HP Smart Card SIPRNet and NIPRNet Solutions for US Government using HP Large Format Printers

Administrator's Guide

SUMMARY

The following sections provide details for this topic.

About this edition

Edition 2

Legal notices

The information contained herein is subject to change without notice.

The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Table of contents

1 Introduction

The HP SmartCard NIPRNet Solution for US Government and the HP SmartCard SIPRNet Solution for US Government are designed to optimize security in imaging and printing environments for the US government.

NOTE: LDAP Channel Binding and LDAP signing features are not supported at this moment.

Please consult with your network administrator for the details.

2 Getting started

The following sections provide details for this topic.

Prerequisites

The following outlines the necessary prerequisites.

1. The root and intermediate CA certificates that issued the Domain Controller (Active Directory) certificate.
2. A compatible Smart Card and HP Smart Card reader.
3. Update the firmware of the printer to the latest version.

Supported Card Readers

The following is a list of the Supported Card Readers.

- HP SmartCard US Govt NIPRNet Solution: CC543B
- HP SmartCard US Govt SIPRNet Solution: F8B30A

Supported Large Format printers

The following is a list of the HP Large Format Printers that are compatible with the HP SmartCard SIPRNet/NIPRNet Solution for US Government.

- DesignJet T2600
- DesignJet XL 3600
- DesignJet XL 3800
- PageWide XL 3950
- PageWide XL 4250
- PageWide XL 3920
- PageWide XL 4200
- PageWide XL 4700
- PageWide XL 5200
- PageWide XL 8200
- PageWide XL Pro 5200
- PageWide XL Pro 8200

- PageWide XL Pro 10000

Installing the HP SmartCard NIPRNet or SIPRNet Solution

Follow the instructions in the order presented to install the HP SmartCard reader on your printer.

For more information, refer to the Installation Guide (c04797700).

IMPORTANT: Before installing the HP SmartCard reader, update the printer firmware to the latest version.

1. Turn off the printer.
2. Locate the HIP pocket of your printer (the following images use the HP DesignJet T2600 as reference). Remove the HIP pocket cover.

3. Install the supported HP Smart Card reader.

4. Turn on the printer.

3 HP DesignJet XL 3800

If you are setting up the HP DesignJet XL 3800 printer model, please follow the instructions in this section. For other printers models, please refer to Other supported printer models on page 10.

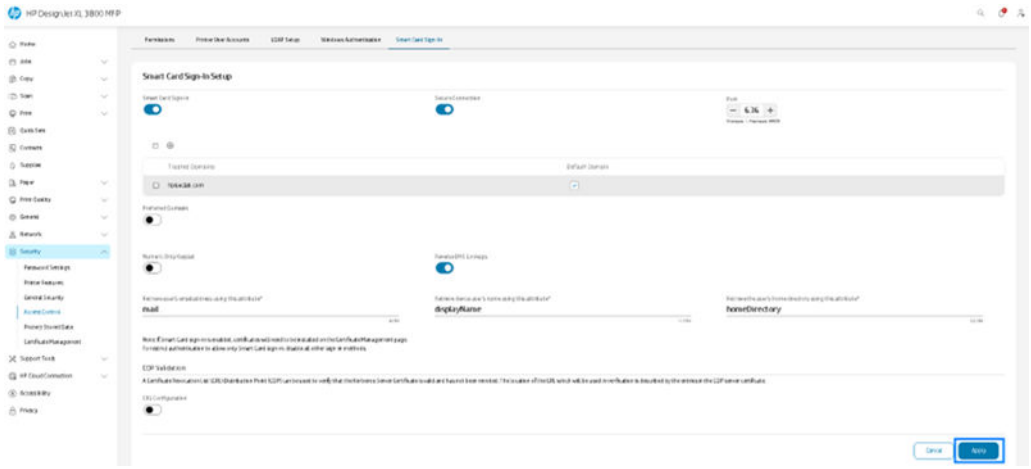
Configuring Smart Card sign in

The following sections provide details for this topic.

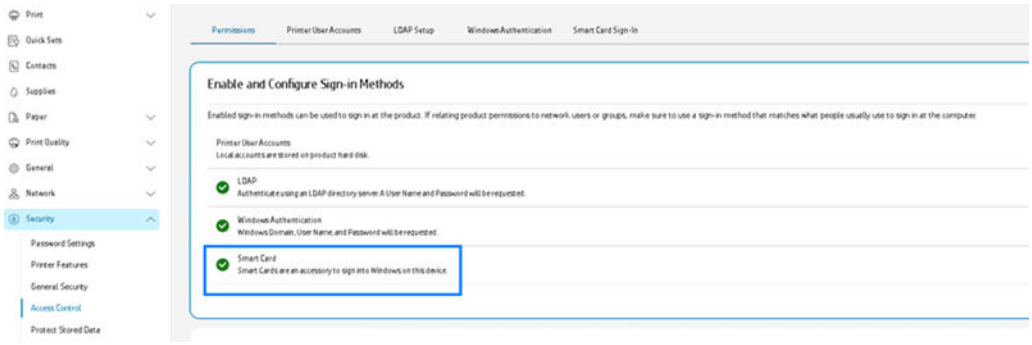
Setting up Smart Card sign-in

Follow the instructions to configure the Smart Card authentication on a compatible DesignJet or PageWide XL printer.

1. From the printer EWS, enter **Security** > **Smart Card sign-in configuration**.



2. After setting up the Smart Card sign-in, ensure that Smart Card sign-in methos is enabled.

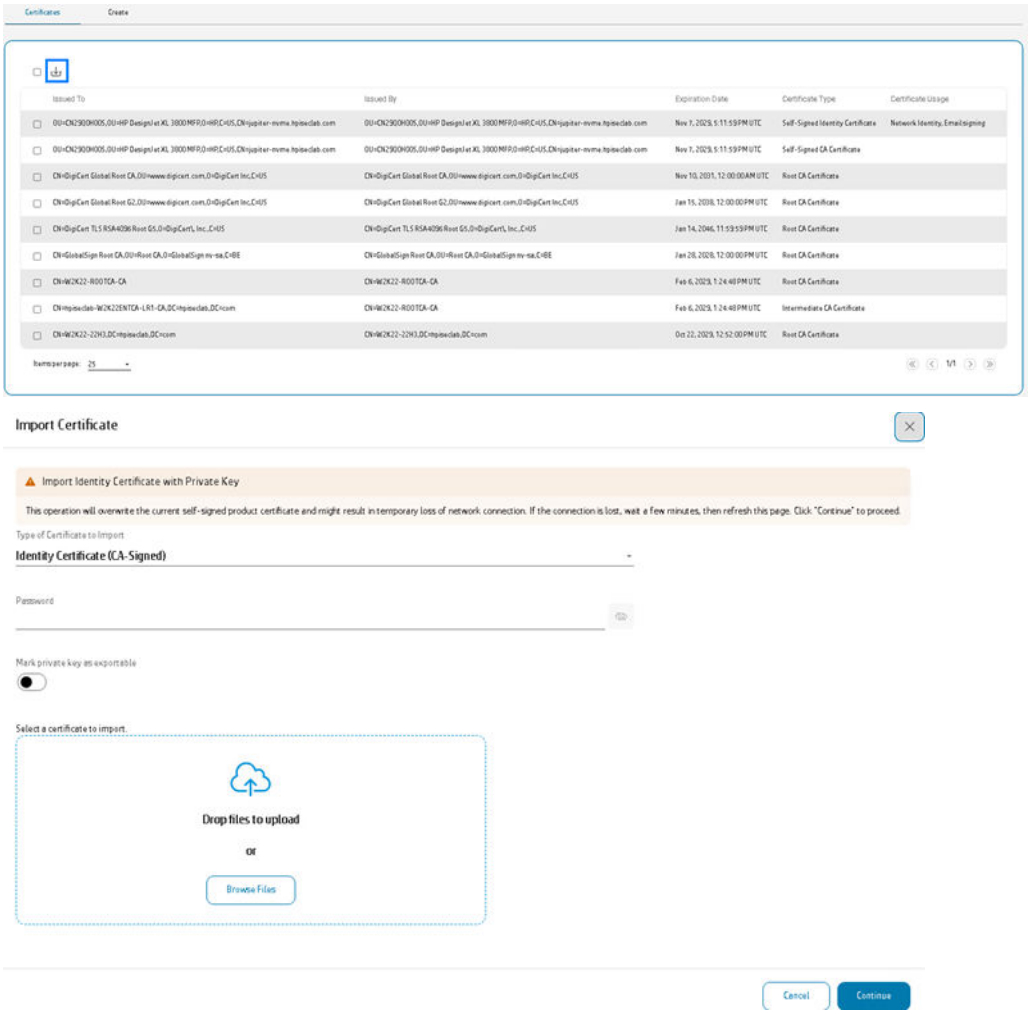


Importing CA certificates

Smart Card sign-in requires the printer to trust the authentication server (Domain Controller). Trust is established by exchanging x509 certificates. During authentication, the Domain Controller will present its certificate to the printer, which will then verify if that certificate is trusted. For the certificate to be trusted, you must import the root and intermediate CA certificates that issued the Domain Controller certificate.

Follow the instructions to import the root and intermediate CA certificates that signs the Domain Controller certificate.

- From the printer EWS, enter Security > Certificate settings, and click **Import**.



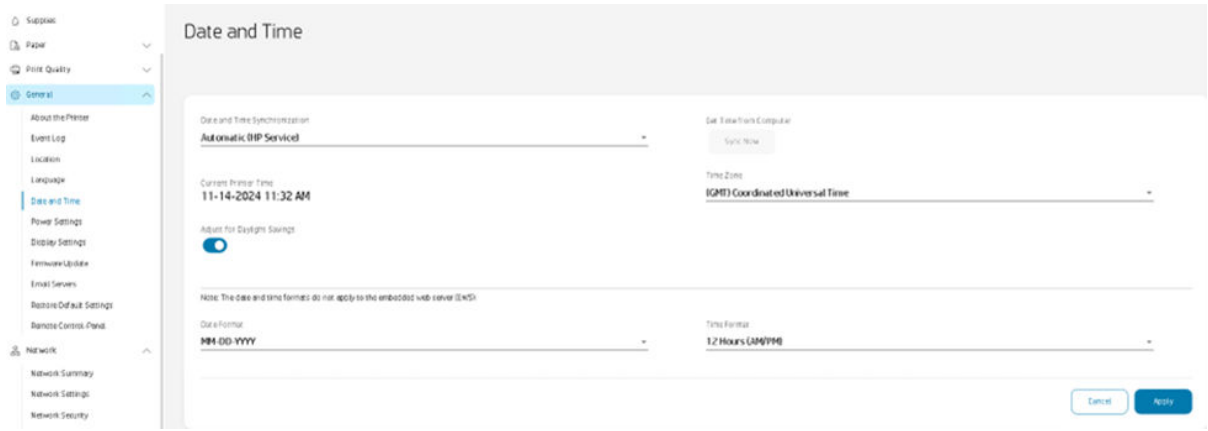
Setting up date and time

Smart Card sign-in uses Kerberos authentication protocol, which requires the date and time of the client (printer) and the server (Domain Controller) to be synchronized. Normally, a time difference of up to 5 minutes is permitted.

Follow the instructions to configure the date and time of the printer and ensure that Kerberos authentication works properly.

- From the printer EWS, enter **Settings** > **Date and time**, and follow one of the approaches outlined:

- If the printer is connected to the internet, select Automatic, HP service under Date and time synchronization.



Configuring user roles for Smart Card users

Follow the instructions to configure the user roles/permissions that Smart Card users will receive after signing in with their Smart Card.

1. From the printer EWS, enter **Security** > **Access Control**.
2. **Smart Card sign-in configuration** will appear with status **On**.

3. Scroll down to **Relationships Between Network Users or Groups and Printer Permissions** and select the default role that you want the user to receive when authenticating with their Smart Card.

4. To apply a custom permission set for specific users or groups, use the Windows sign in method when creating a new relationship.

Setting up Smart Card as the default sign in method

The following sections provide details for this topic.

Setting up Smart Card as the default sign in method for a specific feature

Follow the instructions to set the Smart Card as the default sign in method for a specific feature. Once complete, the printer will prompt you to sign in with your Smart Card by default when accessing the desired feature on the front panel.

1. From the printer EWS, enter **Security** > **Access Control** > **Permissions**.
2. Locate the desired feature under **Sign-In** and **Permissions Policies**.
3. Change the sign in method found in the rightmost column to **Smart Card**.

4. Apply changes.

Setting up Smart Card as the system-wide default sign in method

Follow the instructions to set Smart Card as the global default sign in method for a specific feature. Once complete, the printer will request you to sign in with your Smart Card by default when accessing a feature on the front panel – unless the feature has a specific default sign in method configured.

1. From the printer EWS, enter **Security** > **Access Control**.
2. Under **Sign-In and Permissions Policies** > **Sign-in method**, select **Smart Card**.

3. Click on **Apply**.

Email signing and encryption

This feature is not supported by HP DesignJet XL 3800.

4 Other supported printer models

If you are setting up other printer model than HP DesignJet XL 3800, please follow the instructions in this section.

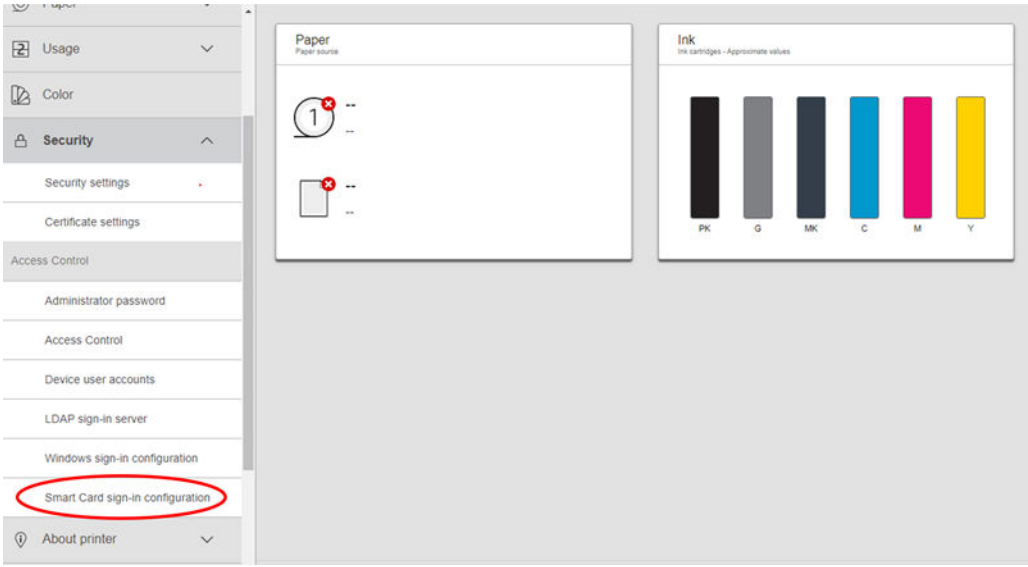
Configuring Smart Card sign in

The following sections provide details for this topic.

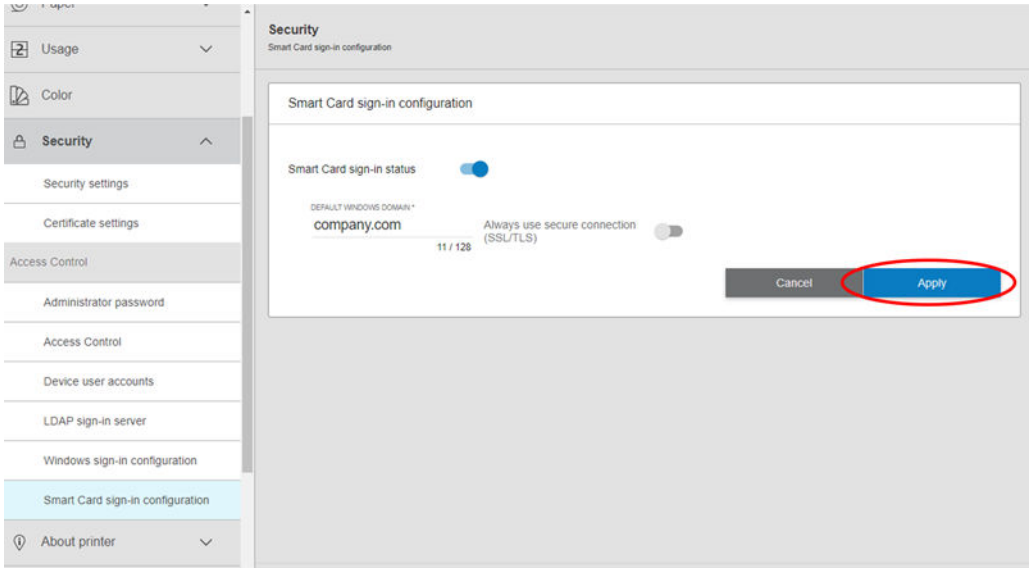
Setting up Smart Card sign-in

Follow the instructions to configure the Smart Card authentication on a compatible DesignJet or PageWide XL printer.

1. From the printer EWS, enter **Security** > **Access Control** > **Smart Card sign-in configuration**.



2. Turn on **Smart Card sign-in status** and input **Default Windows domain** and click **Apply**.

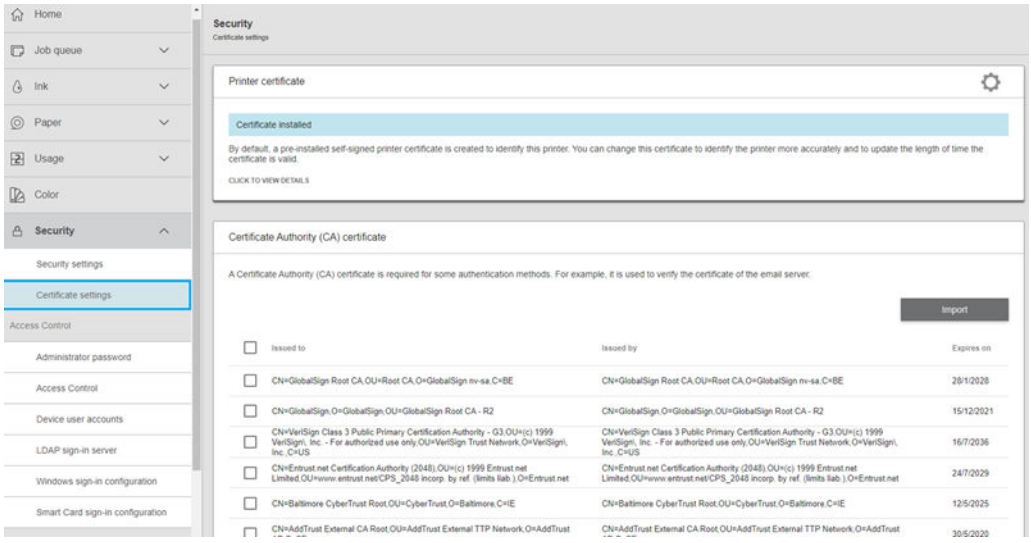


Importing CA certificates

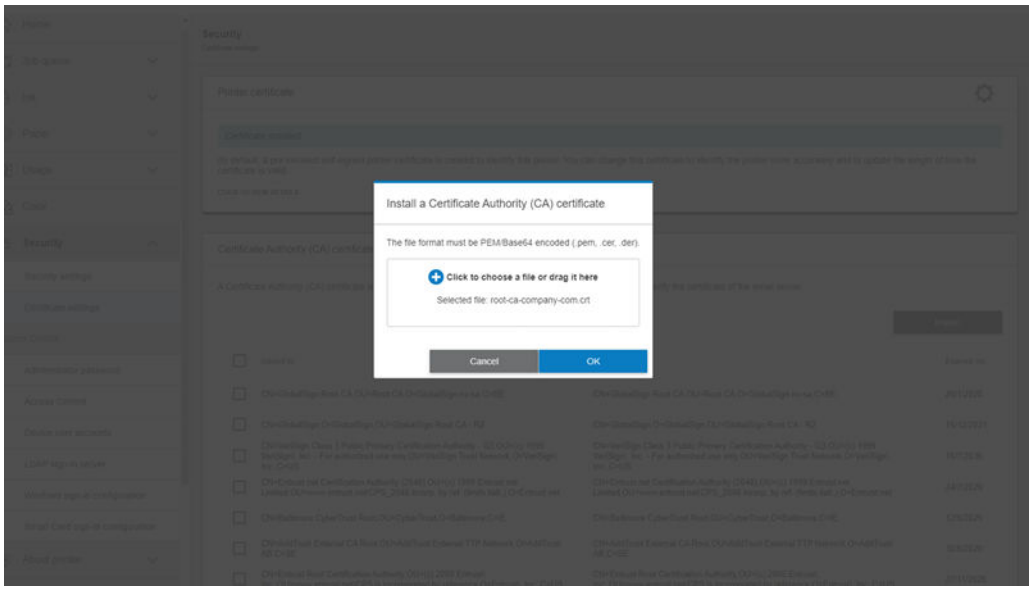
Smart Card sign-in requires the printer to trust the authentication server (Domain Controller). Trust is established by exchanging x509 certificates. During authentication, the Domain Controller will present its certificate to the printer, which will then verify if that certificate is trusted. For the certificate to be trusted, you must import the root and intermediate CA certificates that issued the Domain Controller certificate.

Follow the instructions to import the root and intermediate CA certificates that signs the Domain Controller certificate.

1. From the printer EWS, enter Security > Certificate settings, and click **Import**.



2. Select the CA file to import and click **OK**.



3. The root CA is now imported.

4. Follow the same process to import all intermediate certificates.

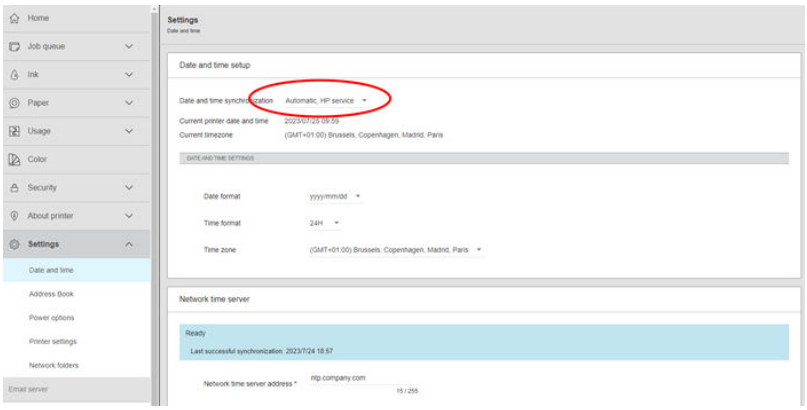
Setting up date and time

Smart Card sign-in uses Kerberos authentication protocol, which requires the date and time of the client (printer) and the server (Domain Controller) to be synchronized. Normally, a time difference of up to 5 minutes is permitted.

Follow the instructions to configure the date and time of the printer and ensure that Kerberos authentication works properly.

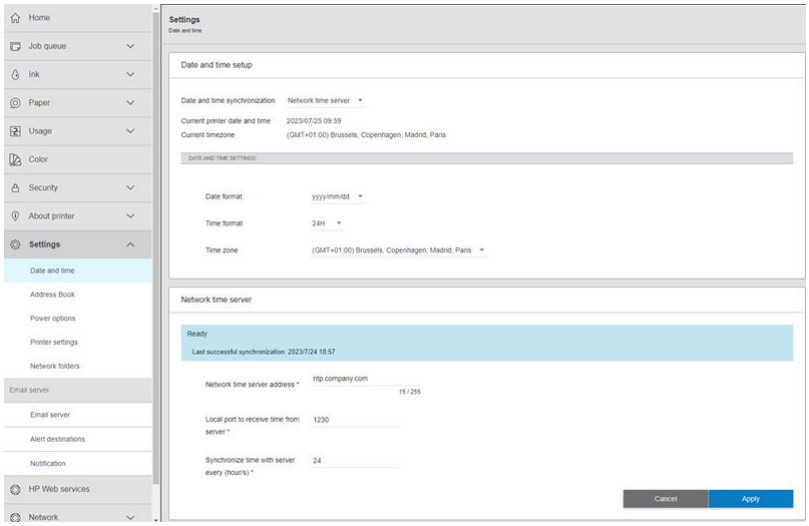
- From the printer EWS, enter **Settings** > **Date and time**, and follow one of the approaches outlined:

  a. If the printer is connected to the internet, select Automatic, HP service under **Date and time synchronization**.

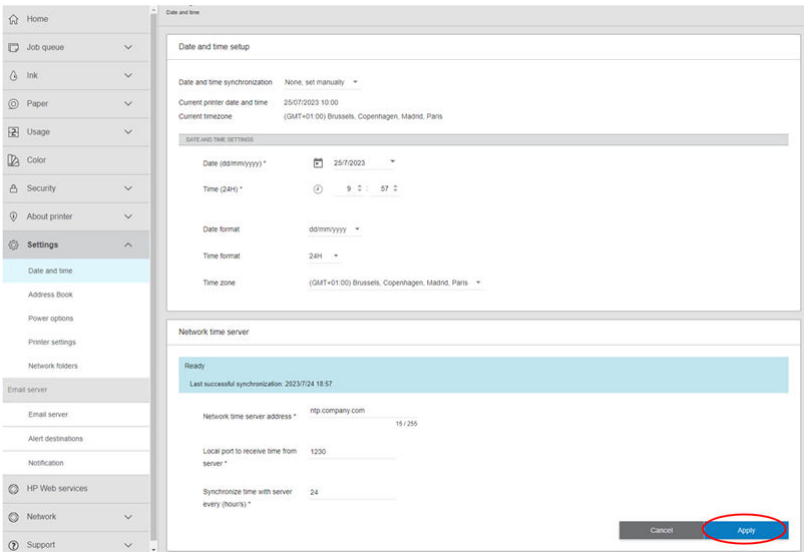


b. If you have an NTP (Network Time Protocol) server running on the network, take the following steps:

- Select **Network time server** under **Date and time synchronization**.
- Under **Network time server** > **Network time server address**, input the hostname of IP of the server where the NTP service is running.
- Under **Network time server** > **Local port to receive time from server**, input the local port where the printer will listen to the NTP broadcast message. This can be any available port on the printer and it is not the port the printer will use when connecting to the NTP server.
- Under **Network time server** > **Synchronize time with server every (hour/s)**, select the desired interval for time synchronization.



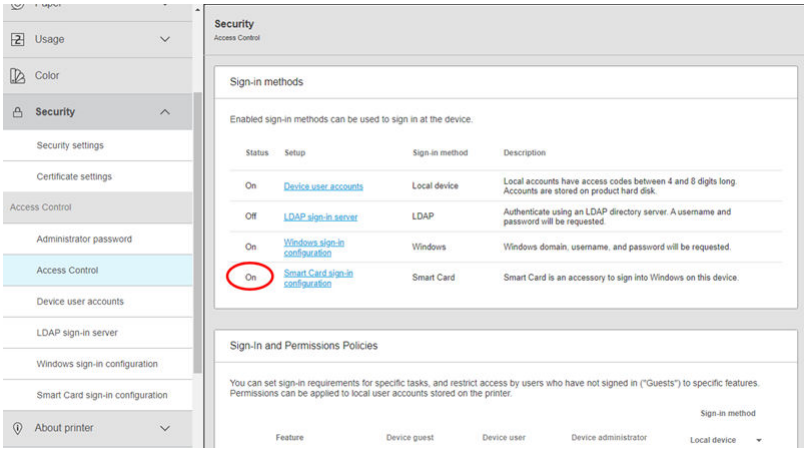
c. If the printer is not connected to the internet and an NTP server is not available on the network, then select **None, set manually** under **Date and time synchronization**. Following this, manually enter the date and time.



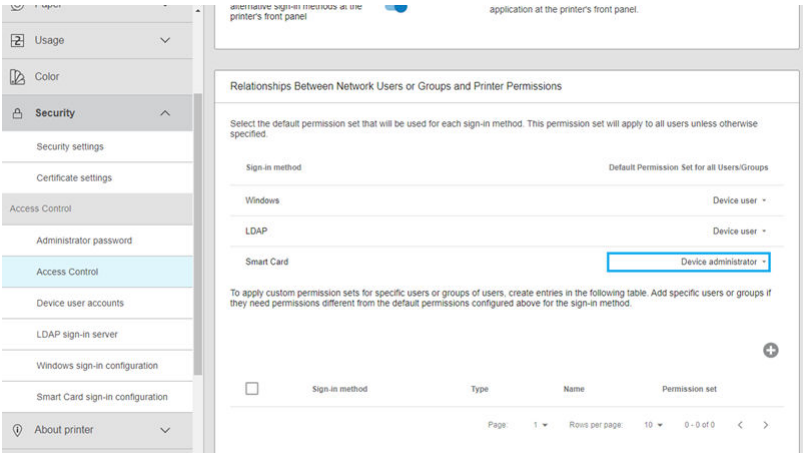
Configuring user roles for Smart Card users

Follow the instructions to configure the user roles/permissions that Smart Card users will receive after signing in with their Smart Card.

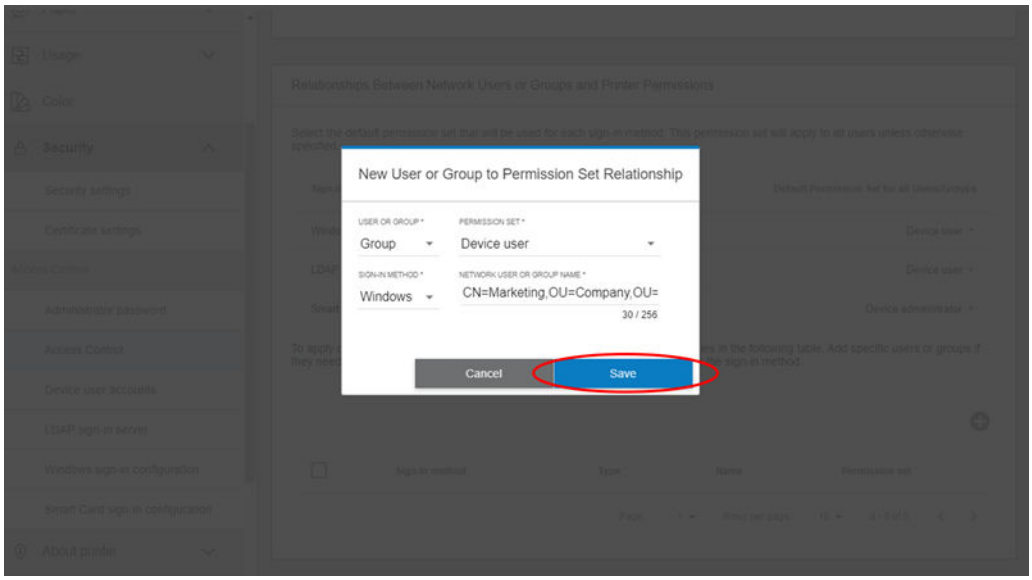
1. From the printer EWS, enter **Security** > **Access Control**.
2. **Smart Card sign-in configuration** will then appear with the status as **On**.



3. Scroll down to **Relationships Between Network Users or Groups and Printer Permissions** and select the default role that you want the user to receive when authenticating with their Smart Card.



4. To apply a custom permission set for specific users or groups, use the Windows sign in method when creating a new relationship.

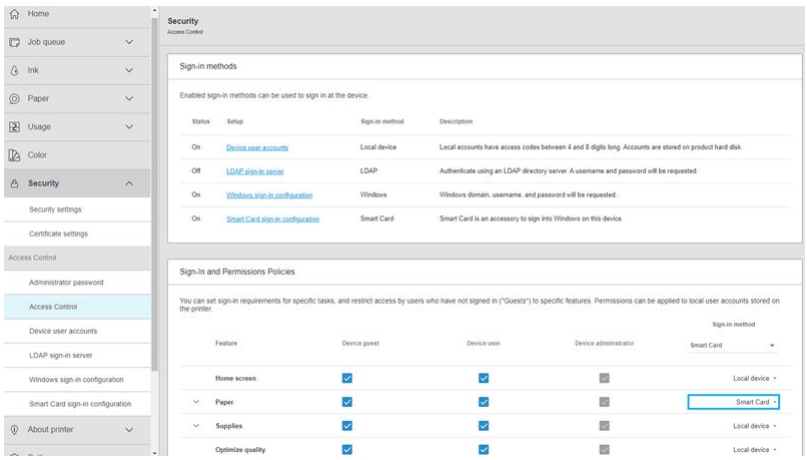


Setting up smart card as default sign in method

Setting up smart card as the default sign in method for a specific feature

Follow the instructions to set the Smart Card as the default sign in method for a specific feature. Once complete, the printer will request you to sign in with your Smart Card by default when accessing the desired feature on the front panel.

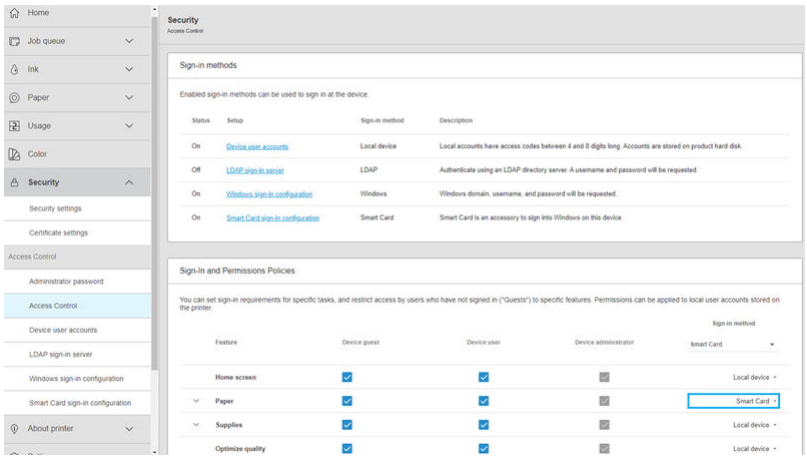
1. From the printer EWS, enter **Security** > **Access Control**.
2. Locate the desired feature under **Sign-In** and **Permissions Policies**.
3. Change the sign in method found in the rightmost column to **Smart Card**.



Setting up Smart Card as the system-wide default sign in method

Follow the instructions to set Smart Card as the global default sign in method for a specific feature. Once complete, the printer will request you to sign in with your Smart Card by default when accessing a feature on the front panel – unless the feature has a specific default sign in method configured.

1. From the printer EWS, enter **Security** > **Access Control**.
2. Under **Sign-In and Permissions Policies** > **Sign-in method**, select **Smart Card**.



Email signing and encryption

This is a feature that is compatible with the workflow of U.S. Department of Defense (DoD).

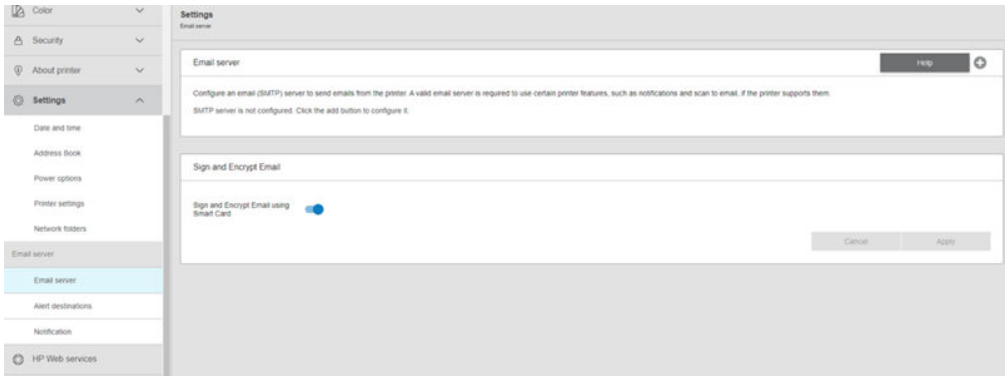
Configuring email signing and encryption

Once Smart Card sign-in is set up, you can require email signing and encryption when scanning to email, as well as the “self-send” feature. With “self-send”, the scanned files are sent to the email address of the user who is signed in. The user cannot modify the destination of the scanned documents.

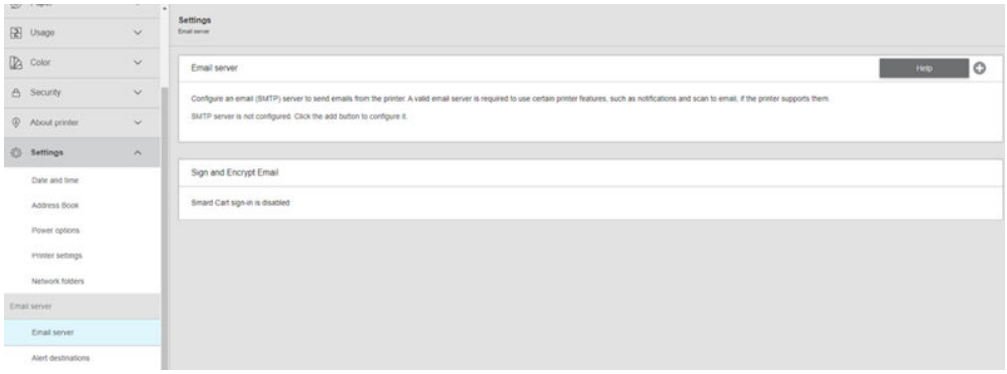
To enable “self-send” and email signing and encryption, follow the steps in the order presented:

1. From the printer EWS, enter **Settings** > **Email server**.
2. Under **Sign and encrypt email**, toggle **Sign and encrypt email using Smart Card**.

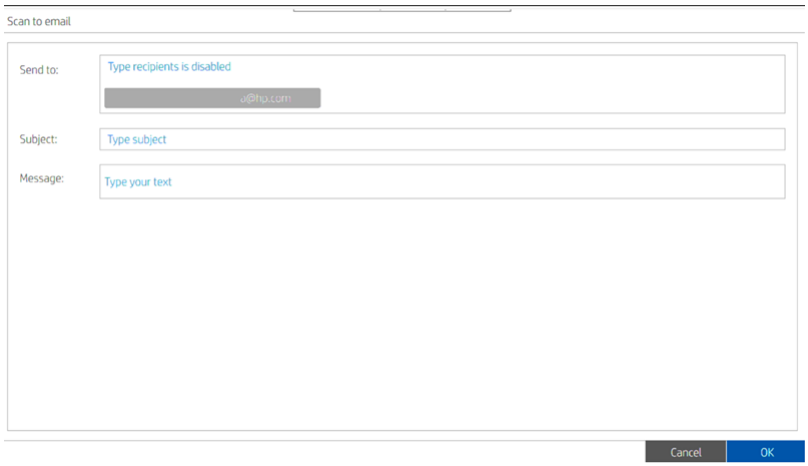
3. Click **Apply** for the setting to take effect.



NOTE: Email signing and encryption is only available when Smart Card sign in is configured. It will appear as disabled if Smart Card sign in is disabled.



4. When email signing and encryption is enabled, all emails are sent to the signed-in user's email address and the user is not allowed to modify the recipient list, as shown in the following image.



NOTE: In addition to the above configurations, basic configurations are required to use the Scan to Email feature. Refer to the printer's User Guide, chapter "Configure the email server" for further details.

Smart Card requirements

For the device to be able to encrypt and sign documents, the Smart Card must meet the following conditions:

1. The Smart Card must have a provisioned certificate with email encryption capabilities.
2. The email encryption certificate must be trusted by the device. See Importing CA certificates on page 11.
3. The Smart Card must have a provisioned certificate with email signing capabilities.
4. The email signing certificate must be trusted by the device. See Importing CA certificates on page 11.

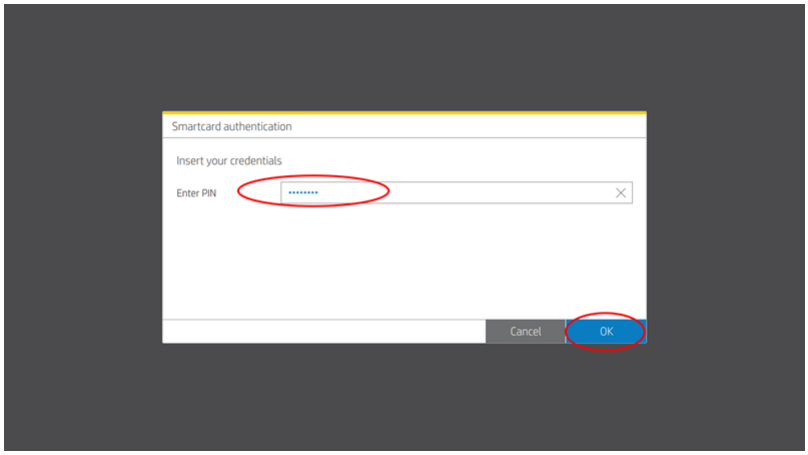
5 Signing in with Smart Card

The following sections provide details on how to sign in with your Smart Card.

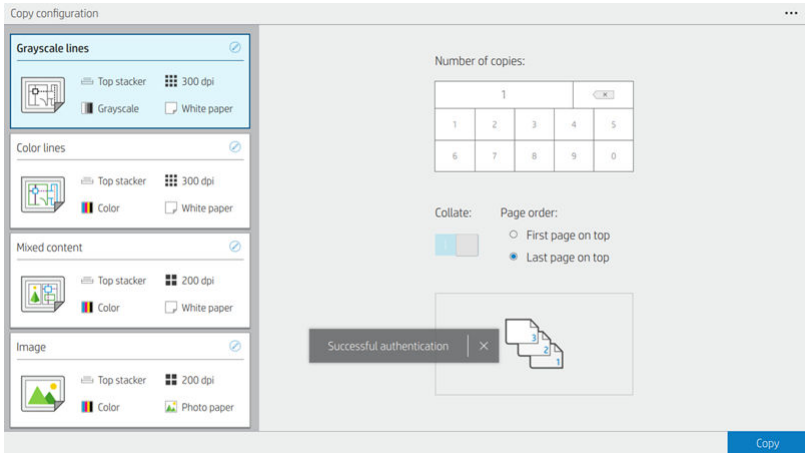
Signing in

Follow the instructions to sign in with your Smart Card.

1. Insert your Smart Card into the Smart Card reader.
2. When prompted, enter your Smart Card PIN on the printer control panel and click **OK**.

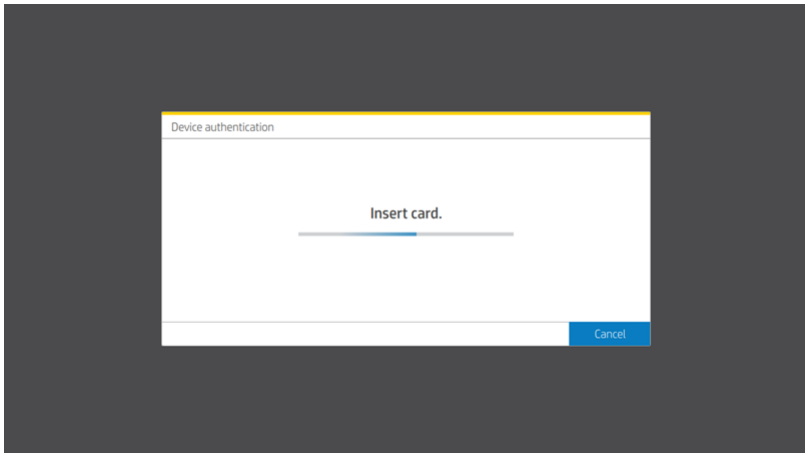


3. A message will appear to confirm that you have successfully authenticated. You are now signed in.



4. On the home screen, you will find the session icon on the dashboard.

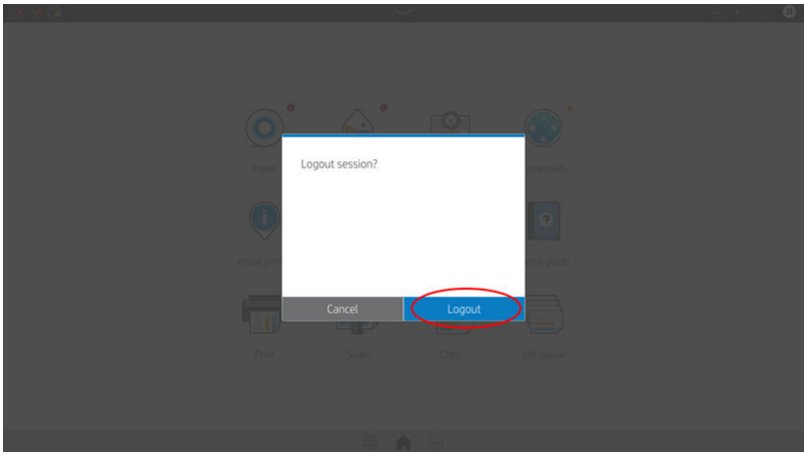
NOTE: An alternative way to sign is by accessing a restricted application configured to use the Smart Card sign in. A screen will pop up requesting you to insert your Smart Card. Once inserted, your PIN will be requested as described previously.



Signing out

Follow the instructions to sign out.

- To sign out, either remove the Smart Card or click on the session icon and then on **Logout**.



NOTE: The printer will close your session and sign you out once the configured inactivity timeout expires, regardless of whether the Smart Card is still inserted in the reader.