Xerox® AltaLink® Series Smart Card Installation and Configuration Guide
Table of Contents

1 Introduction ........................................................................................................................................ 5

   Introduction ................................................................................................................................. 6
   Supported Printers .................................................................................................................... 6
   Minimum Software Levels ........................................................................................................ 6

2 Preparation ....................................................................................................................................... 11

   Preparation Overview ................................................................................................................ 12
   Configuration Checklist ............................................................................................................. 13

3 Installation ....................................................................................................................................... 15

   Installation Overview ................................................................................................................ 16
   Hardware Installation ................................................................................................................ 17
      Connect the USB Smart Card Reader to the Printer ................................................................. 17
   Software Configuration ............................................................................................................. 20
      Accessing Administration and Configuration Settings ......................................................... 20
      Enter the Smart Card Enablement Key ................................................................................ 21
   Configuring the Smart Card ....................................................................................................... 24
      Configure Smart Card Authentication .................................................................................. 24
      Enable NTP Service ............................................................................................................... 26
      Configure Alternate Authentication ..................................................................................... 27
      Configure a Security Certificate ............................................................................................ 29
      Configure Secure Sockets Layer (SSL) ................................................................................. 34
      Configure Certificate Validation ............................................................................................ 35
      Configure Smart Card Inactivity Timer ................................................................................ 38
      Configure Acquiring Logged-In Email Addresses for Users ............................................... 39
   Printing Features ....................................................................................................................... 58
      Configure Hold All Jobs ......................................................................................................... 58
      Configure Secure Print Driver Defaults ............................................................................. 59
      Configure the Print Driver .................................................................................................... 61
   Confirm the Installation ............................................................................................................... 64
   Using the Smart Card .................................................................................................................. 65

4 Troubleshooting ............................................................................................................................. 67
# Table of Contents

Troubleshooting..................................................................................................................... 68  
Fault Clearance ...................................................................................................................... 69  
  Locating the Serial Number .............................................................................................. 69  
Troubleshooting Tips .............................................................................................................. 70  
  During Installation ........................................................................................................... 70  
  After Installation ............................................................................................................. 70
Introduction

This chapter contains:

- Introduction ................................................................................................................................6
- Smart Card Feature Overview ....................................................................................................... 7
- Documentation and Support........................................................................................................9
Introduction

The Smart Card solution brings an advanced level of security to sensitive information. Organizations can restrict access to the walk-up features of a Xerox® multifunction printer. This practice ensures that only authorized users are able to print, copy, scan, email, and fax information.

After validation, you are logged in to the Xerox® printer for all walk-up features. For added security, the functions are tracked.

This guide explains how to install and configure the Smart Card solution. The guide identifies the resources and equipment required for a successful installation.

Note: Depending on the printer model and software version you are using, the configuration instructions can vary.

For more information, contact your local Xerox Representative.

Supported Printers

- Xerox® AltaLink® Series B8045/8055/8065/8075/8090 Multifunction Printers
- Xerox® AltaLink® Series C8030/8035/8045/8055/8070 Multifunction Printers
- Xerox® WorkCentre® EC7856/7836 Multifunction Printers

Minimum Software Levels

<table>
<thead>
<tr>
<th>Printer</th>
<th>Minimum Printer Software Version</th>
<th>Smart Card</th>
<th>PIV</th>
<th>.NET</th>
<th>Access Client</th>
<th>Rijkspas</th>
</tr>
</thead>
<tbody>
<tr>
<td>Xerox® AltaLink® C8030/8035/8045/8055/8070 Multifunction Printer</td>
<td>100.xxx.037.03830</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Xerox® AltaLink® B8045/8055/8065/8075/8090 Multifunction Printer</td>
<td>100.008.037.03831</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

To identify the software version on your printer, at the control panel, touch Device, then touch About. The software version number appears.
Smart Card Feature Overview

Authentication

Xerox offers the Smart Card authentication feature. This authentication enables users who possess Smart cards to use the card for network authentication at the multifunction printer. Smart cards contain user identity certificates and public and private keys. This certificate enables the multifunction printer to perform a Kerberos authentication to the Windows active domain controller that issued the identity certificate.

The Smart Card feature was developed to support smart cards and has been extended to support PIV, CAC, Gemalto ID, Prime MD and other smart cards. This document describes the configuration settings for these smart cards.

The multifunction printer determines automatically which type of smart card is inserted in the card reader. The multifunction printer uses the appropriate software libraries to communicate with the specific card. Authentication settings are configured on the multifunction printer, according to the network infrastructure.

Hold All Jobs

The Xerox Hold All Jobs feature ensures that jobs are held securely at the multifunction printer. Jobs are available for release only after you authenticate at the printer. The printer holds the jobs for a specified time until they are released. It is not necessary to enter a Secure Print PIN to use this feature.

To use the Hold All Jobs feature, configure the print driver to pull the user name alias from the Smart Card certificate or Windows operating system. Refer to Configure the Print Driver.

This feature provides the following benefits:

- Banner Pages are not required to separate jobs, which reduces waste.
- You can manage your held jobs more efficiently. You can select only the jobs that you want to print, and delete older versions of documents that you no longer want to print.
- Confidential jobs are held in the queue for the owner to release them, rather than the documents waiting in the output tray to be picked up.

Email Signing and Encryption

With Smart Card authentication, the multifunction printer has full access to the public and private keys of the user. The printer can use these keys to sign and encrypt emails.

You can sign an email payload through the Smart Card with your private key. This action enables other users to validate the signature with your public key, which they can obtain from you or from LDAP. This validation assures the recipient that the content is original and was not compromised in transit.

You can encrypt an email payload with your public key through the Smart Card or LDAP, then send the encrypted email to the user. This option offers the benefit that, while in transit through the infrastructure, no one can decipher the contents of the email. After the email is in your Inbox, you can decrypt the email with your private key, making the payload readable again.
Supported Card Readers

The customer is responsible for providing a card reader for each Xerox® multifunction printer. Most Chip Card Interface Device (CCID)-compliant card readers can be used, but not all card readers are validated. It is recommended that you use the Indentive SCR3310 v2.0 smart card reader.

Supported Card Types

Customers are responsible for purchasing and configuring the access cards. The following card types are supported:

- CAC
- PIV
- Gemalto ID Prime MD

Other card types function with the Smart Card solution, but they are not validated.
Documentation and Support

For information about your Xerox® multifunction printer, the following resources are available:

- A System Administrator Guide provides detailed instructions and information about connecting your printer to the network and installing optional features. This guide is intended for system administrators.

- A User Guide provides detailed information about all the features and functions on your printer. This guide is intended for general users.

Most answers to your questions are provided by the support documentation supplied for your printer. Alternatively, you can contact Xerox Technical Support or access the Xerox website at www.xerox.com.
Introduction
Preparation

This chapter contains:

- Preparation Overview ................................................................. 12
- Configuration Checklist ................................................................. 13
Preparation Overview

This section explains the preparation and resources required to install the Smart Card feature.
# Configuration Checklist

The following items are required to complete the installation:

<table>
<thead>
<tr>
<th>Summary</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Obtain the IP address or host name for each applicable Windows domain controller.</td>
<td></td>
</tr>
<tr>
<td>2. If domain controller certificate validation is required, obtain the certificate for each applicable domain controller, including all intermediate certificates up to the root certificate.</td>
<td>Note: Typically, this procedure is required only for the Smart Card solution.</td>
</tr>
<tr>
<td>3. If Online Certificate Status Protocol (OCSP) is available, obtain the IP address or host name for the OCSP server.</td>
<td></td>
</tr>
<tr>
<td>4. If a software upgrade is required, obtain and install the required software release.</td>
<td></td>
</tr>
<tr>
<td>5. Mount the Smart Card Reader to the multifunction printer, then connect the USB cable to one of the rear ports. Refer to Connect the USB Smart Card Reader to the Printer.</td>
<td></td>
</tr>
<tr>
<td>6. Install the Smart Card software feature enablement key. Refer to Enter the Smart Card Enablement Key.</td>
<td></td>
</tr>
<tr>
<td>7. Configure Smart Card authentication, the optional NTP, and the optional Alternate Control Panel Login. Refer to Configuring the Smart Card.</td>
<td></td>
</tr>
<tr>
<td>8. Install any required certificates, then configure the validation settings. Refer to Configure a Security Certificate.</td>
<td></td>
</tr>
<tr>
<td>9. Configure the multifunction printer LDAP settings. Refer to Configure Acquiring Logged-In Email Addresses for Users.</td>
<td></td>
</tr>
<tr>
<td>10. Configure the multifunction printer SMTP email, signing and encryption settings. Refer to Configure SMTP Email Settings.</td>
<td></td>
</tr>
<tr>
<td>11. Configure the Hold All Jobs and Secure Print policies, if necessary. Refer to Printing Features.</td>
<td></td>
</tr>
</tbody>
</table>
Preparation
Installation

This chapter contains:

- Installation Overview ................................................................. 16
- Hardware Installation ................................................................. 17
- Software Configuration .............................................................. 20
- Configuring the Smart Card ...................................................... 24
- Printing Features ........................................................................ 58
- Confirm the Installation ............................................................. 64
- Using the Smart Card ................................................................. 65
Installation Overview

This section provides instructions for installing and configuring the Smart Card solution.

There are four main installation procedures to follow in the sequence given:

1. Hardware Installation: Unpack the Smart Card Enablement kit, then install the card reader device.
2. Enabling the Smart Card: To enable the Smart Card for configuration, use the feature enable key.
3. Configuring the Smart Card: Enable the Smart Card function, then customize the settings.
4. Using the Smart Card: For instructions on how to use the card reader to access the printer functions, refer to Using the Smart Card.

Note: Depending on the printer model and software version you are using, the configuration instructions can vary.
Hardware Installation

Connect the USB Smart Card Reader to the Printer

To install the card reader:

1. Unpack the Xerox® Smart Card Enablement Kit (CAC/PIV). The kit contains the following items:
   - Xerox® Smart Card Enablement Guide (CAC/PIV)
   - Card Reader SCR3310v2
   - Four Velcro® dual-lock fastener pads
   - Two cable ties
   - One ferrite bead
   - Five cable clamps
   Before you install the hardware, ensure that you have read the license agreement and agree to the terms and conditions.

2. Locate the card reader device, then install and configure the device.

   Note: The system administrator configures the cards before the card reader is installed on the printer.
Installation

3. Attach the ferrite bead to the reader cable.

   ![Note: Clip the ferrite bead onto the cable that is behind the connector.]

4. Attach the dual-lock fastener pads to the card reader device.
   Fasteners are provided to secure the card reader to the multifunction printer.
   - Peel back the fastener pad backing strip, then position the fastener pad on the under-side of the card reader, as shown.
   - Repeat these steps for each of the fastener pads supplied.
5. When all the dual-lock fastener pads are attached to the card reader, remove the backing strips on each of the pads.

6. Place the card reader on the multifunction printer.
   - Gently place the card reader on the printer. Do not fix the card reader in place at this time.
   - Position the card reader in a suitable location. Ensure that the card reader does not obstruct any access points or the opening of doors or covers.
   - Verify that the cable has sufficient length to connect to the rear of the network controller.
   - When the card reader is in a suitable location, to fix the card reader device in place, press firmly on the reader.

7. Connect the card reader to the multifunction printer.
   - Insert the USB connection into the slot provided on the rear of the network controller.
   - Use the cable clamps and cable ties provided to bundle the cables and ensure that the cabling is neat.

The hardware installation is now complete.
Software Configuration

Accessing Administration and Configuration Settings

The Embedded Web Server is the administration and configuration software installed on the printer. This software allows you to configure and administer the printer from a Web browser.

The administrator password is required to access locked settings in the Embedded Web Server or at the control panel. Most printer models have a default configuration that restricts access to some settings. In the Embedded Web Server, you can restrict access for settings on the Properties tab. At the device touch screen, you can restrict settings in the Tools menu.

To access the Embedded Web Server and log in as the administrator:

1. At your computer, open a Web browser.
2. In the URL address field, type http:// followed by the IP Address of the multifunction printer. For example: If the IP Address is 192.168.100.100, type the following into the URL address field: http://192.168.100.100. Press Enter or Return.
3. In the top-right area of the page, click Login.
   a. For User ID, type admin.
   b. For Password, type the administrator password. The default administrator password is 1111, or the printer serial number. You can obtain the serial number from inside the front door of the printer, from the configuration report, and from the home page of the Embedded Web Server. The password is case-sensitive.
4. Click Login.

For more information about accessing and configuring the Embedded Web Server settings, refer to the System Administrator Guide for your Xerox multifunction printer.
Enter the Smart Card Enablement Key

Before you configure the Smart Card solution, use the Embedded Web Server to enable the Smart Card feature on your Xerox® multifunction printer. The Feature Enablement Key is printed on the inside cover of the enablement guide provided within the Xerox® Smart Card (CAC/PIV) kit.

To enable the device software:

1. Access the Embedded Web Server, then click the Properties tab. For more information, refer to Accessing Administration and Configuration Settings.
2. Click the Login/Permissions/Accounting link.
3. Click the Login Methods link.
4. Click the Control Panel Login button.
   a. From the Control Panel Login menu, select Smart Cards.
   b. If users need an alternate method of authentication, from the Alternate Control Panel Login menu, select User Name/Password — Validate on the Network.
c. If the device uses the email address registered to the authenticated user, select the check box for **Personalized User Profile**.

5. In the Smart Card Enablement area, enter the unique Feature Enablement Key provided on the inside cover of the *Xerox® Smart Card Enablement (CAC/PIV) Guide*.
6. Click **Next**.

A confirmation message appears.

7. Click **Next**. The Smart Card settings are now ready to configure.

   **Note:** No services are restricted until the Smart Card is configured fully through the Embedded Web Server.
Configuring the Smart Card

After the Smart Card feature is enabled on the multifunction printer, you can use the Embedded Web Server to configure the smart card.

Configure Smart Card Authentication

To enable and configure the Smart Card:

1. Access the Embedded Web Server, then click the **Properties** tab. For more information, refer to Accessing Administration and Configuration Settings.

2. Click the **Login/Permissions/Accounting** link, then click **Login Methods**.

3. For Domain Controller, enter the details for the authentication server.
   a. From the Configuration Settings list, for Domain Controllers, click **Edit**.

   ![Configuration Settings List]

   Note: Initially, the domain controllers are empty and the NTP server is not set.

   b. Click **Add Domain Controller**.

   ![Add Domain Controller]

   c. Select the check box for Windows Based Domain Controller. Or, to select the Linux-Based Domain Controller, clear the check box.

   d. Select the IP Address or the fully qualified host name, then enter the domain controller details.
e. Unless your Kerberos Port is different, ensure that Port 88 is selected.

f. For the Domain Name field, enter the fully qualified domain name.

g. Click Save.
Enable NTP Service

To configure the date and time to update automatically:

1. From the Configuration Settings list, for Network Time Protocol, click **Edit**.

   ![Network Time Protocol Configuration](image1)

   a. To enable NTP, select the check box for **Enabled**.

   ![Enabled NTP](image2)

   b. Enter the IP address or host name for the primary and alternate time server. Often this address is the same address as the domain controller.

   ![Enter IP Address](image3)
c. Click **Save**.

2. View the Summary screen and ensure that all settings are correct.
3. Click **Close**.

---

**Configure Alternate Authentication**

If Alternate Authentication is not required, refer to [Configure a Security Certificate](#).

If Alternate Authentication is enabled, configure the authentication server.

1. In the Configuration Settings list, for Authentication Servers / Control Panel (Alternate), click **Edit**.
a. From the Authentication Type menu, select Kerberos.
b. Click Add New.
c. Enter the required domain or realm details.
d. Select the IP Address or the host name, then enter the server details. For most installations, the Alternate Authentication server is the same as the Smart Card domain controller.

2. Click **Save**.
3. Click **Close**.

**Configure a Security Certificate**

If the multifunction printer requires certificate validation, perform the instructions in this section:

- **Create a Device Certificate**
- **Import a Certificate Authority Certificate**
- **Install a Domain Controller Certificate**

If certificate validation is not required, refer to **Configure Smart Card Inactivity Timer**.

**Create a Device Certificate**

If you do not have a server that functions as a certificate authority, install a Xerox® Device Certificate on the printer. When you create a Xerox® Device Certificate, the printer generates a certificate, signs it, and creates a public key used in Secure Sockets Layer (SSL) encryption.

To create a device certificate:

1. Click the **Properties** tab, then click the **Security** link.
2. Click **Certificates** -- **Security Certificates**.
Installation

a. Click the Xerox Device Certificate tab.

b. Click **Create New Xerox Device Certificate**.

c. Complete the Self Signed Certificate fields with the required information.
3. Click **Finish**.

4. When you configure security certificates on the printer, SSL provides a secure connection between your computer and the multifunction printer. To configure SSL, refer to Configure Secure Sockets Layer (SSL).

**Import a Certificate Authority Certificate**

To import a certificate from the Certificate Authority, perform the following steps:

1. Click the **Properties** tab, then click the **Security** link.
2. Click **Certificates → Security Certificates**.
   a. Click the **Root/Intermediate Trusted Certificates** tab.
   b. Click **Install Certificate**.
   c. Click **Browse**, then navigate to your certificate authority certificates.
   d. Select the certificate required, then click **Open**.
Installation

e. If the certificate is encrypted, on the Password Required screen, enter the password.

f. To install the certificate, click **Next**.

Note: Import both the Root CA and the Intermediate CA certificates to the multifunction printer. This action establishes a chain of trust for certificates on individual smart cards.

3. Click **Next**.

4. When you configure security certificates on the printer, SSL provides a secure connection between your computer and the multifunction printer. To configure SSL, refer to [Configure Secure Sockets Layer (SSL)](#).

**Install a Domain Controller Certificate**

To install a domain controller certificate, perform the following steps:

1. Click the **Properties** tab, then click the **Security** link.
2. Click **Certificates** → **Security Certificates**.
a. Click the **Domain Controller Certificates** tab.

b. Click **Install Certificate**.

c. Click **Browse**, then navigate to the domain controller certificates.

d. Select the certificate required, then click **Open**.
Installation

e. If the certificate is encrypted, enter the password.

f. To install the certificate, click Next.

3. Repeat the process until you have uploaded all the required certificates.

Configure Secure Sockets Layer (SSL)

When you configure security certificates on the printer, Secure Sockets Layer (SSL) provides a secure connection between your computer and the multifunction printer. SSL is enabled on the printer automatically. If you do not want to configure SSL, proceed to Configure Certificate Validation.

To configure SSL, perform the following steps:

1. Click the Properties tab, then click the Connectivity link.

2. Click Setup.
   a. From the Protocol settings list, for HTTP, click Edit.
b. If you want to force traffic over a secure connection, such as HTTPS, click **Yes (All HTTP requests are switched to HTTPS)**.

![Image](image1.png)

3. If you made changes, click **Save**. The device restarts automatically. If you have not made changes, click **Cancel**.

### Configure Certificate Validation

To configure certificate validation information, perform the following steps. If you do not require certificate validation, proceed to **Configure Smart Card Inactivity Timer**.

1. Click the **Properties** tab, then click the **Login/Permissions/Accounting** link.
2. Click **Login Methods**.

![Image](image2.png)
Installation

a. From the Configuration Settings list, for Certificate Validation click **Edit**.

b. Select the required validation options.

3. If you have selected one or more options, to configure further settings, click **Next**.
4. If prompted, enter the OCSP server URL for certificate validation.
5. If prompted, to enter the proxy server information, for Proxy Server, click **Configure**. If the OCSP server is outside the firewall, a proxy server can be required to access the server.

6. To validate each domain controller, select the domain controller certificates required.

7. Click **Save**.
Configure Smart Card Inactivity Timer

To configure the smart card inactivity timer, perform the following steps. If you do not require inactivity settings for smart card authentication, proceed to Configure Acquiring Logged-In Email Addresses for Users.

1. Click the Properties tab, then click the Login/Permissions/Accounting link.
2. Click Login Methods.
   a. For Smart Card Inactivity Timer, click Edit.
   b. For Timer, enter the required number of minutes.
3. Click Save.
Configure Acquiring Logged-In Email Addresses for Users

To configure LDAP and SMTP server information, perform the following steps.

If you do not want to configure the settings for Configure Acquiring Logged-In Email Addresses for Users, proceed to Confirm the Installation.

1. Click the Properties tab, then click the Login/Permissions/Accounting link.
2. Click Login Methods.
   a. For Acquiring Logged-In Email addresses for Users, click Edit.
   b. Select the required option for Acquire Logged-In Email Addresses for Users.
c. If you select Auto or Only Network Address Book (LDAP), configure LDAP server settings. For Network Address Book (LDAP), click Edit.

d. Click Add New.

e. At the LDAP Server screen, enter a friendly name.

f. Enter the IP address or host name of the primary and alternate LDAP server.
g. From the list, select the required LDAP server.

h. Enter the LDAP search directory root. Typically, this directory root is related to the domain name for the server. For example, if the fully qualified domain name for the server is Hostname.Example.Search.Root the search directory root is dc=Example,dc=Search,dc=Root.

i. For Login Credentials to Access LDAP Server, enter the required information.

j. Click Apply.

3. Click Close.


a. Select Enable SASL Binds to LDAP.

Note: Smart Cards use a ticket-based authentication to LDAP and require SASL for authentication.
5. Click **Close**.

**Configure SMTP Email Settings**

To configure SMTP email settings, perform the following steps:

1. Click the **Properties** tab.
2. Click **Apps → Email → Setup**.
3. In the Email Setup screen, click the **Required Settings** tab.

a. For SMTP, click **Edit**.
b. To configure the server address, click **Use DNS (to identify SMTP Server)**. Or, click **IP Address** or **Host Name**, then enter the SMTP server address.
c. For Device E-mail Address, enter the required information.

4. Click Save.

Configure SMTP Authentication

To configure SMTP authentication, perform the following steps.

1. Click the Properties tab.
2. Click Apps → Email → Setup.
3. For SMTP, click Edit.
a. Click the **SMTP Authentication** tab.

![Image](image1.png)

b. For the required method of authentication, select **for SMTP**. For Login credentials used for user initiated email jobs, select **Logged-in User**.

![Image](image2.png)

*Note:* The credentials for the logged-in user typically provide authentication for the SMTP server when you enable Smart Card authentication.

c. Click **Always Use Kerberos Tickets**.
d. For automated emails, click **None**.

4. Click **Save**.

**Configure Connection Encryption**

To configure connection encryption, perform the following steps.

1. Click the **Properties** tab.
2. Click **Apps → Email → Setup**.
3. For SMTP, click **Edit**.
   a. Click the **Connection Encryption** tab.
   b. Select the required encryption setting.
4. Click **Save**.
Configure File Size Management

To configure file size management settings, perform the following steps:
1. Click the Properties tab.
2. Click Apps → Email → Setup.
3. For SMTP, click Edit.
   a. Click the File Size Management tab.
      
      Note: This screen defines how to manage large email payloads.
   b. Select the required settings.
4. Click Save.

Test Configuration

To enter test configuration settings, perform the following steps:
1. Click the Properties tab.
2. Click Apps → Email → Setup.
3. For SMTP, click Edit.
Installation

a. Click the **Test Configuration** tab.

   ![Image]

Note: This screen allows you to send a test email to confirm that all email settings are correct.

b. In the To Address field, enter a valid email address.

![Image]

C. Click **Send Email**.

![Image]

Note: If the SMTP settings are correct, a success message appears and an email is received at the address.
4. Select the **Required Information** tab.

If the required settings are configured correctly, the message **Required Settings Configured** appears.

5. Click **Save**.

**Configure General Email Settings**

To configure general email settings, perform the following steps:

1. Click the **Properties** tab.
2. Click **Apps → Email → Setup**.
3. Click the **General** tab.
Installation

a. Enter the required information to appear in the Subject line of an email that is sent from the multifunction printer.

b. For Message Body, select the required information that you want to appear in the body of an email.

c. For the Signature field, enter the information that you want to include in an email signature.

d. To print a confirmation sheet, from the menu, select the required option.

e. If you want the multifunction printer to add your email address automatically to the To field when you are logged in, for Auto Add Me, click Enabled.

4. Click Apply.

Configure Address Books
To configure address books, perform the following steps:
1. Click the Properties tab.
2. Click Apps→Email→Setup.
3. Click the **Address Books** tab.

4. LDAP was configured in a previous step. To configure the device address book, for Device Address Book, click **Edit**.

5. Configure the device address book. For more information, refer to the *System Administrator Guide* for your Xerox multifunction printer.

### Configure Email Defaults

To configure default email settings, perform the following steps:

1. Click the **Properties** tab.
2. Click **Apps → Email → Setup**.
3. Click the **Defaults** tab.

4. For default email settings, click **Edit**, then select the required options. To save selections, click **Save**.
5. Click **Apply**.
Configure Email Compression
To configure email compression settings, perform the following steps:
1. Click the Properties tab.
2. Click Apps → Email → Setup.
3. Select the Compression tab.
4. For Compression Settings, select the required settings.
5. Click Save.

Configure Email Security
To configure email security settings, perform the following steps:
1. Click the Properties tab.
2. Click Apps → Email → Setup.
3. Click the Security tab.
a. For Encryption/Signing, click **Edit**.

b. Select the required Enablement setting:

- **Off**: You cannot sign email.
- **Always On**: An email signature is required.
• **Editable by user**: The local user settings determine if an email signature is required.

c. If you selected Editable by User, and if the ability to sign is required by default, for the Email App Encryption Default setting, click **On**.

d. For Encryption Algorithm, select the required setting.
e. Click Apply.

4. If you want to configure email domain restrictions, in the Network Policies area, click Edit.
Installation

a. Select the required restrictions.

- **Domain Filtering**: This option enables you to configure a list of domains to allow or block emails.
- **Email Filtering**: This option allows you to send internal email without a corporate name. This option requires configuration of your email server.

b. Click **Save**.

5. If you want to configure restrictions on email recipients, in the User Policies area, click **Edit**.
a. Select the required settings for User Permissions.
b. Click Save.
c. If necessary, in the Only Send to Self area, click Edit.

d. Select the required Security settings.
e. Click Save.

The configuration of the smart card settings is complete.
Printing Features

To hold jobs at the multifunction printer until you authenticate at the control panel, configure the Hold All Jobs and Secure Print features.

Configure Hold All Jobs

The Hold All Jobs feature allows you to configure the multifunction printer to require users to release print jobs manually at the control panel. If you want to configure Hold All Jobs, perform the following steps:

1. Access the Embedded Web Server, then click the Properties tab. For more information, refer to Accessing Administration and Configuration Settings.

2. Click Apps → Printing → Hold All Jobs.
   a. Select the required Enablement option:

   - **Hold Jobs in a Private Queue**: This option holds jobs in a locked folder. Users are required to log in at the control panel to view, print, and delete jobs.
   - **Hold Jobs in a Public Queue**: This option holds sent jobs in an unlocked folder. Users are not required to log in at the control panel.

   b. Select the required option for Unidentified Job Policies (Unknown User ID). For more information, refer to the System Administrator Guide for your Xerox multifunction printer.
Configure Secure Print Driver Defaults

The Secure Print feature allows you to send a job to the multifunction printer with a unique passcode. Jobs are stored at the printer until you enter the same passcode to release the jobs. For more information about how to use Secure Print, refer to the User Guide for your Xerox multifunction printer. You can configure the settings to require a User ID instead of a passcode to release jobs at the control panel.

To configure the Secure Print driver defaults, perform the following steps:

1. Access the Embedded Web Server, then click the Properties tab. For more information, refer to Accessing Administration and Configuration Settings.

2. Click Apps → Printing → Secure Print.
   a. Click the Defaults tab.
b. Select the required release method.

- **Passcode**: This option requires that you type a passcode to release your Secure Print jobs at the control panel. If required, enter a number from 4–10 to specify the length of the Secure Print passcode.

- **User ID**: This option requires you to log in at the control panel to release your Secure Print jobs.

c. **Click Save.**

For more information on how to configure Secure Print settings, refer to the System Administrator Guide for your Xerox multifunction printer.
Configure the Print Driver

You can configure your print driver to pull the user name alias from the smart card certificate, or from the Windows operating system. To configure the print driver to pull the user name from the smart card certificate, install the Xerox print driver for your Xerox printer. For more information, refer to the System Administrator Guide for your Xerox multifunction printer.

1. Install your Xerox® Print Driver.

2. Access the properties for your print driver.

3. Click the Administration tab.
4. From the Access and Verification menu, select **Enabled**.

5. Click **OK**.
Note: If you configure Hold All Jobs or Secure Print Driver defaults at the multifunction printer, the settings can override the settings in your print driver. For more information, refer to Configure Hold All Jobs and Configure Secure Print Driver Defaults.
Confirm the Installation

When you install and configure the card reader and the software, the Card Reader Detected screen appears on the Xerox® multifunction printer control panel touch screen.

The smart card is now ready for use.

Note: If the card reader is not detected, refer to Troubleshooting Tips.
Using the Smart Card

When the Smart Card solution is installed and enabled, insert a valid card, then enter your Personal Identification Number (PIN) on the touch screen. When you finish, to end the session, remove your card from the card reader. If you forget to remove your card, the printer ends the session automatically after a specified period of inactivity.

To use the Smart Card, perform the following steps:

The Authentication Required window can appear on the touch screen, if that is how your device is configured.

1. Insert your card into the card reader.
2. Use the touch screen and numeric keypad to enter your PIN, then touch **Enter**.

   If the card and PIN are authenticated, access is granted.

   **Note:** If the access attempt fails, refer to [Troubleshooting Tips](#).

3. Complete the job.
4. To end the session, remove your card from the card reader.

The current session is terminated and the Authentication Required window appears.
Installation
This chapter contains:
- Troubleshooting
- Fault Clearance
- Troubleshooting Tips
Troubleshooting

For optimal performance from your card reader, follow these guidelines:

- Ensure that the card reader is compatible with network-connected products only.
- Ensure that the card reader is plugged into the network controller. Refer to **Connect the USB Smart Card Reader to the Printer**.
- Do not position the card reader in direct sunlight or near a heat source, such as a radiator.
- Ensure that the card reader does not get contaminated with dust and debris.
- To clean the outer surfaces of the card reader, use a lint-free cloth moistened with water and a mild detergent. Wipe the outer surfaces of the card reader with the lint-free cloth.
Fault Clearance

When a fault occurs, a message appears on the printer control panel touch screen. The message provides information to clear the fault. If you cannot resolve the fault using the onscreen instructions, refer to Troubleshooting Tips.

If the problem persists, identify if the problem is related to the card reader device or the Xerox® printer:

- For problems with the card reader device, for further assistance, contact the manufacturer.
- For problems relating to the Xerox® printer:
  - Before you contact Xerox Technical Support, ensure that you have the printer serial number and the fault code.
  - Contact Xerox Technical Support. Contact Xerox at 1-800-ASK-XEROX or 1-800-275-9376.

Locating the Serial Number

At the Xerox multifunction printer control panel, touch Device, then touch About. The printer serial number appears on the About screen.

Note: You can find the serial number inside the front cover of the Xerox multifunction printer.
Troubleshooting Tips

The table provides a list of problems, the possible cause, and a recommended solution.

If you experience a problem during the installation process, refer to the **During Installation** problem-solving table.

If you installed the Smart Card solution successfully, but you now experience problems, refer to the **After Installation** problem-solving table.

## During Installation

<table>
<thead>
<tr>
<th>Problem</th>
<th>Possible Cause</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>The card reader is installed but no message appears on the user interface.</td>
<td>The card reader is faulty.</td>
<td>• Try a different card reader.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Contact your system administrator.</td>
</tr>
<tr>
<td>The card reader connection is faulty.</td>
<td></td>
<td>• Check that the cable is plugged in correctly. For more information, refer to <a href="#">Connect the USB Smart Card Reader to the Printer</a>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Unplug the card reader cable, then plug it back in.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Plug the card reader into a different USB port.</td>
</tr>
<tr>
<td>The card reader is not compatible.</td>
<td>To verify that the card reader is on the list of compatible devices, refer to <a href="#">Supported Card Readers</a>.</td>
<td></td>
</tr>
<tr>
<td>Smart Card access is not enabled on the Xerox multifunction printer.</td>
<td></td>
<td>Use the Embedded Web server to enable Smart Card through the Properties setup screens. For more information, refer to <a href="#">Software Configuration</a>.</td>
</tr>
</tbody>
</table>

## After Installation

<table>
<thead>
<tr>
<th>Problem</th>
<th>Possible Cause</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>The login was successful, however you do not have the appropriate access to the operation that you requested.</td>
<td>LDAP is not configured properly or the local user permission roles are not configured properly.</td>
<td>Verify the authorization method.</td>
</tr>
<tr>
<td>The passcode entered was incorrect.</td>
<td>Incorrect PIN was entered.</td>
<td>Carefully re-enter the PIN.</td>
</tr>
<tr>
<td>Problem</td>
<td>Possible Cause</td>
<td>Solution</td>
</tr>
<tr>
<td>---------</td>
<td>---------------</td>
<td>----------</td>
</tr>
<tr>
<td><strong>Authentication failed. There is a problem with your card that is preventing successful login.</strong></td>
<td>Certificates cannot be read from the card.</td>
<td>To reload the certificates or get a new card, contact the Registration Authority.</td>
</tr>
<tr>
<td><strong>Authentication failed because the device was unable to access the remote server, domain controller, or the authentication sequence failed.</strong></td>
<td>The domain controller IP address or host name is incorrect.</td>
<td>Verify that the server address is entered correctly.</td>
</tr>
<tr>
<td></td>
<td>Incorrect domain.</td>
<td>Verify that the domain is configured properly.</td>
</tr>
<tr>
<td></td>
<td>Network error.</td>
<td>Verify that the network cable is connected firmly.</td>
</tr>
<tr>
<td><strong>The number of attempts exceeded the allowable limit.</strong></td>
<td>Card was locked due to failed login attempts.</td>
<td>To reset the PIN or to get a new card, contact the Registration Authority.</td>
</tr>
</tbody>
</table>
| **Server Certificate Failed. Authentication failed because the remote server or domain controller certificate were not found, are invalid, are expired, or access was revoked.** | This problem usually occurs because the device does not trust the certificates on the smart card. | • Ensure that all the chain of trust certificates are imported on the multifunction printer.  
• Verify which root certificate authority and intermediate certificate authority issued the smart card certificates. |
| **The card reader was not detected.** | The card reader was disconnected. | • Verify that the card reader is connected properly.  
• If you suspect that the reader has failed, uninstall the card reader, then install a known working card reader. |
<p>| <strong>Invalid time stamp. Authentication failed due to a time or date difference between the device and the remote server, or domain controller.</strong> | NTP not enabled or properly configured. | Verify that Network Time Protocol is set up correctly. Refer to Enable NTP Service. |</p>
<table>
<thead>
<tr>
<th>Problem</th>
<th>Possible Cause</th>
<th>Solution</th>
</tr>
</thead>
</table>
| GMT offset is not set correctly.                                       |                                             | • If you are not using DHCP, verify that the date, time, GMT offset, and time zone are correct. For more information, refer to the System Administrator Guide for your Xerox printer.  
• Verify that GMT offset is correct for Daylight Saving Time.        |
| The devices on your network cannot see the Embedded Web Server pages. | The IP address is incorrect or was reset.   | • Verify that the IP address that is printed on the configuration report matches the DHCP settings for your site.  
• To print a configuration report at the Xerox printer, touch Device, then touch Information Pages. Select the configuration report from the list, then touch Print. |