes.

If the SafeCom Mobile Print server host and/or port is changed, you may check whether the new settings are correct by clicking Test Connection.



Click Save to store the new settings. The Gateway does not need to be restarted, as changed settings are picked up automatically.

You can use the Profile screen to update the administrator login password.

Using a custom keystore file

The standard keystore file (`{path}\keystore`) includes a self-signed certificate that should suffice for most use cases. With Mobile Gateway version 4.2, you can create a custom keystore file for using custom SSL/TLS certificates.

For this custom keystore file, a custom password can be defined.

i Be aware that this is a not a trivial process. If the keystore file configuration or certificates therein are not correctly set up, the gateway application or the encrypted ports may not work properly.

To create a new keystore file and configure the mobile gateway:

1. Follow this guide to create a custom keystore file:
<https://www.eclipse.org/jetty/documentation/jetty-11/operations-guide/index.html#og-keystore>
 Use this only to create the keystore file and import the certificates.
2. Make a backup of the old keystore file under the `{path}` folder.
3. Copy the new keystore file to `{path}`. The new keystore file must be named "keystore".

4. Open defaults.xml and enter the custom password of the keystore file into the entry field **KeystorePassword**.

You can enter the password in either plain text or in an encrypted form. If using plain text, ensure that the defaults.xml file is not accessible to everyone. However, the gateway application must have rights to read and write to it. You can also enter the encrypted password. The gateway comes with a tool that can encrypt the password for you:

- a. Open a command prompt and browse to the tools folder in your gateway installation.
- b. Execute the command keystore_pw_enc.bat with the keystore password as parameter.

Example:

```
C:\Program Files (x86)\SafeCom Mobile Print Gateway
\tools>keystore_pw_enc.bat foo SUCCESS
```

Your encrypted keystore phrase is: "ENC:8bC2IR8dxTE=".

- c. Enter the keystore phrase to defaults.xml into the entry field **KeystorePassword**.
5. Now save defaults.xml and re-start the gateway.

Be aware that the encryption of the keystore password is not a 100% security guarantee.

You should make sure that the defaults.xml file is properly protected on a file system basis.

Windows Firewall – ports that must be opened

If Windows Firewall is enabled, it may prevent SafeCom Mobile Print from working.

Make sure to disable the firewall or manually open the ports mentioned below.

- Web interfaces and Web Print

SafeCom Mobile Print includes web interfaces for administrator configuration and web print upload. Per default the following ports are used:

- HTTP (non-SSL): TCP port 7290
- HTTPS (SSL): TCP port 9443

- Email Print

The ports used depend on the mail server's configuration, but typical ports are:

- POP3 non-SSL: TCP port 110
- POP3 SSL: TCP port 995
- IMAP non-SSL: TCP port 143
- IMAP SSL: TCP port 993
- SMTP non-SSL: TCP port 25
- SMTP SSL: TCP port 465
- Exchange MAPI: TCP port 135 and Windows RPC protocols
- Exchange WS: HTTP TCP port 80 and HTTPS TCP port 443

- Driver Print

Printing to SafeCom Mobile Print through driver is either handled through HTTP/HTTPS IPP printing protocol or the LPD server for LPR print. By default, the following ports are used:

- IPP print: TCP port 631

- IPP print (SSL): TCP port 9443
- LPR print: TCP port 515
- Google Cloud Print
The SafeCom Mobile Print server communicates with the Google Cloud Print services hosted with Google through the following ports:
 - TCP ports 80 and 443
 - XMPP protocol TCP port 5222
- iOS and Wide Area Mobile Print
The SafeCom Mobile Print server communicates with the iOS devices and on the Wide Area Mobile Print through the following ports:
 - UDP port 5353 (iOS, multicast DNS)
 - TCP and UDP port 53

Chapter 4

Configure SafeCom Mobile Print

Log in to the SafeCom Mobile Print web interface


To configure SafeCom Mobile Print, open the SafeCom Mobile Print web interface from the shortcut either in the Windows start menu, the desktop icon, or by entering one of the following two URLs for the SafeCom Mobile Print web interface:

- `http://127.0.0.1:7290/admin`
- `https://127.0.0.1:9443/admin`

Change the IP address to that of the SafeCom Mobile Print server.

Log in using the default username and password:

- Username: admin
- Password: nimda

 It is recommended to change the default username and password. See [Manage user email addresses](#).

Add devices to SafeCom Mobile Print

The print jobs that are sent through SafeCom Mobile Print are processed on the SafeCom Mobile Print server, from where the data is sent to the SafeCom Server.

The SafeCom Mobile Print server might contain many printers that are or are not used in SafeCom Mobile Print. It is therefore necessary to add the printers to be used in SafeCom Mobile Print, through the admin interface.

Import printers automatically to import all available printers, or import only selected printers manually.

Add all devices from the server

1. Open and log in to the SafeCom Mobile Print web interface.
2. Click the **Devices** tab. If no printers have been added previously, it automatically opens the **Add New Device** page. Otherwise, click the **Add New Device** in the left menu.

Add New Device

Add printers to SafeCom Mobile Print to allow users to send prints from mobile devices to printers on the internal network.

Import All Printers from Server

New Printer Details

Printer ID:
(Leave Printer ID blank and an ID will be created automatically)

Printer Description:

Output Printer:

Send a test print to printer after adding

Advanced Driver Print

Enabling advanced driver print on a print queue, lets users print directly to the print queue using any print driver compatible with the output device, and enabling use of all advanced output features on the device.

Enable advanced driver print

Specify the printer model for users to install the correct driver:

Direct Email Print Alias

If an email forwarding account has been created for this specific printer, enter the email address associated with this printer below:

This printers direct print email address alias:

Add New Printer

3. Click **Import All Printers from Server** to automatically add all printers that exists on the SafeCom Mobile Print server.

i Imported printers can be changed or removed at any time if any adjustments are necessary later.

Add devices manually

1. On the **Add New Device** page, select the device you want to add from the menu under **New Printer Details**.
2. Enter printer details according to the following descriptions.
The fields **Printer Description** and **Printer Path** are pre-filled, but can be changed.
 - **Printer ID:** Enter the unique identifier for the printer. Can be a number, serial number, IP address, or similar.
 - **Printer Description:** Enter a user-friendly description of the device, to identify the printer to the end user.
 - **Printer Path:** The corresponding Windows print queue as installed on the SafeCom Mobile Print server.
3. Check the box **Send a test print** to send a test print job from the SafeCom Mobile Print web interface after adding the device.
This is useful to verify the configuration of the device.

General settings

In the SafeCom Mobile Print web interface, the following few settings must be configured under the General Settings tab.

- [Check for updates](#)
- [Debug logging](#)
- [Document support](#)
- [Application settings](#)

Check for updates

You can set up the SafeCom Mobile Print web interface to check periodically for new updates. This is for notification only.

Updates are not installed automatically. Instead, a side bar notification box appears if a new version is available.

To enable check for updates:

1. Click the **Settings** tab and then **General Settings** in the left menu.
2. In the **Check for updates** menu, select **Yes**.
3. Click **Save Changes**.


Debug logging

All errors and other information from SafeCom Mobile Print are logged to the central SafeCom Mobile Print log `eopapp_yyyy_mm_dd.log` located by default in `C:\Program Files\SafeCom\SafeCom Mobile Print\logs`.

On Windows 64-bit, it is in `C:\Program Files (x86)\SafeCom\SafeCom Mobile Print\logs`.

Other SafeCom Mobile Print components, such as the built-in IPP print server, also create log files in the logs directory.

1. To enable debug logging, go to the **General Settings** menu under the **Settings** tab.
2. Under **Debug Logging**, select **Yes** in the **Enable debug logging** menu.

 Do not enable debug logging in production unless necessary for troubleshooting. Debug logging can create very large log files.

3. Click **Save Changes**.

Document support

SafeCom Mobile Print includes a built-in Microsoft Office and OpenOffice conversion engine, which means that users can send Office documents to print, and SafeCom Mobile Print can convert and print those documents without relying on any outside third-party applications.

The built-in conversion engine is enabled by default, but you can select to either use the built-in engine or use Microsoft Office and OpenOffice to convert and print documents.

i Before enabling these options, Microsoft Office or OpenOffice must be installed on the server to avoid conversion errors.

Document Support
Choose document formats to support in addition to the standard PDF, images and txt formats.

Microsoft Office 2007 SP2, Microsoft Office 2010 or Microsoft Office 2013
For conversion and processing of Microsoft Office documents, choose the conversion engine you wish to use.

Use Microsoft Office 2007 SP2, Microsoft Office 2010 or Microsoft Office 2013 application installed on the SafeCom Mobile Print server. Requires Microsoft Office installed on the SafeCom Mobile Print server.

Run Document Conversion Tests

Use built-in Microsoft Office document conversion engine, no Microsoft Office installation required on the SafeCom Mobile Print server. (Requires SafeCom Mobile Print Professional license).

Refer to the SafeCom Mobile Print documentation for requirements and limitations when using the built-in conversion engine.

This feature is part of the SafeCom Mobile Print Professional license. Your evaluation license enables this feature, but to continue using this feature when the evaluation expires, make sure you purchase a Professional license.

OpenOffice 3.3 or 3.4
For conversion and processing of OpenOffice documents, choose the conversion engine you wish to use.

Use OpenOffice 3.x application installed on the SafeCom Mobile Print server. Requires OpenOffice 3.x installed on the SafeCom Mobile Print server.

Use built-in OpenOffice document conversion engine, no OpenOffice installation required on the SafeCom Mobile Print server. (Requires SafeCom Mobile Print Professional license).

Refer to the SafeCom Mobile Print documentation for requirements and limitations when using the built-in conversion engine.

This feature is part of the SafeCom Mobile Print Professional license. Your evaluation license enables this feature, but to continue using this feature when the evaluation expires, make sure you purchase a Professional license.

Application settings

Under the Settings tab in the SafeCom Mobile Print Administrator, a timeout can be adjusted to set when unreleased jobs are cleaned up and deleted.

This setting does not have any effect when Mobile Print is set up with SafeCom and with user authentication set to Direct with Authentication.

You can define how documents by default are printed with Mobile Print. Select options as required. By default, users are allowed to change the predefined print mode. However, this can also be restricted so that print jobs are always printed in, for example, duplex or black/white.

Settings can be modified as needed to regulate user access to output formats.

Language and location

SafeCom Mobile Print supports multiple languages and locale for displaying dates and numbers in local formats.

Language And Location Settings

Configure location and language settings. Make your changes below, and click Save Changes when done.

Web Interface Languages

Choose the languages that should be available in the SafeCom Mobile Print Web interfaces.

- | | | |
|--|--|---------------------------------------|
| <input type="checkbox"/> Cymraeg (CY) | <input type="checkbox"/> Dansk (DK) | <input type="checkbox"/> Deutsch (DE) |
| <input type="checkbox"/> Eesti keel (ET) | <input checked="" type="checkbox"/> English (EN) | <input type="checkbox"/> Español (ES) |
| <input type="checkbox"/> Français (FR) | <input type="checkbox"/> Italiano (IT) | <input type="checkbox"/> Magyar (HU) |
| <input type="checkbox"/> Nederlands (NL) | <input type="checkbox"/> Norsk (NO) | <input type="checkbox"/> Polski (PL) |
| <input type="checkbox"/> Portughesa (PT) | <input type="checkbox"/> Slovenščina (SL) | <input type="checkbox"/> Suomi (FI) |
| <input type="checkbox"/> Svenska (SE) | <input type="checkbox"/> Türkçe (TR) | <input type="checkbox"/> Čeština (CZ) |
| <input type="checkbox"/> Русский (RU) | <input type="checkbox"/> Български (BG) | <input type="checkbox"/> 日本語 (JP) |
| <input type="checkbox"/> 簡化字 (CN) | <input type="checkbox"/> 한국어 (KR) | |

Default Language And Email Language

Choose the default language shown in Web interfaces at first, and what language should be used in email responses sent from SafeCom Mobile Print.

- | | | |
|---------------------------------------|---|------------------------------------|
| <input type="radio"/> Cymraeg (CY) | <input type="radio"/> Dansk (DK) | <input type="radio"/> Deutsch (DE) |
| <input type="radio"/> Eesti keel (ET) | <input checked="" type="radio"/> English (EN) | <input type="radio"/> Español (ES) |
| <input type="radio"/> Français (FR) | <input type="radio"/> Italiano (IT) | <input type="radio"/> Magyar (HU) |
| <input type="radio"/> Nederlands (NL) | <input type="radio"/> Norsk (NO) | <input type="radio"/> Polski (PL) |
| <input type="radio"/> Portughesa (PT) | <input type="radio"/> Slovenščina (SL) | <input type="radio"/> Suomi (FI) |
| <input type="radio"/> Svenska (SE) | <input type="radio"/> Türkçe (TR) | <input type="radio"/> Čeština (CZ) |
| <input type="radio"/> Русский (RU) | <input type="radio"/> Български (BG) | <input type="radio"/> 日本語 (JP) |
| <input type="radio"/> 簡化字 (CN) | <input type="radio"/> 한국어 (KR) | |

Locale

Locale determines currency, number and date formatting.

English (US)

Select language and locale:

1. Click the **Settings** tab in the SafeCom Mobile Print web interface, then click **Language and Location**.
2. Select the languages that should be available for users.
Selected languages appear as flags in the top right corner of the web interface.
3. Under **Default Language and Email Language**, select the default language, which is the language used in emails sent from SafeCom Mobile Print.
4. Under **Locale**, select the locale, which determines how numbers and dates are formatted.
5. Click **Save Changes**.

Printing and security

On the Printing and Security web page, the primary settings that determine the overall printing behavior of SafeCom Mobile Print must be set.

i To use the Ready to Print function on your mobile device, use the device selection option in Web Print and select Privacy with authentication as Print Behavior. On the Mobile Print Settings page, select **Enable strict mobile device authentication** and **Enable job release**.

Mobile Print Settings

Configure settings for prints sent from mobile devices. Make your changes below, and click Save Changes when done.

To enable native printing from supported mobile devices, the SafeCom Mobile Print Mobile Gateway must be installed and configured. See documentation for details.

Mobile Print Settings

Customize the name of the mobile printer, as it will appear on mobile clients that support printer naming, for example "Secure Printer", "WiFi printer", "Student Printer" or similar.

Printer name:

(Changing the printer name may require a restart of the mobile gateway to force the change to clients)

Mobile Print Authentication

Your current configuration is: **Privacy with Authentication**. [Click here to change](#).

In this configuration, users must authenticate once when printing from their mobile device.

Enable strict mobile device authentication

When enabling strict mobile device authentication:

- Users must authenticate when their mobile device uses a new IP address
- Users have the ability to logout using the SafeCom Mobile Print mobile apps
- Users can be forced to re-authenticate after a set period of time (useful for shared iPads or similar)

Users must relogin on mobile devices after minutes.

(Default value is 43200 minutes (30 days). Minimum is 5 minutes.)

Mobile Printers

Customize how users can print in this mode:

- Allow authenticated users to send print jobs from mobile devices, print jobs are held in SafeCom Mobile Print until release
- Allow authenticated users to send print jobs from mobile devices, print jobs are held in SafeCom Mobile Print until release and also allow authenticated users to send print jobs directly to devices
- Allow authenticated users to send print jobs directly to devices

Mobile App Settings

Customize settings that apply to the SafeCom Mobile Print Mobile Apps

Enable job release

Allow users to release print jobs held in SafeCom Mobile Print, using the Mobile Apps (only relevant if SafeCom Mobile Print is configured for a "privacy" mode where jobs are held in SafeCom Mobile Print until release)

Printing And Security

Configure primary printing behavior in SafeCom Mobile Print. Make your changes below, and click **Save Changes** when done.

Please refer to the SafeCom Mobile Print documentation for detailed explanation of the different modes.

Print Behavior

Choose how users print and SafeCom Mobile Print should behave when receiving and processing print jobs.

Privacy Print

With Privacy print modes, print jobs are held in SafeCom Mobile Print until release.

- Privacy with Release Code** – What this means?
 - Web print – User sees release code on screen
 - Driver print – User supplies release code in printer configuration
 - Email Print – User gets email reply with release code
 - Mobile Print – User use SafeCom Mobile Print mobile App to obtain release code
- Privacy with Authentication** – What this means?
 - Web print – Users must logon Web portal to upload print jobs
 - Driver print – Users supplies authentication information in printer configuration
 - Email print – Users must logon and associate email address with username
 - Mobile Print – Users must authenticate when they print from mobile device

Direct Print

Print jobs are released immediately to the selected print queue below. Use this option if an external secure printing solution is used or if print jobs should be printed directly immediately.

Print queue for direct print:

- Direct with No Authentication** – What this means?
 - Web print – Any user can access the Web print portal and upload documents to print
 - Driver print – All users can print via driver. Prints are released directly to selected queue
 - Email Print – All email print jobs are directly released to specific queue
 - Mobile Print – All users are allowed to print from a mobile device.
- Direct with Authentication** – What this means?
 - Web print – Users must logon Web portal to upload print jobs.
 - Driver print – Users supplies authentication information in printer configuration
 - Email print – Users must logon and associate email address with username
 - Mobile Print – Users must authenticate when they print from mobile device

To set up the authentication mode in SafeCom Mobile Print:

1. Click the **Settings** tab, then click **Printing and Security** in the left menu.
2. Under **Direct Print**, select the **SafeCom Pull Print** port.
3. Select **Direct with Authentication** if it is not already selected.
4. Click **Save Changes**.

User authentication

When **Printing and security** is set to **Direct with Authentication**, then the actual authentication method, how user logins are validated, is configured in the User Authentication web page.

The authentication method can be set to:

- No authentication: No validation at login is performed.
- Authentication through LDAP: See [LDAP authentication](#) to set up LDAP authentication.

LDAP authentication

Enter the details for the LDAP authentication server, including a test username and the password of a valid user account in the LDAP, then click Save and Test to verify the configuration.

If the test authentication fails, an error message is shown. See common LDAP error codes and typical causes in [LDAP troubleshooting](#).

A highly recommended tool for identifying proper LDAP settings to use is LDAP Browser 2.6, which can be downloaded for free at [LDAP Administrator](#).

To enable guest printing ([SafeCom authentication](#)), you must check the **Enable guest user account creation** option, then the **Authentication through SafeCom** option, and ensure that the specified server credentials correspond to the credentials used for accessing your SafeCom server.


Email and Google Cloud Print authentication

When a user sends a print job to SafeCom Mobile Print through an email address unknown to SafeCom, the user receives an email that prompts him/her to use their Windows credentials to register his/her email address.

No registration is necessary if users are known in SafeCom Mobile Print, either because their email address has been manually added or imported from a CSV, or if LDAP email address lookup is enabled. Alternatively, non-registered users can use guest accounts, if the relevant settings are met.

Set up Email authentication under Email and Google Cloud Print Authentication

Select the **Search LDAP for email address to lookup username** check box to let Mobile Print automatically retrieve the email addresses of internal users as needed. Be sure to have [LDAP authentication](#) configured.

 Exchange MAPI does not always share the complete email sender address (user@company.com). This will cause Email Authentication in Mobile Print to fail. To work around this, configure LDAP authentication and select **Search LDAP for email address to lookup username**.

Set up handling of Unknown Senders under Email and Google Cloud Print Authentication

Select the **Search LDAP for email address to lookup username** check box to let Mobile Print automatically retrieve the email addresses of internal users as needed. Be sure to have [LDAP authentication](#) configured.

- Select the **Unknown senders are guests, create guest account in and send welcome email with the created username and password** radio button to allow guest printing.

- Select the **Allow user self registration** radio button if you want to allow users to create their own accounts.

SafeCom authentication

i Steps 1-6 are only required if you installed the SafeCom Mobile Print components to separate servers. If you installed SafeCom Mobile Print on a dedicated server, you only need to perform steps 7-8 below.

1. From Windows services, stop the Mobile Print Web Service.
2. In the root directory of the Mobile Print installation, open eop.xml in a text editor such as Notepad.
3. Find the entry <edition> and change it to <edition>waccount</edition>.
4. Find entry <editionacct> and change it to <editionacct>safecom</editionacct>.
5. Save the eop.xml file.
6. Start the SafeCom Mobile Print Web Service.
7. Log in to SafeCom Mobile Print and go to **Settings > User Authentication**.
8. Under the **Authentication through Safecom** part, enter the administrator credentials you use to access your SafeCom server, and provide the server IP and hostname of your SafeCom server.

For user credentials, you need either user logon and password or user logon and PIN code.

i Under **Additional Options**, you can specify a timespan for created guest user accounts. When the timespan specified here elapses for a given guest account, said account is deleted.

SafeCom Guest Users Self-Signup

When a user does not have an account that is accessible through the LDAP authentication server, and still needs to use the Mobile Print, you can set guest user access. To set up this access, you have to perform configuration steps both in the SafeCom Administrator and the SafeCom Mobile Print.

1. Log in to SafeCom Administrator, and ensure that the **Create Users at First Print** option is checked under the **User** tab. You must also configure the **SMTP server address** properly.
2. On the devices you want to use with Guest Printing, ensure that the **Login method** is set to either **ID code** or **Card and ID code**.
3. Log in to SafeCom Mobile Print as administrator, and open **Settings > User Authentication**.

i Under **User Authentication > Additional Options**, you can specify a timespan for created guest user accounts. When the timespan specified for a guest account expires, said account is deleted.

4. Select the **Search LDAP for email address to lookup username** check box to let Mobile Print automatically retrieve the email addresses of internal users as needed. Be sure to have [LDAP authentication](#) configured.
5. Select the **Unknown senders are guests, create guest account in and send welcome email with the created username and password** check box to allow guest printing.

6. Select the **Enable guest user account creation** check box.
7. Select the **Authentication through SafeCom** option under Authentication method above, and provide the credentials for your SafeCom server there.

You can use the check boxes under **Optional Settings** to configure additional security measures.

8. Select the **Send a welcome email to the user with the created username and password** check box.

Guest users receive a welcome email with login, containing a 6-digit and a 4-digit credential, which are used as SafeCom User Logon, SafeCom ID Code (the 6-digit code), and SafeCom PIN code (the 4-digit code). Thus, guest user credentials can be used in ID Code with PIN authentication-based login scenarios. Self-card registration is not possible with guest users.

User web portal configuration

The User Web Portal is where users can upload documents to print through Web Print (see [Upload document for print](#)), as well as an overview of their print jobs awaiting collection and if set, the balance of their SafeCom accounts.


The User Web portal is accessible for HTTPS/SSL on:

- <http://127.0.0.1:7290>
- <https://127.0.0.1:9443>


Change the IP address to that of the SafeCom Mobile Print server.

To configure the User Web Portal:


1. Open and log in to SafeCom Mobile Print web interface.
2. Click the **Settings** tab and then **Web Portal** in the left menu.
3. Under **External Web Portal Address**, the URL address for the **User Web Portal** must be specified.

 Since the User Web Portal may be accessed by users from outside of the local server, a URL address must be an address that is accessible to users externally.

4. If an SSL certificate has been successfully installed and configured, select **Redirect non-SSL users to HTTPS/SSL** to automatically redirect users that access the Web portal with non-SSL HTTP to HTTPS/SSL.

 Before enabling this option, be sure that HTTPS/SSL is fully working.

5. Under **Web Portal Logo**, click **Browse** to find and upload a new logo on the user web interfaces.

 The logo can either be a GIF, JPG, or PNG file. There are no fixed size restrictions, but the guideline is to not exceed 320x80.

The logo replaces the SafeCom logo.

6. Check the **Reset logo to default logo** at any time to clear a custom logo and revert to the SafeCom logo.
7. The My Print Jobs screen is the main page that users see in the SafeCom web portal. Customize what is displayed in this page by enabling or disabling the following options:
 - **Show printer selection:** Allow users to select a device to print to from the My Print Jobs page.
 - **Show print history:** Allow users to see their most recent print job activity in the My Print Jobs page.
8. Click **Save Changes**.
9. To customize the text shown on the **User Web Portal** login page with a welcome message or special login instructions, enter any text or HTML in the **Custom login text** field.

Example:

This login text results in the following login page:



10. After making the necessary changes, click **Save Changes**.

Web Portal single sign-on

It is possible to implement your own authentication procedure so users are authenticated and registered to SafeCom Mobile Print without having to provide their login credentials. It is also possible to have both single sign on authentication and normal login authentication.

When an authenticated user is registered in SafeCom Mobile Print, they are automatically logged on and have access to standard functionality. When a user is finished with their session, they can either log out or close the browser window.

You can implement user authentication in any way required, and register users to SafeCom Mobile Print using either HTTP POST or a HTTP header redirection. Two variables are included, the username and an MD5 check hash value consisting of a username and a pass key known only to the administrator and SafeCom Mobile Print.

Authentication example:

```
Username = test
SSO Pass Key = password
check = md5("testpassword")
```

If the user is transferred to SafeCom Mobile Print using a web form:

```
<form action="https://servername/ssologin.cfm" method="post">
<input type="hidden" name="username" value="test">
<input type="hidden" name="check" value="e16b2ab8d12314bf4efbd6203906ea6c">
<input name="submit" type="submit" value="continue" />
</form>
```

If the user is transferred to SafeCom Mobile Print using HTTP header, redirect them to `https://servername/ssologin.cfm?username=test&check=e16b2ab8d12314bf4efbd6203906ea6c`.

i Due to browsers caching URLs, you should use a "301 permanently moved" status code redirection for the HTTP header redirection and no traditional HTML anchors. For example:

```
<a href="URL">click here</a>
```

Modify language text strings

With the SafeCom Mobile installation language files, containing the raw text for the user web portal, are included and these can manually be edited. This means that any text appearing in SafeCom Mobile Print can be changed.

The language files are by default located in `C:/program files(x86)/SafeCom/Kofax SafeCom Mobile Print/languagefiles`.

Files are named `public_` for the user web portal interface and the language abbreviation `_en` for English `_se` for Swedish and so on.

To edit, for example, the English text strings in the user web portal:

1. Open `public_en.xml` in an editor such as Notepad, and edit the text.

Both plain text and HTML tags are possible.

2. As an example, to insert a link in the Advanced Driver Print instructions for Windows 7 in english, edit the following part:

Example: `<cfcase value="dp_win7_7b">Choose the driver for the printer model specified below or click Have Disk.. to install driver, and click OK.</cfcase>`

This part should be edited as follows:

```
<cfcase value="dp_win7_7b">Choose the driver for the printer
model specified below or click <strong>Have Disk..</strong>
to install driver, and click <strong>OK</strong>. To download
the driver <a href="http://www.acme.com/driver.zip">click
here</a>.</cfcase>
```

This would change the appearance in the SafeCom Mobile Print web interface to:

7. Choose the driver for the printer model specified below or click **Have Disk..** to install driver, and click **OK**. To download the driver [click here](#)

i Language files are provided as is. It is recommended to back up the language files prior to editing. Kofax SafeCom provides no assistance or support relating to changing of language files. Any changes done to language files will automatically be overwritten by any SafeCom Mobile Print update.

Change default Web ports from 7290 and 9443

The user web interfaces in SafeCom Mobile Print run on TCP ports 7290 (http) and 9443 (https) by default. These can be changed to common HTTP ports 80 and HTTPS port 443 if no other web server software is running on the server.

i Before changing default ports, ensure there are no port conflicts with other software running on the same server.

Change the default HTTP port

1. Open the file `C:\Program Files\SafeCom\SafeCom Mobile Print\etc\jetty.xml`.
2. Find the line: `<Set name="port"><SystemProperty name="jetty.port" default="7290"/></Set>`.
3. Change 7290 to the port of your choice and save the file.
4. Open the file `C:\Program Files\SafeCom\SafeCom Mobile Print\etc\jetty-ssl.xml`.
5. Find the line: `<eopapiendpoint>http://127.0.0.1:7290/api/</eopapiendpoint>`.
6. Change 7290 to the same port as used in jetty.xml above.
7. Restart the SafeCom Mobile Print Web service.

Change the default HTTPS port

1. Open the file `C:\Program Files\SafeCom\SafeCom Mobile Print\etc\jetty-ssl.xml`.
2. Find the line: `<Set name="Port">9443</Set>`.
3. Change 9443 to the port of your choice and save the file.
4. Restart the SafeCom Mobile Print Web service.

Web print configuration

Web Print is the feature in the User Web Portal that allows users to upload a document to print or print by entering a Web URL address.

To configure SafeCom Web Print:

1. Click the Settings tab in the SafeCom Mobile Print web interface.
2. Select **Web print** in the left menu.

The web print feature is enabled by default allowing users to use web print.

- Clear **Web Print enabled** to disable the functionality for the users.
- If **Web Print enabled** is selected, it is further possible to select **Web URL address print enabled**, allowing users to print a web page.

- When users enter a Web URL address to print, SafeCom Mobile Print connects to the Internet to retrieve the contents of the entered address and convert to print data.
3. If SafeCom Mobile Print must go through a proxy server to reach the Internet, enter the following proxy server details under **Web Proxy**:
 - Proxy server
 - Proxy port
 - Proxy username
 - Proxy password
 4. Click **Save Changes**.

Driver print configuration

When configuring driver print, users can print directly from within their programs and applications, on Windows, Mac, and Linux across the network or Internet to the local SafeCom Mobile Print server.


The network configuration determines where users can print from. If the network is open for communication from the outside to the IPP print server in SafeCom Mobile Print on the ports used (default TCP 631), then users can print. Usage examples include students at a university using a public Wi-Fi connection, or corporate employees printing from satellite offices in remote locations, or users printing from home. User must add the printer.

The printing protocol used in Driver Print to SafeCom Mobile Print is IPP through HTTP (default port 631) or HTTPS/SSL (default port 9443).

The default address for Driver Print is `http://127.0.0.1:631` or `https://localhost:9443`. However, since this is a local address, it can only be used on the local server. It is necessary to enter an address that is accessible from outside the server, such as: `http://print.companyname.com:631`

Before using HTTPS/SSL, make sure a valid SSL certificate is created for the web server by a certified authority or IPP printing will fail for users using Windows.

Users on Windows clients will see the name of the printer as specified in the Driver Print configuration.

 Select a descriptive, easily identifiable name for the printer, such as Secure Printer, Student Printer, or similar.

To configure the SafeCom Driver Print:

1. Click the **Settings** tab in the SafeCom Mobile Print web interface.
2. Select **Driver Print** in the left menu.
3. Check **Driver print enabled** and then **Show option "Simple Direct" driver print** to enable driver print for SafeCom Mobile Print.

Simple Direct driver print allows users to create a print queue on their local machine that sends print jobs through SafeCom Mobile Print and to the output print queue of their choice. This Driver Print option is enabled by default.

4. Make sure the **Advanced driver print** option is cleared.

Advanced Driver Print

With advanced print, users select a printer driver that is compatible with the printers they want to print to, which will make it possible to use the advanced features of the output printer, such as binding and stapling. SafeCom Mobile Print does not convert or modify the print data stream when sending jobs through Advanced Driver Print. It is forwarded as is to the destination print queue, when released.

1. Click the **Settings** tab in the SafeCom Mobile Print web interface.
2. Select **Driver Print** in the left menu.
3. Check **Driver print enabled** and then check all three options.
4. Log in to the SafeCom Mobile Web Portal and select **Driver Print**.
5. Select the OS you want to use, then select **Advanced (3)**.
6. Select the destination printer from the displayed list, then follow the on-screen instructions.
7. Ensure that the printer address contains the /IPP/r parameters when displayed.
8. Follow the on-screen instructions to the end to configure Advanced Driver Print.

LPD server

SafeCom Mobile Print includes an LPD server which makes it simple to print from workstations in network environments, such as business computers or workstations. LPR/LPD is a printing protocol commonly used in TCP/IP networks and is very simple to implement and widely supported on all clients.

To print to the SafeCom Mobile Print server, first enable the LPD server under the Driver Print settings in SafeCom Mobile Print Admin, and then add a printer on a client using standard TCP/IP port with LPR protocol.

The Printer Name or IP Address is the IP or hostname of the SafeCom Mobile Print LPD server.


For LPR Queue name, use either the Printer ID or the External ID in parentheses under a printer in SafeCom Mobile Print. Ensure that LPR Byte counting Enabled is checked.

Select a printer driver which is compatible with the output device. Print jobs sent to the LPD server are not modified, the original print data (Postscript, PCL and so forth) is sent untouched to the output queue, which means that any output settings selected in the driver, duplex, binding and so on, are also sent to output device.

Email print configuration

With SafeCom Mobile Print, users can send emails from their mobile devices or computers to the SafeCom Mobile Print server. SafeCom Mobile Print then retrieves and processes those emails and makes them available for the users to collect at any network printer.

The SafeCom Mobile Print server supports POP3 and IMAP4 email accounts, either with or without SSL encryption. There are no limitations to the mail servers supported if they adhere to normal POP3 or IMAP4 mail specifications.

 Email Print is not enabled per default. Mail server settings, both incoming and outgoing, must be set up correctly. See [Configure incoming mail](#) and [Configure outgoing mail](#).

Enable Email Print

1. Open and log in to SafeCom Mobile Print web interface.
2. Click the **Settings** tab and then **Email Print** in the left menu.
3. Under **Email Print**, select **Email print enabled**.
4. Continue configuring the incoming and outgoing mail.

Configure incoming mail

Use Email Print Server Settings to configure the connection between SafeCom Mobile Print and your email server.

- **Email Print Address:** Type in the email address to which users send their print jobs. Default is `print@safecom.eu`.
- **Incoming Mail Server Settings:** From the "Mail server type" list, select appropriate mail server type depending on protocol and encryption. In the "Mail server address" field, type in the mail server address details. If you select Exchange Web Services from the list, you must type in the fully accessible URL to the Exchange web interface, for example `https://myServer.myDomain.com`.
- **Incoming Mail Account Settings:** Enter the user login details for the account from which to retrieve email. **Check Mail Frequency:** Select how frequently SafeCom Mobile Print should check for new emails. The default is every 10 seconds, but if the mail server is not on the same internal network, a higher interval, such as every 30 seconds, is recommended.
- **Test Incoming Mail Settings:** Check to test the entered email settings to ensure that SafeCom Mobile Print can connect successfully. When you click Save Changes, SafeCom Mobile Print makes a connection test.

When you see the following message, the incoming mail settings are correct.

"Changes saved successfully. Incoming mail test completed successfully. Your settings appear to be correct."

Email print settings

If the email message itself is a print job, check **Create print job of email message body**. Now users can print the attachments to the email as well as the email body text.

Check **Send email response for unsupported formats** for the system to notify users by email when file users have sent are in an unsupported format.

Adjust in the list the size of image files to be ignored when printing. This will allow you skip printing for example company logos in email signatures.

Email print permissions

Emails can only be sent from approved domains. Any email sent from a domain not listed is automatically discarded. Enter the domain names in the "Allow only print jobs from the following domains" field. If there is more than one domain, separate each domain name by a comma.

Email Print Permissions

Allow only print jobs from the following domains:

 (separate multiple domains with comma. Leave blank to allow all domain names.)

Do not allow print jobs from the following domains:

 (separate multiple domains with comma. Leave blank to allow all domain names.)

The above domain restriction list will apply for all email print jobs regardless of settings in [Printing and Security](#).

Configure outgoing mail

SafeCom Mobile Print must be able to send outgoing email in the following cases:

- A print job is in a format that is not supported.
- The size of an email is too large.
- A user needs to register.

Click the **Settings** tab and then **Outgoing Mail**.

- **Outgoing Mail Server:** Enter the mail server's SMTP settings for outgoing email, including relevant ports and security protocols as needed for the SMTP mail server.
- **Customer Information:** Enter the company name and the sender email address. These are the details that appear for the sender on the email.
- **Send Test Email:** Test the settings by entering an email address to receive a test email, and check the box saying **Send test email**. It is recommended to select an external test email address, to confirm that SafeCom Mobile Print can send emails to all users. It is important to use a different address than the Email Print address; otherwise, you risk creating an infinite email print loop.

Click **Save Changes**, and a test email is sent to confirm that SafeCom Mobile Print can successfully send emails to end users.

i If SafeCom Mobile Print says email was sent successfully, but no email is received, check the file `C:\Program Files\SafeCom Mobile Print\temp\cfmail\mail.log` (or an alternate installation directory) for errors such as:

```
02/10/11 13:29.27: MailOutFail:
To=john.smith@company.com; From=Company
<support@company.com>; Subject=Outgoing test mail from
SafeCom Mobile Print; Server=mail.company.com;25; Size=515
bytes:javax.mail.MessagingException: Could not connect to SMTP
host: mail.company.com, port: 25; nested exception is:
java.net.ConnectException: Connection timed out: connect
```


With the above error message in mail.log, SafeCom could not successfully deliver the test email to the mail server due to lack of connection. Make sure that no firewalls are interrupting the connection.

Configure HTML zoom rendering

You can modify the zoom level of HTML documents, ensuring the font size is set to your preference. The option is only available on Windows platforms.

1. Stop the SafeCom Mobile Print Web service.
2. From the installation directory, open eop.xml in a text editor such as Notepad.
3. Within the <settings></settings> section, insert the following if not present:

```
<converthtmlzoom>1</converthtmlzoom>
```


"1" is the default zoom factor. Adjust the zoom factor as needed, depending on the font size you want.

4. Save the file and start the SafeCom Mobile Print Web service.

HTML emails print with the adjusted font size.

Printing HTML emails with inline images

This feature allows you to process and print html emails with embedded images rendered properly inline.

 This is an experimental feature. Deploying it in production environments without thorough testing and validation is not advised.

1. Stop the SafeCom Mobile Print Web service.
2. From the installation directory, open eop.xml in a text editor such as Notepad.
3. Within the <settings></settings> section, insert the following if not present:

```
<mailprocessinlineimages>>true</mailprocessinlineimages>
```

Here, "true" means that inline images are processed and printed.

Inversely, "false" would mean that inline images are not printed.

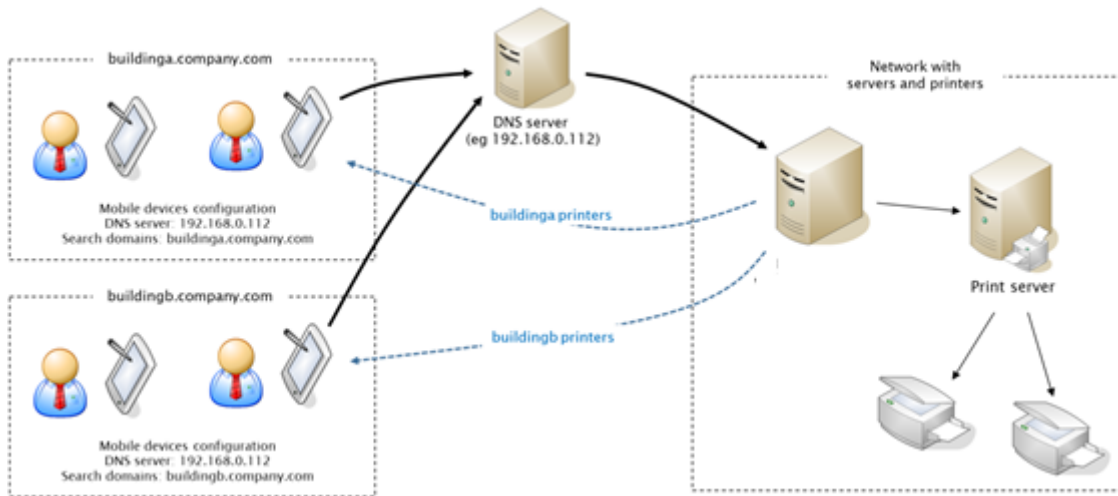
4. Save the file and start the SafeCom Mobile Print Web service.

HTML emails with embedded images are rendered with the images inline.

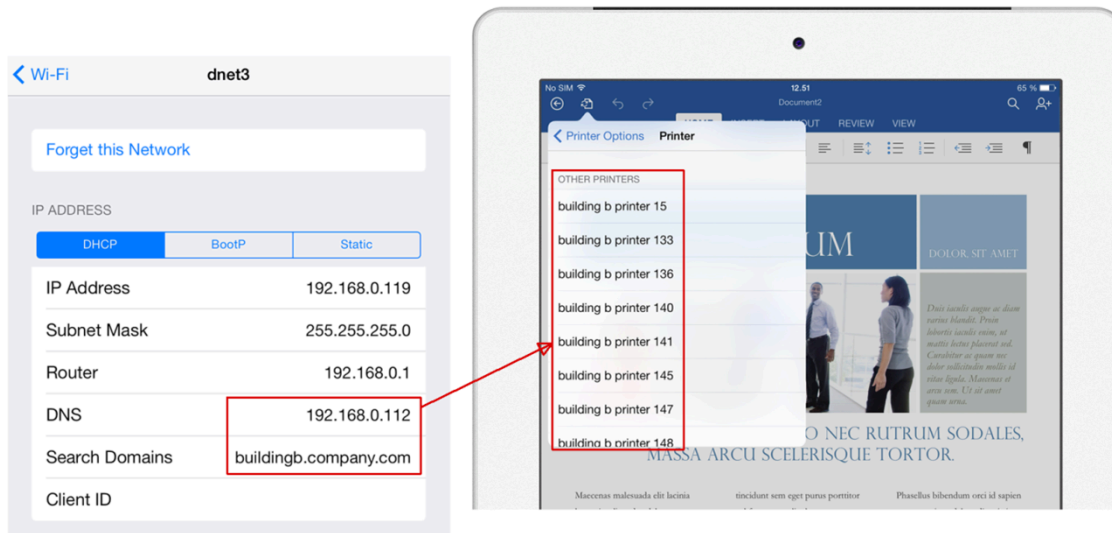
Wide Area Mobile Print

Wide Area Mobile Print is a highly flexible and powerful alternative to the Apple multicast DNS Bonjour method of announcing printers to Apple iOS devices.

Wide Area Mobile Print uses Unicast DNS-SD, and announcing available printers in SafeCom Mobile Print to Apple iOS devices can be achieved with extreme ease using the Wide Area Mobile Print feature combined with simple standard DNS records created on the DNS server. With Wide Area Mobile Print, AirPrint can be enabled across large and complex networks.



In the example above, two subdomains have been created, one for each building, Building A and Building B. Mobile devices in each network, query the DNS server, which forwards DNS requests to the SafeCom Mobile Print Gateway. SafeCom Mobile Print Gateway responds with relevant printers for the sub domains available to specific mobile device.



An Apple iOS device with buildingb sub domain specified, see only those printers in that sub domain. Multiple sub domains can be specified as needed.

The following assumes that SafeCom Mobile Print has been configured and one or more printers have been added to SafeCom Mobile Print.

Configuration overview

The Wide Area Mobile Print configuration involves the following overall steps:

1. Create one or more Wide Area Mobile Print sub domains in SafeCom Mobile Print Admin.

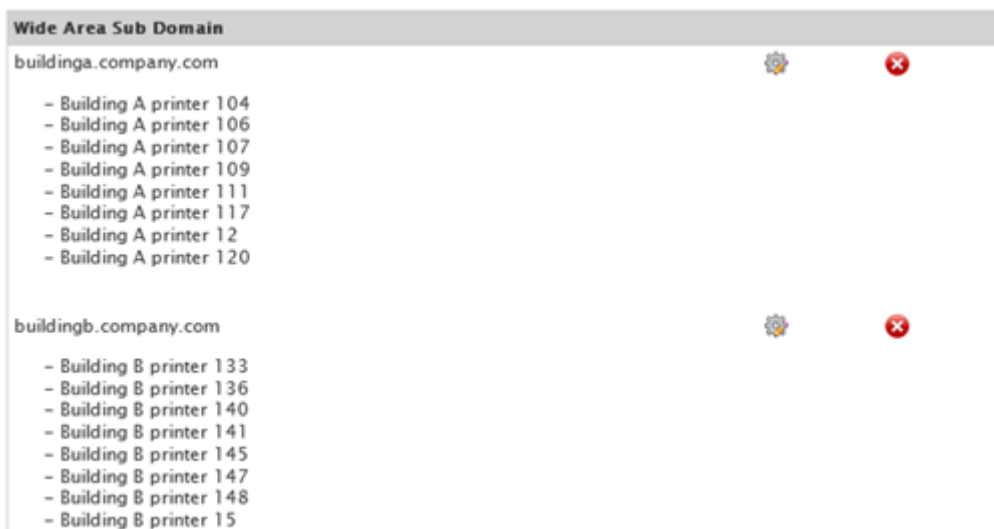
2. Install and configure the SafeCom Mobile Print Gateway.
3. Configure the network DNS server.
4. Set search domain on mobile devices.

Create Wide Area Mobile Print sub domains

Start in the SafeCom Mobile Print administrator interface and the section Wide Area Mobile Print, and create one or more sub domains for the printers.

Multiple sub domains can be created, to separate access to printers, for example:

- By location (one sub domain per building, campus, city, department)
- By user access level (one sub domain for teachers, another for students, or one sub domain for employees, another sub domain for guests)



In this example, two sub domains have been created, one for each building.

There are no limitations in SafeCom Mobile Print as to how the separation can be configured, as it all depends on which of the sub domains created in SafeCom Mobile Print that a particular mobile device has access to.

Kofax recommends creating a single subdomain containing all printers for Wide Area Mobile Print to simplify the setup of the search domain.

Note that the Unicast DNS-SD used by Wide Area Mobile Print does not work with .local domain name. For more information, refer to <https://support.apple.com/en-us/HT204684>.

Configure SafeCom Mobile Print Gateway

Install SafeCom Mobile Print Gateway, either on the SafeCom Mobile Print server or on its own server.

Mobile devices will communicate with the Mobile Gateway and not directly to the SafeCom Mobile Print server, so the gateway can be placed in a DMZ zone or similar, to further separate mobile devices from the secure printing infrastructure.

With SafeCom Mobile Print Gateway installed, open the gateway admin web interface, configure the server connection details, test the connection, then save.

Connection was successful

Configuration

Main server host/IP:	<input type="text" value="192.168.0.116"/>
Main server port:	<input type="text" value="7290"/>
Main server SSL port:	<input type="text" value="9443"/>
IPP server port:	<input type="text" value="631"/>
Use SSL encrypted connection to main server:	<input type="checkbox"/>
Enable debug logging:	<input checked="" type="checkbox"/>
How long to authenticate window (minutes):	<input type="text" value="60"/>
Publish services on NICs (select multiple):	<input type="checkbox" value="Intel(R) PRO/1000 MT Network Connection - 192.168.0.109"/>

Configure DNS server

For each created Wide Area Mobile Print sub domain, the DNS requests for those sub domains, should be delegated to the SafeCom Mobile Print Gateway, so SafeCom Mobile Print can respond with relevant printer details for the sub domains.

For more information about Zone Delegation, refer to the following articles:

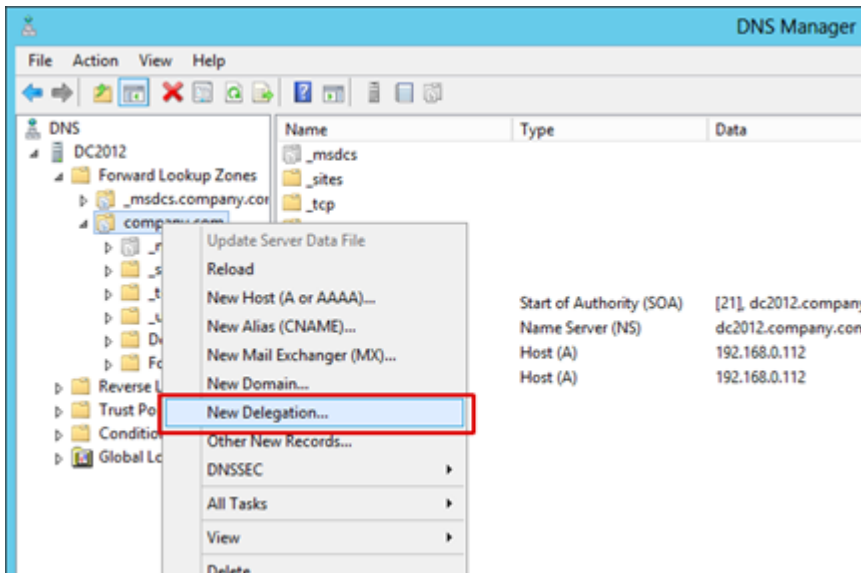
- [DNS zone](#)
- [Understanding Zone Delegation](#)
- [Create a Zone Delegation](#)

For configurations of the zone delegation, see the two sections below about Microsoft Windows DNS or BIND (Mac OSX or Linux).

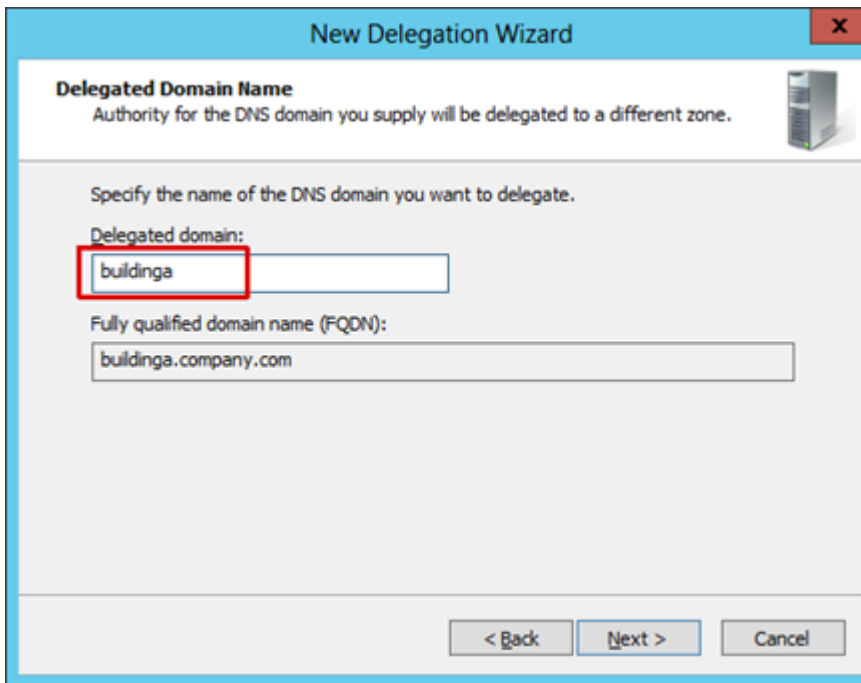
Configure Windows DNS

To configure zone delegation for the created Wide Area Mobile Print sub domains on Windows DNS, open Windows DNS on the DNS server that mobile devices use.

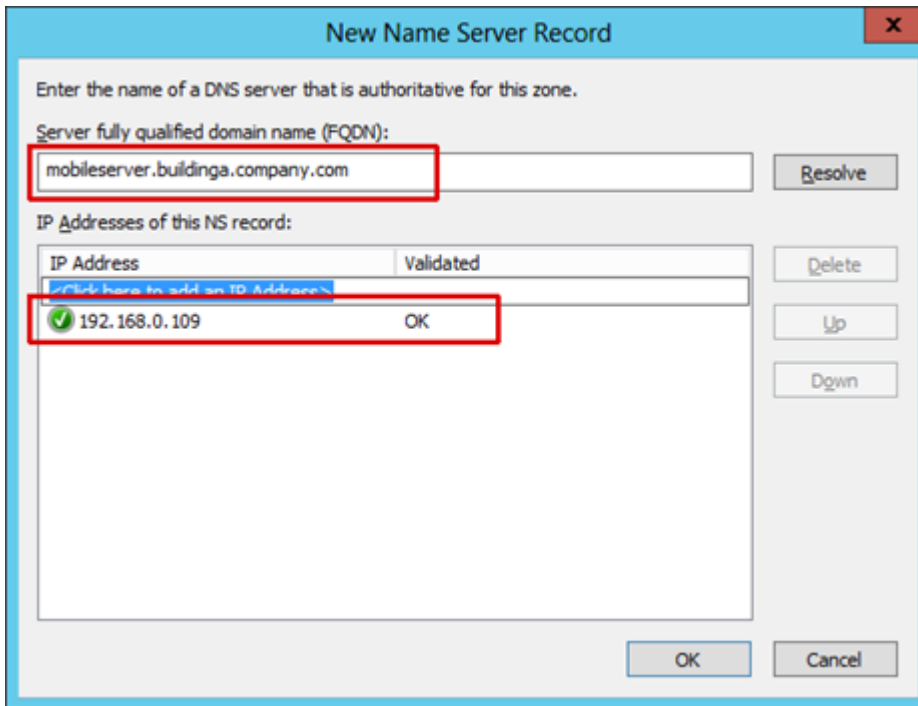
1. Right-click the domain and select **New Delegation**.



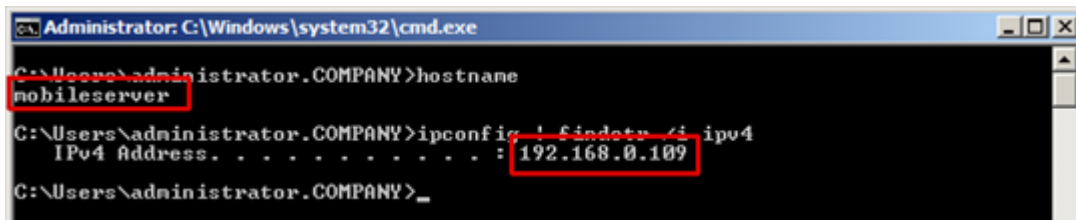
2. Enter the sub domain name as created in SafeCom Mobile Print.



3. Select **Add** to add the name server.
4. Enter the **server name/hostname** of the SafeCom Mobile Print Gateway server followed by the Wide Area Mobile Print sub domain and Active Directory domain, and then enter the **IP address** of the SafeCom Mobile Print Gateway server.



- In this example, the hostname of the SafeCom Mobile Print Gateway server is "mobileserver" and its IP address is 192.168.0.109.



- Repeat for each created sub domain.

Configure BIND

Configure zone delegation for the created Wide Area Mobile Print sub domains on BIND running on Mac OSX or Linux, by adding the sub domains to the domains master zone file.

In this example, the sub domains are added to the BIND master zone file for the domain "company.com".

```

;
; Zone file for company.com
;
$TTL 360
@      IN      SOA      ns.company.com. root.company.com. (
                201404011      ; serial, todays date + todays serial #
                8H              ; refresh, seconds
                2H              ; retry, seconds
                4W              ; expire, seconds
                1D )            ; minimum, seconds

```

```

ns                 NS      ns           ; Inet Address of name server
ns                 A       192.168.0.139

; Delegation for Wide Area Mobile Print sub domains
$ORIGIN buildinga.company.com.
@                 IN      NS      mobileserverserver.buildinga.company.com.
mobileserverserver IN      A       192.168.0.109

$ORIGIN buildingb.company.com.
@                 IN      NS      mobileserverserver.buildingb.company.com.
mobileserverserver IN      A       192.168.0.109

$ORIGIN buildingc.company.com.
@                 IN      NS      mobileserverserver.buildingc.company.com.
mobileserverserver IN      A       192.168.0.109

```

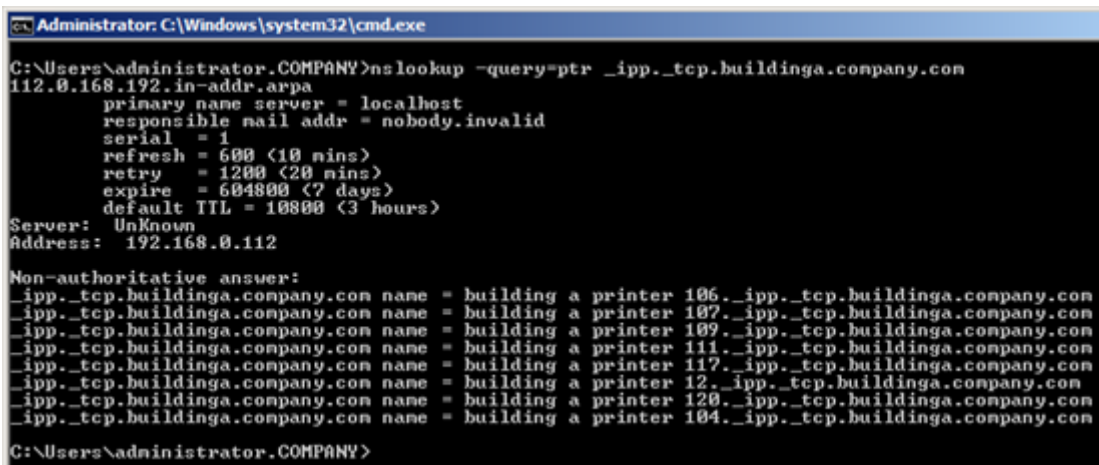
Now any DNS requests for one of the sub domains to the primary DNS server will be forwarded to the SafeCom Mobile Print Gateway server.

Verify DNS configuration

To confirm the proper DNS configuration with either Windows DNS or BIND on Mac OSX or Linux, run the nslookup command for each of the sub domains:

```
nslookup -query=ptr _ipp._tcp.buildinga.company.com
```

If successfully configured, this will return a list of the printers in the sub domain as configured in SafeCom Mobile Print.



```

Administrator: C:\Windows\system32\cmd.exe
C:\Users\administrator.COMPANY>nslookup -query=ptr _ipp._tcp.buildinga.company.com
112.0.168.192.in-addr.arpa
primary name server = localhost
responsible mail addr = nobody.invalid
serial = 1
refresh = 600 (10 mins)
retry = 1200 (20 mins)
expire = 604800 (7 days)
default TTL = 10800 (3 hours)
Server: Unknown
Address: 192.168.0.112

Non-authoritative answer:
_ipp._tcp.buildinga.company.com name = building a printer 106._ipp._tcp.buildinga.company.com
_ipp._tcp.buildinga.company.com name = building a printer 107._ipp._tcp.buildinga.company.com
_ipp._tcp.buildinga.company.com name = building a printer 109._ipp._tcp.buildinga.company.com
_ipp._tcp.buildinga.company.com name = building a printer 111._ipp._tcp.buildinga.company.com
_ipp._tcp.buildinga.company.com name = building a printer 117._ipp._tcp.buildinga.company.com
_ipp._tcp.buildinga.company.com name = building a printer 12._ipp._tcp.buildinga.company.com
_ipp._tcp.buildinga.company.com name = building a printer 120._ipp._tcp.buildinga.company.com
_ipp._tcp.buildinga.company.com name = building a printer 104._ipp._tcp.buildinga.company.com
C:\Users\administrator.COMPANY>

```

Nslookup result from Windows

An nslookup result from Linux is as follows:

```

[root@lab4linuxdev1 /]# nslookup -query=ptr _ipp._tcp.buildinga.company.com
Server:          192.168.0.139
Address:         192.168.0.139#53

Non-authoritative answer:
_ipp._tcp.buildinga.company.com name = Building\032A\032printer
\032104._ipp._tcp.buildinga.company.com.

```

```
ipp.tcp.buildinga.company.com name = Building\032A\032printer
\032106._ipp._tcp.buildinga.company.com.
ipp.tcp.buildinga.company.com name = Building\032A\032printer
\032107._ipp._tcp.buildinga.company.com.
ipp.tcp.buildinga.company.com name = Building\032A\032printer
\032109._ipp._tcp.buildinga.company.com.
ipp.tcp.buildinga.company.com name = Building\032A\032printer
\032111._ipp._tcp.buildinga.company.com.
ipp.tcp.buildinga.company.com name = Building\032A\032printer
\032117._ipp._tcp.buildinga.company.com.
ipp.tcp.buildinga.company.com name = Building\032A\032printer
\03212._ipp._tcp.buildinga.company.com.
ipp.tcp.buildinga.company.com name = Building\032A\032printer
\032120._ipp._tcp.buildinga.company.com.
```

```
Authoritative answers can be found from:
buildinga.company.com nameserver = mobileserver.buildinga.company.com
```

If no printers appear, confirm with telnet that a connection can be established to the SafeCom Mobile Print Gateway IP address on port 53.

Remember that mobile device clients must have access to the SafeCom Mobile Print Gateway server on port 53, to retrieve the printer lists.

Set search domains on mobile devices

For Apple iOS mobile devices to retrieve the printers available for Wide Area Mobile Print, the iOS devices must be instructed to query the sub domains, using DNS-SD.

This can be done in one of two ways, depending on one or multiple sub domains having been created in SafeCom Mobile Print.

One Wide Area Mobile Print sub domain

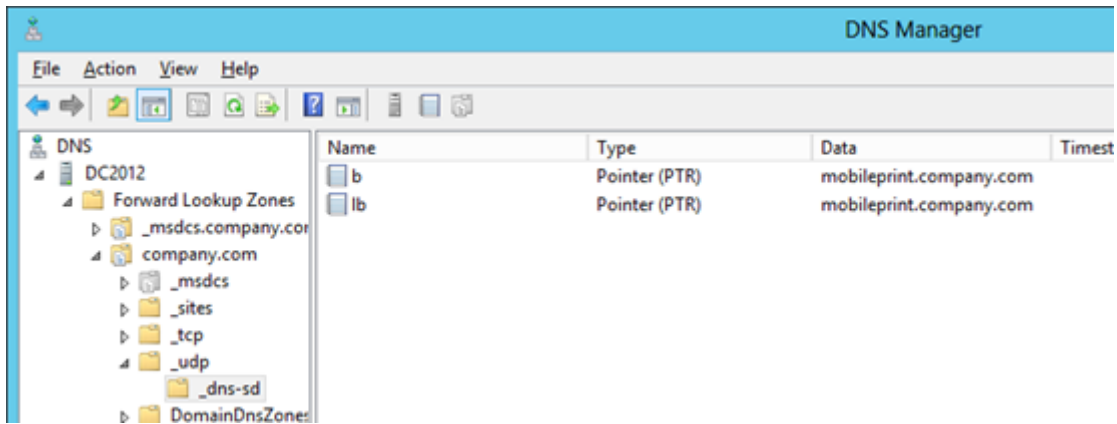
If only one Wide Area Mobile Print sub domain has been created (recommended), the configuration needed to instruct Apple iOS devices to query the domain is simple.

Configure single sub domain on Windows DNS

In addition to a delegation DNS record for the single "mobileprint.company.com" sub domain, create DNS-SD discovery record in Windows DNS.

1. Under the domain (in this case company.com), right-click `_udp` and select **Other new records**.
2. Select to insert a **Service Location (SRV)** record.
3. In the **Service** field, type in any characters, and in Protocol, enter **_dns-sd**.
There should now be an `_dns-sd` folder under `_udp`.
4. Delete the SRV record from within the `_dns-sd` folder that was created.
5. Right-click the `_dns-sd` folder and select **Other new records**, then select to insert a **Pointer (PTR)** record.
6. In **Host IP Address**, enter the letter "b" and in **Host Name**, enter the Wide Area sub domain, such as "mobileprint.company.com".
7. Create an additional **Pointer (PTR)** record with letters "lb" also pointing to the same sub domain.

The final structure should look like below.



Now any Apple iOS device with the search domain set to just "company.com" will discover the "mobileprint" sub domain and query the SafeCom Mobile Print Gateway for printers.

Single sub domain configuration on BIND

In addition to a delegation DNS record for the single "mobileprint.company.com" sub domain, create DNS-SD discovery record in BIND.

In the domains master zone file, insert the following two DND-SD records:

```
b._dns-sd._udp IN PTR mobileprint.company.com.
lb._dns-sd._udp IN PTR mobileprint.company.com.
```

Replace "mobileprint.company.com." with the actual sub domain as created in SafeCom Mobile Print.

```
;
; Zone file for company.com
;
$TTL 360
@      IN      SOA     ns.company.com. root.company.com. (
                    201404011      ; serial, todays date + todays serial #
                    8H              ; refresh, seconds
                    2H              ; retry, seconds
                    4W              ; expire, seconds
                    1D )            ; minimum, seconds

ns     NS      ns      ; Inet Address of name server
ns     A       192.168.0.139

b._dns-sd._udp IN PTR mobileprint.company.com.
lb._dns-sd._udp IN PTR mobileprint.company.com.

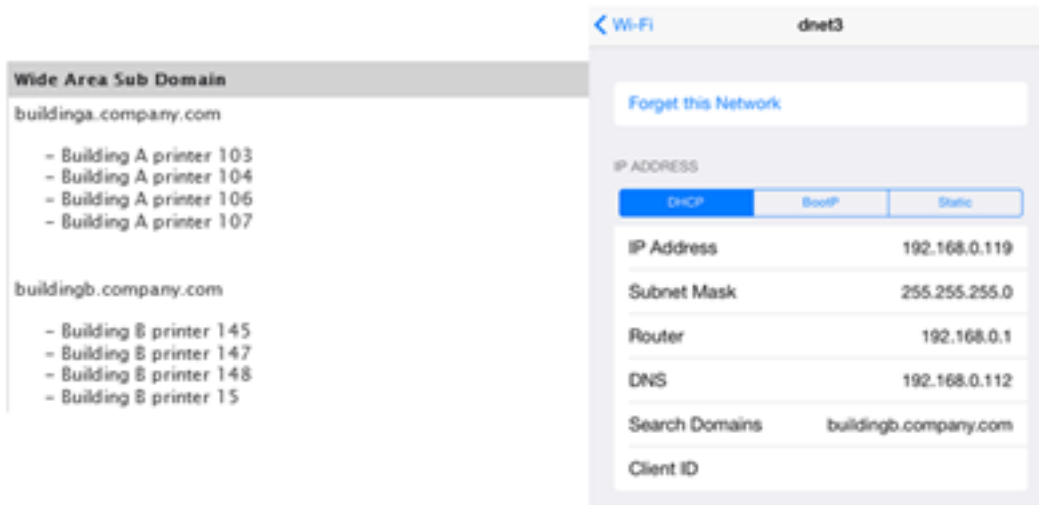
; Delegation for Wide Area Mobile Print sub domains
$ORIGIN buildinga.company.com.
@      IN      NS      mobileserver.mobileprint.company.com.
mobileserver IN A      192.168.0.109
```

Sample BIND zone configuration file for the domain "company.com" with a single "mobileprint.company.com" Wide Area Mobile Print sub domain.

Now any Apple iOS device with the search domain set to just "company.com", will discover the "mobileprint" sub domain and query the SafeCom Mobile Print Gateway for printers.

Multiple Wide Area Mobile Print sub domains

If multiple Wide Area Mobile Print sub domains have been created, access to the sub domains on Apple iOS devices is given, by populating the search domain on the mobile device, with the search domain or domains that the particular device should have access to.



This can be done either manually, or by having the DHCP server provide this value, using what is called "DHCP option 119".

See the sections below for instructions on how to populate the search domain using Windows and Linux DHCP.

Configure multiple sub domains on Windows DHCP

Microsoft Windows DHCP does not provide a friendly configuration interface for the DHCP option 119.

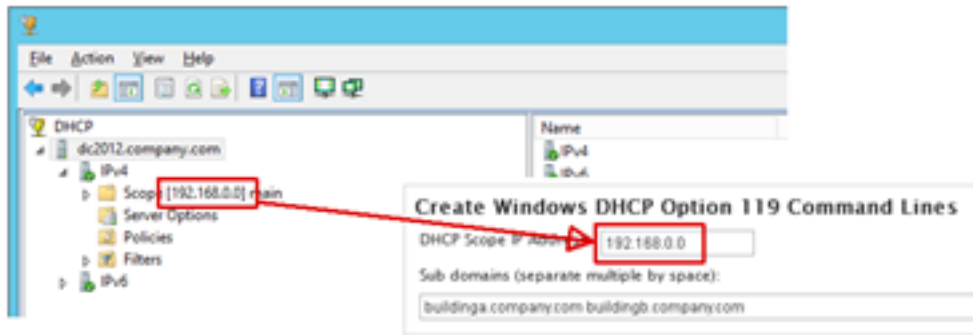
Configuration of DHCP option 119 on Windows DHCP involves the following steps:

1. If not done previously, first define the DHCP option 119 to the Windows DHCP server by running the following command on the DHCP server:

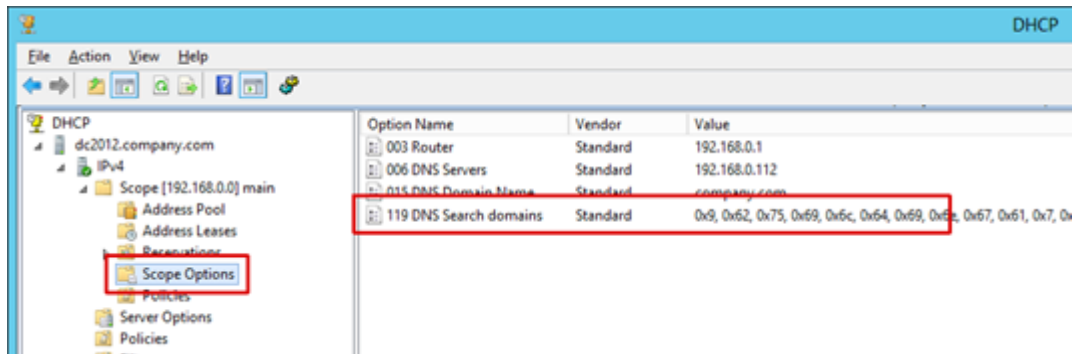
```
netsh dhcp server V4 add optiondef 119 "DNS Search domains" BYTE 1
```

A message comes up saying "Command completed successfully".

2. In the SafeCom Mobile Print Administrator interface, go to Wide Area Mobile Print and click **Windows DHCP Configuration Utility**.
3. Enter the **DHCP Scope IP Address**.



4. Enter the Wide Area Mobile Print sub domains that should be published to this DHCP scope. Separate multiple sub domains with space.
Example: buildinga.company.com buildingb.company.com
5. Click **Continue** when ready.
The required commands appear on the screen.
6. Copy/paste and run these commands on the DHCP server to create the DHCP entries.
7. Confirm the entries appear under Scope Options in the DHCP server (refresh the DHCP server view to show the new settings).



8. Mobile devices obtaining a new lease from the DHCP should now show the correct search domains.

Multiple sub domains configuration on Linux DHCP

To specify search domains for a subnet on Linux DHCP, edit the dhcpd.conf file and insert a domain-search option with the sub domains to publish.

```

subnet 192.168.0.0 netmask 255.255.255.0 {
    range 192.168.0.101 192.168.1.199;
    option domain-name "company.com";
    option domain-search "buildinga.company.com", "buildingb.company.com";
    option domain-name-servers 192.168.0.139;
    option routers 192.168.0.1;
}
    
```

Configure Google Cloud print

With Google Cloud, users can print from their Google Chromebook, phone or tablets, Google Apps such as Gmail, Google Docs, Google Sheets, or using any other application or device which supports Google Cloud Print, to the printers you select in SafeCom Mobile Print.

1. Create a Google account or select an existing one.
2. [Enable Google API access](#) for your Google account.
3. [Register your printers](#).
4. [Enable Public Link sharing](#) for your printers.

Enable Google API access

To use your Google account with SafeCom Mobile Print, you must establish an authenticated API access.

1. Start by going to Google Cloud Console at <https://cloud.google.com/console>.
2. Click **CREATE PROJECT**.
3. Enter a project name, used only internally in the Cloud Console for reference.
Google suggests a Project ID that can be used as is.
4. Depending on your account status, you may be asked to verify your account through SMS.
5. Click **APIs & Auth > Credentials > CREATE NEW CLIENT ID**.
6. Select **Installation application** and **Other**, then click **Create Client ID**.
The Google account **Client ID** and **Client secret** needed for integration are now created under "Client ID for native application".
7. Copy/paste the **Client ID** and **Client secret** into the SafeCom Mobile Print Google Cloud Print configuration screen.

Register printers


Configuring forward accounts on Microsoft Exchange involves creating a standard mailbox, and then setting a forwarding address.

1. Click **Register** for each of the printers that you would like to make available in Google Cloud Print.
The printer status changes to "Awaiting authentication" and a new button appears.
2. Click **Authenticate** to continue.
A new window opens with a Google Printer registration page.
3. Click the link in the middle of the page.
4. Click the **Finish printer registration** button.
The status of the printer in the SafeCom Mobile Print configuration page changes to **Active**, and the registration of the printer is now complete.

Enable Public Link sharing

When a printer has been added to Google Cloud Print, by default, it is only available to the Google Account owner.

We strongly recommend to share printers using a Google Cloud Print Public Link; otherwise, users can only print to the printer through Google Cloud Print if they are explicitly invited to the printer from the Google Cloud Print management pages.

 Depending on authentication settings in SafeCom Mobile Print, a user attempting to print through Google Cloud Print is always authenticated first to ensure only authorized users can print.

1. Click the **Not shared** link next to a printer.
2. Go to Google Cloud Printer Manage Printers page at <https://www.google.com/cloudprint#printers>.
3. Select the printer to modify and click **Share**.
4. To change from **Private access**, click **Change**.
5. Select **Anyone with the link has access to the printer**.
6. Change the limit of how much users can print to this printer by clicking **15 pages/day**.
7. Select **Unlimited quota**.
8. Copy the **Link to share** and insert this link in the printer's **Public Link** page in SafeCom Mobile Print, and then click **Save Changes**.

Print with AirPrint on iOS

You can use the native AirPrint function of iOS devices to print your documents with SafeCom Mobile Print.

1. To print from any app through AirPrint, select the export symbol and select **Print**.
2. In the print dialog box, select a SafeCom Mobile Print-exposed printer from the list.

Depending on the SafeCom Mobile Print server release configuration, the print job may be held in a queue for release or printed directly to the output printer.

The following output options are supported:

- Number of copies
- Color / B&W
- Page range

Authenticated print

If the release configuration is either Direct with authentication or Privacy with authentication, a login prompt is displayed for the username and password. This is because the printer resource is secured and requires authentication.

Once credentials have been entered, iOS normally does not prompt for them again. iOS will cache them and use them automatically when using the printer.

To reset the stored credentials, the iOS network settings must be reset, or the Strict mobile authentication feature of SafeCom Mobile Print may be used, which is able to work around this behavior.

Print with Android

The SafeCom Mobile Print Android app version 4 has a set of features similar to the iOS app.

Documents on Android apps can be printed using the "Share via" function that is similar to the "Open in" and "Print with SafeCom Mobile Print" actions on iOS.

Select the SafeCom Mobile Print app in the "Share via" dialog box.

The QR-code scanning uses the "zxing" (zebra crossing) third-party library. This library is required for the feature. If unavailable, install the Barcode Scanner app to make the "zxing" library available system-wide.

Native print on Android

Version 4.2 of the SafeCom Mobile Print Android app includes support for native print functionality of Android OS. This is only available for Android OS 5.0 or newer.

To use this functionality, do the following:

1. Open the SafeCom Mobile Print app and configure the connectivity (and log in if required).
2. Go to **Android Settings System > Printing**.
3. Select the SafeCom Mobile Print service and enable it at the switch control.

A list of printers is displayed. The number of printers depends on your SafeCom Mobile Print configuration. Now you can use the native print function from apps supporting this operating system feature.

4. For example, to print from Google Chrome, just open a web page, open the menu, and select **Print**. In the print screen, select one of the printers displayed when enabling the print service.

The following list of apps is known to work with native printing on Android 5 and 6:

- Google Chrome
- Firefox
- Google Mail (Gmail)
- Google Docs
- Google Photos
- Adobe Acrobat
- Microsoft Word
- Microsoft Excel
- Microsoft PowerPoint

The following output options are supported:

- Number of copies
- Color / B&W
- Page range

Card server

SafeCom Mobile Print includes a card server for network TCP/IP based swipe card readers. This enables card swipe authentication on printers or multifunction devices, thus users no longer need to enter login credentials.

The card server runs on TCP port 7292 per default (Card server port). Configure the network card readers to send data to the SafeCom Mobile Print server IP on this port.

Associate the network card reader with a device added in SafeCom Mobile Print, by going to the device enabling card reader, and entering the IP address of the network card reader.

Printer Details
Printer ID: 192.168.0.11 (39088457)
Printer Description:
Output Printer:
 Send a test print to printer after saving

Advanced Driver Print
Enabling advanced driver print on a print queue, lets users print directly to the print queue using any print driver compatible with the output device, and enabling use of all advanced output features on the device.
 Enable advanced driver print
Specify the printer model for users to install the correct driver:

Card Reader
 This device has a network card reader attached
Card reader IP address:
Card reader profile:
 Automatically print all the users jobs when swiping card

Card swipe timeout is the time from when the user swipes their card, and until the swipe authentication expires.

By default, the user has 30 seconds from swiping the card to activating the release application on the device.

SafeCom Mobile Print can look up usernames by searching the LDAP for card ID numbers. For card ID LDAP lookup to function, the LDAP settings under User Authentication must be configured successfully.

Card Self Registration settings are relevant for multifunction device terminals, so if a user swipes an unknown card, the user can associate the card with their network username, by authenticating with username and password.

Card Reader Profile

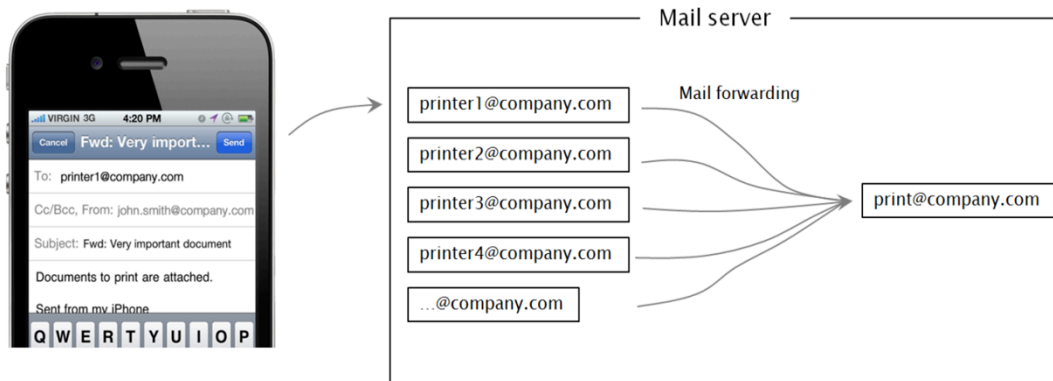
There are many different types of cards and card number formats. Use card reader profiles to modify the incoming data stream from the card reader to match a predefined format, for card numbers imported to the SafeCom Mobile Print database or stored in LDAP.

If no special card number translation is needed, just use the general ALL DATA profile.

Direct E-mail Print to Printer Email Alias

SafeCom Mobile Print supports email addresses for specific printers, making it possible for users to select the exact printer needed, considering for example driver compatibility, color, or paper size.

Users can send print jobs directly to a print queue, simply by emailing a specific email address. The e-mail forwarding accounts are created on the email server for each printer, which forwards emails to the central Email Print account.



SafeCom Mobile Print will retrieve email from the central Email Print account, and if an email was sent to an alias email address, SafeCom Mobile Print will immediately forward the print job to the relevant print queue.

To configure the Printer Email Alias:

1. Create email accounts for each printer which forward to main email print account.

2. Add the email address to the devices in SafeCom Mobile Print Admin:
 - a. Click the **Devices** tab and then the edit icon for the device to which you want to add an email address.
 - b. Under **Direct Email Print Alias**, enter the alias for the printer and click **Save Changes**.

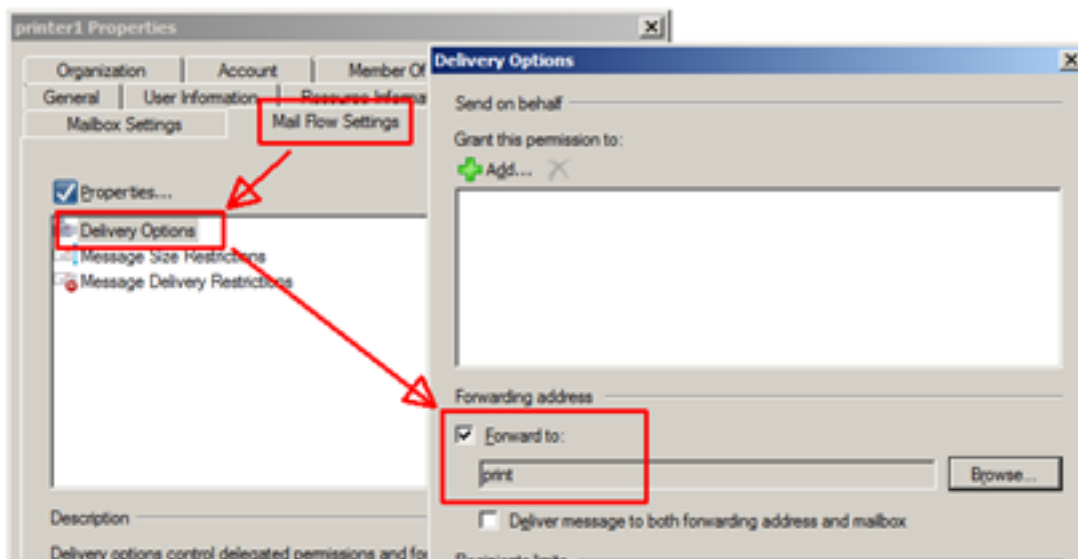
i The configuration of email forwarding addresses varies between mail servers.

Any print job now sent to the alias email address will be sent to the specific print queue. The usual authentication settings apply.

Configure mail forwarding account on Microsoft Exchange

Configuring forward accounts on Microsoft Exchange involves creating a standard mailbox, then setting a forwarding address.

1. Go to the individual printer's email account properties and open the **Mail Flow Settings** tab.
2. Select both **Delivery Options**, the **Forward to** check box, and the main **Email Print** account.
3. Repeat this for all individual printer email addresses.



In this example, any emails sent to printer1 will be forwarded to the "print" email account.

Mobile Print configuration

To enable native printing from supported mobile devices, the SafeCom Mobile Print Gateway must be installed and configured as detailed in [Mobile Gateway installation](#).

Configure the name of the main printer as it will appear on users' mobile devices, for devices that support printer naming.

In the Mobile Print screen, manage feature behavior for native printing from mobile devices, such as AirPrint on Apple iOS devices (iPhone and iPads) and Android-based smartphones and tablets.

Depending on the configuration in Printing and Security, different behavior is available. Select the relevant setting for the current configuration. For example, whether users are allowed to only send print jobs to SafeCom Mobile Print in general, or are users allowed to send print jobs directly to all devices configured in SafeCom Mobile Print.

Strict Mobile device authentication applies to Mobile Print using Apple iOS and Android printing.

When enabling strict mobile device authentication:

- Users must authenticate when their mobile device uses a new IP address.
- Users have the ability to log out using the SafeCom Mobile Print mobile apps.
- Users can be forced to re-authenticate after a set period of time (useful for shared iPads or similar).

Using SSL with SafeCom Mobile Print

Secure Socket Layer (SSL) allows Web browsers and Web servers to communicate over a secured connection using the HTTPS protocol where both the server and the browser encrypt data before sending it.

SSL also authenticates the credentials of your Web server as proof that the website is what it claims to be. In order to implement SSL, a Web server must have a certificate for each IP address that accepts secure connections. Certificates to test the SSL listener can be self-signed; trusted certificates are issued by a certificate authority.

The following steps are briefly described in these sections:

- [Generate a test certificate](#)
- [Configure SafeCom Mobile Print with the test certificate](#)
- [Verify the test certificate](#)
- [Obtain a trusted certificate](#)

Generate a test certificate

A keystore containing a public key/private key pair and a certificate for testing SSL can be generated using keytool, a command-line utility provided in the Java JDK. The following instructions allow you to generate a simple key pair and certificate keystore that is valid for three months. This keystore allows you to test that the SSL listener can run, but its certificate is self-signed and is not trusted by the browser.

To generate a test certificate:

1. Locate the Java keytool utility.

By default, the keytool utility can be found in `C:\Program Files\SafeCom\SafeCom Mobile Print\jre\bin`.

2. Generate a simple key pair and non-trusted certificate into a keystore file named keystore by typing:

```
keytool -keystore keystore -alias jetty -genkey -keyalg RSA
```

i A highly recommended graphical user interface alternative to the command line keytool is the free Keystore Explorer by Lazgo Software, available at <https://lazgo-software-ltd.software.informer.com/>.

You are now prompted to provide answers to several questions for the certificate.

3. Press Enter to submit each of your answers.
4. When prompted for "What is your first and last name?", enter the fully qualified domain name of the SafeCom Mobile Print server, such as "localhost" or "print.company.com". Write down the two passwords that you enter.

In the next section, [Configure SafeCom Mobile Print with the test certificate](#), you enter these passwords to configure the SSL function.

If you answer these questions accurately for the test certificate, the certificate that you generate can be used as the basis of your trusted certificate that you obtain from a certificate authority.

The generated keystore file is located in the directory in which you ran the keytool. If connections to SafeCom Mobile Print come only from inside your organization, a non-expiring, self-signed certificate that is added to each internal user's Web browser certificate store may be adequate. See the options for keytool to generate a non-expiring, self-signed certificate.

Configure SafeCom Mobile Print with the test certificate

To configure SafeCom Mobile Print with the test certificate you just generated, you will copy the keystore into the SafeCom Mobile Print directory structure, make a configuration change in a Web configuration file, and then restart SafeCom Mobile Print Web services.

1. Copy the keystore file, keystore, to C:\Program Files\SafeCom\SafeCom Mobile Print\etc.
2. Open the configuration file jetty-ssl.xml located in C:\Program Files\SafeCom\SafeCom Mobile Print\etc.
3. Change the password, keyPassword, and trustPassword values to the passwords chosen when generating the certificate.
4. If you want the port to be something other than 9443, change the Port value.
5. Save the file and restart SafeCom Mobile Print Web service.

If you are already running a Web server with SSL encryption enabled on the same server on which SafeCom Mobile Print is installed, it will be necessary to change the port on which SSL is running for either SafeCom Mobile Print or the other Web service. SSL default listens on port 9443. Change to a different port in jetty-ssl.xml and restart SafeCom Mobile Print Web services if there is a port conflict.

Verify the test certificate

Now that you have reconfigured SafeCom Mobile Print to accept HTTPS requests and restarted it, verify that you can log in to SafeCom Mobile Print using HTTPS.

1. Open a browser and type `https://localhost:9443/admin`.

Use the fully qualified domain name (FQDN) for the host that you specified when you generated the keystore.

2. Replace 9443 with the HTTPS port number you configured.
Because you generated the certificate yourself, a dialog box appears, warning that the SafeCom Mobile Print web interface is certified by an unknown authority.
3. Accept this certificate temporarily for this session and select **OK**.
The login page for the SafeCom Mobile Print web interface is displayed.

Obtain a trusted certificate

If users are connecting to SafeCom Mobile Print from outside your organization, you probably want to obtain a trusted certificate. To obtain a trusted certificate, contact a certificate authority such as Verisign, Thawte, Geotrust, or similar.

Each certificate authority has its own instructions, but all require that you submit a certificate signing request (CSR) that you can generate from the test keystore using the keytool utility.

To obtain a trusted certificate:

1. To generate a CSR in a file named `mobile_print.csr` for a key pair and certificate already in a keystore in the current directory, type:

```
keytool -certreq -alias jetty -keystore keystore -file mobile_print.csr
```

By Default, the keytool utility is installed by default under `C:\Program Files\SafeCom\SafeCom Mobile Print\jre\bin`.

2. Submit this CSR as instructed by the certificate authority you chose.
3. After you receive a trusted certificate from the certificate authority, load the certificate into the keystore used to generate the CSR. If the certificate is in a format understood by the keytool utility, type:

```
keytool -keystore keystore -import -alias jetty -file mobile_print.crt \ -  
trustcacerts
```

If it is not in a format understood by the keytool utility, refer to *Configuring SSL/TLS KeyStores* at the following link or the documentation from the certificate authority: <https://www.eclipse.org/jetty/documentation/jetty-11/operations-guide/index.html#og-keystore>.

Chapter 5

Administer SafeCom Mobile Print

Log in to the SafeCom Mobile Print web interface


To configure SafeCom Mobile Print, open the SafeCom Mobile Print web interface from the shortcut either in the Windows start menu, the desktop icon, or by entering one of the following two URLs for the SafeCom Mobile Print web interface:

- `http://127.0.0.1:7290/admin`
- `https://127.0.0.1:9443/admin`

Change the IP address to that of the SafeCom Mobile Print server.

Log in using the default username and password:

- Username: admin
- Password: nimda

 It is recommended to change the default username and password. See [Manage user email addresses](#).

Access SafeCom Mobile Print web interface remotely

The SafeCom Mobile Print web interface can also be accessed remotely from any client with access to the IP address of the computer hosting SafeCom Mobile Print.

This can be done through the URL `http://127.0.0.1:7290`, where the IP address must be that of the SafeCom Mobile Print server.

Use the default username and password to log in.

Dashboard with statistics

When you log in to the SafeCom Mobile Print web interface, the Dashboard opens, which is an overall view of completed print job usage and activity in SafeCom Mobile Print.

See the reporting data for a specific period

By default, the reporting data shown is for the past month from today's date.

1. Select a reporting date range for the dashboard by selecting the **date from** and **date to** fields in the upper right corner.
2. Click **Apply**.

The number of pages reported in the Dashboard does not reflect the accurate printed output on device, as SafeCom Mobile Print reports the number of pages contained in the document, not the actual output. For accurate output tracking, use SafeCom Mobile Print together with a print accounting system.

See all activity from a specific user in a date range

1. Select a reporting date range for the dashboard by selecting the **date from** and **date to** fields in the upper right corner.
2. Click **Apply**.
3. Click **Show all users**.
4. Select the user you want to check.

SafeCom Mobile Print monitor

On the Monitor tab in the SafeCom Mobile Print web interface, you can see recent print jobs and email activity in the SafeCom Mobile Print server. This is useful for verifying the status of certain print jobs or just monitoring activity, and for searching for specific activities.

Hide user and document information in Monitor

For situations where administrators should not be able to view user names or document names in the Monitor, for privacy reasons, a settings parameter can be added to the main SafeCom Mobile Print configuration file eop.xml.

1. Stop the SafeCom Mobile Print Web service.
2. From the installation directory, open eop.xml in a text editor such as Notepad.
3. Add/edit the following parameter:

```
<adminprivacy>{0-3}</adminprivacy>
```

The {0-3} number in the parameter can be any of the following numbers:

- 0 = Normal operation
 - 1 = User name is hidden
 - 2 = Document name is hidden
 - 3 = User name and Document name are hidden
4. Start the SafeCom Mobile Print Web service.

Hide the Monitor completely

For situations where the Monitor view should be hidden completely from the SafeCom Mobile Print administration interface, a settings parameter can be added to the main SafeCom Mobile Print configuration file eop.xml.

1. Stop the SafeCom Mobile Print Web service.
2. From the installation directory, open the eop.xml in a text editor such as Notepad.
3. Add/edit the following parameter:

```
<hidemonitor>true</hidemonitor>
```



4. Start the SafeCom Mobile Print Web service.

Manage existing printers

To open the Devices web page, click the Devices tab.

If printers already have been added to SafeCom Mobile Print, the Devices web page automatically lists installed printers.

From the Devices web page, the installed printers can be edited, deleted, or a test print can be sent to the selected printer.

- Click the Delete  icon to delete the printer from SafeCom Mobile Print.
- Click the Edit  icon to change settings or send a test print to the selected printer.

Use the drop-down menu to view different settings for the listed printers.

- Output printer: The corresponding Windows print queue
- Advanced Printer Model: The printer model specified under Advanced Driver Print
- Advanced Print enabled: Shows whether Advanced Driver Print is enabled
- Printer Email Alias: What, if any, printer email address alias has been configured
- External Printer ID: The external Printer ID for the device for use in IPP or LPD print

Associate network card reader with device

If using the built-in card server in SafeCom Mobile Print with network-based card readers, associate the network card reader with a device added in SafeCom Mobile Print, enabling the card reader, and entering the IP address of the network card reader.

Card Reader

This device has a network card reader attached

Card reader IP address:

Card reader profile:

Automatically print all the users jobs when swiping card

Checking **Automatically print all users jobs when swiping card** is a useful setting to enable if using card readers on simple network printers. Enable this setting to release all print jobs of the user when the user swipes its card.

You can use the Device Groups for grouping printers for easier viewing or controlling the visibility of printers for users - that is, you can set that certain printers are only accessible to certain user groups.

To create device groups, simply click **Add New Device Group**, enter a name, and select the devices you want to add to the group, and click **Save**. Devices can be part of multiple groups.

To limit device visibility for users, you can set the **Field containing users device group names** field on the **User Authentication** screen of the SafeCom Mobile Print Administrator. This field can be filled either based on a valid LDAP field (if you are using LDAP authentication), or you can use the Windows Active Directory security groups. For this latter, ensure that the **Field containing users device group names** field is set to **memberOf**, and that the **External name** property of your Device Groups matches the name of the Windows group.


Manage user email addresses


The first time a user sends an email print jobs, the user is prompted to register their email address with their username. See [Email and Google Cloud Print authentication](#).

Click the Users tab to see the registered users.

The email addresses that a user has associated can either be deleted from the user or a new email address can be added to the user, which means that the user do not have to register that email address in the system the first time using the email address.

Delete an email address from a user

1. Click **User Email Addresses** in the left menu.
2. Browse to the right username and click the **Delete**  icon next to the email address you would like to delete.

 The user is not deleted from SafeCom Mobile Print. Only the email address is deleted.

Associate a new email address to a user

1. Click **User Email Addresses** in the left menu.
2. Under **Add New User Email Address**, enter the username and the email address that you would like to associate with each other.
3. Click **Add New Email Address**.

Import User Email Addresses from a CSV file

To allow users to print through Email Print from mobile devices without having to register, user email addresses can be imported into SafeCom Mobile Print from a comma-separated file (CSV).

Click Import User Email Addresses in the left menu. In the Import Users dialog box, browse to the CSV file from where you want to import users.

Files need to be in the following format:

```
username,emailaddress
```

For example:


```
user1,user1@domain.com  
user2,user2@domain.com  
user2,user2@anotherdomain.com
```

One user can have many email addresses.

Change Administrator Login

Change the default admin password:

1. Open and log in to SafeCom Mobile Print web interface.
2. Click the **Settings** tab and then **Administrator login** in the left menu.
3. Enter the current password and the new password.

 If the password to the admin is lost, it is necessary to contact Kofax for support.

4. Click **Save Changes**.

Back up SafeCom Mobile Print data

To back up SafeCom Mobile Print settings, copy the following files or directories to a safe location:

- C:\Program Files\SafeCom\SafeCom Mobile Print\eop.xml
- C:\Program Files\SafeCom\SafeCom Mobile Print\printers.xml
- C:\Program Files\SafeCom\SafeCom Mobile Print\data (entire folder with subdirectories)


If you have changed Web port configuration or configured SSL certificates, back up this folder:

- C:\Program Files\SafeCom\SafeCom Mobile Print\etc

Upgrade SafeCom Mobile Print

Before upgrading to a new version, make sure to:

- Verify that your license has valid maintenance for access to software updates.
- Back up any existing data and configuration files in SafeCom Mobile Print. See [Back up SafeCom Mobile Print data](#).

 If maintenance has expired and a new version is installed, the program ceases to function until the license is renewed or upgraded.


To upgrade SafeCom Mobile Print:

1. Download and run the installer with the latest version of SafeCom Mobile Print.
The installer updates your existing installation.
2. Confirm your settings in SafeCom Mobile Print and, if necessary, re-activate Email Print in the SafeCom Mobile Print web interface.

Licensing

SafeCom Mobile Print installs with a 60-day trial license. Under the Settings tab in SafeCom Mobile Print Administrator, you can enter the permanent license key. Remember to save any changes by clicking the Save Changes button.

A SafeCom Mobile Print license can be purchased from your local SafeCom partner.

 License keys are unique to the particular SafeCom Mobile Print server. If the server is renamed or changed significantly, a new license key must be issued. For a new license to take effect, it is necessary to restart the SafeCom Mobile Print Web service after saving a new license key on the Settings page.

Uninstall SafeCom Mobile Print

Before uninstalling SafeCom Mobile Print, make sure to back up any existing data and configuration files in SafeCom Mobile Print. See [Back up SafeCom Mobile Print data](#).

Chapter 6

Use SafeCom Mobile Print

The User Web Portal is where users can upload documents to print through Web Print (see [Upload document for print](#)), as well as an overview of their print jobs awaiting collection.

Log in to User Web Portal

The User Web Portal can be accessed by default for HTTPS/SSL on:

- <http://127.0.0.1:7290>
- <https://127.0.0.1:9443>

Change the IP address to that of the SafeCom Mobile Print server.




To log in, the user must enter the Windows username and password.

Send a print job through AirPrint

SafeCom Mobile Print allows you to fully utilize the iOS AirPrint of your iPhone or iPad to print your documents.

Using AirPrint

To use the native AirPrint:

1. Tap the  or  icon.
These icons are at the bottom of the screen of the mobile device.
2. Tap .
3. Select the printer you want to use.
4. Set the number of copies you want to print and tap **Print**.
5. When prompted, use your Windows credentials to authenticate yourself.

Send a print job through email

With Email Print, the user can either send or forward an email from a computer, a mobile device, or any other email client to the specified email print address (for example: print@company.com).

If Email Print is enabled, the User Web Portal includes an Email Print tab, containing instructions for the user on how to print through email.

Send email print

To send a document for print through email:

1. Open the email program and create a new email.
2. In the **To:** field, enter the specified email address for Email Print (print@company.com).
3. Attach the documents to print.
4. Click **Send**.

i If the user's email address is unknown to the system, the user is prompted through email to register the email address using the Windows username and password. See [Register a new email address](#).

It is also possible to send an email notification from the system to the user when the document attached to an email is in an unsupported format.

The SafeCom Mobile Print server now collects and processes the email, and makes it available for collection at any company network printer. Depending on the setup in the SafeCom Mobile Print web interface, only the document is created as a print job or both the document and the body content of the email are created into print jobs.

5. Open and log in to the User Web Portal and click **My Print Job** to get an overview of the print jobs available for collection at the printer.

i The list of print jobs on the My Print Job web page is a list of print jobs processed through SafeCom Mobile Print. The list is not updated to, for example, show whether the documents are actually printed or deleted at the printer.

Send email printer and control choice of printer

If multiple SafeCom Pull printers have been defined and there is a desire to control which one is used, this can be achieved through the Subject field by writing "P:" before the printer name.

For example: P:Color or P:Mono.

This can be useful in an environment with devices from different vendors or if you wish to control for example color printing and mono printing.

Alternatively, the mail server should be configured to accept multiple mail addresses and then manipulate the subject field accordingly. Example:

Before as submitted by user	After as manipulated by mail server
To: printcolor@company.com	To: print@company.com Subject: p:colorprinter

Before as submitted by user	After as manipulated by mail server
To: printmono@company.com	To: print@company.com Subject: p:monoprinter

Register a new email address

When a user sends an email print job from an unknown email address to SafeCom Mobile Print, an email is immediately sent back to the user prompting the user to register the new email address with the user's Windows username and password.

1. Click the link in the email that you have received prompting to register the email address.
2. Enter your Windows username and password.

i It is very important that the user registers the email address with the Windows username and password, because this is how the user is recognized by the SafeCom solution.

3. Click **Continue**.
The email registration is now complete.
4. If you want to register another email address with your Windows credentials, click **Register Another Email Address** and enter the email address and Windows username and password.
5. Close the web browser.

Send a print job through web

Via the user web portal, it is also possible to upload a document for print and, if set up in the SafeCom Mobile Print web interface, a specific URL to be printed.

By default, the SafeCom server does not impose a limitation on file size, but a maximum file size limit can be implemented. Due to browser limitations, the SafeCom Mobile Print server does not know the actual size of the upload until upload is completed. If the limit is set to 10 MB, for example, a user can still upload a 20 MB job. However, the job is deleted and an error message shown once upload is completed. This ensures no jobs exceeding the set limit are processed.

Upload document for print

To upload a document for print:

1. Open and log in to the User Web Portal.
2. Click the **Web Print** tab in the top menu.

Users can upload Microsoft Office documents (.doc, .docx, .xls, .xlsx, .ppt, and .pptx), PDF, TXT, RTF, as well as OpenOffice documents.

i Microsoft Office and OpenOffice must be set up to be supported in the SafeCom Mobile Print web interface.

3. To upload a document for print, click **Browse** under **Upload Document To Print** and select the file locally. Click **Next**.
4. To print a web address or a web link to a document, enter the URL address or the web link in the **Web Address To Print** field and click **Next**.

i The web addresses entered must be publicly accessible. SafeCom Mobile Print cannot access URLs that require authentication or a specific user session, as SafeCom Mobile Print connects to the URL directly as a new user and attempt to retrieve the contents.

After uploading a job for print, the user is redirected to the My Print Jobs page. In the list of print jobs, the job is now listed at the top, and when the status changes to Printed, the document is ready to be collected at the printer.

If Privacy with Authentication is selected as the Print behavior, after uploading the document, the user is required to select a printer on the displayed printer selection section, as well as advanced settings for print (if available).

Driver Print

To configure use of the Driver Print:

1. Open and log in to the User Web Portal.
2. Click the **Driver Print** tab in the top menu.
3. Select your operating system (Windows, Mac OS, or Linux).
4. Select how you would like to print.
 - With simple print, users print using a generic PostScript driver they already have on their computer. Setup is very quick and simple, and users can print without downloading and installing special drivers. SafeCom Mobile Print will convert the PostScript on the server to PDF and store encrypted. When the user releases the job, the PDF is printed using the correct driver installed on the SafeCom Mobile Print server compatible with the output device.
 - With advanced print, users use a printer driver which is compatible with the printers they want to print to, which will make it possible to use the advanced features of the output printer, such as binding and stapling. SafeCom Mobile Print does not convert or modify the print data stream when sending Advanced. It is forwarded as is to the destination print queue, when released.

Users can create multiple printers on their computer for different print queues in the SafeCom Mobile Print system.

5. Click **Continue** and follow the on-screen steps.

Guest printing

Guest printing allows you to print your documents with SafeCom Mobile Print without having to access the LDAP authentication server. For more information on setting up guest printing, see [SafeCom authentication](#).

The guest printing process is as follows:

Submit your print job through the SafeCom Mobile Print server.

A guest user account is created automatically for you, and the system sends you an email message containing the credentials (User ID and PIN code) needed for accessing the SafeCom Mobile Print web portal, and which you can use to authenticate yourself at the printer, and print your document.

Private Print Clouds

With Private Print Clouds, users can print from their laptops or workstations using Advanced Driver Print, to a virtual print queue on the SafeCom Mobile Print server. Jobs are held paused in this queue until the user walks to a device to pull the jobs. Users can release jobs in a number of ways, including from a web interface, on the panel display of multifunction devices, or by swiping a card on a card reader.

Virtual print clouds and pull printing are often referred to as other terms such as "follow me printing".

The typical workflow:

1. The user prints from a workstation to the virtual print queue on the SafeCom Mobile Print server.
2. The user walks to a device and logs in with a swipe card, or by entering a username and password, depending on the configuration.
3. The user can view waiting jobs on the panel display, and can select jobs to print, which are then pulled from the virtual cloud queue on the SafeCom Mobile Print server and sent to print on the device.

A release printer is not required to have a full panel display for release. A network printer can be used with a network attached card reader as an alternative. Print jobs in the private print cloud can also be released from the SafeCom Mobile Print web interface.

Pull print essentials

When a user prints a job on the client workstation or laptop using Driver Print, the print job is rendered using a manufacturer's printer driver, in a print language such as Postscript or PCL. This rendered print data is sent to the SafeCom Mobile Print server where it is stored as is, until the user decides to release the job. When the print job is released, the SafeCom Mobile Print server sends the raw print data as delivered from the original printer driver, through the Windows spooler system, to the output printer.

Using a driver compatible with the output device is a must. If the user prints using a Postscript driver, but the output device uses PCL, the print job will fail.

When you create the Private Print Cloud queue in SafeCom Mobile Print, specify what driver to use, and if deploying printers through login script or group policies, use the appropriate compatible driver.

If you have a mixed fleet of devices with multiple manufacturers and models, you can create multiple Private Print Cloud queues, with separate drivers.

The same output device can also be associated with multiple Private Print Clouds.

It is strongly recommended to thoroughly test driver compatibility if you have a mixed printer environment.

Create Private Print Cloud

To create a virtual private print cloud:

1. First add output devices with Advanced Driver Print enabled, then click **Private Print Clouds** and click to add a new queue.
2. Create a recognizable Queue ID, as it can later be used for printing to the queue.
3. Enter a descriptive Printer Name and the Device Model for the output devices.

Print to Private Print Cloud

Print to the private print clouds using the Driver Print feature in SafeCom Mobile Print, either via http/https IPP printing or using the built-in LPD server.

To print to the queue created through IPP, make sure Driver Print has been configured and enabled in the SafeCom Mobile Print Admin. Then log on to the SafeCom Mobile Print end user web portal, and select Driver Print and Advanced.

Select the print queue, and instructions for that queue and operating system will appear. For more information about Driver Print, see [Driver print configuration](#).

Using the SafeCom Mobile Print iOS app

Configuration

When using the SafeCom Mobile Print app for the first time, it is required to connect it to the mobile gateway server application.

To do that, select the Settings tab in the app and tap the Discover button. The discovery process will try to find the gateway service announcement through mDNS and DNS-SD. Once it is found, the domain name and the port number of the mobile gateway host are automatically inserted in the text field.

If the mobile app consistently is not able to discover the gateway, this may result in mobile devices also not being able to discover the SafeCom Mobile Print printers enabled for AirPrint.

To validate the connection details, test the connection. The connection test will use the connection details from the text field to connect to the mobile gateway server. If it succeeds, the Save button appears.

When the connection test has succeeded, you should keep the settings by tapping the Save button.

This process also retrieves the SafeCom Mobile Print server settings to update the layout of the UI of the app according to the configuration made on the SafeCom Mobile Print server.

Account

Depending on the release configuration of the SafeCom Mobile Print server, the second tab of the app is Account.

Account tab

Enter account information here if the release configuration is either "Privacy with authentication" or "Direct with authentication".

This is especially required for the job release functionality of the app.

Use the "Create guest account" button for guest account creation.

Creating a guest account

Use this screen to create guest accounts. Be aware that this feature may be disabled, depending on your SafeCom Mobile Print server settings.

Releasing available print jobs

Available print jobs for an authenticated user are listed in the MyJobs tab. Use the refresh button in the toolbar to reload the list.

Swipe left on a job for quick access to print and delete.

Multiple jobs can be selected for batch release/delete using the Select button.

Releasing with customized output options

The MyJobs screen is, in fact, a master detail screen. Selecting a job opens the job details. On this screen are also the configurable output options.

Output options can only be applied for a single job release.

The values for copies, duplex (simplex, long edge, short edge), black/white and page range can be configured.

Selecting the output printer

Releasing one or more jobs using the Print button will open the printer selection screen if there is more than one available printer to select from.

Print using Open in or the Print with Mobile Print action

There are two options to print content from one app using the SafeCom Mobile Print app:

- **Open in**
- The share or action extension (iOS 8.0 or newer)

Open in is only supported by a minor number of apps.

The action extension is supported by a higher number of apps.

In both cases the apps that distribute the data must support either **Open in** or the action extension.

Printing with Open in

To print documents using **Open in**, select the export symbol in the app of which you would like to print the content and select **Open in**. In the next dialog box, select **Open with Mobile Print**.

Printing using the Print with Mobile Print action

To print documents using the action extension select the export symbol in the app of which you would like to print the content. In the bottom of the export dialog box are two rows of available apps for sharing. The SafeCom Mobile Print action extension is in the lower row.

If the **Print with Mobile Print** symbol is not visible at first, it must be manually enabled.

To do that, click the **More** button and enable **Print with Mobile Print** in the next screen.

After doing this, the **Print with Mobile Print** should from then on be visible in the export dialog box if the document to be printed is supported by SafeCom Mobile Print.

After the **Print with Mobile Print** symbol was selected, you may need to select an output printer if more than one printer is available.

Setting custom output options

Similar to releasing a print job, it is also possible to configure output options when submitting a job.

The values for number of copies, duplex (simplex, long edge, short edge) and black/white can be configured.

Output printer selection

During the process of releasing a job or printing a shared document using **Open in** or the **Print with Mobile Print** action, it may be required to select an output printer from a list of available printers. If only one printer is available, you do not see this screen.

Favorites

The favorites section is the default screen when the printer selection opens.

Here you can quickly select your favorite printers.

To remove printers from the favorites either swipe left on a printer and select Delete or select the Edit button from the toolbar.

Any available printer can be defined as favorite. To do that, open the All section to show all available printers.

Available printers

Available printers are displayed in a two-level master-detail view.

Printers may be configured to be part of a printer group. If there is only one or no group at all, the printers are shown right away. Otherwise, a printer group must be chosen to select a printer of that group.

If a printer is chosen by tapping on it, it will be used as the output printer.

It is also possible to define printers as favorites by swiping left on a printer and clicking Favorite.

Scan a printer

Instead of selecting a printer from the lists, it is also possible to scan a printer from a QR-code.

To do that, select the Scan section button.

A new screen opens with a camera view. Get the QR-code in view to be scanned.

If the QR-code is a valid SafeCom Mobile Print printer QR-code as configured in the SafeCom Mobile Print server, it is automatically chosen as output printer.

Due to iOS security and iOS action extension API limitations, the Print with Mobile Print action cannot access the camera and thus scanning does not work.

AirPrint vs. Open in vs. Print with Mobile Print action

SafeCom Mobile Print on iOS offers three ways of printing content.

- The iOS native method AirPrint has the widest app support, meaning it is possible to print from almost all apps that have printable content.
Output options like number of copies, duplex, and so forth are currently not supported for the native AirPrint method.
- **Open in** is only available in a very low number of apps. Apps supporting this share the content with the SafeCom Mobile Print app. The SafeCom Mobile Print app sends the shared data to the SafeCom Mobile Print server for conversion.
Output options are supported.
- The action extension works similarly to the **Open in** method, except that it is available from a larger range of apps.
Output options are supported.
QR-code scanning is not available.

Chapter 7

Troubleshooting

Common LDAP authentication error codes

Configuring Lightweight Directory Access Protocol (LDAP) can be complex. Included in SafeCom Mobile Print is a testing function, but before using the test function you need to obtain the path and settings of the internal LDAP system. We recommend using a LDAP browser, together with the path, to view the directory and gain a better understanding of how LDAP is implemented at your organization.

Using an LDAP browser

One example of a free LDAP browser is available from Softerra. If you can connect with the browser, you can navigate through the tree to see where the users are stored. When you find the directory with the users, look at the top bar of the LDAP browser to get your Start Search DN path. Groups can be found in the same way.

Using the LDAP browser, you can verify a user's information. Typically you use "sAMAccountName" or "cn".

Log files

When configuring LDAP authentication, it is useful to enable debug logging in General Settings. This ensures that any relevant details are logged to file. Log files are located in \logs subdirectory of the SafeCom Mobile Print installation.

LDAP errors

Error: com.server.exception.DBException: Error in bind() from LDAP source: [server]:[port]

This is a very general error, and it means something went wrong when trying to bind to LDAP/AD. Check to see if the LDAP/AD server name and/or port number you have specified is incorrect or an incorrect DN was specified as the administrator username.

Error: javax.naming.CommunicationException: [server]:[port] [Root exception is java.net.ConnectException: Connection refused: connect]

The port name you have specified for the LDAP/AD server is incorrect.

Error: javax.naming.CommunicationException: [server]:[port] [Root exception is java.net.UnknownHostException: [server]]

The LDAP/AD server name you have specified is incorrect.

Error: javax.naming.NamingException: Cannot parse url: [protocol]://[server]:[port] [Root exception is java.net.MalformedURLException: Not an LDAP URL: [protocol]://[server]:[port]]

The protocol you have specified is incorrect.

Error: javax.naming.AuthenticationException: [LDAP: error code 49 - Invalid Credentials]

The DN path or password specified for the administrator is invalid. Any of the following issues may cause this error:

- Pointed to non-user DN
- Pointed to a non-existent user, but in existing DN
- Pointed to non-existent DN
- Pointed to an existing user, but non-existent DN
- Pointed to an incorrect admin DN, uid instead of cn
- Pointed to a non-administrator user
- Pointed to a valid admin but password is incorrect

Error: com.server.exception.DBException: Error in searchForUserList from LDAP plugin: [LDAP: error code 32 - No Such Object]

Very general error when there is a problem finding the users in LDAP/AD. Could be that the DN pointing to the users is pointing to the wrong place or is just incorrect and does not exist.

Error: javax.naming.NameNotFoundException: [LDAP: error code 32 - No Such Object]; remaining name '[DN]'

The DN path that points to where the users are located in the directory is invalid.

Error: com.server.exception.DBException: Error in searchForUserList from LDAP plugin: [LDAP: error code 2 - Bad search filter]

Invalid search filter passed to the LDAP/AD server.

Error: javax.naming.directory.InvalidSearchFilterException: Missing 'equals'; remaining name '[DN]'

The filter specified is wrong or CPS constructed a bad filter.

Error: javax.naming.directory.InvalidSearchFilterException: Unbalanced parenthesis; remaining name [DN]

You did not have correct opening and closing of parenthesis in your search filter.

**Error: Error in bind from LDAP source: [LDAP: error code 49 - Invalid Credentials]
javax.naming.AuthenticationException**

Could not authenticate the user trying to log in. This can be the result of an incorrect username or password, or an incorrect prefix and/or suffix specified in the LDAP Authentication screen, depending on the type of LDAP/AD system. Could also mean the authentication type is incorrect.

**Error: Error in bind from LDAP source: [LDAP: error code 34 - invalid DN]
javax.naming.InvalidNameException**

This is caused by a bad prefix specified in the LDAP Authentication screen, on most LDAP/AD systems. This could mean you did not specify a prefix at all, which means the LDAP/AD server did not receive a full DN from SafeCom Mobile Print or that you did not specify a correct prefix, such as CN instead of UID, which results in the LDAP/AD server not receiving a correct DN from SafeCom Mobile Print.

This can also be caused by a missing comma at the beginning of the suffix or an extra comma at the end of the suffix. This error could also mean the authentication type is incorrect.

Error: NoSuchAttributeException

This is caused by providing a name for an attribute which is not correct or does not exist.

Active Directory Specific Errors

**Error: com.server.exception.DBException: Error in bind() from LDAP source: [LDAP: error code 49 - 80090308: LdapErr: DSID-0C09030F, comment: AcceptSecurityContext error, data 525, vece]
javax.naming.AuthenticationException**

The administrator domain name, username, and or password is incorrect in the LDAP Authentication screen.

Error: com.server.exception.DBException: Error in searchForUserList from LDAP plugin: [LDAP: error code 32 - 0000208D: NameErr: DSID-031001C6, problem 2001 (NO_OBJECT), data 0, best match of: '[DN]'] javax.naming.NameNotFoundException

A non-existent DN specified in the Start Search field.

Error: javax.naming.PartialResultException [Root exception is javax.naming.CommunicationException: [server]:[port] [Root exception is java.net.UnknownHostException: [server]]]

An incorrect DN was specified in the Start Search field.

Error: com.server.exception.DBException: Error in searchForUserList from LDAP plugin: [DN]: [LDAP: error code 34 - 0000208F: NameErr: DSID-031001B3, problem 2006 (BAD_NAME), data 8350, best match of: '[DN], '] javax.naming.InvalidNameException

An incorrectly formatted DN was specified.

Error: javax.naming.NameNotFoundException: [LDAP: error code 32 - 0000208D: NameErr: DSID-03100198, problem 2001 (NO_OBJECT), data 0, best match of: "]; remaining name "

This error appears if you do not have Group settings filled in, but have User Search filled in. Some systems do not care, while some systems experience problems with the empty DN.

**Error: Error in bind from LDAP source: [LDAP: error code 49 - 80090308: LdapErr: DSID-0C09030F, comment: AcceptSecurityContext error, data 52e, vece]
javax.naming.AuthenticationException**

Could not authenticate the user trying to log in. This can be the result of an incorrect username or password, or an incorrect prefix and/or suffix specified in the LDAP Authentication screen, depending on the type of LDAP/AD system. Could also mean the authentication type is incorrect. Also an incorrect username attribute or incorrect name attribute can cause this. Common cause of this error is a user trying to log in with DOMAIN\login instead of just login.

Error: javax.naming.NamingException: [LDAP: error code 1 - 000020D6: SvcErr: DSID-03100690, problem 5012 (DIR_ERROR), data 0];

The DN specified in the Start Search tab is incorrect, wrong, or incorrectly formatted.

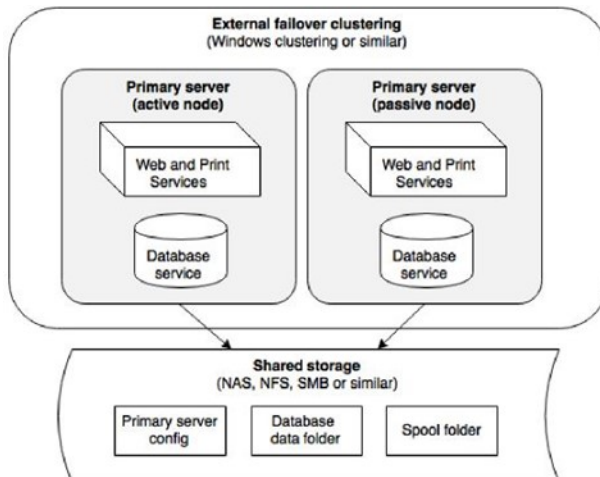
Chapter 8

Clustering for high availability and scalability

With the SafeCom Mobile Print clustering features, you can configure SafeCom Mobile Print for Enterprise scalability through load balancing, multiserver deployments and high availability through failover and redundancy.

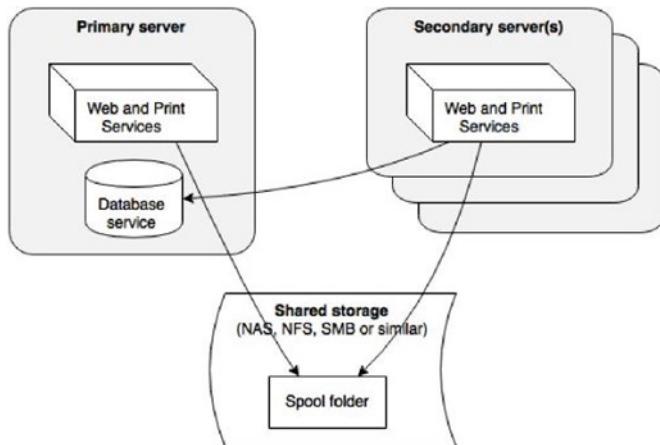
Although numerous cluster configuration options are available, some typical configurations are provided below:

- High availability redundancy with multiple servers in failover cluster.



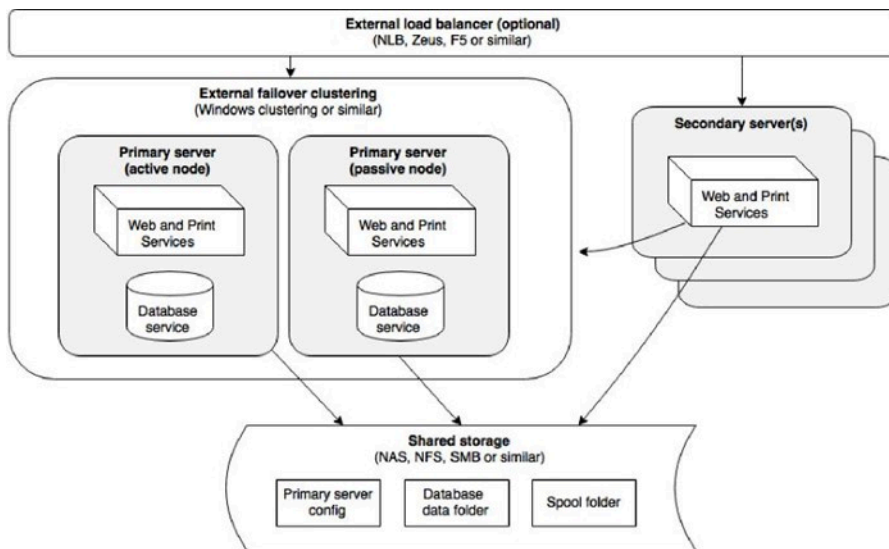
Primary servers in a failover cluster configuration, with one active primary server and any number of passive standby server nodes in case the active fails.

- High scalability with several additional servers for load balancing and job processing.



A single primary server and any number of additional secondary servers for load balancing and job processing for very high print job volumes.

- High availability and high scalability combining both failover clustering and load balancing.



A configuration for highest availability and redundancy, and highest scalability for very large job processing, with multiple primary servers in a failover cluster and multiple secondary servers for scalability behind a load balancer.

The configuration possibilities with high availability and scalability are endless, and these examples and guides are for common configurations only. For the best configuration for a particular project, contact your SafeCom Mobile Print specialist for guidance and recommendations.

Cluster servers overview

When a SafeCom Mobile Print server starts up and connects to the SafeCom Mobile Print database, it will register itself in the SafeCom Mobile Print system.

Servers are continually checked for status. If a server fails, an alert is displayed in the view and a notification email is sent to the administrator notification email address, if configured.



Clicking the server address opens a new browser window with the administration interface of the server.

Server types

There are two types of servers: primary and secondary.

Primary servers

Primary servers run all the SafeCom Mobile Print Web, Print, and Database services, and manage overall internal processes as well as licensing when using Enterprise licenses. A single SafeCom Mobile Print server installation will always run as a primary server.

i There must be only one active primary server in a cluster configuration, because the primary server runs essential database and management tasks.

Secondary servers

Secondary servers run the SafeCom Mobile Print Web and Print services, and are designed to be additional servers for load balancing, additional job processing and printing, or additional servers configured for specific roles, such as servers dedicated to downloading emails and similar.

Possible Functions	Primary	Secondary
Web services	Yes	Yes
Print Service	Yes	Yes
Database Service	Yes	No
Job conversion and printing	Yes	Yes
Web Print	Yes	Yes
Driver Print	Yes	Yes
Email Print	Yes	Yes
Mobile Print	Yes	Yes
Google Cloud Print	Yes	No
Management of Devices	Yes	No
Configuration of Wide Area Mobile Print	Yes	No

Google Cloud Print services run only from the Primary server.

Configuration types

A SafeCom Mobile Print server in a cluster configuration can use either its own configuration, or it can use a configuration shared by multiple servers.

Local configuration

A local configuration means the server uses its own configuration stored locally on the server. It will use printers from the central system database, but all other settings, such as email or authentication configuration, are set locally. This is useful in a cluster configuration when adding additional secondary servers which perform a dedicated role, such as downloading email from a mail server.

Shared configuration


A shared configuration means that the configuration is stored in a shared location such as a network file share or similar, and shared between multiple servers. Configuration can be set from any of the shared servers, using that same shared configuration.

In a cluster configuration with numerous servers with different roles, different groups of servers can share different configurations, for example, a group of secondary servers dedicated to job processing can share their own specific configuration.

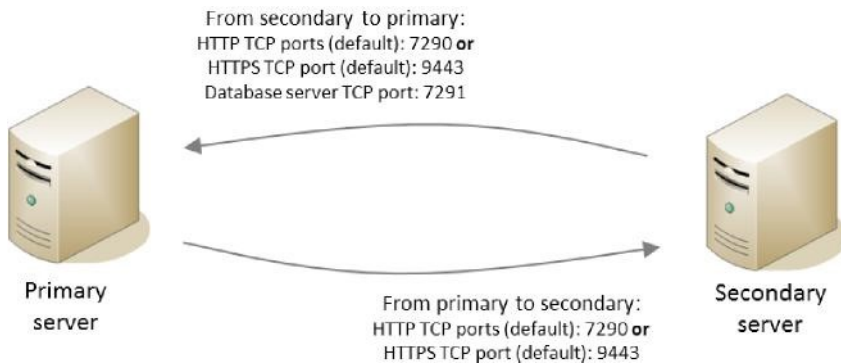
Prerequisites for a cluster configuration

For a successful SafeCom Mobile Print cluster configuration, all servers in the cluster must have stable and fast network connections.

- High speed network, such as 1 Gigabit Ethernet
- Highly available shared storage, such as NAS or SAN
- Firewall ports open for servers:
 - Primary server type:
 - HTTP tcp port (default): 7290
 - HTTPS tcp port (default): 9443
 - Database server port: 7291
 - Secondary server type:
 - HTTP tcp port (default): 7290
 - HTTPS tcp port (default): 9443

 When multiple default ports are listed for a server type, only one of them can apply.

Secondary servers connect to the primary server for job information, licensing validation and similar. The primary server connects to the secondary server for regular status checks.



Configure a primary server

A primary server in a cluster configuration is a standard SafeCom Mobile Print server, running all the usual SafeCom Mobile Print Web, Print and Database services. An existing single SafeCom Mobile Print can automatically act a primary server for other secondary servers in a cluster configuration.

1. Install a primary server simply by running the SafeCom Mobile Print installer, and select to install **Server as part of a cluster configuration**.
2. Select **This server will run the database service**.

This installs a server with the standard Web, Print and Database services, as a standard single SafeCom Mobile Print server.

Open firewall on primary server

Since secondary servers communicate with the database running on the primary server, ensure that firewalls allow incoming traffic on default database TCP port 7291.

SafeCom Mobile Print includes a command line script for easily configuring the Windows firewall on the server.

The script is located in the tools sub folder of the SafeCom Mobile Print installation folder, typically `C:\Program Files (x86)\SafeCom Mobile Print\tools`.

Run this script as administrator and select option 1 to open ports for server.

This creates the necessary rules in the local Windows firewall.

Configure shared spool in primary server

Aside from the normal configuration of SafeCom Mobile Print, such as creating and adding print queues to SafeCom Mobile Print, it is necessary to configure the spool directory where SafeCom Mobile Print stores files received from users are being processed and stored until printing.

1. Open the SafeCom Mobile Print Administrator interface.
2. Go to **General Settings**.

3. Under **Application Settings**, change the application spool folder to a highly available shared storage, accessible by all servers in the cluster.

Example:

```
\\sharedstorage\mobileprint\spool
```

This must be entered as a full path to the directory: either a network share UNC path (for example `\\fileserver\spool`) or a local mapped drive and folder (for example `x:\spool`).

4. Confirm that the user account under which the SafeCom Mobile Print Web service is running has read and write rights to the shared path.

Configure additional secondary servers

Secondary servers run the SafeCom Mobile Print Web and Print services, and are designed to be additional servers for load balancing, additional job processing and printing, or additional servers configured for specific roles, such as servers dedicated to downloading emails and similar.

1. Install a secondary server simply by running the SafeCom Mobile Print installer, and select **Server as part of a cluster configuration**.
2. Select **This server will connect to an existing database** and enter the server IP/hostname of the primary server or primary server failover cluster IP address.
3. Click **Next**.
A connection is attempted to the database service, which may take a few seconds.
4. If a connection cannot be established and an error is shown, either go back and change the parameters or continue.
Be aware that the secondary SafeCom Mobile Print server will not function without a working connection to the primary database.

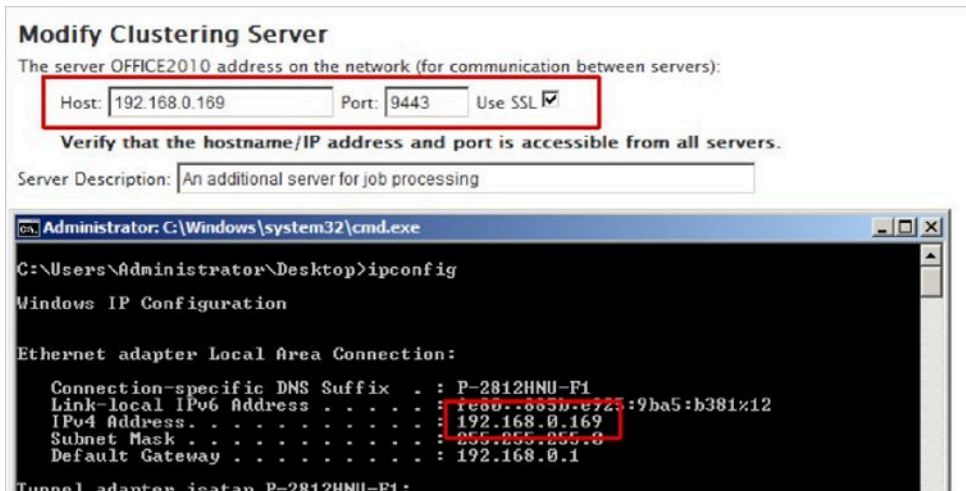
Configure shared spool in secondary server

1. After installation, open the SafeCom Mobile Print Administrator interface on the secondary server.
2. Go to **General Settings**.
3. Under **Application Settings**, change the **Application spool folder** to the same shared storage as the primary server.
Example:

```
\\sharedstorage\mobileprint\spool
```
4. Confirm that the user account under which the SafeCom Mobile Print Web service is running has read and write rights to the shared path.

Modify secondary server's cluster configuration

1. In SafeCom Mobile Print Admin, go to **Clustering** and edit the new server's entry.
2. Enter the secondary server's hostname or IP address and port on the network, so other servers in the cluster can communicate with the server.
For your own convenience, you may want to enter a server description as well.



3. Select whether the secondary server's configuration is local to the server or if it should use a shared configuration.
 - Specify the parent server as a specific primary server if there are no failover cluster configuration or external load balancers included in the configuration.
 - Alternatively, specify the parent server if the primary server is behind a central failover cluster IP address/hostname or an external load balancer.

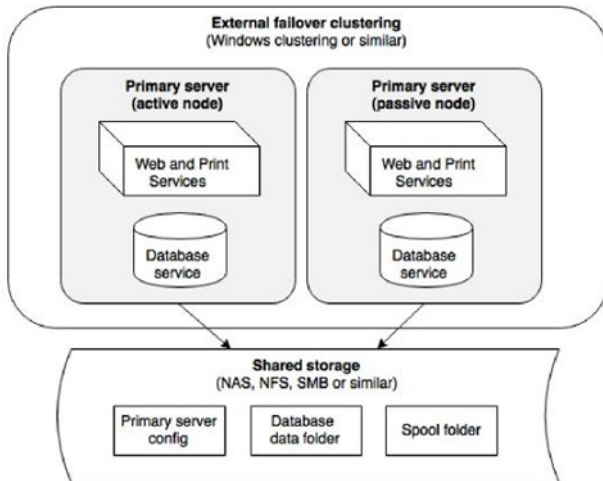
Replicate printers from primary server

Printers that exist on the primary server, must be replicated to the secondary server.

See [Replicate printers across all servers](#) for more information.

Install SafeCom Mobile Print in a Windows failover cluster

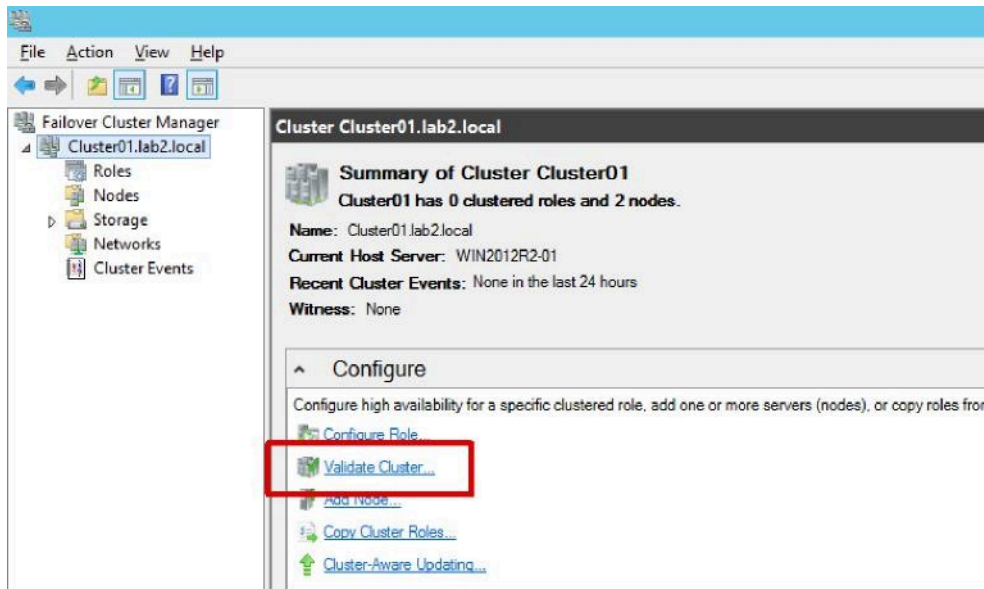
For high availability and redundancy, SafeCom Mobile Print can be installed in a Windows active/passive failover cluster, using Windows clustering services.



This guide does not cover the core setup and configuration of a Windows cluster, because comprehensive information already exists on the subject, but assumes that Windows clustering services have been successfully installed.

Validate cluster

1. Begin by validating the cluster.

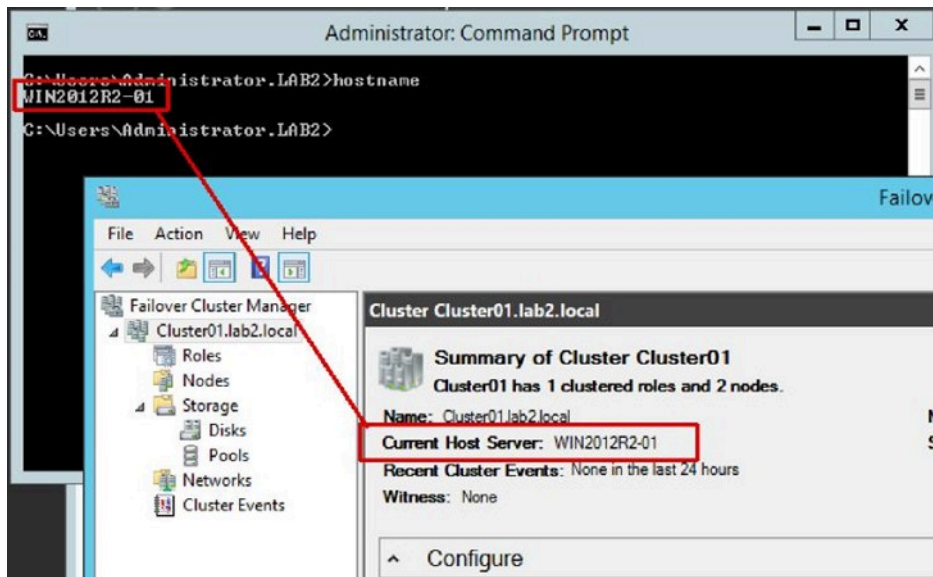


2. Select **Run all tests**.
3. Include all cluster storage devices in the validation tests.
The tests must complete successfully without errors for SafeCom Mobile Print to run successfully in a failover cluster configuration.

Install SafeCom Mobile Print on first active node

SafeCom Mobile Print must be installed on the active node.

1. To make sure that SafeCom Mobile Print is installed on the active node, ensure that the current host is the current host owner.



2. Confirm that the current active node has access to all relevant cluster disk storage.
3. Now run the installer, selecting any local directory on the server.
4. Select **Server as part of a cluster configuration**.
5. Select **This server will run the database service**.

Change service logon accounts

1. After the installer finishes, open the Windows services and change the logon account of the SafeCom Mobile Print Web service and the SafeCom Mobile Print Data service.

i The SafeCom Mobile Print Print Service must always run as localsystem. The service logon account used must have full read/write rights to the shared cluster storage.

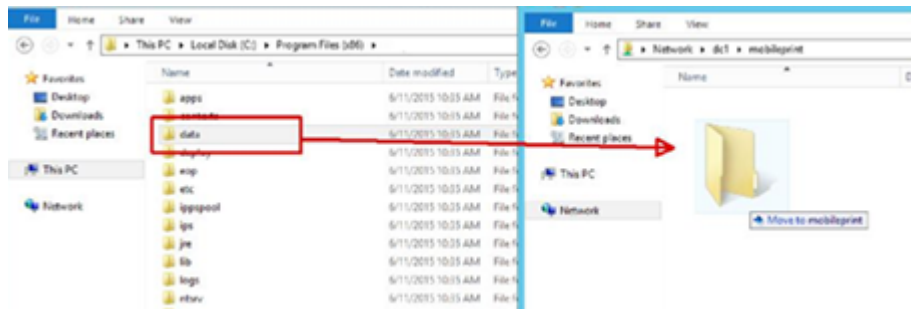
2. Restart services to confirm that the services can successfully start under the new accounts, then stop all services (start and stop of services will be controlled by the cluster services).

Move database to shared storage

As the database will be run by any of the nodes in the cluster, the database must be placed in a shared storage or cluster disk, accessible to all nodes in the failover cluster.

1. With services confirmed stopped, move the \data subfolder of the SafeCom Mobile Print installation folder to the shared storage (for example \\dc1\mobileprint).

The default SafeCom Mobile Print installation folder is at `C:\Program Files (x86)\SafeCom Mobile Print`.



2. Browse to the `\ntsrv` folder under the SafeCom Mobile Print installation folder.
3. Open the `eopdata.conf` file in an editor, for example Notepad++.
4. Modify the following entry from `wrapper.java.additional.1=-Dderby.system.home=../data` to either the absolute path of the new location of the data folder (for example, `wrapper.java.additional.1=-Dderby.system.home=\\dc1\mobileprint\data`) or another shared cluster disk path, such as `z:\mobileprint\data`.
5. Save the file.

If the overall SafeCom Mobile Print cluster configuration is planned to include additional secondary role servers, ensure that the firewall on the primary node has been configured to allow for incoming connections on the database port 7291 (default). See [Open firewall on primary server](#) about configuring Windows firewall with a script.

Repeat the following steps on all additional nodes:

6. Run the installer, select Server is part of cluster and the server will run the database service.
7. Change logon account on SafeCom Mobile Print Web and Database to the same service account.
8. Stop all SafeCom Mobile Print services.
9. Edit the `\ntsrv\leopdata.conf` to have the SafeCom Mobile Print Data service use the shared `\data` folder.

When all nodes have the SafeCom Mobile Print services installed, configure the SafeCom Mobile Print cluster resource in the Windows cluster services.

10. On the current cluster owner node, open **Windows Failover Cluster Manager**, select the cluster, and click **Configure Role**.
11. Enter a name and the address for the SafeCom Mobile Print primary cluster as it will be accessed by users and other secondary SafeCom Mobile Print servers.
12. Select any storage as needed for the cluster configuration.
13. Skip the section on Windows registry replication, as SafeCom Mobile Print does not store values in the registry.

With the cluster resource created and first service added, add SafeCom Mobile Print Data and SafeCom Mobile Print Print Services to the cluster resource.


14. Under the **Roles** section, right-click the cluster resource, then click **Add Resource > Generic Service**.
15. Select the SafeCom Mobile Print Data service
16. Repeat for the SafeCom Mobile Print Print Service.

17. Confirm that all services have been added by selecting the cluster group and viewing the resources, and bring all services online.

The SafeCom Mobile Print web interface is now accessible on the cluster IP address. If not accessible, confirm that there are no firewalls blocking access on the current active node, otherwise check logs on the active node.

Modify primary cluster nodes configuration

Next configure the primary nodes to share the same configuration, so when the active node changes, everything remains the same.

1. Confirm the current active node and go to the **Clustering** section of the SafeCom Mobile Print Admin interface, and click to edit  the current active node.
2. Enter the cluster IP address under **Host** and a description, and set the store configuration in a location accessible by all nodes in the cluster.

This shared location can either be a network share, or a cluster disk which moves with the active node.


The server WIN2012R2-01 address on the network (for communication between servers):

Host: Port: Use SSL

Verify that the hostname/IP address and port is accessible from all servers.

Server Description:

The server WIN2012R2-01 is a:

Primary server 

With its configuration stored:

Locally on WIN2012R2-01 server only

Shared on remote path:

3. Repeat this for all other primary cluster nodes.
4. Enter the cluster host, description, set it as a primary server and to use the same shared configuration.
5. Save changes.

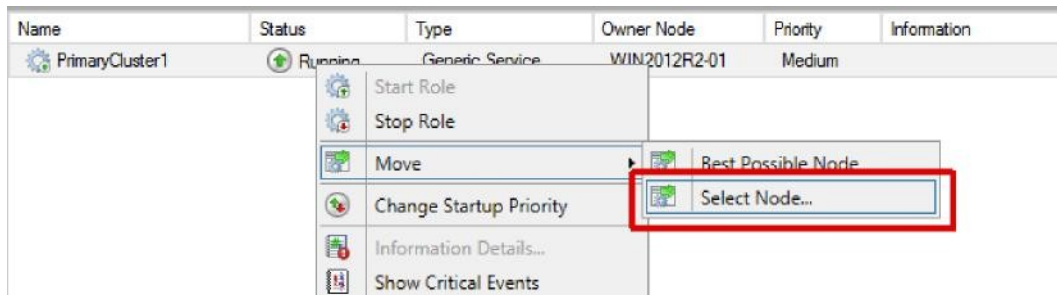
When returning to the list, a warning is displayed that only a single primary server can run at the same time. With the failover configuration in place, Windows starts and stops services as necessary, so only a single active node exists.

Change the primary server's spool folder

The spool directory of SafeCom Mobile Print, where print jobs are held while being processed, awaiting release and so forth, must be located in a shared storage, such as network share or cluster disk volume that moves with the active node.

1. Create a dedicated folder, for example `\\dc1\mobileprint\spool`, and then go to **General Settings**.
2. Under Application Settings change the Application spool folder to the shared storage.

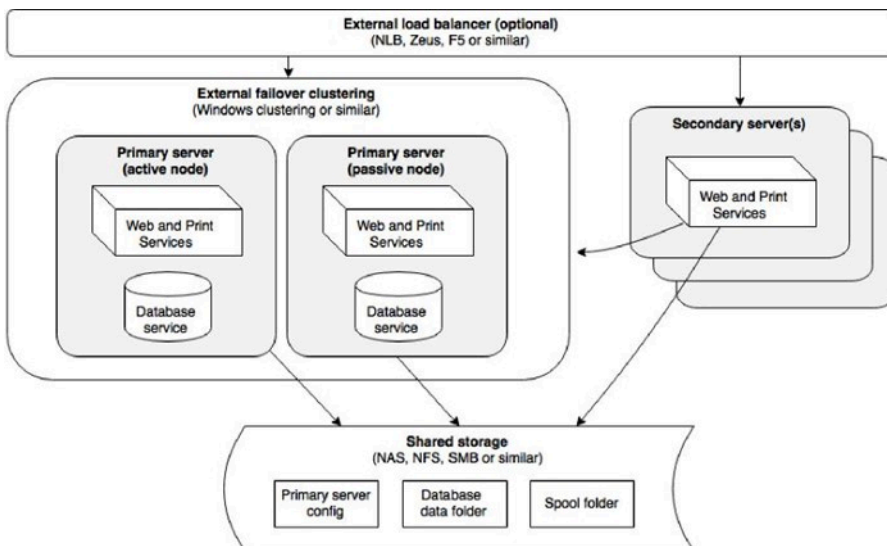
3. Confirm that the user account under which the SafeCom Mobile Print Web service is running has read and write rights to the shared path.
The cluster configuration is now complete.
4. It is strongly recommended to thoroughly test failover, by simulating failures and changing the active node several times, confirming in between each switch, that SafeCom Mobile Print is functioning correctly.



i Ensure that all printers created on the active primary server are replicated across all nodes in the failover cluster, or printing will fail when nodes failover.

Add external load balancer for high front-end scalability

SafeCom Mobile Print clusters can be combined with external load balancing, to achieve very high scalability and redundancy.



Use an external load balancer, when many users will access the front-end interfaces, such as Web Print, Driver Print or Mobile Print, to balance the requests between many servers behind the load balancer.

Configure primary and secondary servers as needed, as described above, then add an external load balancer, such as [F5](#) or [ZEVENET](#), which can be either a physical appliance or a software-based load balancer, or [Windows NLB](#).

The configuration possibilities with high availability and scalability are endless, and these examples and guides are for common configurations only. For the best configuration for a particular project, contact your SafeCom Mobile Print specialist for guidance and recommendation.

Replicate printers across all servers

Since any server in a cluster configuration can be sending print jobs to printers, all servers are required to have all print queues installed.

In many cases, customers using a single "follow me" print queue, this is trivial, since there has to be only a single print queue on each server. But for customers with thousands of printers, it is impractical to manually create and manage print queues across servers.

Fortunately, it is very simple to script print replication across many servers using the Windows Print Migration tools.


Windows Print Migration Printbrm.exe command-line tool

The Windows print migration tool, `printbrm.exe`, is an excellent tool for replicating printers across multiple servers.

For detailed information about print migration on Windows servers, see:

- [Migrate Print Servers](#)
- [Printbrm.exe Command-Line Tool Details](#)

The migration tool is included in the Print Management Windows tools that come with the Print Server role service on Windows servers.

 For Print Migration to work using `printbrm.exe`, at least one printer must be created and shared on all servers involved in replication.

1. Add the **Print and Document Services** Role on all servers.
2. Check the **Print Server** role service.
3. Create at least one print queue on all servers and share this queue.
4. Do NOT publish the shared printer in the domain directory, to avoid users printing to the queue directly.

With the Print Management tools installed, we can replicate printers.

5. Open a command prompt as administrator, as a user with administrative rights on source and destination server on the source server, containing all the printers to replicate.
6. Back up the printers using the command line:

```
Printbrm.exe -b -s \\servername -f printers.printerexport
```

7. Now in the same command line window, run the command to restore the backup file to the new destination server.

```
Printbrm.exe -r -s \\newserver -f printers.printerexport
```

The above commands can be included in a BAT or CMD file and be scheduled using Windows Task Manager, for example:

```
@echo off
C:\Windows\System32\spool\tools\printbrm -b -s \\primary -f c:\temp\printer
s.printerexport C:\Windows\System32\spool\tools\printbrm -r -s \\secondary1 -f
c:\temp\printer s.printerexport C:\Windows\System32\spool\tools\printbrm -r -s
\\secondary2 -f c:\temp\printer s.printerexport
```

Printers now exist on destination server, identical to the source.

Licensing in clustered configurations

SafeCom Mobile Print clustering features are available in Trial, Professional and Enterprise license levels. No license key required to deploy a SafeCom Mobile Print cluster during the initial trial license.

If using a Professional license, a Professional license key must be entered on each server in the cluster configuration.

If using an Enterprise license, an Enterprise license key is only needed on the first primary server. All other servers in the cluster configuration validate their license from the parent server, the primary server containing the Enterprise license, and it is not necessary to enter any license keys on additional servers.

SafeCom Mobile Print clustering in high-availability virtual configurations

Virtual server platforms such as VMWare, Hyper-V and Xen offer features to achieve very high availability and very quick disaster recovery of individual virtual servers, and are generally recommended as part of a disaster recovery policy.

SafeCom Mobile Print can work seamlessly with virtual machine platforms, as the use of a virtual server is transparent to the SafeCom Mobile Print server application. This includes Windows print servers with Hyper-V high availability.

The high availability features offered by the virtual platforms, generally only apply to the individual virtual server instance as a whole, and does not in itself provide an application level redundancy, so a multiserver SafeCom Mobile Print cluster configuration is still recommended, if high application availability or redundancy is required.