Version: 1.0
07/11

Xerox® Common Access Card Installation Guide

Xerox® WorkCentre 4250/4260

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

Document version 1.0: July 2011

Table of Contents

Introduction 1

The Common Access 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 Common Access 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 Common Access 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 4250	15.004.02.000
Xerox WorkCentre 4260	30.104.08.000

- 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 Readers

The customer is responsible for providing a card reader for each Xerox device. The following card readers are compatible with the solution:

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

Additional information from your System Administrator may be required to validate which card reader works best in your environment.

> Note: Information about CCID compliant card types 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 Common Access Card software.

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 Readers and Access Cards (refer to Card Readers and Card Types on page 7)	Customer
Common Access Card Enablement Kit 497K09950 (one required 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 certificates • Check that all certificates are in 64 bit X.509 format	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

The method to validate the Domain certificate requires installation of the certificate chain including the Root certificate on to the Xerox device. The Xerox WorkCentre may be configured to validate all certificates via OCSP (Online Certificate Status Protocol Responder). It submits the Domain Certificate and any associated Intermediary Certificates to the OCSP Responder, to verify that these certificates are valid and not revoked. The WorkCentre then receives a response from the OCSP responder stating whether these certificates are valid.

> Note: Certificates are often obtained from the Information Technology professionals that support your organization. The certificate chain consists of all Intermediate Certificates up to and including the Root Certificate. 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 *Common Access 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 *Common Access Card* solution.

There are 4 main installation procedures to follow in sequence.

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

Software Enablement

Prior to installing the *Common Access Card* solution, the software requires enabling on your Xerox device using CentreWare Internet Services. The Feature Enable Key and the instructions are provided in your Enablement Kit. Follow the instructions provided in the Xerox Common Access Card Enablement Guide to upgrade your device software and install the Feature Enable Key.

Once the *Common Access Card* software has been enabled, use the following instructions to configure Common Access Card on your device using CentreWare Internet Services.

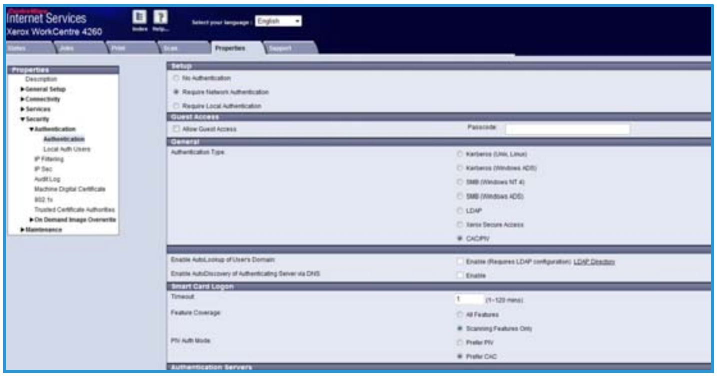
Configuring Common Access Card

Once the *Common Access Card* feature has been enabled on the device it can be configured using CentreWare Internet Services.

Follow the instructions below to configure *Common Access Card*:

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

1. Access CentreWare 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. Configure the *Common Access Card* software.



Setup
○ No Authentication
● Require Network Authentication
○ Require Local Authentication

Guest Access
□ Allow Guest Access   Passcode:

General
Authentication Type
○ Kerberos (Unix, Linux)
○ Kerberos (Windows ADS)
○ SMB (Windows NT 4)
○ SMB (Windows ADS)
○ LDAP
○ Xerox Secure Access
● CAC/PIV

Enable AutoLookup of User's Domain   □ Enable (Requires LDAP configuration) LDAP Directory
Enable AutoDiscovery of Authenticating Server via DNS   □ Enable

Smart Card Logon
Timeout   1 (1-120 mins)
Feature Coverage   ○ All Features   ● Scanning Features Only
PIV Auth Mode   ○ Prefer PIV   ● Prefer CAC

   a. Select the **Security** link.
   b. Select the **Authentication** link.
   c. Select **Authentication** in the Directory Tree.
   d. In the *Setup* section, select **Require Network Authentication**.
   e. In the *Authentication Type* option select **CAC/PIV** (Common Access Card/Personal Identity Verification).
   f. In the *Timeout* option enter the number of minutes the system waits before logging out the user.

g. In the *Feature Coverage* option, select if a CAC card is required for **Scanning Features Only** (network scanning, Server fax and email) or for **All Features** (copy, print, scan, email).

h. In the *PIV Auth Mode* option, select **Prefer PIV** or **Prefer CAC** depending on what type of cards are utilized in your environment.

i. Select **Apply**.

4. Configure the Authentication Servers.

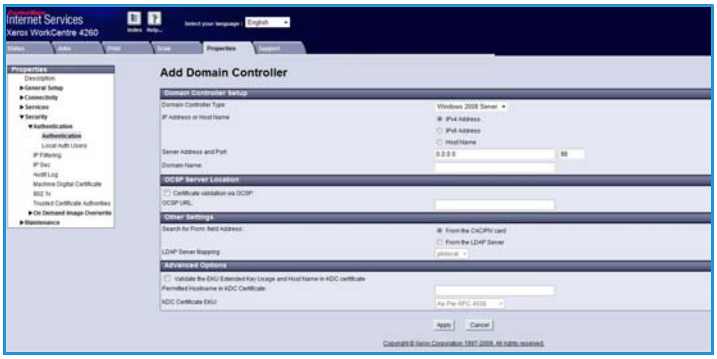
   Add your LDAP server for authentication purposes with your PIV/CAC card.

   a. Select **Add**.

   b. Select the type of server for authentication (for example Windows 2003, Windows 2008).

   c. Enter the *IP Address* or enter the *Domain Controller Host name* (this must be the fully qualified Host Name).

   d. Ensure *Port 88* is selected, unless your Kerberos Port is different.



Add Domain Controller

Domain Controller Setup

Domain Controller Type: Windows 2008 Server

IP Address or Host Name: ● IPv4 Address ○ IPv6 Address ○ Host Name

Server Address and Port: 0.0.0.0 88

Domain Name:

OCSP Server Location

□ Certificate validation via OCSP

OCSP URL:

Other Settings

Search for From: field Address: ● From the CAC/PIV card ○ From the LDAP Server

LDAP Server Mapping: ptdocal

Advanced Options

□ Validate the EKU Extended Key Usage and Host Name in KDC certificate

Permitted Hostname in KDC Certificate:

KDC Certificate EKU: As Per RFC 4556

   e. Enter the *Domain Name* (this must also be the fully qualified Domain Name).

   f. Set the *OCSP Server Location*. If you wish to validate the DC against an OCSP server, select the **Certificate validation via OCSP** checkbox and enter the *OCSP Server Service URL* details.

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

   g. In the *Other Settings*, select to search **From the CAC/PIV Card** or **From the LDAP Server** (already configured on the printer) for the *From* field population when sending email at the device. The field will be populated with the email address and username contained in the email signing certification on the CAC card or from your LDAP server settings in the *Connectivity > Protocols > LDAP server* section. Select the checkbox to enable. After enabling from the LDAP server, select which LDAP servers you would like to use depending on how many you have setup in your LDAP directory listing.

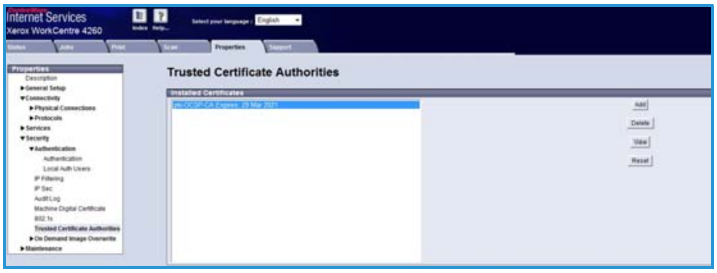
   h. If required, in the *Advanced Options* select to **Validate the EKU Extended Key Usage and Host Name in KDC certificate**. This will validate the encryption key in your certificate on the CAC card with the hostname.

   i. Select **Apply**. This will save all of the current settings and return to the *Authentication* screen in CentreWare Internet Services.

5. If required, enable a *Logoff Reminder*. After each scan job a prompt is provided to remind the user to logoff the printer.

6. Select **Apply**. You may be requested to enter your administrator User ID and Password. The default is **admin** and **1111**.

7. Load the DC root and intermediate certificates and the OCSP root and intermediate certificates.
    a. Select **Security** then **Trusted Certificate Authorities** page.
    b. At the *Trusted Certificates Authorities* screen, select **Add**.

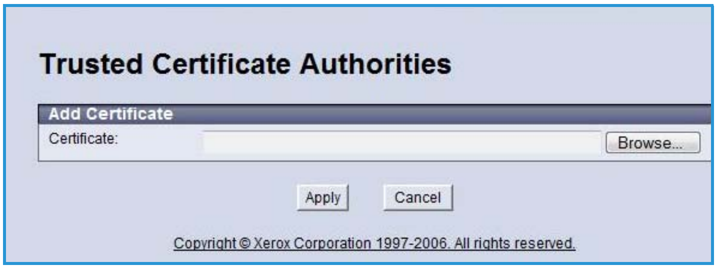


Trusted Certificate Authorities

Installed Certificates

[illegible]-OCSP-CA Expires: 29 Mar 2021

    c. Browse to the Root certificate of your server and add your certificates one at a time.
    d. An *Updated Successfully* screen is displayed if your certificates are valid and have been updated to the printer successfully.
    e. Select **OK**.



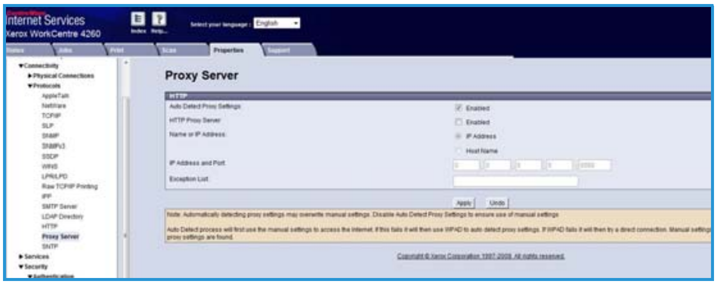
Trusted Certificate Authorities

Add Certificate

Certificate:

Copyright © Xerox Corporation 1997-2006. All rights reserved.

8. Check the Proxy Server details are configured.
    a. Select the **Properties** tab, then **Connectivity, Protocols** and **Proxy Server** and enter the details for your proxy server if required.
    b. Select **Apply**.



Proxy Server

HTTP

Auto Detect Proxy Settings ☑ Enabled

HTTP Proxy Server □ Enabled

Name or IP Address ● IP Address ○ Host Name

IP Address and Port

Exception List

Note: Automatically detecting proxy settings may overwrite manual settings. Disable Auto Detect Proxy Settings to ensure use of manual settings

Auto Detect process will first use the manual settings to access the internet. If this fails it will then use WPAD to auto detect proxy settings. If WPAD fails it will then try a direct connection. Manual setting proxy settings are found.

Copyright © Xerox Corporation 1997-2008. All rights reserved.

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

Hardware Installation

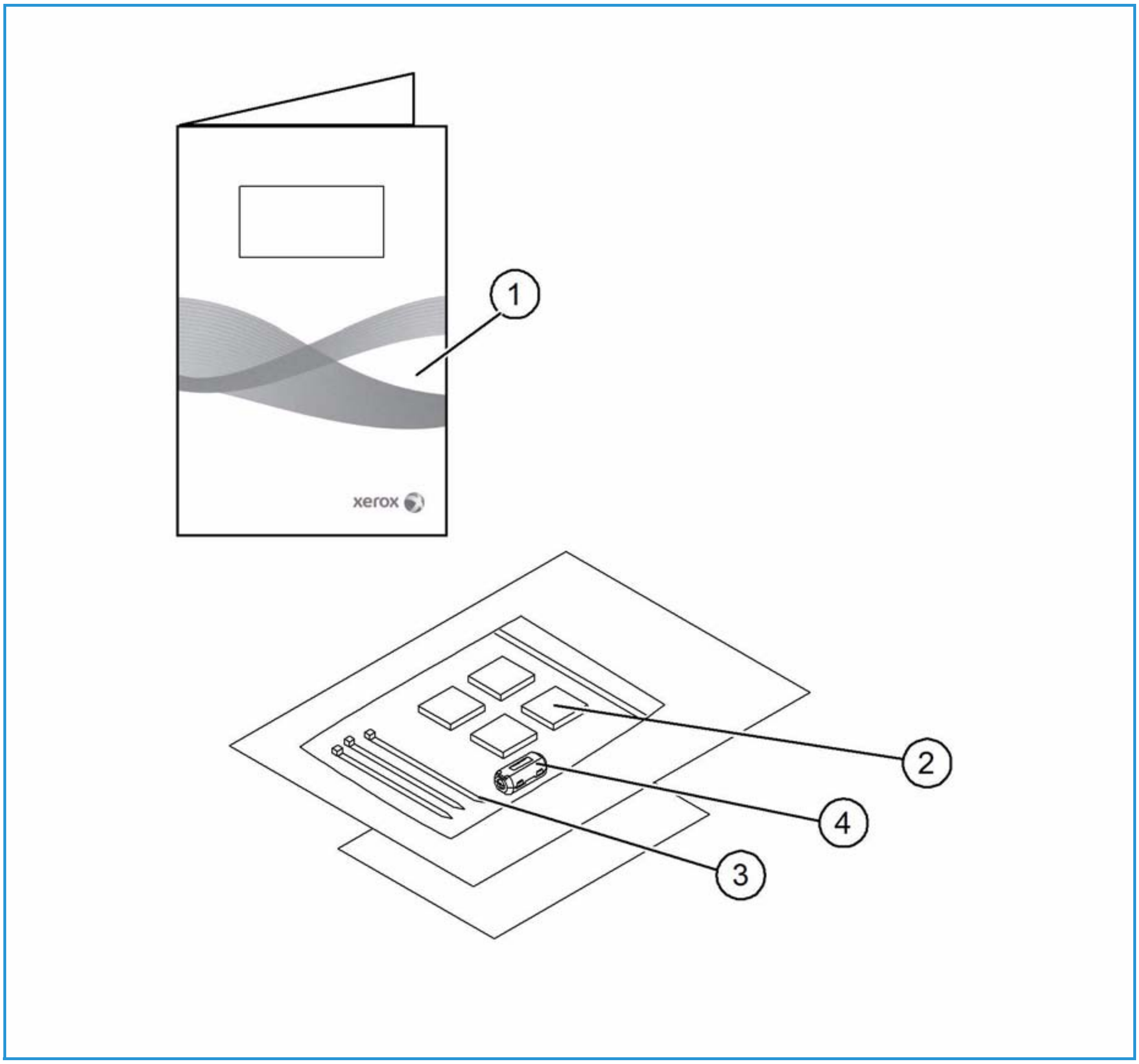
Install the card reader device using the following instructions.

1. Unpack the Common Access Card Enablement Kit

   The kit contains the following items:

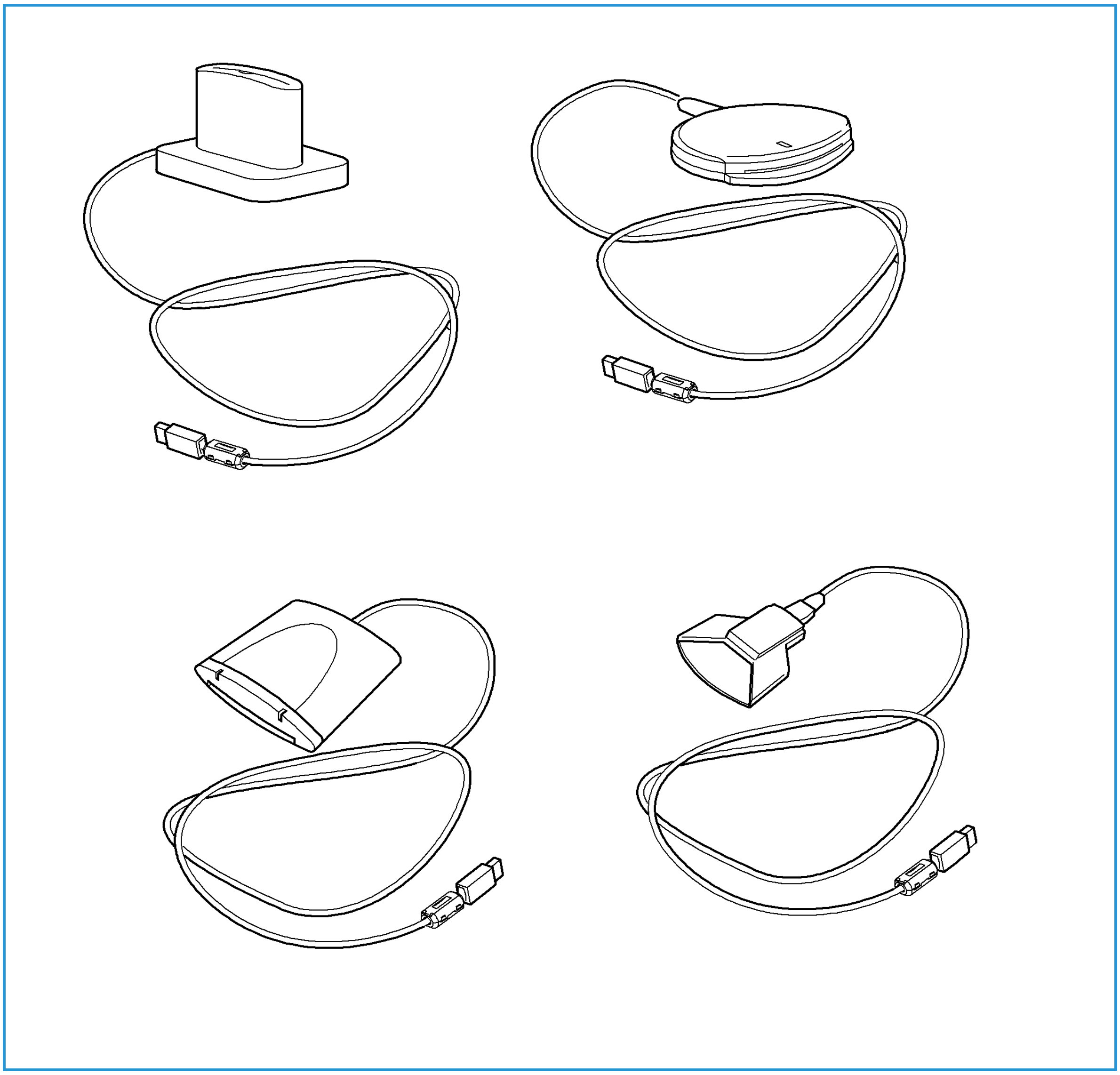
   - Xerox Common Access Card Enablement Guide (1)
   - Four Dual Lock Fastener pads (Velcro) (2)
   - Three Cable Ties (3)
   - One Ferrite Bead (4)

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



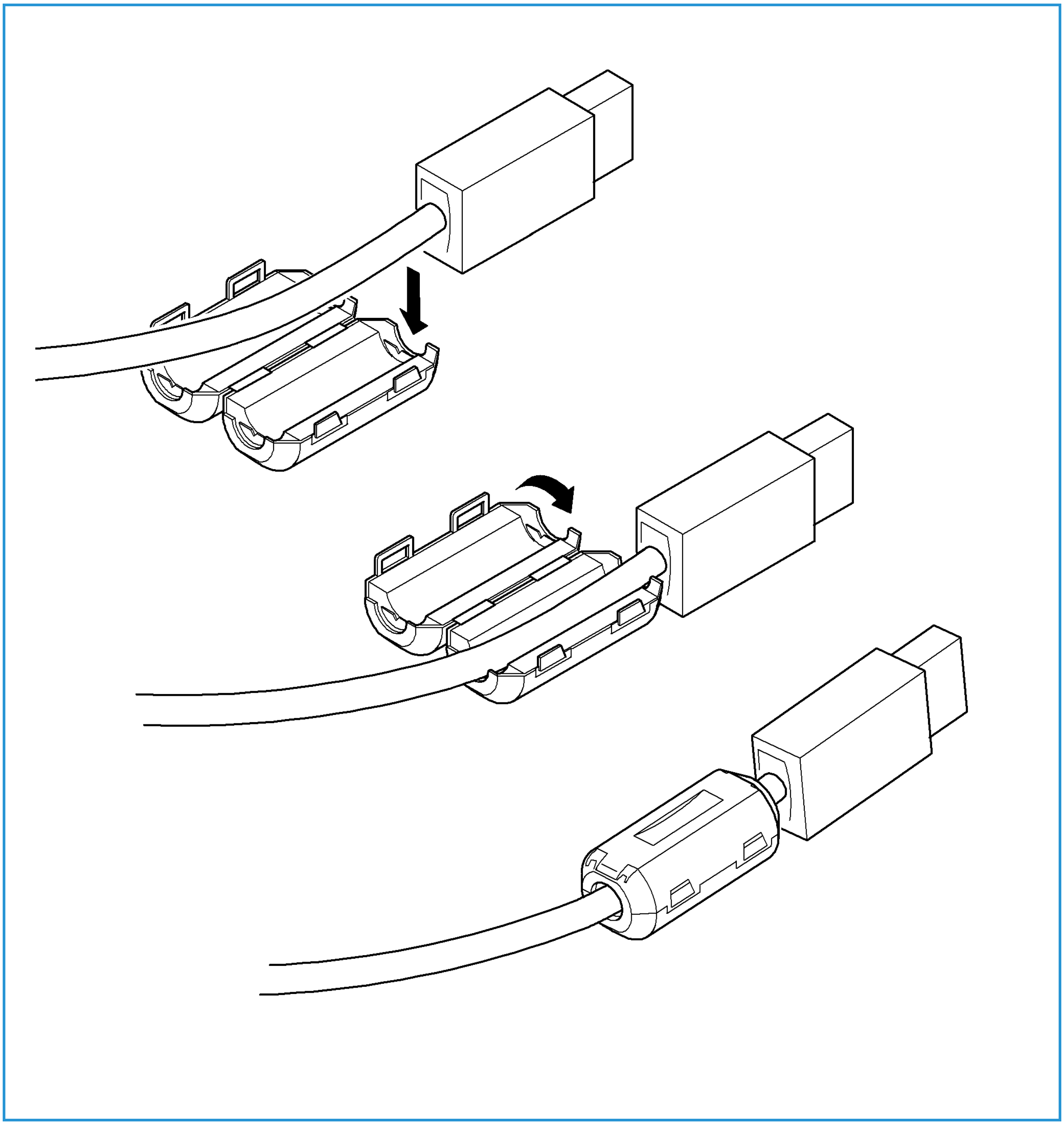
2. Locate the card reader device being installed
    - There are four types of card reader available, one upright model or three slimline models.
    - Locate the device being installed and ensure it has been configured.

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

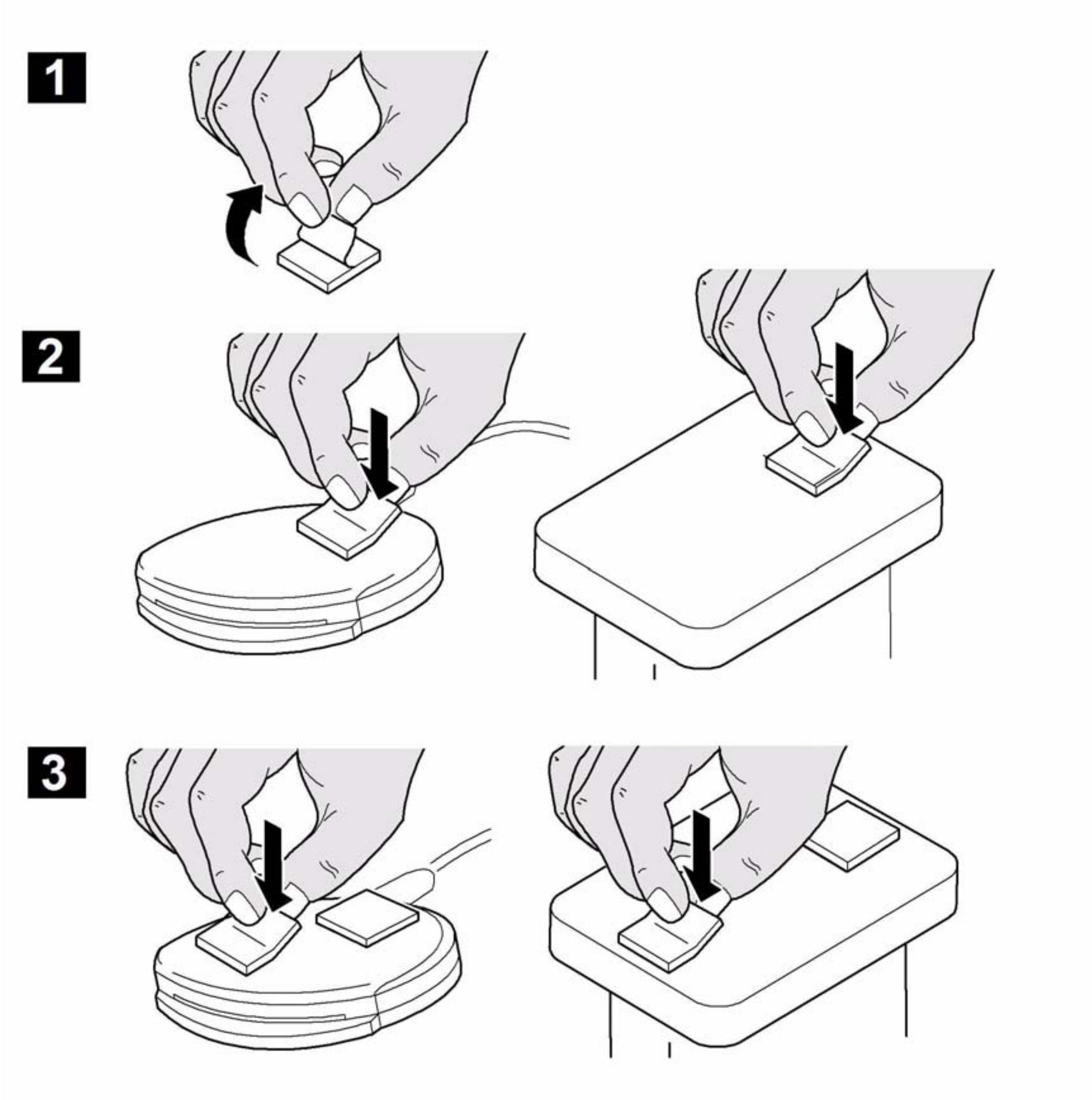


3. Attach the ferrite bead to the reader cable.

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

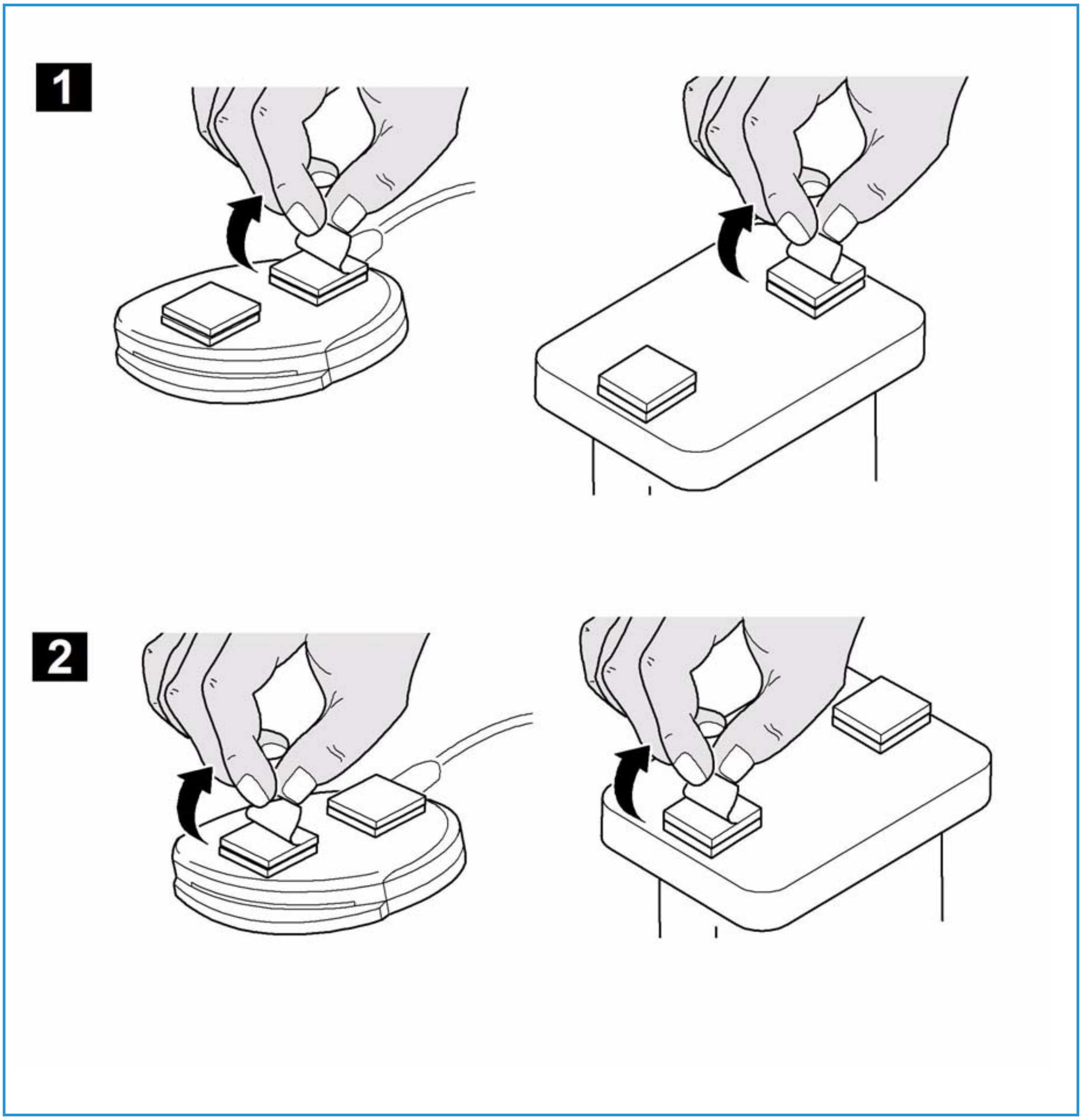


4. Attach the fasteners to the card reader device
   - Fasteners have been provided to secure the card reader to the Xerox device.
   - Peel back the fastener backing strip.
   - Position the fastener on the under-side of the card reader, as shown.
   - Repeat for each of the fasteners supplied.



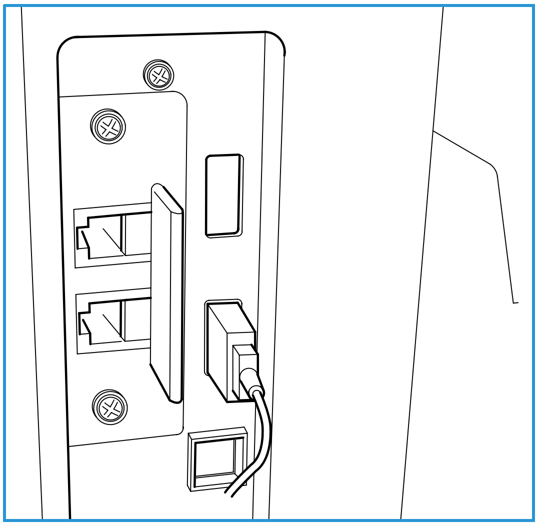
5. Remove the fastener backing strips

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

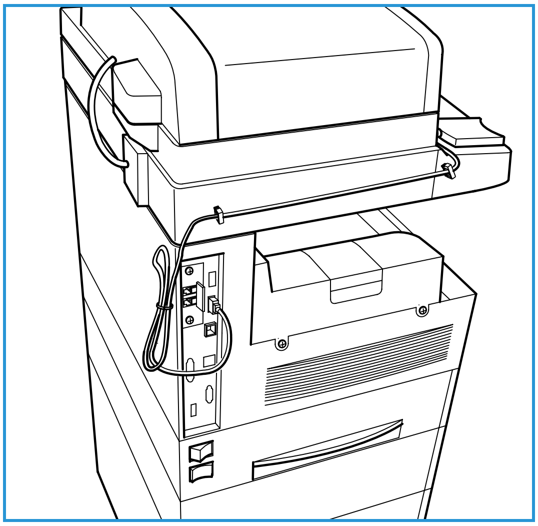


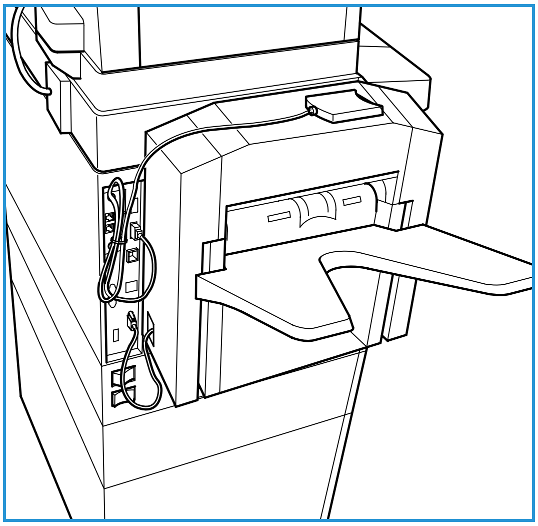
6. Place the card reader on the Xerox device
   - Gently place the card reader on the device (do not fix in place at this point).
   - Position the card reader in a suitable location, ensure it does not obstruct the opening of the document handler side cover.
   - Check the cable has sufficient length 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
   - Insert the USB connection into the slot provided on the rear of the network controller.



8. Use the cable ties provided to ensure the cabling is neat and tidy. The hardware installation is now complete.





9. 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**.

Common Access Card is now ready for use.

Note: If the card reader is not detected, refer to Troubleshooting Tips on page 25 for information.

Using Common Access Card

Once the *Common Access 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 *Common Access 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 25.

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.

4 Troubleshooting

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 20 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 25.

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 Common Access Card solution but are now experiencing problems, refer to After Installation on page 26.

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 20 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 Readers on page 7.
	Common Access Card access is not enabled on the machine.	• Enable CAC through the *Properties* set up screens using CentreWare 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.	
	Common Access Card Authentication System Failed.	
	Authentication Failed.	
	System Administrator has not selected All Features or Scanning Service Only.	• Contact the System Administrator.
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, • Verify that GMT offset is correct for Daylight Savings Time. • Contact your System Administrator.
Cannot see the CentreWare 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:

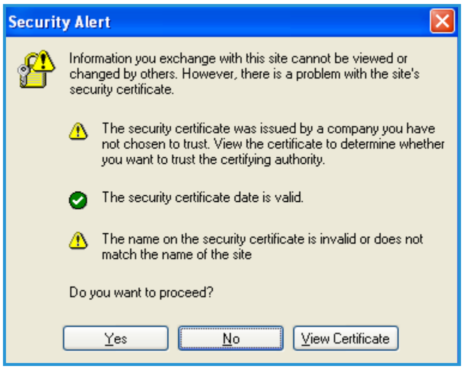
   https://IP Address of the Domain Controller:636

   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.



Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.

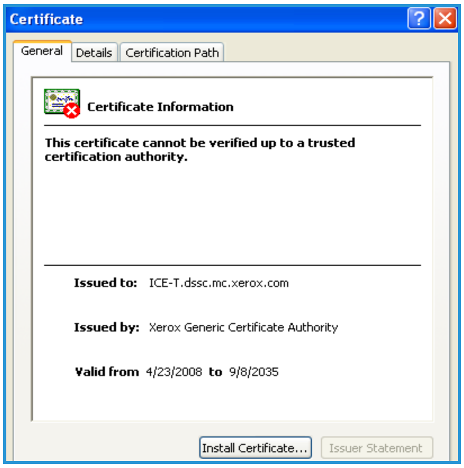
The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.

The security certificate date is valid.

The name on the security certificate is invalid or does not match the name of the site

Do you want to proceed?

The *Certification Information* window is displayed.



Certificate Information

This certificate cannot be verified up to a trusted certification authority.

Issued to: ICE-T.dssc.mc.xerox.com

Issued by: Xerox Generic Certificate Authority

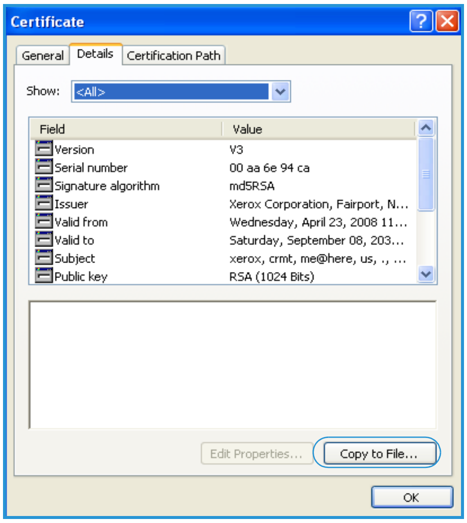
Valid from 4/23/2008 to 9/8/2035

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 *Common Access Card* setup.

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

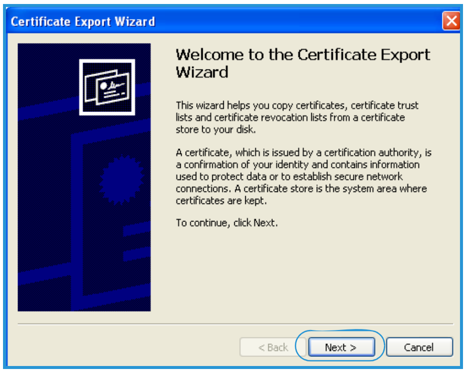


Show: <All>

Field	Value
Version	V3
Serial number	00 aa 6e 94 ca
Signature algorithm	md5RSA
Issuer	Xerox Corporation, Fairport, N...
Valid from	Wednesday, April 23, 2008 11...
Valid to	Saturday, September 08, 203...
Subject	xerox, crmt, me@here, us, ., ...
Public key	RSA (1024 Bits)

The *Certification Export Wizard* is displayed.

5. Select **Next**.



Welcome to the Certificate Export Wizard

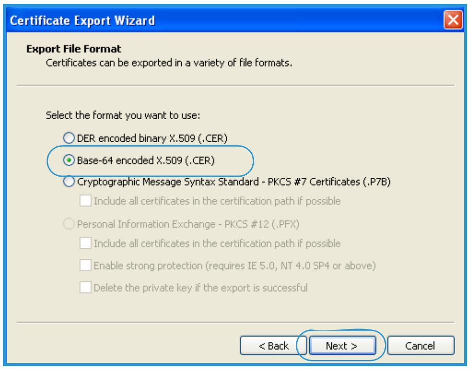
This wizard helps you copy certificates, certificate trust lists and certificate revocation lists from a certificate store to your disk.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

To continue, click Next.

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

7. Select **Next**.



Export File Format

Certificates can be exported in a variety of file formats.

Select the format you want to use:

○ DER encoded binary X.509 (.CER)

● Base-64 encoded X.509 (.CER)

○ Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)

□ Include all certificates in the certification path if possible

○ Personal Information Exchange - PKCS #12 (.PFX)

□ Include all certificates in the certification path if possible

□ Enable strong protection (requires IE 5.0, NT 4.0 SP4 or above)

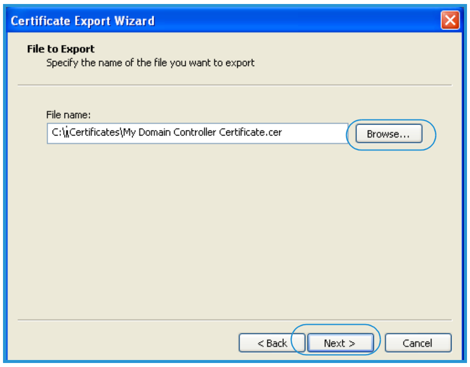
□ Delete the private key if the export is successful

8. Select **Browse**.

   Browse to a directory to save the Certificate.

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

10. Select **Next**.



Certificate Export Wizard

File to Export

Specify the name of the file you want to export

File name:

C:\Certificates\My Domain Controller Certificate.cer

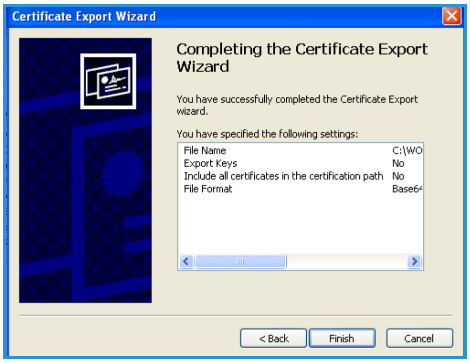
11. Select **Finish**.

    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.



Certificate Export Wizard

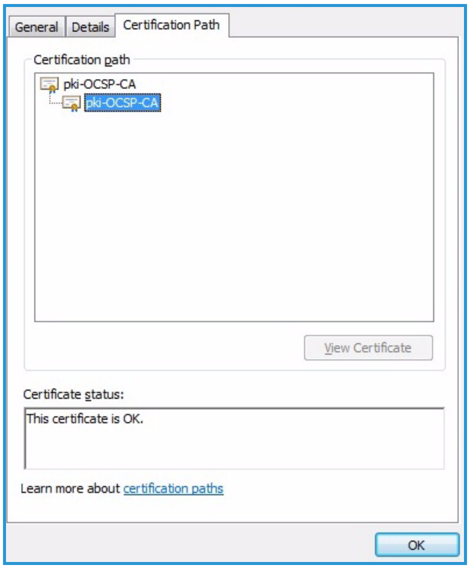
Completing the Certificate Export Wizard

You have successfully completed the Certificate Export wizard.

You have specified the following settings:

File Name	C:\WO
Export Keys	No
Include all certificates in the certification path	No
File Format	Base64

Note: Depending on your server, you may need to install a Root Certificate or one or more intermediate certificates. This can be determined by viewing the Certification path tab on your Domain certificate and installing all certificates listed on to your Xerox WorkCentre.



Certification path

pki-OCSP-CA

pki-OCSP-CA

Certificate status:

This certificate is OK.

Learn more about certification paths

Determining the Domain in which your Card is Registered

B

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 CentreWare Internet Services user interface.

   Refer to Configuring Common Access Card on page 12 for instructions.
4. Select **Cancel** to close the *System Properties* window.