Version 4.0
09/11

Xerox® Smart Card

Xerox® WorkCentre 7525/7530/7535/7545/7556

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

Document version 4.0: September 2011

Table of Contents

1 Introduction

The Xerox 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.

The key benefit of this solution is its two-factor identification requirement. Users must insert their access card and enter a unique Personal Identification Number (PIN) at the device. This provides added security in the event that a card is lost or stolen.

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.

The Xerox Smart Card enablement kit integrates with Xerox multifunction printers and existing smart and personal identity verification cards and readers.

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.

Compatibility

This solution is compatible with the following product and configurations:

Configuration	Software Level
Xerox WorkCentre 7525/7530/7535/7545/7556	06x.120.xxx.xxxxx

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

Card Readers and Card Types

Supported Card Types

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

- Gemalto TOP DL GX4 144K V2.6.2b Applets
- Oberthur ID-One Cosmo v5.2 128K V2.6.2 Applets
- Oberthur ID-One Cosmo v5.2 72K V2.6.1 Applets
- Oberthur ID-One Cosmo v5.2D 72K V2.6.1 Applets
- Oberthur ID-One Cosmo v5.2 72K V2.6.2 Applets
- Gemalto GemCombiXpresso R4 dual interface 72K V2.6.2 Applets
- Axalto Access 64KV1
- Axalto Access 64KV1
- Gemplus GXP3 64V2N V2.6.1 Applets
- Gemalto Cyberflex Access V2C 64K V2.6.1 Applets
- Oberthur ID-One Cosmo V5.2D 64K
- Oberthur OCS Galactic V1 32K V1 Applets
- Oberthur Cosmo V4 32K V1 Applets
- Schlumberger / Axalto Cyberflex V2 32K V1 Applets

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

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 firmware

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

> Note: Information about CCID compliant card readers can be obtained from various websites, for example www.pcsclite.alioth.debian.org/ccid.This site is not a Xerox website and is not endorsed by Xerox.

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 on disc with 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*.

The installation will take approximately one hour for each device. The following items are required in order to complete the installation:

Item	Supplier
Compatible Card Reader (refer to Supported Card Types on page 7)	Customer
Compatible Access Card (refer to Supported Card Types on page 7)	Customer
Smart Card enablement kit 498K17543 (one for each Xerox device)	Xerox
Feature Enable Key	Xerox
TCP/IP enabled on the device	Customer
DNS Host name or static IP address assigned	Customer
Network Settings to be checked to ensure network is fully functional	Customer
Domain Controller (DC) information: • Domain Controller authentication environment • IP address or Host Name • Domain information • Domain Controller Root and Intermediate certificates • Check that all certificates are in 64 bit X.509 format • Determine if the DC is registered with the OCSP at this site	Customer
Online Certificate Status Protocol (OCSP) Server Information: • OCSP Server URL • OCSP - Root and Intermediate Certificates • Check that all certificates are in 64 bit X.509 format	Customer
Proxy Server configuration details	Customer

To set up the Domain Controller (DC) validation, you will need to determine if your site validates the DC against the Online Certificate Status Protocol (OCSP) server. Many sites use OCSP to validate individuals, but do not register the DC with it. If you set up the Xerox device to validate the DC and it isn't registered, the procedure will fail.

If your site does register the DC with OCSP, you will need to decide whether:

- to validate the DC against OCSP before validation of the user, or
- to validate the DC after validation of the user

The first method requires installation of the DC certificate as part of this procedure and is the more accepted method for validation. The second method retrieves the DC certificate automatically for each authentication and doesn't require installation of the DC certificate onto the Xerox device.

An additional option is to combine the first and second options and compare the retrieved DC certificate to the one stored at installation. This provides the most security as it prevents rogue DCs masquerading as the real DC.

> Note: Certificates are often obtained from the Information Technology professionals that support your organization. If you are unable to obtain the required certificates, refer to the process outlined in Appendix A. You can determine the domain that you are registered in using the process outlined in Appendix B.

Server Specifications

Prior to installation, ensure your network infrastructure supports *Smart Card* or *Personal Identification Verification (PIV)*.

Names or IP addresses of all servers and domains are required during setup.

Electrical Requirements

The USB port on the back of the Xerox device network controller provides the power required for any of the supported card readers.

Installation

3

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

There are 4 main installation procedures to follow in sequence.

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

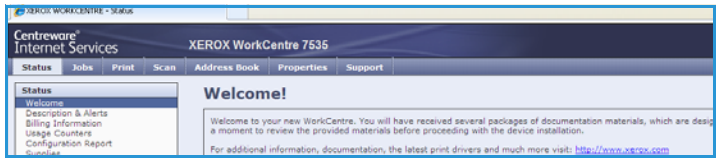
Software Enablement

Prior to installing the *Xerox Smart Card* solution, the software requires enabling on your Xerox device using the Internet Services. The Feature Enable Key is printed on the inside cover of the Enablement guide provided within the *Xerox Smart Card* kit.

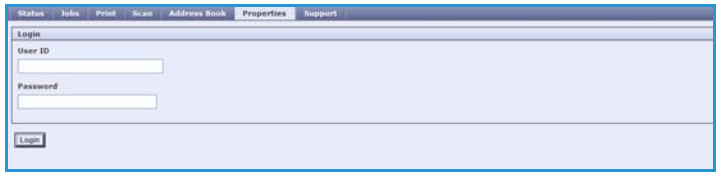
Follow the instructions below to enable the device software.

Note: Some of the steps shown may require the System Administration password for your device to be entered.

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.

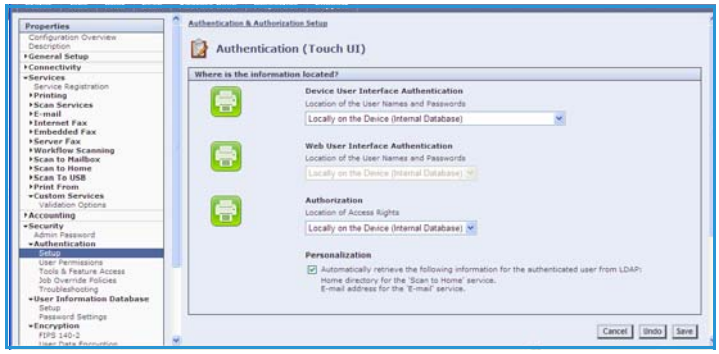


   c. Press **Enter** to view the Home page.
2. Access **Properties**
   a. Select the **Properties** tab.
   b. If prompted, enter the Administrator User ID and Password. The default is **admin** and **1111**.



   c. Select the **Login** button.
3. **Enable the** *Smart Card* **software**
   a. Select the **Security** link.
   b. Select the **Authentication** link.
   c. Select **Setup** in the directory tree.
   d. In the **Authentication & Authorization Setup** area, select **Edit Methods....**

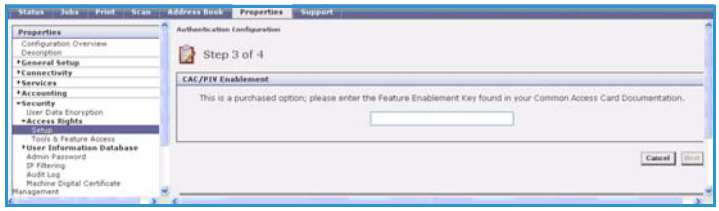
   e. Set the *Device User Interface Authentication* option to **Smart Card (CAC)/Personal Identity Verification (PIV)** using the drop-down menu. If you require the device to use the E-mail address registered to the authenticated user, select **Personalization.**



   f. Select **Save**.

g. Enter the unique *Feature Enable Key* provided on the inside cover of the Smart Card Enablement Guide.

h. Select **Next**.



A confirmation message is displayed.

i. 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.

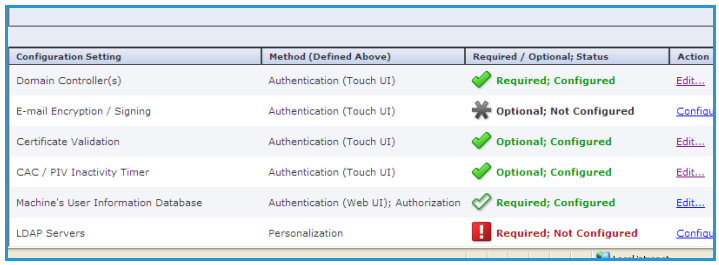
Configuring Smart Card

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

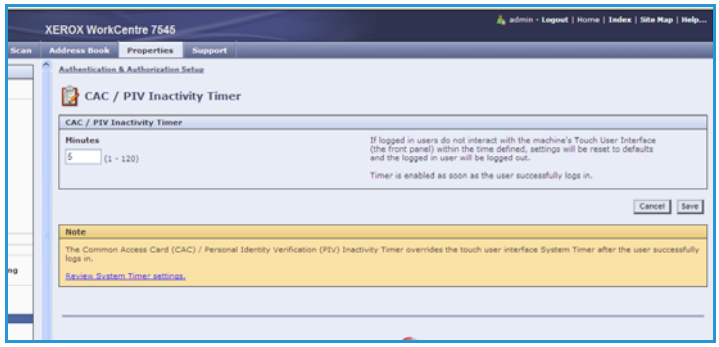
Follow the instructions below to enable and configure the *Smart Card*:

1. Access **Internet Services** and select **Properties**. Refer to Access Internet Services on page 12 for instructions.
2. Configure the **Date & Time** to update automatically
   a. Select the **General Setup** link, then **Date & Time**.
   b. Select **Automatic Using NTP**.
   c. Check the Time Zone is set to the correct option for your region.
   d. Select **Apply**. The device will reboot to apply the changes.

   Notes:
   - The sign in front of the number is important. Most of Europe is plus of Greenwich Mean Time, while North America is minus. Please consider the implications of *Daylight Savings Time* when selecting the *Offset of Local Time Zone* option.
   - If *Network Time Protocol* is not available, check that the time set on the device matches the network time on the Domain Controller Authentication Server. Refer to the System Administrator guide for instructions. If using Network Time Protocol (NTP) do not change the time on the device.
3. Access the **Smart Card** settings
   a. Select the **Authentication** link.
   b. Select **Setup** in the directory tree.
   c. Select **Smart Card Inactivity Timer** from the *Authentication Configuration* window.



   d. Enter the **Smart Card Inactivity Timeout** required between *1* and *120* minutes. The default setting is *5* minutes.
   If the machine is inactive for the period of time specified, it will end the session automatically.
   e. Select **Save**

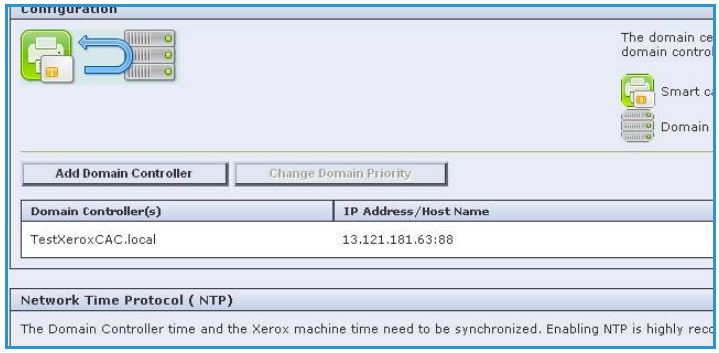


Note: At the completion of configuration of Smart Card, you can return to this screen and Configure the Device Access permissions if required. Refer to the System Administrator guide for your product.

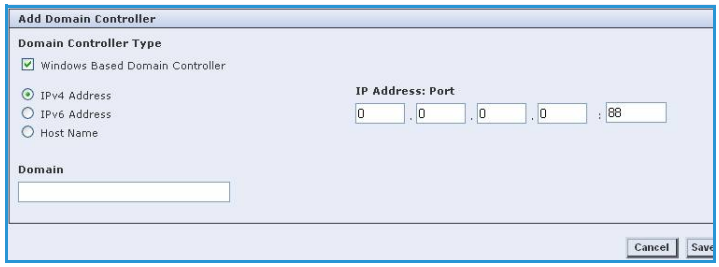
4. Enter the **Domain Controller** details for the authentication server.
   a. Select **Domain Controller(s)** from the *Authentication Configuration window*.

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

   b. Select **Add Domain Controller**.



   c. Ensure the **Domain Controller Type** is configured correctly for your authentication environment.
   d. Enter the IP Address or enter the Domain Controller Host Name (this must be the fully qualified Host Name).



   e. Ensure Port 88 is selected unless your Kerberos Port is different.
   f. Enter the *Domain Name* (this must be the fully qualified Domain Name).
   g. Select **Save**.
5. Configure Certificate Validation
   a. Select the **Certificate Validation** configure option.

   Note: Ensure the Domain Controller is configured prior to the next step.

   The default settings for registering the DC with OCSP is **No.**

   If you wish to validate the DC against OCSP before validation of the user:

   a. Select the **Yes** check box for **Validate the domain controller certificate stored on the device against the OCSP server**.
   b. Select **Next.**
   c. Enter the *OCSP Server Service URL* details.

   Note: Depending on your environment, these details may be case sensitive.

   If you wish to validate the DC against OCSP after validation of the user:

   a. Check the box for **Validate the certificate returned from the domain controller server against the OCSP server**.
   b. Enter the *OCSP Server Service URL* details.

6. If you wish to validate the DC certificate retrieved as part of the user authentication process against the one stored during installation, check the box for **Validate domain controller certificate returned by the domain controller server matches the domain controller certificate stored on the device**.

   Note: To change the Domain Controller search order, select the controller and use the up and down arrows on the right side of the screen to promote or demote the controller order.

7. Load the DC root and intermediate certificates and the OCSP root and intermediate certificates.
   a. Select **Security** then **Trusted Certificate Authorities Page** option or select **Trusted Certificate Authorities** from the menu.
   b. At the *Trusted Certificates Authorities* screen, select **Add**.
   c. Browse to the previously retrieved certificates and add them one at a time.
   d. Select the certificate then select the **Upload Certificate Authority** button to add each one.
   e. Repeat the process until all certificates are installed.
   f. Select **Close**.
8. Check the Proxy Server details are configured.
   a. If required by your network environment, ensure the Proxy Server details have been configured.
   b. Select the **Properties** tab, then **Connectivity, Protocols** and **Proxy Server** and enter the details.
   c. Select **Apply**.

The Smart Card settings are now configured. You are now ready to install the Smart Card hardware using the instructions starting on the next page.

Hardware Installation

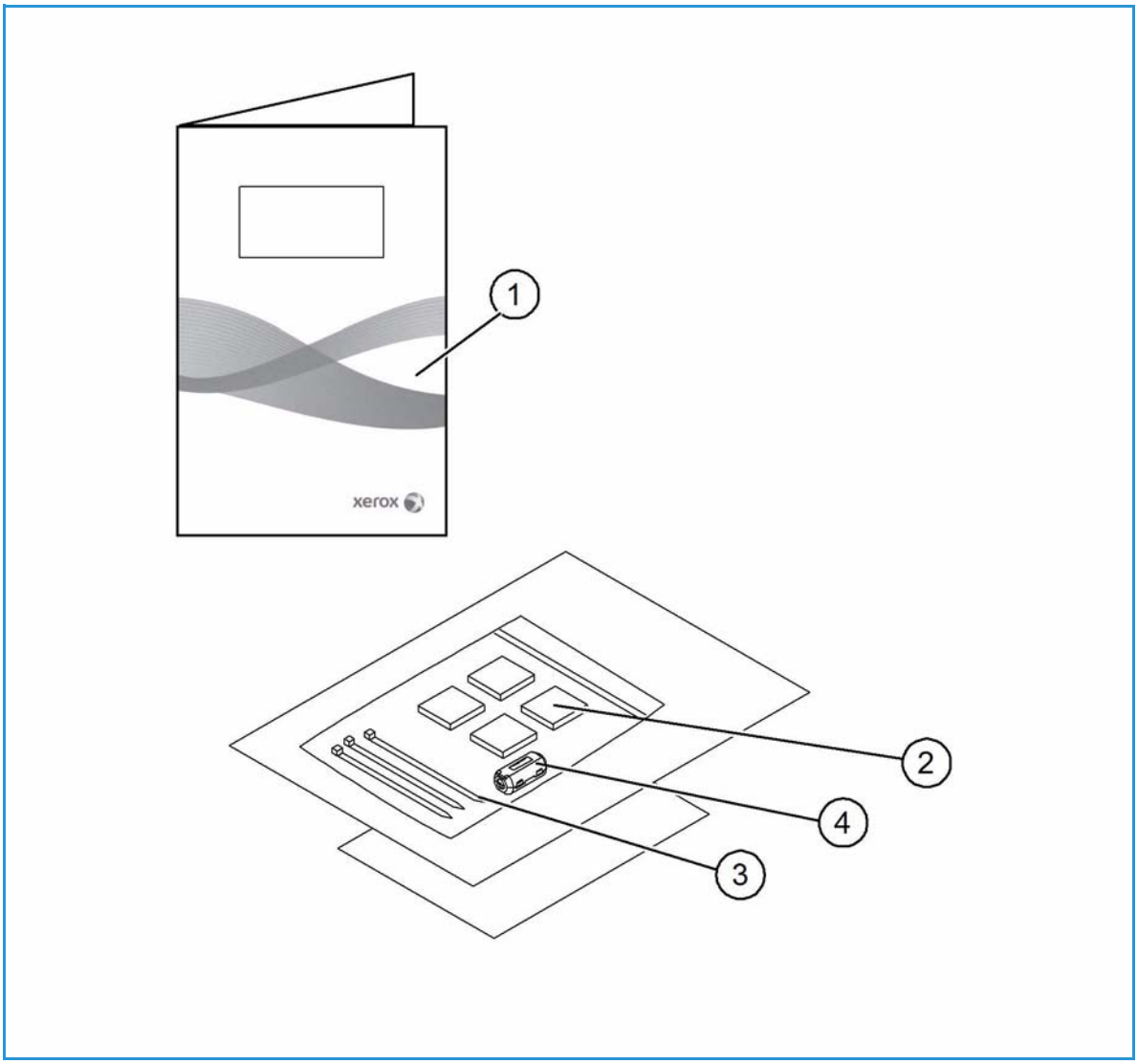
Install the card reader device using the following instructions.

1. Unpack the Smart Card Enablement Kit

   The kit contains the following items:

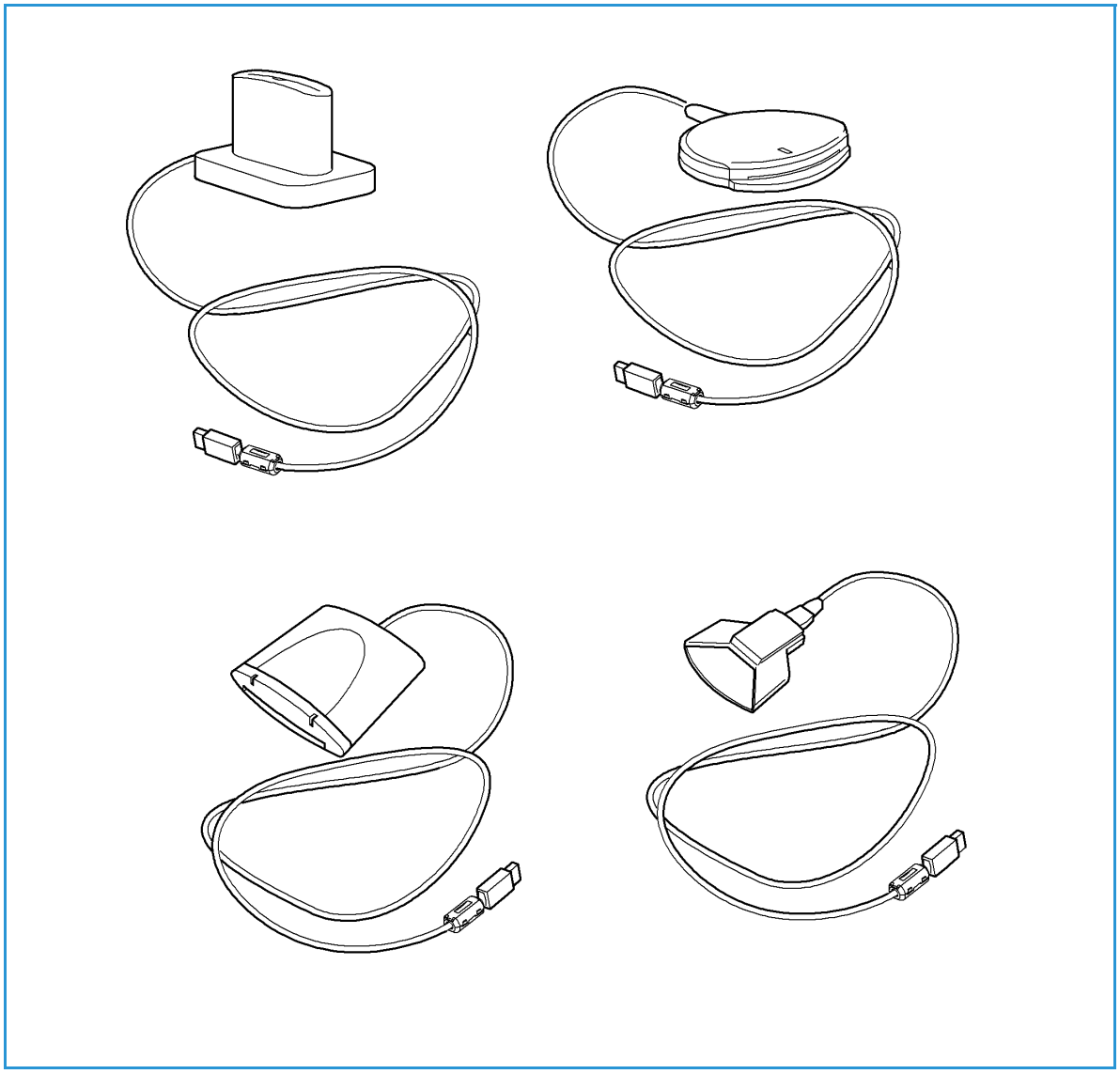
   - Xerox Smart Card Enablement Guide (1)
   - Four Dual Lock Fastener pads (Velcro) (2)
   - Three Cable Ties (3)
   - One Ferrite Bead (4)

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



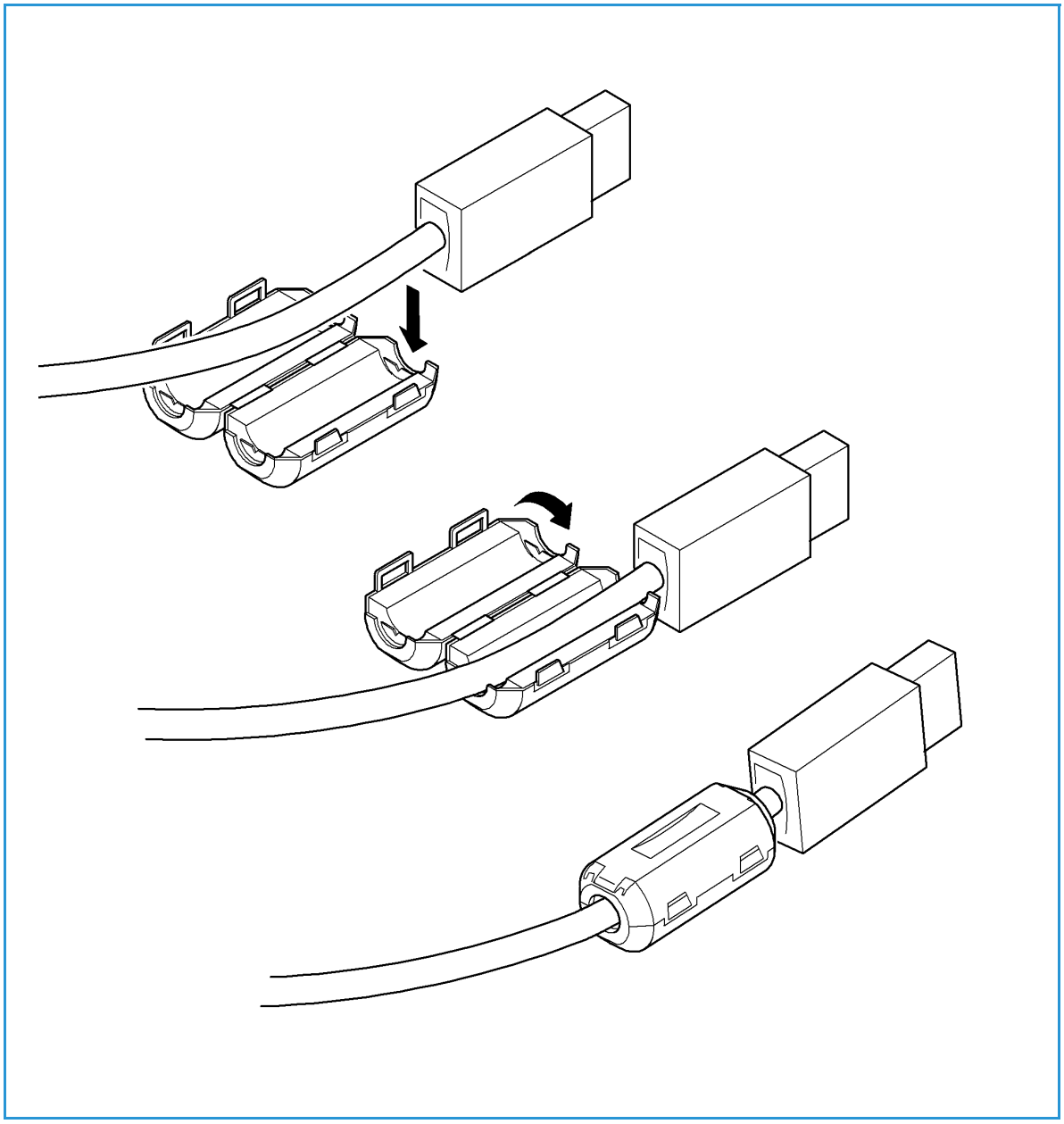
2. Locate the card reader device being installed
   - There are four types of card reader available, one upright model or three slimline models.
   - Locate the device being installed and ensure it has been configured.

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

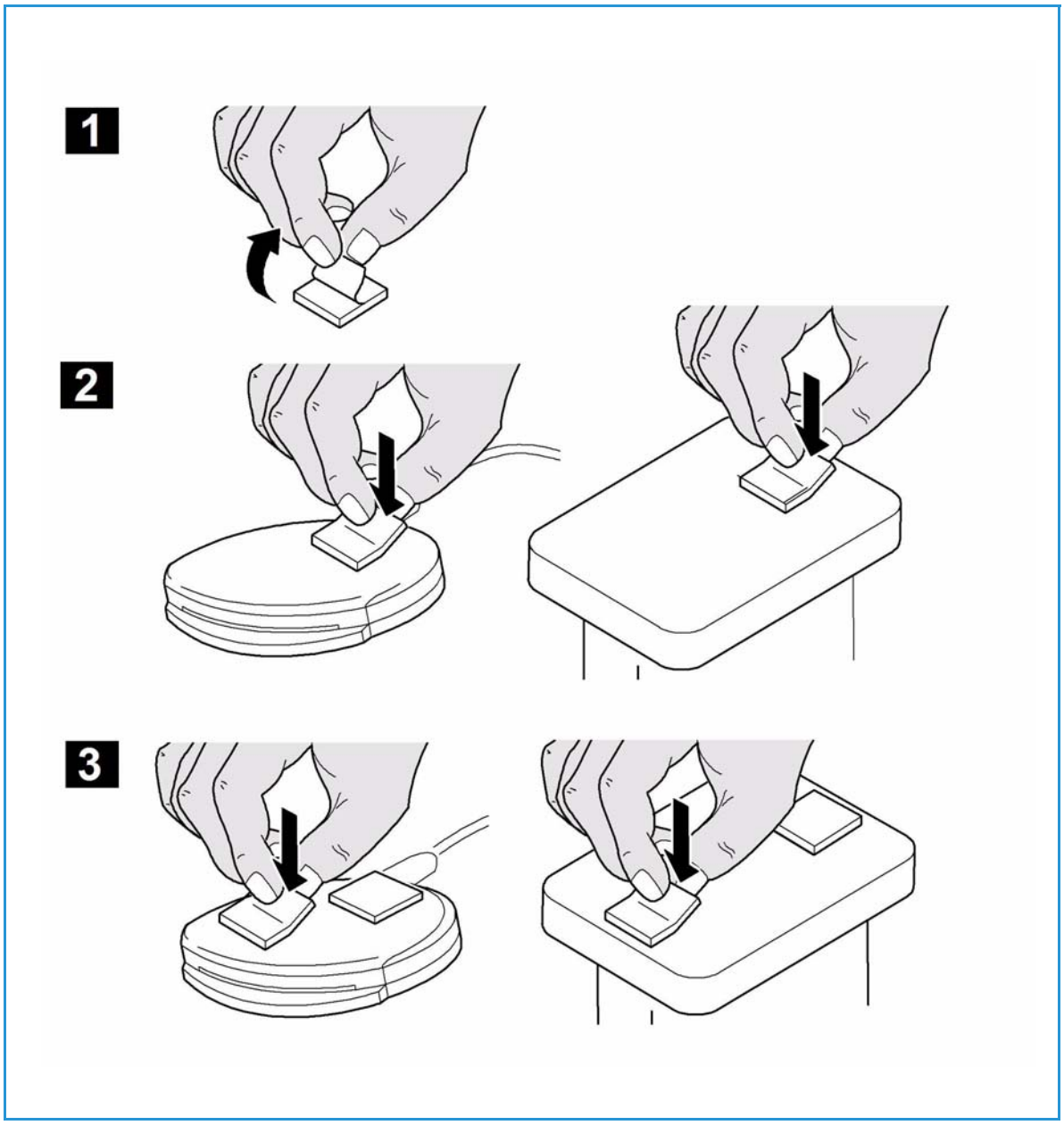


3. Attach the ferrite bead to the reader cable.

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

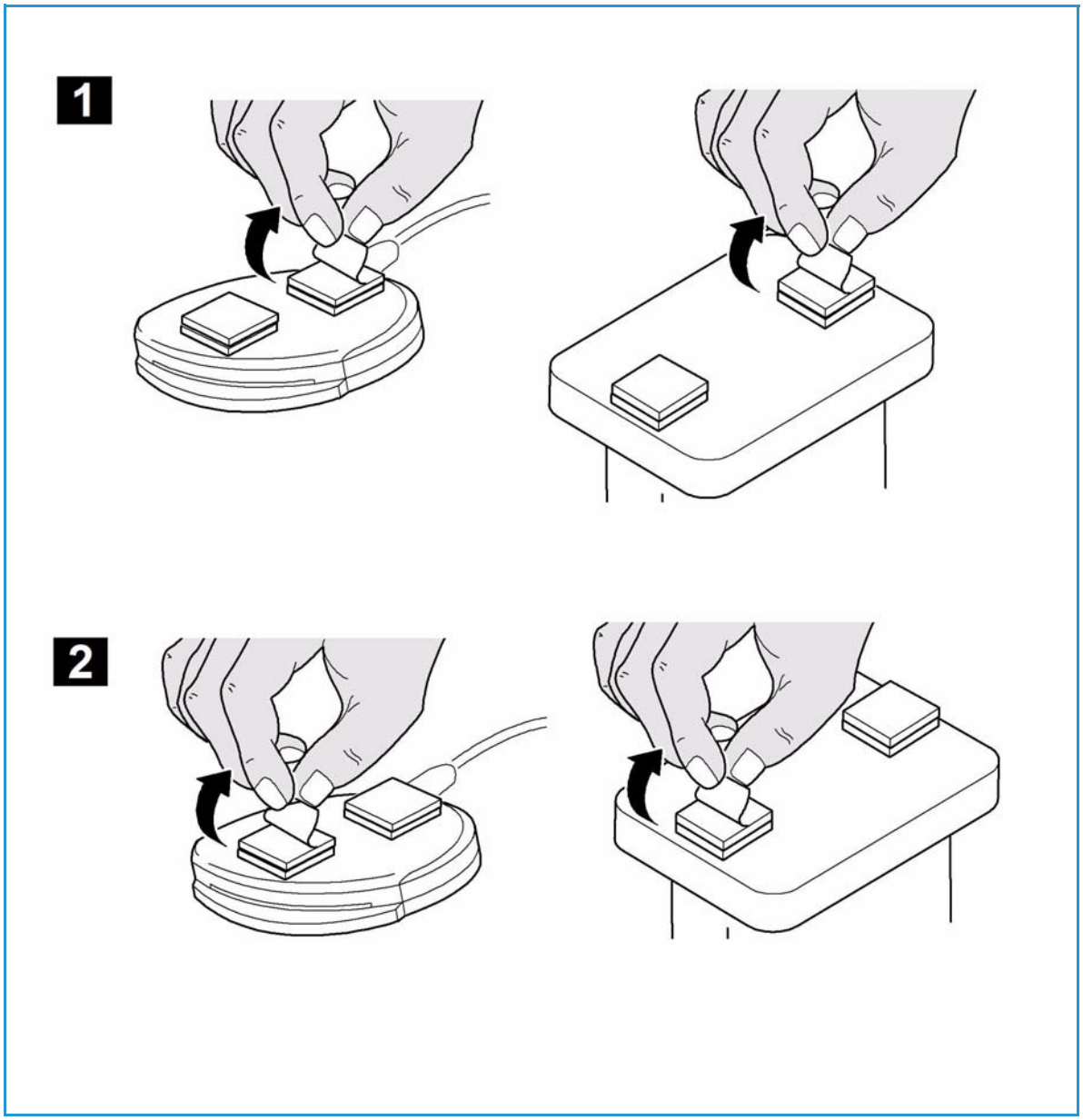


4. Attach the fasteners to the card reader device
   - Fasteners have been provided to secure the card reader to the Xerox device.
   - Peel back the fastener backing strip.
   - Position the fastener on the under-side of the card reader, as shown.
   - Repeat for each of the fasteners supplied.

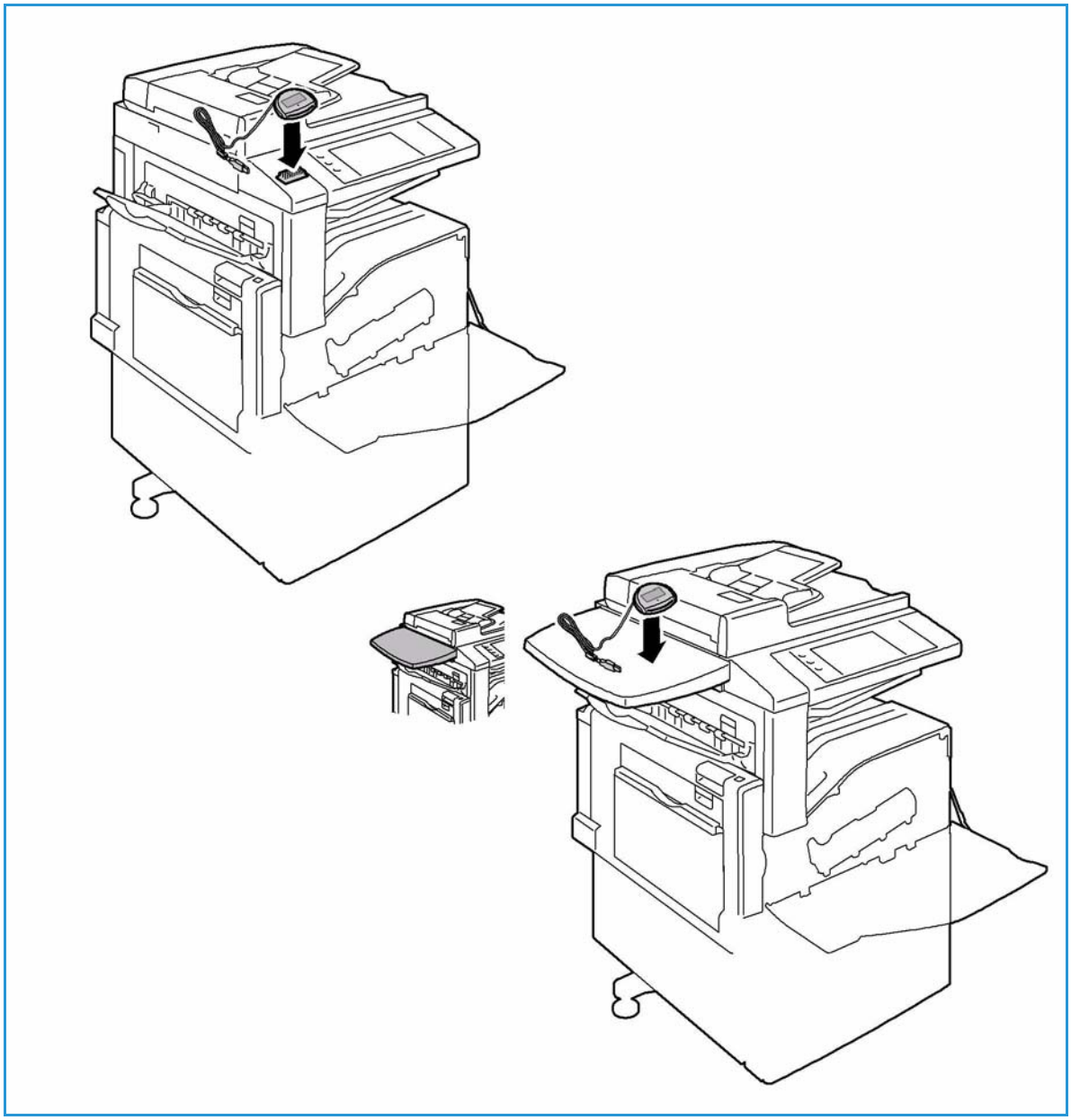


5. Remove the fastener backing strips

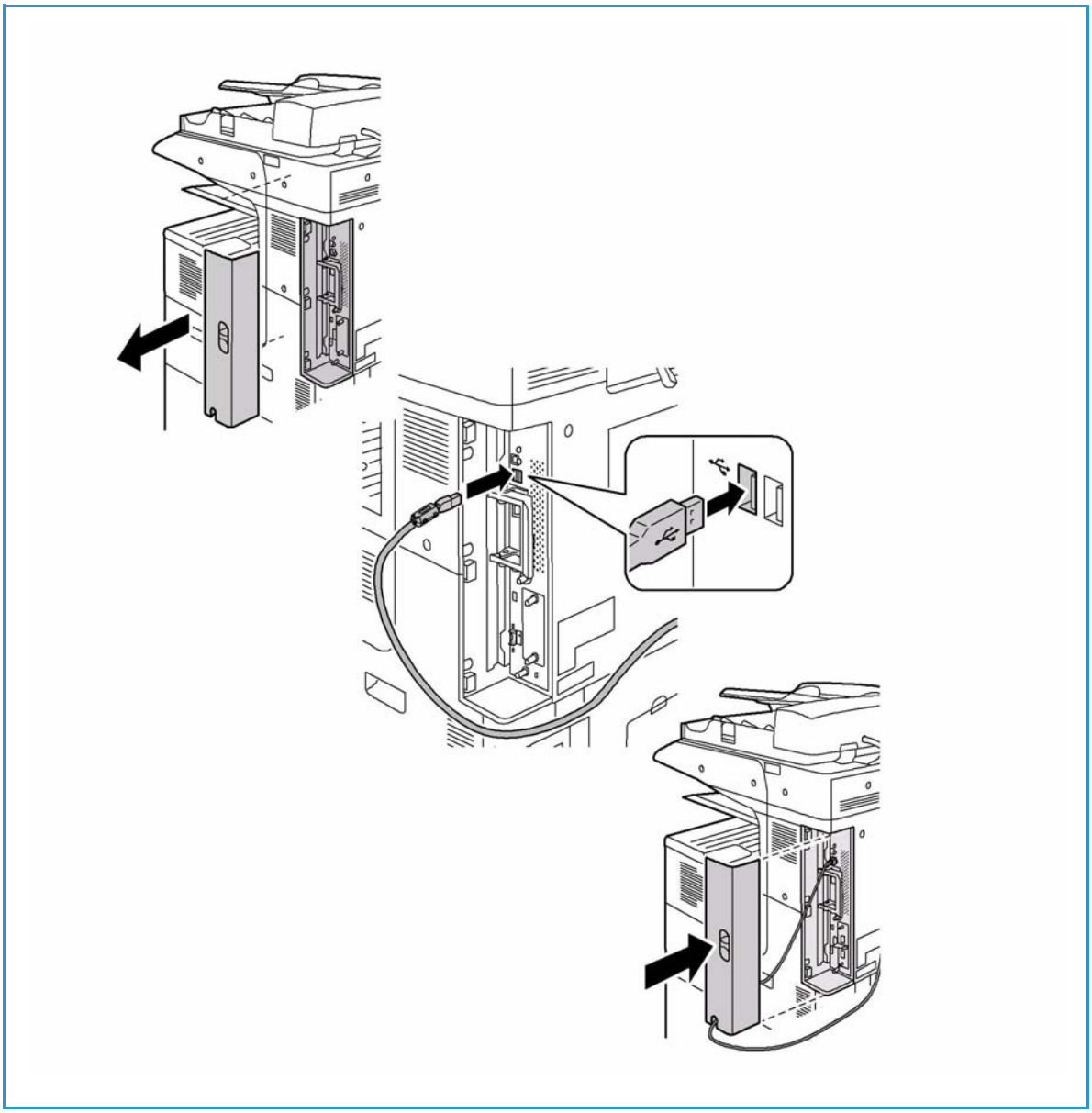
   When all the fasteners have been attached to the card reader, remove the backing strips on each of the fasteners.



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 the opening of the document handler side cover.
   - 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
   - Remove the Device Connector Cover.
   - Insert the USB connection into the slot provided on the rear of the network controller.
   - Replace the Device Connector Cover ensuring the USB cable passes through the slot at the base of the cover.
   - Use the cable ties provided to ensure the cabling is neat and tidy.



The hardware installation is now complete.

8. 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.
   - Select **OK**.

Smart Card is now ready for use.

Note: If the card reader is not detected, refer to Troubleshooting Tips on page 29 for information.

Using the 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 29.
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 22 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 29.

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 30.

During Installation

Problem	Possible Cause	Solution
Card reader is installed but no message displays on the User Interface	Card reader is faulty.	• Try a different card reader. • Contact the System Administrator.
	Card reader connection is faulty.	• Check the cable is plugged in correctly. Refer to Connect the card reader to the Xerox device on page 22 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.	• Check that the card reader is on the list of compatible devices, refer to Supported Card Types on page 7.
	Smart Card access is not enabled on the machine.	• Enable CAC through the *Properties* set up screens using Internet Services, refer to Software Enablement on page 12.

After Installation

Problem	Possible Cause	Solution
Authentication failures	Incorrect PIN has been entered.	• Retry entering the correct PIN. If problem persists, contact the System Administrator for advice.
	Card is locked due to too many failed PIN attempts.	• Contact Registration Authority to reload or to get a new card.
	Unable to find identity certificate.	
	Identity certificate has been revoked.	
	Authentication with Domain Controller Failed.	• Check network cable is firmly connected. • Contact the System Administrator.
	Unable to validate server certificate.	
	Smart Card Authentication System Failed.	
	Authentication Failed.	
	System Administrator has not selected All Features or Scanning Service Only.	• Contact the System Administrator.

Problem	Possible Cause	Solution
Time for date mismatch error	There is a mismatch between the time and date setting on the Xerox device and the authentication server time or date setting.	• Verify that Network Time Protocol is properly set up. • Verify that the date and time and GMT Offset (Time Zone) is correct, refer to Configure the Date & Time to update automatically on page 14 for instructions. • Verify that GMT offset is correct for Daylight Savings Time. • Contact your System Administrator.
Cannot see the Internet Services web page after software upgrade	IP Address incorrect or has been reset.	• 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**.

A

Retrieving the Certificate from a Domain Controller or OCSP Server

1. Access the Domain Controller using a web browser using the following syntax:

   https://IP Address of the Domain Controller:636

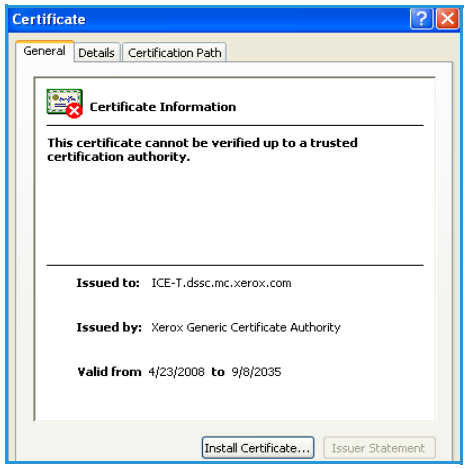
   For example: *https://111.222.33.44:636* where *111.222.33.44* is the IP address of the appropriate server.

   A *Security Alert* warning window is displayed, similar to the one shown.

2. Click on **View Certificate** to proceed.

   If the window does not display, double click on the padlock icon in the lower right hand corner of your browser window.

   The *Certification Information* window is displayed.

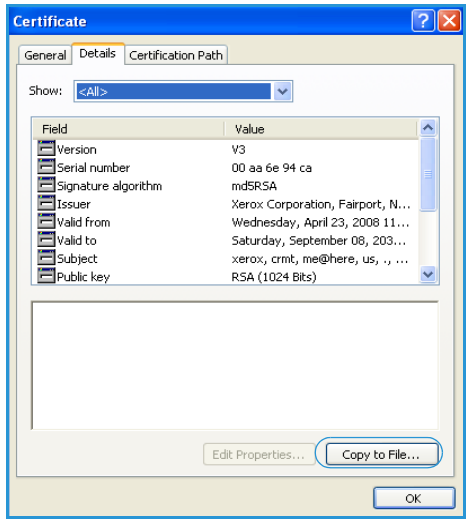


3. Select the **Details** tab.

   Record the name of the *Certificate Authority (CA)* that issued this certificate, the "Issuer".

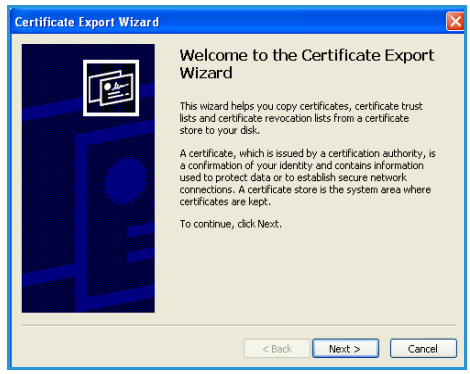
   A certificate from this CA will be required during *Smart Card* setup.

4. Select the **Copy to File** button.

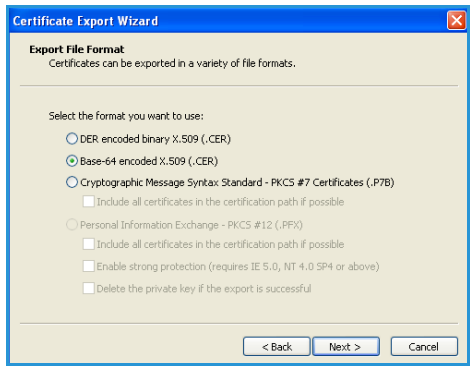


   The *Certification Export Wizard* is displayed.

5. Select **Next**.



6. Select **Base-64 encoded X.509 (.CER).**
7. Select **Next.**

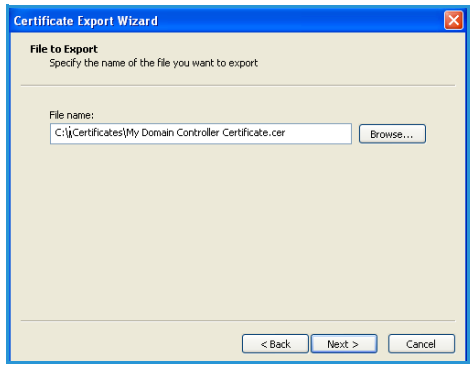


8. Select **Browse**.

   Browse to a directory to save the Certificate.

9. Enter a filename for the *Certificate* and select **Save**.

10. Select **Next**.



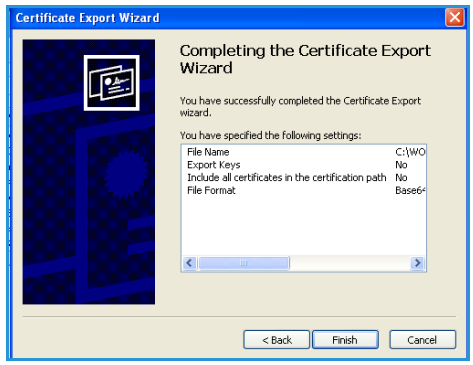
11. Select **Finish**.

    The *Certificate* is retrieved from the server and saved in the selected directory.

    A pop-up message will confirm that the *Certificate* has been successfully saved.

    Once saved the *Certificate* can be loaded onto the device.

This process can be repeated to retrieve the *Certificates* from each of the required servers.



B

Determining the Domain in which your Card is Registered

1. From your PC, click the **Start** menu and right click on **My Computer**.
2. From the drop down list, select **Properties**.
   When the *System Properties* window opens, click on the **Computer Name** tab.
   Beneath the *Full Computer* name is the *Domain Name*.
3. Copy and paste the *Domain Name* directly into the CAC setup page on the Internet Services user interface.
   Refer to Configuring Common Access Card on page 14 for instructions.
4. Select **Cancel** to close the *System Properties* window.