

Smart Card Installation and Configuration Guide

(CAC/PIV/.Net/Access Client & Rijkspas)

Xerox® WorkCentre® 3655 Multifunction Printer

Xerox® WorkCentre® 5845/5855/5865/5875/5890 Multifunction Printer

Xerox® WorkCentre® 5945/5955 Multifunction Printer

Xerox® WorkCentre® 6655 Multifunction Printer

Xerox® WorkCentre® 7220/7225 Multifunction Printer

Xerox® WorkCentre® 7830/7835/7845/7855 Multifunction Printer

Xerox® ColorQube® 8700/8900 Multifunction Printer

Xerox® ColorQube® 9301/9302/9303 Multifunction Printer



©2014 Xerox Corporation. All rights reserved. Xerox®, Xerox and Design®, ColorQube® and WorkCentre® are trademarks of Xerox Corporation in the United States and/or other countries. BR10996

Other company trademarks are also acknowledged.

Changes are periodically made to this document. Changes, technical inaccuracies, and typographic errors will be corrected in subsequent editions.

Document version 3.0: October 2014

Table of Contents

1	Introduction	
	Smart Card Feature Overview	6
	Authentication	6
	Hold All Jobs	6
	E-mail Signing and Encryption	6
	Supported Card Readers	7
	Supported Card Types	7
	Minimum Software Levels	8
	Documentation and Support	8
2	Preparation	
	Configuration Checklist	9
3	Installation	
	Hardware Installation	12
	Connect the USB Smart Card Reader to the MFD	12
	Software Configuration	18
	Enter the Smart Card Enablement Key	18
	Configuring the Smart Card	20
	Configure Smart Card Authentication	20
	Enable NTP Service	21
	Configure Alternate Authentication	22
	Configure a Security Certificate	22
	Configure SSL	24
	Configure Certificate Validation	25
	Configure Smart Card Inactivity Timer	26
	Configure Acquiring Logged-In User's E-mail Address	26
	Printing Features	32
	Configure Hold All Jobs	32
	Configure Secure Print Driver Defaults	33
	Configure the Print Driver	33
	Confirm the Installation	34
	Using Smart Card	35
4	Troubleshooting	
	Fault Clearance	38
	Locating the Serial Number	38
	Troubleshooting Tips	39
	During Installation	39
	After Installation	40

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 ensures only authorized users are able to copy, scan, e-mail and fax information.

Once validated, a user is logged into the Xerox® device for all walk-up features. The system allows for functions to be tracked for an added layer of security.

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

Should you require any further information, please contact your local Xerox Representative.

Smart Card Feature Overview

Authentication

Xerox offers a feature called Smart Card authentication. This enables users who possess smart cards to use them for network authentication at the multifunction device (MFD). Smart cards contain the user's Identity Certificate along with their public and private key. This enables the MFD to perform a Kerberos authentication to the Windows Active Domain Controller which originally issued the Identity Certificate.

The Smart Card feature was developed to support CAC 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 will automatically determine which type of smart card type is inserted in the card reader and use 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 all jobs are held securely at the MFD and are only available for release after a user has authenticated at the MFD. The MFD holds the jobs for a specified period of time and releases them only when the user releases them at the MFD. It is not necessary to enter a secure print PIN to use this feature.

To use Hold All Jobs, the print driver needs to be configured to either pull the user's name (alias) from the smart card certificate or from the Windows Operating System. See the instructions in this document to configure the print driver.

This feature provides the following benefits:

- Banner Pages are not required to separate jobs, which reduces waste.
- Users can manage their held jobs more efficiently. Users can select only the jobs they want to print and delete older versions of documents that they no longer wish 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.

E-mail Signing and Encryption

With Smart Card authentication the MFD has full access to the user's public and private keys and can use these keys for e-mail signing and encryption.

An e-mail payload can be signed via the smart card with the user's private key. This enables other users to validate the signature with the user's public key, which can be obtained from the user or from LDAP. This assures the recipient that the content is original and has not been tampered with in transit.

An e-mail payload can also be encrypted with the user's public key via the smart card or LDAP, and then sent to the user. This offers the benefit that while in transit from the MFD through the e-mail infrastructure, no one can decipher the contents of the mail note. Once in the user's inbox, the e-mail can be decrypted with the user's 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
- SCM Micro SCR3311
- OmniKey Cardman 3021 USB
- OmniKey Cardman 3121 USB
- ActivCard USB Reader V2 with SCR-331 firmware¹
- Cherry ST1044U

Other CCID compliant readers may function with the solution, but have not been validated.

Supported Card Types

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

- CAC
- PIV & PIV II
- Gemalto.NET

Other card types may function with the solution, but have not been validated.

Minimum Software Levels

Product	Minimum System Software Version	CAC	PIV	.NET	Access Client	Rijkspas
WorkCentre 3655	072.060.034.16800	Yes	Yes	Yes	No	No
WorkCentre 58xx	071.xxx.xxx.xxx.xxxxx	Yes	Yes	Yes	No	No
WorkCentre 59xx	071.xxx.xxx.xxx.xxxxx	Yes	Yes	Yes	No	No
WorkCentre 6655	072.060.034.16800	Yes	Yes	Yes	No	No
WorkCentre 72xx	072.110.044.20500	Yes	Yes	Yes	No	No
WorkCentre 78xx	071.xxx.xxx.xxx.xxxxx	Yes	Yes	Yes	No	No
ColorQube 87xx/89xx	071.160.222.26601	Yes	Yes	Yes	No	No
ColorQube 93xx	071.xxx.xxx.xxx.xxxxx	Yes	Yes	Yes	No	No

To identify the software level on your machine, press the **Machine Status** button on the Control Panel. The System Software Version number is displayed.

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 will be 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.

Preparation

2

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:

Summary	Status
1. Obtain the IP address or Host Name for each applicable Windows Domain Controller	
2. If Domain controller certificate validation is required, obtain the DC certificate for each applicable controller including all intermediate certificates up to the root cert. Note: This is typically only required for CAC	
3. If Online Certificate Status Protocol (OCSP) is available, obtain the IP address or Host Name for the OCSP server	
4. If a software upgrade is required obtain and install the required software release	
5. Mount the smart card reader to the MFD and connect the USB cable to one of the rear ports. See Connect the USB Smart Card Reader to the MFD on page 12	
6. Install the Smart Card software Feature Enablement Key. See Enter the Smart Card Enablement Key on page 18	
7. Configure Smart Card Authentication, NTP (optional), and Alternate Login (optional). See Configuring the Smart Card on page 20	
8. Install any required certificates and configure validation settings. See Configure a Security Certificate on page 22	
9. Configure the MFD LDAP settings. See Configure Acquiring Logged-In User's E-mail Address on page 26	
10. Configure the MFD SMTP (E-mail) and Signing/Encryption settings. See Configure SMTP (E-mail) Settings on page 27	
11. Configure Hold All Jobs/Secure Print policy if required. See Printing Features on page 32	

Installation

3

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

There are four main installation procedures to follow in sequence.

- **Hardware Installation**
 - Unpacking the Smart Card Enablement kit and installing the card reader device.
- **Enabling the Smart Card**
 - Use the Feature Enable Key to enable the Smart Card to be configured.
- **Configuring the Smart Card**
 - Enabling the Smart Card function and customizing the settings.
- **Using Smart Card**
 - Instructions on how to use the card reader device to access the device functions.

Hardware Installation

Connect the USB Smart Card Reader to the MFD

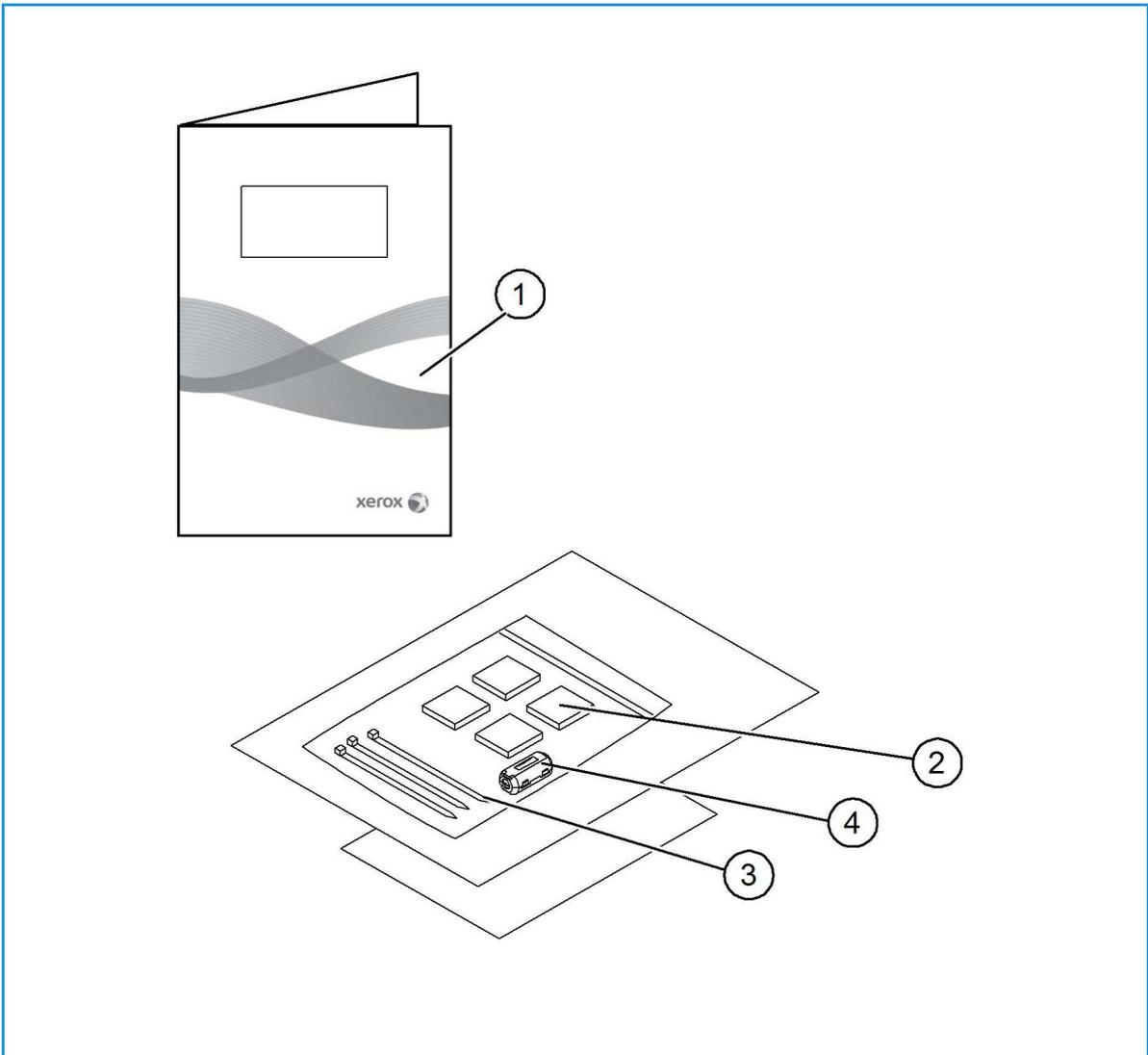
Install the card reader device using the following instructions.

1. Unpack the Smart Card Enablement Kit

The kit contains the following items:

- Smart Card Enablement Guide (1)
- Four Dual Lock Fastener pads (Velcro) (2)
- Three Cable Ties (3)
- One Ferrite Bead (4)

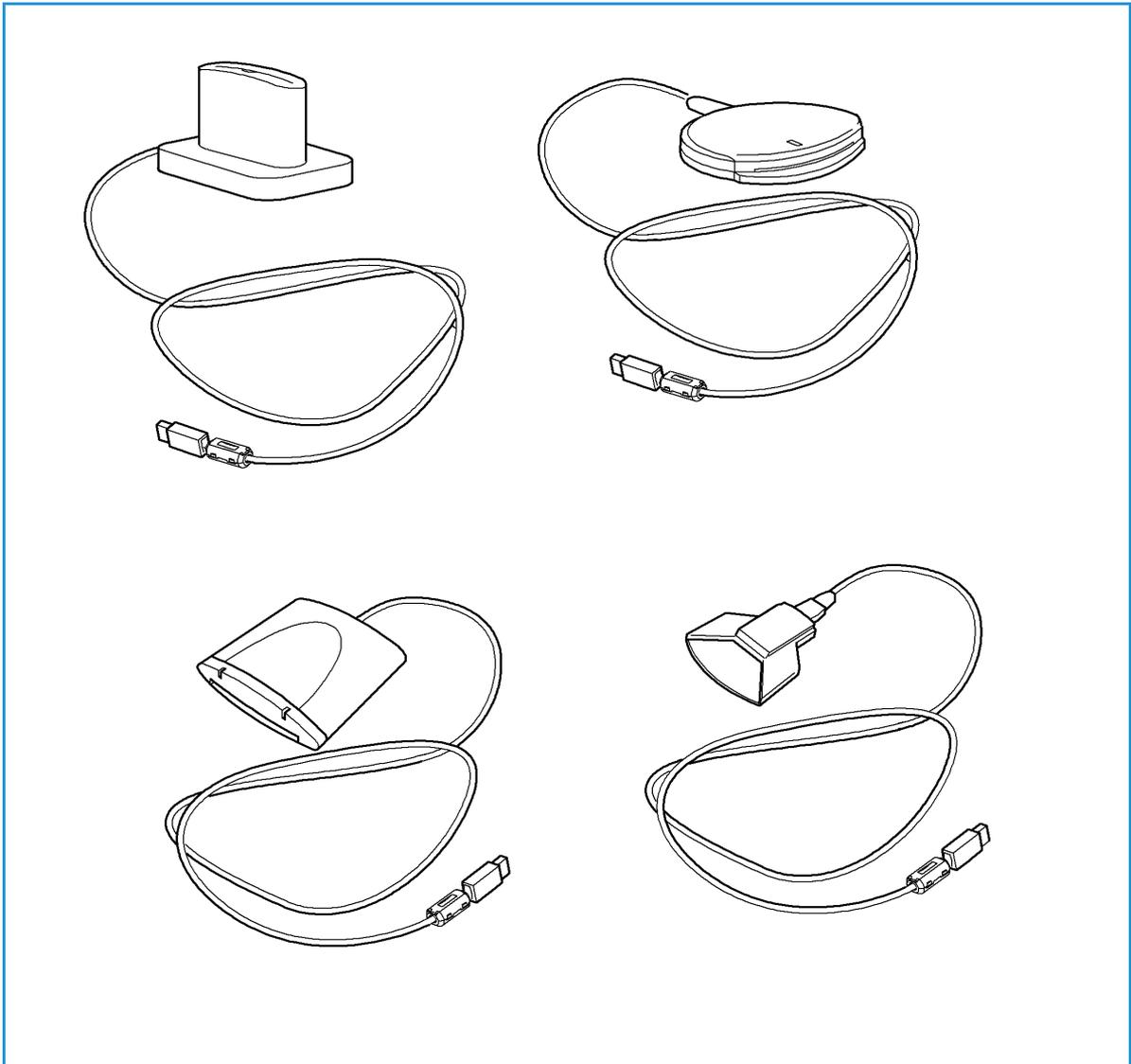
Ensure you have read the licence agreement and agree to the terms and conditions specified prior to installation.



2. Locate the card reader device being installed

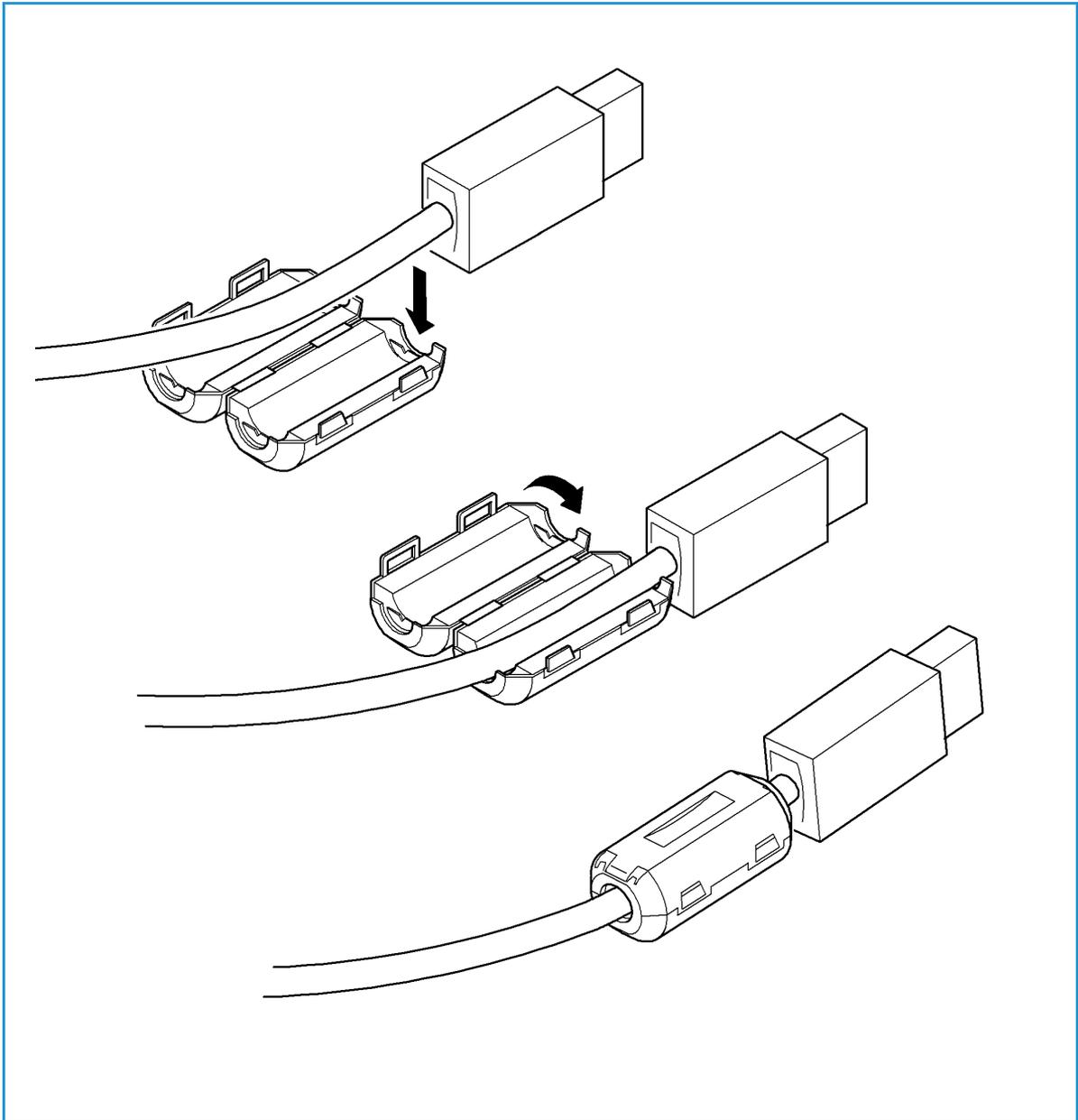
- There are four types of card reader available, one upright model or three slimline models.
- Locate the device being installed and ensure it has been configured.

Note: The System Administrator should configure the cards prior to the card reader being installed on the machine.



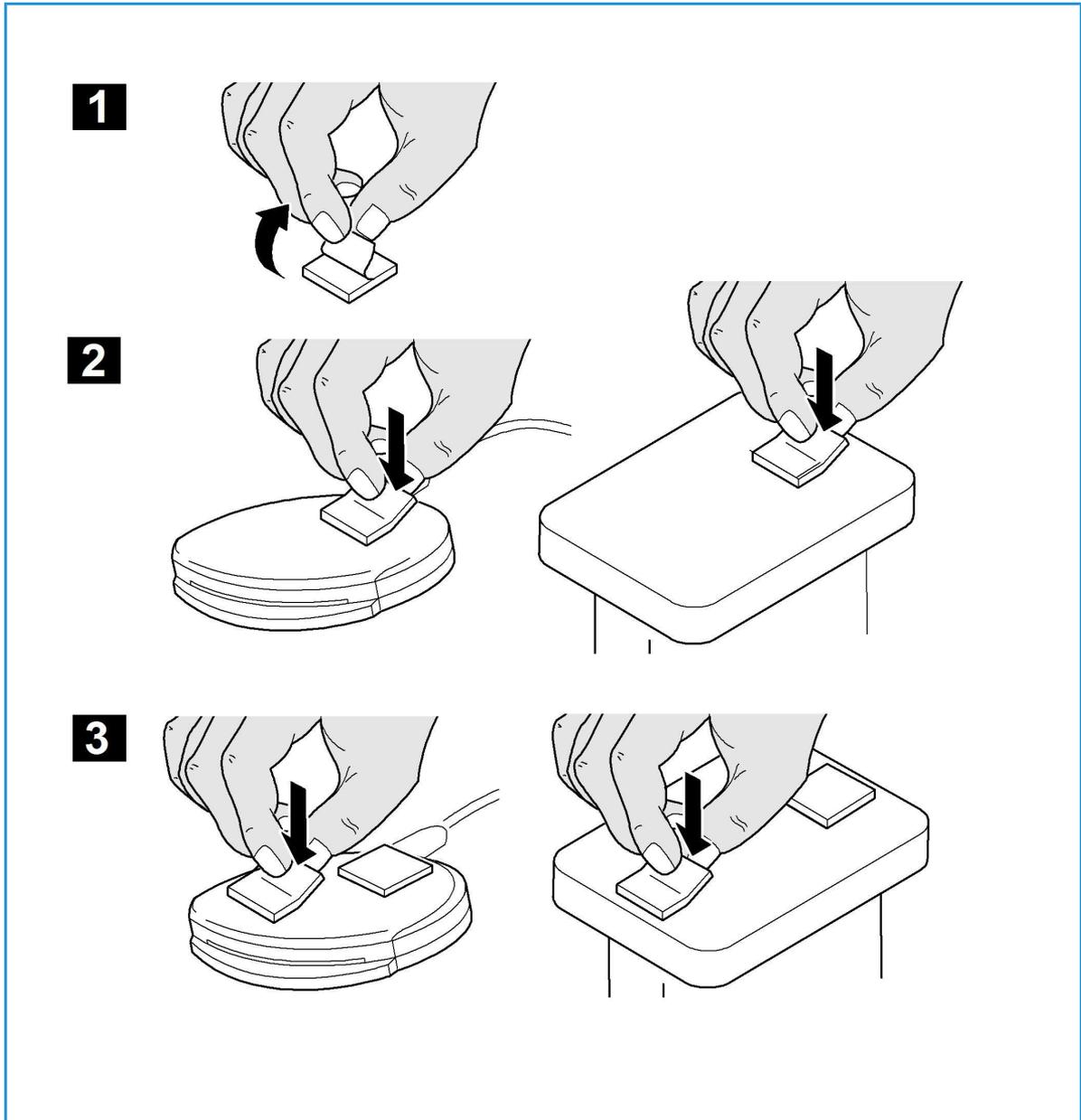
3. Attach the ferrite bead to the reader cable.

Note: The ferrite bead should be clipped onto the cable directly behind the connector.



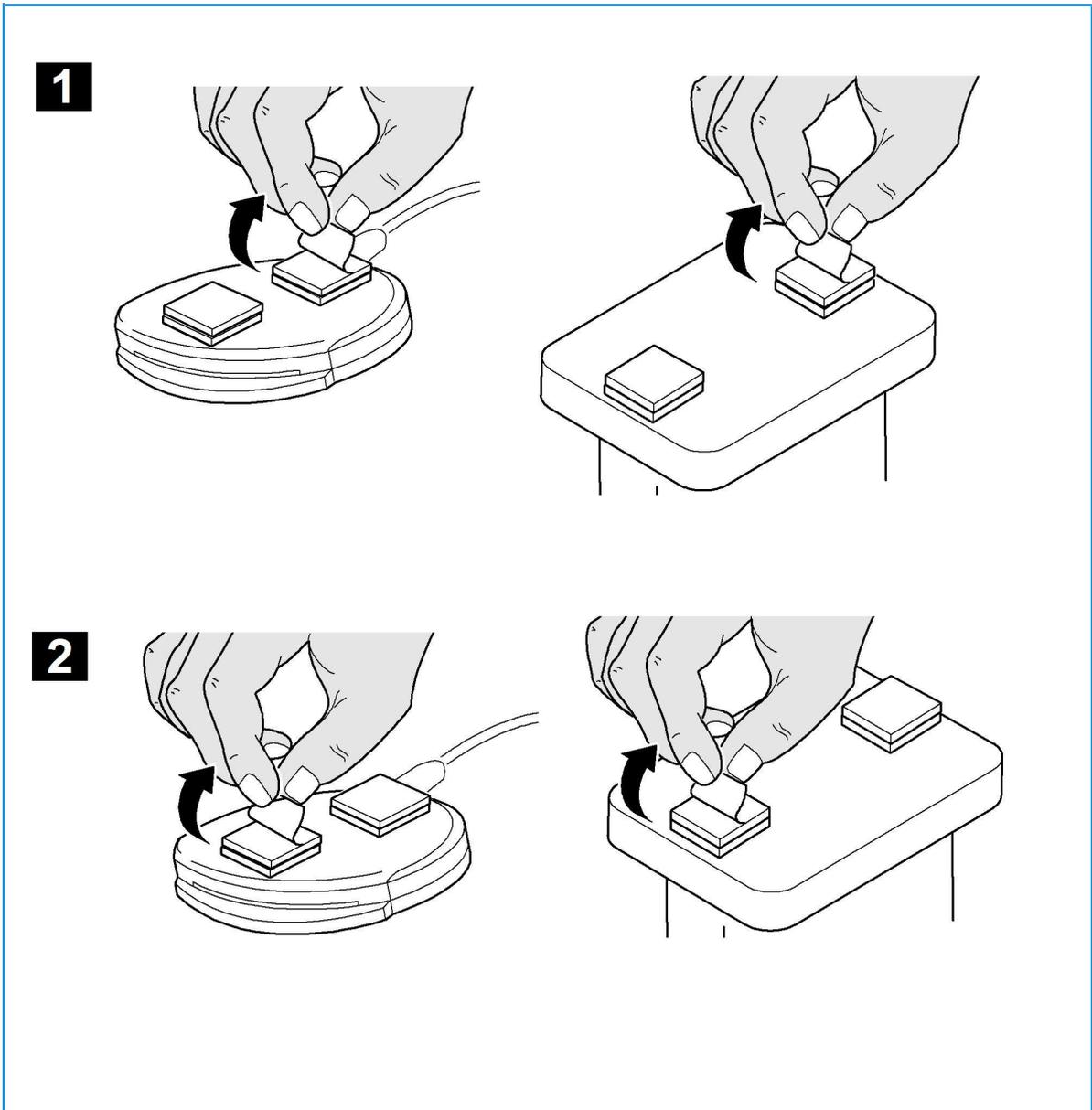
4. Attach the fasteners to the card reader device

- Fasteners have been provided to secure the card reader to the Xerox® device.
- Peel back the fastener backing strip.
- Position the fastener on the under-side of the card reader, as shown.
- Repeat for each of the fasteners supplied.



5. Remove the fastener backing strips

When all the fasteners have been attached to the card reader, remove the backing strips on each of the fasteners.



6. Place the card reader on the Xerox® device
 - Gently place the card reader on the device (do not fix in place at this point).
 - Position the card reader in a suitable location, ensure it does not obstruct any access points or the opening of doors or covers.
 - Check the cable has sufficient length to connect to the rear of the network controller.
 - Once it is in a suitable location, press firmly on the card reader 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 the cabling is neat and tidy.

The hardware installation is now complete.

Software Configuration

Enter the Smart Card Enablement Key

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

Follow the instructions below to enable the device software.

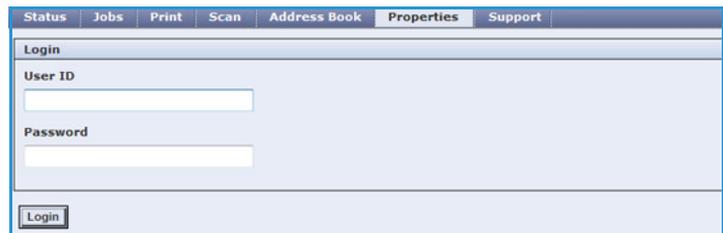
1. Access **Internet Services**

- Open the web browser from your Workstation.
- 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.`
- Press **Enter** to view the Home page.



2. Access **Properties**

- Select the **Properties** tab.
- If prompted, enter the Administrator User ID and Password. The default is **admin** and **1111**.
- Select the **Login** button.

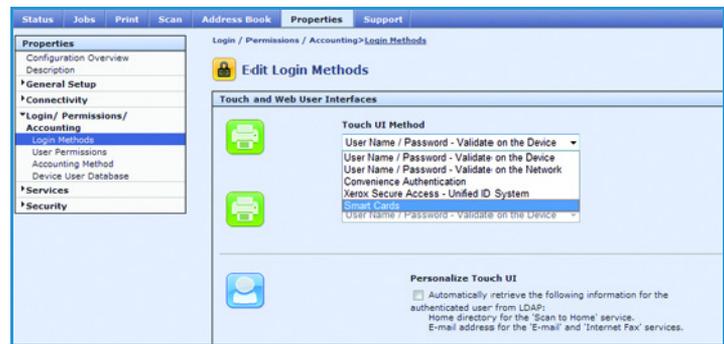


3. Enable the Smart Card software

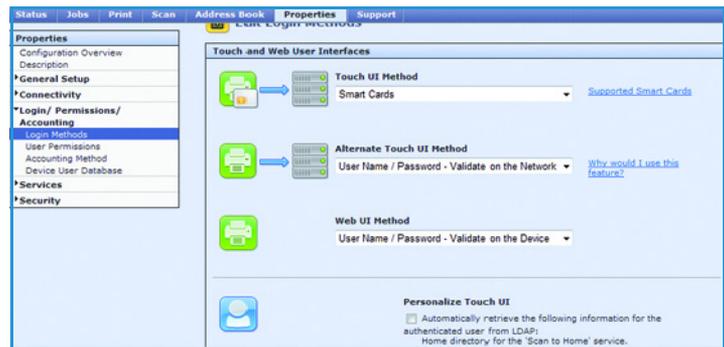
- Select the **Properties** link.
- Select the **Login/Permissions/Accounting** link.
- Select the **Login Methods** link.
- Select the **Touch UI Method** button.



- e. From the Touch UI Method drop-down menu, select **Smart Cards**.



- f. If you require users to have an alternative method of authentication, select **User Name/Password** from the Alternate Touch UI Method drop-down menu.
- g. If you require the device to use the E-mail address registered to the authenticated user, select the **Personalize Touch UI** checkbox.
- h. Select **Save**.



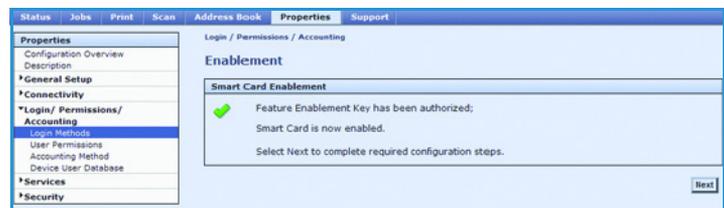
- i. In the **Smart Card Enablement** area, enter the unique Feature Enablement Key provided on the inside cover of the [Smart Card Enablement Guide](#).
- j. Select **Next**.



A confirmation message is displayed.

- k. Select **Next**. The Smart Card settings are now ready for configuring.

Note: No services will be restricted until Smart Card has been fully configured using Internet Services.



Configuring the Smart Card

Once the Smart Card feature has been enabled on the device it can be configured using Internet Services.

Configure Smart Card Authentication

Follow the instructions below to enable and configure the Smart Card:

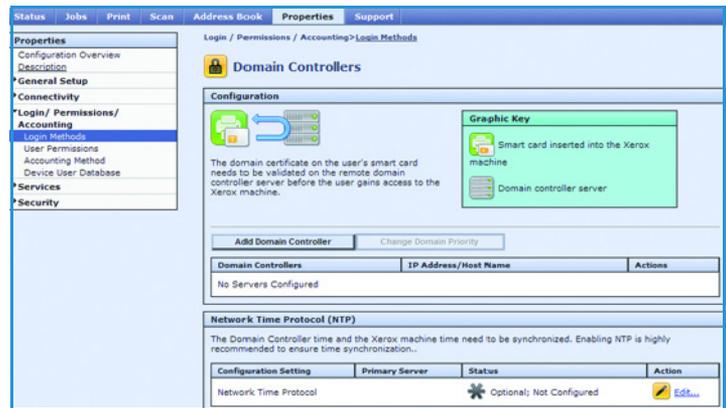
- In the Internet Services **Login/Permissions/Accounting** menu, ensure you have the **Login Methods** link selected.



- Enter the **Domain Controller** details for the authentication server.
 - Select **Domain Controller(s) - Edit** from the Configuration Settings list.

Note: Initially the Domain Controller(s) will be empty and the NTP server will not be set.

- Select **Add Domain Controller**.



- Select **Windows Based Domain Controller** or leave this box unchecked to select Linux Based Domain Controller.

- Select either IP Address or Host Name and enter the Domain Controller details. If you enter the Host Name, this must be the fully qualified Host Name.



- Ensure Port 88 is selected unless your Kerberos Port is different.
- Enter the **Domain** (this must be the fully qualified Domain Name).
- Select **Save**.

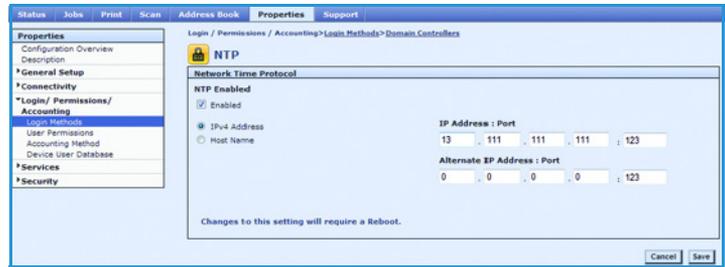
Enable NTP Service

3. Configure the **Date & Time** to update automatically

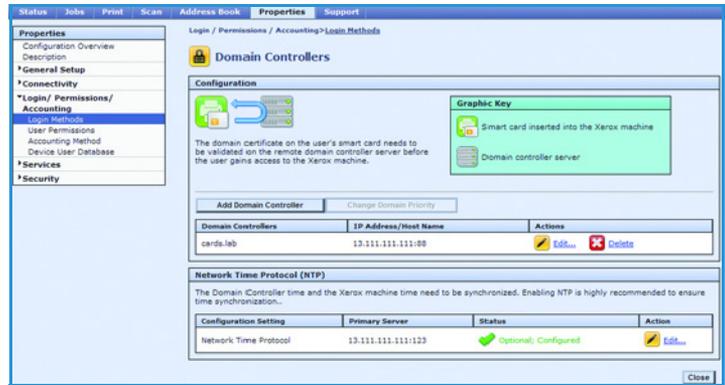
- a. Select the **Network Time Protocol - Edit** link.



- b. Select the **Enabled** box to enable NTP.
- c. Enter the IP address or Host Name of the Primary and Alternate Time Server. Often this can be the same address as the Domain Controller.
- d. Select **Save**.



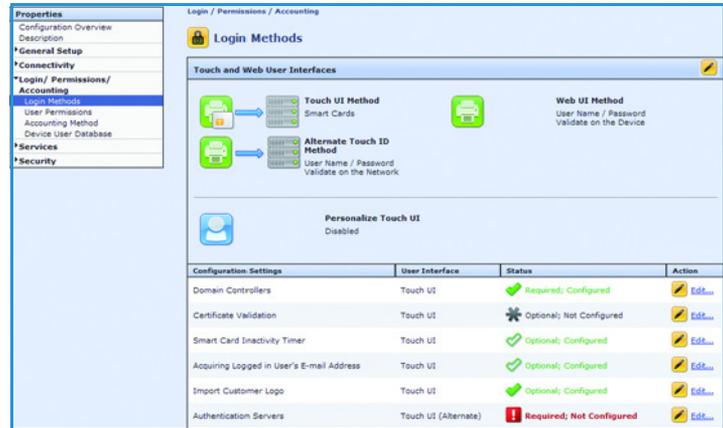
- e. View the summary screen and ensure all settings are correct.
- f. Select **Close**.



Configure Alternate Authentication

If Alternate Authentication is not required, go to [Configure a Security Certificate](#) on page 22.

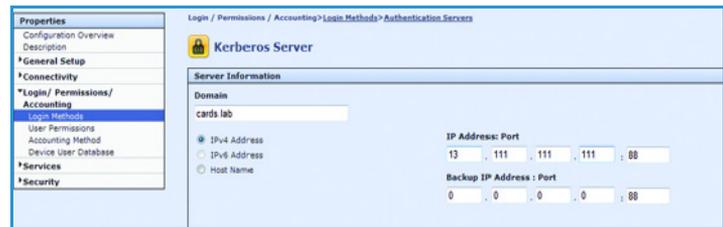
4. If Alternate Authentication is enabled, select the **Authentication Servers / Touch UI (Alternate) - Edit** link in the Configuration Settings list to configure the server.



- a. Select the **Authentication Type** from the drop-down menu.
- b. Select **Add New**.



- c. Enter the required **Domain** or **Realm**.
- d. Select either IP Address or Host Name and enter the server details. For most installations the Alternate Authentication server will be the same as the Smart Card Domain Controller.
- e. Select **Save**.
- f. Select **Close**.



Configure a Security Certificate

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

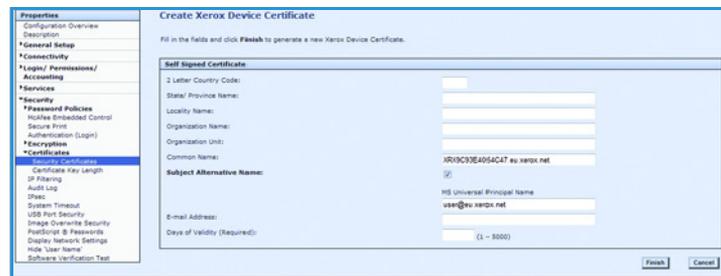
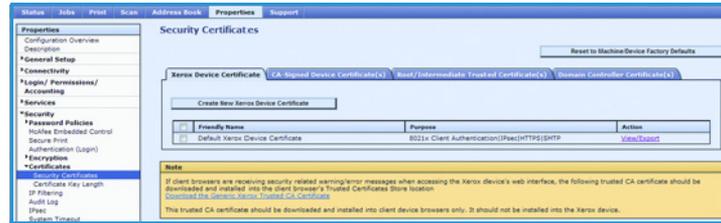
- [Create a Device Certificate](#) on page 23
- [Import a Certificate Authority Certificate](#) on page 23
- [Install a Domain Controller Certificate](#) on page 24

If certificate validation is not required, go to section [Configure Smart Card Inactivity Timer](#) on page 26.

Create a Device Certificate

The device automatically creates a self-signed certificate. Complete this section if you want to create a new device certificate.

5. To create a new device certificate:
 - a. In the Properties tab select the **Security** link.
 - b. Select **Certificates > Security Certificates**.
 - c. Select the **Xerox Device Certificate** tab.
 - d. Select **Create New Xerox Device Certificate**.
 - e. Complete the **Self Signed Certificate** fields.
 - f. Select **Finish**.
 - g. Proceed to [Configure SSL](#) on page 24.



Import a Certificate Authority Certificate

6. Complete these steps if you want to import a certificate from a Certificate Authority:
 - a. In the **Properties** tab select the **Security** link.
 - b. Select **Certificates > Security Certificates**.
 - c. Select the **Root/Intermediate Trusted Certificate(s)** tab.
 - d. Click **Install external Root/Intermediate trusted certificates**.
 - e. Click the **Browse** button and navigate to the location of your Certificate Authority certificates.
 - f. Click **Next**.
 - g. If the certificate is encrypted, enter the password at the **Password Required** screen.
 - h. Click **Next**.



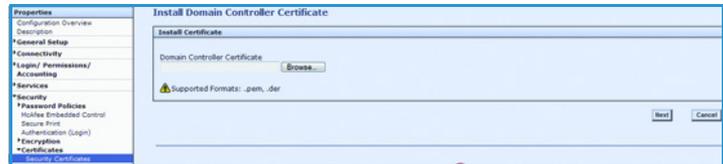
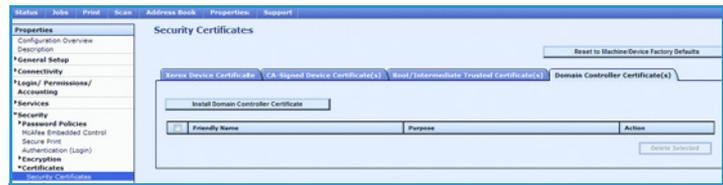
Note: Both RootCA and Intermediate CA certificates need to be imported to the MFD to establish a 'Chain of Trust' for the certificates located on the operator's smart card.

- i. Proceed to [Configure SSL](#) on page 24

Install a Domain Controller Certificate

7. Complete these steps if you want to install a domain controller certificate.

- a. In the **Properties** tab select the **Security** link.
- b. Select **Certificates > Security Certificates**.
- c. Select the **Domain Controller Certificates** tab.
- d. Click **Install Domain Controller Certificate**.
- e. Click the **Browse** button and navigate to the location of your Domain Controller certificates.
- f. Click **Next**.
- g. Continue until all required certificates have been uploaded.



Configure SSL

8. SSL is used to provide a secure connection between your computer and the MFD when security certificates are configured on the MFD. SSL is automatically enabled on the device. If you do not want to configure SSL, proceed to [Configure Certificate Validation](#) on page 25.

- a. In the **Properties** tab select the **Connectivity** link.
- b. Select **Setup**.
- c. In the **Protocol** list, select **HTTP - Edit**.

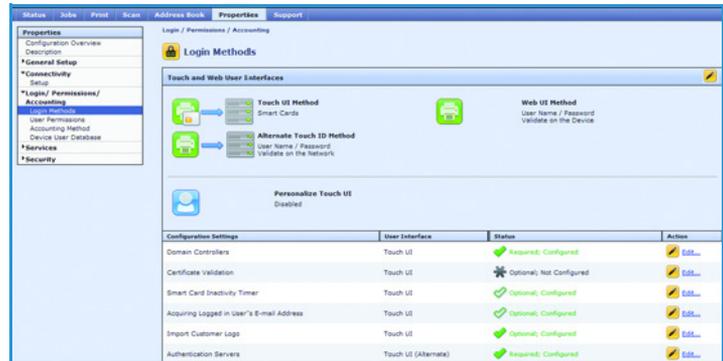
- d. If you want to Force Traffic over SSL, select **Yes (All HTTP requests will be switched to HTTPS)**.
- e. Select the required certificate from the **Choose Device Certificate** drop-down menu.
- f. If you have changes to apply, select **Save** and the device will reboot automatically. If you have not made any changes, select **Cancel**.



Configure Certificate Validation

9. If you do not require certificate validation proceed to [Configure Smart Card Inactivity Timer](#) on page 26.

- In the **Properties** tab, select the **Login/Permissions/Accounting** link.
- Select **Login Methods**.
- Select **Certificate Validation - Edit** in the Configuration Settings menu.



- Select the required **Validation Options**.
- If you have selected one or more option, click **Next** to configure further settings.



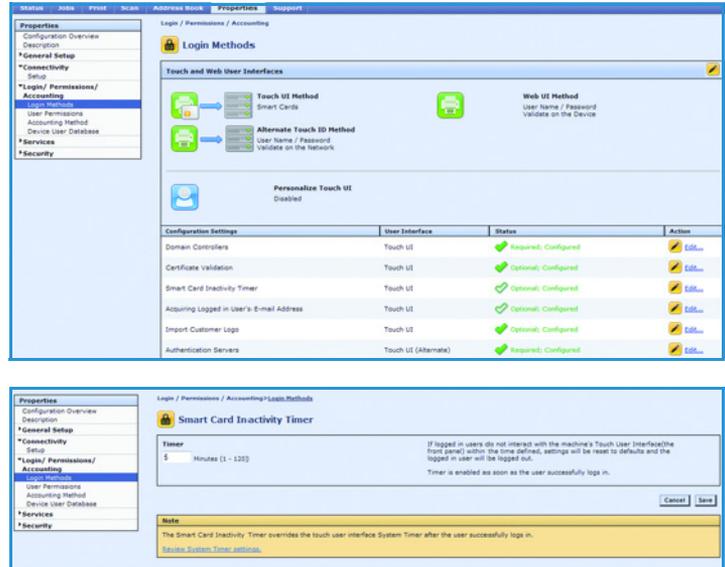
- If prompted, enter the **OCSP Server URL** to be used for certificate validation.
- If prompted, select **Proxy Server - Configure** to enter the proxy server information. If the OCSP server is outside the firewall, a proxy server may be required to access the server.
- Select the **Domain Controller Certificate(s)** to be used to validate each domain controller.
- Click **Save**.



Configure Smart Card Inactivity Timer

10. If you do not require inactivity timeout settings for Smart Card authentication, proceed to [Configure Acquiring Logged-In User's E-mail Address](#) on page 26.

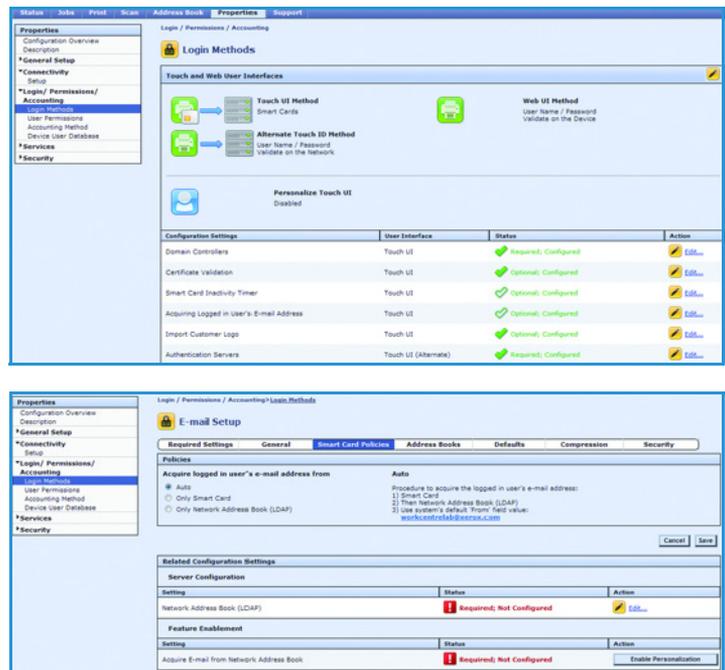
- a. In the **Properties** tab, select the **Login/Permissions/Accounting** link.
- b. Select **Login Methods**.
- c. Select **Smart Card Inactivity Timer - Edit**.
- d. Enter the required number of minutes for **Timer**.
- e. Click **Save**.



Configure Acquiring Logged-In User's E-mail Address

11. This section requires you to configure LDAP and SMTP server information. If you do not want to configure Acquiring Logged-In User's E-mail Address settings, proceed to [Confirm the Installation](#) on page 34.

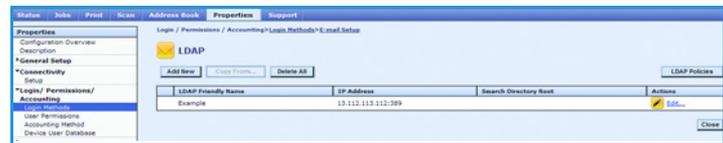
- a. In the **Properties** tab, select the **Login/Permissions/Accounting** link.
- b. Select **Login Methods**.
- c. Select **Acquiring Logged In User's Address - Edit**.
- d. Select the required option for **Acquire logged in user's e-mail address**.
- e. If you select **Auto** or **Only Network Address Book (LDAP)**, click **Network Address Book (LDAP) - Edit** to configure LDAP server settings.
- 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**. This is typically related to the server's domain name. For example, if the server's Fully Qualified Domain Name 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**.



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

Note: Smart cards use a ticket based authentication to LDAP and require SASL for authentication.

- p. Click **Save**.
- q. Click **Close**.

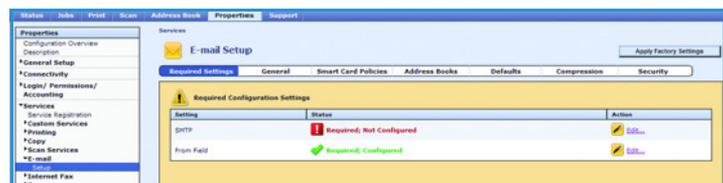


Configure SMTP (E-mail) Settings

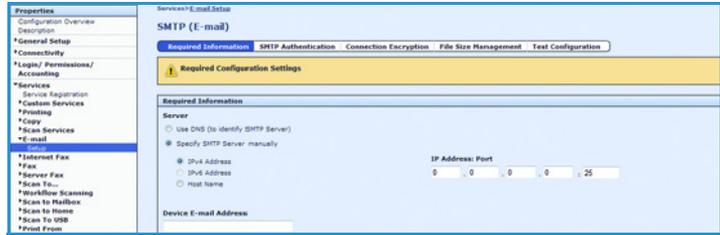
- 12. In the **E-mail Setup** screen, select the **Required Settings** tab.



- a. Select **SMTP - Edit**.



- b. Select **Use DNS (to identify SMTP Server)** to configure the server address using DNS, or select **IP Address** or **Host Name** and enter the SMTP server address.
- c. Enter the required **Device E-mail Address**.
- d. Select **Save**.



Configure SMTP Authentication

- 13. Select **SMTP - Edit**.
 - a. Select the **SMTP Authentication** tab.
 - b. For the required method of authentication for **SMTP Login credentials applied to e-mail jobs sent from the machine's touch interface** select **Logged-in User**.



Note: The Logged-in user's credentials are typically used to provide authentication for the SMTP server when Smart Card authentication is enabled.

- c. Select **Always Use Kerberos Tickets**.
- d. Select **None** for automated emails.
- e. Select **Save**.

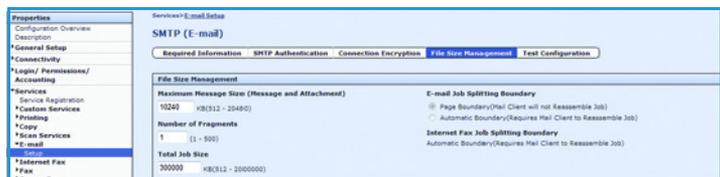
Configure Connection Encryption

- 14. Select **SMTP - Edit**.
 - a. Select the **Connection Encryption** tab.
 - b. Select the required encryption setting.
 - c. Select **Save**.



Configure File Size Management

- 15. Select **SMTP - Edit**.
 - a. Select the **File Size Management** tab.



Note: This screen defines how large email payloads are managed.

- b. Select the required settings.
- c. Select **Save**

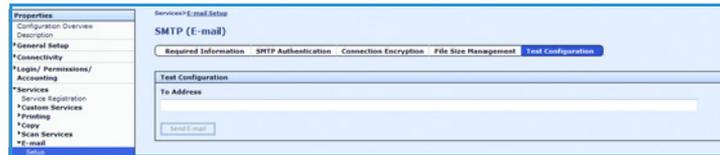
Test Configuration

16. Select **SMTP - Edit**.

- Select the **Test Configuration** tab.

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

- Enter a valid e-mail address in the To Address field.
- Select **Send E-mail**.



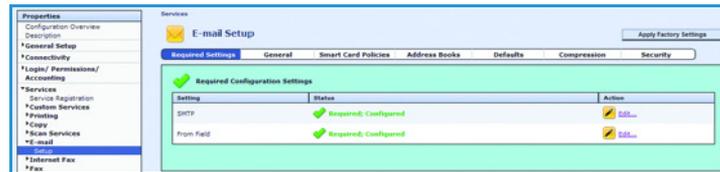
Note: If the SMTP settings are correct, the screen will display a success message and an e-mail will be received at the address

- Select the **Required Information** tab.
- Required Settings Configured** displays to confirm required settings are configured.
- Select **Save**.

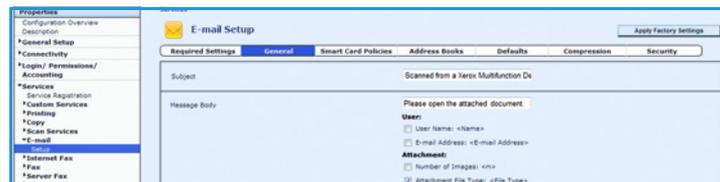


Configure General E-mail Settings

17. In the **E-mail Setup** screen, select the **General** tab.



- Enter the required information to display in the **Subject** of an e-mail sent from the MFD.
- Select the required information to display in the **Message Body**.
- Enter the information to be included in the **Signature**.
- Select the required option for printing a **Confirmation Sheet** from the drop-down menu.
- Select **Enabled** for **Auto Add Me** if you want the MFD to automatically add the logged-in user's e-mail address to the To: field.
- Select **Enabled** for **Only Send to Self** if you want the MFD to only send e-mails to the user who is logged in at the MFD.
- Select **Apply**.



Configure Address Books

18. Select the **Address Books** tab.

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



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

Configure E-mail Defaults

19. Select the **Defaults** tab.

- a. Select the required options for e-mail default settings.
- b. Save your changes.



Configure E-mail Compression

20. Select the Compression tab.

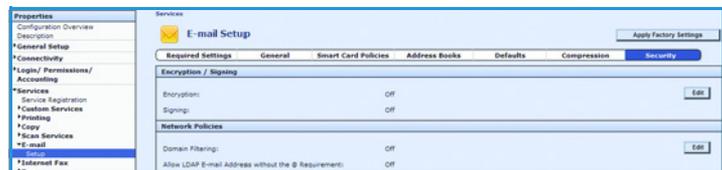
- a. Select the required **Compression Settings**.
- b. Click **Apply**.



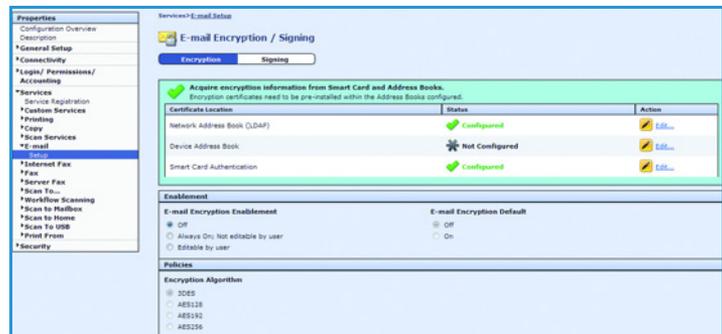
Configure E-mail Security

21. Select the **Security** tab.

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

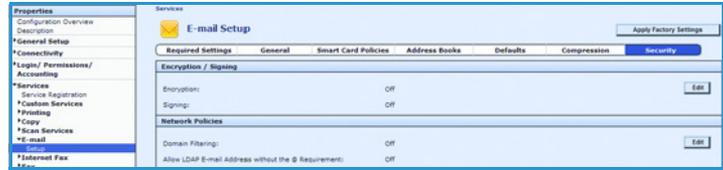


- b. Select the required **Encryption Enablement** setting;
 - **Off** -E-mail cannot be signed
 - **Always On** - E-mail must be signed
 - **Editable by user** - E-mail can be sent signed or unsigned according to local user settings.

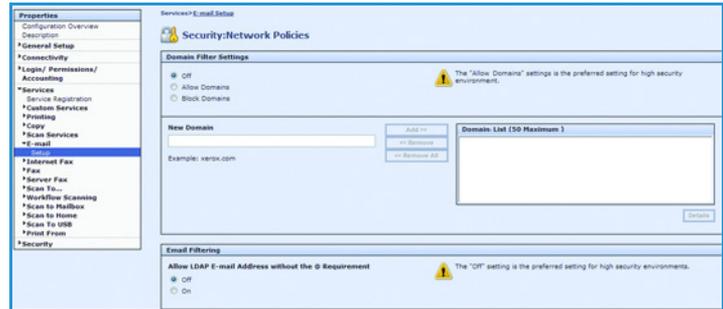


- c. If you selected Editable by User, select **On** for **E-mail Encryption Default** if you require signing to be on by default.
- d. Select the required **Encryption Algorithm**.
- e. Select **Apply**.

22. If you want to configure e-mail domain restrictions, click **Edit** in the **Network Policies** area.

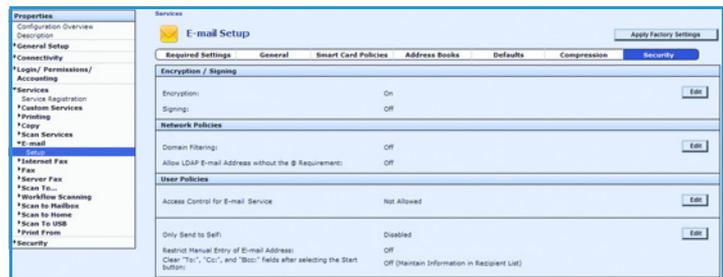


- a. Select the required restrictions.
- **Domain Filtering** enables you to configure a list of domains to allow or block e-mails.
 - **E-mail Filtering** allows you to send internal e-mail without the need to add @ corporate name. This option requires your e-mail server to be configured to allow this.
- b. Select **Save**.



23. 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 required, click **Edit** in the **Only Send to Self** area.
- d. Select the required settings for **User Policies**.
- e. Save your changes.



The Smart Card settings are now configured.

Printing Features

The Hold All Jobs and Secure Print features can be configured to ensure jobs are held securely at the MFD until the user authenticates at the Control Panel.

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.

1. Access **Internet Services** and select **Properties**. Refer to [Access Internet Services](#) on page 18 for instructions.

- a. Select **Services > 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 must 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 (User ID Unknown)**. 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 the user enters the same passcode to release them. Further information about how to use Secure Print is available in your User Guide. You can configure the Secure Print Driver Default settings to require the user to enter a User ID to release secure print jobs at the Control Panel, instead of a passcode. If you want to configure Secure Print Driver Defaults, follow these instructions.

1. Access **Internet Services** and select **Properties**. Refer to [Access Internet Services](#) on page 18 for instructions.
 - a. Select **Services > Printing > Secure Print**.
 - b. Select the **Print Driver Defaults** tab.
 - c. Select the required **Method**:
 - **Passcode**: requires users to type a passcode to release their 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 users to log in at the Control Panel to release their Secure Print jobs.
 - d. Click **Apply**.



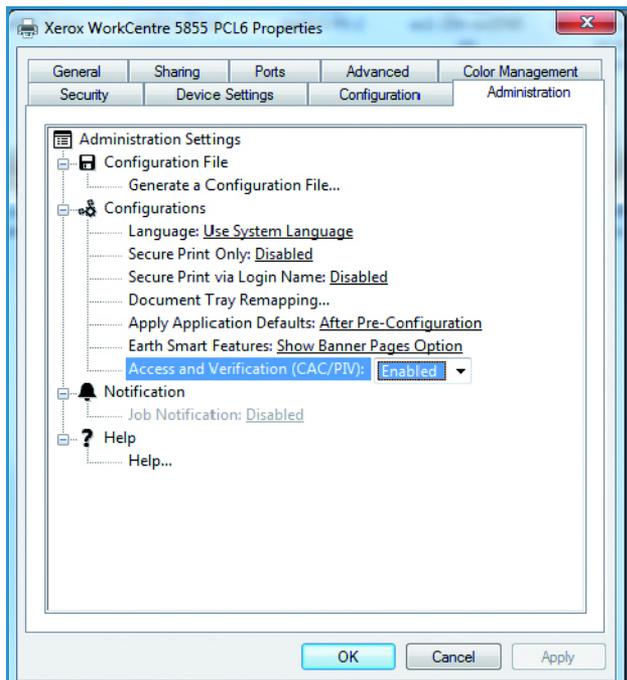
Further information on how to configure Secure Print Settings is available in the System Administrator Guide.

Configure the Print Driver

Your print driver can be configured to pull the user's name (alias) from the smart card certificate, or from the Windows Operating System. To configure the print driver to pull the user's name from the smart card certificate follow these instructions.

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

Note: If Hold All Jobs or Secure Print Driver Defaults are configured at the MFD, they may override the settings configured in your print driver. Refer to [Configure Hold All Jobs](#) on page 32 and [Configure Secure Print Driver Defaults](#) on page 33.



Confirm the Installation

When the card reader and the software has been installed and configured, the Card Reader Detected screen displays on the Xerox® device local user interface.

Smart Card is now ready for use.

Note: If the card reader is not detected, refer to [Troubleshooting Tips](#) on page 39 for information.

Using Smart Card

Once the Smart Card has been enabled, each user must insert a valid card and enter their Personal Identification Number (PIN) on the touch screen. When a user has finished using the Xerox® device, they are then required to remove their card from the card reader to end the session. For instances where a user forgets to remove their card, the machine will end the session automatically after a specified period of inactivity.

Follow the instructions below to use the Smart Card:

1. The Authentication Required window may be displayed on the touch screen, depending on your device configuration.
2. Insert your card into the card reader.
3. Use the touch screen and numeric keypad to enter your PIN and then select **Enter**.
4. If the card and PIN are authenticated, access is granted.

Note: If the access attempt fails, refer to [Troubleshooting Tips](#) on page 39.

5. Complete the job.
6. To end the session, remove your card from the card reader.
The current session is terminated and the Authentication Required window is displayed.

Troubleshooting

4

For optimal performance from your card reader, ensure the following guidelines are followed:

- The Card Reader is only compatible with network connected products.
- Ensure the Card Reader is plugged into the Network Controller. Refer to [Connect the card reader to the Xerox® device](#) on page 17 for instructions.
- Do not position the Card Reader in direct sunlight or near a heat source such as a radiator.
- Ensure the Card Reader does not get contaminated with dust and debris.

Fault Clearance

When a fault occurs, a message displays on the User Interface which provides information relating to the fault. If a fault cannot be resolved by following the instructions provided, refer to [Troubleshooting Tips](#) on page 39.

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 Welcome and Support Center. The Welcome and Support Center will want to know the nature of the problem, the Machine Serial number, the fault code (if any) plus the name and location of your company.

Contact Xerox using the numbers 1-800-ASK-XEROX or 1-800-275-9376.

Locating the Serial Number

- Press the **Machine Status** button on the Control Panel.
The Machine Information tab is displayed.
- The Machine Serial Number is displayed on this screen.

Note: The serial number can also be found on a metal plate inside the front door.

Troubleshooting Tips

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

If you experience a problem during the installation process please refer to the [During Installation](#) problem solving table below.

If you have successfully installed the Smart Card solution but are now experiencing problems, refer to [After Installation](#) on page 40.

During Installation

Problem	Possible Cause	Solution
Card reader is installed but no message displays on the User Interface	Card reader is faulty.	<ul style="list-style-type: none"> Try a different card reader. Contact the System Administrator.
	Card reader connection is faulty.	<ul style="list-style-type: none"> Check the cable is plugged in correctly. Refer to Connect the card reader to the Xerox® device on page 17 for instructions. Unplug the card reader cable then plug back in. Plug the card reader into a different USB port.
	Card reader is not compatible.	<ul style="list-style-type: none"> Check that the card reader is on the list of compatible devices, refer to Supported Card Readers on page 7.
	Smart Card access is not enabled on the machine.	<ul style="list-style-type: none"> Enable Smart Card through the Properties set up screens using Internet Services, refer to Software Configuration on page 18.

After Installation

Problem	Possible Cause	Solution
The login was successful, however you do not have the appropriate access to the operation you requested	LDAP not configured properly or local user permission roles not configured properly.	<ul style="list-style-type: none"> Check the authorization method.
The passcode entered was incorrect	Incorrect PIN has been entered. Caution: Consecutive incorrect entries may lead to your card being locked.	<ul style="list-style-type: none"> Carefully re-enter the PIN.
Authentication failed. There is a problem with your card that is preventing successful login	Certificates cannot be read from the card.	<ul style="list-style-type: none"> Contact the Registration Authority to reload the certificates or get a new card.
Authentication failed because the device was unable to access the remote server (Domain Controller) or the authentication sequence failed	Domain Controller IP Address or Host Name is incorrect.	<ul style="list-style-type: none"> Verify the server address is entered correctly.
	Incorrect Domain.	<ul style="list-style-type: none"> Verify the Domain has been properly configured.
	Network error	<ul style="list-style-type: none"> Check the network cable is firmly connected.
The number of attempts have been exceeded	Card has been locked due to failed login attempts.	<ul style="list-style-type: none"> Contact the Registration Authority to reset the PIN or to get a new card.
Server Certificate Failed Authentication failed because the remote server (Domain Controller) certificate could not be found, is invalid, has expired or been revoked	This is usually because the device does not trust the certificates on the Smart Card.	<ul style="list-style-type: none"> Ensure all the "chain of trust" certificates are imported on the device. Check the Operator's CAC to see which Root CA and Intermediate CA issued the CAC certificates.
Card reader not detected	The card reader has been disconnected.	<ul style="list-style-type: none"> Verify that the card reader is properly connected. If you suspect the reader has failed, swap with a known working reader.

Problem	Possible Cause	Solution
Invalid Timestamp. Authentication failed due to a time or date difference between the device and the remote server (Domain Controller)	NTP not enabled or properly configured.	<ul style="list-style-type: none"> • Verify that Network Time Protocol is correctly set up, refer to Enable NTP Service on page 21.
	GMT offset is not set correctly.	<ul style="list-style-type: none"> • If you are not using DHCP, verify the date and time and GMT Offset (Time Zone) is correct. Instructions are available in the System Administrator Guide. • Verify that GMT offset is correct for Daylight Savings Time. • Unforeseen errors are mapped to this error message.
Cannot see the Internet Services web page	IP Address incorrect or has been reset.	<ul style="list-style-type: none"> • 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 Machine Status, then Information Pages. Select the Configuration Report from the list and select Print.

