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

1 Introduction .......................................................................................................................... 1-1  
   Supported Printers............................................................................................................. 1-2  
   Smart Card Feature Overview ........................................................................................ 1-2  
   Authentication ............................................................................................................... 1-2  
   Hold All Jobs ................................................................................................................ 1-2  
   Email Signing and Encryption ....................................................................................... 1-2  
   Supported Card Readers............................................................................................... 1-3  
   Supported Card Types................................................................................................. 1-3  
   Minimum Software Levels ........................................................................................... 1-4  
   Documentation and Support ....................................................................................... 1-4  

2 Preparation ....................................................................................................................... 2-1  
   Configuration Checklist ............................................................................................... 2-1  

3 Installation ......................................................................................................................... 3-1  
   Hardware Installation .................................................................................................... 3-2  
   Connect the USB Smart Card Reader to the MFD ......................................................... 3-2  
   Software Configuration ................................................................................................. 3-7  
   Enter the Smart Card Enablement Key ....................................................................... 3-7  
   Configuring the Smart Card ......................................................................................... 3-10  
   Configure Smart Card Authentication ........................................................................ 3-10  
   Enable NTP Service ..................................................................................................... 3-12  
   Configure Alternate Authentication ............................................................................ 3-14  
   Configure a Security Certificate .................................................................................. 3-15  
   Create a Device Certificate ......................................................................................... 3-16  
   Import a Certificate Authority Certificate .................................................................. 3-17  
   Install a Domain Controller Certificate .................................................................... 3-19  
   Configure Secure Sockets Layer (SSL) ......................................................................... 3-21  
   Configure Certificate Validation ............................................................................... 3-22  
   Configure Smart Card Inactivity Timer ...................................................................... 3-25  
   Configure Acquiring Logged-In Email Addresses for Users ..................................... 3-26  
   Configure SMTP Email Settings ................................................................................. 3-30  
   Configure General Email Settings ............................................................................. 3-36  
   Printing Features .......................................................................................................... 3-44  
   Configure Hold All Jobs ............................................................................................. 3-44  
   Configure Secure Print Driver Defaults ..................................................................... 3-45  
   Configure the Print Driver ......................................................................................... 3-47  
   Confirm the Installation ............................................................................................... 3-49  

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

Using Smart Card..............................................................................................................................................3-50

4 Troubleshooting.............................................................................................................................................4-1
  Fault Clearance.....................................................................................................................................................4-1
  Locating the Serial Number.................................................................................................................................4-1
  Troubleshooting Tips..........................................................................................................................................4-2
  During Installation.............................................................................................................................................4-2
  After Installation................................................................................................................................................4-2
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® device. 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® device 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.

For further information, contact your local Xerox Representative.
Supported Printers

- Xerox® AltaLink® Series B8045/8055/8065/8075/8090 Multifunction Printer
- Xerox® AltaLink® Series C8030/8035/8045/8055/8070 Multifunction Printer

Smart Card Feature Overview

Authentication

Xerox offers a feature called Smart Card authentication. This authentication enables users who possess Smart Cards to use them for network authentication at the Multifunction Device (MFD). Smart Cards contain the Identity Certificate for the user, along with their public and private key. This certificate enables the MFD to perform a Kerberos authentication to the Windows Active Domain Controller that originally issued the Identity Certificate.

The Smart Card feature was developed to support smart cards and has been extended to support PIV, .NET, Access Client, Rijkspas, and other smart cards. This document describes the configuration settings for these smart cards.

The MFD automatically determines which type of Smart Card is inserted in the card reader and uses the appropriate software libraries to communicate with the specific card. Authentication settings are configured on the MFD according to the network infrastructure.

Hold All Jobs

Xerox offers a feature called Hold All Jobs. This feature ensures that jobs are held securely at the MFD and only are available for release after you authenticate at the MFD. The MFD holds the jobs for a specified period and releases them only when you release them at the MFD. It is not necessary to enter a secure print PIN to use this feature.

To use Hold All Jobs, 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 reduce waste.
- You can manage your held jobs more efficiently. You can select only the jobs you want to print, and delete older versions of documents you no longer want to print.
- Confidential documents are held in the queue for the owner to release them, rather than waiting in the output tray to be picked up.

Email Signing and Encryption

With Smart Card authentication, the MFD has full access to the public and private keys of the user. The MFD 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 also encrypt an email payload with your public key through the Smart Card or LDAP, then send it to the user. This option offers the benefit that, while in transit through the infrastructure, no one can decipher the contents of the mail note. After it 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® device. The following card readers are compatible with the solution:

- Gemplus GemPC USB SL
- Gemplus GEMPC Twin
- SCM Micro SCR3310 v1
- SCM Micro SCR3311 v1
- HID Omnikey 3021
- HID Omnikey 3121
- Identive - SCR3310v2.0 USB Smart Card Reader

Other Chip Card Interface Device (CCID) compliant readers can function with the solution, but they are not validated.

**Supported Card Types**

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

- Smart Card
- PIV and PIV II
- Gemalto.NET

Other card types function with the solution, but they are not validated.
Minimum Software Levels

<table>
<thead>
<tr>
<th>Product</th>
<th>Minimum System 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® B8045/8055/8065/8075/8090 Systems</td>
<td>100.008.037.03831</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Xerox® AltaLink® C8030/8035/8045/8055/8070 Systems</td>
<td>100.xxx.037.03830</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

To identify the software level on your printer, press the Device button on the Control Panel. The System Software Version number appears.

Documentation and Support

For information specifically about your Xerox® product, the following resources are available:

- **System Administrator Guide** provides detailed instructions and information about connecting your device to the network and installing optional features. This guide is intended for System/Machine Administrators.
- **User Guide** provides detailed information about all the features and functions on the device. This guide is intended for general users.

Most answers to your questions are provided by the support documentation supplied for your product. Alternatively you can contact the Xerox Support Center or access the Xerox website at [www.xerox.com](http://www.xerox.com).
Preparation

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 DC certificate for each applicable controller, including all intermediate certificates up to the root certificate.</td>
<td></td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td></td>
</tr>
<tr>
<td>This procedure typically is required only for Smart Card.</td>
<td></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 MFD and connect the USB cable to one of the rear ports. Refer to Connect the USB Smart Card Reader to the MFD.</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 Login. Refer to Configuring the Smart Card.</td>
<td></td>
</tr>
<tr>
<td>8. Install any required certificates and configure validation settings. Refer to Configure a Security Certificate.</td>
<td></td>
</tr>
<tr>
<td>9. Configure the MFD LDAP settings. Refer to Configure Acquiring Logged-In User’s Email Address.</td>
<td></td>
</tr>
</tbody>
</table>
10. Configure the MFD SMTP email and Signing/Encryption settings. Refer to *Configure SMTP (Email) Settings.*

11. Configure the Hold All Jobs/Secure Print policy, if necessary. Refer to *Printing Features.*
Installation

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

There are four main installation procedures to follow in sequence:

- **Hardware Installation**: Unpack the Smart Card Enablement kit, then install the card reader device.
- **Enabling the Smart Card**: To enable the Smart Card for configuration, use the Feature Enable Key.
- **Configuring the Smart Card**: Enable the Smart Card function, then customize the settings.
- **Using Smart Card**: For instructions on how to use the card reader to access the device functions, refer to *Using Smart Card*, in this guide.
Hardware Installation

Connect the USB Smart Card Reader to the MFD

To install the card reader:
1. Unpack the Smart Card Enablement Kit. The kit contains the following items.
   - Smart Card Enablement Guide
   - Four Velcro Dual-Lock Fastener pads
   - Three Cable Ties
   - One Ferrite Bead

   Ensure that you have read the license agreement and agree to the terms and conditions specified before installation.

2. Locate the card reader device to install.
   - There are four types of card reader available, one upright model, or three slimline models.
   - Locate the device to install and ensure it is configured.
Note
The System Administrator configures the cards before the card reader is installed on the printer.

3. Attach the ferrite bead to the reader cable.
Installation

**Note**
Clip the ferrite bead onto the cable directly behind the connector.

4. Attach the fasteners to the card reader device.
   Fasteners are provided to secure the card reader to the Xerox® device.
   a. Peel back the fastener backing strip.
   b. Position the fastener on the under-side of the card reader, as shown.
c. Repeat these steps for each of the fasteners supplied.

5. Remove the fastener backing strips.
When all the fasteners are attached to the card reader, remove the backing strips on each of the fasteners.

6. Place the card reader on the Xerox® device.
   a. Gently place the card reader on the device. Do not fix the card reader in place at this time.
   b. Position the card reader in a suitable location. Ensure it does not obstruct any access points or the opening of doors or covers.
   c. Check that the cable has sufficient length to connect to the rear of the network controller.
   d. Once the card reader is in a suitable location, press on it firmly to fix it in place.

7. Connect the card reader to the Xerox® device.
   - Insert the USB connection into the slot provided on the rear of the network controller.
   - Use the cable ties provided to ensure that the cabling is neat.

The hardware installation is now complete.
Software Configuration

Enter the Smart Card Enablement Key

Before you configure the Smart Card solution, use Internet Services to enable the Smart Card feature on your Xerox® device. The Feature Enablement Key is printed on the inside cover of the Enablement guide provided within the Smart Card kit.

To enable the device software:

1. Access Internet Services.
   a. Open the Web browser from your Workstation.
   b. In the URL field, enter http:// followed by the IP Address of the device. For example: If the IP Address is 192.168.100.100, enter the following into the URL field: http://192.168.100.100.
   c. Press Enter to view the Home page.

   a. Click the Properties tab.
   b. If prompted, enter the Administrator User ID and Password. The default is admin and 1111.
   c. Click the Login button.

3. Enable the Smart Card software.
   a. Click the Properties link.
   b. Click the Login/Permissions/Accounting link.
   c. Click the Login Methods link.
d. Click the **Control Panel Login** button.

![Image of Control Panel Login](image1)

e. From the Control Panel Login menu, select **Smart Cards**.

f. If users need an alternate method of authentication, select **User Name/Password** from the **Alternate Control Panel Login** menu.

![Image of Alternate Control Panel Login](image2)

g. If the device uses the email address registered to the authenticated user, select the **Personalized User Profile** check box.

![Image of Personalized User Profile](image3)
h. Click **Save**.

![Image of a user interface with options and buttons]

i. In the **Smart Card Enablement** area, enter the unique Feature Enablement Key provided on the inside cover of the Smart Card Enablement Guide.

![Image of a user interface with a text field for entering a key]

j. Click **Next**. A confirmation message appears.

![Image of a user interface with a confirmation message]

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

**Note**

No services are restricted until the Smart Card is configured fully through Internet Services.
Configuring the Smart Card

After the Smart Card feature is enabled on the device, you can use Internet Services to configure the Smart Card.

Configure Smart Card Authentication

To enable and configure the Smart Card:
1. In the Internet Services Login/Permissions/Accounting menu, click Login Methods.
2. Enter the Domain Controller details for the authentication server.
   a. Click Domain Controllers – Edit from the Configuration Settings list.

   ![Image of configuration settings]

   **Note**
   Initially the Domain Controllers are empty and the NTP server is not set.

   b. Click Add Domain Controller.

   ![Image of domain controller addition]

   c. Select the Windows Based Domain Controller check box. Or, to select the Linux-Based Domain Controller, clear the check box.
d. Select either 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. Enter the fully qualified **Domain Name**.
g. Click **Save**.

Enable NTP Service

Configure the **Date and Time** to update automatically.

a. Click **Network Time Protocol - Edit**.
b. Select the **Enabled** check box to enable NTP.

c. Enter the IP address or Host Name of the Primary and Alternate Time Server. Often this address is the same address as the Domain Controller.

d. Click **Save**.
e. View the Summary screen and ensure that all settings are correct.
f. Click **Close**.

Configure Alternate Authentication

If Alternate Authentication is not required, refer to **Configure a Security Certificate**.

If Alternate Authentication is enabled, to configure the server, click **Authentication Servers / Control Panel (Alternate) - Edit** in the Configuration Settings list.

a. Select **Authentication Type as Kerberos** from the menu.
b. Click Add New.

c. Enter the required **Domain** or **Realm**.

d. Select either the IP Address or the Host Name and enter the server details. For most installations, the Alternate Authentication server is the same as the Smart Card Domain Controller.

e. Click **Save**.

f. Click **Close**.

**Configure a Security Certificate**

If you require the MFD to be configured for certificate validation, complete this section. The following instructions are included:

- 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

To create a device certificate, complete this section.

To create a device certificate:

a. In the Properties tab, click Security.
b. Click Certificates > Security Certificates.
c. Click the Xerox Device Certificate tab.

d. Click Create New Xerox Device Certificate.

e. Complete the Self Signed Certificate fields.
f. Click Finish.

![Image of a user interface page]

3-17 Xerox® AltaLink® Series
Smart Card Installation and Configuration Guide

3-17

Installation

g. Refer to Configure SSL.

**Import a Certificate Authority Certificate**

To import a certificate from the Certificate Authority:

a. In the **Properties** tab, click **Security**.

b. Click **Certificates > Security Certificates**.

c. Click the **Root/Intermediate Trusted Certificates** tab.

![Image of a user interface page]
d. Click **Install Certificate**.

e. Click **Browse** and navigate your Certificate Authority certificates.

f. Click **Next**.

g. If the certificate is encrypted, enter the password on the **Password Required** screen.
h. Click **Next**.

**Note**
Import both Root CA and the Intermediate CA certificates to the MFD. This action establishes a Chain of Trust for certificates on individual Smart Card.

i. Refer to **Configure SSL**.

### Install a Domain Controller Certificate

To install a Domain Controller Certificate:

a. In the **Properties** tab, click **Security**.

b. Click **Certificates > Security Certificates**.

c. Click the **Domain Controller Certificates** tab.
d. Click **Install Certificate**.

e. Click **Browse** and navigate to your Domain Controller certificates.

f. If the certificate is encrypted, enter the password on the **Password Required** screen.
g. Click **Next**.

h. Continue until you upload all required certificates.

**Configure Secure Sockets Layer (SSL)**

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

a. In the **Properties** tab, click **Connectivity**.
b. Click **Setup**.
c. In the **Protocol** list, click **HTTP - Edit**.
d. If you want to Force Traffic over a Secure Connection, such as HTTPS, click Yes. All HTTP requests are switched to HTTPS.

![Image of device configuration settings]

e. Select the required certificate from the **Choose Device Certificate** menu.

![Image of device configuration settings]

f. If you have changes to apply, click **Save** and the device automatically reboots. If you have not made changes, click **Cancel**.

**Configure Certificate Validation**

If you do not require certificate validation, proceed to Configure Smart Card Inactivity Timer.

a. In the **Properties** tab, click the **Login/Permissions/Accounting** link.

b. Click **Login Methods**.
c. Click **Certificate Validation - Edit** in the Configuration Settings menu.

d. Select the required **Validation Options**.

e. If you have selected one or more options, to configure further settings, click **Next**.

f. If prompted, enter the **OCSP Server URL** to use for certificate validation.
g. If prompted, to enter the proxy server information, select **Proxy Server - Configure**. If the OCSP server is outside the firewall, a proxy server can be required to access the server.

h. Select the **Domain Controller Certificates** to validate each domain controller.
i. Click **Save**.

Configure Smart Card Inactivity Timer

If you do not require inactivity settings for Smart Card authentication, proceed to Configure Acquiring Logged-In User Email Address.

a. In the **Properties** tab, click **Login/Permissions/Accounting**.
b. Click **Login Methods**.
c. Click **Smart Card Inactivity Timer-Edit**.
Installation

d. Enter the required number of minutes for the **Timer**.

e. Click **Save**.

---

Configure Acquiring Logged-In Email Addresses for Users

This section requires you to configure LDAP and SMTP server information. If you do not want to Configure Acquiring Logged-In Email Addresses for Users settings, proceed to Confirm the Installation.

a. In the **Properties** tab, click the **Login/Permissions/Accounting** link.

b. Click **Login Methods**.

c. Click **Acquiring Logged-In Email Addresses for Users - Edit**.
d. Select the required option for **Acquire Logged-In Email Addresses** for Users.

![Diagram showing options for acquiring email addresses]

e. If you select **Auto** or **Only Network Address Book (LDAP)**, click **Network Address Book (LDAP) - Edit** to configure LDAP server settings.

![Diagram showing editing options for LDAP]

f. Click **Add New**.
g. At the LDAP Server screen, enter a **Friendly Name**.

h. Enter the **IP address** or **Host Name** of the Primary and Alternate LDAP server.

i. Select the required **LDAP Server** from the drop-down list.

j. 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".

k. Enter the required **Login Credentials to Access LDAP Server**.

l. Click **Apply**.

m. Click **Close**.
n. Select **LDAP Policies**.

![Image of LDAP Policies selection](image1)

o. Select **Enable SASL Binds to LDAP**.

![Image of Enable SASL Binds to LDAP selection](image2)

**Note**

Smart Cards use a ticket-based authentication to LDAP and require SASL for authentication.

p. Click **Save**.

![Image of Save button](image3)

q. Click **Close**.
Configure SMTP Email Settings

Click Apps > Email > Setup. In the Email Setup screen, click the Required Settings tab.

a. Click SMTP - 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. Enter the required **Device Email Address**.

d. Click **Save**.
Configure SMTP Authentication

Click SMTP - Edit.

a. Click the SMTP Authentication tab.

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

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. Click **None** for automated emails.

e. Click **Save**.

**Configure Connection Encryption**

Click **SMTP - Edit**.

a. Click the **Connection Encryption** tab.

b. Select the required encryption setting.

c. Click **Save**.
Configure File Size Management

Click SMTP - Edit.

a. Click the File Size Management tab.

Note
This screen defines how to manage large email payloads.

b. Select the required settings.

c. Click Save.

Test Configuration

Click SMTP - Edit.
a. Click the **Test Configuration** tab.

![Test Configuration tab](image)

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

b. Enter a valid email address in the To Address field.

![Enter email address](image)

c. Click **Send Email**.

![Send Email](image)

**Note**
If the SMTP settings are correct, a success message appears and an email is received at the address.
Installation

d. Select the **Required Information** tab.

![Required Settings Configured](image)

**Required Settings Configured** appear to confirm that the required settings are configured.

e. Click **Save**.

**Configure General Email Settings**

Click **Apps > Email > Setup**. On the **Email Setup** screen, click the **General** tab.
a. Enter the required information to display in the **Subject** of an email sent from the MFD.

b. Select the required information to display in the **Message Body**.

c. Enter the information to be included in the **Signature**.

d. Select the required option for printing a **Confirmation Sheet** from the menu.

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

f. Click **Apply**.
Configure Address Books

Click the Address Books tab.

a. LDAP was configured in a previous step. If you require the Device Address Book, click Device Address Book - Edit.

b. Configure the Device Address Book. Instructions are available in the System Administration Guide.

Configure Email Defaults

Click the Defaults tab.

a. Select the required options for email default settings.

b. Save your changes.
Configure Email Compression

Select the Compression tab.

a. Select the required Compression Settings.

b. Click Save.

Configure Email Security

1. Click the Security tab.
Installation

a. Click **Encryption/Signing - Edit**.

b. Select the required **Encryption Enablement** setting:

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

c. If you selected Editable by User, if the ability to sign is required by default, click On for **Email Encryption Default**.
d. Select the required **Encryption Algorithm**.
2. If you want to configure email domain restrictions, click **Edit** in the **Network Policies** area.

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

3. If you want to configure restrictions on email recipients, click **Edit** in the **User Policies** area.

   a. Select the required settings for **User Permissions**.
   b. Save your changes.
c. If necessary, click **Edit** in the **Only Send to Self** area.

d. Select the required settings for **User Policies**.
e. Save your changes.

The configuration of the Smart Card settings is complete.

### Printing Features

To hold jobs at the MFD until you authenticate at the Control Panel, configure the Hold All Jobs and Secure Print features.

#### Configure Hold All Jobs

Hold All Jobs allows you to configure the MFD to require users to release print jobs manually at the Control Panel. If you want to configure Hold All Jobs, follow these instructions.

- **Access Internet Services** and select **Properties**. Refer to Access Internet Services in the **Enter the Smart Card Enablement Key** procedure for instructions.
  - a. Click **Apps > Printing > Hold All Jobs**.
  - b. Select the required **Enablement** option.
• **Hold Jobs in a Private Queue**: the MFD 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**: the MFD holds sent jobs in an unlocked folder. Users are not required to log in at the Control Panel.

c. Select the required option for **Unidentified Job Policies (Unknown User ID)**. Further details are available in the System Administrator Guide.

---

### Configure Secure Print Driver Defaults

The Secure Print feature allows you to send a job to the MFD with a unique passcode. Jobs are stored at the MFD until you enter the same passcode to release them. Further information about how to use Secure Print is available in your User Guide. 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:

1. **Access Internet Services** and click **Properties**. Refer to Access Internet Services in the **Enter the Smart Card Enablement Key** procedure for instructions.
2. **Click Apps > Printing > Secure Print**.
3. **Click the Defaults tab**.
c. Select the required **Method**:

- **Passcode**: 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**: requires you to log in at the Control Panel to release your Secure Print jobs.

d. Click **Save**.
Further information on how to configure Secure Print Settings is available in the System Administrator Guide.

**Configure the Print Driver**

You can configure your print driver to either 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:

1. Install your Xerox® Print Driver. Instructions are available in the System Administrator Guide.
2. Access the **Properties** for your print driver.
3. Click the **Administration** tab.
c. Select **Enabled** from the **Access and Verification** menu.
d. Click OK.

**Note**
If you configure Hold All Jobs or Secure Print Driver Defaults at the MFD, they can override the settings in your print driver. 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® device local user interface.

The Smart Card is now ready for use.
Using Smart Card

When the Smart Card is enabled, insert a valid card and 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:

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.
   - 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.
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 MFD.
- 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.

Fault Clearance

When a fault occurs, a message appears on the User Interface that provides information relating to the fault. If a fault cannot be resolved by following the instructions provided, refer to Troubleshooting Tips on page 45.

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

- For problems with the card reader device, contact the manufacturer for further assistance.
- For problems relating to the Xerox® device, contact the Xerox Technical Customer Support. The Technical Customer Support Center wants to know the nature of the problem, the Device Serial number, the fault code, if any, plus the name and location of your company.

Contact Xerox at 1-800-ASK-XEROX or 1-800-275-9376.

Locating the Serial Number

Press the Device button on the Control Panel.

- The Device Information tab appears.
- The Device Serial Number is on this screen.

Note

You can also find the serial number on the metal plate inside the front cover.
## 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 After Installation.

### 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 the System Administrator.</td>
</tr>
<tr>
<td></td>
<td>The card reader connection is faulty.</td>
<td>• Check that the cable is plugged in correctly. Refer to Connect the USB Smart Card Reader to the MFD for instructions.</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></td>
<td>The card reader is not compatible.</td>
<td>Check that the card reader is on the list of compatible devices, refer to Supported Card Readers.</td>
</tr>
<tr>
<td></td>
<td>Smart Card access is not enabled on the device.</td>
<td>Use Internet Services to enable Smart Card through the Properties setup screens. Refer to Software Configuration.</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 you requested.</td>
<td>LDAP is not configured properly or the local user permission roles are not configured properly.</td>
<td>Check the authorization method.</td>
</tr>
<tr>
<td>Problem</td>
<td>Possible Cause</td>
<td>Solution</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>---------------------------------------------------------</td>
<td>-------------------------------------------------------------------------</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></td>
<td><strong>Caution</strong></td>
<td>Consecutive incorrect entries can lead to your card being locked.</td>
</tr>
<tr>
<td>Authentication failed. There is a problem with your card that is</td>
<td>Certificates cannot be read from the card.</td>
<td>Contact the Registration Authority to reload the certificates or get a new card.</td>
</tr>
<tr>
<td>preventing successful login.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Authentication failed because the device was unable to access the</td>
<td>Domain Controller IP Address or Host Name is incorrect.</td>
<td>Verify that the server address is entered correctly.</td>
</tr>
<tr>
<td>remote server, Domain Controller, or the authentication sequence failed.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Incorrect Domain.</td>
<td>Verify that the Domain was configured properly.</td>
</tr>
<tr>
<td></td>
<td>Network error.</td>
<td>Check that the network cable is connected firmly.</td>
</tr>
<tr>
<td>The number of attempts were exceeded.</td>
<td>Card was locked due to failed login attempts.</td>
<td>Contact the Registration Authority to reset the PIN or to get a new card.</td>
</tr>
<tr>
<td>Server Certificate Failed. Authentication failed because the remote</td>
<td>This problem usually occurs because the device does not trust the certificates on the Smart Card.</td>
<td>• Ensure that all the chain of trust certificates are imported on the device.</td>
</tr>
<tr>
<td>server, Domain Controller, certificate was not found, is invalid, is</td>
<td></td>
<td>• Check the Operators Smart Card Smart Card to see which Root CA and Intermediate CA issued the Smart Card certificates.</td>
</tr>
<tr>
<td>expired, or was revoked.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Card reader not detected.</td>
<td>The card reader was disconnected.</td>
<td>• Verify that the card reader is connected properly.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• If you suspect the reader has failed, swap with a known working reader.</td>
</tr>
<tr>
<td>Problem</td>
<td>Possible Cause</td>
<td>Solution</td>
</tr>
<tr>
<td>---------</td>
<td>---------------</td>
<td>----------</td>
</tr>
<tr>
<td>Invalid Timestamp. Authentication failed due to a time or date difference between the device and the remote server, or Domain Controller.</td>
<td>NTP not enabled or properly configured.</td>
<td>Verify that Network Time Protocol is set up correctly, refer to Enable NTP Service.</td>
</tr>
<tr>
<td></td>
<td>GMT offset is not set correctly.</td>
<td>• If you are not using DHCP, verify the date and time and GMT Offset, or Time Zone is correct. Instructions are available in the System Administrator Guide. • Verify that GMT offset is correct for Daylight Savings Time.</td>
</tr>
<tr>
<td>Note</td>
<td>Unforeseen errors are mapped to this error message.</td>
<td></td>
</tr>
<tr>
<td>Cannot see the Internet Services web page.</td>
<td>The IP Address is incorrect or was reset.</td>
<td>• Check the IP Address printed on the configuration report. Ensure the DHCP settings match your site settings. • To print a configuration report at the Xerox® device, select Device, then Information Pages. Select the Configuration Report from the list, then select Print.</td>
</tr>
</tbody>
</table>