

Kofax Equitrac

Windows System Manager Guide

Version: 6.1.0

Date: 2020-04-16

The KOFAX logo is displayed in a bold, blue, sans-serif font. The letters are thick and closely spaced, with a clean, modern appearance.

©2020 Kofax. All rights reserved.

Kofax is a trademark of Kofax, Inc., 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 Kofax.

Table of Contents

| | |
|---|----|
| Windows System Manager Applications..... | 5 |
| Reports Manager..... | 6 |
| Reports overview..... | 6 |
| Report categories..... | 7 |
| Determine which report to run..... | 8 |
| Change the currency symbol used when viewing reports..... | 9 |
| Running standard reports..... | 9 |
| Report criteria..... | 10 |
| Customizing standard reports..... | 11 |
| Adding a custom logo..... | 11 |
| Creating a custom format..... | 11 |
| Saving a custom report..... | 12 |
| Running custom reports..... | 13 |
| Deleting custom reports..... | 13 |
| Configuring and running a savings report..... | 14 |
| Running a savings report..... | 14 |
| Scheduling reports to run automatically..... | 15 |
| Running consolidated reports..... | 15 |
| Configuring CAS servers..... | 15 |
| Running subsidiary reports only..... | 16 |
| Printing, emailing and exporting reports..... | 16 |
| Printing a report..... | 16 |
| Emailing a report..... | 17 |
| Saving a report to a file..... | 17 |
| Device monitoring with DME console..... | 18 |
| DME workflow..... | 18 |
| SNMP communication requirements..... | 19 |
| Viewing device status in the DME console..... | 19 |
| Viewing session status in the DME console..... | 21 |
| Creating alert rules..... | 21 |
| Name..... | 21 |
| Action..... | 21 |
| Criteria..... | 22 |
| Creating custom alert messages..... | 23 |

| | |
|--|----|
| Assigning alerts to devices..... | 24 |
| Generating device status reports..... | 24 |
| Change status report contents..... | 25 |
| Print Queue Viewer..... | 26 |
| Running Print Queue Viewer on a workstation..... | 26 |
| Campus Card interface..... | 28 |
| Configuring a Campus Card interface..... | 28 |
| Blackboard IP interface..... | 30 |
| CBORD Odyssey interface..... | 31 |
| CBORD CS Gold interface..... | 32 |
| Working with Campus Card..... | 32 |
| Using Campus Cards with embedded devices..... | 33 |
| Cashier..... | 34 |
| Using Cashier..... | 34 |
| Modifying the printed Cashier receipt..... | 35 |

Windows System Manager Applications

Kofax Equitrac supports the following Windows related administrative applications.

- **Reports Manager** - used to produce comprehensive summary or detailed reports on accounts, account activity and printer use.
- **Device Monitoring Console** - works with the Equitrac Device Monitoring Engine (DME) to provide historical data on device performance.
- **Print Queue Viewer** - provides a tool for Administrators to view and delete documents within the secure print queue.
- **Campus Card Interface** - works with Blackboard, CBord Odyssey and CBord CS Gold card payment systems. A Campus Card account inside CAS may have an account name which can be used to identify the print jobs in the print queue.
- **Cashier** - used by staff members who have a role in managing account balances. Service staff at a print/copy desk use Cashier to add and remove funds from user accounts. Cashier can reside on any network client workstation.

Reports Manager

Reports Manager contains a selection of standard reports, or you can modify standard reports to create your own custom reports. If your deployment uses multiple CAS servers, you can also generate reports on transaction data uplinked from subsidiary accounting servers.

For example, you can use Reports Manager to generate a printer usage audit trail in order to recover costs. You can audit usage patterns, user or department activity, activity load on specific devices, analyze inefficiencies, and access device fault tolerances.

Equitrac also provides reports that allow you to analyze devices trend usage, color or black & white usage over time, usage patterns, etc. Graphical device configuration reports provide usage analysis of print queues, ports, control terminals, etc.

If you installed the DME component, you can also generate device status reports. See [Generating device status reports](#) for details.

To open Reports Manager, go to **Start > All Programs > Kofax > Reports Manager**. For more information on generating and analyzing reports, see [Creating and Running Reports](#) in the [Kofax Equitrac® Administration Help file](#).

Reports overview

Reports allow you to analyze system performance in order to troubleshoot usage, load balancing, and overall workflow. You can run either standard or dashboard reports.

Reports Manager provides a set of standard reports and allows you to customize report look and feel, schedule reports to run at a specific time automatically, and print or export generated reports to a number of file formats or as email attachments.

[Dashboard reports](#) are special reports that display data in table, pie, or bar graphs. Dashboard reports are viewed on a web browser, and are accessed via Web System Manager. See the [Kofax Equitrac® Administration Help file](#) for details.

If you have deployed more than one CAS, you can generate reports using data from all CAS servers, or you can run reports on individual servers.

This section provides information about:

- working with standard reports
- setting report criteria
- customizing reports
- scheduling reports to run as automated tasks
- generating uplinked reports on transaction data uploaded from subsidiary accounting servers

Report categories

Reports Manager provides a number of standard reports designed to help you analyze your system performance. These reports are organized into categories, such as Accounts, Analysis, Detailed activity, Summary activity, and Total activity.

Reports are organized into the following categories.

| Report Category | Description |
|-------------------|--|
| Accounts | <p>Reports in this category provide data about accounts including:</p> <ul style="list-style-type: none"> • how, when, and where accounts are being used • account balances and transaction histories • how accounts are organized |
| Analysis | <p>Reports in this category are designed to help you maximize your device usage. They provide information about your devices including:</p> <ul style="list-style-type: none"> • their current status • when and how often they are being used • how often they are online or offline • when and how often they experience faults such as paper jams or toner outages • total and percentage usage of color, black and white, or monochrome in simplex or duplex pages by activity type, application, account or network user. <p>This category also includes a Savings report detailing how much money was saved by not releasing all jobs sent to the printer (e.g. expired or deleted jobs). 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. See Scheduling Reports to Run Automatically.</p> |
| Detailed activity | <p>Reports in this category provide detailed information about the documents users are creating. You can view information by:</p> <ul style="list-style-type: none"> • billing code account • department account • device • network user • user account <p>This category also includes reports on the documents currently in a print queue. These reports only contain data if you have enabled secure printing on one or more device queues.</p> |

| Report Category | Description |
|------------------|---|
| Summary activity | <p>These reports list the number of color, black and white, and monochrome pages created by accounts, devices, application, network user, organizational structure (membership and account), disposition of routed documents (by user account and device), etc. Summary of activity reports allow you to summarize that information by date, device, network user, or transaction type.</p> <p>This category also includes reports on the documents currently in a print queue. These reports only contain data if you have enabled secure printing on one or more device queues.</p> |
| Total activity | <p>These reports list the number of color, black and white, or monochrome in simplex or duplex pages created by:</p> <ul style="list-style-type: none"> • account type • billing code account • department account • device • desktop device • account or network user • user account • activity type • application • device and user location |

Determine which report to run

The following table lists some scenarios and the report to run in each case. Use the table to help determine which report provides the information you need.

| If you want to... | Then run this report... |
|---|---|
| View the account balance for a user. | Accounts > Account adjustment |
| View all accounts assigned to a department or billing code. | Accounts > Account listing |
| View a detailed list of a user's activities. | Accounts > Account statement |
| Manage users' color quotas. | Account > Color quota summary |
| Determine which devices are the most reliable. | Analysis > Device availability, or Analysis > Device faults |
| Create a maintenance schedule for your devices. | Analysis > Device faults vs. usage |
| Identify over- or under-used devices. | Analysis > Device usage |
| Identify high- and low-usage times of day for a device. | Analysis > Hourly activity |

| If you want to... | Then run this report... |
|--|---|
| View a list of all documents created for a billing code. | Detailed activity > Detailed activity by billing code account |
| Determine if a department prints enough color copies to justify buying a second color printer. | Total activity > Total activity by department account |
| View a detailed list of activity by a device within a certain location. | Total activity > Total activity by device location |

Change the currency symbol used when viewing reports

If your regional settings use a currency symbol other than the dollar sign (\$), or if you use any character outside the standard ASCII set (such as the umlaut “ö”), you need to adjust the browser encoding before you can see the correct symbol within a browser window.

1. Open a web browser.
2. From the View menu, select **Character Encoding**, then select **Unicode (UTF8)** from the menu.
3. Run a report to check the result.

Run one of these reports (which contain the currency symbol): Account adjustment, Account listing, Account Adjustment or Hourly activity.

Running standard reports

The process for running standard reports is the same for all reports—only the criteria available to limit the scope of the report change based on the report you are running.

To run a standard report, do the following:

1. Open **Reports Manager**.
2. Expand a category node and select the report you want to run. The **Select report criteria** dialog box opens.

Note The authentication report under the Analysis node provides an authentication audit trail for both successful and failed authentication attempts at all MFPs.

3. Select the criteria to limit the scope of the report.
4. Click **OK** to close the **Select report criteria** dialog box. The generated report displays in the Reports Manager window.

When the report is generated, you can print, email, or save it in one of several file formats.

You can also customize any standard report once it has been generated and save your customization as a new report definition. See [Customizing Standard Reports](#) for details.

Report criteria

The following table lists the criteria available to limit the scope of a standard report. Not all criteria are available in every report.

| Criteria | Description |
|------------------|---|
| Account status | Filters the report to include all accounts, or only overdrawn, locked, active, or deleted accounts. |
| Account type | Filters the report to include user, department, or billing code account types. |
| Billing code | Filters the report by a specific billing code. |
| By billable | Filters the report by billable accounts. |
| Custom group | Filters the report to devices assigned to a specific group. |
| Date | Limits the report to a specific date range. Select one of the pre-defined date ranges, or select Custom range and enter the start and end dates for the report. Date range format is dependent on system regional settings. |
| Department | Filters the report by a specific department. |
| Device name | Filters the report by a specific device. |
| Device type | Filters the report by a specific device type. |
| Disposition type | Filters the report by the status of a document in a print queue. |
| Limit | The number of rows that are returned in the report. |
| Location | Filters the report to the physical location of users and devices. |
| Order by | Orders transactions by account, balance or creation date. |
| Summarize by | Orders transactions; options vary by summary report. |
| Transaction type | Filters the report to include all, print, copy, fax send, fax receive, or scan transaction types. Select or clear multiple transaction types as desired. |
| User | Filters the report by a specific user. |
| User ID | Filters the report by User ID (by network user reports only). |
| Vending account | Filters the report by a specific vending account. |

Customizing standard reports

You can add your own logo to your reports, and change the specific columns that are included in the standard reports to create your own custom reports.

Note The Program Files\Nuance\Equitrac\Database folder contains CAS_SQLServer_Views.sql which can be run to create views of the transaction data stored in the database. These views can be used for reporting purposes or to help better understand the underlying data captured.

Adding a custom logo

The Equitrac logo appears in all generated reports, by default. You can customize that logo by loading a different image to the accounting server. Reports Manager supports any graphics file format that Windows Internet Explorer supports, such as .bmp or .jpg. Every report you generate from that accounting server uses the same logo image.

The logo appears in the upper right corner of the report, and uses 25% of the total table width. As a best practice, prepare your logo to a maximum width of 180 pixels. Add the logo, then perform an onscreen test and a print test to ensure the logo is sized appropriately. As a guideline, the Equitrac logo used by default measures 154 x 40 pixels.

To customize the generated reports logo, do the following:

1. Copy your custom image file to **Program Files\Nuance\Equitrac\Accounting Service**. This folder is located on the machine where CAS is installed and running.
2. Open a command prompt and go to **Program Files\Nuance\Equitrac\Accounting Service**.
3. On the command line, type:

```
eqrptload.exe -a <accounting server> -b imagefilename
```

where `imagefilename` is the custom image file you want to appear on all generated reports. For example:

```
eqrptload.exe -a CASSRV1 -b AcmeLogo.bmp
```

loads the `acmeLogo.bmp` file from the **Accounting Service** folder.

Note The image file must be in the working directory. Do not enter the full path to the image on the command line.

Creating a custom format

In the Reports Manager window, you can customize a report's format by modifying the column display.

Note In the Configure Report Layout dialog box, applicable generated reports contain an Alt cost column that displays secondary (dual) pricing data.

To customize the content of a report, do the following:

1. In Reports Manager, select **View > Configure report layout**.

2. In the **Columns to display** list, select or clear the column checkbox for each column you want to display or hide in the generated report. The defaults are pre-selected from the list.
3. Customize the selected columns to display by doing the following:
 - Click the **Up** or **Down** arrows to re-order the columns to appear in the generated report from left to right.
 - Enter a new column title in the **Label** field. You cannot use the following special characters: '@', '&' or '<'.
 - Enter the column **width** as a percentage of the overall width of the report. The column widths should add up to a total of 100%. If the selection exceeds 100% of the report's total columns width, a **Configure report layout** warning pops up.

If the warning appears, you have three options:

- **Yes** – Automatically adjusts the new and existing columns to add up to 100% of the overall report width.
 - **No** – Exits without adjusting the column widths to equal 100%. The column is added to the report, but since it exceeds the total columns width, it does not display.
 - **Cancel** – Return to layout dialog box and enter a different value.
4. Click **OK** to save the customized formatting and close the dialog box.

Saving a custom report

The standard reports available in Reports Manager are templates from which you can create and save customized reports, known as report definitions. When creating report definitions, you can configure Reports Manager to prompt for specific criteria at generation time and save the report definition as a personal or site report.

To save a customized format as a report definition, do the following:

1. Run a report. See [Running Standard Reports](#) for details.
 2. In Reports Manager, select **File > Save Definition As** to open the **Save report definition as** dialog box.
 3. Indicate whether you want to select criteria each time you run the report, or if you want to save the current criteria selections as part of the report definition. If you save the current criteria selections, they are used each time the report is run.
 - Select the **Prompt for <criteria>** option to prompt for filter criteria when the report is generated.
- Or-
- Select the **Define in the report definition** option and select an option from the drop-down list to save existing criteria selections in the report definition. For example, if you always want the report to include only copy transactions, select **copy** in the list.
4. Click **Next** to continue.
 5. Enter a **Name** for this report definition. The custom report name cannot be greater than 50 characters.
 6. Select a **Report type** from the list.
 - Select **Personal report** to save the report to the local machine. Only those with access to the local machine can access and generate personal reports.
 - Select **Site report** to save the report to the server. Anyone can access and generate site reports.

7. When Site report is selected as the Report type, an additional option is available allowing users to run certain reports from User Dashboard. Select the **Allow users to run this report from user's personal webpage** checkbox for any of the following reports:
 - Account statement
 - Detailed activity by network user
 - Detailed activity by user account
 - Detailed activity for queued documents by user account
 - Detailed activity for routed documents by user account
8. Optionally, enter a **Description** in the field.
9. Click **Finish** to save the custom report.

Note You can schedule events to generate automatic site reports from existing site report definitions. For more information, see [Scheduling reports to run automatically](#). Personal reports cannot be scheduled.

Note A secondary custom site report can be created from an existing custom site report, however, the secondary report cannot be run in User Dashboard.

Running custom reports

Custom reports are displayed in Reports Manager as sub-items under the standard report they are based on.

To run a custom report, do the following:

1. In Reports Manager, select **File > Open**.
2. Expand the node for the standard report that your custom report is based on, and select the report to run.

If the criteria for the custom report have already been defined, the report displays in the Reports Manager window, otherwise the **Select report criteria** dialog box opens.

3. When the report is generated, you can print it, email it, or export it in one of several file formats.

Deleting custom reports

To delete a custom report, do the following:

1. In Reports Manager, select **File > Open**.
2. Expand the node for the standard report that your custom report is based on.
3. Right-click the custom report, and select **Delete**.

Note You cannot delete a custom report through the Reporting section in Web System Manager.

Configuring and running a savings report

A Savings report details the cost savings and environmental impacts associated with using an Equitrac system. These reports show how many pages have been printed from a workstation, but have NOT been released to the printer (e.g. expired or deleted jobs). Cost savings can be also measured by the number of force monochrome or forced duplex pages. 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 by not printing expired or deleted jobs, or by forcing simplex jobs to be duplexed.

To configure a Savings report for environmental measures, do the following:

1. In Web System Manager, go to **System Configuration > Global Configuration Settings > User Interaction > Savings Report Metrics**.

Note The default values based on average global consumption, however, these values can be changed to suit your geographic location and environment.

2. Select **U.S.** or **Metric** from the **Measurement system** drop-down list.
3. Enter the number of **Letter/A4 pages** that **One tree is equivalent to**.
4. Enter the **gallons (or litres) of water** that **One letter/A4 page uses**. The volume unit depends on the measurement system used—U.S. (gallon) or Metric (kg).
5. Enter the **pounds (or kg) of CO2** that **One pound (or kg) of paper releases**. The volume unit depends on the measurement system used—U.S. (pound) or Metric (kg).
6. Click **OK** to close the Savings report metrics dialog box.

Note The Reset to defaults button resets ALL fields to their default values.

Running a savings report

To run a Savings report, do the following:

1. In Reports Manager, expand the **Analysis** node and select **Savings**.
2. In the **Select report criteria** dialog box, select the criteria to limit the scope of the report.
The Savings report can be summarized by User, Department, or Printer.
3. Click **OK** to close the Select report criteria dialog box. The Savings report displays in the Reports Manager window.

The Cost column indicates a total cost for Deleted, Expired, Forced monochrome, Forced duplex pages, and number of sheets not printed. The cost savings can be further measured by listing the individual savings for forced monochrome, forced duplex, forced mono/duplex pages. These columns are not in the report by default, but they can be added to display the individual breakdown for each feature.

When the report is generated, you can print, email, or save it in one of several file formats.

Note The cost savings for forced monochrome and forced duplex are dictated by the price lists associated for those features. For example, if the price lists for color pages and for black & white pages are set to the same amount, then the forced monochrome offers no savings and displays the cost as “0”. However, if the price list for a color page is \$0.05, and black & white is \$0.01, and 20 color pages were printed with forced monochrome applied, then the cost savings is \$0.80. (i.e. \$0.04 price difference x 20 pages = \$0.80).

Scheduling reports to run automatically

Use Web System Manager to create scheduled tasks to run automatically at a preset date, time, and interval. When scheduling tasks, you can specify whether you want a particular task to run only once, or on a daily, weekly, or monthly basis.

If you want to schedule a report to run automatically, refer to [Schedule A Report Task](#) in the [Kofax Equitrac® Administration Help file](#).

Running consolidated reports

If you deployed more than one accounting server, you can uplink the subsidiary CASs to the master CAS. This allows the subsidiary servers to upload data to the master CAS, while also keeping a copy on its local server. You can then run consolidated reports on the master CAS to view transaction and account data from all CAS servers, or you can run reports on individuals' servers. Optionally, you can set the subsidiary servers not to post transactions to the master CAS. The transactions remain local to each subsidiary server.

Configuring CAS servers

Configuration is required on the master and subsidiary CAS servers.

1. In Web System Manager, go to **System Configuration > Network Environment > Domain Qualification, Uplink, SMTP Mail and SNMP Configuration**.
2. Enter the **Name** of the designated master CAS.
3. Select the **Uplink time of day** for the subsidiary CAS to connect to the master CAS.

By default, Equitrac sets the uplink time at 1:00 am—a time that CAS is not heavily accessed by DRE, DCE, DME, or client workstations. If your site experiences a heavy load on CAS at 1:00 am, then change this to a different time. Sites with multiple subsidiary servers should stagger the uplink time.

4. The **Transaction set** options allow you to configure how the subsidiary and master CAS handle data transactions.

Note The Transaction set options must be set on the Master CAS, not the subsidiary CAS.

- **Do not post transactions** – the subsidiary servers do not send transactions to the master CAS.
- **Post individual transactions** – the subsidiary servers send individual transactions to the master CAS. This option allows the master CAS to view transaction and account data from all CAS servers.
- **Collate transactions** – the subsidiary servers bundle transactions in one of two ways: **Daily** or **Hourly**. Equitrac collates daily transactions at the time you selected in Uplink time of day.

You can also select the **By Network user** option to send or to separate the transactions per network user.

5. Click **OK** to save the changes.

Running subsidiary reports only

If you want to run reports from the master CAS that contain only the transaction data from the subsidiary CAS, do the following:

1. Open a command prompt, go to **Program Files\Nuance\Equitrac\Accounting Service** and execute the following command:

```
eqrptload.exe -a <accounting server> -f reports\uplinkreportlist.csv -u
```

where `accounting server` represents the system name of your accounting server.

For example:

```
eqrptload.exe -a PRINTSV1 -f reports\uplinkreportlist.csv -u
```

2. When the command prompt displays the message `EQRptLoad success`, all of the uplinked reports loaded successfully. You can select any uplinked report in the **Select report to open** dialog box.

Printing, emailing and exporting reports

When you generate a report, it is displayed in the Reports Manager window. You can either print the report, or export the report to a file or as an email attachment. When exporting a report, you can select a number of file formats, including XML, HTML, CSV-Unicode, or CSV-ANSI.

Printing a report

You can print reports to a configured local or network printer. In the Reports Manager window:

- Select **File > Print Setup** to configure printer output settings.
- Select **File > Print Preview** to see a preview of the printed report.
- Select **File > Print** to send the generated report to the printer.

Note The Print Preview option requires Internet Explorer version 9 (or higher).

Emailing a report

You must ensure that Web System Manager is properly configured for a valid email server before emailing generated reports in Reports Manager. See [Configure the Mail Server for Email Notifications](#) in the [Kofax Equitrac® Administration Help file](#).

To email a report, do the following:

1. Select **File > Mail** to open the Send Mail dialog box. Alternately, click the **Send Mail** button at the top of the report window.
2. Enter email information:
 - In the **To** field, enter the email address of the recipient. To email multiple recipients, separate email addresses by commas or semi-colons, without any spaces between addresses.
 - In the **Subject** field, enter subject text.
 - In the **Message** field, enter message text.
3. Select or clear attachment file formats.

To use the selected columns options, ensure that you first open the Report Layout dialog box (View > Report Layout) and choose the columns you want to show in the report. When you mail the report, all columns listed in the Report Layout dialog box are exported, regardless of the columns you choose to show. When you select either Selected columns option in the Send Mail dialog box, only the columns currently displayed in the report are exported.
4. Click **Send**.

Saving a report to a file

To save a report to a file, do the following:

1. In the Reports Manager window, select **File > Save as**.
2. Select a file location, file name, and file format. You can save the file in XML, HTML, CSV-Unicode, or CSV-ANSI format.
3. Click **Save**.

To generate reports on a regular basis and save the reports to a selected destination.

Device monitoring with DME console

The Device Monitoring Engine (DME) is an optional server component that gives an Administrator the power to identify potential device problems based on historical performance data.

DME monitors Simple Network Management Protocol (SNMP) messages generated by specified devices for status information. Each time a status change message is intercepted, DME logs the information in the database. If the new status matches a pre-set alert condition on that device, a notification message is forwarded to designated individuals or desktops. You can view the current device status at any time within the DME Console, or you can run reports to ascertain the overall device health, and plan maintenance based on historical performance.

This section provides information about:

- the workflow required to configure and use DME
- communication required between Equitrac components and SNMP devices to capture status change information
- creating Alert Rules that specify the faults you want to be notified about per device
- assigning rules to specific devices
- viewing status information within the DME Console
- generating reports to analyze system status information over time
- allowing DME to prevent automatic print job release from endpoints based on device status

DME workflow

Setting up DME to monitor devices is a straightforward task. The DME console automatically contacts CAS to determine the list of devices to monitor. Without any further configuration, you can view the current device status within the Device Monitoring Console, or you can generate reports within the Reports Manager to view historical status detail.

However, if you implement more than one DME, you need to establish which devices are monitored by each DME respectively. In addition, if you want to be notified of faults as they occur, you can set up Alert Rules that send a notification message when a particular fault condition is met. After you establish the rules, you can apply them to one or more devices within the DME Console.

Follow the workflow below to configure full DME functionality.

1. Select devices to monitor in Web System Manager. Refer to the [Kofax Equitrac® Administration Help file](#) for DME monitoring.

DME automatically contacts CAS to retrieve the list of devices to be monitored. Within Web System Manager, you can manually remove devices from DME monitoring, or assign devices to a particular DME.

2. Create alert rules in the DME Console.

Create custom rules that are applied only when certain fault conditions are met. Alert rules include configuration notification options that alert specific Administrators when the fault occurs.

Note To use the DME Console, you must be a part of either the Administrator or Device Administrator group within Web System Manager's Access Permissions.

3. Assign alert rules to specific devices.

Apply the rules to one or more devices.

4. Run reports to monitor device health and historical performance.

Use Reports Manager to generate standard reports or custom reports that provide a historical performance analysis based on device status.

SNMP communication requirements

DME reports on device status by polling for SNMP status changes. Therefore, only SNMP-enabled printers and devices can be monitored by DME. DME continually polls for these status change messages, and for any status faults that match the Alert Rules you applied to one or more devices.

Refer to the [Kofax Equitrac® Administration Help file](#) to configure [SNMP communication](#).

When DME intercepts a status change message, it performs the following tasks in order:

1. Logs the start time of the fault and updates the device status in its database.
2. References the list of Alert Rules.
3. Applies all rules whose criteria matches the device and fault condition.
4. When the status changes again, DME logs the end time of the fault and once again updates the device status.
5. Sends device status information to CAS to use for reporting purposes.

DME maintains the list of status changes in its database, including the start and end time of each fault. The end time remains NULL until the status of the device changes. When the end time is set, the fault is considered "closed". Only closed faults are forwarded to CAS, so reports reflect device faults that have been resolved only. DME also holds faults that were closed within the last 7 days in its local database.

The diagram below depicts the communication workflow between the DME component, SNMP-enabled devices, and CAS when the DME Console service first launches or is refreshed.

Viewing device status in the DME console

The Device view within the Console provides a complete set of device properties and device status information at a glance. DME listens for SNMP status changes on each device, then updates CAS if the status changes.

To open The DME Console, go to **Start > All Programs > Kofax > Device Monitoring Console**.

The Message view displays all DME generated messages, event log message, and DME service start and stop events. Status information is shown in the Device view and in the Devices properties dialog box. To view the device properties, you can select the device from the **Hostname** column, or right-click the device and select **View properties**.

Note Within the DME Console, the status column is updated only when you press the Refresh button. If you are checking the current status of a device within the Console, make sure you refresh the window to force the Console to retrieve the current status information from the DME component.

If DME cannot populate the device type information (i.e. it was not provided when the device was added to Equitrac), the DME Console retrieves the information from SNMP data. DME then populates the Manufacturer and Model fields with the retrieved data, followed by an asterisk *.

Use the following table to map the status code to the SNMP fault condition that has occurred on the device.

| Status | Description |
|-----------------------|---|
| Down | The printer is reporting its status as DOWN, but DME cannot determine the cause. DME has received an unrecognized error status. |
| Empty input tray | A job cannot continue because there is no medium in the specified input tray. |
| Full output tray | The output tray is full and jobs cannot be printed. |
| Missing input tray | An input tray has been removed from the device. |
| Missing marker supply | The marker supply has been removed from the device. Marker supply refers to the toner, ink, dye, etc. that is specifically used on this device. |
| Missing output tray | The output tray has been removed from the device. |
| Near full output tray | The output tray has almost reached capacity. Jobs are not printed when the tray reaches capacity. |
| Not available | The device is not online, or is shut down. |
| Offline | The device has been set to offline mode. |
| Overdue Maintenance | The maintenance date has passed, as per the date set on the device by a service person or Administrator. |
| Paper jam | Paper Jam |
| Paper low | Paper is low |
| Paper out | Paper is out |
| Toner low | Toner is low |
| Toner out | Toner is out |

| Status | Description |
|-------------|---|
| Unreachable | DME did not receive a reply when asking the device for its status. |
| Warning | <p>The device is reporting a general status warning, but DME is unable to specify the cause.</p> <p>For example, some printers report a warning when a paper tray is empty, even though that tray is not requested as the paper source for a print job.</p> |

Viewing session status in the DME console

The Device view within the console provides session status information at a glance. The session column indicates the current session status on an associated embedded device, when available.

A session can be in one of three states:

- **Active** – a session is active on the device
- **Inactive** – no session is active on the device
- **Offline** – the device is not connected

If the session state cannot be determined (such is the case with Xerox JBA), or if there is no embedded device attached to the physical device, nothing is displayed in the session column.

Creating alert rules

If you want to be notified when a specific fault occurs on a device, you can create an alert rule that DME applies when the fault criteria is met. You can apply one alert rule to multiple devices, or multiple rules to a single device. For example, you may want to monitor one high-traffic device for both toner low and paper low messages, but another less-used device for toner out and paper out only.

To create alert rules within the DME Console, select **Alert rules**, then click **<Add...>** in the right pane.

There are three facets to each alert rule: Name, Action, and Criteria.

Name

Each rule must have a unique name. The rule is stored within the CAS database. Use the name to identify the rule within the DME Console. You can optionally include a description of the rule which allows other Administrators to understand the rule criteria at a glance from within the DME Console.

Action

Select one or more notification methods that DME uses when the Rule's criteria is met. By default, Email and Event Viewer are selected. The table below describes what happens if you choose each option.

| Notification Method | Description |
|---------------------|---|
| Event viewer | Logs an event in the Windows Event viewer. |
| Email | <p>Sends a standard or custom email message to designated email addresses.</p> <p>If you select this method, you must also select email recipients. Enter one or more recipients in the space provided, separated by semi-colons.</p> <p>You can optionally create a custom notification message that is used in the body of the email.</p> <p>You must configure the Mail Server if you the system to send email messages. See Configure the Mail Server for Email Notifications in the <i>Kofax Equitrac® Administration Help file</i>.</p> |
| Network pop-up | <p>Sends a network pop-up message to specified users.</p> <p>If you select this method, you must enter the network computer names or IP Addresses in the Computers field. To send the notification to more than one user, separate the computer names with a semi-colon.</p> |
| Console | Sends a pop-up message to the machine where the DME Console is installed. |

Criteria

Criteria refers to the type of fault that initiates the notification. Criteria optionally refers to the duration and frequency of occurrence.

DME can monitor SNMP-enabled devices for the following fault types:

- Down
- Empty input tray
- Full output tray
- Missing input tray
- Missing marker supply
- Missing output tray
- Near full output tray
- Not available
- Offline
- Overdue maintenance
- Paper jam
- Paper low
- Paper out
- Toner low
- Toner out
- Unreachable
- Warning

You can select one or more fault types in the Alert Rule criteria. If a selected fault occurs on a device to which you assigned the Alert Rule, the **Action** options are applied. If you want to receive separate alerts for more than one type of fault per device, you must create a separate rule for each fault type, then apply the rules to each device as needed.

Note Although you can select multiple fault types, as a best practice limit each rule to a single fault only. An alert is triggered only when a status change is detected while the device is in its “ready” state. If one fault triggers an alert, and another fault is triggered before the device resets to “ready” a second alert message is not generated. Instead, ensure that you select a single fault type per alert rule.

If you want to receive notification of a fault only if the fault continues to occur for a period of time, you can set the **Fault active for** field. For example, if you want to receive notification when devices are Unreachable for five minutes or more, set the Fault active to 5 minutes. If the device was unreachable only for a reboot, it is likely that the device comes back online before 5 minutes is exceeded. The notification message is sent only when the Unreachable status persists for the period of time you indicate. Use this setting to minimize the possibility of a false alarm, and eliminate the need for an Administrator to follow up on false alarms.

Alternatively, you can hold the notification message until the same fault has occurred a set number of times. For example, if you want to monitor a device for recurring paper jams, you can set the number of occurrences to 5 jams over the course of 2 days. The notification is sent only when these conditions are met, rather than each time there is a paper jam on the device.

An alert is a one-time event. Once DME performs the Action dictated by the alert rule, the notification is sent just once. If you want to be notified more than once of a particular status change, you can use the **Fault active for** or **At least** options. For example, if users within your organization are expected to fix paper jams themselves, you might want to be notified when the paper jam first occurs, then every 5 minutes. After 20 minutes, you fix the jam yourself, or call someone to do it. To accomplish this, create the following alert rules, and apply them all to the device:

| Rule Name | Fault | Fault Active for |
|------------------------|-----------|------------------|
| Paper Jam | Paper Jam | 0 minutes |
| Paper Jam - 5 minutes | Paper Jam | 5 minutes |
| Paper Jam - 10 minutes | Paper Jam | 10 minutes |
| Paper Jam - 15 minutes | Paper Jam | 15 minutes |
| Paper Jam - 20 minutes | Paper Jam | 20 minutes |

Creating custom alert messages

Alert Messages use standard default message text unless you specify a custom message. Within the custom message window, enter the text and substitution values you want the notifications to contain.

DME replaces the substitutions used with the actual fault type, occurrence, duration, or device type values that are logged for the fault condition that cause the notification. For example, the notification message sent to the user might state:

```
"Warning: A paper jam has occurred 5 times on the HPLaserJet."
```

Custom messages can contain any desirable text, plus the variable substitutions described in the table below.

| Substitution | Description |
|--------------|--|
| %1 or %f | Inserts the fault type that triggered the alert. Fault types may be: Down, Offline, Paper Jam, Paper Low, Paper Out, Toner Low, Toner Out, Unreachable or Warning. |
| %2 or %o | The number of times the fault has occurred. If your Alert Criteria uses the At least field, include the number of occurrences within the message. |
| %3 or %t | The length of time the fault has been active. Duration is calculated using the start time field logged in the DME database when the fault first occurred. If your Alert Criteria uses the Fault active for criteria, include this information in the message. |
| %4 or %n | The name of the device on which the fault occurred. |
| %i | The IP Address of the device on which the fault occurred. |
| %l | The physical location of the device on which the fault occurred. |
| %d | The description of the device, as created in Web System Manager, on which the fault occurred. |

Assigning alerts to devices

Alert Rules are effective only after you apply them to one or more devices within the DME Console.

1. To assign a rule, right-click on a device in the Devices view and select **Assign alert rules** from the menu.
2. From the list of available alert rules, select as many rules as you want to apply to the device, and click **OK**.

To view the Alert rules applied to a device, click on a device Hostname to open the Device Properties dialog box. In the properties dialog box, click the Alert rules link, open the **Alert rules** dialog box.

Generating device status reports

Reports Manager provides device status reports that you can use to analyze device health over time.

1. To view these reports, open Reports Manager and expand the **Analysis** list.
Use the following table to determine what report to run.

| Report name | Report contents | When to run the report |
|----------------------|--|---|
| Device availability | <ul style="list-style-type: none"> • % offline • % online • % unreachable | Determine the percentage of time a device is offline or unreachable. |
| Device configuration | <ul style="list-style-type: none"> • Device name • Device type • IP Address | Determine the full suite of devices controlled and tracked by Equitrac. |

| Report name | Report contents | When to run the report |
|------------------------|--|---|
| | <ul style="list-style-type: none"> • Manufacturer • Model | |
| Device faults | <ul style="list-style-type: none"> • Total • Down • Unreachable • Warning | Determine if a service call may be required for particular devices based on how often the device is down, unreachable, or in a warning state. |
| Device faults vs usage | <ul style="list-style-type: none"> • Total Faults • Total Pages • Faults per 1000 pages | Determine how often a device is down in direct relation to the amount of usage on the device. |

- Click on the report you want to view. The **Select report criteria** dialog box opens.
 - Select a time frame to run the report from the **Date** drop-down list.
 - Select the number of events to view from the **Limit** drop-down list.
- Click **OK** to open the report.

Change status report contents

You can change the default contents displayed in a report to suit your tracking needs.

- To change the report contents, select **View > Configure Report Layout**.
- From the **Columns to display** list, select the categories you want in the report. The defaults are pre-selected from the list.
- The **Label** field displays the default name that corresponds to the selection. You can use the default or enter a custom label for the column.
- The **Width** field represents the percentage of how wide the column appears in the overall width of the report. You can set the column width as you desire, but if the selection exceeds 100% of the report's total columns width, a **Configure report layout** warning pops up.

If the warning appears, you have three options:

| Option | Results |
|--------|---|
| Yes | Automatically adjusts the new and existing columns to add up to 100% of the overall report width. |
| No | Exits without adjusting the column widths to equal 100%. The column is added to the report, but since it exceeds the total columns width, it does not display |
| Cancel | Return to layout dialog box and enter a different value. |

Print Queue Viewer

The Print Queue Viewer provides a tool for Administrators to view and delete documents within the secure print queue. Each DRE has its own print queue, and therefore its own Viewer. If you deployed multiple DREs you can run multiple Viewers at the same time. You must specify the print server (DRE) you want to connect to when you launch the Viewer.

The Print Queue Viewer utility is installed as part of the management tools when Equitrac is installed on your system. The EQPrintQueueViewer.exe file is placed in the **Program Files\Nuance\Equitrac\Tools** folder, and a shortcut is created in the Equitrac group under the Windows Start menu.

To open the Print Queue Viewer, do the following:

1. Go to **Start > All Programs > Kofax > Print Queue Viewer**.
2. Double-click the Viewer icon in the Windows task tray to open the Print Queue Viewer.
3. Click any document in the list to select it. Hold down shift or ctrl to select multiple documents in the queue.

You can sort documents in the list by clicking any of the column headings visible in the Viewer.

4. To delete selected documents from the queue, press the **Delete** key or choose Delete from the Document menu.

Select **View > Simple view** or **View > Full view** to change the default view depending on how many document details you want to display.

Note Start the Print Queue Viewer with the `-s` option to customize Viewer's visible columns. Select *View > Custom view*, and then select *View > Select columns* to select or clear columns as desired.

Select **View > Hide** to close the Viewer without shutting down the service. The Viewer icon remains visible in the Windows Task tray. Use the Refresh option to update the Viewer document list while the Viewer is open; the list does not refresh automatically.

To shut down the service, right-click the icon in the task tray and select **Exit**. You can also select Show/Hide to open or close the Print Queue Viewer window.

Running Print Queue Viewer on a workstation

To run the Print Queue Viewer application on a workstation, choose one of the following options:

- Use Equitrac Installer with one of the management tools, such as Web System Manager. The EQPrintQueueViewer.exe file is placed in the **Program Files\Nuance\Equitrac\Tools** folder, and a shortcut is automatically created in the Equitrac group under the Windows Start menu.

-Or-

- Copy the EQPrintQueueViewer.exe file to the workstation.
When manually copying EQPrintQueueViewer.exe you need to run it with the -s<DRE_server> option if you want to customize the Print Queue Viewer columns, and to view other user's print jobs.

If the -s<DRE_server> option is not used, then the Print Queue Viewer only shows print jobs for the current user. After running EQPrintQueueViewer.exe, a shortcut is created in the Equitrac group under the Windows Start menu.

Campus Card interface

Equitrac allows users to swipe a Campus Card at a release endpoint as a method of payment from a third-party account using the Campus Card (also called Foreign Accounting System or FAS) functionality. The bridge between Equitrac and a Campus Card system is the Campus Card interface.

Note Equitrac currently integrates with Blackboard, CBord Odyssey and CBord CS Gold interfaces. Any system can be integrated using the Campus Card API, as described in the [Campus Card API Reference Guide](#).

Equitrac users can authenticate themselves as valid Campus Card account holders at embedded devices, make copies, release jobs, and pay for these services in real time directly from their Campus Card accounts.

You can configure CAS to cache Campus Card IDs, tender keys (if available) and transactions when the Campus Card system is offline. CAS stores offline transactions while the Campus Card system remains unavailable. When the Campus Card system is back online, the cost of the offline transactions are applied against the appropriate account (and tender key).

Configuring a Campus Card interface

To configure a Campus Cards interface, do the following:

1. Go to **Start > All Programs > Kofax > Equitrac > System Manager**.
2. Select **Configuration > Campus card interface**.

Note The following example displays Campus Card interface dialog box of Windows System Manager when Campus Card interface is not configured.

The following example displays Campus Card interface dialog box of Windows System Manager when Campus Card interface is selected.

3. Select a Campus Card interface from the Campus Card System drop-down list.

Note Blackboard IP, CBORD CS Gold and CBORD Odyssey interfaces are already available with Equitrac. If you create and deploy a new interface using the Campus Card API, as described in the Campus Card API Reference Guide, it is also selectable.

To configure the details of the selected interface, click the **Configure...** button. A configuration dialog box of the selected Campus Card interface appears. Configuration details of the built-in interfaces are described further below.

If the CBORD CS Gold interface, the CBORD Odyssey interface or an interface created by the Campus Card API is selected, the following additional options are applicable:

| Campus card interface option | Description |
|--------------------------------|--|
| Charge before copy | <ul style="list-style-type: none"> • When enabled, this feature validates account information and charges the user account for a requested copy transaction prior to starting the copying. |
| Disable server temporarily | <ul style="list-style-type: none"> • When enabled, this feature disables communication between CAS and the selected Campus Card interface. • When disabled, this feature disables CAS to upload transactions or validate account data—such as when performing maintenance on the Campus Card system. |
| Card swipe only | <ul style="list-style-type: none"> • When enabled, CAS uses the selected Campus Card interface only if authentication was performed with swiping a card. |
| Forward password (if provided) | <ul style="list-style-type: none"> • When enabled, CAS sends the secondary identifier to the selected Campus Card interface. This option has impact only if the controller or the embedded device client asks for a secondary PIN based on the Secondary prompt option of User authentication. |

4. Select **Enable offline account caching** to allow users to login when the Campus Card system is offline.
 - a. Enter a **Maximum offline balance** for users while the Campus Card system is offline. The user is refused further activity once the balance reaches zero or the cost of the job exceeds the remaining balance.
 - b. Enter the **Account expiry time** (in minutes) for how long the user’s offline account is active.
 - c. Enter the **Transaction posting interval** (in minutes, with a 15 minute minimum) for CAS to check if the Campus Card system is back online and to post any offline transactions.

While the Campus Card system is offline, you can manually check its status, or delete any cached accounts and transactions, using the following options:

- **Process cache now** – Temporarily overrides the Transaction posting interval to check the Campus Card system status. If the Campus Card system is still offline, the Transaction posting interval resets to the time entered in the field.
- **Purge cached transactions** – Deletes all unprocessed cached Campus Card transactions.
- **Purge cached accounts** – Deletes all cached Campus Card accounts.

5. Select **Enable user registration prompt** to allow users to register an unrecognized Campus Card for future use.

To complete the card registration, the user is required to login with valid network ID and password. Once the card is registered, the user is able to log in as normal without being prompted for their login credentials.

Note If the user skips card registration (e.g. by entering a blank User name) or if registration fails, then the user can still log in as normal, however, the user is not able to release print jobs unless they are prompted for a Release Key.

Only a valid Campus Card account (i.e. with available funds) can be associated with a user ID in CAS.

The registration process does not record the Campus Card account number as the user's Primary PIN. Instead it records it in a separate table in CAS—the same table populated by the CampusCardImport.exe utility. See [Import Campus Card Account Information](#) in the *Kofax Equitrac® Administration Help file*.

A user may only register one card against their user ID. Registering a new card will overwrite an existing card.

6. To remove users from the Campus Card mapping table in CAS, do the following:
 - Select **all** from the drop-down list, and click **Delete** to remove all users.
 - Select **by user name or by card ID** from the drop-down list, enter the associated user name or card ID in the text field, and then click **Delete** to remove users individually.

A Campus Card Holding Account is created in Accounts Manager after the Campus Card is used for the first time. This account acts as a system audit log to capture all activity from card swipes.

Blackboard IP interface

To configure the Blackboard IP Interface, do the following:

1. In the **Campus Card System** drop-down list, select **Blackboard IP interface**.
2. Click **Configure** to open the Blackboard IP Interface dialog box.
3. Complete the following fields:

| Option | Details |
|------------------------------------|---|
| Host | IP address or host name of the Blackboard server. Equitrac confirms the address and displays the port number and interface version. |
| Disable Server | When selected, this feature disables communication between CAS and the Blackboard server. Disable temporarily when you do not want CAS to upload transactions or validate account data—such as when performing maintenance on the Blackboard server. |
| Enable Encryption & Encryption key | Enable if your Blackboard configuration requires encryption for account data. Provide the encryption key. |
| Terminal number | Enter a unique terminal number for Equitrac. |

| Option | Details |
|--------------------|--|
| | Blackboard treats Equitrac as an individual terminal. Enter the same number you assigned to Equitrac during the Blackboard configuration. |
| Tender Keys | <p>If your Blackboard configuration uses tender keys, click Add to enter one or more new keys.</p> <p>Equitrac treats each tender key associated with a FAS account as a separate account when displaying accounts to a user signing on at an embedded device. After the user swipes his or her card at the embedded device, Equitrac checks for a FAS account. If it finds a single account, the user may proceed with printing as usual. If Equitrac finds either multiple matching accounts, or an account with tender keys, the embedded device displays the matches in a list, and the user can select the appropriate account or tender key.</p> |
| PINs required | When this option is enabled in combination with the Control terminals > Swipe any campus card for payment option, then the user is prompted for a secondary PIN after swiping for payment, and the secondary PIN is validated by the Blackboard server. |
| Charge before copy | When enabled, this feature validates account information and charges the user account for a requested copy transaction prior to starting the copying. |

After the configuration is complete, you may import the Blackboard account information into the CAS database. See [Import Campus Card Account Information](#) in the [Kofax Equitrac® Administration Help file](#).

CBORD Odyssey interface

To configure the CBORD Odyssey interface, do the following:

1. In the **Campus Card System** drop-down list, select **CBORD Odyssey interface**.
2. Click **Configure** to open the CBORD Odyssey interface dialog box.
3. Complete the following fields:

| Option | Details |
|-----------------|--|
| Host | IP address or host name of the CBORD server. |
| Port Number | Enter the port number that Equitrac should use to communicate with the CBORD server. |
| Terminal number | <p>Enter a unique terminal number for Equitrac.</p> <p>CBORD treats Equitrac as an individual terminal. Enter the same number you assigned to Equitrac within the CBORD configuration.</p> |
| Vendor | A unique number assigned to each system console operator. In addition to the terminal number, this allows auditing the performance of each operator. |
| Tender Keys | <p>If your CBORD configuration uses tender keys, right-click on the table to add or remove tender keys.</p> <p>Equitrac treats each tender key associated with a FAS account as a separate account when displaying accounts to a user signing on at an</p> |

| Option | Details |
|--------|--|
| | embedded device. After the user swipes his or her card at the embedded device, Equitrac checks for a FAS account. If it finds a single account, the user may proceed with printing as usual. If Equitrac finds either multiple matching accounts, or an account with tender keys, the embedded device displays the matches in a list, and the user can select the appropriate account or tender key. |

After the configuration is complete, you may import the CBORD Odyssey account information into the CAS database. See [Import Campus Card Account Information](#) in the [Kofax Equitrac® Administration Help file](#).

CBORD CS Gold interface

To configure the CBORD Odyssey interface, do the following:

1. In the **Campus Card System** drop-down list, select **CBORD CS Gold interface**.
2. Click **Configure** to open the CBORD CS Gold interface dialog box.
3. Complete the following fields:

| Option | Details |
|-----------------|---|
| Host | IP address or host name of the CBORD server. |
| Port Number | Enter the port number that Equitrac should use to communicate with the CBORD server. |
| Use SSL | Enable to use Secure Socket Layer communication between Equitrac and CBORD. |
| Terminal number | Enter a unique terminal number for Equitrac. CBORD treats Equitrac as an individual terminal. Enter the same number you assigned to Equitrac within the CBORD configuration. |
| Provider | Indicates the provider or the Data Xchange license. |
| Location | Enter the location from where the transaction occurs. |
| Account Name | The name of the user account displayed on the embedded device. |

After the configuration is complete, you may import the CBORD CS Gold account information into the CAS database. See [Import Campus Card Account Information](#) in the [Kofax Equitrac® Administration Help file](#).

Working with Campus Card

The Equitrac Campus Card feature enables users to login to an embedded device by either swiping a Campus Card or entering their login credentials (e.g. primary PIN) using the device's keypad.

Using Campus Cards with embedded devices

To login with Campus Card at an embedded device, do the following:

1. Configure a Campus Card system in Windows System Manager as described in [Print Queue Viewer](#).
2. Swipe the Campus Card at the card reader attached to the embedded device or enter the associated login credentials.

Note If Secondary prompt is configured in Web System Manager > Configuration > Security and authentication > User authentication, a Secondary PIN is also needed.

3. Select the desired account if multiple accounts with funds are available. A Campus Card account may have several tender keys (similar to purses). In this case, CAS handles them as separate Campus Card accounts.

A CAS account can be selected when:

- The primary identifier of the Campus Card account has been imported and an Equitrac User ID was assigned to it with CampusCardImport.exe. See [Import Campus Card Account Information](#) in the [Kofax Equitrac® Administration Help file](#) for further details.
- The administrator of the Campus Card system being used has associated an Equitrac User ID for the Campus Card account in the Campus Card system which is returned with the Campus Card account.
- The primary identifier also detects an Equitrac account.

Cashier

Cashier is an Equitrac administrative tool used to adjust balances on user, department, and billing codes. Designed for use by staff members who perform a role similar to a library cashier, the staff member can collect money from a user then use Cashier to deposit the equivalent amount into the user's Equitrac printing account. When you launch the Cashier application, you need to select the Accounting Server you want to work with. CAS processes the account transactions you perform using Cashier, updating balances and writing transaction information to the accounts database.

To use Cashier, staff members must be granted Cashier Access Permissions. Generally, you should create a separate Domain group that contains only the staff members who will use Cashier. Then, open **Web System Manager > System Configuration > Global Configuration Settings > Security and Authentication > Access Permissions**, and add the new Domain group to the Cashier permission. For more information on permissions, see [Application-level Access Permissions](#) in the *Kofax Equitrac® Administration Help* file.

Equitrac stores connections between Cashier and the accounting server separately for each logged-on administrative user. Each Cashier user must connect to the accounting server to manage the accounts database.

Using Cashier

Cashier can be installed on any server station within the Equitrac deployment.

To use Cashier, do the following:

1. Go to **Start > All Programs > Kofax > Cashier**.
2. Select **Search > Criteria** from the Toolbar to configure the search criteria.
3. In the Search Criteria dialog box, do the following:
 - a. Select the **Account type – User, Department, or Billing Code**.
 - b. Select the search **Field** for the Account type:
 - For User – select **User ID, Full name, or Primary or alternate PIN**.
 - For Department and Billing Code – select **Name, Description, or Primary PIN**.
 - c. Select the **Match criteria** for the Field:
 - For User ID, Full name, Name, and Description – select **Prefix or Containing**.
 - For Primary or alternate PIN and Primary PIN – **Match** is the only option.
 - d. Click **OK** to save the search criteria.

4. Enter a search criteria in the **Find** field, then click **Search**.

Note If the search criteria is set to find a User Primary or alternate PIN, then card readers configured as keyboard emulators can be used to populate the Find User PIN match field. A leading ^ or ` character as well as a trailing ; character will be ignored when using a card reader in keyboard emulation mode.

Note Before swiping a card, ensure that the cursor is in the Search field first.

5. Select an account from the list.
6. Enter the Transaction **Paid amount**. The funds are transferred into the selected account's Paid balance.
Amounts can be positive or negative. To enter a negative amount to remove funds from the account, use a minus (-) sign before the amount.
7. Enter a **Comment** for the transaction.
By default, the user is required to enter a comment before the Record button is enabled. However, the Administrator can change the **Cashier behavior** option which allows staff members to record the transaction without a comment.
Go to **Web System Manager > System Configuration > Global Configuration Settings > User Interaction > Billing Code Access, Cashier Behavior and Error Notification > Cashier Behavior** and uncheck the **Require comment by user** option.
8. Click Record to update the account balance.
The new balance displays in the **Paid balance** and **Total balance** columns.
9. Print the receipt (optional).
The user is prompted to select a printer where the receipt will be printed. If the user presses cancel, the receipt is not printed.

Modifying the printed Cashier receipt

Administrators can modify the contents of the printed receipt. A standard receipt is installed in the same folder as the Cashier executable (**Program Files\Nuance\Equitrac\Tools\cashier.html** by default).

To customize the receipt contents, modify the html file, but ensure that the file name remains "cashier.html". You can add or replace the variables in the file with any of the following substitutions:

| Variable | Result |
|----------|--|
| %a | Prints the date in the default date format. |
| %b | Prints the account balance. |
| %c | Prints the amount of the last transaction performed on the account. |
| %f | Prints the User's full name |
| %r | Prints the transaction comment. If no comment was entered for the transaction, "Cashier transaction" is printed. |
| %t | Prints the time. |

| Variable | Result |
|-----------------|---|
| %u | Prints the name of the staff member who is logged into the Cashier application (using the network User ID). |
| %w | Prints the Cashier workstation name. |
| %z | Prints the opening balance (prior to recording the last transaction). |
| %% | Prints the percentage % character. |

Note To turn the receipt option off, either delete or rename the cashier.html file to any other name. The receipt option will not appear to the user if the application is unable to locate this file.