



Xerox Secure Access Unified ID System® Installation Guide

Copyright © 2007-2010 by Xerox Corporation. All rights reserved. XEROX[®], Secure Access Unified ID System, SMARTsend, and FreeFlow are trademarks of or licensed to Xerox Corporation in the United States and other countries.

Contents

1 Safety Notes

| | |
|--|----|
| Electrical Supply | 5 |
| WARNING - Electrical Safety Information..... | 6 |
| Disconnect Device | 6 |
| Regulatory Information | 7 |
| Radio Frequency Emissions..... | 7 |
| Product Recycling and Disposal | 9 |
| European Union | 9 |
| North America (USA, Canada)..... | 9 |
| Other Countries | 10 |
| EH&S Contact Information..... | 10 |

2 Installation Checklist

3 Installation Overview

| | |
|--|----|
| Secure Access Components | 14 |
| Core Authentication Server (CAS)..... | 15 |
| Device Control Engine (DCE) | 15 |
| Document Routing Engine (DRE) | 15 |
| Multi-Server Deployment..... | 16 |
| Secure Access Server System Requirements | 18 |
| User Authentication Settings under Windows XP Pro..... | 18 |
| Secure Access Hardware Component Requirements | 20 |
| Supported Card Readers | 20 |

4 Installing the Secure Access Server

| | |
|---|----|
| Preparing the Network and Database..... | 22 |
| Run the Installation Wizard | 23 |
| Upgrading Secure Access | 25 |

5 Setting Up the Secure Access Hardware

| | |
|---|----|
| Configure the Authentication Device IP Address..... | 28 |
| Configure the DHCP Server to Locate the Authentication Devices..... | 28 |
| Manually Assign the IP Address | 29 |
| Mount the Secure Access Authentication Device..... | 31 |
| Connect the Hardware..... | 32 |
| Mount/Connect the Secure Access USB Card Reader..... | 33 |

6 Configuration Tear Sheet

Contents


Safety Notes

1

Read these safety notes carefully to ensure you operate the equipment safely and in compliance with applicable legislation.

The equipment has been designed and tested to meet strict safety requirements. These include safety agency approval, and compliance to established environmental standards.

Please read the following instructions carefully before operating the equipment and refer to them as needed to ensure continued safe operation.

 **WARNING:** Any unauthorized alteration, which may include the addition of new functions or connection of external devices, may impact the product certification. Please contact your authorized local dealer for more information

Electrical Supply

The power supply provided with the equipment must be operated from the type of electrical supply indicated on the data plate label. If you are not sure that your electrical supply meets the requirements, please consult your local power company for advice.

WARNING - Electrical Safety Information

- Use only the power supply supplied with this equipment.
- Do not place this equipment where people might step on or trip on the power cord or its associated power supply.
- Do not place objects on the power supply power cord.
- If any of the following conditions occur, switch off the power to the equipment immediately and disconnect the power cord from the electrical outlet. Call an authorized local service representative to correct the problem.
 - The equipment emits unusual odors.
 - The power cord is damaged or frayed.
 - A wall panel circuit breaker, fuse, or other safety device has been tripped.
 - The equipment is exposed to water.
 - Any part of the equipment is damaged.

Disconnect Device

The power cable to the power supply is the disconnect device for this equipment. To remove all electrical power from the equipment, disconnect the power cable from the electrical outlet.

Regulatory Information

Radio Frequency Emissions

United States, Canada

Note: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Re-orient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Shielded interface cables must be used with this equipment to maintain compliance with FCC regulations in the United States

Canada

This Class "B" digital apparatus complies with Canadian ICES-003.

Cet appareil Numérique de la classe "B" est conforme à la norme NMB-003 du Canada.

Europe



The CE mark applied to this product symbolizes XEROX's declaration of conformity with the following applicable Directives of the European Union, as of the dates indicated:

- December 12, 2006:** Council Directive 2006/95/EC as amended. Approximation of the laws of the member states related to low voltage equipment.
- December 15, 2004:** Council Directive 2004/108/EC as amended. Approximation of the laws of the member states related to electromagnetic compatibility.
- March 9, 1999:** Council Directive 99/5/EC, on radio equipment and telecommunications terminal equipment and the mutual recognition of the conformity.

A full declaration of conformity, defining the relevant directives and referenced standards, can be obtained from your XEROX Limited representative.

WARNINGS:

- In order to allow this equipment to operate in proximity to Industrial Scientific and Medical (ISM) equipment, the external radiation from the ISM equipment may have to be limited or special mitigation measures taken.
- Shielded interface cables must be used with this product to maintain compliance with Council Directive 89/336/EEC.

"Regulatory information for RFID"

Readers provide with this product generates 13.56 MHz using an Inductive Loop System as a Radio Frequency Identification device (RFID). This RFID device complies with the requirements specified in FCC Part 15, Industry Canada RSS-210, European Council Directive 99/5/EC, and all applicable local laws and regulations.

Operation of this device is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Changes or modifications to this equipment not specifically approved by the Xerox Corporation may void the user's authority to operate this equipment.

Product Recycling and Disposal

If you are managing the disposal of your equipment, please note that the product contains lead, mercury and other materials whose disposal may be regulated due to environmental considerations in certain countries or states. The presence of lead and mercury is fully consistent with global regulations applicable at the time that the product was placed on the market.

European Union

Disposal Information for Commercial Users



Application of this symbol on your equipment is confirmation that you must dispose of this equipment in compliance with agreed national Procedures.

In accordance with European legislation end of life electrical and electronic equipment subject to disposal must be managed within agreed procedures.

Prior to disposal please contact your local dealer or Xerox representative for end of life take back information.

North America (USA, Canada)

Xerox operates a worldwide equipment take back and reuse/recycle program. Contact your Xerox sales representative (1-800-ASK-XEROX) to determine whether this Xerox product is part of the program. For more information about Xerox environmental programs, visit <http://www.xerox.com/environment>

If you are managing the disposal of your Xerox product, please note that the product may contain lead, mercury, Perchlorate, and other materials whose disposal may be regulated due to environmental considerations. The presence of these materials is fully consistent with global regulations applicable at the time that the product was placed on the market. For recycling and disposal information, contact your local authorities. In the United States, you may also refer to the Electronic Industries Alliance web site: <http://www.eiae.org>

Perchlorate Material – This product may contain one or more Perchlorate-containing devices, such as batteries. Special handling may apply; please see <http://www.dtsc.ca.gov/hazardouswaste/perchlorate>

Disposal Information for Domestic Users



Application of this symbol on your equipment is confirmation that you should not dispose of the equipment in the normal household waste stream.

In accordance with European legislation, end of life electrical and electronic equipment subject to disposal must be segregated from household waste.

Private households within EU Member States may return used electrical and electronic equipment to designated collection facilities free of charge. Please contact your local disposal authority for information.

In some Member States when you purchase new equipment your local retailer may be required to take back your old equipment free of charge. Please ask your retailer for information.

Other Countries

Please contact your local waste authorities and request disposal guidance.

EH&S Contact Information

Contact Information

For more information on Environment, Health, and Safety in relation to this Xerox product and supplies, please contact the following customer help lines:

USA: 1-800 828-6571

Canada: 1-800 828-6571

Europe: +44 1707 353 434

www.xerox.com/environment safety information US (Product Safety Information for US)

www.xerox.environment_europe safety information EU (Product Safety information for EU)

Installation Checklist

2

The Xerox Secure Access Installation and Administration Guides include step-by-step instructions for installing and configuring the Secure Access server and MFPs. This chapter provides a table outlining the order in which the installation should occur based on the type of Secure Access hardware configuration starting with the Installation Guide.

| Steps (* indicates Required step) | Xerox Secure Access with USB Card Reader | Xerox Secure Access with Authentication Device and Card Reader |
|---|--|--|
| Installation Guide | | |
| 1. Read Chapter 3 Installation Overview | * | * |
| 2. Chapter 4 Installing the Secure Access Server: Preparing the Network and Database | * | * |
| 3. Chapter 4 Installing the Secure Access Server: Run the Installation Wizard | * | * |
| 4. Chapter 5 Setting Up the Hardware: Step 1. Configure the Authentication Device IP Address | Skip | * |
| 5. Chapter 5 Setting Up the Hardware: Step 2. Mount the Secure Access Authentication Device | Skip | * |
| 6. Chapter 5 Setting Up the Hardware: Step 3. Connect the Hardware | Skip | * |
| 7. Chapter 5 Setting Up the Hardware: Step 4. Mount/Connect the Secure Access USB Card Reader | * | Skip |
| Administration Guide | | |
| 8. Read Chapter 3 Secure Access Overview | * | * |
| 9. Chapter 4 Configuration Workflow Step 1. Configure Xerox MFP device to accept network authentication through the Xerox Secure Access mechanism | * | * |
| 10. Chapter 4 - Add MFP devices to the Secure Access Database | * | * |
| 11. Chapter 4 - Associate the MFP with a Secure Access Authentication Device | Skip | * |
| 12. Chapter 4 - Configure Follow-You Printing (optional) | * | * |
| 13. Chapter 4 - Set authentication parameters | * | * |
| 14. Chapter 4 - Import and synchronize user accounts | * | * |
| 15. Chapter 4 - Configure the Release My Documents Custom Service | * | * |

Installation Overview

3

This chapter includes:

- [Secure Access Components](#) on page 14
- [Secure Access Server System Requirements](#) on page 18
- [Secure Access Hardware Component Requirements](#) on page 20

This guide provides instructions to help you install the Xerox Secure Access Unified ID System™ Server software, and perform the physical setup of the Authentication Devices. You must install the Server before you setup the Authentication Devices.

After the Secure Access Server software is installed correctly, refer to the Secure Access Administration Guide for complete instructions for physical device deployment and software configuration.

This chapter provides information about:

- components that comprise the Secure Access Server
- system requirements

Secure Access Components

The Xerox Secure Access Unified ID System (herein called "Secure Access") is a hardware and software solution consisting of:

- The Secure Access Server software that manages the user database and contains services that communicate with the MFPs (Multi-function Printers) and the Secure Access Authentication Devices.
- A Secure Access Authentication Device, that includes a Card Reader and controls access to Xerox MFPs.
OR
- A Secure Access USB Card Reader

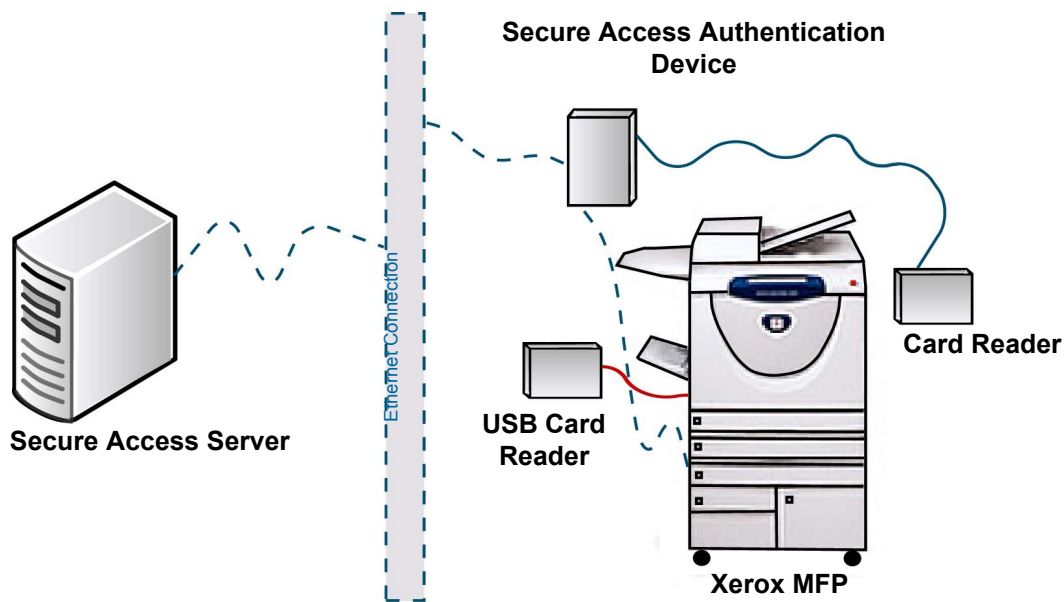


Figure 3-1: Secure Access Components

Each Secure Access Server software installation requires at least three services:

- Core Authentication Server (CAS)
- Device Control Engine (DCE)
- Document Routing Engine (DRE)

In addition, you must also install the Secure Access Manager, an administrative tool used to establish communication between the various Secure Access components.

Core Authentication Server (CAS)

The Core Authentication Server (CAS) houses the database that contains all user and MFP device data.

Every Secure Access installation requires a pre-installed database. The CAS uses the database instance to create an accounts database that contains all user and device information. See [Secure Access Server System Requirements](#) on page 18 for information about supported databases.

Device Control Engine (DCE)

The Device Control Engine (DCE) handles all communication with the MFP devices. When a user wants to use the copy, scan, or fax functionality on a MFP, they must first trigger the card reader. A swipe or proximity read initiates an access request.

The Authentication Device forwards the login request to the DCE, which then contacts the CAS to verify the user account data associated with the card.

Document Routing Engine (DRE)

The Document Routing Engine (DRE) is the print server. It's primary function is to enable document flow from user workstations to MFP devices. The following describes a typical DRE workflow:

1. A user generates a print request to an MFP that is registered in the Secure Access Manager database.
2. If the user prints to a print queue that is using a Secure Access Manager port the DRE holds the job on the print server.
3. When the user logs in at the MFP the DRE searches the jobs queued for that printer (and/or pull group) and releases those that were submitted by the logged in user.

If a Secure Access port is not installed on the device, the print job is printed without validation.

If you want print jobs to be held in a secure queue, you can configure Follow-You printing. To enable this functionality, you must configure the MFP to use a Secure Access port rather than a standard port. The Port Monitor integrates with the Windows printing subsystem and functions as part of the spooler service, allowing the Port Monitor to receive print jobs and then hold the jobs in a secure virtual queue until a verified user releases them to a particular MFP.

In addition, you can add the Release My Documents custom service to the MFP. This service allows users to access the secure print queue directly from the MFP front panel. See the [Xerox Secure Access Administration Guide](#) for configuration instructions.

Multi-Server Deployment

An installation where all services are installed on the same server is referred to as a "local" install. However, some installations may require more than one server to distribute the management load. Installations where services are distributed over two or more servers is referred to as a "remote" install.

Whether you deploy a single or multiple server installation, the DRE and DCE services must always be on the same server.

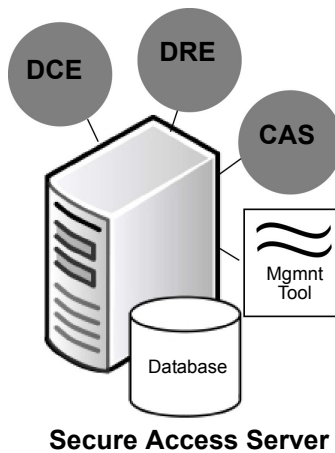


Figure 3-2: Local Installation Scenario

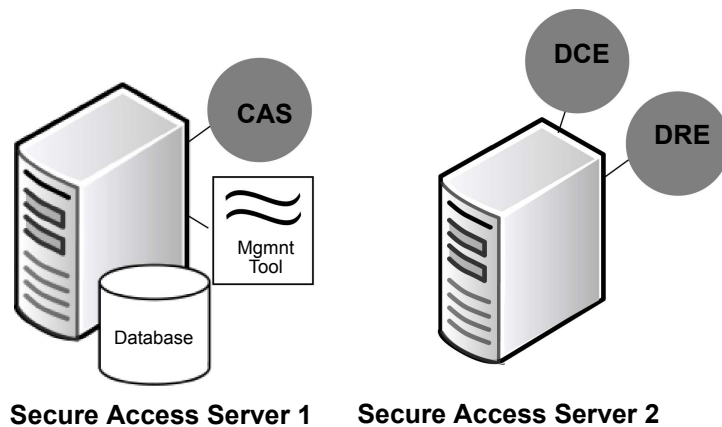


Figure 3-3: Remote Installation Scenario

In addition, if Secure Access will manage a large number of MFPs, you can deploy multiple DRE Print Servers to balance the communication load.

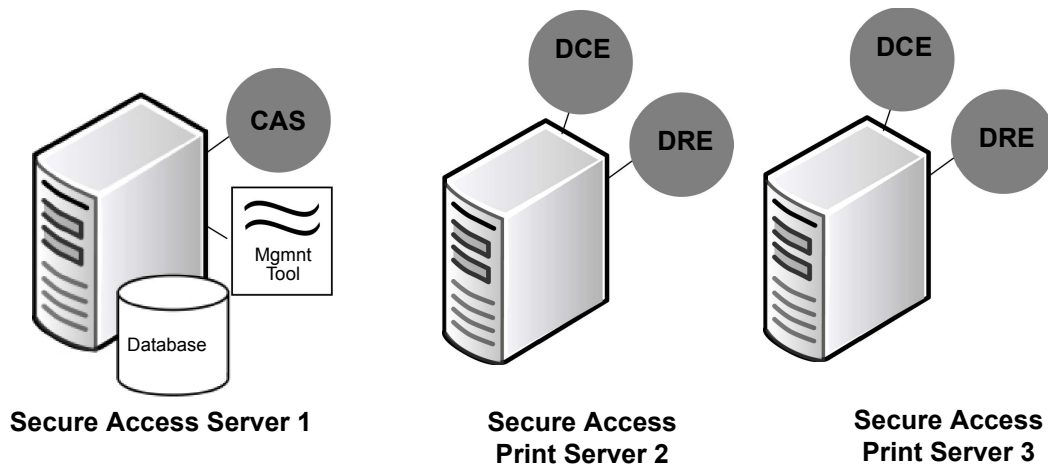


Figure 3-4: Multiple Print Server Deployment

See [Run the Installation Wizard](#) on page 23 for details on installing and setting up a multi-server deployment. The Install wizard allows you to select only the components that you want to install on each server. The DRE and DCE services can be installed on multiple server, and they must always be installed on the same server.

Secure Access Server System Requirements

Before you install Secure Access ensure that the server machines you plan to use meet the minimum operating requirements outlined below.

The table below lists minimum operating requirements only. To maximize performance in high-volume print environments, you require additional disk space and memory, and a faster processor.

| Component | Minimum Requirements |
|------------------------------|--|
| Hardware | <ul style="list-style-type: none"> • Processor: Pentium III, Athlon or better • System memory: minimum 512 MB • Application Disk space: 100 MB • Database Disk space: 20 MB • Display Resolution: 1024 x 768 |
| CAS/DCE/DRE Operating System | <p>One of:</p> <ul style="list-style-type: none"> • Windows Server 2003 (32 bit) • Windows XP Professional (32 bit only)¹ • Windows Server 2008 (32 and 64 bit), 2008 R2 (64 bit) <p>Note: All necessary operating system Critical Updates must be installed prior to installing the Secure Access Server software.</p> |
| Databases | <ul style="list-style-type: none"> • Microsoft SQL Server 2005 Express² • Microsoft SQL Server 2008 Express (64 bit) <p>Note: Secure Access cannot be installed on a server running an MSDB application such as FreeFlow™ SMARTsend™ since these databases conflict with the SQL Server database.</p> |

¹ If you plan to install the CAS service on a Windows XP Professional server that is not joined to a domain, follow the instructions on page 15 to configure user authentication settings.

² SQL Server 2005 Express requires Windows Service Pack 2 (SP2) or higher in order to run on Windows Server 2008 or 2008 R2.

User Authentication Settings under Windows XP Pro

If you plan to install the Secure Access CAS service on the Microsoft Windows XP Professional platform, and the machine is not joined to a domain, you must change the Windows XP security settings to accommodate logins into named user accounts.

By default under Windows XP Pro, network logons that use local accounts are automatically mapped to the Guest account. If you want users to authenticate as themselves, you must change this setting.

Complete these steps prior to running the Secure Access install wizard.

1. Open the Local Security Settings window on the machine where you will install the CAS service.
2. In the left navigation pane, double-click **Local Policies**, then double-click **Security Options**.

3. In the right pane, scroll down to locate the entry for **Network access: Sharing and Security model for local accounts**.
4. Double-click this entry and choose **Classic: local user authenticate as themselves**.
5. Click **Apply**, then click **OK** to close the window.
6. Close the Local Security Settings.

Secure Access Hardware Component Requirements

You should ensure that you have all the hardware provided:

Configuration 1

- Power supply
- Power cable
- Bypass key (metal key used to reset the device to defaults) See Resetting an Authentication Device in the Administration Guide Appendices.
- 10/100 Base-T Ethernet network cable
- Card Reader

OR

Configuration 2

- Secure Access USB Card Reader.

Supported Card Readers

Secure Access supports the following card readers:

- ABA Magstripe
- Mifare (including HID iCLASS readers)
- Legic
- HID 125 kHz
- Indala
- EM Marin
- Hitag

Installing the Secure Access Server

This chapter includes:

- [Preparing the Network and Database](#) on page 22
- [Run the Installation Wizard](#) on page 23
- [Upgrading Secure Access](#) on page 25

This section provides instructions for using the Secure Access Server installation wizard to install the Secure Access Server. Ensure that you follow the instructions carefully, and that the server machines meet the minimum operating requirements outlined in [Secure Access Server System Requirements](#) on page 18.

This chapter contains information to:

- Prepare the network and database prior to installation
- Use the Installation wizard to select install components per Secure Access Server

Preparing the Network and Database

Although the Secure Access installation routine is very simple, you must perform the following tasks prior to running the Install wizard:

1. Plan system roles.
2. Enable Xerox Secure Access on the MFP by using the CentreWare Internet Services software.

Notes:

- Using a web browser, log into the CentreWare Internet Services software on the MFP. Access the page to enable Xerox Secure Access. This setup will require SSL to be enabled, and a certificate be created. Consult the MFP System Administration CD for more information.
 - For USB Card Readers the MFP may require a software upgrade. Please contact your Xerox Representative or go to the support page for your Specific MFP by navigating to "Support and Drivers" on www.xerox.com
3. Determine the installation destination for each of the Secure Access components.
Note: Before you deploy Secure Access on the network, ensure that you have Administrator privileges on all machines that must be installed and configured.
 4. Verify that your network configuration is prepared to handle the communication between Secure Access components.
 5. Using Windows Updates, ensure all necessary operating system Critical Updates are installed.
 6. Install the Microsoft .NET Framework 2.0.
Note: Refer to the Microsoft website for a complete list of SQL Server 2005 or 2008 Express Edition prerequisite installation requirements.
 7. Install and configure the database.
Note: If you are using SQL Server 2005 or 2008 Express, you must configure the database to use Windows Authentication Mode. Secure Access does not support mixed mode authentication.

Run the Installation Wizard

During the Secure Access installation, the installation wizard enables you to select the features you want to install per server machine. If you are distributing the components across multiple server machines, you must run the wizard on each server machine, selecting only the required components. If you are installing on a single server machine, you only need to run the wizard once.

Each deployment requires at least one CAS, DCE, DRE, and Secure Access Manager.

1. Ensure that the steps in "Preparing the Network and Database," are completed before running the installation.
2. Close all other applications on the server machine prior to running the Secure Access installation.
3. Launch the Secure Access installation wizard.

- If you are installing from the Secure Access CD, select the **32-bit Setup.exe** to begin the install for a 32-bit machine, or select the **64-bit Setup.exe** to begin the install for a 64-bit machine.

OR

- If you are installing from an electronic distribution, download the ZIP file and run the 32-bit or 64-bit server **Setup.exe** file.

Note: If you attempt to run the setup.exe file and receive an error message, you may need to update the version of the Microsoft Installer. Visit the Microsoft website and download and install the latest Microsoft installer for your operating system.

4. At the Welcome screen, click **Next** to begin the installation process.
5. Review the Software License agreement, and click **I accept**, then click **Next**.
6. Choose the options you want to install on this machine, then click **Next**.

By default, all components are selected. Select only those components that you need on this particular server machine. For example, if this machine is your Print Server, install only the DRE and DCE components. Run the Installer on another server machine to install the remainder of the components as needed.

Note: Read the component descriptions provided in [Secure Access Components](#) on page 14 before you install any component. This information will help you determine how to best deploy the components to suit the needs of your organization.

7. Choose the interface language you want in the **Select Language** screen. This is the language that will be used in the Secure Access Manager only. The language used in all MFP front panel prompts is controlled by the MFP settings.
8. In the **Instance for SQL Express** screen, enter the database instance name that you created for the SQL Express database. Click **Next**.

Note: The instance name you enter in this field **MUST** match the instance name you created for the Secure Access database when you installed SQL Express. The installation cannot proceed without the correct instance name. If you performed a standard SQL Express install and did not change any parameters from the default, leave this setting as SQLEXPRESS, then click Next.

9. Specify a **UserID** and **Password** for services in the **User Name for Services** screen.

When deploying the components on more than one machine, you **MUST** enter the same user credentials for each install. These credentials are used to start and run all services. If you fail to enter the same credentials on all components, the Core Authentication Server will not respond to requests by the DCE or DRE.

Domain accounts must use the domain name (for example, domain\username).

Although this account does not require Administrative privileges on the Secure Access Server, the account must have Print Operator privileges to allow the DRE to process print requests.

10. Enter the name of the Xerox Secure Access Authentication Server.

When you launch the Secure Access Manager, you need to identify the Core Authentication Server by the name you enter here.

11. Click **Install** to start the installation process. The installation wizard copies files, sets up services, and creates shortcuts to the Secure Access Manager.

12. At the end of the process, click **Finish** to exit the installation wizard.

13. The Secure Access server installation is now complete. Refer to Chapter 5 to set up the Secure Access hardware.

Upgrading Secure Access

Whether performing a phased upgrade, or upgrading all components during a period of scheduled downtime, the instructions below step you through the Installation wizard for upgrading Secure Access.

Note: It is recommended that you back up your database prior to performing an upgrade.

During the Secure Access upgrade, the installation wizard detects the Secure Access components already installed on the machine (e.g. the database). These components will be automatically selected in the installation wizard. You can leave the default selections, or you can select additional components to install.

To upgrade Secure Access, do the following:

1. Close all other applications on the server machine prior to running the Secure Access installation.
2. Launch the Secure Access installation wizard.
 - If you are installing from the Secure Access CD, select the **32-bit Setup.exe** to begin the install for a 32-bit machine, or select the **64-bit Setup.exe** to begin the install for a 64-bit machine.OR
 - If you are installing from an electronic distribution, download the ZIP file and run the 32-bit or 64-bit server **Setup.exe** file.

Note: If you attempt to run the setup.exe file and receive an error message, you may need to update the version of the Microsoft Installer. Visit the Microsoft website and download and install the latest Microsoft installer for your operating system.

3. At the Welcome screen, click **Next** to begin the installation process.
4. Review the Software License agreement, and click **I accept**, then click **Next**.
5. Choose the options you want to install on this machine, then click **Next**.

By default, all components are selected. Select only those components that you need on this particular server machine. For example, if this machine is your Print Server, install only the DRE and DCE components. Run the Installer on another server machine to install the remainder of the components as needed.
6. Enter the name of the Xerox Secure Access Authentication Server.
7. Click **Finish** to exit the installation wizard.

The Secure Access server upgrade is now complete. Refer to Chapter 5 to set up the Secure Access hardware.

Setting Up the Secure Access Hardware

This chapter includes:


- [Configure the Authentication Device IP Address](#) on page 28
- [Mount the Secure Access Authentication Device](#) on page 31
- [Connect the Hardware](#) on page 32
- [Mount/Connect the Secure Access USB Card Reader](#) on page 33

This chapter provides instructions to perform the physical setup of the Secure Access Hardware. Prior to setting up any Secure Access Hardware, you must have installed the Secure Access Server software. Follow the instructions provided in Chapter 4 to complete the Secure Access Server installation.

If you are using a USB card reader for Secure Access skip to page 33.

1. Set the IP Address for each Authentication Device.
2. Mount the Secure Access Authentication Device hardware on or near the MFP.
3. Plug in the power, serial, expansion, and card reader connections.

Configure the Authentication Device IP Address

 **CAUTION:** If you are not using a DHCP server to assign IP addresses, DO NOT CONNECT THE AUTHENTICATION DEVICE TO THE NETWORK until you have set the IP Address manually. See [Manually Assign the IP Address](#) on page 29.

Secure Access Authentication Devices are configured for DHCP communication by default. You need to assign an IP address to each Authentication Device, and set the server IP address of the DCE component. There are two methods to assign the IP address:

- You can use a DHCP server to assign addresses. Follow [Configure the DHCP Server to Locate the Authentication Devices](#) on page 28.
- If you are not using a DHCP server, or if you prefer not to set option 230 on your DHCP server, you need to use the Authentication Device Web Admin application to set the addresses manually. Follow [Manually Assign the IP Address](#) on page 29.

Configure the DHCP Server to Locate the Authentication Devices

The instructions below are specific to a Windows DHCP server. If your DHCP server runs on a different platform (for example UNIX, Linux, OS X server, OpenVMS, AS/400 DHCP servers), ensure that you configure the DHCP server to pass the DCE server address in value 230.

Note: For additional technical information on using DHCP to assign IP Addresses to the Secure Access Authentication devices, refer to the Setting the Secure Access Authentication Device IP Address White Paper located on www.xerox.com.

1. In Windows Administrative Tools, open the DHCP windows management console.
 2. Select the DHCP server root node.
 3. From the **Action** menu, select **Set Predefined Options**.
 4. From the **Option Class** drop-down list, select **DHCP Standard Options**.
 5. In the **Option Name** section, click **Add**.
 - a. In the **Name** field, type: Xerox Secure Access
- Note:** The **Name** field label is for identification purposes.
- b. From the **Datatype** drop-down list, select String.
 - c. In the **Code** field, type 230.
 - d. In the **Description** field, type: Secure Access
6. Click **OK**.
 7. In the **String Value** section, enter EQ;A;<DCE Server IP address> in the **String** field, where <DCE Server IP address> is the IP address of your DCE server.
 8. Expand the **Scope** node and select **Scope Options**.
 9. From the **Action** menu, select **Configure Options**.
 10. Select **230**.
 11. Click **OK** to save the changes.

Manually Assign the IP Address

Follow these instructions only if you are not using a DHCP server to set the IP Address of the Authentication Device OR if you are using a DHCP server, but prefer to use static IP Addresses rather than using option 230.

When first powered up, the Authentication Device looks for a DHCP server to secure an IP Address. If no DHCP server is found, the device switches to static communication and defaults to a static IP Address of 192.168.2.1. You can use an Ethernet cable to connect a system (for example, a laptop) to each Authentication Device, then use a Web Admin tool to change the IP Address, and enter the DCE Server IP Address.

Print out the Configuration Tear Sheet found on page 32 before you start. Use this sheet to record the IP addresses you assign to each Authentication Device.

Configure the Laptop:

The system running the Web Admin tool must recognize the static IP Address before you can access the Web Admin tool.

1. On the system (laptop) that will run the Web Admin tool, select **Network Connections > Local Area Connection > Properties**.
2. Double-click **Internet Properties (TCP/IP)**, then click **Advanced**.
3. In the IP addresses section, click **Add**.
4. Enter the following:
IP Address: 192.168.2.x (where x is an unassigned IP)
Subnet Mask: 255.255.255.0
5. Click **Add** to save the changes.

Use the Web Admin Tool to Set IP Addresses:

Perform the following procedure on each Authentication Device.

1. Use a regular Ethernet cable to connect a laptop to the Downlink port on the Secure Access Authentication Device.
2. To power up the Authentication Device, attach one end of the AC power cable to the Authentication Device, then plug the other end into an available outlet.
3. Launch a web browser, and type 192.168.2.1 in the Address field.
This is the factory default IP address assigned to the Secure Access Authentication Device.

Note: For French, select the link provided.

4. Click on the **Configure** link at the top of the page.
5. Enter the following to login:
User name: deviceadmin
Password: pc_passwd

Setting Up the Secure Access Hardware

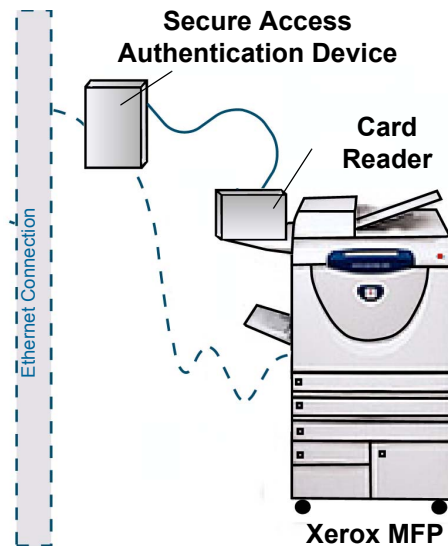
6. Change the password used to access the Web Admin tool. You can reset the password at any time, but ensure that you change the password from the default setting before the Secure Access system is up and running.
7. In the **Configure Xerox Secure Access Authentication Device** section, choose Static IP from the **Addressing mode** field.
8. Enter a static IP address in the **IP Address** field to set the address of this Authentication Device.
9. In the **Configure Server** section, enter the DCE Server's IP Address in the Server IP Address field.
10. Click the **Update Configuration** button located below the Configure Server fields.
11. Click the **Restart** link at the top of the page, then click "Click here to confirm restart" to restart the terminal.

Repeat these instructions for each Secure Access Authentication Device that you are deploying.

Note: Remember to reconfigure the laptop Internet Properties when you are done.

Mount the Secure Access Authentication Device

Print out the [Configuration Tear Sheet](#) on page 35. As you work, complete the columns on this sheet. You need this information when you configure communication between devices on the Secure Access Server.



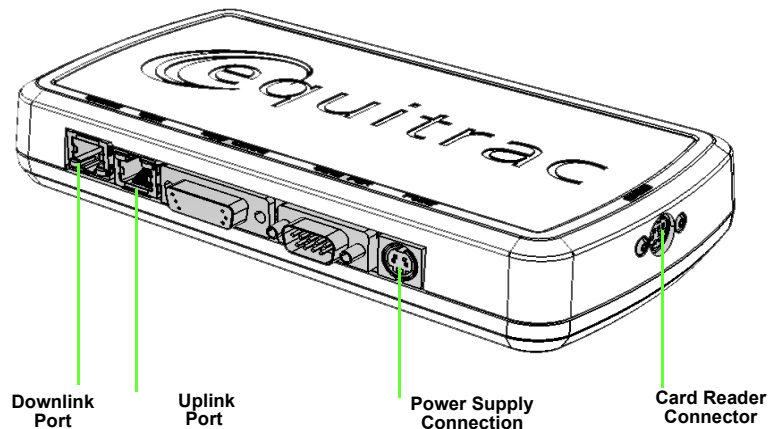
1. Lay the Authentication Device on the floor, behind and on the input side of the MFP. **The device should be placed in an unobtrusive location, but ensure that you have enough cable length (6') to connect to the Card Reader.**
2. Mount the Card Reader on the shelf on the left side of the MFP front panel using the supplied Velcro strip. If you have the Convenience Stapler option, place the Card Reader to the right of the stapler so the Card Reader is between the stapler and MFP. **Ensure the Document Handler top cover can be opened without being obstructed by the Card Reader before attaching the Velcro strip.**
3. Use the Tear sheet to record the IP and MAC Address of the Authentication Device as well as the IP Address and Hostname of the MFP that this Authentication Device will control.

Note: Refer to the MFP System Administration CD for other suggested mounting locations.

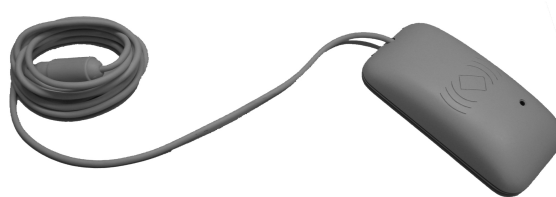
Connect the Hardware

Ensure that you have performed the configuration tasks provided in [Configure the Authentication Device IP Address](#) on page 28 before you connect the Secure Access Authentication Device hardware.

Using the labeled graphic below for reference, connect the components. Note that the Authentication Device provides a serial port and a copy control port that is not used in this configuration.



1. Use the Tear sheet to record the MAC address of the Authentication Device. Enter this address in the same row as the MFP it will control.
2. Plug the Card Reader serial cable into the Card Reader connector on the Authentication Device.



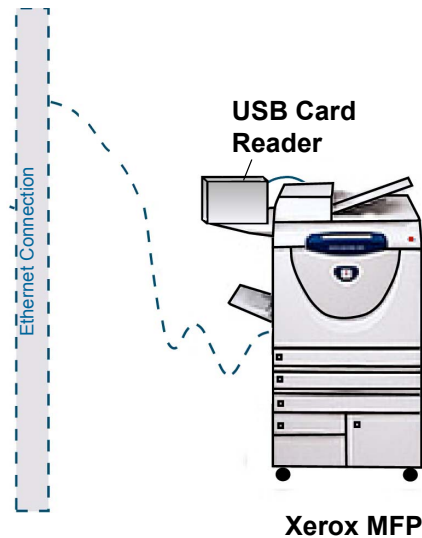
3. Connect one end of the Ethernet cable into the network drop and the other end into the Uplink port on the Secure Access Authentication Device.
4. Connect the MFPs Ethernet cable to the Downlink port on the Authentication Device.

Note: When the Authentication Device is powered off, there is no Ethernet connectivity available from the Downlink port. Alternatively, you can plug the MFP Ethernet cable directly into another Ethernet port. The Downlink port is provided on the Authentication Device in the event that another Ethernet port is not available.

5. Connect the power supply to the Authentication Device, then plug the other end into the nearby receptacle.

The hardware setup is now complete. Use the instructions in the Secure Access Administration Guide to configure the Secure Access Server and enable communication between the Authentication Devices and MFPs.

Mount/Connect the Secure Access USB Card Reader



1. Mount the Card Reader on the shelf on the left side of the MFP front panel using the supplied Velcro strip. If you have the Convenience Stapler option, place the Card Reader to the right of the stapler so the Card Reader is between the stapler and MFP. **Ensure the Document Handler top cover can be opened without being obstructed by the Card Reader before attaching the Velcro strip.**
2. Plug the Secure Access USB Card Reader cable into a free USB port on the back of the MFP. Refer to the MFP System Administration CD for other suggested mounting locations.

Configuration Tear Sheet

Tear this sheet out and use it when performing the physical setup of the Authentication Devices. You must keep careful track of the IP and MAC Address of each Authentication Device and the corresponding MFP that it will control.

| | Authentication Device | | Multifunction Device | |
|----|-----------------------|------------|----------------------|----------|
| | MAC Address | IP Address | IP Address | Hostname |
| 1 | | | | |
| 2 | | | | |
| 3 | | | | |
| 4 | | | | |
| 5 | | | | |
| 6 | | | | |
| 7 | | | | |
| 8 | | | | |
| 9 | | | | |
| 10 | | | | |
| 11 | | | | |
| 12 | | | | |
| 13 | | | | |
| 14 | | | | |
| 15 | | | | |
| 16 | | | | |
| 17 | | | | |
| 18 | | | | |
| 19 | | | | |
| 20 | | | | |

