



Kofax Equitrac Planning Guide

Version: 6.5.0

Date: 2024-04-17

KOFAX

© 2011– 2024 Tungsten Automation. All rights reserved.

Tungsten and Tungsten Automation are trademarks of Tungsten Automation Corporation, registered in the U.S. and/or other countries. All other trademarks are the property of their respective owners. No part of this publication may be reproduced, stored, or transmitted in any form without the prior written permission of Tungsten Automation.

Table of Contents

Overview.....	6
Benefits of Equitrac.....	6
Ensure document security.....	6
Reduce expenses.....	7
Improve workflow.....	7
Why plan for an Equitrac deployment?.....	8
ControlSuite integration.....	8
Virtual server support.....	9
Universal C Runtime prerequisite.....	9
Database requirements.....	10
System requirements.....	10
Components.....	11
Core server components.....	11
Core Accounting Server.....	11
Document Routing Engine.....	12
Device Control Engine.....	12
Scan Processing Engine.....	13
Device Monitoring Engine.....	13
Document Routing Client.....	14
Copy & print control mechanisms.....	14
Embedded devices.....	14
Establishing a secure print environment.....	15
Print-to-Me.....	15
Delegate printing.....	15
Send To Printing.....	15
Workstation Client support.....	16
I-Queue printing.....	16
I-Queue printing method.....	17
I-Queue Direct printing method.....	18
Managed Queues.....	18
Deployment Variables.....	20
Enterprise topology.....	20
Deploying Equitrac as part of ControlSuite.....	21
Network interconnection.....	21

- Single vs. multiple core accounting servers.....21
 - Network reliability and setup.....22
 - Ease of administration..... 22
 - Consolidated reporting..... 22
- Print server platform.....22
 - Windows print server..... 23
 - UNIX print server..... 23
 - Print server platform feature comparison chart.....23
- Print server calculation..... 23
- SPE and load balancing.....25
 - Scan load balancing with OCR calculation..... 26
- Client workstations..... 27
 - Deploying client software.....27
 - Client workstation caching..... 27
- Network bandwidth..... 27
- Network outage.....28
- CAS offline planning..... 28
- User Account Management..... 29
 - Creating user accounts..... 29
 - Preparing the user base for synchronization..... 31
 - Implementing PINs.....32
 - Multi-domain authentication.....32
- Security Considerations.....33
 - Establishing access permissions..... 33
 - Auditing..... 34
 - Database and messenger communication..... 35
 - Encryption.....35
 - Enabling SSL communication.....36
 - Securing print output.....36
 - Secure the DRE spool directories..... 37
 - Establish IP masking..... 37
 - Virus scanning setup..... 37
 - Server folders to exclude.....37
 - File extensions to exclude..... 38
- Backup and recovery..... 39
 - Database backups.....39
 - Print server configuration.....39
 - Recovery..... 39

Disaster recovery through virtual computing.....40

Overview

Equitrac is a server-based print management and cost recovery solution which measures, monitors, and manages document output on your network. Equitrac controls access to printers, copiers, scanners, and multi-function devices, and manages cost allocation for the purpose of reporting, budgeting, and usage pattern analyses. The Equitrac print tracking and document accounting solution reduces print expenses, eliminates wasteful printing, deploys equipment for maximum efficiency, and even contributes to a better environment. Equitrac is designed to create a secure document output environment that helps your organization gather usage data to control costs and minimize waste.

Equitrac is an ideal solution for both small businesses with a few devices, and for large enterprises with multiple offices and thousands of devices. Equitrac is well suited for educational institutions by letting students, faculty and staff print what they need and when they need it, wherever they are located. The Equitrac solution controls student and staff access to networked output devices such as printers, copiers, scanners, and multi-function devices. The solution manages payment methods, tracks usage, and provides a secure document output environment across the entire campus. Equitrac provides vendor-neutral support for multiple print workflows, database types, and operating systems.

Benefits of Equitrac

Integrating Equitrac into your document output environment offers the following benefits to your organization:

Ensure document security

- Devices are accessible to authorized users only for all print/fax/copy/scan functionality.
- Secure print queues hold documents in a virtual queue until the user releases the documents via a control mechanism.
- The user is on-hand at the output device to retrieve their document as it is printed, ensuring privacy of document content.
- Each user can see only their own documents in the secure queue; other users documents are not visible.
- Provides a comprehensive audit trail of all document input and output activities, whether printing, copying or scanning.

Reduce expenses

- Reduce waste and uncollected prints.
- Set up rules to limit the type of printing each user is granted; control access to color devices.
- Establish least-cost routing rules to pro-actively route print jobs to the most appropriate output device, based on certain criteria such as the group membership of the originating user, the size and other attributes of the job.
- Silent print tracking to assess printer usage by user, or department.
- Secure print queues eliminate cases where jobs are sent to a printer and never retrieved and eliminates the need to print banner pages as a means to identify personal output.
- Analyze usage patterns to determine the correct purchasing solution to support user needs.
- Establish a color quota system to set allowable limits for color output on a per-user basis.
- Measure cost savings via a Savings Report which details how much money was saved by not releasing all jobs from the printer, or by forcing monochrome and duplex printing. Additionally this report details the environmental savings—such as the number of trees and amount of water saved, plus the volume of CO2 not released into the atmosphere.

Improve workflow

- Allow the user to pull their job to a specific output device (Print-to-Me).
- Configure Multi-server Print-to-Me to support retrieval of jobs securely queued on any print server in the organization without imposing heavy network traffic; enables users to release their print job on any printer within the organization, regardless of where it was originally destined, enhancing the print workflow throughout the enterprise.
- Use DME-based routing to eliminate user frustration – and reduce IT helpdesk calls – when devices go offline due to paper jams, low toner, or insufficient paper. Automatic routing allows users to (be informed where to) get their jobs quickly from an alternate printer without impeding their workflow.
- Users can preview their print job attributes (including cost, number of pages and more) before they release a job to a printer.
- Single sign-on delivers non-repudiation for the scan to e-mail function of certain supported MFPs and operates in conjunction with certain scan and fax server providers to personalize workflows.
- Use the Send To printing feature to let authorized users distribute print jobs to another user or a distribution list. The distributed print job is held in a secure print queue on the server, and can be released by the recipient. For example, the HR department may send pay slips to employees. Or a teacher may send a workbook to all students in its class and choose to accept or pass on the costs.
- Assign a user to act as a delegate to release another user's print jobs. For example, an assistant can be assigned to a manager's account, thus allowing the manager to send a job for printing, and the assistant (delegate) can then release the job via Print-to-Me for the manager.
- Use the Equitrac Capture & Send feature for select manufacturer devices to allow users to quickly and easily send scanned documents to email, fax, network folders or Microsoft SharePoint.

Why plan for an Equitrac deployment?

Kofax Equitrac is a highly customizable solution that can help your organization reduce costs and improve efficiencies related to document output. As with any software solution, there are many different installation and configuration variables that can affect how you deploy, license, and use the product.

Creating a deployment plan is essential for a scalable, well-executed Equitrac installation. This guide will help you plan:

- the features and components you will license
- the physical installation location (topology) of the Equitrac services across servers
- the number of print servers you need
- the environment variables that will affect product configuration
- security requirements strategies for integrating and maintaining user accounts

This guide does not provide a comprehensive requirements checklist. Instead, this guide examines the variables you should consider before you install the product. Use this guide to select the appropriate combination of variables to support the needs of your organization.

While this guide provides summary information and general details that will affect the installation plan, it does not provide specific configuration details. This guide is intended to help customers design and plan an Equitrac deployment strategy. It can also assist Network Administrators and IT personnel who are responsible for specific installation and configuration tasks.

This guide provides information to help determine deployment variables such as, the number of Core Accounting Servers (CAS) needed, the amount of network bandwidth required, the number of dedicated print servers, and how many Scan Processing Engines (SPE) are needed for scan load balancing with OCR processing.

Some sections this guide assume substantial knowledge of networking, database management, and print servers. If you do not possess skills and knowledge comparable with an MCSE designation, consult an MCSE regarding your deployment plan prior to performing the installation.

ControlSuite integration

Equitrac can be installed as a standalone product or as part of the ControlSuite integrated print and output management, capture and mobile document workflow solution, which also includes AutoStore, Output Manager and Business Connect. Regardless of the how Equitrac is deployed, all products require that the ControlSuite core components are installed and configured in order to utilize the shared services.

ControlSuite combines individual components that work together in various configurations to create multiple document processing workflows. ControlSuite manages the secure document distribution and information collection process. It features document security and document workflow automation; including scanning and archiving, document routing, print management and document print stream transformation technology.

Deployments that included Equitrac and Output Manager may have documents received by both systems for a given user. All of a user's documents (both Equitrac and Output Manager jobs) are displayed in a unified job list and can be released at any Equitrac endpoint client. Print preferences and finishing options of Output Manager jobs are passed to Equitrac for release via the Print Job Management Service.

Equitrac has print rules to send documents and their associated metadata to AutoStore or Output Manager. Equitrac routes all documents to AutoStore, where a copy of each document is sent to an offsite archival application. AutoStore then reroutes the remaining copy of the document to Equitrac for Print-to-Me release. Equitrac securely sends context sensitive printed documents to Output Manager where it runs a custom script to flag any document containing sensitive information. Documents that pass this inspection can be released from Equitrac endpoints.

AutoStore administrators can configure an AutoStore route component to send a document and all associated metadata to Equitrac. Equitrac then routes that document through print rules like any other document received by the system. Users can release those documents for secure print from their Print-to-Me queue.

Business Connect allows users to submit documents directly from their mobile devices, then to walk to an Equitrac endpoint to release them. After submitting the print job, the user walks to a printer, authenticates within the Business Connect application, and then scans the QR code on the printer. Users can select documents from the list of print jobs and release the job at an Equitrac endpoint. If installations included both Equitrac and Output Manager, all jobs are displayed in a unified job list and can be released at any Equitrac endpoint client through the Business Connect app.

Please refer to the [Kofax ControlSuite Webhelp](#) for deployment options.

Virtual server support

Equitrac is fully supported on all hardware platforms compatible with Windows Server 2012 R2, 2016, 2019 and 2022. The use of Equitrac under virtual environments such as Virtual Server or VMWare is generally supported and is expected to work correctly, as long as such environments fully support the server operating system, as Equitrac 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 Equitrac solution. If adequate resources are not defined or available there can be an impact on performance. Consult your account representative for details.

Universal C Runtime prerequisite

Equitrac 6.4 Server and Client installations use Windows 10 Universal CRT for Visual Studio 2015. Universal CRT is a Windows OS component that enables C Run-time Library (CRT) functionality on Windows operating systems and must be installed prior to installing Equitrac on a non-Windows 10 OS (such as Server 2012 R2). Server 2016, 2019 and 2022 do not require CRT to be installed.

The installer checks if the Universal CRT is installed, and if it is not found, an error message pops up, and the installation stops. The error message displays the URL to where the Universal CRT can be downloaded from.

Go to <https://support.microsoft.com/en-us/kb/2999226> and follow the instructions for installing the Universal C Runtime package.

Database requirements

All Equitrac installations require at least one Core Accounting Server (CAS) that connects to a SQL Server database. Two-way trust is required when the CAS and database servers are on different domains. The SQL Server database can be on a separate domain from the CAS server, however, two-way communication between domains is required in order for information to be added to the database (e.g. users, departments, billing codes), and for reporting purposes.

Microsoft indicates that the maximum size of a SQL 2012 Express Edition database is 10 GB. If you are deploying Equitrac to support a large number of users (>1000) and anticipate a large volume print and copy jobs (>10 million pages per year) considering implementing a Microsoft SQL Server database only.


System requirements

Before installing Equitrac ensure that the client and server machines you plan to use meet the minimum operating requirements. To maximize performance in high-volume print environments, you may require additional disk space and memory, and a faster processor.

32-bit server components are not supported in Equitrac version 6.x. CAS, DRE, DCE, DME, SPE, Administrative applications, Auxiliary applications and Web System Manager are only available in 64-bit. Workstation Client are available in both 32-bit and 64-bit installers.

A direct upgrade from an earlier version of Equitrac running 32-bit server components to version 6.x running 64-bit cannot be done. If you currently have any 32-bit server components installed on a 64-bit system, you must remove them and then re-install the 64-bit components.

.Net Framework package 4.5 must be installed on Windows 8.1 and 10 prior to installing the Windows Client.

 The system operating requirements are updated regularly. Please refer to the latest [Equitrac Requirements](#) for the most up-to-date information.

Components

Core server components

Equitrac is comprised of a set of core services that reside on one or more network servers. Each component communicates with the other services on a designated port.

- The **Core Accounting Server (CAS)** communicates with the central database containing all Equitrac accounts, transaction tracking and device information. Considered the central core of all print and copy tracking activity, CAS handles user authentication requests and tracks activity forwarded by DRE and DCE.
- The **Document Routing Engine (DRE)** tracks print jobs originating from network printers.
- The **Device Control Engine (DCE)** manages and tracks walk-up secure document release, copy, scan, and fax jobs.
- The **Device Monitoring Engine (DME)** is an optional service that continually monitors the status of MFPs, print, or copy devices to proactively alert Administrators of potential problems.
- The **Scan Processing Engine (SPE)** is an optional service required to run the Equitrac scanning features.

Core Accounting Server

The Core Accounting Server (CAS) verifies users, calculates transaction charges, and assigns those charges to an appropriate user or group account. CAS calculates charges using page count and job attribute information received from DRE, along with printer costs defined by the administrator.

CAS primarily handles user authentication requests for network print jobs (forwarded by DRE) and for copy/scan/fax jobs (forwarded by DCE). The CAS server is the only component with access to the database. All other component/services must communicate with the CAS server to send data to or receive data from the database.

Every Equitrac installation requires a pre-installed database. CAS uses the database instance to create an accounts database that contains all printer, user, department, billing code, transaction, and balance information. The database can reside on the same machine as CAS, or on a separate server if needed.

Document Routing Engine

The Document Routing Engine (DRE) is the print server. If you plan to enable document flow from user workstations to networked output devices and capture the document characteristics of all output, you need to implement one or more DRE print servers. DRE integrates with the print server, and manages all communication with physical printing devices. Each time a user releases a print job, DRE communicates the job characteristics to CAS.

For installations that require secure document printing, you can configure DRE to hold documents in a print queue until the user releases them from a printer. See [Establishing a secure print environment](#) for details.

The following diagram shows a typical DRE workflow. First, a user generates a print request. DRE intercepts the request before it gets to the printer and “holds” the print job while it waits for a user validation response from CAS. CAS checks its database and either validates the user, or denies the request. The response is sent back to DRE, and the print job is forwarded to the printer if the user was validated. If denied, the user receives a notification message on their desktop (if configured). After the job is printed, the page count and job attributes are forwarded to the CAS database for tracking.

Although DRE is a core component, it is not required in all deployments. DRE manages communications with physical printing devices. If you are only tracking photocopy transaction on devices with embedded devices (rather than tracking printing), you do not need to install the DRE component.

The number of DREs you require depends upon the number of devices you need to control, and the anticipated print volume. See [Print server platform](#) for details.

Device Control Engine

The Device Control Engine (DCE) provides communication with copy, scan, and fax devices and with multi-function devices that provide scan and fax features. If you plan to control access to copy, scan, and fax functionality, you require at least one DCE. DCE communicates with control mechanisms such as Equitrac embedded software, to authorize access to and track document output on devices that provide copy, fax and scan features.

DCE communicates with CAS to verify user credentials, and forwards the copy, scan, fax information generated by these devices for tracking in the accounting database.

The following diagram shows a basic DCE workflow. First, a user requests access to an MFP, and then DCE forwards a user validation request to CAS. CAS checks its database and either validates the request, or denies it. After the user completes their photocopy, fax, or scan, the job attributes are forwarded to CAS for tracking.

Although DCE is a core component, it is not required in all deployments. If you intend to track printing from workstations only, and do not need to track photocopy, scan, or fax jobs, you do not need to install the DCE component. Instead, you need the DRE component only.

The number of DCEs you require depends upon the number of devices you need to control, and the number of transactions per day that you anticipate.

Device Web Server

The Device Web Server (DWS) is an optional feature of DCE, and is required to manage and control embedded applications on web-based MFPs. When a user logs in at a web based device, the login data is sent to DWS, which communicates with DCE, and then DCE contacts CAS to verify the user credentials, and forwards the information generated by these devices for tracking in the accounting database. Currently, DWS and DCE must reside on the same server. DWS is only for 64-bit systems.

Device Control Server

The Device Control Server (DCS) is a feature of DCE, and is required to manage and control Ethernet card readers. DCS is also required to communicate with DWS in order to work with some web-based MFPs. DCS is only for 64-bit systems.

Scan Processing Engine

The Scan Processing Engine (SPE) is responsible for managing and controlling the scan features once authentication has taken place. When a scan request is received by DCE, all information relevant to the request is passed to SPE to process. SPE then sends the scans to the appropriate scan destination, and sends the scan information to CAS for costing and reporting.

An SPE requires at least one DCE to operate, and multiple SPEs can be deployed per DCE to manage the scan load requirements. Scanning requirements for organizations differ based upon the amount of scanning performed, and how much OCR processing is used during the scanning process. If minimal scanning or OCR processing is used, then SPE can be installed on the same server as other Equitrac Core Components. Typically, a separate SPE server option is selected only if OCR processing is used. See [SPE and load balancing](#) for deployment options.

SPE is required for Equitrac's Scan-to-Me and Capture and Send workflows. Scan-to-Me allows users to scan a document and email it to their own address, and optionally to other addresses via the CC field (if enabled).

Capture and Send uses SPE to scan documents to a particular URL on the Internet via SharePoint, a telephone fax number via RightFax, network folders on your local area network, and email through your server. In the case of SharePoint and RightFax, there must be as many SharePoint or RightFax destinations as there are SharePoint or RightFax servers (one destination per server).

Device Monitoring Engine

The Device Monitoring Engine (DME) is an optional component that monitors physical device status and faults. Installed on a server station, DME monitors selected devices for SNMP status changes and logs the status changes. You can view the current status of any monitored device in the Device Monitoring Console. If you want to monitor a device for a particular type of fault (e.g. offline status or paper jams), you can create Alert Rules that send notifications when the fault occurs.

IT Managers can run standard or custom device status reports to pro-actively identify devices requiring service or replacement. These reports track the historical status of a device over time, allowing you to understand the performance history of the device.

Document Routing Client

The Document Routing Client (DRC) is a component of the Equitrac workstation client which provides DRE printing behavior for sites that prefer to print via direct IP printing instead of to a print server. A physical device appears in System Manager the first time a workstation prints using DRC. As other DRC clients print to the same printer, additional ports and queues associated with each workstation name appear under the same physical device. This is repeated for each printer accessed by a DRC client. Reporting is the same as if they had printed to DRE printers.

DRC has all the same capabilities as DRE, such as tracking, rule sets, and secure document release. DRC supports the same workstation popup features as DRE (e.g. billing code, cost preview, interactive rules).

DRC is part of I-Queue Printing solution. There are no print servers involved with DRC I-Queue Printing, resulting in reduced network traffic and lower hardware cost and setup. Although similar to standard direct IP printing in its capabilities, the main difference is that I-Queue printing utilizes the I-Queue printer which is auto-created on the client workstation when DRC is installed.

The I-Queue printing solution eliminates the need for the user to select the appropriate printer for their print jobs, but rather allows the users to send their print requests to the I-Queue printer, and then release their jobs through any available Equitrac configured MFP through secure document release.

Copy & print control mechanisms

There are several ways to track copies and network print jobs when using Equitrac. The following section outlines each method and describes the benefits to consider when selecting one method or combining methods.

Embedded devices

Embedded devices are manufacturer-specific software bridges that eliminate the need for a central print server, since the MFP devices themselves track and report activity. Embedded devices handle the transfer of user authentication and transaction details between these devices and your accounting server database. Embedded solutions offer streamlined workflow for the user because the interface is accessed via the familiar device panel, eliminating the need for an external keyboard.

Equitrac has developed embedded solutions to support select devices. With embedded functionality installed, these devices prompt users for valid user and account ID information for walk-up copy, scan, and fax jobs. Users can also release jobs from secure print queues directly from the MFP front panel.

Establishing a secure print environment

In environments where users print proprietary or confidential documents, secure printing gives users the power to control the timing of their output. Equitrac hold documents sent to registered devices in DRC and DRE's secure print queue. Through a client application or control terminal, users can view documents in the queue, then select, delete, or release documents for printing.

Depending on the needs of your organization, you can set up basic secure printing only or extend the functionality to use Print-to-Me and/or Send To printing. In a basic setup (illustrated in the diagram below), the print job is held in a secure queue until released to the destination printer. Secure printing prevents private or sensitive materials from sitting unattended and unclaimed at remote printers.

In an advanced Print-to-Me setup, the user can choose a different destination printer—they do not have to release the job to the printer originally selected at the user workstation. In a Send To printing setup, the user can release a job to the secure queue on behalf of other users, and the print job appears in the secure queue for each user selected.

Print-to-Me

Print-to-Me extends the basic secure printing setup by allowing users to release print jobs to compatible printers from any control terminal. The administrator creates custom pull groups, which are logical groups of printers that share output capabilities. When a user submits a print job to a printer within a pull group, the job is held in a secure print queue. The user can walk to a control terminal, authenticate, then select any printer within the pull group to produce the job. If your organization is spread across multiple buildings, Print-to-Me offers the flexibility to release documents at networked devices whenever convenient, and ultimately improves productivity because users can avoid out-of-service printers, or submitting jobs to a busy printer.

Equitrac also offers multi-server Print-to-Me, which allows users direct print jobs across print servers.


Delegate printing

In Delegate printing, users can be assigned to act as a delegate to release another user's print jobs. For example, an assistant needs to release a manager's print jobs from a device, therefore the assistant is assigned to the manager's account as a delegate. The manager (delegator) sends a job for printing, and the assistant (delegate user) logs in to the device with their user credentials to release the job via Print-to-Me. The delegate is presented with a list of their documents, followed by a list of the delegator's documents. The jobs released by the delegate are charged to the delegator's account. A delegator may have multiple delegates, and a delegate may be assigned to multiple delegators.

Send To Printing

In a Send To printing setup, the user can submit a job to the secure queue on behalf of other users, and the print job appears in the secure queue for each user selected. The user who submits the


print job (called the originating user), can select any combination of User Accounts, Departments, or Windows Active Directory Groups as the recipients. Alternatively, in Equitrac, the user can set an identifier (called a release key) for the job that must be entered before the job can be released from the secure queue. The originating user can also assign charges or accept costs for the print job.

 Send To printing is not supported in Mac environments.

Workstation Client support

The Workstation Client provides four distinct features: Client Billing, Desktop Printing, Cost Preview, and User Authentication. These features provide job information or prompts to the user when they request a print job from a networked workstation.

- **Client Billing** prompts users to assign billing codes when they print their documents.
- **Desktop Printing** tracks print jobs sent to a locally-connected printer. Desktop Printing records user ID, page count, document title, and workstation information. Desktop Printing supports simple pricing on a per-page basis, and advanced price lists tracking, but does not enforce account limits. Charging for color attributes is also possible but depends on the properties of the printing application and the printer driver. Desktop Printing does not support charging for attributes such as duplexing or page size. Desktop Printing is not supported on Mac workstations.
- **Cost Preview** provides a summary of the print request cost prior to sending the job to the printer and prior to recording the transaction in CAS. Users can accept or cancel transactions before printing. Cost preview only works with DRE- and DRC-based print tracking (printers tracked via Desktop Printing do not display the cost preview popup).
- **User Authentication** displays a prompt for Windows login credentials any time a user tries to print to a device monitored by Equitrac. Users must enter a valid windows username and password to complete the print request.
- **Workstation direct IP printing (DRC)** enables Print-to-Me and provides print tracking on par with DRE server-based print tracking. This is for direct IP printing only.
- **Interactive Print Rules** enables users to interact with rules providing multiple options. This does not apply to desktop printing rules or copy rules.

 Desktop Printing, Message Client and Interactive Print Rules are not supported on Mac clients. Although Equitrac Message Client is not supported for Mac users, the Mac Client has its own message popup capability. The Mac popup will display Equitrac messages except those generated by Interactive Print Rules.

I-Queue printing

The I-Queue Printing feature is a cost-effective solution for network printing by reducing the need for system administrators to setup and configure multiple MFPs for users to print to from their workstations.

I-Queue printing utilizes the I-Queue printer which is accessible through the user workstation, eliminating the need for the user to select the appropriate printer for their print jobs, but rather allows the users to send their print requests to the I-Queue printer, and then release their jobs through any available Equitrac configured MFP or SFP through secure document release.

I-Queue provides a single print queue for every user and every printer. When submitting a print job, the I-Queue can be setup to use one or both of the following printing modes:

- Secure printing via a single Print-to-Me queue where all printers are combined into a single pull group. The I-Queue holds print jobs sent to the I-Queue printer from a user workstation. The I-Queue method only supports secure printing and holds print jobs until the user releases them at a networked printer via Print-to-Me.
- Direct printing via the I-Queue Direct printer enables printing directly to a printer (without printer driver installation and authentication or a Print-to-Me queue) in a simple and straightforward method.

There are no pull group restrictions when using the I-Queue print option. Rules and price lists can be applied to the I-Queue for all associated print jobs.

I-Queue printing method

The I-Queue printer is auto-created on the DRE print server when the I-Queue feature is installed, or on a client workstation when the DRC feature is installed. The I-Queue printer uses the I-Queue Printer Port and Universal Print Driver and appears in the Windows built-in printer list. After I-Queue printing has been enabled on the server, the user can print to the I-Queue printer on their workstation and release their jobs at any system-configured printer.

1. The user prints to the I-Queue printer on their workstation. They do not have to select a destination printer.
2. The user authenticates at any system-configured printer on the network and releases their documents via Print-to-Me. The job is held in the I-Queue until it is released. The user has the option to force monochrome or force duplex at the printer before releasing their documents.
3. The DCE acquires DREs and DRCs that are holding jobs for that user and instructs each of them to release the appropriate documents. They are found through the use of SLP.
4. The DRE/DRC requests driver details from the CAS and downloads the appropriate driver package from the Equitrac Driver Repository and installs it locally. The drivers are installed only at first print. The printer information and queue is cached, and all subsequent prints are released without installing a new print driver.
5. The document is rendered and sent directly to the printer.
6. The user then collects their print jobs and logs out of the printer.


i A driver package for each client workstation OS should be set up in the Equitrac Driver Repository, OR ensure that the Windows image has an appropriate driver installed. If the driver cannot be found, the user will get a printout stating that there is no print driver and the job fails to print. If they select Print & Save, the job re-spools and job would be duplicated.

I-Queue Direct printing method

I-Queue Direct enables the user to print directly to a printer (without driver installation and authentication, or Print-to-Me at a printer) in a simple and straightforward method.

The I-Queue Direct printer is created on a client workstation when the DRC I-Queue feature is installed. The I-Queue printer uses the I-Queue Printer Port and Universal Print Driver and appears in the Windows built-in printer list after a DRC cache update (either manual or automatic). After I-Queue Direct printing has been enabled on the server, the user can print straight to the I-Queue Direct printer from their workstation without authentication.

1. The user prints to the I-Queue Direct printer on their workstation.
2. The I-Queue Direct Printers pop-up window appears with a list of printers configured for I-Queue printing with associated I-Queue Port in System Manager.

 The user's recently used printers are displayed first in the list. This way they can quickly select the desired printer the next time they print.

3. The document is released immediately at the selected printer.

Managed Queues

The Managed Queue is a printing mode that enables users to print to a queue using a vendor specific printer driver. The Managed Queue is a workstation print queue which is configured and deployed through the Workstation client and managed via System Manager. The print queue with the selected printer driver is automatically installed and updated on workstation computers. Print jobs are submitted to one print queue and then released on any MFP assigned to the Managed Queue.

Managed Queues utilize the vendor specific printer driver and allow all print driver functionality to be available to the user. The workstation client automatically creates the print queue (as configured in System Manager) and installs and updates the vendor printer driver on the workstation client. The Managed Queue settings are updated on the workstation computers at normal synchronization periods (as configured in System Manager) Optionally, you can force a synchronization to roll out immediate updates.

Administrators can setup an environment with similar devices using one common printer driver. This allows for one common queue to be automatically installed on all workstation computers without any further configuration. Additional Managed Queues can be setup for different groups of devices using different printer drivers. This functionality simplifies the deployment of print queues to workstations and allows the use of standard print queues to be easily maintained in the environment. Pull groups are used to filter which MFP can release the jobs sent to a Managed Queue. Pull groups can be set for a Managed Queue and print jobs can be released on any MFP within the pull groups assigned to the Managed Queue. Pull groups are needed as print jobs from one vendor may not be compatible with other vendor's devices, and care should be used in selecting which print drivers to use.

A Managed Queue print queue appears in the list of printers on workstation computers when the DRC Managed Queue feature is installed via the client installer, and the Managed Queue driver assignment for the supported workstation OS/platform is configured on the server. If the Managed Queue does not have valid driver assignment for the target OS, the print queue is not created on the workstation computer. For example, if the workstation OS is Windows 10 64-bit, then the matching print driver version must be assigned in System Manager for the Windows 10 64-bit OS.

Deployment Variables

How you deploy Equitrac depends upon the specific needs of your site.

- Will you need a single Core Accounting Server?
- Will you need multiple Document Routing Engines?
- Do you need to manage only a small number of users operating within a LAN, or do you have a large number of users spread across multiple sites and operating on a WAN?
- Can you rely upon your network to provide a constant connection to CAS?

This chapter provides information on the variables that can affect how you deploy Equitrac, and how you can adjust the configuration to suit your specific needs. Not all of these variables may apply to your site, however, read this section in its entirety to ensure that you understand all of the factors that must be addressed—or ruled out—before you create your deployment plan.

Enterprise topology

Physical geography primarily determines how you will deploy the Equitrac services. Your deployment can be a single office or campus (LAN) or Corporate office with remote offices or a central campus (WAN)

A single office or campus offers the simplest deployment possibilities. If supporting a relatively small number of users and transactions, you can install all Equitrac services on a single server. If your user base and anticipated number of transactions is very large, also read [Single vs. multiple core accounting servers](#).

A corporate office with remote offices or a central campus operating across a Wide Area Network (WAN) poses a slightly more complicated deployment. To ensure availability of each CAS server to accommodate user authentication requests originating from within the LAN, you may need to install one CAS on each branch of your WAN (one per LAN). However, there are a number of factors to consider before determining the most effective CAS deployment for your site. For complete details on determining the number of CAS servers you will need, see [Single vs. multiple core accounting servers](#).

When deploying across a WAN, it is important to keep the Document Routing Engine (DRE), the Document Control Engine (DCE), and the Device Management Engine (DME) locally within the same network branch to keep the intra-server communication local and thereby optimize performance. See [Network interconnection](#) for further information about Equitrac component deployment.

Deploying Equitrac as part of ControlSuite

If you are considering deploying Equitrac as part of ControlSuite, it is best practice to install Equitrac, AutoStore and Output Manager on their own servers. Business Connect can be installed on the same server as any of the ControlSuite products.

There are many ControlSuite deployment options and the individual components can work together in various configurations to create multiple document processing workflows. Please refer to the [ControlSuite Installation Help](#) file to installation and configurations options to suite your deployment needs.

Network interconnection

Careful consideration should be given to the location of the servers used for the DRE and DCE components on the network. In general, these rules apply:

Install DCE on the same server as CAS only if the following criteria are met:

- The WAN/LAN is slow or unreliable
- DCE will control 150 terminals or less
- CAS is on the same side of the switch/router as the control terminals and output devices

The DCE server should always be placed locally to the output devices it controls. Each time a user authenticates, or job details are uploaded from a terminal to the CAS database, the request is intercepted and handled by DCE. DCE then communicates with CAS on a private port to forward job attributes for inclusion in the database. Direct communication from DCE to the controlled devices maximizes performance.

If deploying within a single LAN, consider deploying DREs and DCEs according to department. Identify similar usage groups and then segment them from one another so you do not disrupt network traffic flow.

i DME is an optional component that can be installed on any server but is most often deployed on the same server as DRE. In the event that there is no DRE in the system, DME is most often on the CAS server.

Single vs. multiple core accounting servers

This section presents a number of factors to consider when determining the number of CAS servers that would best serve the needs of your site.

Network reliability and setup

It is very important to understand that user authentication requests usually require a connection to CAS before the user is allowed to proceed with their print or copy/scan/fax job (the exception is when offline caching is enabled – see [Network bandwidth](#)). If the connection is impeded in any way (network traffic, network reliability, etc.), the user will be unable to proceed with their job until CAS can verify their login credentials. A reliable connection to the CAS server is important when deciding on a single or multiple CAS server setup.

In deployments across sites, you should deploy a single CAS only in situations where you can guarantee network uptime, and can provide enough bandwidth for Equitrac at all times. If your WAN is unreliable or if you have limited bandwidth, you should install multiple CAS servers.

Ease of administration

Each CAS requires its own pre-installed database, and these databases are managed separately. Therefore, multiple CAS servers requires separate administration of devices, user accounts, and configuration. If you are managing completely separate user populations and the networks within each LAN are also managed separately, multiple accounting servers offers the ability to maintain each server independently.

Consolidated reporting

If you deploy more than one CAS, you will have two or more distinct databases. To generate consolidated reports and analyze system-wide print tracking or copy data, you must configure the Uplink feature to upload transaction data from slave CAS servers to a main server at a pre-set interval. When Uplink is configured, you can view transaction and account data reports from all CAS servers, or you can report on individual servers only. The Uplink feature operates independently of the WAN speed and will not inhibit the flow of network traffic. See [Run consolidated reports](#) in the [Kofax Equitrac Administration Help](#) file.

The following diagram illustrates a multiple server scenario. Each CAS requires its own unique database that you administer separately, including account, device, and pricing information. When the Uplink is configured, the data from the slave CAS is uploaded to the Master CAS. However, the data on each CAS is maintained separately, even when Uplink has occurred. The Uplink feature consolidates report generation, but not consolidate the databases themselves.

Print server platform

DREs can be installed on Windows or UNIX platforms. DRE should be deployed on a server that is local to the printers and clients it will control. This optimizes print traffic speed and handling. To calculate the number of DREs you need to implement, see [Print Server Calculation](#).

Windows print server

DRE installed on a Windows print server supports the following:

- Network print-tracking and charging
- Rules and routing
- Secure Document Release (SDR), including Print-to-Me
- PjL and Data Stream Interpreter Page Counting

UNIX print server

The Equitrac UNIX print server enables accounting on UNIX print servers by monitoring printing and reporting printer usage on the standard UNIX printing subsystem to an Equitrac accounting server.

Print server platform feature comparison chart

Feature	Windows	UNIX
Network print tracking and charging	Y	Y
Pop-up billing codes	Y	N
Email user notifications	Y	Y
Popup user notifications	Y	N
User authentication for Mac clients	Y	N
Secure document release	Y	Y
Print-to-Me	Y	Y
DataStream Interpreter page counting	Y	Y
PjL page counting	Y	N
iPrint	N	Y
Print rule sets - (UNIX print servers do not support rules based on group memberships)	Y	Y

Print server calculation

Calculating the approximate number of dedicated print servers you will need requires a three-part calculation.

Part 1: Peak pages per minute calculation

The first part of the calculation accounts for the estimate peak pages per minute, then factors in color and PostScript adjustments to derive the Total PPM.

Peak pages per minute	Requirements	Example
1) Estimated PPM peak rating		
a - Enter the number of output devices within the deployment that will be controlled	a	400
b - What is the average required speed out of output (PPM)?	b	45
c - Multiply (a) and (b) to determine the theoretical peak PPM rating	$a * b = c$	$400 * 45 = 18000$
d - Calculate 50% of the theoretical peak PPM rating (c) to determine the estimated peak PPM rating	$c * 0.5 = d$	$18000 * 0.5 = 9000$
2) Color-adjusted peak PPM		
e - Enter the average% of color output you anticipate (as a percentage of the total amount of output)	e	10%
f - Add the color percentage to the estimated peak PPM rating (d)	$d * e = f$	$9000 * 1.10 = 9900$
3) PostScript adjustment		
g - Enter the % of PostScript (as a percentage of the total amount of output)	g	25%
h - Multiple the PostScript percentage (g) by a factor of 4 and add 100 to include black and white printing.	$g * 4 + 100 = h$	$(4 * 25) + 100 = 200$
4) PDL adjusted peak		
i - Multiply the PostScript adjustment value (h) by the Color Adjusted peak PPM (f)	$h * f = i$	$200 * 9900 = 1980000$
j - Divide the result of (i) by 100 to calculate the PDL Adjusted Peak	$i \div 100 = j$	$1980000 \div 100 = 19800$

Part 2: Safe capacity calculation

The second part of the calculation gives you the opportunity to add a safety margin into the calculation, ensuring that the print server is capable of continuously processing all print requests.

I-Queue printing requires additional processing to re-render print jobs at release, and the increase demand must be taken into consideration when planning server size and processing capacity.

1) Server capacity	Requirements	Example
k - Enter the Server CPU size in MHz	k	3000
l - Enter the number of CPU cores	l	2
m - Multiply (k) and (l)	$k * l = m$	$3000 * 2 = 6000$
n - Multiply (m) by 100 to calculate the total desired server capacity	$m * 100 = n$	$6000 * 100 = 600000$

2) Safety margin	Requirements	Example
o - Enter the margin that you want to add to the total server capacity to ensure that the print server continues to function	o	50
p - Divide (n) by (o) to calculate the safe capacity rating (MHz)	$n \div o = p$	$600000 \div 50 = 12000$

Part 3: Print Server calculation

Estimate the number of print servers by dividing the PDL Adjusted peak value by the Safe Capacity Rating.

Print server calculation	Requirements	Example
q - Divide the PDL adjusted peak (j) by the Safe capacity rating (p) to estimate the number of dedicated print servers.	$j \div p = q$	$19800 \div 12000 = 1.65$
		Calculation complete

SPE and load balancing

The Scan Processing Engine (SPE) is an optional server component required to run the Equitrac scan feature. SPE can be installed either in a single server configuration, or scaled for larger deployments with the availability of load balancing to ensure uptime and throughput.

Certain endpoints can be configured to use the Capture and Send feature enabling them to send scanned documents to email, network folders, RightFax servers and SharePoint servers. In the case of SharePoint and RightFax, there must be as many SharePoint or RightFax destinations as there are SharePoint or RightFax servers (one destination per server). For example, if each department has a SharePoint server, then each server must be added as a valid Scan Destination. See the [Configure scan destinations](#) section in the [Kofax Equitrac Administration Help](#) file for more detail.

Scan load balancing with OCR calculation

An SPE requires at least one DCE to operate, and multiple SPEs can be deployed per DCE to manage the scan load requirements. If performing a large amount of scanning with OCR processing, scale the SPE requirements to suit their needs. One or more SPEs can be deployed to their own servers if the shared DCE/SPE server cannot resolve the scan and OCR needs. Various configurations are possible in such a setup.

When calculating SPE scanning load with OCR processing, consider the following:

- average number of pages per scan (a)
- number of scan jobs per hour peak (b)
- percentage of jobs which are OCR, represented as a decimal (i.e. 50% is 0.5) (ocrp)
- average GHz per core (agc)

The following calculation can be used to determine the number of cores needed for scans and for scans with OCR processing. The number of OCR cores cannot exceed the number of scan cores.

- $\text{scan} = (a*b)/3000*(2.5/agc)$
- $\text{ocr} = (a*b*ocrp)/3000*(2.5/agc)$

For example, if you have 1000 scan jobs per hour, with an average of 10 page/scan, and 50% of the scans are OCR, and the average core speed is 2 GHz, then:


- $\text{scan} = (10*1000)/3000*(2.5/2) = 4.17$ or 5 cores
- $\text{ocr} = (10*1000*0.5)/3000*(2.5/2) = 2.08$ or 2-3 cores

Depending if this is a dedicated server or a shared server:

- CPUs for Shared DCE/SPE server with 8 cores or less
 - Maximum SPE threads should be set to no more than N (# of cores)
 - Maximum OCR threads should be set to no more than N (# of cores / 2)
- CPUs for Shared DCE/SPE server with greater than 8 cores
 - Maximum SPE threads should be set to no more than N (# of cores)
 - Maximum OCR threads should be set to no more than N (# of cores – 4)
- CPUs for Dedicated SPE server
 - Maximum SPE threads should be set to no more than 2 x N (# of cores)
 - Maximum OCR threads should be set no more than N (# of cores – 1)

The amount of memory allocated for the system for scans is 512MB + (scan)*512MB.

Therefore, the amount of memory required in the example above would be (512) + (5)*512 = 3GB.

 The system should have a dedicated disk and dedicated NIC.

Refer to the [Configuring load balancing](#) section in the [Kofax Equitrac Administration Help](#) file for more detail on configuring your OCR scanning needs.

Client workstations

If you plan to control network and/or desktop printing, you need to deploy the Equitrac Client software to any client workstation from which a print request may be generated.

Equitrac can track printing sent to networked printers or locally connected printers (i.e. USB, LPT:1, Bluetooth, Firewire). To fully track workstation printing (including job detail attributes such as color, binding, stapling, and punching), server-based printing is normally required. However, the workstation direct IP printing feature with Equitrac Workstation client provides the same tracking detail without using a print server.

Deploying client software

Depending on the number of clients you must track, you can deploy in one of three ways:

- Manual – Run the installer local to each client workstation.
- Automatic – Use distribution software such as SMS or other MSI-capable management systems.
- Silent Install – Push the client installation software from a central shared folder on a network server to target clients.

Client workstation caching

Equitrac is capable of tracking printing that occurs even when CAS is offline.

While CAS is offline, all print tracking information generated from the workstation is logged locally until a direct connection with CAS is re-established. The details are automatically uploaded to CAS, and after confirmation of successful upload (transparent to the user), the cache is flushed.

Network bandwidth

In general, a single communication between Equitrac components is approximately 1.5kb. However, depending on the configuration and the activities generated by the user, the network traffic increases accordingly.

The following table is provided to help you estimate the transaction bandwidth you must anticipate when deploying Equitrac to track network printing and/or copying. The numbers shown below reflect the network traffic generated by Equitrac components only, and do not include Ethernet or TCP/IP packet headers, nor print job traffic.

Equitrac event traffic	Estimated Bytes	When event occurs
DCE start	19kb	Copy job requires DCE start.
DRE start	7kb	A print job is sent to DRE and secure document release is configured.

Equitrac event traffic	Estimated Bytes	When event occurs
Print job (no secure document release)	5kb	A print job is sent to DRE and secure document release is not configured.

Network outage

In the event of a network outage that extends beyond CAS (no network communication occurs between any Equitrac components), jobs in the secure print queues are not retrievable until network communication is re-established. Any transactions that have not yet been transmitted to CAS (whether for print or copy jobs) are not retrievable for release by the user and will not be logged in the Equitrac database.

CAS offline planning

Equitrac can be configured to continue print and copy tracking when CAS is unreachable.

Network and direct IP print tracking can continue in the absence of a connection to CAS if you configure DRE or DCE to print and charge later. Data can be stored until the drive space on the DRE server or DRC workstation is completely utilized. DRE and DCE automatically upload cached information to CAS when the connection is restored.

All print tracking except client billing validation is supported when the print device is configured in System Manager to print and charge later. Client billing (billing codes) requires a direct query to CAS to verify account details. With CAS offline, these details cannot be verified. Therefore, if your configuration will implement billing codes, you can configure the workstations to validate billing code information locally. The user can then authenticate against the data stored locally, and the user workflow is not interrupted.

If you enabled DCE Server caching and the DCE and DRE servers are reachable then d embedded devices will support Print-to-Me. If configured, a billing code prompt will still appear but cannot be validated against CAS. DCE and DRE cache full print and copy attributes and uploads them to CAS once communication is restored. The first time a user logs onto an embedded device while it was connected to CAS ensures that their user credentials have been cached on DCE and are available to all devices accessing DCE.

If you enabled DCE caching and the DCE server is unreachable, embedded devices that support local caching will still track copying. The user must have logged onto the embedded device just once while it was connected to CAS to ensure their user credentials have been cached locally. The device sends a periodic ping to DCE to determine if communication is possible. If not, all user login requests are authenticated against cache data automatically. The device will continue to try to communicate with DCE, and if successful, normal terminal operation resumes and all tracking activity is uploaded to DCE and ultimately, the Equitrac database.

User Account Management

Equitrac uses account information for user authentication and for transaction tracking. Each time a user performs a print, copy, scan, or fax job, the user must authenticate with their unique credentials before Equitrac allows access to the device. Equitrac logs and/ or charges the transaction details to a specified user account and maintains an audit trail of activity for reporting purposes. Equitrac tracks and charges every document that the user sends to any networked printer or walk-up copier.

Sites often choose to associate Equitrac accounts with an existing identity card such as a swipe card, a proximity card, Smart card, an employee pass key, or a campus card to offer the user a single mechanism used to authenticate at a variety of different applications. Card readers are then placed on or near the MFPs and device they control to allow the user to swipe or pass their identity card to authenticate before making copies, scanning documents, sending faxes, or releasing documents from the secure print queue.

Creating user accounts

Equitrac offers different methods to create user accounts. The size and complexity of your site primarily determines the method you should choose.

Method	Purpose and Benefits	Site Description
Active Directory Synchronization - or - LDAP Synchronization	Use Directory Services to batch import user data, then synchronize updates as they occur. <ul style="list-style-type: none">Minimizes administration because updates occur automatically via communication with the directory servicePIN code (ID card number) synchronization is automated (if implemented)Multi-server Print-to-Me is configured when the home server is designated upon	<ul style="list-style-type: none">Large sites that primarily rely upon Windows print serversAn existing user base that is managed by the directory serviceLDAP directory service must support persistent search (e.g. eDirectory)

Method	Purpose and Benefits	Site Description
	initial account import into Equitrac <ul style="list-style-type: none"> • Department mapping is performed automatically (if configured) 	
Flat-file import	Use the EQCmd.exe utility to import a file containing user account data. <ul style="list-style-type: none"> • Once imported, the accounts are managed solely with the Equitrac Accounts Manager or Department Manager. • Import pin or card numbers from a separate database. 	<ul style="list-style-type: none"> • Sites that do not rely on ADS or eDirectory user management • Typically 250-1000 users
Add users individually	Use Accounts Manager within Equitrac to add users one at a time.	<ul style="list-style-type: none"> • Sites that do not rely on ADS or eDirectory user management • Typically 1-249 users
Allow Equitrac to create users automatically	Configure Equitrac to create a new account automatically when a print request is received from a user not known to the Accounting Server, or when a user logs in to the front panel with their network credentials to perform copying. New accounts are assigned the default settings for quotas.	<ul style="list-style-type: none"> • Sites that prefer to issue temporary PIN codes for user authentication (when the email address is generated at auto user creation)
Create guest accounts	Configure Equitrac to enable users to create temporary guest accounts.	<ul style="list-style-type: none"> • Sites that prefer to grant guest user accounts in order to add funds via Cashier or Web Deposit
Create LDAP user account at login	Configure System Manager to auto-create users based on their email address.	<ul style="list-style-type: none"> • Sites that prefer to use employee's email address for login at MFPs

Preparing the user base for synchronization

Synchronization with an existing set of user accounts from another source such as Active Directory Services (ADS) or eDirectory (formerly NDS), offers the least amount of overhead and administration because you can maintain all user accounts required within your organization from a single source. You can perform an initial import of the accounts, then configure Equitrac to listen for changes on the ADS or eDirectory server. However, if you choose this method, you must carefully plan your account groups before you first populate the Equitrac database.

If your existing user account data is managed by eDirectory or other LDAP import solution, you can use LDAP Synchronization to monitor changes to the directory service. Subsequently, when a new user is added to the directory, or if a change is made to an existing account, Equitrac receives a notification specifying the change details. eDirectory Synchronization does not support domain qualification.

Whether you choose ADS or eDirectory, you can limit the initial account import to specific Organizational Units (OU) that contain user account data. Before you perform the first import, you should create specific OU containers on the ADS or eDirectory server that you will use for import and synchronization purposes.

i The EQ services must be started by a domain account with access to the contact Active Directory. If services are started under a local machine account, the Active Directory synchronization may fail.

If you deploy multiple Core Accounting Servers (CAS), consider that each server manages a separate set of users. You can have a separate instance of the same user account in each database, if needed. However, the accounts are managed separately.

To manage a set of users without duplicating accounts, configure your OUs to group user accounts that will be managed by a particular CAS. You can then import specific OUs into each CAS database.

There are several Equitrac attributes you may need to map within your existing user base. Ensure that these attributes are completed within your existing user accounts before you perform the initial import into the CAS database:

- The **Department** attribute maps the ADS or eDirectory department name to the Department field in the Equitrac database. If the department name does not already exist within Equitrac, it is automatically created and the selected users are added to the new department.
- The **Home Server** attribute maps the name of a particular print server to the Home Server field in the Equitrac database.
- The **PrimaryPIN** and **SecondaryPIN** attributes map the alpha-numeric PIN or ID card number code on the ADS or eDirectory Server to the PrimaryPIN and SecondaryPIN fields in Equitrac. A Primary PIN is generally the user identifier, and the optional Secondary PIN is equivalent to a password or card pin code.

Implementing PINs

PIN information connects an Equitrac printing account with user logon information. Control mechanisms can be configured to require the user to enter primary and/or secondary PIN information. The system tracks and charges printer and copier use to the appropriate account in the Equitrac database when users use PINs to log on to a control terminal or release a print job.

The primary PIN is the alpha-numeric sequence that uniquely identifies the user. The primary PIN can be data encoded on a magnetic swipe card, an HID, Legic or Mifare contactless ID card, or the user can enter it using the control terminal keypad. The secondary PIN acts as a device password or card pin code. The user enters it using the control terminal keypad or on the front panel in the case of embedded devices.

You can configure Equitrac to allow users to self-manage their user PIN information at a control terminal or Equitrac User Dashboard. Users can reset their PIN code at any time, reducing administrative overhead normally spent performing this task. Equitrac 6.x offers alternative primary PIN functionality. You can assign two different primary PINs to each user account, providing the user with additional flexibility when logging in.

Where supported, embedded devices can be configured to prompt a user to register a PIN when a new card is swiped. Embedded devices can also be configured to prompt for a Secondary PIN if the Primary PIN is manually typed (i.e. there is no secondary prompt if a swipe card is used).

Multi-domain authentication

When using the Equitrac solution in a multi-domain environment, it is recommended that the username be entered in either a Windows NT4 format (e.g. NT4domain\userid) or UPN format (e.g. userid@domain) when registering a swipe card. Using a fully qualified username for swipe-card authentication will greatly reduce the response time by eliminating the need to search through all the domains for that user.

If a fully qualified username is used for swipe-card authentication in a multi-domain environment, it is recommended that the Windows External authority is used for authentication, without specifying a domain. Typically, user accounts are validated against a default Windows domain, however, by not specifying a domain, CAS searches and authenticates by fully qualified username, not domain.

For details on setting external authorities, see [User Authentication](#) in the [Kofax Equitrac Administration Help](#) file.

Security Considerations

Equitrac offers the ability to secure the Equitrac services, the administration tools, and the secure print queues.

Establishing access permissions

To prevent unauthorized access to the Equitrac Administrative Applications or modifications to registry entries, Equitrac relies on Windows-level authentication and application-level Administrative accounts. All Equitrac installations require at least one user with Windows Administrator privileges who can start and stop services and the print spooler on the server workstation(s).

Application-level permissions are fully configurable. Access is granted to a Windows-level group, as opposed to individual users. For example, if you want to establish department-level account administrators, create a separate group within Windows that includes all users who will be allowed to administer accounts through Department Manager. Assign the group to the Department access permission.

The following table provides a description of each access permission and a use case detailing how you might organize your windows-level groups per domain to accommodate your site needs.

Permission	Description	Use Case
Admin	Controls access to System Manager.	<ul style="list-style-type: none">• System Manager contains all configuration tasks and device detail.• Limit access to users from IT or to an Equitrac super administrator group.• Separate device administration from accounts administration - assign separate user groups to each permission.
Reports	Controls Access to Reports Manager.	<ul style="list-style-type: none">• Create a reports administrator group that is responsible for auditing the system.
Accounts	Controls Access to Accounts Manager.	<ul style="list-style-type: none">• Establish a group of users that can create and modify all user accounts.
Department	Limits the view of user accounts to a specific department only. Equitrac	<ul style="list-style-type: none">• Create a group that is responsible for administering accounts within a specific

Permission	Description	Use Case
	checks which department the user belongs to, then limits the view within Department Manager to accounts within the same department only.	department only. This group can make modifications to existing accounts, but cannot create accounts.
Device Admin	Controls access to the Device Monitoring Console.	<ul style="list-style-type: none"> Create a group that is responsible for monitoring device status only. All SNMP status change UI notifications can be directed to any user via email, creating a proactive approach to solving device downtime and supply replacement.
Print Distribution	Allows this group of users to use Send To printing.	<ul style="list-style-type: none"> Allows certain users to submit print jobs on behalf of other users. These jobs are held in a secure print queue until the recipient releases the job from a control mechanism.
Cashier	Controls access to the Cashier application.	<ul style="list-style-type: none"> Create a group of staff members that can adjust balances on user, department, and billing code printing accounts (similar to a library cashier) via the Cashier application.

Auditing

Equitrac provide the ability to audit device and account activity based on a number of factors. Specifically, detailed activity reports provide statistics about:

- device usage
- user account
- network user
- billing code account
- department account
- queued documents by device
- queued documents by user account

Depending on the report you generate, the following data fields may appear in the report.

Report Field	Description
Account	Indicates if the activity was charged to a user, department, or billing code account type.
Cost	The amount of money that was charged to the account for the job.

Report Field	Description
Date	You can limit the report contents to a specific date range. When the report is run, the Date field shows the specific date on which the activity occurred within the date range selected.
Description	Document title for print job. If the activity was a copy job, the description is listed as 'copying'.
Details	Lists the specific details of the print job, such as page size, color output, duplex output, stapling, punching, binding, etc. For example, the following details might be displayed for a print job that is seven pages in total: 4xLetter/D = 4 letter-size pages, duplexed 3xLegal/C/Punch = 3 legal-size pages, color and punched output
Device Name	The name of the output device where the copy, scan, or fax job was released or performed.
Disposition	The status of the job. When you run the report, you can select 'all', 'deleted', 'expired', or 'released'. Deleted jobs were removed from the queue by the user without releasing them, expired jobs exceeded the time limit set on the secure queue and were automatically removed from the queue, and released jobs were jobs the user printed on an output device. Select 'all' to view all disposition types.
Pages	The number of pages produced.
Type	The job type that was produced. When you run the report, you can select 'all', 'copy', 'fax receive', 'fax send', 'print', or 'scan'.
User	Lists the Equitrac user account that produced the activity.
User ID	Lists the network user ID that produced the activity (appears in network user reports only).

Database and messenger communication

If you require remote access to the SQL server database, you must open the port first.

If you configure "Sending a popup message" as the method of notifying users of print errors, you must open TCP port 139. This port is not open by default.

Encryption


Equitrac reduces the threat of network sniffing through dynamic encryption keys. At the beginning of each communication with the server regarding PINs or passwords, DCE performs a dynamic public/private key exchange. If the device firmware does not support dynamic encryption keys, Equitrac automatically uses 128-bit AES fixed encryption keys.

You can optionally configure IPsec encryption if you prefer to encrypt communication between all Equitrac server components, such as DCE, DRE, CAS, DME, and Scheduler.

Print Assistant and Workstation Client use 128-bit AES encryption for the login prompt. If you want encryption on other workstation components, then you need to enable SSL or IPsec. To enable SSL, see [Enabling SSL Communication](#).


It is possible to encrypt the print stream. There are two options depending upon what the printer supports.

1. Configure the port to use IPP over SSL.
- Or -
2. Configure IPsec between the DRE server and the printer. This will encrypt all traffic between the two devices.

 Enabling SSL or IPsec may impact performance.

Enabling SSL communication


Communication between Equitrac components running in a Windows environment can utilize SSL (Secure Socket Layer) if required. To enable this feature, run the EQEnableSSL.exe utility located in the Program Files\Nuance\Equitrac\Tools folder.

 EQEnableSSL.exe must be run on every system running Equitrac software that uses an SSL connection. (e.g. CAS, DRE, DCE). Shutdown all Equitrac services and utilities (e.g. System Manager) before running this command.

The command-line utility accepts the following command:

```
EQEnableSSL.exe [-e -d -h]
```

Value	Description
-e	Enables SSL communication from this system.
-d	Disables SSL communication from this system.
-h	Displays this help screen. No parameters display the current settings.

 For compatibility reasons, management communications are not currently encrypted even if this feature is enabled. Non-Windows DREs do not support encrypted connections.

Securing print output

In environments where users print proprietary or confidential documents, secure printing gives users the power to control the timing of their output. Equitrac holds documents sent to registered

devices in the DRE's secure print queue until the user releases the document from a control mechanism, such as embedded device.

Secure the DRE spool directories

Securing the DREs spool directories will ensure that other users cannot find proprietary documents on the DRE server. On each Windows DRE server, ensure that you set full control for the User ID that is running the DRE service only. Grant read-only access to the User ID that is responsible for running system backups. Remove access to any other user IDs.

Windows: C:\Users\<>userid>\AppData\Local\Equitrac\Equitrac Platform Component\<>version>\EQDRESrv\EQSpool. Where <userid> is the account under which the Equitrac services are running.

UNIX: <installdir>\EQSpool

Establish IP masking

If supported on the output device, mask the IP Address of the MFP to ensure that users cannot directly connect via the IP address.

Virus scanning setup


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

Server folders to exclude

Equitrac recommends that you exclude the following server folders from virus scanning:

- The folder and sub-folders containing Equitrac
- 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\Equitrac

Where <userid> is the account under which the Equitrac services are running.

 The installation path depends on the location where Equitrac was installed on the server. If you installed Equitrac 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 Equitrac 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) and trace log files (.log)

Backup and recovery

The design and implementation of an effective backup and disaster recovery process is essential to any network environment. Equitrac conform to the requirements and standards for Windows server-based applications, and standard backup procedures should be utilized for backing up and restoring the binary files, configuration and data.

Database backups

Equitrac database backups are crucial for ensuring the safety of both the collected data and the system configuration data, which is also stored in the database, with the exception of the print queue definitions. The print queue definitions should be backed up in accordance with backup best practices, including data retention, rotation schemes and off-site storage.

 The Equitrac databases are 'live' and cannot perform basic file-based backups without endangering the internal consistency of the databases.

Major backup software applications include specific database backup options or connectors for backing up SQL Server (including SQL Express) databases, and should be used whenever possible.

If specific backup connectors are not available, it may be possible to dump the data from the database to an external file or to stop the database engine prior to backing up the files. Consult your database documentation for details.

Print server configuration

The Windows print queue configuration is stored in each print server's registry. This configuration data can be secured by either backing up the complete print server registry using standard backup software, or by using the Print Migration utility (downloadable from microsoft.com)

Recovery

When restoring a backup after a complete system failure, backup recovery systems can generally restore the system to a consistent state. However, when restoring multiple systems or a single

system backed-up using a hybrid method, it is necessary to ensure that all aspects of the system have been restored to fully operational state.

The following checklist outlines the items to verify after a recovery process:

- Database restored
- ODBC connection (DSN) restored
- Equitrac software either (1) restored, or (2) reinstalled, and appropriate hotfixes applied
- Equitrac software licenses correct and valid in System Manager (should the server name have changed, the licenses will need to be re-activated)

Disaster recovery through virtual computing

One approach to recover after a server failure is to utilize virtualization software—such as Virtual Server or VMware—on the Equitrac servers. The Equitrac server can be deployed as the only virtual machine on the physical server to ensure that the full performance of the underlying hardware is available to Equitrac.

By using a virtual machine, it is relatively easy to recover from a disaster even in the absence of repaired or identical server hardware, by installing the Equitrac virtual machine on another physical server. This can reduce dependence on specific server hardware and enable more rapid recovery of the server environment.