

Software Version 5.3  
August 2014  
702P03155



# Xerox Secure Access Unified ID System<sup>®</sup> 5.3 Installation Guide



©2014 Xerox Corporation. All rights reserved. XEROX<sup>®</sup> and XEROX and Design<sup>®</sup>, and Xerox Secure Access Unified ID System<sup>®</sup> are trademarks of Xerox Corporation in the United States and/or other countries.

Equitrac<sup>®</sup> and Follow-You Printing<sup>®</sup> are registered trademarks of Nuance Communications.

Document Version: 1.0 (August 2014)

# Table of Contents

<b>1</b>	<b>Introduction</b> .....	<b>1-1</b>
	Installation Overview .....	1-2
	Xerox Secure Access Server Components .....	1-3
	Xerox Secure Access Administrative Applications .....	1-4
	Virtual Server Support .....	1-4
	Account Synchronization Support .....	1-4
	Preparing the Network and Database .....	1-5
	Determining the Install Locations .....	1-5
	System Requirements .....	1-6
	Virus Scanning Setup .....	1-8
	Server Folders to Exclude .....	1-8
	File Extensions to Exclude .....	1-8
	Additional Documentation .....	1-8
<b>2</b>	<b>Server Installation</b> .....	<b>2-1</b>
	Local Installation Workflow .....	2-2
	Installing the Server Components .....	2-2
	Installing the Master CAS .....	2-7
	Microsoft SQL Server Configuration .....	2-7
	Install Specific Server Components .....	2-8
	Applying Xerox Secure Access Licenses .....	2-12
	Xerox Secure Access Licensing Workflow .....	2-12
	Installing DRE .....	2-15
	Installing DCE .....	2-15
	Verifying the Server Installation .....	2-16
	Add a Printer on a TCP/IP Printer Port .....	2-16
	Add a Printer on an Equitrac Printer Port .....	2-17
	Convert a TCP/IP Port to Equitrac Port .....	2-18
	Device Registry Confirmation .....	2-21
	Spool Setting Verification .....	2-21
	Installation Troubleshooting .....	2-22
	If Device Does not Display in System Manager .....	2-22
	If Licensing Fails .....	2-22
	If the Serial Number is Denied .....	2-22
<b>3</b>	<b>Upgrade Xerox Secure Access</b> .....	<b>3-1</b>
	Planning the Upgrade .....	3-2
	Single Machine Upgrade .....	3-2
	Multiple Machine Upgrade .....	3-2
	Upgrading from Xerox Secure Access 5.2 to 5.3 .....	3-3
	Upgrading from Xerox Secure Access to Equitrac Office® 5.3 .....	3-3
	License Upgrade .....	3-3
	Full Product Upgrade .....	3-3
	Installing Equitrac Office 5.3 .....	3-4
<b>4</b>	<b>Uninstall Xerox Secure Access</b> .....	<b>4-1</b>

Restoring Printers to Defaults .....	4-2
Uninstalling Server Components .....	4-2

# Introduction

## Topics

[Installation Overview](#)

[Xerox Secure Access Server Components](#)

[Preparing the Network and Database](#)

[Determining the Install Locations](#)

[System Requirements](#)

[Virus Scanning Setup](#)

[Additional Documentation](#)

Xerox Secure Access measures, monitors, and manages document output on your network. By regulating devices on the network, and local desktop printers, Xerox Secure Access tracks and controls photocopies, print jobs, scan jobs, and faxes with minimal administration.

There are several different installation methods you can follow to get Xerox Secure Access up and running. Read this chapter before beginning the installation to confirm the best option for your site, the system requirements, and the tasks to complete before you can install the software.

# Installation Overview

Xerox Secure Access provides installation wizards to guide you through the server installs. There are several different types of deployment. Follow the instructions indicated to install the components in the correct order.

Deployment	Description
Local	<ul style="list-style-type: none"><li>All Xerox Secure Access server components are installed on a single machine. See <a href="#">Local Installation Workflow on page 2</a>.</li></ul>
Remote	<ul style="list-style-type: none"><li>Xerox Secure Access server components are deployed across multiple networked machines. See <a href="#">Installing the Master CAS on page 7</a>.</li></ul>
Cluster	<ul style="list-style-type: none"><li>Xerox Secure Access components are distributed in a Windows cluster environment. See the <i>Cluster Deployment Guide</i>.</li></ul>
Upgrade	<ul style="list-style-type: none"><li>An existing Xerox Secure Access 4.x installation currently in place. See <a href="#">Upgrade Xerox Secure Access on page 1</a>.</li></ul>

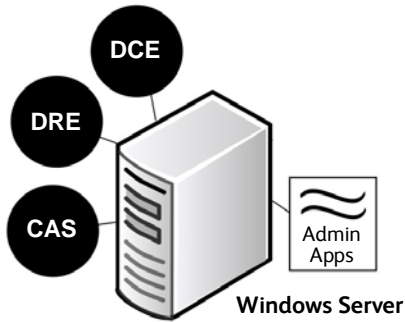
## Note

Refer to [ReleaseNotes.pdf](#) on the Partner Portal for potentially important installation or upgrade information not contained in this document.

# Xerox Secure Access Server Components

Xerox Secure Access is comprised of core server components. Core server components are essential and must be installed on a Windows Server system.

Every Xerox Secure Access installation relies upon a set of core components to provide basic accounting functionality. Core components can reside on a single Windows Server or you can deploy these components across multiple servers as outlined in [Installing the Master CAS on page 7](#).



Core Component	Description
Core Accounting Server (CAS)	<ul style="list-style-type: none"> <li>• verifies users, calculates printing charges, and assigns charges to an appropriate user or group account</li> <li>• calculates charges using page count and job attribute information</li> <li>• contains an accounting database where all printer, user, department, billing code, transaction, and balance information is stored</li> <li>• provides primary and secondary pricing structures to track different costs/billing scenarios</li> <li>• provides dual pricing capabilities</li> </ul>
Document Routing Engine (DRE)	<ul style="list-style-type: none"> <li>• routes network print jobs to the appropriate device</li> <li>• communicates with attached printers to determine size and attributes of each print job; passes the information to the Core Accounting Server (CAS)</li> <li>• fully integrated with the Windows printing subsystem</li> <li>• enables the Port Monitor to receive and route print jobs to parallel or network-connected printers</li> </ul>
Device Control Engine (DCE)	<ul style="list-style-type: none"> <li>• enables document flow from user workstations to output devices such as printers, digital copiers, scanners, and plotters</li> <li>• provides transaction tracking at the device level</li> <li>• communicates via different interfaces to control and management copy, fax, and hardware devices.</li> <li>• provides the ability to optionally configure caching of login credentials, enabling users to log in on embedded clients even when network connection to CAS is lost</li> </ul>

## Xerox Secure Access Administrative Applications

Xerox Secure Access Administrative Applications provide the tools to configure and manage network printing and tracking. When deploying Xerox Secure Access, you must install the Administrative Applications on each machine that will host CAS.

When installing CAS, the installation wizard also selects all Administrative Applications, forcing you to install these tools on the CAS server system. If you want to manage the system remotely, simply install the Administrative Applications on another machine within the deployment. If you correctly identify the master CAS server, and have Admin Access Permissions when you launch the tools, you can easily manage the system remotely. For information on settings Access Permissions, see the *Xerox Secure Access Unified ID System® Administration Guide*.

Admin Tool	Primary Function
System Manager	<ul style="list-style-type: none"> <li>manage system settings and configuration, including licensing</li> </ul>

Refer to the *Xerox Secure Access Unified ID System® Administration Guide* for detailed information on these tools.

## Virtual Server Support

Xerox Secure Access is fully supported on all hardware platforms compatible with Windows Server 2008, 2008 R2, 2012 and 2012 R2. The use of Xerox Secure Access under virtual environments such as Virtual Server or VMWare is generally supported and is fully expected to work correctly, as long as such environments fully support the server operating system (e.g. Windows Server 2008), as Xerox Secure Access does not make any assumptions about the underlying hardware platform. Care must be taken when configuring the virtual environment to ensure adequate CPU and memory resources are available to the systems running the Xerox Secure Access solution. If adequate resources are not defined or available there can be an impact on performance. Consult your account representative for details.

## Account Synchronization Support

Xerox Secure Access supports account synchronization with Active Directory (AD), Active Directory Lightweight Directory Services (AD LDS) and Lightweight Directory Access Protocol (LDAP).

### Note

AD LDS synchronization is supported under certain conditions. Please refer to Microsoft TechNote entitled “**Synchronize with Active Directory Domain Services**” ([http://technet.microsoft.com/en-us/library/cc794836\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/cc794836(WS.10).aspx)) for further information.



# Preparing the Network and Database

Although the Xerox Secure Access installation process is quite simple, you must gather network details and prepare the database prior to the install. It is recommended that the SQL Express database be installed prior to running the Xerox Secure Access installation.

Prior to install, you should:

1. Plan system roles.
2. Determine the installation destination for each of the Xerox Secure Access components.

## Note

Before you deploy Xerox Secure Access on the network, ensure that you have Administrator privileges on all machines that must be installed and configured.

3. Verify that your network configuration is prepared to handle the communication between Xerox Secure Access components, including document routing to the network printers.
4. Install and configure TCP/IP protocol on the intended print server machine and on network printers.

# Determining the Install Locations

Depending on the size of the Xerox Secure Access deployment and your network requirements, you can choose to install all server components on a single machine or you can deploy across multiple servers. If you deploy on a single machine, the install is referred to as “local”. See [Local Installation Workflow on page 2](#). If you deploy across multiple servers, the install is considered “remote”. See [Installing the Master CAS on page 7](#).

# System Requirements

Before you install Xerox Secure Access ensure that the client and server machines you plan to use meet the minimum operating requirements outlined below. To maximize performance in high-volume print environments, you require additional disk space and memory, and a faster processor.

## Note.

Net Framework packages 3.5 and 4.5 must be installed on Windows 8 and Windows 8.1 prior to installing the Windows Client.

## Server Requirements

Server Components	Software Platforms <sup>1</sup>	Recommended Hardware <sup>2</sup>
Core Accounting Server (CAS) Device Control Engine (DCE)	<ul style="list-style-type: none"> <li>Windows Server<sup>3</sup> 2008 (x86 or x64)<sup>4,5</sup></li> <li>Windows Server 2008 R2 (x64)<sup>5</sup></li> <li>Windows Server 2012 (x64)</li> <li>Windows Server 2012 R2 (x64)</li> <li>Windows Small Business Server 2011 Essentials/ Standard</li> <li>SharePoint Server 2007 and 2010</li> <li>RightFax Server 9.4 and higher</li> </ul>	<ul style="list-style-type: none"> <li>Processor: 2 GHz or greater</li> <li>Memory: 2 GB or greater</li> <li>Hard disk: 1 GB or greater</li> </ul>
Core Accounting Server (CAS) – Database	<ul style="list-style-type: none"> <li>Microsoft SQL Server 2008 and 2008 Express</li> <li>Microsoft SQL Server 2012 and 2012 Express</li> </ul>	<ul style="list-style-type: none"> <li>Processor: 2 GHz or greater</li> <li>Memory: 2 GB or greater</li> <li>Hard disk: 1 GB or greater</li> <li>Hard disk: 2.2 GB required for SQL Server 2012</li> </ul>
Document Routing Engine (DRE) Print Server – with Rules and Routing or Secure Document Release	<ul style="list-style-type: none"> <li>Windows Server 2008 (x86, x64)<sup>5</sup>, 2008 R2 (x64)<sup>5</sup>, 2012 (x64), 2012 R2 (x64)</li> <li>Windows Small Business Server 2011 Essentials/ Standard</li> <li>SUSE Linux 10 SP4 OES2 SP3 iPrint (x86, x64)</li> </ul>	<ul style="list-style-type: none"> <li>Processor: 2 GHz or greater</li> <li>Memory: 2 GB or greater</li> <li>Hard disk: 1 GB or greater + allocation for print jobs</li> </ul>
Core Accounting Server (CAS) Device Control Engine (DCE) – Cluster server	<ul style="list-style-type: none"> <li>Windows Server 2008, 2008 R2, 2012, 2012 R2 cluster<sup>5</sup></li> </ul>	<ul style="list-style-type: none"> <li>Processor: 2 GHz or greater</li> <li>Memory: 2 GB or greater</li> <li>Hard disk: 1 GB or greater</li> </ul>
Document Routing Engine (DRE) Print Server – Cluster server	<ul style="list-style-type: none"> <li>Windows Server 2008, 2008 R2 cluster<sup>5</sup></li> </ul> <p><b>Note:</b> Windows Server 2012, 2012 R2 cluster not supported on DRE</p>	<ul style="list-style-type: none"> <li>Processor: 2 GHz or greater</li> <li>Memory: 2 GB or greater</li> <li>Hard disk: 1 GB or greater + allocation for print jobs</li> </ul>

## Management Tools Requirements

Management Tools	Software Platforms <sup>1</sup>	Recommended Hardware <sup>2</sup>
System Manager	<ul style="list-style-type: none"> <li>Windows Server 2008 (x86, x64)<sup>5</sup>, 2008 R2 (x64)<sup>5</sup>, 2012 (x64), 2012 R2 (x64)</li> <li>Windows Small Business Server 2011 Essentials/ Standard</li> <li>Windows Vista Business/ Enterprise/Ultimate (x86, x64)</li> <li>Windows 7 Professional/ Enterprise/Ultimate (x86, x64)</li> <li>Windows 8 and 8.1 Professional/ Enterprise (x86, x64)</li> </ul>	<ul style="list-style-type: none"> <li>Processor: 2 GHz or greater</li> <li>Memory: 2 GB or greater</li> <li>Hard disk: 50MB or greater</li> </ul>

### Footnotes

<sup>1</sup> For all software platforms, ensure that the latest service packs are applied.

<sup>2</sup> This column indicates minimum hardware requirements only; high printing or high scanning volumes, and/or large installations may require substantially higher performance hardware.

<sup>3</sup> Users/Site Network Administrators are responsible for securing Microsoft Client Access Licenses as required.

<sup>4</sup> x86 refers to 32-bit architecture; x64 refers to 64-bit architecture (IA64 chip set is not supported).

<sup>5</sup> Windows Server 2008 Server Core and Windows Server 2012 Server Core are not supported.

### Note

The system operating requirements are updated regularly. Please refer to the latest Xerox Secure Access Technical Specifications document available from the Equitrac Partner Portal for the most up-to-date information.

# Virus Scanning Setup

To ensure successful communication between Xerox Secure Access services, there are certain folders and file extensions that you should exclude from virus scanning.

## Server Folders to Exclude

It is recommended that the following server folders be exclude from virus scanning:

- The folder and sub-folders containing Xerox Secure Access
- The SPOOL folder that the Windows spooler service is configured to use. The default location for all printer spool files is % SystemRoot % \System32\Spool\Printers.
- C:\Users\**<userid>**\AppData\Local\Temp
- C:\Users\**<userid>**\AppData\Local\Xerox Secure Access

Where **<userid>** is the account under which the Xerox Secure Access services are running.

### Note

The installation path depends on the location where Xerox Secure Access was installed on the server. If you installed Xerox Secure Access services on another drive letter or at another location altogether, substitute that drive letter and path in the paths listed above.

On a cluster, also exclude cache folders on any shared disks used by Xerox Secure Access components, including the spool folders used by print spooler shared disks.

## File Extensions to Exclude

Exclude the following file extensions from virus scanning:

- database files (mdf, ldf)
- trace log files (log)

# Additional Documentation

To learn more about the advanced features and functionality of the Xerox Secure Access Suite, refer to the following guides:

Guide	When to refer to this guide
<b>Planning Guide</b>	Use this guide to evaluate and plan an Xerox Secure Access deployment on your network.
<b>Administration Guide</b>	After installing Xerox Secure Access, use this guide to configure Xerox Secure Access for use in your organization.
<b>Cluster Deployment Guide</b>	If you are deploying Xerox Secure Access in an existing cluster environment, use this guide to plan the installation.
<b>Xerox Embedded Guides</b>	Use these specific guides for Xerox embedded clients.

# Server Installation

# 2

## Topics

[Local Installation Workflow](#)

[Installing the Server Components](#)

[Installing the Master CAS](#)

[Applying Xerox Secure Access Licenses](#)

[Installing DRE](#)

[Installing DRE](#)

[Installing DCE](#)

[Verifying the Server Installation](#)

[Installation Troubleshooting](#)

This chapter provides the steps required to install all Xerox Secure Access components on either a single machine, or across multiple machines. A local installation places all Xerox Secure Access server components and Administrative Applications on a single machine. This type of installation is appropriate for small site deployment. If you want to install all components on a single machine, refer to [Local Installation Workflow](#) on page 2.

Xerox Secure Access server components can be installed across multiple machines to balance the print and transaction load. This distribution of components is called a Remote installation, and involves two or more networked machines that will house specific Xerox Secure Access components. You must determine the appropriate network deployment for your enterprise before you install a single Xerox Secure Access component. If you are deploying Xerox Secure Access across a large site, refer to [Installing the Master CAS](#) on page 7.

Ensure that you follow the workflow steps carefully to guarantee a successful installation. Refer to [ReleaseNotes.pdf](#) on the CD for potential important installation or upgrade information not contained in this document.

## Local Installation Workflow

Before installing Xerox Secure Access, ensure that the network and database are prepared for the installation. See [Preparing the Network and Database](#) on page 5 for instructions.

1. **Install Server Components** – Install the Xerox Secure Access server components and the Administrative Applications on the server system(s). See [Installing the Server Components](#) on page 2.
2. **Apply Licenses** – Activate and register all Xerox Secure Access server components. You require the serial numbers for each component. See [Applying Xerox Secure Access Licenses](#) on page 12.
3. **Verify the Installation** – Create a printer and ensure that print tracking is successful. See [Verifying the Server Installation](#) on page 16.

## Installing the Server Components

When installing Xerox Secure Access, the installation wizard allows you to select the server components to install per machine. For a local installation, install all components on the same machine. If you are installing all server components on a single machine, you only need to run the wizard once.

### Note

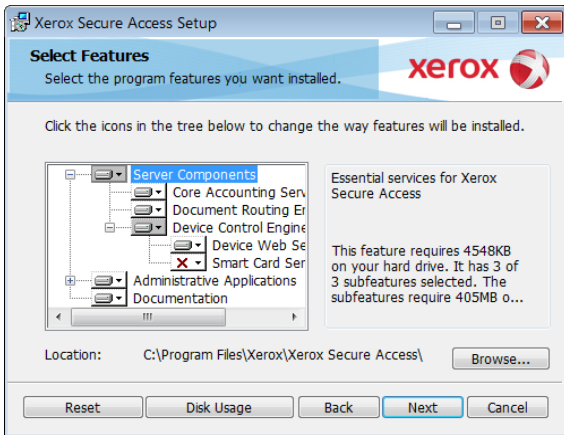
For Windows Servers 2008, 2008 R2, 2012 and 2012 R2, make sure the server is up to date with the latest service packs, or manually download and install the latest version of Windows Installer from [www.microsoft.com](http://www.microsoft.com). Windows Installer 4.0 (or higher) is required to install Xerox Secure Access 5.3. If you do not have Windows Installer 4.0 (or higher) the following error displays: **“This installation package cannot be installed by the Windows Installer service. You must install a Windows service pack that contains a newer version of the Windows Installer Service.”**

To install Xerox Secure Access locally on a single machine, do the following:

1. Close all other applications on the server prior to running the Xerox Secure Access installation.
2. Obtain the Xerox Secure Access software zip file from the Equitrac® Product Download site.
3. Select and run the 64-bit Installer file (**Xerox.XSA.x64.msi**) or select and run the 32-bit Installer file (**Xerox.XSAs.x86.msi**) to launch the Xerox Secure Access installation wizard
4. At the **Welcome** screen, click **Next** to begin the installation process.
5. Read and accept the terms of the **End-User License Agreement**, and click **Next** to continue.



6. On the **Select Features** dialog, choose the features you want to install. Additionally, change the default installation folder with the **Browse** button. Click the **Next** button to continue.

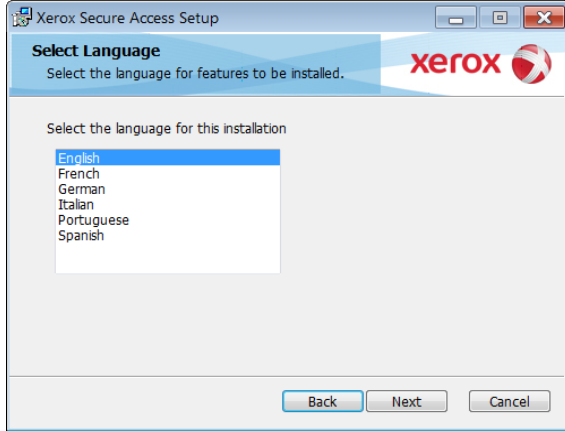


By default, all Server Components and Administrative Applications are selected. Deselect all options not required for the machine you are installing.

Note

Smart Card Reader Support is an optional feature of DCE (available on 64-bit operating systems only). It is required in order to support authentication from a device via a Smart Card.

- 7. On the **Select Language** screen, select the language you want to display in the user interface, and click **Next**.



 **Caution**

You cannot change the display language after installation. To change the language, you must uninstall and reinstall Xerox Secure Access, setting the language during installation. The display language is independent of the regional language set on the machine. For example, Xerox Secure Access can display Italian even if the regional setting is French.

- 8. On the **Service Log On Credentials** screen, enter the **Account** and **Password** of the user who will run the Windows services. Alternatively, click the **Browse** button to search for valid user from a specific location. Click the **Test Credentials** button to verify the user credentials, and click **Next**.

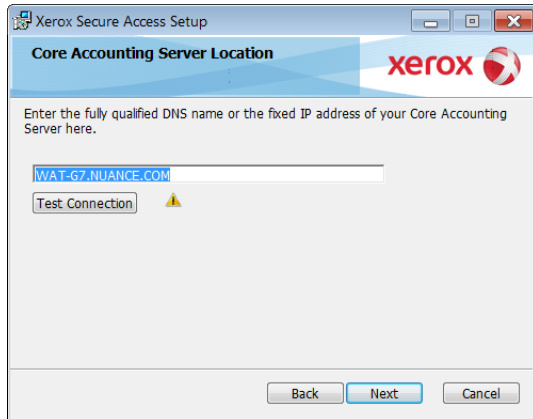




### Note

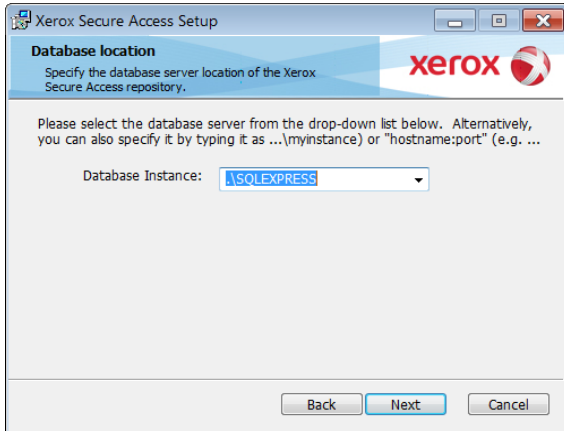
The **Account** field contains the account name in domain\username format. If you are using a SQL Express database that is not on a domain and you are using local accounts, you must enter computername\username. If neither domain or computer name prefix is specified, the user is handled as local user.

9. If any Windows service except Core Accounting Service (Document Routing Engine or Device Control Engine) is selected for installation, the **Core Accounting Server Location** screen appears.



Here you can optionally enter the fully qualified domain name or fixed IP address of the CAS server, and click **Test Connection** to validate a connection across the network, and click **Next** to continue. Otherwise just click **Next** without testing the CAS server.

10. On the **Database location** screen, select the database server, and click **Next**.



11. If the specified SQL Express database (“eqcas”) already exists (e.g., in the case of an upgrade), the **Database Already Exists** screen appears. Select whether to **Replace** or **Keep** the existing database, and click **Next**.



12. Click **Install** to start the installation process. The installation wizard copies files, sets up services, and creates shortcuts to the Administrative Applications.
13. At the end of the process, click **Finish** to exit the installation wizard and begin initial configuration.

# Installing the Master CAS

Run the Server installation wizard on **each** machine within the deployment, and select only the components required per machine. Follow the order of the **steps shown in the Installation Workflow** on the previous page for each machine.

Component	Select these features:
<b>Master CAS</b>	<ul style="list-style-type: none"> <li>• Core Accounting Server</li> <li>• All Administrative Applications</li> </ul>
<b>Subsidiary CAS</b>	<ul style="list-style-type: none"> <li>• Core Accounting Server</li> <li>• System Manager</li> </ul>
<b>DRE</b>	<ul style="list-style-type: none"> <li>• Document Routing Engine</li> </ul>
<b>DCE</b>	<ul style="list-style-type: none"> <li>• Device Control Engine</li> </ul>

## Microsoft SQL Server Configuration

For general instructions on implementing Microsoft SQL Server, refer to the Microsoft SQL Server documentation.

1. On your SQL Server database system, create a database named **eqcas**.
2. Open SQL Server Management Studio, connect to the **eqcas** database and execute the **SQLServerInit.sql** script located on CAS in **C:\Program Files\Xerox\Xerox Secure Access\Database**.
3. Remove all connections to the eqcas database.
4. Connect to the same instance and run the **SQLServerOpt.sql** script to streamline functionality.

### Note

If you name the SQL Server database something different from *eqcas*, you must also change the database name accordingly in the SQLServerInit.sql script and the SQLServerOpt.sql script.

5. Start the EQ Scheduler service and then the Equitrac Core Accounting Server service (EQ CAS).

Xerox Secure Print Manager Suite is now configured to use the Microsoft SQL Server database.

## Install Specific Server Components

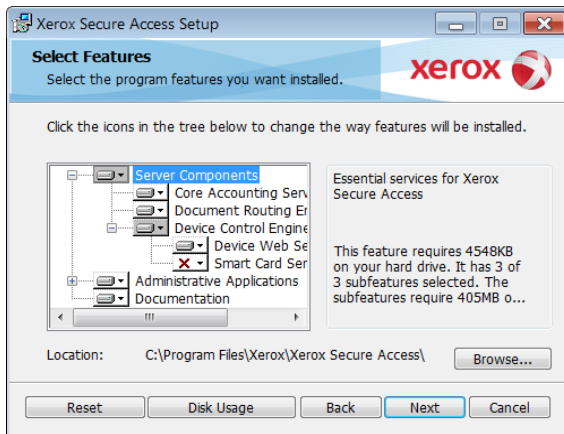
### Note

For Windows Servers 2008, 2008 R2, 2012 and 2012 R2, make sure the server is up to date with the latest service packs, or manually download and install the latest version of Windows Installer from [www.microsoft.com](http://www.microsoft.com). Windows Installer 4.0 (or higher) is required to install Xerox Secure Access 5.3. If you do not have Windows Installer 4.0 (or higher) the following error displays: **“This installation package cannot be installed by the Windows Installer service. You must install a Windows service pack that contains a newer version of the Windows Installer Service.”**

1. Close all other applications on the server prior to running the Xerox Secure Access installation.
2. Obtain the Xerox Secure Access software zip file from the Equitrac Product Download site.
3. Select and run the 64-bit Installer file (**Xerox.XSA.x64.msi**) or select and run the 32-bit Installer file (**Xerox.XSAs.x86.msi**) to launch the Xerox Secure Access installation wizard
4. At the **Welcome** screen, click **Next** to begin the installation process.
5. Read and accept the terms of the **End-User License Agreement**, and click **Next** to continue.



6. On the **Select Features** dialog, choose the features you want to install. Additionally, change the default installation folder with the **Browse** button. Click the **Next** button to continue.



By default, all Server Components and Administrative Applications are selected. Deselect all options not required for the machine you are installing.

### Note

Smart Card Reader Support is an optional feature of DCE (available on 64-bit operating systems only). It is required in order to support authentication from a device via a Smart Card.

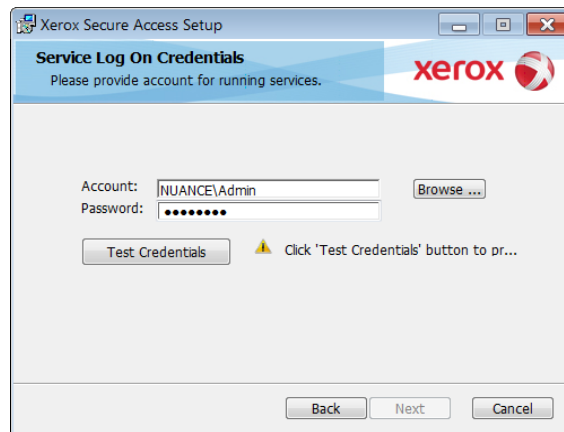
7. In the **Select Language** screen, select the language you want to display in the user interface, and click **Next**.



### ! Caution

You cannot change the display language after installation. To change the language, you must uninstall and reinstall Xerox Secure Access, setting the language during installation. The display language is independent of the regional language set on the machine. For example, Xerox Secure Access can display Italian even if the regional setting is French.

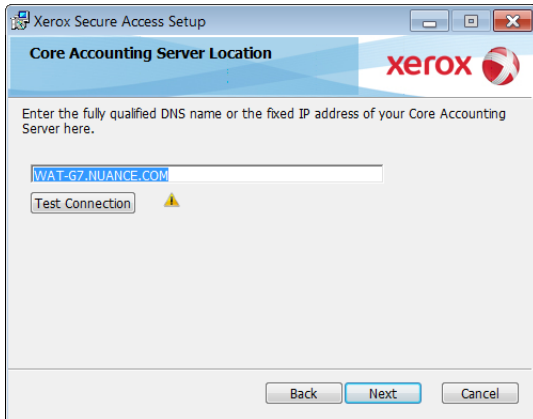
8. On the **Service Log On Credentials** screen, enter the **Account** and **Password** of the user who will run the Windows services. Alternatively, click the **Browse** button to search for valid user from a specific location. Click the **Test Credentials** button to verify the user credentials, and click **Next**.



### Note

The **Account** field contains the account name in domain\username format. If you are using a SQL Express database that is not on a domain and you are using local accounts, you must enter computername\username. If neither domain or computer name prefix is specified, the user is handled as local user.

- 9. If any Windows service except Core Accounting Service (Document Routing Engine or Device Control Engine) is selected for installation, the **Core Accounting Server Location** screen appears.



Here you can optionally enter the fully qualified domain name or fixed IP address of the CAS server, and click **Test Connection** to validate a connection across the network, and click **Next** to continue. Otherwise just click **Next** without testing the CAS server.

- 10. On the **Database location** screen, select the database server, and click **Next**



11. If the specified SQL Express database (“eqcas”) already exists (e.g., in the case of an upgrade), the **Database Already Exists** screen appears. Select whether to **Replace** or **Keep** the existing database, and click **Next**.



12. Click **Install** to start the installation process. The installation wizard copies files, sets up services, and creates shortcuts to the Administrative Applications.
13. At the end of the process, click **Finish** to exit the installation wizard and begin initial configuration.

# Applying Xerox Secure Access Licenses

When Xerox Secure Access is installed for the first time on a specified machine, a limited default license is generated and applied during installation. The auto-generated default license allows full operation of System Manager's features for 45 days, however, there is a limit of only one of each licensable item.

After installation, obtain and register the Base and Feature component licenses in the System Manager Administrative Application before the 45-day default license expires. A new default license cannot be generated by reinstalling Xerox Secure Access on the same machine. When applying the full licenses, the default license is automatically overwritten.

## Xerox Secure Access Licensing Workflow

The Xerox Secure Access solution requires a combination of a Base license (with a system expiry date) and the desired feature licenses. Xerox Secure Access licensing needs to be applied in the following order:

1. Obtain and install a Base license.
2. Obtain and install any feature licenses as required.

### Note

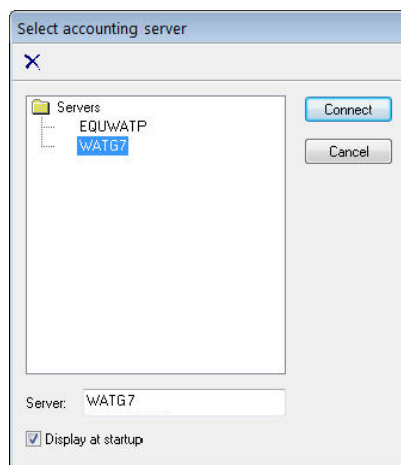
Some feature licenses may require that another feature license is installed as on the system as a prerequisite. For example, the Follow-You Printing® license requires an authentication license already installed on the system.

3. Once the desired licenses are installed, they need to be assigned to devices in the License Assignment View in System Manager.

Licensing requires a combination of serial numbers and activation codes to enable each Xerox Secure Access component. There are two ways to enter this license information: automatically via an Internet connection, or manually by requesting the codes via telephone or email. Regardless of the preferred method, use the following instructions to apply licenses and activate components

To license Xerox Secure Access, do the following:

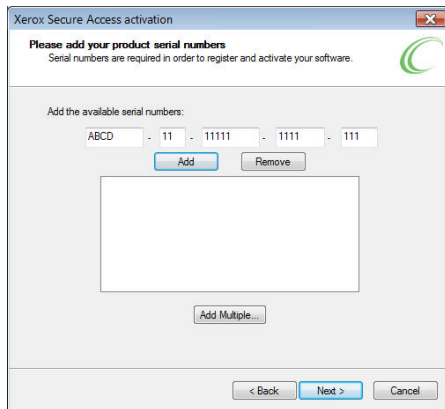
1. Start System Manager by selecting **Start > All Programs > Xerox Secure Access > System Manager**.
2. In the Select Accounting Server dialog box, choose the Core Accounting Server (CAS) with which System Manager is associated, then click **Connect**.





CAS coordinates all Xerox Secure Access components and acts as a guardian for your device resources. The System Manager must be able to establish a connection with CAS before the Administrative Applications will open and you can begin configuration. CAS collects information from and writes to a single accounts database, so you can connect to only one accounting server at a time.

3. Click the **System Manager > Licensing** link in the left pane.
4. Under **Current tasks**, click **Add license** or click **<Add...>** in the right pane.
5. When the Xerox Secure Access activation window opens, click **Next** to begin the activation process.
6. Enter the serial numbers for the components you want to activate. These serial numbers were supplied with your software. After you enter each number, click **Add** to add it to the list, then enter additional numbers as required.



7. When all numbers are entered, click **Next**.
8. Select **Automatic online activation** or **Manual activation**, and click **Next**.

#### Note

If you do not have a connection to both the Internet and CAS, choose **Manual activation**.

9. For **Manual activation**, do the following:
  - a. Contact Equitrac at [www.nuance.com/for-business/by-product/equitrac/index.htm](http://www.nuance.com/for-business/by-product/equitrac/index.htm) or by telephone to obtain the corresponding activation codes.
  - b. After receiving the required activation codes, click **Finish** to continue.
  - c. On the Add licensing Information dialog box, enter the **Activation code**, and click **Add**.  
The activated software license displays in System Manager.
10. For **Automatic online activation**, do the following:
  - a. Follow the Activation wizard prompts to provide contact information. If you have already registered one or more Xerox Secure Access component, the Activation wizard fills the form with previously-collected data.
  - b. The Activation wizard displays a **Collecting information...** message while retrieving system data. If you want to omit technical details about your system, click the **Show technical details** button and select the information you do not want to transmit. You must transmit the following:
    - Accounting server serial number
    - Domain-qualified print server name
    - Organization name as registered in Windows
    - Fully-qualified CAS server DNS name
  - c. When the Activation wizard is ready to transmit the information, review the collected data. Choose whether to send optional data with your activation request.

### Note

The Activation wizard transmits the data using an HTTP connection to the activation server. If the connection fails, the Activation wizard prompts for verification that you have configured the default gateway correctly, and that the Internet is accessible from this machine. You can retry or cancel the activation request at this point.

- d. The Activation wizard transmits the data and returns the status of the activation code(s). The Wizard automatically records the license activation in System Manager, and displays the following activation results:
  - Serial number
  - Activation code
  - Status (either **Success**, **Invalid**; the serial number and activation code is an invalid combination, or **Denied**; the serial number was valid but not accepted).

### If the License is Invalid

If the status is **Invalid**, ensure that you entered all serial numbers and activation codes precisely. Each component requires a separate license—unless you purchased an Enterprise license. If the problem persists, contact the Equitrac Customer Support Center to resolve this problem.

### If the Serial Number is Denied

If the status is **Denied**, the serial number may already be registered to a different system ID. Contact the Equitrac Customer Support Center to resolve this problem.

### When the License is Successful

After successfully licensing Xerox Secure Access, go to [Verifying the Server Installation](#) on page 16 to complete the local install, or proceed to [Installing DRE](#) on page 15 to continue installing the remaining server components for a remote install.

### Note

After applying the full license(s), the 45-day default license is automatically overwritten and removed from the system.

## Installing DRE

You can install a single Print Server (DRE) or multiple print servers to distribute the load across servers.

To install a DRE, follow the instructions provided in [Microsoft SQL Server Configuration](#) on page 7. Install only the Document Routing Engine component and the System Manager Administrative Tool from the Select Features screen. Perform these steps for each DRE you install.

## Installing DCE

You can install a single Document Control Engine (DCE) or multiple engines to manage the communication load from control terminal devices.

To install a DCE, follow the instructions provided in [Microsoft SQL Server Configuration](#) on page 7. Install only the Device Control Engine component from the Select Features screen. Perform these steps for each DCE you install. The DCE sub-features Device Web Service and Smart Card Reader support must reside on the DCE machine.

# Verifying the Server Installation

After the server components are installed, you need to verify the following:

1. The device is registered in System Manager.
2. Print transactions are recorded in the database.
3. The printer spool is setup correctly.

Once verification is successful, you can install additional components or begin initial configuration.

Device registration requires the use specialized ports for Xerox Secure Access. Each monitored device must use an Equitrac printer port. You can create Equitrac printer ports directly for new devices, or convert devices from standard TCP/IP ports into Equitrac ports. For new devices, see [Add a Printer on a TCP/IP Printer Port](#) on page 16 or [Add a Printer on an Equitrac Printer Port](#) on page 17. If new devices are created using TCP/IP ports, they must then be converted into Equitrac ports for Xerox Secure Access to track them. For existing devices, see [Convert a TCP/IP Port to Equitrac Port](#) on page 18. Converting from TCP/IP to Equitrac ports allows them to be quickly converted back to TCP/IP ports to determine if reported errors within the print environment are due to the Equitrac server or the normal print environment.

## Add a Printer on a TCP/IP Printer Port

### Note

The following procedures outline how to add a printer in a Windows environment. Xerox Secure Access also supports Unix print servers. For printer setup details, refer to the *Unix Print Server Guide*.

1. Using the standard Windows interface, open the **Add Printer** wizard.
2. Follow the prompts to **add a local printer** and create a new port.
3. Select **Standard TCP/IP Port** as the type of port you want to create and click **Next**.
4. Specify a **Printer name** or **IP Address**, and click **Next**.

The wizard supplies a Port name based on the printer name or IP address. If another naming convention is preferred, rename the port accordingly.

Ensure the **Query the printer and automatically select the driver to use** checkbox is not selected.

5. Specify the Manufacture and model to install the printer driver, and click **Next**.

### Note

If the device is part of a pull group, it must use the same drivers as all other devices in the pull group. You must select the model of the pull group driver, not the model of the device.

### Note

If the DRE is a 64-bit server you must remember to also load the 32-bit driver to the server.

6. Specify the version of the print driver to use, and click **Next**.
7. Enter the **Printer name**, and click **Next**. This is the name of the device that is displayed in System Manager.
8. Select to share or not to share the printer with others, and click **Next**. If sharing the printer, enter a Share name, and optionally provide a printer location and any comments.
9. Click the **Print a test page** button, and click **Finish** to close the Add Printer wizard.
10. Confirm that the test page printed successfully.

## Add a Printer on an Equitrac Printer Port

To create Equitrac printer ports for new devices, do the following:

1. Using the standard Windows interface, open the **Add Printer** wizard.
2. Follow the prompts to **Add a local printer** and **Create a new port**.
3. Select **Equitrac Port** as the type of port you want to create and click **Next**.
4. The Add Equitrac Printer Port wizard displays and you are prompted to ensure that the printer device is turned on, connected to the network, and properly configured. Click **Next** to continue.
5. Select **Physical printer** from the **Device Type** drop-down list.
6. Specify a **Printer name** or **IP Address**. The wizard supplies a Port name prefaced with "EQ\_" based on the printer name or IP address. If another naming convention is preferred, rename the port accordingly.
7. Click **Next** to continue with the port configuration options. The Port Configuration screen displays. The **Detected device information** displays automatically if the wizard is able to collect this data from the printer.
8. Select the **Use custom settings** option:
  - If you select **Raw port** communication, identify the TCP **Port** number, and specify if the port monitor should hold the connection open.
  - If you select **LPR**, specify the name of the print **Queue** on the physical device (e.g. PORT1).
  - If you select **Specific device**, select the appropriate **Manufacturer** and **Model** from the drop lists. The device uses the relevant default communications parameters based on these selections.
9. Click **Next** and specify the **Physical device name**. This is the name of the device that is displayed within Xerox Secure Access System Manager.
10. Review the details for this new port and device registration, and click **Finish** to close the Add Equitrac Printer Port wizard, or **Back** to change any of the settings.
11. Specify the Manufacture and model to install the printer driver, and click **Next**.

### Note

If the device is part of a pull group, it must use the same drivers as all other devices in the pull group. You must select the model of the pull group driver, not the model of the device. If the DRE is a 64-bit server you must also load the 32-bit driver to the server.

12. Specify the version of the print driver to use, and click **Next**.
13. Enter the **Printer name**, and click **Next**. This is the name of the device that is displayed in System Manager.
14. Select to share or not to share the printer with others, and click **Next**. If sharing the printer, enter a Share name, and optionally provide a printer location and any comments.
15. Click the **Print a test page** button, and click **Finish** to close the Add Printer wizard.
16. Confirm that the test page printed successfully.
17. Verify that the physical device and its corresponding printer port and print queue display in **System Manager > Devices**. See [Device Registry Confirmation](#) on page 21.

## Convert a TCP/IP Port to Equitrac Port

Use the Printer Configuration Wizard to convert from a TCP/IP port to Equitrac ports. Converting from TCP/IP to Equitrac ports allows them to be quickly converted back to TCP/IP ports if desired. The ability to convert back is helpful in the event that you need to determine if reported errors within the print environment are due to the Equitrac server or the normal print environment.

### Note

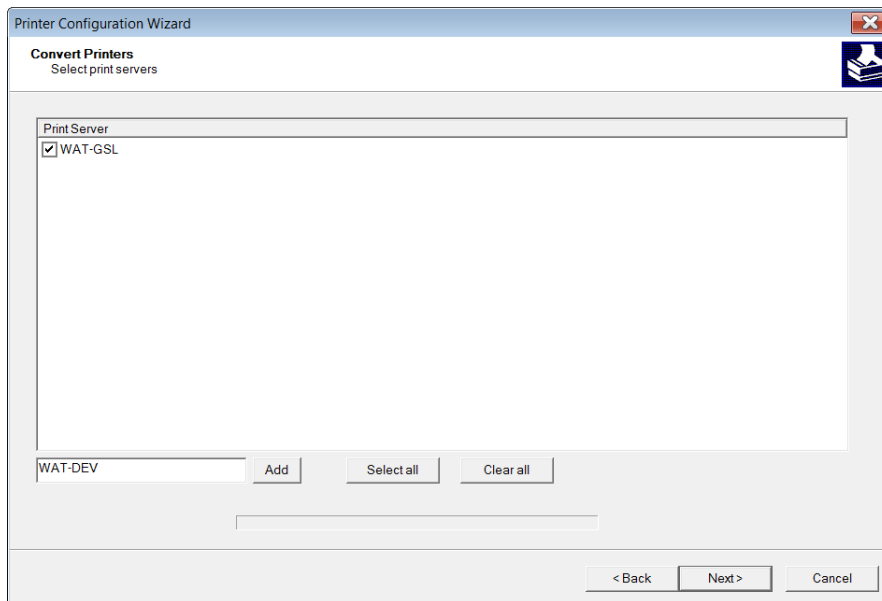
If you are working in a cluster environment, these instructions do not apply. See the *Cluster Deployment Guide* to set up Equitrac Ports for clusters.

To convert from TCP/IP printer ports to Equitrac ports, do the following:

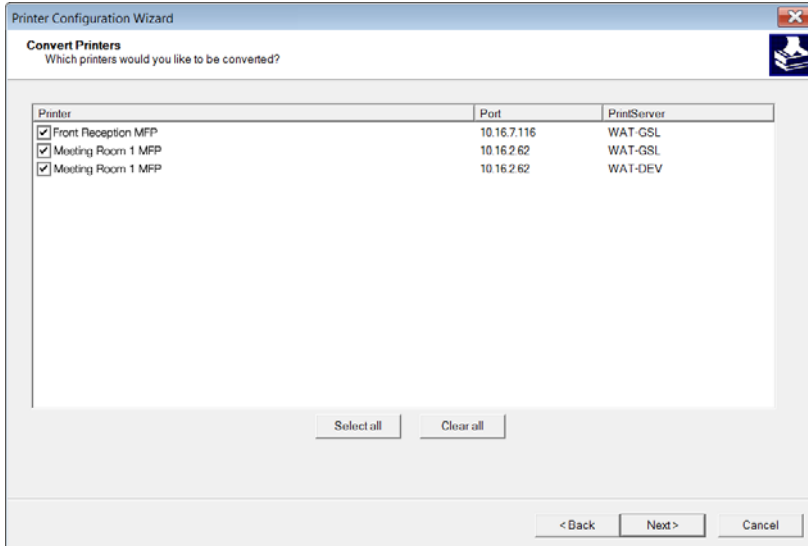
1. Select **Start > All Programs > Xerox Secure Access > Printer Configuration Wizard**.
2. Click **Next** on the Welcome screen to continue with the conversion.
3. Select **Convert printers to use Equitrac Ports**, and click **Next**.

Optional – Uncheck **Auto-discover model** if the printers are off-line or have SNMP disabled. If selected, the wizard sends an SNMP request to each device, and then times-out on each failed connection attempt, greatly increasing the time to run the conversion.

4. Select the desired print server(s) from the list, and click **Next**. Optionally, enter the name of other print servers in the Add field, and click the **Add** button to place them in the **PrintServer** list. Print servers can only be added one at a time.

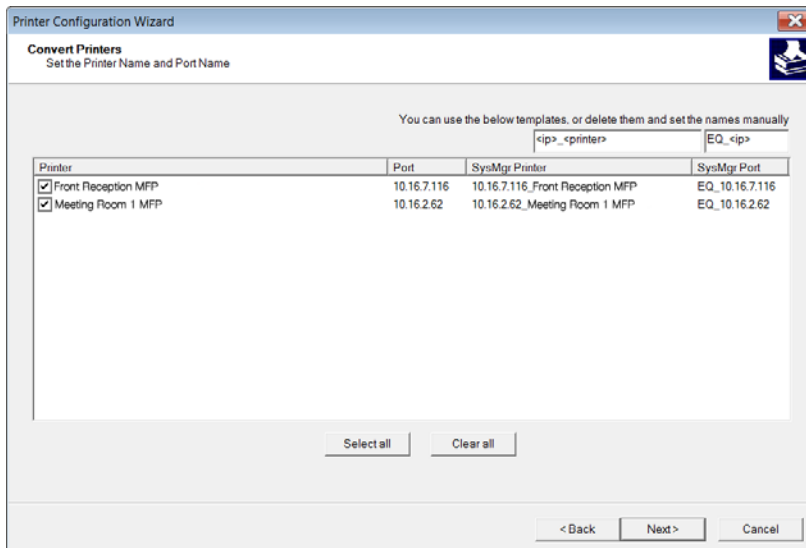


5. Select the printer(s) to be converted, and click **Next**. If a printer exists on more than one print server, it displays multiple times in the **Printer** list along with the name of its associated server in the **PrintServer** list.



6. Set the **Printer Name** and **Port Name** as they will display in the System Manager Devices view. You can use the default naming templates for the printer "**<ip>\_<printer>**" and port "**EQ\_<ip>**", or change the names as desired.

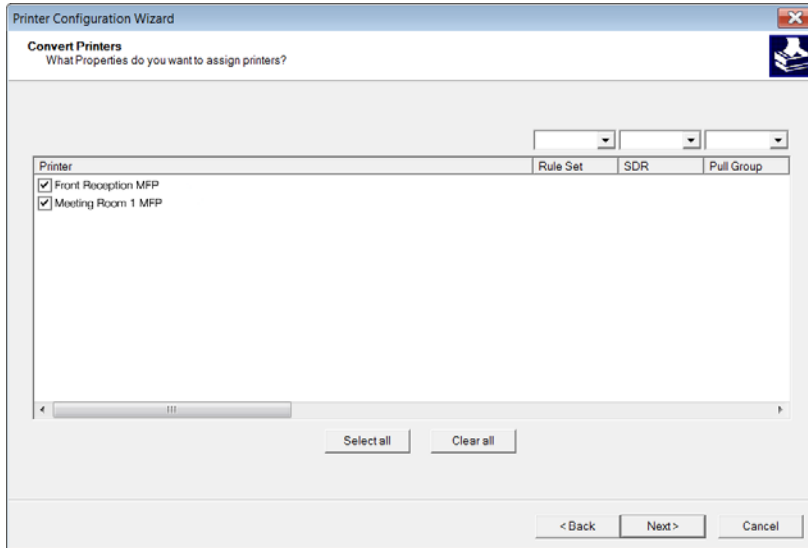
For example, you can change the printer default from "**<ip>\_<printer>**" to "**2nd floor <printer>**" to associate the selected printer(s) with the 2nd floor in your environment, or you can remove "**<printer>**" from the name to only display the printer's IP address in System Manager (where **<ip>** is typed, the printers IP will be automatically replaced; where **<printer>** is typed, the queue name will be automatically replaced).



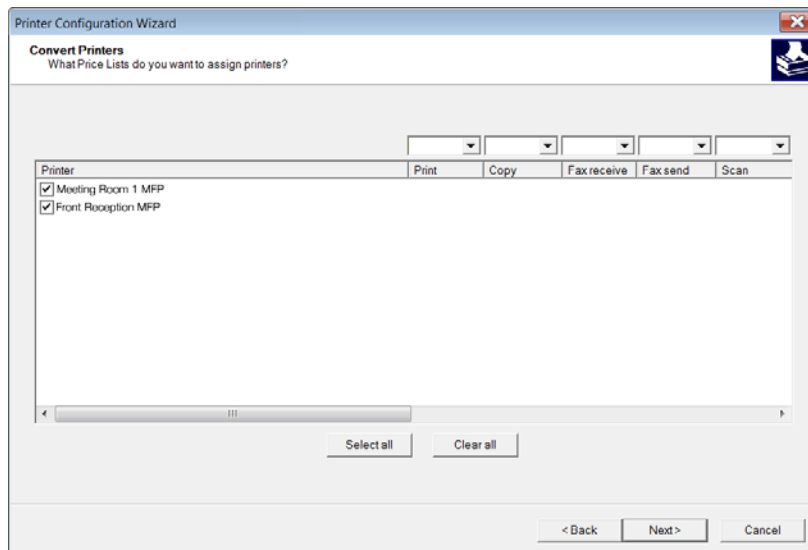
**Note**

The printer and port names can be changed individually or as a group. If multiple printers are selected, the naming convention affects the entire selection.

- On the **Properties** page, click **Next** to continue without selecting any values. The Rule Set, SDR and Pull Group drop-down lists will be empty when initially installing Xerox Secure Access, and will not be populated until they are configured in System Manager. See the *Xerox Secure Access Unified ID System® Administration Guide* to configure Equitrac printers.



- On the **Price Lists** page, click **Next** to continue without selecting any values. The Print, Copy, Fax receive, Fax send and Scan drop-down lists will be empty when initially installing Xerox Secure Access, and will not be populated until they are configured in System Manager. See the *Xerox Secure Access Unified ID System® Administration Guide* to configure Equitrac printers.



- Click **Finish** to complete the conversion process. Alternatively, you can select the **Return to Start** checkbox and click **Next** to return to the Wizard's main page without completing the conversion.
- Open the Printers and Faxes window, and print a test page for EACH converted printer.
- Confirm that the test page printed successfully.



12. Verify that the physical device and its corresponding printer port and print queue display in **System Manager > Devices**. See [Device Registry Confirmation](#) on page 21.

#### Note

The Printer Configuration Wizard also supports LPR Port Monitors, although the LPR Port Monitor option is not available by default in Windows. You can access this option in the Add Printer wizard.

## Device Registry Confirmation

After the printer ports have been set up, confirm that Xerox Secure Access is able to monitor the print queue of the new printer.

1. Start System Manager by selecting **Start > All Programs > Xerox Secure Access > System Manager**.
2. If necessary, select the local server and click **Connect**. The System Manager window displays.
3. Select the **Devices** link in the left pane. When you select the link, the application retrieves device information from any network devices configured with an Equitrac Port Monitor.
4. Verify that the right pane displays a physical device with the name you specified within the Add Equitrac Printer Port wizard. If the device is not listed, disregard the remaining steps in this procedure, and refer to [Installation Troubleshooting](#) on page 22.
5. In the right pane, select and expand the device to view the **port** and **print queue** for the device you just added.
6. Select the print queue to review default information such as pricing and device behavior. Xerox Secure Access is installed with default pricing of 0.01 per page.

## Spool Setting Verification

On each printer managed by DRE, confirm the following:

1. Open the **Printer properties** dialog box, and switch to the **Advanced** tab.
2. Verify that the **Spool print documents so program finishes printing faster** option is selected; and not the **Print directly to the printer** option.

By default, printers installed on Windows Servers 2008, 2008 R2, 2012 and 2012 R2 are set to **Spool print documents so program finishes printing faster > Start printing immediately**, and do not need to be changed. The **Start printing after last page is spooled** option can also be selected.

#### Caution

If the **Print directly to the printer** option is selected, a job may start printing before the job details can be sent from a workstation to DRE. In this case, DRE does not know to hold the job until data such as release key or billing code can be associated to the job, or to wait for a cost preview dialog box for users to accept or cancel the print job.

# Installation Troubleshooting

## If Device Does not Display in System Manager

Devices display in System Manager only when you add an Equitrac port to the device, or convert an existing port to an Equitrac Port. If a device is not displaying, try the following:

- Refresh the System Manager window often while adding new or converted devices. CAS requires about 30 seconds of time to update all required environment variables before populating System Manager with device information. If the System Manager devices view is open while adding new devices or converting ports, you may solve the problem with a simple refresh.
- For existing devices, convert the port. See [Convert a TCP/IP Port to Equitrac Port](#) on page 18.
- For new devices, add a standard TCP/IP port and then convert it, or add an Equitrac port directly. See [Add a Printer on a TCP/IP Printer Port](#) on page 16 or [Add a Printer on an Equitrac Printer Port](#) on page 17.

## If Licensing Fails

If licensing fails during Automatic Activation, ensure that the Accounting Server is available prior to activation. CAS controls licensing for all components, and if unavailable during activation, the activation fails. Components remain in an unlicensed state until CAS confirms a valid license.

After initial licensing, components cache their assigned license codes locally and use the cached information if the accounting server is unavailable. However, these temporary cached licenses will expire.

Ensure that you entered all serial numbers precisely. Remember that each component requires a separate license, unless you purchased a Suite license.

## If the Serial Number is Denied

If you apply a license and the Licenses view shows the status as “Denied”, the serial number may already be registered to a different system ID. Call the Customer Support Center to resolve this problem.

# 3

# Upgrade Xerox Secure Access

## Topics

[Planning the Upgrade](#)

[Upgrading from Xerox Secure Access 5.2 to 5.3](#)

[Upgrading from Xerox Secure Access to Equitrac Office® 5.3](#)

This chapter provides detailed instructions to upgrade to Xerox Secure Access 5.3 from a previous version, and how to upgrade from Xerox Secure Access to Equitrac Office® 5.3.

To migrate from PAS or PRS to Xerox Secure Access contact Technical Support Centre for information and requirements.

Refer to ReleaseNotes.pdf on the CD for potential important installation or upgrade information not contained in this document.

## Note

If you require assistance while upgrading, please contact the Technical Support Centre:  
Phone: 1.877.EQUITRAC (1.877.378.4872) or +1.519.885.2417 for calls outside of North America.

# Planning the Upgrade

When planning to upgrade Xerox Secure Access, there are different upgrade scenarios to consider:

- **Xerox Secure Access 5.2 to Xerox Secure Access 5.3** – This is a straight upgrade, and you do not need to uninstall the previous version of the product. This upgrade involves installing version 5.3 over version 5.2, and changing any selectable features as desired.
- **Xerox Secure Access 5.2 or 5.3 to Equitrac Office 5.3** – Upgrading to Equitrac Office is an option when more feature functionality is desired. This can be done by either removing the existing Xerox Secure Access 5.3 licenses and add Equitrac Office 5.3 licenses to the already installed Xerox Secure Access; or by uninstalling Xerox Secure Access (while keeping existing database and printer ports) and installing Equitrac Office.

Before upgrading Xerox Secure Access, gather the following information:

- A list of the Secure Access services installed on one or more machines. Possible components are:
  - Core Authentication Server (CAS)
  - Device Control Engine (DCE)
  - Document Routing Engine (DRE)
  - Secure Access Manager
- SQL Express instance name that was used for the Xerox Secure Access installation.
- The user name and password used to install Xerox Secure Access.

## Single Machine Upgrade

If you installed all Xerox Secure Access services on a single machine, you can run the Equitrac Installation Wizard once to upgrade all Equitrac services on that machine.

## Multiple Machine Upgrade

If you distributed the Xerox Secure Access services across multiple machines, you should follow a phased approach to upgrade the Equitrac services. Phasing allows you to upgrade different components at different times, which minimizes the copy interruption within your organization.

For example, if CAS and System Manager are on one machine, and DRE and DCE are on another machine, you should upgrade the CAS machine first, and then upgrade the DRE/DCE machine.

When updating the CAS machine, select only the CAS service from the install options. If you also installed the Xerox Secure Access System Manager on CAS, ensure that you install the Equitrac Administration Applications on the CAS machine.

When updating the DRE/DCE machine, select only the DRE and DCE services from the install options.

## Upgrading from Xerox Secure Access 5.2 to 5.3

This is a straight upgrade, and you do not need to uninstall the previous version of the product. This upgrade involves installing version 5.3 over version 5.2, changing any selectable features as desired. The existing Xerox Secure Access database is preserved, and any configured printer ports are maintained.

## Upgrading from Xerox Secure Access to Equitrac Office® 5.3

Upgrading to Equitrac Office is an option when more feature functionality is desired. This can be done in one of two ways: 1) Remove the existing Xerox Secure Access 5.3 licenses and add Equitrac Office 5.3 licenses to the already installed Xerox Secure Access; 2) Uninstall Xerox Secure Access (while keeping existing database and printer ports) and install Equitrac Office.

A license change upgrade from Xerox Secure Access 5.2 to Equitrac Office 5.3 cannot be done. You must first uninstall Xerox Secure Access, and then install Equitrac Office.

### License Upgrade

You can upgrade from Xerox Secure Access 5.3 to Equitrac Office 5.3 by changing software licenses. When the Xerox Secure Access license is used, only Xerox embedded devices are available to support authentication. Adding Equitrac Office licensing enables a full range of supported devices, and a more robust set of product features.

To perform a license upgrade from Xerox Secure Access 5.3 to Equitrac Office 5.3, do the following:

1. Select **System Manager > Licensing** in the left pane.
2. Right-click the Xerox Secure Access license, and select **Remove license** from the menu.
3. Refresh System Manager, and then click **Add** in the right pane to open the software activation wizard.
4. Follow the wizard prompts to add the Equitrac Office license(s).

### Full Product Upgrade

To perform a full product upgrade from Xerox Secure Access 5.2 or 5.3 to Equitrac Office 5.3, do the following:

1. From the Start menu, go to **Control Panel > Programs and Features**.
2. Select **Xerox Secure Access** from the installed programs list.
3. Click **Uninstall** and click **Yes** when prompted to remove the software.  
The uninstall process keeps the existing database and any configured Equitrac ports.
4. Obtain the Equitrac Office software and licenses, and then follow Equitrac Office Installation wizard prompts. See [Installing Equitrac Office 5.3](#) on page 4.

## Installing Equitrac Office 5.3

If you are installing Equitrac Office on a single machine, you only need to run the wizard once. If the Equitrac Office components are distributed across multiple machines, run the Installation Wizard on each machine, and select only those components that you want to install per machine.

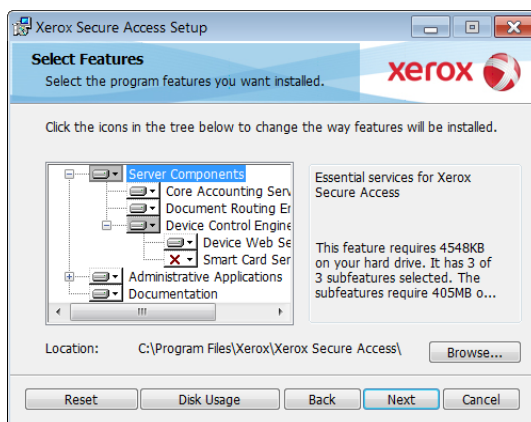
To install Equitrac Office, do the following:

1. Close all other applications on the server prior to running the Equitrac Office installation.
2. Obtain the Equitrac Office software file, product serial number and activation code from the Equitrac Product Download site.
3. Select and run the 64-bit Installer file (**Equitrac.Office.x64.msi**), or select and run the 32-bit Installer file (**Equitrac.Office.x86.msi**) to launch the Equitrac Office Installation wizard.
4. At the **Welcome** screen, click **Next** to begin the installation process.
5. Read and accept the terms of the **End-User License Agreement**, and click **Next** to continue.
6. On the **Select language** screen, select the language you want to display in the user interface, and click **Next**.

### **Caution**

You cannot change the display language after installation. To change the language, you must uninstall and reinstall Equitrac Office, setting the language during installation. The display language is independent of the regional language set on the machine. For example, Equitrac Office can display Italian even if the regional setting is French.

7. On the **Select Features** screen, choose the features you want to install. Click the **Next** button to continue.



By default, all Server Components (except the Scan Processing Engine) and all Administrative Applications are selected for installation. Deselect all options not required for the machine you are installing to. Any feature not selected by default can be installed during initial installation, or they can be installed afterwards.

### Note

To change the default installation folder for any of the program features, select the feature icon and then click the **Browse** button to open the *Change destination folder* dialog box. The top-level **Server Components** icon must be selected to change the location of the individual Server components.

8. On the **Service Log On Credentials** screen, enter the **Account** and **Password** of the user who will run the Windows services. Click the **Test Credentials** button to verify the user, and click **Next** to continue.

### Note

The **Account** field contains the account name in domain\username format. If you are using a SQL Express database that is not on a domain and you are using local accounts, you must enter computername\username. If neither domain or computer name prefix is specified, the user is handled as local user.

9. On the **Windows Firewall Exceptions** screen, select either a **manual** or **automatic** setup method for the firewall exceptions, and then click **Next** to continue.
10. On the **Database platform** screen, select **SQL Server**, and click **Next**.
11. On the **Database location** screen, select any available database server from the **Database Instance** drop-down list, and then click **Next**.
12. On the **Database Credentials** screen, select the authentication type of the selected SQL Server:
  - **Windows Authentication** (default selection): select this option when the user running the Windows Service account connects to the database server. This user was specified on the Service Log On Credentials screen.
  - **SQL Authentication**: enter the user credentials in the Login and Password fields, (this can be another Windows user or a SQL Server user). Click the **Test Connection** button to check the connection to the database with the selected user, then click **Next**.
13. If the specified SQL Express database (“eqcas”) already exists (e.g., in the case of an upgrade), the **Database Already Exists** screen appears. Select **Keep** the existing database, and click **Next**.
14. If any of the Web Client features are selected for installation, the **Web Client - Application Pool** screens appears. For more detailed setup information and prerequisites, see the *Equitrac Office and Express Installation Guide*.
15. Click **Install** to start the installation process.
16. At the end of the process, click **Finish** to exit the installation wizard and begin initial configuration.
17. Before running System Manager, start the EQCAS service.
18. Open System Manager and activate the Equitrac Office software license(s).

Refer to the *Equitrac Office and Express Installation Guide* for instructions to apply licensing and the *Equitrac Office and Express Administration Guide* for system configuration information.





# 4

# Uninstall Xerox Secure Access

## Topics

[Restoring Printers to Defaults](#)

[Restoring Printers to Defaults](#)

[Uninstalling Server Components](#)

To uninstall Xerox Secure Access, you must remove the server components from the appropriate machines.

This chapter provides uninstall instructions for the server components, and details on how to restore printers to defaults.

## Restoring Printers to Defaults

If you used the Printer Configuration Wizard at any time prior to uninstalling Xerox Secure Access, you must run the wizard again prior to uninstalling Xerox Secure Access to revert the printers back to their original ports.

If there are printers assigned to Equitrac® ports, then the uninstall process prompts you with a series of questions to determine how to proceed:

- If you choose to remove the Equitrac ports, the uninstall will convert existing printers to use the FILE: port. If you created Equitrac ports using the Equitrac Printer Configuration Utility, you can exit the uninstall and use the conversion utility to revert printers to their original ports. When finished, return to the uninstall to complete the process.
- If you choose to leave the Equitrac ports, any printers associated with those ports will not be functional unless you reinstall the port monitor. The uninstaller will restart the print spooler so the Equitrac ports do not appear in Explorer.

## Uninstalling Server Components

The uninstall automatically removes any Xerox Secure Access program files on the machine, including DRE, DCE, CAS and Administrative Applications. After you remove the server files, verify that the files have been removed, and clean the server registry. You must perform the uninstall on each machine that Xerox Secure Access is currently deployed on.

To uninstall Xerox Secure Access, do the following:

1. From the Start menu, go to **Control Panel > Programs and Features**.
2. Select **Xerox Secure Access** from the installed programs list.
3. Click **Uninstall** and click **Yes** when prompted to remove the software.

The uninstall process keeps the existing database and any configured Equitrac ports.

### Note

If you attempt to uninstall Xerox Secure Access from a single cluster node while the DRE or DCE cluster resources are assigned to Cluster Applications (groups), the uninstall fails. All DRE and DCE service resources assigned to cluster groups must be deleted before uninstalling Xerox Secure Access. Once the DRE and DCE resources are removed from the cluster groups, then Xerox Secure Access can be uninstalled from the single cluster node. However, the deleted DRE and DCE resources are now unavailable to all remaining nodes in the cluster even though those nodes may still have Xerox Secure Access installed on them. See the *Cluster Deployment Guide* for more details.



