



# Kofax Equitrac Print Stream Encryption Guide

Version: 6.4.0

Date: 2023-03-11

©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

Print Stream Encryption Overview.....	4
About IPP.....	4
About HTTPS.....	4
About Windows Encrypting File System (EFS).....	5
Printing from a workstation to shared printer with Internet (IPPS) port.....	5
Configure SSL/TLS.....	6
Configure the print server.....	6
Configure workstations.....	7
Printing from a workstation to TCP/IP printer with DRC.....	7
Printing to an I-Queue.....	8

# Print Stream Encryption Overview

Print data can take various routes when traveling over the network from applications to print devices. When passing a print stream over the network, from print application to print server or printer, secure IPP (Internet Printing Protocol) is used. Whenever a print stream is stored on disk while waiting to be released for printing, it is encrypted using Windows Encrypting File System (EFS).

## About IPP

IPP (Internet Printing Protocol) is a protocol for passing print data from one point on the network to another. For instance, when printing a document from an application to a print server on the network, or when the server sends data to an actual printer on the network. IPP is utilized by configuring windows printer to print to an "Internet Port". This type of port contains an HTTP URL to reach a printer driver installed on the print server machine or on the printer directly.

Typically, when printing to a shared printer on the server, the URL has the following format:

```
http://[PrintServerName]/printers/[Print Driver Name]/.printer
```

With this type of port, the Windows printing subsystem on the workstation communicates to an HTTP server (such as IIS) running on the print server machine, using HTTP protocol. The HTTP server prints to an actual printer using the Windows printing subsystem.

When printing directly to printer this URL has the following format:

```
http://yourprintername/printer
```

## About HTTPS

HTTPS (Hypertext Transfer Protocol Secure) is a protocol for secure communication over a computer network. In HTTPS, the client and server endpoints use security certificates to validate each other, and use a set of encryption keys to encrypt data before passing it over the network and decrypt that data when receiving it.

To secure the print stream from workstation to server, or directly to the printer, SSL/TLS must be enabled on the HTTP server and the printer, and change the "Internet Port" URL to use secure HTTP protocol (HTTPS).

When using HTTPS, the URLs have the following formats:


```
https://[PrintServerName]/printers/[Print Driver Name]/.printer
```

```
https://yourprintername/printer
```

## About Windows Encrypting File System (EFS)

With Windows Encryption File System (EFS), any file or any folder (and all subfolders and files) can be encrypted. When encrypted, this file or folder becomes available only to the logged-in user who encrypted it. Users logged into the same machine or accessing the file system on that machine from network, cannot access files or folders encrypted by other users.

To encrypt a file or folder, do the following:

 Ensure the appropriate user is logged into the machine. If enabling encryption on EQSpool folder the appropriate user would be the user under who's credentials the DRE service is running).

1. Right-click the file or folder.
2. Select **Properties**.
3. Click the **Advanced** button under the **Attributes** section.
4. Select the "**Encrypt contents to secure data**" checkbox.
5. Click **OK** to close the Advanced Attributes window.
6. Click **OK** on the file/folder Properties window.
7. An **Encryption Warning** dialogue box appears. The message will vary depending on whether you are trying to encrypt just a file or an entire folder:
  - For a file, the message provides two choices:
    - Encrypt the file and the parent folder (recommended)
    - Encrypt the file only
    - Optionally, check **Always encrypt only the file** for all future file encryption actions. If you check this option, the message box will not appear for future file encryptions. Unless you are sure of that choice however, I recommend you leave this box unchecked.
  - For a folder, the message provides two choices:
    - Apply changes to this folder only
    - Apply changes to this folder, subfolders and files
8. After making your selection, click **OK**.

## Printing from a workstation to shared printer with Internet (IPPS) port

There are number of steps required in order to configure the printer, print server and workstations for storing the encrypted print stream and passing it over the network encrypted.

To establish the encrypted print stream, do the following:

1. Ensure the printer is configured for **SSL/TLS**.
2. Export the **security certificate** from the printer.
3. Import the printer's security certificate at the print server.
4. Create or acquire a **website security certificate**. This can be done by using IIS manager to create a self-signed certificate.

**i** If a self-signed certificate from IIS is not enough to create IPPS printers on workstations, you can create a self-signed certificate using [openssl tools](#) instead of IIS.

5. Install the **website security certificate** on the print server and configure IIS to use the certificate.
6. Ensure that both Windows **Print and Document Services and Web Server (IIS)** role are installed.
7. Add **Internet Print Client** feature on the server and the workstations.
8. At the print server, add a new shared printer and configure the port for **IPPS**.
9. At each workstation, import the same certificate installed on both the print server and IIS.
10. At each workstation, add a new printer configured to print to the shared printer using IPPS.

## Configure SSL/TLS

The printer's user interface for configuring and enabling SSL/TLS is different between manufacturers and models. However, if supported, administrators should have the ability to enable SSL/TLS and to create/configure/export a security certificate. Refer to the manufacturer's documentation on how to access and configure SSL/TLS and security certificates.

## Configure the print server

To configure the print server, do the following:

1. Open **Server Manager**, and navigate to **Roles > Print and Document Services**.
2. Install the **Web Server (IIS)** role, the **Print Services** role, and the **Internet Printing** role service in the Print and Document Services role.
3. To prepare the server for adding an IPPS printer, install the printer's security certificate. Follow the procedure in this [knowledge based article](#) from Microsoft to import the certificate from the print server.  
Another way to import the certificate is by using MMC. See [Printing from a Workstation to TCP/IP Printer with DRC](#).
4. Add a printer with a standard **TCP/IP port** to use with the print queue, and then print a test page when finished. Communication between the print spooler and DRE is encrypted using TLS.
5. In System Manager, select a physical device, and click the **Output Options** button on the physical device summary. Change the **Protocol** to **IPP** and enter the **IPPS URL** for the device (e.g. <http://printerIP:631/printer>). The URL should contain the name of the printer matching the one in security certificate.

6. Acquire a certificate or create a self-signed certificate using IIS. Workstations printing to this server will import this certificate. Follow these instructions to [import the certificate](#).
7. To create a self-signed certificate, do the following:
  - a. Open the **IIS Manager** and select the appropriate connection.
  - b. Double-click the **Server Certificates** icon.
  - c. Click the **Create Self-Signed Certificate** link on the right pane.
  - d. On the **Create Self-Signed Certificate** dialog box, enter a name, and click **OK**.

## Configure workstations

To enable the Internet Printing Client feature on the computer, do the following:

1. Open **Programs and Features** from the Control Panel.
2. Click **Turn Windows features on or off**.
3. In the **Windows Features** dialog box, expand **Print and Document Services**, select the **Internet Printing Client** checkbox, and then click **OK**. The Print Spooler service (or the System if prompted) must be restarted.
4. Follow the procedure in this [knowledge based article](#) from Microsoft to import the certificate from the print server.
5. Open the Windows Add Printer wizard, and add a network printer configured to use HTTPS.
  - a. Click Add a network, wireless or Bluetooth printer.  
On the Find a printer by name or TCP/IP address screen, enter an HTTPS URL in the following format:  
`https://yourprintservername/printers/yourprintername/.printer`  
Follow the prompts on the wizard to complete adding the printer.

The Add printer wizard will add a new printer configured to send print stream over HTTPS connection to server.

## Printing from a workstation to TCP/IP printer with DRC

1. Enable the Internet Printing Client feature on the computer.
  - a. Open **Programs and Features** from the Control Panel.
  - b. Click **Turn Windows features on or off**.
  - c. In the **Windows Features** dialog box, expand **Print and Document Services**, select the **Internet Printing Client** checkbox, and then click **OK**. The Print Spooler service (or the System if prompted) must be restarted.
2. Import the certificate from the printer to **Trusted Root Certificates** on the workstation. Follow these instructions to [import the certificate](#).

OR

3. Another way to install printer's certificate to Trusted Root Authorities is to use MMC (Microsoft Management Console).
  - a. Click the **Start** button, and type **mmc** in the Start Search box, and then press **Enter**.
  - b. On the MMC Console, navigate to **File >Add remove snap-in**.
  - c. Select **Certificates** from the snap-ins list, and click **Add**.
  - d. Select **Computer account** and click **Next**.
  - e. Leave the default setting **Local computer** and click **Finish**.
  - f. Click **OK**.
  - g. Under **Certificates (Local computer)**, right-click **Trusted Root Certificates Authorities**, and select **All tasks >Import** from the menu.
  - h. Click **Next** on the **Certificate Wizard Welcome** screen.
    - i. Click **Browse** to open a certificate file previously exported from the printer, and click **Next**.
    - j. Confirm the **Certificate store** location, and click **Next**.
    - k. Click **Finish**.
4. Open the Windows Add Printer wizard, and add a network printer configured to use HTTPS.
  - a. Click **Add a network, wireless or Bluetooth printer**.
  - b. On the **Find a printer by name or TCP/IP address** screen, enter an HTTPS URL in the following format: `https://yourprintername/printer`
  - c. The Add Printer wizard will connect to the printer and prompt for driver location.
  - d. Follow the prompts on the wizard to complete adding the printer.

Print jobs held for release will be stored in the following folder:

C:\Windows\System32\config\systemprofile\AppData\Local\Equitrac\Equitrac Platform Component\EQDRESrv\EQSpool.

This folder should be encrypted using EFS. See [About Windows Encrypting File System \(EFS\)](#).

## Printing to an I-Queue

When printing to an I-Queue, the print job may be held for release and then printed. While waiting for release, print jobs are stored in folder:

C:\Windows\System32\config\systemprofile\AppData\Local\Equitrac\Equitrac Platform Component\EQDRESrv\EQSpool.

This folder should be encrypted using EFS. See [About Windows Encrypting File System \(EFS\)](#). When a job is ready to be released, the DRC running on the workstation reads the print job from a file and sends the job over the network to the DRE that is associated with the printer set to release the job. To ensure the print job is passed with encryption over the network, SSL must be enabled to establish communication between our services. See [Configure SSL/TLS](#).