

# **PrintFleet Optimizer**

**Version 3.13.0**

**User Guide**



*PrintFleet Optimizer User Guide*

The content of this user manual has been created for informational use only, and is subject to change without notice.

Except as permitted by license, no part of this publication may be reproduced or transmitted, in any form or by any means, electronic, mechanical, recording, or otherwise, without the prior written permission of PrintFleet Inc.

PrintFleet®, PrintFleet Enterprise™, PrintFleet Optimizer™, PrintFleet Vision®, PrintFleet DCA Pulse™, PrintFleet QuickAssess™, and PrintFleet LINK® are trademarks of PrintFleet Inc.

VERISIGN and thawte are registered trademarks of VeriSign in the United States and/or other countries.

Microsoft, Windows, Internet Explorer, and SQL Server are trademarks or registered trademarks of Microsoft Corporation in the United States and other countries.

Canon is a registered trademark of Canon Inc.

Digital Gateway and e-automate are trademarks or registered trademarks of Digital Gateway Inc.

OMD, OMD Vision, NetVision, and OMD iManager are registered trademarks of OMD Corporation.

Evatic is a trademark or registered trademark of Evatic AS.



Revision 3.13.0

©Copyright 2020 ECi Software Solutions Canada Inc. d/b/a PrintFleet® Inc. All rights reserved.

# Table of Contents

---

<b>Chapter 1</b>	<b>Introduction .....</b>	<b>1</b>
1.1	Device Support .....	1
1.2	Introduction to the PrintFleet Optimizer Interface .....	2
	Logging in to the system .....	3
	Resetting a password .....	3
	Using the search function.....	4
	Accessing the PrintFleet knowledgebase.....	4
1.3	Software Updates .....	4
1.4	Contacting Technical Support .....	5
<b>Chapter 2</b>	<b>Device Views .....</b>	<b>6</b>
2.1	Working with Device Views .....	6
	Viewing data using device view.....	6
	Sorting data.....	6
	Filtering data by management status.....	7
	Filtering data by device type .....	7
	Filtering data by last active date .....	8
	Filtering data by supply .....	9
	Filtering data by last supply request .....	11
	Enabling the last supply request filter .....	12
	Filtering data by text.....	13
	Removing the text filter.....	13
	Removing a filter from a device view .....	13
	Removing all filters from a device view .....	13
	Resizing column widths in a device view.....	13
	Resetting a column to the default width .....	14
	Resetting all columns to the default widths.....	14
	Navigating among pages of items within a device view .....	14
	Working with the default views .....	14
	Device states .....	15

Using the Technical View .....	15
Using the Supplies Order View .....	16
Requesting supplies .....	17
Using the Maps View .....	19
Uploading a new map.....	19
Place imaging devices on a map .....	20
Placing computing devices, people, icons on a map .....	20
Moving an imaging device image or other icon .....	21
Removing an imaging device image or other icon .....	21
Rotating or flipping a map.....	21
Changing a map image or title.....	21
Downloading a map image .....	22
Using the Alerts View .....	22
Creating custom device views.....	23
Editing a custom device view.....	24
Deleting a custom device view .....	24
Creating a device view override .....	24
2.2 Working with the Device Detail page .....	24
Accessing the Device Detail page .....	25
Working with the Overview tab .....	26
Changing the model associated with a device.....	28
Working with the Meters tab .....	29
Working with the Supplies tab .....	30
Working with the Attributes tab .....	31
Working with the Alerts tab.....	31
Working with the Codes tab .....	32
Working with the Notes tab.....	34
Working with the Metric History page.....	34
<b>Chapter 3</b>	
<b>Reports .....</b>	<b>37</b>
3.1 Overview of Reports.....	37
Types of reports .....	38
3.2 Accessing report definitions.....	39
Sorting report definitions .....	39
Filtering report definitions .....	39
3.3 Report options .....	40
3.4 Creating Report Definitions .....	50
Creating a Standard report definition .....	50
Creating an Executive report definition .....	52

	Using Variables in Titles, Subtitles, and Comments .....	54
3.5	Specifying Report Parameters.....	55
	Changing the access settings for a report definition .....	55
	Running a report definition.....	57
3.6	Viewing and saving reports .....	57
	Saving a report in Adobe PDF .....	57
	Save a report in tab-separated values format .....	57
	Saving a report in comma-separated values format .....	57
3.7	Scheduling Reports .....	58
3.8	Managing Report Definitions.....	59
	Editing a report definition .....	59
	Copying a report definition.....	59
	Deleting a report definition .....	60
3.9	Managing Report Schedules .....	60
	Managing schedules for a specific definition .....	60
	Viewing the schedules for a specific report definition.....	60
	Editing a schedule for a report definition .....	60
	Deleting a schedule for a report definition .....	61
	Managing schedules for multiple definitions .....	61
	Viewing the report schedules.....	61
	Editing a report schedule .....	61
	Deleting a report schedule .....	62
3.10	Working with Date Variables .....	62
	Specifying date parameters when running a report .....	62
	Specifying date parameters when scheduling a report.....	64
	Scheduling an Executive Report.....	67
3.11	Report Security .....	67
	Security for report definitions.....	68
	Managing shared report definitions.....	68
	Restricting access by role .....	69
	Security for sample report definitions .....	69
	Security for report schedules.....	69

<b>Chapter 4</b>	<b>Alerts .....</b>	<b>70</b>
4.1	Overview.....	70
	Alert notifications .....	71
4.2	Alerts Security .....	71
	Advanced security .....	71
	Possible security scenarios .....	72
4.3	Creating Alert Definitions.....	72

4.4	About Alert Conditions.....	75
	Supply alert conditions .....	75
	Adding a supply condition to an alert definition .....	77
	Adding an EDTE to a supply alert definition .....	78
	Error code alert conditions.....	78
	Adding an error code condition to an alert definition.....	81
	Stale DCA alert conditions.....	81
	Adding a Stale DCA condition to an alert definition .....	81
	Activated DCA alert conditions .....	82
	Page count recurring alert conditions .....	83
	Adding a page count recurring condition to an alert definition.....	84
	Date recurring alert conditions.....	84
	Adding a date recurring condition to an alert definition .....	84
	Combining multiple error code conditions .....	85
4.5	Managing Alert Definitions .....	85
	Viewing the alert definitions .....	86
	Editing alert definitions.....	86
	Disabling and enabling alert conditions .....	86
	Deleting alert definitions.....	87
4.6	Working with Alert Emails .....	87
4.7	Working with Alert Webhooks .....	88
4.8	Supplies Notification .....	89
	Possible supplies notification workflow .....	89

<b>Chapter 5</b>	<b>Settings.....</b>	<b>90</b>
5.1	Changing Preferences.....	90
5.2	Managing Groups .....	92
	Creating, editing, and deleting groups .....	92
	Create a new group .....	92
	Editing users and device counts for a group.....	93
	Viewing users and device counts for a group .....	93
	Creating a DCA key for the group .....	93
	Deleting a group.....	93
	Assigning devices to groups .....	94
	Managing group types .....	95
	Create a new group type .....	95
	Creating a new group by copying an existing group .....	96
	Editing a group type.....	96
	Deleting a group type.....	97
5.3	Managing Devices.....	97

	Management status .....	99
	Editing device information as a group .....	100
	Adding or editing device information on a group-wide basis .....	100
	Editing device information.....	100
	Adding or editing device information for an individual device.....	100
	Device- reported values.....	101
	Creating custom device fields .....	101
	Creating a custom device field .....	102
	Group inheritance.....	102
	Viewing inherited attributes .....	103
	Editing a custom device field .....	103
	Removing a custom device field .....	103
	Editing device status as a group .....	104
	Adding or editing device status on a group-wide basis .....	104
	Editing the management status for one or more devices.....	104
5.4	Virtual Meters .....	105
	Creating a virtual meter .....	105
	Editing a virtual meter .....	105
	Copying a virtual meter .....	106
	Deleting a virtual meter.....	106
	Adding Priority Levels to Virtual Meters.....	106
5.5	Configuring Meter Exports.....	106
	Configuring a meter export system .....	107
	Creating a new meter export configuration.....	108
	Configuring meter maps .....	111
	Creating a new meter map.....	112
	Editing a meter map .....	112
	Using Priority Meters in Meter Mapping .....	113
	Deleting a meter map .....	113
	Viewing the log for a meter map .....	113
	Setting up meter export schedules .....	113
	Creating a new meter export schedule.....	114
	Editing a meter export schedule.....	115
	Deleting a meter export schedule.....	116
	Viewing the log for a meter export schedule .....	116
	Running a meter export schedule.....	116
	Configuring device maps (exceptions only).....	117
	Mapping PrintFleet devices to ERP system devices .....	117
	Testing and troubleshooting .....	117

	Manually forcing a meter export to occur .....	118
	Viewing the meter export log .....	118
6.1	Managing Users.....	122
	Viewing existing users.....	122
	Creating a new user account .....	122
	Creating a user account with duplicate permissions .....	124
	Editing an existing user account.....	124
	Deleting a user account.....	124
	Disabling a user account.....	125
6.2	Exporting and Importing Device Data .....	125
	Exporting device information .....	125
	Importing device information .....	126
6.3	Branding the User Interface .....	127
	Customizing the product logo .....	127
	Customizing the Executive Report cover.....	128
	Customizing Interface Colors.....	129
	Customizing the product name .....	130
	Customizing the login page .....	130
6.4	DCA Installations.....	130
	Installing DCA Pulse .....	131
	Installing DCA Pulse on Raspberry Pi .....	133
	Installing DCA 4.x.....	135
	Manually preconfiguring scan settings.....	137
	Manually preconfiguring scan settings now .....	137
	Downloading the simplified DCA installer.....	138
	Downloading the Manual Installer .....	141
	Checking the status of a DCA .....	142
	Viewing DCA information .....	142
	Updating multiple DCAs.....	142
	Viewing software update status .....	143
	Viewing update status of selected DCAs .....	144
	Disabling and deleting a DCA.....	145
	Enabling and reactivating a DCA .....	146
6.5	Configuring Scan Settings.....	146
	Viewing Scan Configuration settings .....	146
6.6	DCA 4.x: Managing Scan Profiles .....	148
	Creating Scan Profiles .....	149
	Specifying multiple scan ranges.....	150
	Specifying which devices to scan.....	151

	Editing scan profiles .....	151
	Deleting scan profiles .....	151
	Setting network timeouts.....	152
	Setting SNMP retries .....	153
	Setting Web Page scraping timeouts.....	154
	Setting Focus Scans .....	155
	Setting scan types .....	156
	Storing SNMP community strings .....	156
	Using SNMP Version 3 .....	157
6.7	DCA Pulse: Managing Scan Configuration .....	159
	Adding a Scan Range .....	159
	Configuring Scan Intervals .....	159
	Configuring Security: SNMP Version 1/2.....	160
	Configuring Security: SNMP Version 3.....	161
	View Security Configuration Details .....	164
	Delete a SNMP Profile.....	164
	Configuring Communication .....	164
	Configuring Logs .....	166
6.8	Understanding PrintFleet Security .....	170
	Basic group/ role assignment .....	170
	Group inheritance.....	170
	Role inheritance .....	171
	Reports security .....	171
6.9	Troubleshooting Stale Data Issues .....	172
6.11	Distributing Software Updates .....	173

# Chapter 1 Introduction

---

Welcome to PrintFleet Optimizer—a complete remote print management system designed to help owners, sales representatives, service technicians, and administrative personnel grow and streamline their business.

This guide covers all aspects of using PrintFleet Optimizer and administrating the PrintFleet Optimizer system, including:

- "Device Views" on page 6
- "Reports" on page 41
- "Alerts" on page 75
- "Settings" on page 95
- "Administrating PrintFleet Optimizer" on page 127

While this guide will discuss management of DCA 4.x as well as the new DCA Pulse, we encourage you to refer to the *PrintFleet DCA User Guide* for more detailed information.

---

**Note**

DCA Pulse requires PrintFleet Optimizer 3.9.0 or higher to run.

---

## 1.1 Device Support

PrintFleet strives to develop vendor-neutral software products, and to support as many models of printers, copiers, fax machines, and multifunction peripherals as possible. However, our products do not support all models available in the market. PrintFleet is continuously adding model support into our software products.

Supported models are not all supported to the same extent. For example, one model may be supported for all available data types, while another may only be supported for specific data types, such as device description and life page count.

PrintFleet software products collect information from networked imaging devices. Standalone devices are not supported. Locally connected devices can be partially supported by using the PrintFleet Local Print Agent add-on application available for install with DCA 4.x.

If you find a model that is not currently supported, contact PrintFleet to inquire about possible future support. If you are a direct client you can contact PrintFleet Technical Support.

The following table lists the data types that the DCA attempts to collect from networked imaging devices during a network scan.

### Types of data collected by the DCA

IP address	Toner cartridge serial number
Device description	Maintenance kit levels
Serial number	Non-toner supplies
Meter reads (multiple)	Asset number
Monochrome or color identification	Location
LCD reading	MAC address
Device status	Manufacturer
Error codes	Firmware
Toner levels	Miscellaneous (machine specific)

The Local Print Agent collects the following data types:

- Device driver name
- Device manufacturer
- Communications port

<b>Note</b>	Additional data collection (such as counts, toner level, and supplies) from local devices depends on the data the device itself supports.
-------------	---

## 1.2 Introduction to the PrintFleet Optimizer Interface

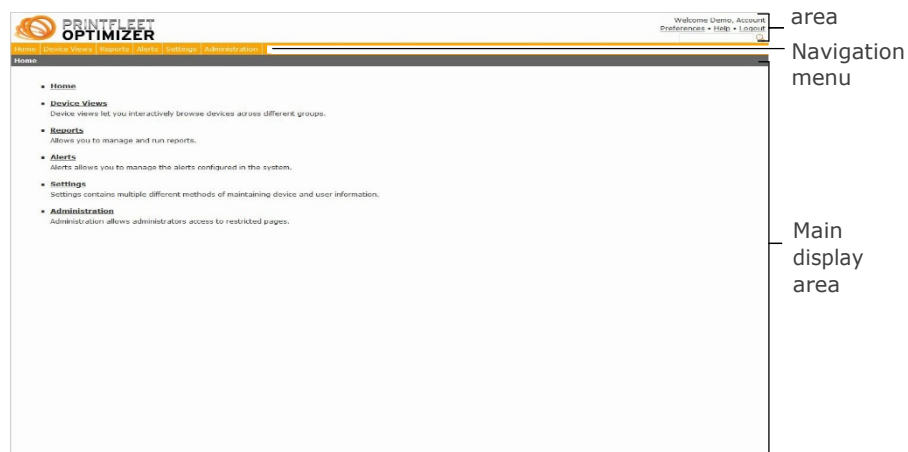
The PrintFleet Optimizer web interface is the primary means by which users view collected imaging device data, configure reports, and manage the system.

The PrintFleet Optimizer interface makes it easy to access the information you need from anywhere with an Internet connection.

The PrintFleet Optimizer interface has three main components:

- The header area
- The navigation area
- The main display area

The specific items displayed in each area, as well as what is displayed on the home page, will depend on the specifications of the user account.



PrintFleet Optimizer Interface

For more information on user accounts, "Managing Users" on page 127.

## Logging in to the system

Each user is assigned a unique user name (typically an email address) and password to log in to the system. See "Managing Users" on page 127.

### Procedure

1. In your browser window, navigate to your designated URL, such as `https://secure.printfleet.com`.
2. Enter your user name and password in the designated boxes, and then click **Login**.

If you have forgotten your password, you can request a password reset if your user name is an email address.

## Resetting a password

If you forget your password, you can request a password reset.

### Procedure

3. Enter your user name (must be an email address for this to work) in the designated box on the login page.
4. Enter one or more characters in the password box.
5. Click **Login**.
6. Click **Forgot Password** (this will appear after a failed login attempt).
7. Click **OK** in the dialog box that states *Are you sure you wish to reset your password?*

8. Check the inbox of the email address used to login.

**Note**

While we strive to support all popular browsers, we recommend that you use the latest version.


Windows Internet Explorer 10 is the minimum requirement for PrintFleet Optimizer 3.9.0. You may also use Windows Edge, or the latest version of Chrome, FireFox or Safari. Staying current will result in a significantly improved user experience, due to improved speed and standards compliance.

The first time you log in, you will see the End User License Agreement. After this is accepted once, it will not be shown again.

## Using the search function

The search function allows you to quickly find specific items in the system.

**Procedure**

1. Type your search string in the text box on the right side of the header area of the interface.
2. Press **Enter**, or click .

Results are displayed and separated into devices, groups and users.

Device results display the device name, management status, license status, group, serial number, IP address, MAC address, asset number, location, last active date and time, and a link to edit the device (if applicable to the current user). See "Managing Devices" on page 102.

Group results display the group name, parent groups, and a link to the group edit page (if applicable to the current user). See "Managing Groups" on page 97.

User results display the login name, first name, last name, last login date and time, the groups and roles assigned to the user, and links to edit, copy, or delete the user from the user edit page (if applicable to the current user). See "Managing Users" on page 127.

## Accessing the PrintFleet knowledgebase

If necessary you can easily access the PrintFleet knowledgebase where you can find additional documentation on such things as best practices, more in-depth explanations of complex concepts, and known issues.

**Procedure**

- Click the **Help** link on the right side of the header area.

## 1.3 Software Updates

New software releases are available on a periodic basis.

For information on updating the DCA, see "Downloading the Manual Installer" on page 142.

To obtain updates for PrintFleet Optimizer components other than the DCA, contact PrintFleet Technical Support.

## 1.4 Contacting Technical Support

When reporting an issue to PrintFleet Technical Support, please be sure to clearly state the nature of the problem. If applicable, please provide screen shots and supporting log files as well.

### Support - North America

Hours	Telephone	Email
8:00-17:00 Eastern Time Monday-Friday*	Toll Free: 1-866-382-8320 Option 1 Tel: 1 (613) 549-3221 Option 1	support@printfleet.com

\* Excludes holidays in the province of Ontario, Canada.

### Support - Europe, Middle East, Africa

Hours	Telephone	Email
8:30-17:00 Central European Time Monday-Friday**	Tel: +41 44 709 11 02	support-emea@printfleet.com

\*\* Excludes holidays within Switzerland.

# Chapter 2 Device Views

---

Device views let you interactively browse devices across different groups.

## 2.1 Working with Device Views

There are several default device views in PrintFleet Optimizer. You can also create unlimited custom device views that contain the precise information you want to see.

### Viewing data using device view

#### Procedure

- On the **Device Views** menu, select the device view you want to use.

For most views (Maps being the exception), a collapsible group hierarchy is displayed on the left side of the page. Select the group that contains the devices you want to view.

---

**Note**

Depending on the number of devices in a selected group, it may take a few moments for the requested information to be processed and displayed. If necessary, you can press the ESCAPE key to cancel the request, and then click somewhere else to proceed with a different action.

---

In some views you can filter the data if you want. Filtering allows you to view a subset of the devices in the selected group. You can filter devices by any of the following:

- Management Status
- Network/Local
- Last Active
- Supply
- Last Supply Request
- Text

### Sorting data

Data in a device view can be sorted. Sorting allows you to view information in ascending or descending order.

### Procedure


- Click the column title you want to sort the data by, and click again to toggle between ascending and descending order.

### Note

An arrow icon is displayed in the header of the column being sorted. The direction of the arrow indicates whether the column is currently being sorted in ascending or descending order.

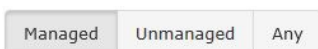
You can customize a default sort order for each view when creating or editing a view. See "Creating custom device views" on page 23.

## Filtering data by management status

If you want, you can filter devices by their management status using the filter  button.

### Procedure

- On a device view, click the filter button and select **Management Status** from the menu that appears. A filter control appears at the top of the view.



By default, the control is set to **Managed**, meaning only devices with a management status of **Managed** will be listed in the view.

- If you want to change the management status on which the view is filtered, do one of the following:
  - Click **Unmanaged** if you only want unmanaged devices to be listed in the view.
  - Click **Any** if you want both unmanaged and managed devices to be listed in the view. This is effectively the same as not filtering by management status.

## Filtering data by device type

If you want, you can filter devices by type (network or local).

### Procedure

- While on a device view, click the filter button and select **Network/Local** from the menu that appears. A filter control appears at the top of the view.



By default, the control is set to **Network**, meaning only devices of type **Network** will be listed in the view.

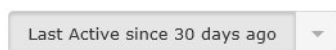
2. If you want to change the device type by which the view is filtered, do one of the following:
  - Click **Local** if you only want local devices to be listed in the view.
  - Click **Any** if you want both network and local devices to be listed in the view. This is effectively the same as not filtering by device type.

## Filtering data by last active date

If you want, you can filter devices by the date on which they were last known to be active.

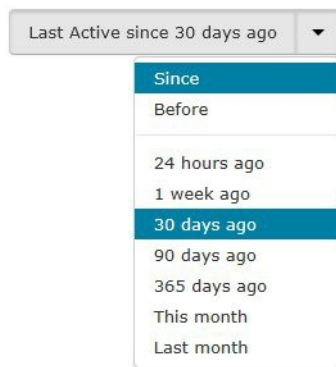
### Procedure

1. While on a device view, click the filter button and select **Last Active** from the menu that appears. A filter control appears at the top of the view.



By default, the control is set to **Last Active in the last 30 days ago**, meaning only devices with a last active date within the last 30 days will be listed in the view.

2. If you want to change the criteria on which the view is filtered, click the arrow to the right of the filter control. A menu will appear.



3. Do one of the following:
  - Choose **Since** if you only want to list devices that have a last active date that is less than the period specified in the menu. For example, if you set your filter to Last Active in the last 30 days ago, devices with a last active date which is more than 30 days ago will not be listed in the view.
  - Choose **Before** if you only want to list devices that have a last active date that is more than the period specified in the menu. For example, if you set your filter to Last Active before 30 days ago, devices with a last active date which is less than 30 days ago will not be listed in the view.

## 4. Choose one of the following periods:

- 24 hours ago
- 1 week ago
- 30 days ago
- 90 days ago
- 365 days ago
- This month

This refers to the first day of the current calendar month.

- Last month

This refers to the first day of the previous calendar month.

**To enable or disable the last active filter**

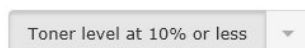
- Click the part of the filter control where the text is displayed (not the part where the arrow appears). This toggles the state of the filter from enabled to disabled and back. The appearance of the control changes to indicate the state of the filter.

**Filtering data by supply**

If you want, you can filter devices by their supplies.

**Procedure**

1. While on a device view, click the filter button and select **Supply** from the menu that appears. A filter control appears at the top of the view.



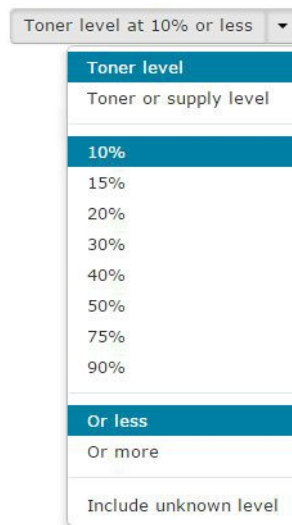
By default, the control is set to **Toner level at 10% or less**, meaning only devices with a toner level for which the last reported value was 10% or less will be listed in the view.

**Note**

If a device has multiple toner supplies (such as a color printer), and any one of those toner supplies matches the specified filter criteria, the device will be listed with all of its toner supplies, even those that did not match the specified filter criteria.

For example, if the control is set to **Toner level at 10% or less**, and a device has both a black toner at 70% and a cyan toner at 5%, the device will be listed in the view, and both the black and cyan toners will be listed along with it.

- If you want to change the criteria by which the view is filtered, click the arrow to the right of the filter control. A menu will appear.



- Do one of the following:
  - Choose **Toner Level** if you only want to list devices that have a toner level that meets the specified criteria.
  - Choose **Toner or Supply** if you want to list devices that have either a toner level or other supply that meets the specified criteria.
- Choose one of the following levels:
  - 10%
  - 15%
  - 20%
  - 30%
  - 40%
  - 50%
  - 75%
  - 90%
- Do one of the following:
  - Choose **Or less** if you only want to list devices that have at least one supply with a level that is equal to or less than the level specified in the menu. For example, if you set your filter to Toner level at 10% or less, all devices with at least one toner level at or below 10% will be listed in the view.
  - Choose **Or more** if you only want to list devices that have at least one supply with a level that is equal to or more than the level specified in the menu. For example, if you set your filter to Toner level at 10% or more, all devices with at least one toner level at or above 10% will be listed in the view.

- If you want to include all devices that have one or more levels that are unknown, choose Include unknown level.

**Note**

If you choose this option, a device will be displayed if it has at least one toner (or supply, if you chose the **Toner or Supply** option) with an unknown level, regardless of whether the other known levels for that device meet the specified level. For example, if a device has a black toner level of 60%, and a maintenance kit with an unknown level, the device would be listed even if you set the filter to show devices with supplies less than 25%.

Conversely, if you do not choose the **Include unknown level** option, that does not mean that devices with unknown levels will be excluded. Such devices would still be displayed if they had other toner (or supply) levels that met the specified criteria.

**To enable or disable the supply filter:**

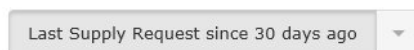
- Click the part of the filter control where the text is displayed (not the part where the arrow appears). This toggles the state of the filter from enabled to disabled and back. The appearance of the control changes to indicate the state of the filter.

## Filtering data by last supply request

If you want, you can filter devices by the date of the last supply request for the device.

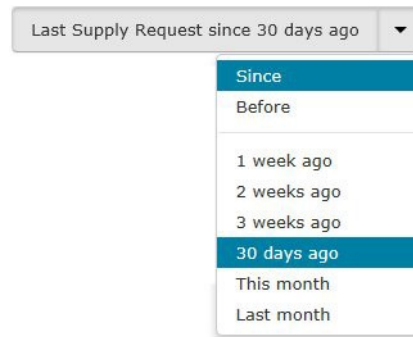
**Procedure**

- While on a device view, click the filter button and select **Last Supply Request** from the menu that appears. A filter control appears at the top of the view.



By default, the control is set to **Last Supply Request in the last 30 days ago**, meaning only devices with at least one supply with a last supply request date within the last 30 days will be listed in the view.

- If you want to change the criteria on which the view is filtered, click the arrow to the right of the filter control. A menu will appear.



3. Do one of the following:
  - Choose **Since** if you only want to list devices that have a last supply request date that is less than the period specified in the menu. For example, if you set your filter to **Last Supply Request in the last 30 days ago**, devices with at least one supply with a last supply request date which is less than 30 days ago will be listed in the view.
  - Choose **Before** if you only want to list devices that have a last supply request date that is more than the period specified in the menu. For example, if you set your filter to **Last Supply Request before 30 days ago**, devices with at least one supply with a last supply request date which is more than 30 days ago will be listed in the view.
4. Choose one of the following periods:
  - 1 week ago
  - 2 weeks ago
  - 3 weeks ago
  - 30 days ago
  - This month  
This refers to the first day of the current calendar month.
  - Last month  
This refers to the first day of the previous calendar month.

## Enabling the last supply request filter

### Procedure

- Click the part of the filter control where the text is displayed (not the part where the arrow appears). This toggles the state of the filter from enabled to disabled and back. The appearance of the control changes to indicate the state of the filter.

## Filtering data by text

If you want, you can filter devices by the text associated with any of the device fields.

### Procedure

1. While on a device view, in the text box to the left of the filter button, enter the text by which you want to filter the devices.

### Note

If you are attempting to filter devices based on the text that appears in a date column (such as the Last Reported column), be aware that the filter is applied to the underlying raw data which is stored in the ISO 8601 format (such as 2013-12-23T16:15:57.987Z.)

## Removing the text filter

### Procedure

- Delete the text from the filter text box.

## Removing a filter from a device view

If you want, you can remove an individual filter from a view.

### Procedure

- While on a filtered device view, click the filter button. A menu will appear. Under **REMOVE FILTER**, choose the filter you want to remove from the view.

## Removing all filters from a device view

If you want, you can remove all filters from a view.

### Procedure

- While on a filtered device view, click the filter button and choose **Reset filters** from the menu that appears.

## Resizing column widths in a device view

Each device view is initially displayed using the default column widths. The default column width values are calculated based on the existing data and are meant to provide a good balance between showing as much of the information as possible while also ensuring everything fits on one screen (without the need to scroll horizontally). If you want, you can easily change the column widths.

### Procedure

- Click the column-resizing handle (the small shaded area) to the right of the column name, and drag it to the desired width.




## Resetting a column to the default width

### Procedure

- Double-click the column-resizing handle for the column you want to reset.

## Resetting all columns to the default widths

### Procedure

- Click the **Manage Views** button  and choose **Reset Column Widths** from the menu that appears.

## Navigating among pages of items within a device view

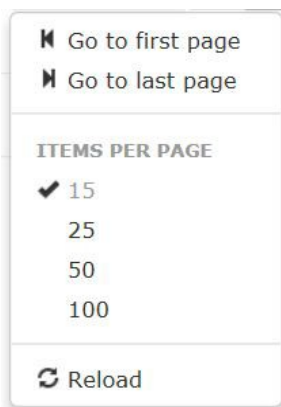
If there are too many items to display on a single page in a device view, the items are automatically broken into multiple pages according to the display limit for the view. For example, if there were 90 items, and the display limit for the view was set to 15 items per page, there would be 6 pages of 15 items per page. A pagination indicator in the upper-right corner of the page would display 1-15 of 90 when you were viewing the first page, 16-30 of 90 when viewing the second page, and so on.

1-15 of 90 ▾

You can click the adjacent right and left arrows to move forward and backward among the pages as necessary.



You can also click the down arrow to access a menu where you have options to go directly to the first or last pages in the device view, or to choose a different display limit for the device view. The menu also includes an option to reload the device view.



## Working with the default views

PrintFleet provides some views that reflect commonly requested functionality. However, because you can create, edit, and delete views, the descriptions of the views on the following pages may not

reflect the views currently available on your system. The following table describes the default device views.

Device View	Data Included
Technical View	device name, device status, page count for the current month, serial number, IP address, location, last active date, lifetime mono pages, lifetime color pages
Supplies Order View	device string, number of pages in last 30 days, current toner level/status, number of supplies being requested, date of last request
Alerts	alert definition name, device identifier, alert type, event description, event start date, event end date, event last active, status
Maps	group, map name, number of devices placed on each map, options for managing maps

## Device states

Some device views include a **Device Status** column which displays text indicating the most recent state of the device. The following table describes what each state means.

State	Interpretation
Critical	The device is reporting an error.
Warning	The device is reporting a warning.
Stale	Data has not been collected from the device for a period exceeding the <b>Days before device stale</b> system setting.
Unknown	Data is not available from the device or not supported by PrintFleet.
OK	The device is not reporting errors or warnings, and is not stale.

Note that the Critical and Warning states reflect the 14 error codes as defined in RFC 1759.

## Using the Technical View

The **Technical View** provides basic information about devices, including the device name, device status, monthly page count, serial number, IP address, location, last reported date, mono life count current value, and color life count current value. You can edit

and override this information via options in the **Device View Manager**.

## Procedure

- On the **Device Views** menu, click **Technical View**.

The screenshot shows the 'Technical View' of the PrintFleet Optimizer. It features a navigation menu on the left with options like 'HQ', 'East', 'Sales', 'Development', 'West', and 'Manufacturing'. The main area displays a table of device information:

Device Group	Device Name	Device Status	Pages this Month	Serial Number	IP Address	Location	Last Reported	Mono Life Count	Color Life Count
HQ	KONICA MINOLTA bizhub 363	Warning	11	A1UE011014238	10.0.0.106		Today at 4:21 PM	33	0
East	Lexmark T634 4130420 551...	Critical	115	SER0123	10.0.0.232	Development	Today at 4:21 PM	278812	0
West	TASKalfa 250d	Ok	678	QJH0Y08729	10.0.0.50		Today at 4:21 PM	34732	17586

The **Technical View** will display the most significant status in the **Device Status** column. For example, if a device has a paper jam and is low on yellow toner, the column will reflect the paper jam error, rather than the yellow toner warning.

If you want more information about the status of a device, click on the device name link and you will be taken to the **Device Detail** page for that device. See "Working with the Device Detail page" on page 24.

## Using the Supplies Order View

You can use the **Supplies Order View** to monitor supplies and to submit requests for replacement supplies. By default, the view includes the device string, pages for the past 30 days, and the **Toner Request** column which you can use to monitor and request toner. If you also want to monitor and request non-toner supplies (such as drums, belts, fusers, and so forth), you would need to add the **Misc. Supply Request** column to the view.

### Note

To create, edit, override, or delete a view you must belong to a role that has been assigned the **Device View Management** permission.

## Procedure

- On the **Device Views** menu, click **Supplies Order View**.

The screenshot shows the 'Supplies Order View' of the PrintFleet Optimizer. It displays a table of device information with columns for 'Device Group', 'Device String', 'Pages in 30 Days (Chart)', and 'Toner Request'. The 'Toner Request' column shows color-coded bars and checkboxes for Black, Cyan, Magenta, and Yellow toner levels and request dates.


Device Group	Device String	Pages in 30 Days (Chart)	Toner Request
ACME Printing	KONICA MINOLTA pagepro 4650	7	Black: 50%, Cyan: 0%, Magenta: 0%, Yellow: 0%
East	Lexmark T634	398	Black: 0%, Cyan: 0%, Magenta: 0%, Yellow: 0%
West	Lexmark X543	0	Black: 0%, Cyan: 0%, Magenta: 0%, Yellow: 0%
	MCS60	10	Black: 50%, Cyan: 0%, Magenta: 0%, Yellow: 0%
	Manjet Office Printer Pro	665	Black: 0%, Cyan: 0%, Magenta: 0%, Yellow: 0%

The **Toner Request** column displays the level or status for each toner supply for the device, the date and time a replacement for the toner was last requested, and an edit box in which you can specify a quantity to request.

If included in the view, the **Misc. Supply Request** column displays the level or status for each non-toner supply for the device, the date and time a replacement for the supply was last requested, and an edit box in which you can specify a quantity to request.

<b>Note</b>	If you do not belong to a role that has been assigned the <b>Supply Request</b> permission, the edit box will not be displayed in either the <b>Toner Request</b> column or the <b>Misc. Supply Request</b> column.
-------------	---

When using the **Supplies Order View**, be aware of the following:

- If you want more information about the status of a device, click on the device string link and you will be taken to the **Device Detail** page for that device. See "Working with the Device Detail page" on page 24.
- If you hover your mouse cursor over a toner level, a tooltip will appear showing the date and time the value was last updated.
- If you want more information about the status of a supply, click on the supply and you will be taken to the Metric History page for that supply. See "Working with the Metric History page" on page 34.
- If you have previously requested a supply, an envelope icon  appears in the **Toner Request** column for that supply, along with the date and time the most recent request was made. If you hover your mouse cursor over the icon or date, a tooltip will appear showing the quantity of the supply that was requested at that time.
- If you have added quantities to the **Toner Request** column, but want to clear all quantities, you can do so by clicking the down arrow to the right of the **Create Supply Request** button, and choosing the **Clear quantities and cancel** menu option that appears.

## Requesting supplies

If you belong to a role that has been assigned the **Supply Request** permission, you can request supplies from the **Supplies Order View** (or any device view that includes the **Toner Request** or **Misc. Supply Request** columns). PrintFleet will generate an email summarizing the supply request. This email can be directed to the person within your organization who is responsible for ordering supplies.

---

## Procedure

1. Under either the **Toner Request** or **Misc. Supply Request** column, in the row for the supply you want to request, do either of the following:
  - In the edit box, enter the number of supplies you want to request.
  - Position your mouse cursor to the right of the edit box, then use the up and down arrows that appear to adjust the number of supplies you want to request.
2. Repeat step 1 for each additional supply you want to request.
3. When you are ready to proceed with the request, click **Create Supply Request**.

The **Supply Request** page appears.

4. On the **Supply Request** page, do the following:
  - Confirm the supplies and quantities you want to request. Use the edit boxes or arrows to adjust the quantities if necessary.
  - In the **Email to** box, enter the email address of the person to whom you want to send the request. If necessary you can type multiple addresses, separated by commas.
  - In the **Subject** box, enter a subject line for the request email.
  - In the **Notes** box, enter any additional information you would like to appear in the body of the request email.
  - The details of the supply request will be summarized in the body of the email that is sent. This information may be sufficient for your needs. However, depending on your company's ordering system, you may be able to expedite the process by providing the information in an XML or CSV format. Use the **Attachment** list to specify which format to attach to the supply request email.
  - Click **Send Supply Request**. A confirmation dialog opens.
  - Click **Send**.

For each supply requested, the supply request email displays the following information:

- Group breadcrumb
- Device string
- Serial number
- Asset number
- Location
- Supply name
- OEM Part Number (if available)
- Quantity requested

## Using the Maps View

The **Maps View** allows you to view, upload, and place images of document output devices, computing devices, people, and other miscellaneous items on one or more maps. Document output devices will display icons to represent their status. A legend for the icons is displayed above the map.



Most browsers also support hovering your mouse pointer over the device to view basic device information, with a link to the device's detail view. See "Working with the Device Detail page" on page 24.



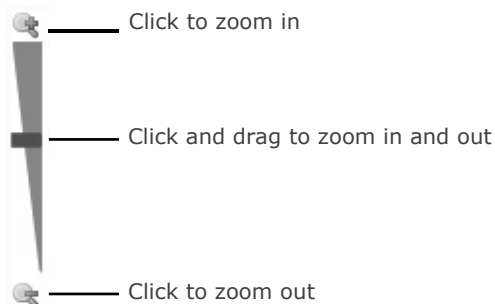
### Procedure

- On the **Device Views** menu, click **Maps**.

## Viewing a map

### Procedure

- In the **Maps View**, under **Options**, click **View**.
- Optionally, use the zoom bar or your mouse scroller to zoom in and out on the map image.



## Uploading a new map

### Procedure

- In the **Maps View**, click **Add Map**. Alternatively, click **Edit** or **View** for an existing map and select **New** in the **Settings** tab.

2. Select a group.
3. In the **Map Name** box, enter a recognizable title for the map.
4. In the **Map image** box, type the location of the map image you want to upload, or click **Browse** to navigate to the image.
5. Click **Add Map**.

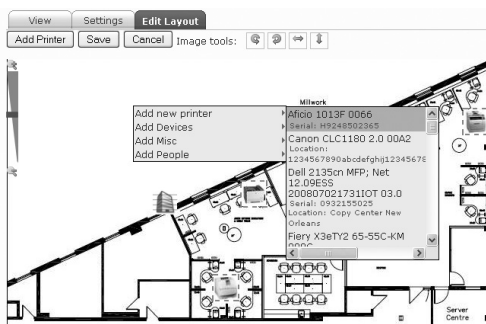
**Note**

Map images must be in .jpg, .gif, .png, .bmp, .tiff, or .wmf format.

## Place imaging devices on a map

### Procedure

1. In the **Maps View**, under **Options**, click **Edit** for the map you want to edit.
2. Click the **Edit Layout** tab.
3. Do one of the following:
  - Click **Add Printer**, select the device you want to add from the list, and then click the location on the map that you want to place the device.
  - Right-click the place on the map image where you want to place a device, point to **Add new printer**, and then select a device from the list.
4. Drag the device until it is in the precise location you want it.
5. Click **Save**.



## Placing computing devices, people, icons on a map

### Procedure

1. In the **Maps View**, under **Options**, click **Edit** for the map you want to edit.
2. Click the **Edit Layout** tab.
3. Right-click the place on the map image where you want to place a computer, building, or person, and do one of the following:
  - To add a computer, point to **Add Devices**, and select the icon you want to add from the list.
  - To add a person or group of people, point to **Add People**, and select the icon you want to add from the list.

- To add other miscellaneous icons, point to **Add Misc**, and select the icon you want to add from the list.
4. Drag the object until it is in the precise location you want it.
  5. Click **Save**.

### Moving an imaging device image or other icon

#### Procedure

1. In the **Maps View**, under **Options**, click **Edit** for the map you want to edit.
2. Click the **Edit Layout** tab.
3. Click and drag the icon you want to move to the new location.
4. Click **Save**.





### Removing an imaging device image or other icon

#### Procedure

1. In the **Maps View**, under **Options**, click **Edit** for the map you want to edit.
2. Click the **Edit Layout** tab.
3. Right-click on the icon you want to remove, and then click **Remove**.
4. Click **Save**.

### Rotating or flipping a map

#### Procedure

1. In the **Maps View**, under **Options**, click **Edit** for the map you want to edit.
2. Click the **Edit Layout** tab.
3. Do one or more of the following to rotate and/or flip the map to the correct position:
  - Click  to rotate the map image counterclockwise.
  - Click  to rotate the map image clockwise.
  - Click  to flip the map image horizontally.
  - Click  to flip the map image vertically.
4. Click **Save**.

### Changing a map image or title

#### Procedure

1. In the **Maps View**, under **Options**, click **Edit** for the map you want to edit.
2. In the **Settings** tab, do one or more of the following:
  - Enter a new title for the map in the **Map name** box, and click **Change**.

- Click **Browse** or type in the location of a replacement image in the **Select file** box, and then click **Upload**.

## Deleting a map

### Procedure

1. In the **Maps View**, under **Options**, click **Delete** for the map you want to delete.
2. Click **OK** to confirm deletion.

## Downloading a map image

### Procedure

1. In the **Maps View**, under **Options**, click **Edit** or **View**.
2. In the **Settings** tab, click **Download** and save the image file to your computer.

## Using the Alerts View

When the conditions specified in an alert definition are met, an alert event is automatically created. You can use the **Alerts View** to view the alert events that have been created. The **Alerts View** shows only the alert events associated with a selected group.

For each alert event, the **Alerts View** displays the following:

- **Alert Definition**—Displays the name of the corresponding alert definition.
- **Identifier**—Displays the name of the device associated with the event. You can click the device name to go to the associated **Device Detail** page. See "Working with the Device Detail page" on page 24.
- **Type**—The type of alert definition (such as Device or DCA).
- **Event Description**—A description of why the event occurred (such as "Display Panel "Door open" active.").
- **Event Start Date**—For an alert of type Device, the date and time of the first DCA scan for which the reported device values met the conditions specified in the alert definition. For an alert of type DCA, the date and time of the first check by the alert engine for which the conditions specified in the alert definition were met. Note that this does not include the initial grace period in which the DCA was stale. For example, if your alert definition was set up to generate an alert event after a DCA had been stale for 3 days, the **Event Start Date** would not coincide with the start of the 3 days, but instead with the first missed report after those 3 days had elapsed.
- **Event End Date**—For an alert of type Device, the date and time of the first DCA scan for which the reported device values did not meet the conditions specified in the alert definition. For an alert of type DCA, the date and time of the first check by the alert engine for which a report was received from the DCA.
- **Event Last Active**—For an alert of type Device, the date and time of the last DCA scan received for which the reported device values met the conditions specified in the alert definition. For an

alert of type DCA, the date and time of the last check by the alert engine for which no report was received from the DCA.

- **Status**—For an alert definition using a Page Recurring or Date Recurring condition type, a gray bell is displayed. For alert definitions using other condition types, a gold bell is displayed while the event is active, and no icon is displayed once the event has ended.

Events associated with disabled alert definitions will not be displayed on this page.

### Procedure

- On the **Alerts View**, in the left pane, select the group for which you want to view the events. After a moment the alert events appear. If there are no events associated with the selected group, the **Alerts View** displays 'No items' at the bottom of the page.


## Creating custom device views

An unlimited amount of custom device views can be created, so that you can view the exact information you want, in the way you want to view it. Custom device views will be added to the **Device Views** menu for groups selected to have access.

### Note

To create, edit, override, or delete a view you must belong to a role that has been assigned the **Device View Management** permission.

### Procedure

1. Do one of the following:
  - On the **Settings** menu, click **Device View Manager**, then click **New View** on the **Device View Manager** page.
  - From any device view, click the Manage Views button , then choose **New View** from the menu that appears.
2. On the **Add/Edit Device View** page, in the **Columns** area, select the data items you want included in the view. In general, you will want to include at least one data item that identifies a device, for example, device name or serial number. Custom Device Fields are denoted by yellow fill.
3. Click and drag the selected data items into the order you want them to appear on the view. The item at the top of the list will be displayed as the first item on the left side of the view.
4. Enter a title for the custom device view in the **Name** box.
5. From the **Default Sorting** lists, choose a default column you want the data to be sorted by initially, and whether you want the sorting to be ascending or descending.
6. From the **Apply To** list, select whether you want the device view to be available to only yourself (**Me**) or to specific **Groups**. If you select Groups, you must select one or more groups that the

view will be available to. Selecting the root group will make the view available to everyone.

7. Click **Save**.

### Editing a custom device view

#### Procedure

1. On the **Settings** menu, click **Device View Manager**.
2. In the row of the device view you want to change, click **Edit**.
3. Change any properties of the view, including name, default sorting, apply to properties (including which specific groups can access the view), and columns (data items).
4. Click **Save**.

### Deleting a custom device view

#### Procedure

1. On the **Settings** menu, click **Device View Manager**.
2. In the row of the device view you want to remove, click **Delete**.
3. When prompted, click **Confirm**.

You can use the override function to allow yourself or specified groups to see one view instead of another. This view could be a slight variation of the original view, or it could be something entirely different. When you delete an override, the properties of the original device view will be reinstated.



### Creating a device view override

#### Procedure

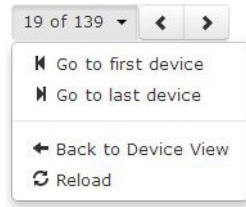
1. On the **Settings** menu, click **Device View Manager**.
2. In the row of the device view you want to create an override for, click **Override**.
3. Create your override view by entering a **Name**, choosing **Default Sorting** and **Apply To** properties, and selecting data items in the **Columns** area.
4. Click **Save**.

## 2.2 Working with the Device Detail page

The **Device Detail** page displays all information relevant to a specific device. The device string and group breadcrumb appear at the top of the page.

In the upper-right corner of the Device Detail page, a counter 19 of 139 displays the ordinal position of the current device within the most recent device view. If you want to switch to a different device from the same device view you can click the adjacent navigation buttons   to move backward and forward among the devices,

or you can click the counter and choose an option from the menu that appears.



If necessary, you can choose the **Reload** command from this menu to refresh the information displayed on the **Device Detail** page.

The information displayed in the **Device Detail** page is read only. If necessary you can edit some properties of the device by clicking the **Edit** button. This will take you to the **Device Information** tab of the **Device Information** page. For information on using the **Device Information** tab, see "Editing device information" on page 108.

To easily copy the device string to your clipboard, click the **Configure** button and choose **Copy Device String to Clipboard** from the menu the appears.

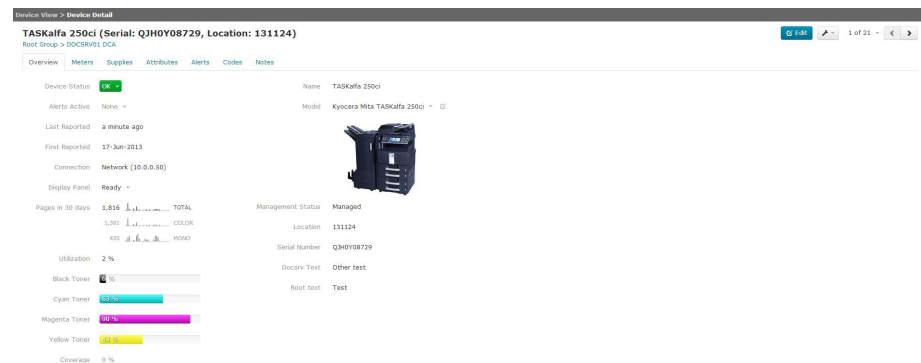


The **Overview** tab displays information identifying the device, some high-level information about meters and supplies, and an image of the device model if available. The **Device Detail** page has other tabs for accessing information about meters, supplies, attributes, alerts, codes, and notes related to the device.

## Accessing the Device Detail page

### Procedure

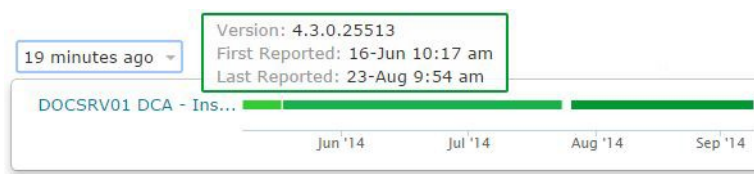
- Click on a device name link anywhere in the system. Usually this is while using one of the device views. See "Working with Device Views" on page 6.



## Working with the Overview tab

The **Overview** tab displays the following information:

- **Device Status** — Displays the status (OK, Warning, or Critical) associated with the most severe active error code for the device. If you hover your mouse cursor over the **Device Status** indicator a tooltip will indicate how many codes are currently active. To see the active codes, click the **Device Status** indicator. A dropdown window opens showing each active code and when it was first reported. You can also click the **View past codes** link to open the **Codes** tab for the device.
- **Alerts Active** — Displays the number of alerts that are currently active for the device. If there are active alerts you can click the **Alerts Active** indicator to open a dropdown window. From the dropdown window you can:
  - View the active alert events and when they were first reported.
  - Click the **View past alerts** link to open the **Alerts** tab for the device where you can view alert events for the device that have been closed.
  - View a list of the enabled alert definitions that are applicable to the device.
  - Click one of the listed alert definitions to view or edit the definition.
  - Click **Create a new alert definition** to create a new alert definition.
- **Last Reported** — Displays the last time an update was received from the device. You can also click the drop-down arrow to the right of this field to view additional information about the reporting history of the device.



The different colored sections of the graph indicate different reporting periods for the associated DCA(s). If you hover the cursor over them a tooltip will display additional information about that period, such as the version of the DCA that was running, and the specific date and time for the start and end of that period. If you have been assigned the **Admin** role you can also click the link to go to the **DCA Information** page.

- **First Reported** — Displays the date and time that the device was first detected on your system by PrintFleet.
- **Connection** — Displays the connection type (**Network** or **Local**) and the IP address of the device (or its host computer if it is a local device).
- **Display Panel** — Displays the last reported message to appear on the device's display panel. You can click the message to view

---

the most recent messages. From the dropdown window that appears you can also click the **View more change history** link to open the **Attribute History** page where you can see all reported messages for the device. Note that some devices do not have a display panel attribute, so this field may not be displayed for all devices.

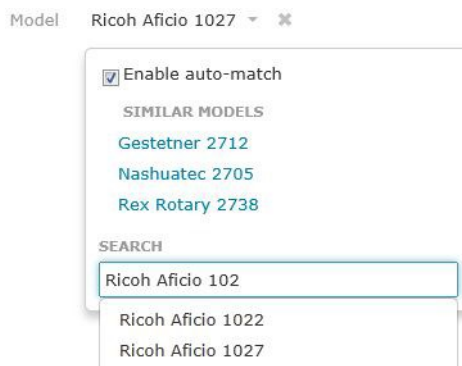
- **Pages in 30 days** — Displays the number of pages printed in the last 30 days, along with a bar graph. If the device is color capable, there will be separate entries for Total, Color, and Mono pages. If you hover your mouse cursor over the bar graph a tooltip will display the page count for the corresponding day.
- **Utilization** — Displays the percentage of the total number of potential pages that the device has printed. If you hover your mouse cursor over the value it will display the date on which the value was last updated.
- **Black Toner** — Displays the percentage of black toner remaining. If you hover your mouse cursor over the value it will display the date on which the value was last reported. If you click the value it will open the associated **Metric History** page.
- **Cyan Toner** — Displays the percentage of cyan toner remaining. If you hover your mouse cursor over the value it will display the date on which the value was last reported. If you click the value it will open the associated **Metric History** page.
- **Magenta Toner** — Displays the percentage of magenta toner remaining. If you hover your mouse cursor over the value it will display the date on which the value was last reported. If you click the value it will open the associated **Metric History** page.
- **Yellow Toner** — Displays the percentage of yellow toner remaining. If you hover your mouse cursor over the value it will display the date on which the value was last reported. If you click the value it will open the associated **Metric History** page.
- **Coverage** — Displays the average percentage of the total printable area of a letter size sheet of paper that is covered by toner. If you hover your mouse cursor over the value it will display the date on which the value was last updated.
- **Name** — Displays the name of the device.
- **Model** — Displays the name of the model associated with the device. If available, a picture of the corresponding model is also displayed. To see the properties associated with the model, click the model name.
- **Management Status** — Displays the management status (Managed or Unmanaged) of the device.
- **Location** — Displays the location of the device (provided one has been specified).
- **Asset Number** — Displays the asset number of the device (provided one has been specified).
- **Serial Number** — Displays the serial number of the device (provided one has been specified).

PrintFleet tries to automatically associate each new device with a corresponding model from its model database. Most of the time this works very well, but occasionally a device gets associated with the wrong model. If necessary, you can manually associate the device with a different model.

## Changing the model associated with a device

### Procedure

1. Click the **Edit** icon to the right of the **Model** field. A popup window opens.



2. If any other models in the model database share the same internal device description, they will be listed under **Similar Models**. If you want you can click one of the listed models to associate it with the device.

### Note

This may be the case for models which are rebranded and sold under two or more different names. For example, the models Ricoh Aficio 1027, Gestetner 2712, Rex Rotary 2738, and Nashuatec 2705 are all essentially the same model, and all identify themselves using the same internal description 'NRG 2705/2738/2712'. There is no way for PrintFleet to automatically determine which of these models a customer has, so it might be necessary for you to indicate the one that you have by selecting it from the **Similar Models** list.

3. If the model you want to associate with the device is not listed under **Similar Models**, it might still exist in the model database. You can try to locate a model in the database by entering the model name in the **Search** box. As you type, a list of model names that include the text you have entered is displayed below the **Search** box. If you see the model you want displayed in the list, click it to associate it with the device.

<b>Tip</b>	<p>When using the <b>Search</b> box, keep the following in mind:</p> <ul style="list-style-type: none"> <li>• If you enter multiple terms separated by spaces, only the entries that include all of the terms will be displayed. For example, if you typed 'Canon 1000' it would display all entries that included both 'Canon' and '1000', such as the Canon BJC-1000 and the Canon LBP-1000 models.</li> <li>• You might start by just typing the model number (such as '1000'), and if there are still too many results consider adding more information (such as 'BJC-1000').</li> </ul> <p>The results list is limited to 15 items, so you may need to type additional characters to refine your search sufficiently.</p>
------------	--

4. PrintFleet regularly updates the printer model database and makes these updates available to customers. Selecting the **Enable auto-match** check box allows PrintFleet to automatically check for a better match for the device each time you update your model database. The check box is cleared when you manually associate a model with a device, including devices that were manually matched in a previous version.

## Working with the Meters tab

The **Meters** tab displays the following information for each of the standard, virtual, and device-specific meters for the device:

- **Meter** — The name of the meter.
- **Page Total** — The total number of pages for the meter.
- **Last 30 Days** — The number of pages for the meter over the last 30 days. If you hover your mouse cursor over the bar graph, a tooltip will display the page counts for the individual days.
- **Last Reported** — The last time a value was reported for the meter. If you hover your mouse cursor over the value, a tooltip will display the specific date and time of the last report. The **filter icon** beside this function also gives you the option to **hide** or **show** stale meters, which is useful if you want to get accurate data of active devices.
- **Standard type** — PrintFleet will map the vendor label to a Standard Type. Standard Types identify basic categories of metric data produced by devices to accurately communicate meter, supply, attribute and error code information.

## Working with the Supplies tab

### Procedure

- On the **Device Detail** page, click the **Meters** tab.

Supply	Level	Last 90 Days	Type	OEM Part Number	Last Reported	Standard Type
CONTRAST_DEV	475	0	all	all	4 hours ago	Impression-Color-Copy-AllInOne-AllPageColor
CONTRAST_DEV_PCL	475	0	all	all	4 hours ago	Impression-FullColor-Copy-AllInOne-AllPageColor
CONTRAST_DEV	34,547	0	all	all	4 hours ago	Impression-Photo-Copy-AllInOne-AllPageColor
CONTRAST_DEV	15,412	0	all	all	4 hours ago	Impression-AllPhoto-Copy-AllInOne-AllPageColor
Copy Center (C) M990	28	0	all	all	4 hours ago	Impression-Photo-Copy-AllInOne-Photo
Copy Center (C) T200	28	0	all	all	4 hours ago	Impression-AllPhoto-Copy-AllInOne-Photo
Copy Center (C) M990Laser	8	0	all	all	4 hours ago	Impression-Publication-Copy-AllInOne-Laser
Copy Center (C) M990	47	0	all	all	4 hours ago	Impression-Photo-Copy-AllInOne-Laser
Copy Center (C) T200L	15	0	all	all	4 hours ago	Impression-AllPhoto-Copy-AllInOne-Laser
Copy Center (C) M990Laser	160	0	all	all	4 hours ago	Impression-Publication-Copy-AllInOne-Laser
Copy Center (C) M990	8,874	0	all	all	4 hours ago	Impression-Photo-Copy-AllInOne-Laser
Copy Center (C) T200L	22,424	0	all	all	4 hours ago	Impression-AllPhoto-Copy-AllInOne-Laser

The **Supplies** tab of the **Device Detail** page displays the following information about toner and non-toner supplies:

- Supply** — The name of the supply.
- Level** — The last level (or status) reported by the supply.
- Last 90 Days** — For supplies that report levels, a bar graph of the level values over the last 90 days. If you hover your mouse cursor over the bar graph, a tooltip will display the level values for the individual days.
- Type** — The type of supply (such as Toner, Fuser, or Developer).
- OEM Part Number** — The OEM part number of the supply. These values are properties of the model that is associated with the device.
- Last Reported** — The last time a level was reported for the supply. If you hover your mouse cursor over the value, a tooltip will display the specific date and time of the last report.
- Standard Type** — PrintFleet will map the vendor label to a Standard Type. Standard Types identify basic categories of metric data produced by devices to accurately communicate meter, supply, attribute and error code information.

### Procedure

- On the **Device Detail** page, click the **Supplies** tab.

Supply	Level	Last 90 Days	Type	OEM Part Number	Last Reported	Standard Type
Black Marker Level	20%	0	Toner	2798003AA	4 hours ago	Cartridge.Marker:Black
Cyan Marker Level	100%	0	Toner	2798003AA	4 hours ago	Cartridge.Marker:Cyan
Magenta Marker Level	20%	0	Toner	2798003AA	4 hours ago	Cartridge.Marker:Magenta
Yellow Marker Level	100%	0	Toner	2812803AA	4 hours ago	Cartridge.Marker:Yellow
Waste Toner	Unknown	0	Waste Toner		4 hours ago	Waste.Marker

### Note

To view more detailed information for a supply, on the **Supplies** tab, click anywhere in the row of the supply you want to view. The **Metric History** page opens. For information on using the **Metric History** page, see "Working with the Metric History page" on page 34

## Working with the Attributes tab

The **Attributes** tab displays additional device information. This information will vary by device, but may include such things as firmware versions, amount of memory, duplex capability, and so forth. Any custom device fields that apply to the associated device also appear on this page. For each attribute, the **Attributes** tab of the **Device Detail** page displays the following information:

- **Attribute** — The name of the attribute.
- **Current Value** — The last value reported for the attribute.
- **Source** — Indicates whether the value was reported directly by the device, or was calculated using other information.
- **Last Reported** — The last time a value was reported for the attribute. If you hover your mouse cursor over the value, a tooltip will display the specific date and time of the last report.
- **Standard Type** — PrintFleet will map the vendor label to a Standard Type. Standard Types identify basic categories of metric data produced by devices to accurately communicate meter, supply, attribute and error code information.

### Procedure

- On the **Device Detail** page, click the **Attributes** tab.

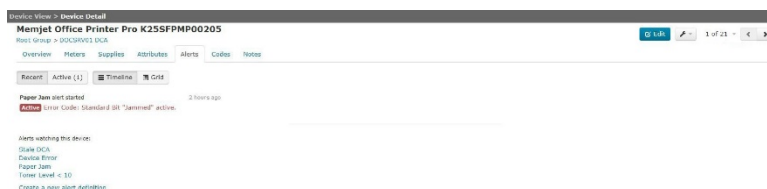
### Note

To view the history for an attribute, on the **Attributes** tab, click anywhere in the row of the attribute for which you want to view the history. The **Attribute History** page opens.

The **Alerts** tab displays all active alert events for the device and any alert events for the device that were active within the last 90 days.

### Procedure

- On the **Device Detail** page, click the **Alerts** tab.



## Working with the Alerts tab

By default, the alert events are displayed as a timeline. Clicking the **Grid** button will toggle the display between the timeline and a grid. The timeline view presents each change related to an alert as a separate entry in a list. This is useful for tracking the changes to alerts over time, including updates to the values of the conditions being monitored. If you hover your mouse cursor over one of the entries in the timeline view, the events associated with other alerts will be dimmed, making it easy to see just the entries for the alert you are interested in. When viewing the alert events as a timeline, each list entry includes the following information:

- Name of the alert definition
- Whether the alert started, ended, or was updated
- The amount of time that has passed since the entry was created
- The specific value for the condition being monitored at the time the entry was created.

The grid view presents each alert event on a separate row of the grid. This is useful when you just want to see the high-level information about an alert (such as when it started and what its current status is) and do not care about any intermediate updates. When viewing the alert events as a grid, the following information is displayed for each alert event:

- **Alert** — The name of the associated alert definition.
- **Last Description** — The specific value for the condition being monitored at the time the entry was created.
- **Started** — How long ago the alert event was created. If you hover your mouse cursor over the value, a tooltip will display the specific date and time the event was created.
- **Duration** — The amount of time the alert event was active. If you hover your mouse cursor over the value, a tooltip will display a more precise value.
- **Status** — Indicates whether an alert event is active or has ended. If you hover your mouse cursor over the value, a tooltip will display the last time the conditions of the associated definition were known to have been met (for active events), or the specific date and time the event ended.

By default the **Alerts** tab displays both active and recently closed alert events. The **Active** button displays the number of active alert events for the device. If you want you can click the **Active** button to filter out the events that have ended and display just the active ones.

The **Alerts** tab also displays links to any alert definitions that are currently associated with the device. You can click these links to view or edit the definitions, or you can click **Create a new alert definition** if you want to create a new alert definition.

## Working with the Codes tab

The **Codes** tab displays all active service or error codes for the device and any closed codes for the device that were active within the last 90 days.

## Procedure

- On the **Device Detail** page, click the **Codes** tab.



By default, the codes are displayed as a timeline. Clicking the **Grid** button will toggle the display between the timeline and a grid.

The timeline view presents each change related to a code as a separate entry in a list. This is useful for tracking the changes to codes over time. If you hover your mouse cursor over one of the entries in the timeline view, the entries associated with other codes will be dimmed, making it easy to see just the entries for the code you are interested in. When viewing the codes as a timeline, each list entry includes the following information:

- Name of the code
- Whether the code started or ended
- The amount of time that has passed since the entry was created
- The specific value for the code at the time the entry was created.

The grid view presents each code on a separate row of the grid. This is useful when you just want to see the high-level information about a code (such as when it started and what its current status is). When viewing the codes as a grid, the following information is displayed for each code:

- Severity** — The severity (Info, Critical or Warning) of the error code.
- Code** — A textual description of the error code.
- Type** — The type (Error Bit, Error Code, Service Code, or Vendor Code) and specific value of the error code.
- Started** — How long ago the error code was first reported. If you hover your mouse cursor over the value, a tooltip will display the specific date and time the error code was first reported.
- Duration** — The amount of time the error code was active. If you hover your mouse cursor over the value, a tooltip will display a more precise value.
- Status** — Indicates whether a code is active or has ended. If you hover your mouse cursor over the value, a tooltip will display the last time the code was reported (for active codes), or the specific date and time the code ended.

By default the **Codes** tab displays both active and recently closed codes. The **Active** button displays the number of active codes for the device. If you want you can click the **Active** button to filter out the closed codes and display just the active ones.

## Working with the Notes tab

The **Notes** tab displays up to 90 notes that have been manually entered for the device. You can use the **Notes** tab to record device specific information that is not captured elsewhere in the system.

### Procedure

- On the **Device Detail** page, click the **Notes** tab. This will display any notes that have been added for the device along with the date and time each note was added.



## Adding a note

### Procedure

- On the **Notes** tab, enter the text you want to add in the edit box at the top of the page, then click the **Add Note** button that appears.

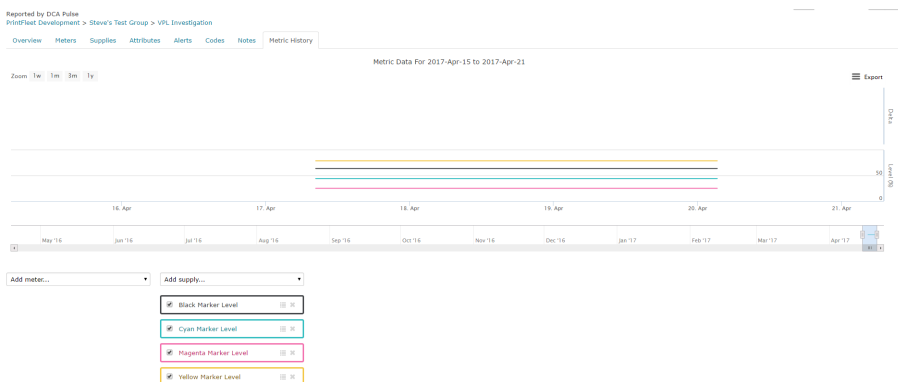
<b>Note</b>	There is a limit of 1000 characters per note.
-------------	---

## Working with the Metric History page

The **Metric History** page displays information for a specific supply for a device. This can help you when trying to make decisions about when to request a supply.

### Procedure

- Do one of the following:
  - On the **Supplies** tab of the **Device Detail** page, click the name of a supply.
  - On a device view that contains either the **Toner Request** or **Misc. Supply Request** columns, click a supply. The **Metric History** page appears.



The **Metric History** page displays an interactive detail of information over a period of time (that you may select) from available supplies and meters.

If any alert definitions are currently applied to the supply, you can click on the name of the alert definition to open the alert definition.

**Working with the supply chart.** You can click and drag on the supply chart to zoom in on a specific time period. To return to the original zoom setting for the chart click the **Reset zoom** button that appears. The chart will also display an icon at any point where PrintFleet has detected the supply has been replaced.

Some devices report supplies as states rather than specific values. For these devices the **Level** will read **OK**, **Warning**, or **Critical** instead of a percentage. Each of these states has a corresponding range of potential supplies. For example, a supply in a **Warning** state might have an actual level anywhere between 10% to 25%. To reflect this uncertainty, a darker shaded band will be displayed below the line on the graph to indicate the range of possible levels associated with the current state.

**Navigating among supplies for a device.** If necessary you can easily navigate to other related supplies pages using the controls displayed in the upper right corner of the page. You can click the right and left arrows to move forward and backward among the supplies for the device. The counter updates to help you keep track of which supply you're viewing (such as 2 of 5). You can also click the down arrow to access a menu of other navigation options.

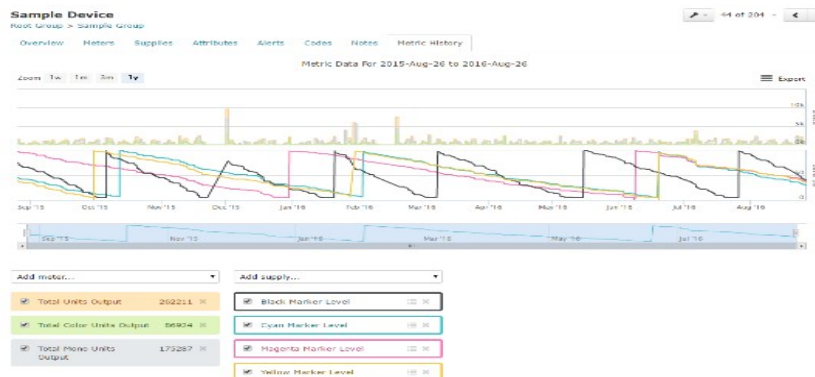
## Working with the Metric History Tab

The **Metric History** tab is an interactive tool that allows you to gain insight into user trends and correlations. This function provides dynamic measurements to compare up to 14 different variables, showing specific detail while also allowing users to gain extra insight into user trends. This lets users to work more effectively, and avoid delays or extra expenditure.

Users can:

- See the correlation between page counts and toner usage. Simply select **Total Units Output**, **Total Colour Units Output** or **Total Mono Units Output** from the **Metric** drop down menu, and then the colour(s) from the **Supply** drop down menu.
- Adjust time periods (i.e. 1 week, 1 month, 3 months, 1 year) to see how trends and patterns change and prevail over different periods of time.
- Select different meters to monitor printer use and supplies.
- Run your cursor over the graph for more detailed information on usage, like day, exact toner usage and page counts.
- Use this function to copy a string to a clipboard.
- Export the graphic to include in reports, correspondence or presentations.

You can also access these metrics from the **Meters** or **Supplies** tabs by selecting a printer or toner you'd like to see.



## Working with HP Smart Device Services

The **HP Smart Device Services (SDS)** page displays information. Users can see the status of the:

- HP Registration
  - Whether the device registered at HP
- Genuine Cartridge
  - Whether there is a Genuine cartridge in the device
- mSKU
  - Whether the device is an HP managed device
- Reboot
  - With this button you can remotely reboot the device

Device View > Device Detail

### HP Color LaserJet FlowMFP M577 (Managed)

Reported by DCA Pulse

Root Group > test6

Overview Meters Supplies Attributes Alerts Codes Notes Metric History HP Smart Device Services

HP Registration ✔ OK

Genuine Cartridge ✔ OK. Genuine HP cartridge installed. Remote operation enabled

mSKU ✔ OK. Toner cartridge yield increased

Reboot Reboot

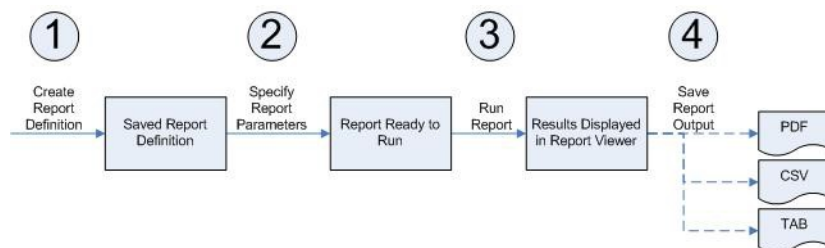
Last succeeded an hour ago

# Chapter 3 Reports

Reports in one word – flexible. You can easily create customizable output which can then be displayed in a number of intuitive graphical arrangements. In other words, PrintFleet reports let you view data when and how you want it.

## 3.1 Overview of Reports

Using reports generally involves the following main stages:



In this section you will find information on every stage of the process, including:

- Accessing report definitions  
Your first step should be to familiarize yourself with the report definitions that are already available to you. PrintFleet has created a number of report definitions that should be available to all users. Other users within your own organization may also have created report definitions that they have shared with you. See "Accessing report definitions" on page 43.
- Planning your report  
Creating reports is so easy that you may be tempted to jump right in, but for the best results it is worth taking some time to familiarize yourself with the powerful options available to you, and then decide how to most effectively apply these options to address your particular needs. See "Report options" on page 44.
- Creating report definitions  
A report definition describes the structure of the report: what to include, and how it should be arranged. You can reuse the same definition as many times as you want, and you can specify

---

different report parameters each time you use the report definition. See "Creating Report Definitions" on page 54.

- **Specifying report parameters**

Report parameters determine what data to use with a report definition. For example, you can create a generic report definition for devices, then run that report definition multiple times, specifying a different group each time. See "Specifying Report Parameters" on page 59.
- **Running reports**

Once you have your report definitions set up how you want them, you can run them whenever you want. Sometimes you will want to schedule a report to run at a certain time, but you can also select a definition and run it at any time. See "Running a report definition" on page 61.
- **Viewing and saving reports**

When you run a report, PrintFleet displays it on screen. You can navigate around within the report, and if necessary go back and change the parameters and run the report again. Even if you rerun a report using the same parameters, the report may be different if new data has been processed in the interim.

If you want to have a more permanent copy of the report, either to store or to send to someone else, you can save the report in PDF, CSV, or TAB format. See "Viewing and saving reports" on page 61.
- **Scheduling reports**

For reports that you know you will want to generate regularly, you can set up a schedule. When the scheduled time arrives the report is automatically run and emailed to specified users. See "Scheduling Reports" on page 62.
- **Managing report definitions**

As you create and refine your report definitions you will likely find it convenient to be able to perform various management activities, such as locating, editing, copying, and deleting report definitions. See "Managing Report Definitions" on page 63.
- **Managing report schedules**

Just as with report definitions, as you create and refine your report schedules you will likely find it convenient to be able to locate, edit, copy, and delete report schedules. See "Managing Report Schedules" on page 64.

## Types of reports

You can create the following types of reports:

**Standard reports.** These reports are created using the interface provided. While this interface places certain restrictions on the data you can access and on how the results are presented, it makes it easy for even the least experienced users to create reports that make sense and look good. See "Creating a Standard report definition" on page 54.

---

**Executive reports.** An executive report is essentially a report that combines other standard and/or SQL reports. Executive reports are typically used to summarize various aspects of your business, such as at the end of each fiscal quarter. An executive report can have cover pages at the front and back, and the cover pages can display custom branding (such as your corporate logo). See "Creating an Executive report definition" on page 56.

## Sample Reports

A number of sample reports are automatically provided. To ensure the integrity of these reports is maintained, these reports are not editable. However, you can create a copy of a sample report and make whatever changes you like to the copied version.

## 3.2 Accessing report definitions

Report definitions describe such things as what the report should include, and how it should be formatted. To generate an actual report, you must either run or schedule the corresponding report definition.

### Procedure

- From the main menu, click **Reports**. The **Reports** page appears with the **Definitions** tab displayed.

By default the **Definitions** tab displays all of the report definitions to which you have been granted access. This will include report definitions that have been created by PrintFleet. It may also include report definitions that have been created and shared by other users within your own organization.

You can even create your own report definitions, which will also be displayed here. Report definitions that you create are **Private** by default. That means that no other users (with the exception of the someone assigned to the **Admin** role in the Root group, who needs to be able to manage all of the report definitions on the system) can see or run the report definition. If you want other users to be able to see and run a report definition that you have created, you must specifically choose to share it. For more information, see "Specifying Report Parameters" on page 59.

## Sorting report definitions

When viewing the report definitions, note that you can click any column heading to sort the definitions by that column. This may help you to locate a particular definition if you have many report definitions.

## Filtering report definitions

If you want, you can filter the list to only display the report definitions that have been shared with a specific group.

**Procedure**

- On the **Definitions** tab of the **Reports** page, click the arrow in the **Filter by Group** box, then select the group you want from the drop-down list that appears.

**Note**

There are a few special cases you should be aware of when filtering report definitions:

- Filtering has no effect on **Private** report definitions that were created by the user applying the filter. In other words, regardless of what group I might filter on, I will always be able to see all of the **Private** report definitions I have created.
- Filtering on the group to which you are associated is effectively the same as not applying a filter. To reduce the number of report definitions displayed you must filter on a group below the group to which you are assigned.

### 3.3 Report options

There are various things you can do to make a standard report appear more professional, or to highlight an aspect of the information being presented. It will be helpful to familiarize yourself with these options before you start creating your report definitions.

**Note**

With the exception of charts, these options are not available for use with a SQL report.

### Nesting

Nesting gathers together all of the rows that share a value for a specific field, creates headings based on the field, and displays the remaining fields under the headings. PrintFleet does all of this for you automatically, but for educational purposes it may help to think of it as following these steps:

- First, the data in the report is automatically sorted in ascending order according to the specified field (Manufacturer in this example).

**BEFORE**

Manufacturer	Model	Pages
Ricoh	Aficio MP 2550SP	63428
Canon	imageRUNNER 3225	8954
Hewlett-Packard	LaserJet 4250	72542
Canon	imageRUNNER 3235	2321

**AFTER**

Manufacturer	Model	Pages
Canon	imageRUNNER 3225	8954
Canon	imageRUNNER 3235	2321
Canon	imageRUNNER 3225	13626
Canon	imageRUNNER 3235	58252

**BEFORE**

Manufacturer	Model	Pages
Ricoh	Aficio MP 2550SP	24593
Hewlett-Packard	LaserJet 4250	86524
Hewlett-Packard	LaserJet 4000	3442
Canon	imageRUNNER 3225	13626
Ricoh	Aficio MP 161	845
Canon	imageRUNNER 3235	58252

**AFTER**

Manufacturer	Model	Pages
Hewlett-Packard	LaserJet 4250	72542
Hewlett-Packard	LaserJet 4250	86524
Hewlett-Packard	LaserJet 4000	3442
Ricoh	Aficio MP 2550SP	63428
Ricoh	Aficio MP 2550SP	24593
Ricoh	Aficio MP 161	845

2. Next, the report removes duplicate values in the specified field.

**BEFORE**

Manufacturer	Model	Pages
Canon	imageRUNNER 3225	8954
Canon	imageRUNNER 3235	2321
Canon	imageRUNNER 3225	13626
Canon	imageRUNNER 3235	58252
Hewlett-Packard	LaserJet 4250	72542
Hewlett-Packard	LaserJet 4250	86524
Hewlett-Packard	LaserJet 4000	3442
Ricoh	Aficio MP 2550SP	63428
Ricoh	Aficio MP 2550SP	24593
Ricoh	Aficio MP 161	845

**AFTER**

Manufacturer	Model	Pages
Canon	imageRUNNER 3225	8954
	imageRUNNER 3235	2321
	imageRUNNER 3225	13626
	imageRUNNER 3235	58252
Hewlett-Packard	LaserJet 4250	72542
	LaserJet 4250	86524
	LaserJet 4000	3442
Ricoh	Aficio MP 2550SP	63428
	Aficio MP 2550SP	24593
	Aficio MP 161	845

3. Finally, the report creates headings from the remaining values and displays the non-nested fields indented below these headings.

**BEFORE**

Manufacturer	Model	Pages
Canon	imageRUNNER 3225	8954
	imageRUNNER 3235	2321

**AFTER**

Manufacturer: Canon		
	Model	Pages
	imageRUNNER 3225	8954
	imageRUNNER 3235	2321

**BEFORE**

Manufacturer	Model	Pages
	imageRUNNER 3225	13626
	imageRUNNER 3235	58252
Hewlett-Packard	LaserJet 4250	72542
	LaserJet 4250	86524

	LaserJet 4000	3442
Ricoh	Aficio MP 2550SP	63428
	Aficio MP 2550SP	24593
	Aficio MP 161	845

**AFTER**

Manufacturer: Canon		
Model	Pages	
imageRUNNER 3225	13626	
imageRUNNER 3235	58252	
Manufacturer: Hewlett-Packard		
Model	Pages	

LaserJet 4250	72542	
LaserJet 4250	86524	
LaserJet 4000	3442	

Manufacturer: Ricoh		
Model	Pages	
Aficio MP 2550SP	63428	
Aficio MP 2550SP	24593	
Aficio MP 161	845	

**Note:** If you want, you can apply nesting to as many as three fields in a report. For example, here is the same information with nesting applied to two fields (Manufacturer and Model).

Manufacturer: Canon		
Model: imageRUNNER 3225		
Pages	8954	
13626		
Model: imageRUNNER 3235		
Pages	2321	
58252		
Manufacturer: Hewlett-Packard		
Model: LaserJet 4000		
Pages	3442	

<b>Manufacturer: Canon</b>
<b>Model: imageRUNNER 3225</b>
<b>Pages</b>
<b>Model: LaserJet 4250</b>
<b>Pages</b>
86524
72542
<b>Manufacturer: Ricoh</b>
<b>Model: Aficio MP 2550SP</b>
<b>Pages</b>
63428
24593
<b>Model: Aficio MP 161</b>
<b>Pages</b>
845

The fields you apply nesting to must be the first fields listed in your report definition. If necessary you can reorder the fields in a definition by dragging them up or down in the **Fields** area of the **Create/Edit Report Definition** page. By default there is no nesting applied.

## Sorting

By default, PrintFleet sorts the report in ascending order using the first field you add to the report definition. When you make certain changes to the report definition, such as applying nesting or deleting fields, the field by which the report will be sorted may be automatically changed, so you should double-check how the sorting is set before you save your changes. If nesting is applied in your report definition, the report will be automatically sorted in ascending order by the nested fields. You can choose any non-nested field in your report definition to sort the report by (after any nesting has been done), and you can specify the sort direction.

## Row Counts

If you want, you can have PrintFleet display row counts in your report. The row counts appear at the top and bottom of each section of rows. If nesting is applied, row counts will appear for

each level of nesting. If the report does not have any nesting applied, the only row counts displayed will be for the entire report.

This example show three levels of nesting. Each level is indented.

This report has a total of 3 rows. ————— Indicates the total row count for the report.

Row counts appear at the start of each nested level.

SERIAL NUMBER	MANAGEMENT STATUS
SER0123	Managed
<b>1 ROWS</b>	

Row counts also appear at the end of the level.

LOCATION: Sales (2)

SERIAL NUMBER	MANAGEMENT STATUS
A1UE011014238	Managed
QJH0Y08729	Managed
<b>2 ROWS</b>	

## Functions

By default, a report displays a separate row for each record, with the values from the individual records appearing in the corresponding columns in the report, as follows:

Group	Device	Life Count - Total
East	Canon LBP6650dn	24263
East	HP LJ Pro CM1415fnw	12561
East	KM bizhub C552DS	1244
East	Oki MPS480mb	51331
West	Kyocera FS-6025MFP	5621
West	Samsung CLX-3175	26626

If your report definition includes a meter or date-based field (such as Life Count - Total in this example), you have the option of changing the field to a function so that it aggregates the records (bundles together all the records that share the same values for the remaining fields) and displays just the aggregated function's value. For example, if you only wanted the sum of the totals for the groups from the previous table, and didn't need to see the individual devices you could use a function to create a report like the one below:

Group	Life Count - Total
East	89399
West	32247

**Available Functions.** For date-based fields, you can choose from MIN or MAX.

- MIN will display the earliest date from the results included in the report.
- MAX will display the latest date from the results included in the report.

For meter fields, you can choose from SUM, AVG, MIN, or MAX.

- SUM will display the sum of the results included in the report.
- AVG will display the average of the results included in the report.
- MIN will display the minimum value from the results included in the report.
- MAX will display the maximum value from the results included in the report.

If you want, you can include multiple functions in your report. For example, in a report on devices, you could include both the Life Count - Mono and Life-Count - Color meter fields, and set each of them to display the sum of the values for the aggregated devices.

**Example.** Imagine that you just want to report on the total number of pages printed by your network and local devices. One way to do that is to display one row for each device and include a SUM summary of the Life Count Total Current Value at the bottom of the report (see "Summaries" on page 51).

DEVICE TYPE: **Local**

DEVICE NAME	TOTAL LIFE COUNT CURRENT VALUE
C710	98
HP Color LaserJet 2605dn	392
HP LaserJet 1020	3135
Lexmark X543 XL	1
<b>SUM</b>	<b>3626</b>

DEVICE TYPE: **Network**

DEVICE NAME	TOTAL LIFE COUNT CURRENT VALUE
B431	7
Canon iR-ADV C2020 30.06	756
HP Color LaserJet 2605dn	392
HP Color LaserJet CP2025dn	315
<b>SUM</b>	<b>1470</b>

That would be a reasonable solution if you wanted to see the individual page totals for every device, but if you have hundreds of devices then it becomes quite a lengthy report for just the one small piece of information you're interested in. If you don't care about the individual devices, you can simply remove the Device Name field from your report definition and change the Life Count Total Current Value field to a SUM function. The corresponding report would now look like this:

DEVICE TYPE	TOTAL LIFE COUNT	CURRENT VALUE
Network		1470
Local		3626

**Limitations.** Using functions can obviously produce a much more concise report, but there are some limitations to be aware of:

- If you need to include in your report a field for which there is a high degree of variability among the values for each record (such as Device Name), or possibly even unique values (such as MAC address), then PrintFleet will not be able to effectively aggregate the rows, and you will end up with lots of rows, most of which are only aggregating one or two records.
- Similarly, each field you add to your report will at least double the number of different combinations of fields, which in turn reduces the number of values that can be aggregated together, to the point where the aggregation can quickly become ineffective.

Putting it another way, when using functions, the fewer fields you include in the report, and the fewer unique values there are among those fields, the more effective the aggregation function will be.

## Record Counts

By default, when you create a report definition, there will be one row in the report output for each record you are reporting on (device or DCA). However, if you include a function in the report (see "Functions" on page 48), the rows in the report are automatically aggregated. For example, consider the following report showing the total number of mono and color pages for each group.

**Page Totals by Group**  
The total number of mono and color pages per group

GROUP BREADCRUMB	MONO LIFE COUNT CURRENT VALUE	COLOR LIFE COUNT CURRENT VALUE
Root Group > ACME Printing	99879	73050
Root Group > ACME Printing > East	0	1
Root Group > ACME Printing > East > Development	127	972
Root Group > ACME Printing > East > Sales	702	159
Root Group > ACME Printing > West	4569	874
Root Group > ACME Printing > West > HQ	324778	21971
Root Group > ACME Printing > West > Manufacturing	77559	6694
SUM	507614	103721

In such a report you can't tell how many records (in this case printers) each row represents. If it is important to know how many records are represented in each row of a report that includes a function, you can add a special field called **Record Count** to your report.

**Page Totals by Group**  
The total number of mono and color pages per group

GROUP BREADCRUMB	MONO LIFE COUNT CURRENT VALUE	COLOR LIFE COUNT CURRENT VALUE	RECORD COUNT
Root Group > ACME Printing	99879	73050	27
Root Group > ACME Printing > East	0	1	2
Root Group > ACME Printing > East > Development	127	972	3
Root Group > ACME Printing > East > Sales	702	159	3
Root Group > ACME Printing > West	4569	874	2
Root Group > ACME Printing > West > HQ	324778	21971	3
Root Group > ACME Printing > West > Manufacturing	77559	6694	4
SUM	507614	103721	

With the addition of the Record Count field, you can now tell how many printers contributed to the aggregated page totals for each group.

## Summaries

When you include a meter or date-based field in a report, you have the option of including a summary for that field at the bottom of the report.

**Page Totals by Group**  
The total number of mono and color pages per group

GROUP BREADCRUMB	MONO LIFE COUNT CURRENT VALUE	COLOR LIFE COUNT CURRENT VALUE	RECORD COUNT
Root Group > ACME Printing	99879	73050	27
Root Group > ACME Printing > East	0	1	2
Root Group > ACME Printing > East > Development	127	972	3
Root Group > ACME Printing > East > Sales	702	159	3
Root Group > ACME Printing > West	4569	874	2
Root Group > ACME Printing > West > HQ	324778	21971	3
Root Group > ACME Printing > West > Manufacturing	77559	6694	4
SUM	507614	103721	
AVG	72516.3	14817.3	
MIN	0	1	
MAX	324778	73050	

For date-based fields, you can choose from MIN or MAX.

- MIN will display the earliest date from the results included in the report.
- MAX will display the latest date from the results included in the report.

For meter fields, you can choose from SUM, AVG, MIN, or MAX.

- SUM will display the sum of the results included in the report.
- AVG will display the average of the results included in the report.
- MIN will display the minimum value from the results included in the report.
- MAX will display the maximum value from the results included in the report.

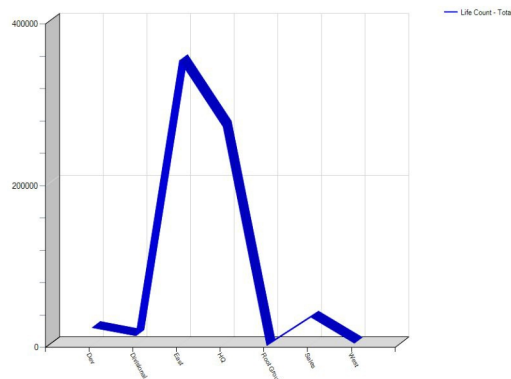
You can select as many of the optional summaries as you want to display in the report. If there are multiple meter or date-based fields in the report, you can also choose which summaries to display for which field. For example, in a report on devices, you could display the **MIN** summary for the **First Seen** field and the **MAX** summary for the **Last Active** field.

If the report has nesting applied, note that the summary only applies to the last level of nesting. You will not get a summary of any fields nested at a higher level, nor will you get a summary of the entire report.

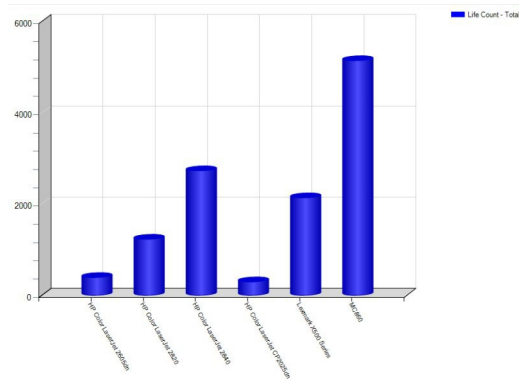
## Charts

Often a chart can be more effective than a table as a way of conveying information. Charts also help make a report look professional. You can add the following types of charts to your reports: Line

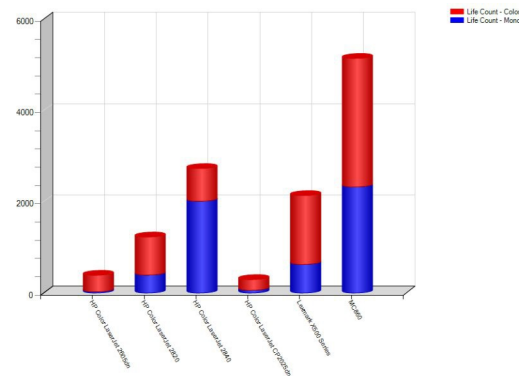
A line chart is good for showing trends.



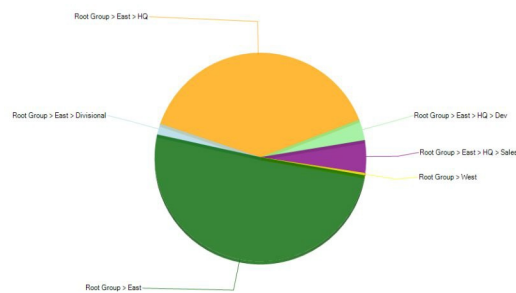
**Bar.** A bar chart is good way to compare different values. For example, you might want to compare the total number of pages printed by the devices in a group.



**Stacked Bar.** A stacked bar chart is effective when there are multiple values that contribute to a total, and you want to compare the totals. For example, you might show the total pages printed by color-capable devices as a combination of mono and color pages.



**Pie.** A pie chart is a good way to show the relative amount each component contributes to a total. For example, you might show how many pages are printed by each group.



Only numeric fields are available to be used in the **Vertical Axis**. Also, in standard report definitions all **Vertical Axis** fields must be

of the same unit (Record Count, Page Count, Percent, PPM, or Yield).

## 3.4 Creating Report Definitions

### Creating a Standard report definition

PrintFleet allows you to generate a variety of Standard reports.

#### Procedure

1. From the main menu, click **Reports**.
2. From the **Reports** page, click **Create Report Definition**. The **Create/Edit Report Definition** page appears.
3. In the **Definition Setup** area, do the following:
  - In the **Name** box, enter a name for the report.
  - In the **Description** box, enter a description for the report.
  - From the **Report Type** drop-down list, select **Standard**.
  - In the **Report Output Template** area, do the following:
    - In the **Title** box, enter the title you want to appear at the top of the report.
    - In the **Subtitle** box, enter a subtitle for the report.
    - In the **Comment** box, enter any additional text that you would like to appear in the report below the title and subtitle.

#### Note

If you want you can include variables in report titles, subtitles, and comments. For more information, see "Using Variables in Titles, Subtitles, and Comments" on page 58.

4. In the **Dataset** area, from the **Dataset** drop-down list, select from one of the following categories of data to base the report on:
  - DCA
  - Device
5. In the **Fields** area, do the following:
  - Click **Add Field**. A new text box will appear. By default, the text box displays the name of the field selected below the text box.
  - Below the new text box, click the name of the field to select a different field. A popup dialog opens.
  - In the popup dialog, under **Field Type**, click the type of field you want to use in the report. The **Field** list changes to reflect your selection.
  - If the **Field Type** you selected is *Meters Custom*, a **Meter Label** box appears. By default, the **Meter Label** box is automatically set to the *LIFECOUNT* meter. If you want to

use a different meter, type the name of the meter you want to use in the **Meter Label** box.

<b>Note</b>	If necessary you can find the names of the meters available for a given device by opening the <b>Meters</b> tab of the <b>Device Detail</b> page for that device.
-------------	---

- From the **Field** list, click the field you want to add. The text box automatically displays the name of the selected field. If you want different text to appear for that field in the report, simply edit the field name in the text box.

<b>Note</b>	When running the report PrintFleet automatically converts all field name text to uppercase column headings.
-------------	---

- Depending on the field you select, a **Function** option may appear below the text box for the field. By default the function is set to None. If you want, you can specify a different function by clicking the selected function. The available functions include SUM, AVG, MIN, and MAX, although only some of these may be available for a given field. See "Functions" on page 48.
- Repeat these steps for each additional field you want to add to the report. To delete a field you have added, click **Delete** below the text box for that field.
- For a tabular report, the fields will appear in the order in which they are listed in the report definition. To change the relative position of fields, click and hold the handle to the left of the text box and drag the field up or down in the list of fields.

<b>Note</b>	If you include the <b>Device String</b> field in a report, keep in mind that the information that appears for this field is determined by the <b>Device Name Template</b> setting in your preferences.
-------------	--

6. In the **Formatting** area, do the following:

- Use the **Nest rows by the first <#> fields** option to specify the number of levels of nesting in the report. By default the nesting level is set to 0, meaning there will be no nesting and all rows will display all fields. You can have up to 3 levels of nesting in a report. See "Nesting" on page 44.
- Use the **Sort rows by <field> in <direction> order** option to specify how the report will be sorted. If you have specified a nesting level greater than 0 for the report, the sorting will be applied after the nesting. See "Sorting" on page 47.

- Select the **Show row counts** check box if you want row counts to be displayed in the report. See "Row Counts" on page 47.
7. In the **Summaries** area, for each field listed, do the following:
- Select the **SUM** check box if you want a sum of the field's values displayed in the report.
  - Select the **AVG** check box if you want an average of the field's values displayed in the report.
  - Select the **MIN** check box if you want the minimum value of the field displayed in the report.
  - Select the **MAX** check box if you want the maximum value of the field displayed in the report.

For more information on Summaries, see "Summaries" on page 51.

In the **Charting** area, if you want the report to display a chart, do the following:

- From the **Chart Type** drop-down list, select the type of chart you want to add (Line, Bar, Stacked Bar, or Pie).
- From the **Horizontal Axis** drop-down list, choose the field you want to use as the horizontal axis for the report.
- From the **Vertical Axis** drop-down list, choose a numeric field you want to use as the vertical axis for the report. When you choose one vertical axis field, another drop-down list will automatically appear to allow you to choose an additional field. You can specify multiple fields for the vertical axis when using a Bar, Stacked Bar, or Line chart type.

<b>Note</b>	If you do not specify fields to use for both the horizontal and vertical axis, you will get an error when you run the report definition.
-------------	--

For more information on charts, see "Charts" on page 52.

8. Click **Save** at the bottom of the page to save the report definition and proceed automatically to the **Report Parameters** page.

## Creating an Executive report definition

PrintFleet allows you to combine multiple standard and SQL reports into a single Executive report. An Executive report can have cover pages which can include custom graphics, allowing you to apply your corporate logo.

<b>Note</b>	If you create an Executive report that includes multiple SQL reports which use date variables, be aware that you will only be able to specify one start date and one end date for the Executive report. For more information, see "Working with Date Variables" on page 66.
-------------	---

### Procedure

1. From the main menu, click **Reports**.
2. From the **Reports** page, click **Create Report Definition**. The **Create/Edit Report Definition** page appears.
3. In the **Definition Setup** area, do the following:
  - In the **Name** box, enter a name for the report.
  - In the **Description** box, enter a description for the report.
  - From the **Report Type** drop-down list, select **Executive**.
4. In the **Report Output Template** area, do the following:
  - In the **Title** box, enter the title you want to appear at the top of the report.
  - In the **Subtitle** box, enter a subtitle for the report.
  - In the **Comment** box, enter any additional text that you would like to appear in the report below the title and subtitle.

<b>Note</b>	If you want you can include variables in report titles, subtitles, and comments. For more information, see "Using Variables in Titles, Subtitles, and Comments" on page 58.
-------------	---

5. In the **Cover Page Options** area, use the **Front Cover** and **Back Cover** lists to determine whether you want cover pages included and if so what to display on them, as follows:
  - **Do not include**—Choose this option if you do not want a cover page included in the report.
  - **Include with branding**—Choose this option if you want a cover page included in the report, and you want the cover page to display a custom image. For information on changing the image that appears, see "Customizing the Executive Report cover" on page 133.
  - **Include without branding**—Choose this option if you want the associated cover page included in the report, but you only want it to display the title, subtitle, and comment specified in the executive report definition.

<b>Note</b>	This option is not available for the back cover.
-------------	--

6. For each report you want to include in your Executive report, in the **Include Report Definitions** area, click in the drop-down list and select the standard or SQL report to include.

<b>Note</b>	The order in which the reports are listed in the definition is the order in which they will appear in the report. If you want, you can click and drag the report definitions to change their relative positions.
-------------	--

- Click **Save** at the bottom of the page to save the report definition and proceed automatically to the **Report Parameters** page.

## Using Variables in Titles, Subtitles, and Comments

If you want you can use variables in the title, subtitle, or comment in a report. Variables act as placeholders for certain properties that can be evaluated and inserted at the time a report is run. By adding a variable to a report definition you can run the same report in different circumstances and be able to easily identify those circumstances from the value of the variable. For example, you could include variables that identify the group the report is run against, the date the report was run, or the user who ran the report. The complete list of supported variables is as follows:

### Supported Report Variables

Variable	Description
\$pfCurrentUserName	Displays the name of the user running the report (or the person who scheduled the report to be run).
\$pfGroupName	Displays the name of the group the report is run against.
\$pfGroupBreadcrumb	Displays the full path of the group the report is run against.
\$pfStartDate	For reports that require a date range, displays the start date of the specified range.
\$pfStartTime	For reports that require a date range, displays the start time of the specified range.
\$pfEndDate	For reports that require a date range, displays the end date of the specified range.
\$pfEndTime	For reports that require a date range, displays the end time of the specified range.
\$pfDate	Displays the date the report is run.
\$pfTime	Displays the time the report is run.

### Procedure

- From the **Create/Edit Report Definition** page, under **Report Output Template**, click in the **Title**, **Subtitle**, or **Comment** fields at the point where you want the variable to appear.
- Type the variable you want to use. The variable can be used along with regular text. For example, if you wanted the report to

display the group name, you might type something like the following:

*Devices in group \$pfGroupName*

## 3.5 Specifying Report Parameters

A report definition specifies the structure of a report. The actual data used to populate the report, such as the group the report is run against, is determined by your selection on the **Report Parameters** page.

<b>Note</b>	The <b>Report Parameters</b> page opens automatically when you save changes to a report definition. You can also access the page by clicking <b>Run</b> from the <b>Reports</b> page.
-------------	---

The **Report Parameters** page is also used to specify who can access the report. The **Access** field in the **Definition Summary** area describes the current access settings for the report. By default, each report you create is private; no other users are able to see, edit, or use the report. If you want to share the report with other users you must change the access settings from this page. For more information, see "Report Security" on page 71.

An executive report has its own security settings that supercede the security settings for the individual reports it includes. For example, one user might create a standard report and set the security to be shared with members of his own group only. Another user with whom that report has been shared can then create an executive report which includes the shared report, and share the executive report with a completely different group.

### Changing the access settings for a report definition

#### Procedure

1. From the **Report Parameters** page, under **Definition Summary**, click **Share with Group**. The **Report Definition Access** dialog opens.
2. In the **Report Definition Access** dialog, select one of the following:
  - **Private**
  - **Share for Full Access (Run & Manage) with Group**
3. If you selected **Share for Full Access (Run & Manage) with Group**, do the following:
  - Click the drop-down arrow in the combo box and use the control to select the group with which you want to share the report definition.
  - Choose the **All Roles** option if you want all roles to be able to access the report definition, or choose the **Restrict to**

**Specific Roles** option if you want to select specific roles within the specified group.

<b>Note</b>	<p>If you choose the All Roles option:</p> <ul style="list-style-type: none"> <li>All users assigned to the specified group, as well as all users assigned to all groups both above and below the specified group, will be able to run and schedule the shared report definition.</li> </ul>
<b>Note</b>	<ul style="list-style-type: none"> <li>All users who have the Report Management permission, and who are assigned to the specified group (or to a higher group), will be able to edit and delete the shared report definition.</li> </ul>
<ul style="list-style-type: none"> <li>If you selected the <b>Restrict to Specific Roles</b> option, a list of roles appears. Select the check box for each role you want to be able to access the report definition.</li> </ul>	
<b>Note</b>	<p>If you choose the Restrict to Specific Roles option:</p> <ul style="list-style-type: none"> <li>All users assigned to the specified role, and who are assigned to either the specified group or to any group above or below the specified group, will be able to run and schedule the shared report definition.</li> <li>All users assigned to the specified role, and who are assigned to either the specified group or a higher group, and who have the Report Management permission, will be able to edit and delete the shared report definition.</li> </ul>

- Click **Save Access Settings** to save your changes.

## Running a report definition

### Procedure

1. On the **Run Now** tab of the **Report Parameters** page, in the **Report Parameters** area, specify any required parameters for the report definition.

### Note

If you are running a SQL report (or an Executive report that includes a SQL report), and the SQL query in the SQL report definition includes date variables, you will be prompted at run time to specify the required date parameters for the report. For more information, see "Specifying date parameters when running a report" on page 66.

2. Click **Run Report**. The report appears in the Report Viewer. For more information, see "Viewing Reports".

## 3.6 Viewing and saving reports

The **Report Viewer** displays the output of a report. From the **Report Viewer** you can also:

Click to return to the **Report Parameters** page where you can change the report parameters and rerun the report definition.

- Save the report output to a file in CSV (Comma-separated values in a text file), TAB (Tab-separated values in a text file), or PDF (Adobe Portable Document Format) format.

### Note

For an executive report only the PDF option is available.

### Saving a report in Adobe PDF

#### Procedure

- After generating a report, in the **Report Viewer**, click **Save As**, and then click **PDF**.

### Save a report in tab-separated values format

#### Procedure

- After generating a report, in the **Report Viewer**, click **Save As**, and then click **TAB**.

### Saving a report in comma-separated values format

#### Procedure

- After generating a report, in the **Report Viewer**, click **Save As**, and then click **CSV**.

## 3.7 Scheduling Reports

For reports that you want to run at specified times or at regular intervals you can create a schedule. When the indicated time arrives PrintFleet will automatically run the report and email the results to a specified user. For standard or SQL reports you can specify whether to create the report in PDF or CSV format.

### Procedure

1. From the main menu, click **Reports**. The **Reports** page opens.
2. From the **Reports** page, under **Options**, click **Schedules** beside the report definition you want to schedule. The **Report Parameters** page opens.
3. From the **Report Parameters** page, click **Create Schedule**. A **Create Schedule** tab appears.
4. In the **Schedule Details** area, in the **Name** box, type a name for the schedule. The name is used to identify the schedule. The name will also appear as part of the subject heading in the email that is sent by PrintFleet to the specified recipient(s). The schedule name does not appear within the report itself.
5. In the **Email Recipients** box, type the email address of the person who should receive the report. If you want to have the report sent to multiple people, enter as many addresses as necessary, separating them with spaces, commas, or semicolons.
6. If you are scheduling a standard or SQL report, from the **Report Format** list, select the file format (PDF or CSV) in which you want to receive the report.
7. Beside **Schedule**, choose the most appropriate interval for the schedule, specifying the details as follows:
  - **Once**—Specify the date on which to run the report definition.
  - **Daily**—Specify the interval in days, and the date from which the schedule should start.
  - **Weekly**—Specify the interval in weeks, the day of the week, and the date from which the schedule should start.
  - **Monthly**—Specify which day of the month, the interval in months, and the date from which the schedule should start.
  - **Advanced**—Specify which week of the month, which day of the week, the interval in months, and the date from which the schedule should start.
8. In the **Report Parameters** area, specify any required parameters for the report. These may include any of the following:
  - **Group**—Click the drop-down arrow to choose the group against which to run the report.
  - **Reporting Period**—Click the drop-down arrow and choose the reporting period. Note that the reporting period is

relative to the date on which the report is scheduled to run. For example, if you scheduled the report to be run once at 5:00 PM on October 15, and you set the reporting period to be **7 Days**, the report would cover the period from 5:00 PM October 8 to 5:00 PM October 15. For more information, see "Specifying date parameters when scheduling a report" on page 68.

- Click **Save Schedule**. The new schedule appears on the **Schedules** tab of the **Report Parameters** page.

**Important:** Do not associate reports to the default user, **Start**. Any items associated with this function may not work properly.

## 3.8 Managing Report Definitions

As you create and refine your report definitions you will likely find it convenient to be able to perform various management activities, such as editing, copying, and deleting report definitions.

<b>Note</b>	You can not edit or delete the sample reports that have been created by PrintFleet.
-------------	---

### Editing a report definition

#### Procedure

- On the main menu, click **Reports**. The **Reports** page opens.
- On the **Reports** page, under **Options**, click **Edit** beside the report definition you want to edit. The **Create/Edit Report Definition** page appears.
- Make the desired changes to the report.
- Click **Save** to save your changes.

### Copying a report definition

#### Procedure

- On the main menu, click **Reports**. The **Reports** page opens.
- On the **Reports** page, under **Options**, click **Copy** beside the report definition you want to copy. The **Create/Edit Report Definition** page appears.
- On the **Create/Edit Report Definition** page, under **Definition Setup**, provide a new name for the report definition in the **Name** box.
- Make any other changes to the report definition.
- Click **Save** to save your changes.

## Deleting a report definition

### Procedure

1. On the main menu, click **Reports**. The **Reports** page opens.
2. On the **Reports** page, under **Options**, click **Delete** beside the report definition you want to delete. A **Delete Confirmation** dialog appears.
3. Click **Continue** to verify that you want to delete the report definition.

## 3.9 Managing Report Schedules

As you create and refine your report schedules you will likely find it convenient to be able to locate, edit, and delete report schedules.

There are two pages from which you can view and manage schedules. Which one you should use depends on whether you are managing schedules for multiple report definitions, or just for one report definition.

## Managing schedules for a specific definition

If you are only interested in the schedules for a particular report definition, you will likely want to open the **Schedules** tab from the **Report Parameters** page for that report definition. Only the schedules associated with that report definition will appear.

## Viewing the schedules for a specific report definition

### Procedure

1. On the main menu, click **Reports**. The **Reports** page opens.
2. On the **Definitions** tab of the **Reports** page, under **Options**, click **Schedules** beside the report definition for which you want to view the schedules. The **Schedules** tab opens in the **Report Parameters** page.
3. The schedules for the specified report definition are displayed in the table. If necessary, you can:
  - scroll down to view additional schedules on the page
  - change the number of schedules that can be displayed on the page
  - view other pages of schedules for the definition
  - sort the schedules for the definition by clicking any column heading

## Editing a schedule for a report definition

### Procedure

1. On the **Schedules** tab of the **Report Parameters** page, under **Options**, click **Edit** beside the schedule you want to edit. The **Edit Schedule** tab opens.
2. Make the necessary changes to the schedule. See "Scheduling Reports" on page 62.

3. Click **Save Schedule**.

### Deleting a schedule for a report definition

#### Procedure

1. On the **Schedules** tab of the **Report Parameters** page, under **Options**, click **Delete** beside the schedule you want to delete. A **Delete Confirmation** dialog opens.
2. Click **Continue**.

### Managing schedules for multiple definitions

If you are managing schedules for multiple report definitions, it might be helpful to see a list of all the schedules you have access to at one time.

### Viewing the report schedules

#### Procedure

1. On the main menu, click **Reports**. The **Reports** page opens.
2. On the **Reports** page, click the **Schedules** tab.
3. On the **Schedules** tab, under **Group Selection**, use the drop-down list to select the group for which you want to view the report schedules.

#### Note

To see all of the report schedules to which you have access, select the highest group available from the group list. To see just the report schedules to which you have access in a subgroup, choose the subgroup from the group list.

4. The schedules associated with the selected group are displayed in the table. If necessary, you can:
  - scroll down to view additional schedules on the page
  - change the number of schedules that can be displayed on the page
  - view other pages of schedules for the group
  - sort the schedules for the group by clicking any column heading
  - select a different group

### Editing a report schedule

#### Procedure

1. On the **Schedules** tab of the **Reports** page, under **Options**, click **Edit** beside the schedule you want to edit. The **Edit Schedule** tab opens.
2. Make the necessary changes to the schedule. See "Scheduling Reports" on page 62.
3. Click **Save Schedule**.

## Deleting a report schedule

### Procedure

1. On the **Schedules** tab of the **Reports** page, under **Options**, click **Delete** in the row of the report schedule that you want to delete.
2. Click **Continue** to verify deletion of the schedule.

## 3.10 Working with Date Variables

Some reports (such as Model Counts, or Hidden Devices) are not date sensitive. For example, with the Model Counts report, you are only interested in how many of each model exist in a group, not how many existed over a specified period. For other reports (such as Volumes by Manufacturer), you will want to be able to determine how many pages were printed over a specified period. This section of the guide will describe how to add date variables to reports you create, and how to provide the corresponding date parameters when running and scheduling reports.

### Specifying date parameters when running a report

When running a SQL report that includes start or end date variables, you will be prompted to specify date parameters for the report. The options available will vary depending on whether the report requires a start date, an end date, or both.

For SQL reports that require a start date, the available **Start Date** choices are as follows:

- **24 hours ago**—The reporting period will cover the 24 hours immediately preceding the time the report runs. If you run the report at 5:00 PM on October 15, and you set the **Start Date** to be **24 hours ago**, the report will cover the period from 5:00 PM October 14 to 5:00 PM October 15.
- **7 days ago**—The reporting period will cover the 7 days immediately preceding the time the report runs. If you run the report at 5:00 PM on October 15, and you set the **Start Date** to be **7 days ago**, the report will cover the period from 5:00 PM October 8 to 5:00 PM October 15.
- **30 days ago**—The reporting period will cover the 30 days immediately preceding the time the report runs. If you run the report at 5:00 PM on October 15, and you set the **Start Date** to be **30 days ago**, the report will cover the period from 5:00 PM September 15 to 5:00 PM October 15.
- **90 days ago**—The reporting period will cover the 90 days immediately preceding the time the report runs. If you run the report at 5:00 PM on October 15, and you set the **Start Date** to be **90 days ago**, the report will cover the period from 5:00 PM July 17 to 5:00 PM October 15.
- **Start of month**—The reporting period will cover the time from the start of the calendar month in which the report is run. If you run the report at 5:00 PM on October 15, and you set the **Start**

---

**Date** to be **Start of month**, the report will cover the period from 00:00 AM October 1 to 5:00 PM October 15.

- **Start of last month**—The reporting period will cover the time from the start of the calendar month preceding the calendar month in which the report is run. If you run the report at 5:00 PM on October 15, and you set the **Start Date** to be **Start of last month**, the report will cover the period from 00:00 AM September 1 to 5:00 PM October 15.
- **Advanced**—If none of the provided options meet your requirements, select this option and then specify the date and time you want to use for the report.
- For SQL reports that just require an end date, the available **End Date** choices are as follows:
  - **Now**—The reporting period will cover the time up to the point the report runs. If you run the report at 5:00 PM on October 15, and you set the **End Date** to be **Now**, the report will cover the period up to 5:00 PM October 15.
  - **End of last month**—The reporting period will cover the time up to the end of the previous calendar month from which the report is run. If you run the report at 5:00 PM on October 15, and you set the **End Date** to be **End of last month**, the report will cover the period up to 00:00 AM October 1.
- **Advanced**—If none of the provided options meet your requirements, select this option and then specify the date and time you want to use for the report.

For SQL reports that require both a start date and an end date, the available **Reporting Period** choices are as follows:

- **Last 24 hours**—The reporting period will cover the 24 hours immediately preceding the time the report runs. If you run the report at 5:00 PM on October 15, and you set the **Reporting Period** to be **Last 24 hours**, the report will cover the period from 5:00 PM October 14 to 5:00 PM October 15.
- **Last 7 days**—The reporting period will cover the 7 days immediately preceding the time the report runs. If you run the report at 5:00 PM on October 15, and you set the **Reporting Period** to be **Last 7 days**, the report will cover the period from 5:00 PM October 8 to 5:00 PM October 15.
- **Last 30 days**—The reporting period will cover the 30 days immediately preceding the time the report runs. If you run the report at 5:00 PM on October 15, and you set the **Reporting Period** to be **Last 30 days**, the report will cover the period from 5:00 PM September 15 to 5:00 PM October 15.
- **Last 90 days**—The reporting period will cover the 90 days immediately preceding the time the report runs. If you run the report at 5:00 PM on October 15, and you set the **Reporting Period** to be **90 Days**, the report will cover the period from 5:00 PM July 17 to 5:00 PM October 15.
- **This month**—The reporting period will cover the time from the start of the calendar month in which the report is run. If you run the report at 5:00 PM on October 15, and you set the

**Reporting Period** to be **This Month**, the report will cover the period from 00:00 AM October 1 to 5:00 PM October 15.

- **Last month**—The reporting period will cover the time from the start of the calendar month preceding the calendar month in which the report is run. If you run the report at 5:00 PM on October 15, and you set the **Reporting Period** to be **Last month**, the report will cover the period from 00:00 AM September 1 to 00:00 AM October 1.
- **Advanced**—If none of the provided options meet your requirements, select this option and then specify the dates and times you want to use for the report.
  - **Start date**—Specify the date and time you want to use for the start date for the report.
  - **End date**—Specify the date and time you want to use for the end date for the report.

**Running an Executive Report.** When you are running an executive report that includes one or more SQL reports with date variables, be aware that the date requirements for the individual reports are amalgamated and presented as though it was a single report. Specifically:

- if one or more individual SQL reports require a start date, the executive report will prompt you to enter one start date. The start date you enter will be used for all of the individual SQL reports that require a start date.
- if one or more individual SQL reports require an end date, the executive report will prompt you to enter one end date. The end date you enter will be used for all of the individual SQL reports that require an end date.
- if both a start and an end date are required by the combined individual SQL reports, the executive report will prompt you for a date range. The start of the range you enter will be used for all start dates required in the individual SQL reports, and the end of the range you enter will be used for all end dates required in the individual SQL reports. Note that the start of the date range has no effect on individual reports that require just an end date, and the end of the date range has no effect on individual reports that require just a start date.

## Specifying date parameters when scheduling a report

When scheduling a SQL report that includes start or end date variables, you will be prompted to specify a reporting period—the dates covered by the report. The reporting period is relative to when the report is scheduled to run. Also, the options available in the **Reporting Period** list will vary depending on whether the report requires a start date, an end date, or both.

For SQL reports that just require a start date, the available choices are as follows:

- **24 hours**—The reporting period will cover the 24 hours immediately preceding the time the report runs. If you schedule the report to be run once at 5:00 PM on October 15, and you set

---

the **Reporting Period** to be **24 hours**, the report will cover the period from 5:00 PM October 14 to 5:00 PM October 15.

- **7 days**—The reporting period will cover the 7 days immediately preceding the time the report runs. If you schedule the report to be run once at 5:00 PM on October 15, and you set the **Reporting Period** to be **7 days**, the report will cover the period from 5:00 PM October 8 to 5:00 PM October 15.
- **30 days**—The reporting period will cover the 30 days immediately preceding the time the report runs. If you schedule the report to be run once at 5:00 PM on October 15, and you set the **Reporting Period** to be **30 days**, the report will cover the period from 5:00 PM September 15 to 5:00 PM October 15.
- **90 days**—The reporting period will cover the 90 days immediately preceding the time the report runs. If you schedule the report to be run once at 5:00 PM on October 15, and you set the **Reporting Period** to be **90 days**, the report will cover the period from 5:00 PM July 17 to 5:00 PM October 15.
- **Calendar month**—The reporting period will cover the time from the start of the month in which the schedule is run. If you schedule the report to be run once at 5:00 PM on October 15, and you set the **Reporting Period** to be **Calendar month**, the report will cover the period from 00:00 AM October 1 to 5:00 PM October 15.
- **Previous calendar month**—The reporting period will cover the time from the start of the calendar month preceding the calendar month in which the schedule is run. If you schedule the report to be run once at 5:00 PM on October 15, and you set the **Reporting Period** to be **Previous calendar month**, the report will cover the period from 00:00 AM September 1 to 00:00 AM October 1.
- **Advanced**—If none of the provided options meet your requirements, select this option and use the **Start Date** options to specify the number of days (or months) before (or after) one of the following:
  - **Report run time**—Determine the start of the reporting period relative to the date the report is scheduled to run.
  - **Month Start**—Specify the start of the reporting period as an offset from the start of the calendar month in which the report is scheduled to be run.
  - **Month End**—Specify the start of the reporting period as an offset from the end of the calendar month in which the report is scheduled to be run.

For SQL reports that just require an end date, the available choices are as follows:

- **Report run time**—The reporting period will end at the time the report runs. If you schedule the report to be run once at 5:00 PM on October 15, and you set the **Reporting Period** to be

**Report run time**, the report will cover the period up until 5:00 PM October 15.

- **Previous calendar month**—The reporting period will cover the time up until the end of the calendar month preceding the calendar month in which the schedule is run. If you schedule the report to be run once at 5:00 PM on October 15, and you set the **Reporting Period** to be **Previous calendar month**, the report will cover the period up until 00:00 AM October 1.
- **Advanced**—If none of the provided options meet your requirements, select this option and use the **End Date** options to specify the number of days (or months) before (or after) one of the following:
  - **Report Run Time**—Determine the end of the reporting period relative to the date the report is scheduled to run.
  - **Month Start**—Specify the end of the reporting period as an offset from the start of the calendar month in which the report is run.
  - **Month End**—Specify the end of the reporting period as an offset from the end of the calendar month in which the report is run.

For SQL reports that require both a start date and an end date, the available choices are as follows:

- **24 hours**—The reporting period will cover the 24 hours immediately preceding the time the report runs. If you schedule the report to be run once at 5:00 PM on October 15, and you set the **Reporting Period** to be **24 hours**, the report will cover the period from 5:00 PM October 14 to 5:00 PM October 15.
- **7 days**—The reporting period will cover the 7 days immediately preceding the time the report runs. If you schedule the report to be run once at 5:00 PM on October 15, and you set the **Reporting Period** to be **7 days**, the report will cover the period from 5:00 PM October 8 to 5:00 PM October 15.
- **30 days**—The reporting period will cover the 30 days immediately preceding the time the report runs. If you schedule the report to be run once at 5:00 PM on October 15, and you set the **Reporting Period** to be **30 days**, the report will cover the period from 5:00 PM September 15 to 5:00 PM October 15.
- **90 days**—The reporting period will cover the 90 days immediately preceding the time the report runs. If you schedule the report to be run once at 5:00 PM on October 15, and you set the **Reporting Period** to be **90 days**, the report will cover the period from 5:00 PM July 17 to 5:00 PM October 15.
- **Calendar month**—The reporting period will cover the calendar month in which the schedule is run. If you schedule the report to be run once at 5:00 PM on October 15, and you set the **Reporting Period** to be **Calendar month**, the report will cover the period from 00:00 AM October 1 to 5:00 PM October 15.
- **Previous calendar month**—The reporting period will cover the calendar month preceding the calendar month in which the schedule is run. If you schedule the report to be run once at

5:00 PM on October 15, and you set the **Reporting Period** to be **Previous calendar Month**, the report will cover the period from 00:00 AM September 1 to 00:00 AM October 1.

- **Advanced**—If none of the provided options meet your requirements, select this option and use the **Start Date** and **End Date** options to specify the number of days (or months) before (or after) one of the following:
  - **Report Run Time**—Determine the start or end of the reporting period relative to the date the report is scheduled to run.
  - **Month Start**—Specify the start or end of the reporting period as an offset from the start of the calendar month in which the report is run.
  - **Month End**—Specify the start or end of the reporting period as an offset from the end of the calendar month in which the report is run.

## Scheduling an Executive Report

When you are scheduling an executive report that includes one or more SQL reports with date variables, be aware that the date requirements for the individual reports are amalgamated and presented as though it was a single report. Specifically:

- if one or more individual SQL reports require a start date, the executive report will prompt you to enter one start date. The start date you enter will be used for all of the individual SQL reports that require a start date.
- if one or more individual SQL reports require an end date, the executive report will prompt you to enter one end date. The end date you enter will be used for all of the individual SQL reports that require an end date.
- if both a start and an end date are required by the combined individual SQL reports, the executive report will prompt you for a date range. The start of the range you enter will be used for all start dates required in the individual SQL reports, and the end of the range you enter will be used for all end dates required in the individual SQL reports. The start of the date range has no effect on individual reports that require just an end date, and the end of the date range has no effect on individual reports that require just a start date.

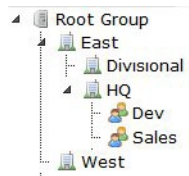
## 3.11 Report Security

To understand how security applies to report definitions and report schedules, you should first familiarize yourself with how security works in general (see "Understanding PrintFleet Security" on page 159). Although these general security principles still apply, there are some additional considerations that affect who can see and use report definitions and report schedules.

## Security for report definitions

The user who creates a report definition can specify whether to keep the report definition Private, or to share it with other users. If the report author chooses to share the report definition, she can specify which group to share it with, and (optionally) which role(s) within the specified group. For more information, see "Specifying Report Parameters" on page 59.

When a report definition is shared with a group, it is automatically shared with all groups above and below the specified group. At first this may seem to include all groups (which would make the selection of a particular group pointless), but the group selection can restrict some groups from accessing the report definition. For example, suppose you have set up your groups like this:



If a user were to share a report definition with the HQ group, that report definition would be automatically shared with the groups below the HQ group (Dev and Sales), as well as the groups above the HQ group (East and Root Group). It would not be shared with either the Divisional or West groups, as they are neither above nor below the specified HQ group.

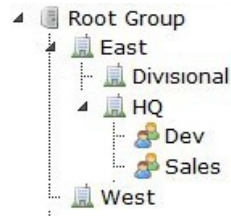
Why are report definitions shared with groups both above and below a specified group? When a user shares a report definition with a group, it is assumed they want to share it with all of that group. As the subgroups of a group are considered to be part of the group, it makes sense that the report definition be shared with the subgroups as well. The reason report definitions are also shared with the groups above the specified group has more to do with management; users in higher groups are considered to require access to any content that users with the same role in a lower group could access.

Any user that is assigned to any group with which a report definition is shared (either directly or indirectly) will be able to run and schedule the report definition.

## Managing shared report definitions

To be able to edit or delete a report definition shared by another user, you must be assigned to either the group to which the report definition was shared or to a higher group. (This is another reason why it makes a difference which group you select when sharing a report definition.)

For example, suppose Betty has been assigned the **Admin** role in the Dev group in the following organization:



If a user were to share a report definition with the HQ group, that report definition would be automatically shared with the groups below the HQ group (Dev and Sales), so Betty would be able to run and schedule the report definition. However, because the report definition was shared with the HQ group (which is above the group to which Betty is assigned), she would not be able to edit or delete the report definition. She would still be able to edit and delete report definitions shared with the Dev group specifically.

### Restricting access by role

The preceding paragraph is based on the assumption that access to the shared report definition was not further restricted by role. If access to a report definition is limited to a specific role, the report definition is still shared with groups above and below the specified group, but only users in those groups that have the specified role(s), will be able to access the report definition.

### Security for sample report definitions

PrintFleet automatically provides a number of sample report definitions. By default these are shared with the root group, which makes them accessible by all users. To protect the integrity of these report definitions, they can not be edited, deleted, or have their access settings modified.

### Security for report schedules

Any user who can see a report schedule can edit or delete the schedule. Whether or not one user can see a report schedule created by another user depends solely on the groups/roles of the user who created the schedule. You can see the report schedules created by another user if you have every group/role combination that they have. To "have" a given group/role combination, you need to have been assigned that role for either the specified group or a higher group.

For example, suppose Henry is a user who has been assigned to the **Dealer** role in the HQ group, and Janet is a user who has been assigned to the **Dealer** role in the Dev group (a subgroup of the HQ group). If Janet were to schedule a report definition, Henry would be able to see the report schedule because he has been assigned the same role as Janet in a group above hers. If Henry were to schedule a report definition, Janet would not be able to see the report schedule because she does not have the **Dealer** role in the HQ group.

# Chapter 4 Alerts

---

Alerts allow you to automatically monitor your devices for problems (or even potential problems) and be notified as soon as they occur. This gives you the ability to respond to service issues quickly, strengthening your just-in-time (JIT) supplies fulfillment and service level agreements (SLAs). With one notification sent per issue you can easily monitor the status of your devices to remain one step ahead.

Alerts can also be used to schedule preventive maintenance. Maintenance can be scheduled based on a device page count or a date.

## 4.1 Overview

To effectively use alerts, you should be familiar with the following concepts:

### Alert definition

You specify how an alert behaves by creating an alert definition. Each alert definition determines:

- what devices or DCAs to monitor
- the alert conditions—what issues you want to check for
- the alert notifications—what you want PrintFleet to do if it determines the alert condition is true

See "Creating Alert Definitions" on page 77.

**Alert conditions** You can use alerts to monitor both DCAs and devices. For DCAs you can check whether or not they are stale. For devices you can check for error codes or supplies. You can also set up recurring alerts for devices based on the number of pages printed or by dates. See "About Alert Conditions" on page 80.

### Alert events

Once an alert definition has been saved and enabled, PrintFleet reads the information in the definition and starts monitoring the indicated objects for the specified conditions. If the alert conditions are found to be true, PrintFleet automatically creates an alert event. The alert event remains "active" until the alert conditions are no longer true.

---

While the alert event is active an icon is displayed. You can view the alert events for all devices from the **Alerts View** page. See "Using the Alerts View" on page 22. You can view the alert events for a specific device from the **Alert Events** tab of the **Device Detail** page. See "Working with the Alerts tab" on page 31.

## Alert notifications

In the alert definition you have the option to specify whether to send notifications of the event. You can choose to send notifications via email, or by posting a Webhook to a URL, or both. You can also specify whether to send the notification at the start of the event, the end of the event, or both.

If necessary, you can also disable an alert definition. When an alert definition is disabled, PrintFleet will ignore the definition; it will not check for the conditions specified in the definition, nor will it send any notifications specified in the definition. See "Disabling and enabling alert conditions" on page 90.

## 4.2 Alerts Security

For each alert definition you create you can specify whether to use basic or advanced security to control:

- Which users can edit an alert definition?
- Which users can see the alert events generated from an alert definition?
- To which devices does the alert definition apply?

### Basic security

In basic security mode (when the **Use advanced security** check box is cleared), you specify all three security settings simply by choosing a Group:

- Any user in the specified group (or a higher group), will be able to see and edit the alert definition.
- Any users who can see the devices that belong to the specified group (or to groups below that group) will be able to see any alert events generated from the alert definition that apply to those devices.
- The alert definition will be automatically applied to all of the devices assigned to the specified group (or to any group below that group).

### Advanced security

In advanced security mode (when the **Use advanced security** check box is selected), you specify the three settings using three different controls:

- As with Basic security, you use the **Group** control to specify who can edit the alert definition. Any user in the specified group (or a higher group), will be able to see and edit the alert definition.
- Use the **Events visible to** control to specify which users can see the associated alert events. You can choose one of the following:
  - **Users that can edit this alert**—Any users who can edit the alert definition will be able to see the alert events generated from it.
  - **Users that can see devices in this alert**—Any users who can see the devices the alert definition applies to will be able to see the alert events generated from the definition for those devices.
- Use the **Applies to** controls to specify what group(s) or device(s) the alert definition applies to. You can choose one or more groups, as well as choose individual devices within groups.

## Possible security scenarios

The advanced security options give you the flexibility to set up your alerts to meet a variety of circumstances. Here are a few possibilities:

### Example #1

Suppose you want all users to be able to see the alert events applied to their devices, but want to restrict access to the alert definition to just those in the root group. In this case you would set the **Group** to be Root Group (or whatever your top-level group is called), and set the **Events visible to** control to **Users that can see devices in this alert**.

### Example #2

Perhaps you want to create an alert that applies to all of your devices, but only want the alert events to be visible to users in the root group. In this case you would set the **Group** to be Root Group (or whatever your top-level group is called), set the **Events visible to** control to **Users that can edit this alert**, and use the **Applies to** control to select the Root Group (all devices in that group and all groups below it).

## 4.3 Creating Alert Definitions

An alert definition determines:

- what devices or DCAs to monitor
- the alert conditions—what issues you want to check for
- the alert notifications—what you want PrintFleet to do if it determines the alert condition is true

### Procedure

1. From the main menu, click **Alerts**.

2. From the **Alerts** page, click **Create Alert Definition**. The **Create/Edit Alert Definition** page appears.
3. In the **Alert Definition** area, do the following:
  - In the **Name** box, enter a name for the alert.
  - From the **Group** drop-down list, choose the group to which the alert will apply.
  - If you want to access additional security options, select the **Use advanced security** check box. An **Advanced Security** tab will open. For more information, see "Alerts Security" on page 76.
  - If you want to disable the alert definition so that it will be temporarily turned off, select the **Disable** check box.
4. If you want to send a notification upon the start or end of the alert event, on the **Notifications** tab, do either or both of the following:
  - To add an email notification:
    - Click **Add Email**.
    - In the **Email(s)** box, type the email address(es) of the person(s) you want to be notified of the alert. If you are adding multiple addresses, separate each address with a space, semicolon, or comma.
    - In the **Subject** box, specify what you would like the subject line of the email notification to include. This must include at least one alert property (such as \$alertname), but can also include regular text (such as "This is an alert"). For a list of the alert properties you can include, see the tooltip that appears when you hover your mouse cursor over the icon to the right of the **Subject** box. The placeholders that you include in the alert definition will be replaced with the actual values when the alert is triggered. For information on changing the default email subject template (the subject that is automatically populated when you create a new alert definition), see "Changing Preferences" on page 95.
    - In the **Header** box, type any information you want to appear above the body in the email.
    - In the **Footer** box, type any information you want to appear below the body in the email.
    - Beside **Trigger on**, select the **event start** check box if you want PrintFleet to send the notification when the alert conditions are met.
    - Beside **Trigger on**, select the **event end** check box if you want PrintFleet to send the notification when the alert conditions are no longer being met.
    - If you want to set up additional email notifications, click **Add Email**, and repeat these steps. For more information about email notifications, see "Working with Alert Emails" on page 91.
  - To add a Webhook notification:

- Click **Add Webhook**. A **Webhook** box appears.
  - In the **Webhook** box, type the full URL (including protocol) to which you want to post a notification of the alert.
  - If you want to verify that PrintFleet is able to successfully post a Webhook notification to the specified URL, click **Test POST**. A message box will appear indicating the result of the test.
  - Beside **Trigger on**, select the **event start** check box if you want PrintFleet to send the notification when the alert conditions are met.
  - Beside **Trigger on**, select the **event end** check box if you want PrintFleet to send the notification when the alert conditions are no longer being met.
  - If you want to set up additional Webhook notifications, click **Add Webhook**, and repeat these steps. For more information about email notifications, see "Working with Alert Webhooks" on page 92.
5. To add a condition to the alert definition, click **Add Condition Type**, and select one of the available types:
- **Supply**—Use this to be notified when a specified supply (such as black toner) is at or below a designated level. For more information, see "Supply alert conditions" on page 80.
  - **Error Codes**—Use this to be notified when a device reports a problem. For more information, see "Error code alert conditions" on page 83.
  - **Stale DCA**—Use this to be notified when a DCA fails to report within a specified number of days. For more information, see "Stale DCA alert conditions" on page 85.
  - **Activated DCA**—Use this to be notified when a DCA has been activated. fails to report within a specified number of days. For more information, see "Activated DCA alert conditions" on page 86
  - **Page Count Recurring**—Use this to be notified every time a device has printed a specified number of pages. For more information, see "Page count recurring alert conditions" on page 87.
  - **Date Recurring**—Use this to be notified on a specific date, or at regularly scheduled intervals. For more information, see "Date recurring alert conditions" on page 88.
6. If you selected the **Use advanced security** check box, complete the **Advanced Security** tab:
- From the **Events visible to** drop-down list, specify who can see the associated alert event.
  - In the **Applies to** area, select the group(s) and/or device(s) to which the alert definition applies.

For more information on the Advanced Security tab, see "Alerts Security" on page 76.

7. Click **Save Definition**. The saved alert definition is displayed in the list of definitions on the **Alerts** page.

## 4.4 About Alert Conditions

There are different condition types you can use in an alert definition: **Supply**, **Error Codes**, **Stale DCA**, **Activated DCA**, **Page Count Recurring**, and **Date Recurring**.

### Supply alert conditions

Use the **Supply** condition type if you want to be alerted when a supply reaches or falls below a specified percentage value.

#### Default Supply Conditions

When you add a **Supply** condition type, PrintFleet automatically creates conditions for the four most common toner colors: Black (TONERLEVEL\_BLACK), Cyan (TONERLEVEL\_CYAN), Magenta (TONERLEVEL\_MAGENTA), and Yellow (TONERLEVEL\_YELLOW). For each of these conditions the threshold value is set to 10%. This is done for your convenience, but you can remove or edit these default conditions, or add other supply conditions, as you like. For example, if you are applying the alert definition to a single device, and that device only has a Black toner cartridge, you could remove the Cyan, Magenta, and Yellow conditions if you want (although they would simply be ignored if the device did not report values for those supplies).

#### Supply Names

The supplies you can monitor will vary between different models and manufacturers. Obviously, a color-capable device will have colored toner supplies that a mono device will not. Less obviously, one mono device might also have supplies (such as waste toner or drum kits) that another mono device does not. In some cases a device may have supplies but not report the levels in a way that allows PrintFleet to recognize them.

The names used to report supplies also vary from one model or manufacturer to another. For example, BLACK IMAGE DRUM UNIT OKI DATA CORP is a valid supply name to enter for an OKI MC860 printer, but would be meaningless for devices from other manufacturers.

PrintFleet has tried to standardize the names for the most common supplies (such as TONERLEVEL\_BLACK, TONERLEVEL\_CYAN, TONERLEVEL\_MAGENTA, and TONERLEVEL\_YELLOW), to make it possible to apply them to as broad a range of devices as possible. However, to be sure which supplies PrintFleet can monitor for a given device, and the names to use for those supplies, go to the **Device Detail** page for that device and click on the **Supplies** tab. Any supply names listed on that tab can be entered in a **Supply** condition in an alert definition applied to that device.

#### Standard Types

---

With the launch of DCA Pulse, PrintFleet introduced Standard Types to identify basic categories of metric data produced by a device's **meters, supplies, error codes** and **attributes**.

DCA Pulse queries each device for specific pieces of information on which the manufacturer has enabled the device to report by using a simple and intuitive hierarchical format going from general to specific as one moves from the top of the hierarchy to the bottom. This means that while BLACK IMAGE DRUM UNIT OKI DATA CORP might mean nothing for devices from vendors other than OKI, DCA Pulse can still make sense of it.

By creating a cohesive system of categorization, DCA Pulse incorporates varying manufacturers' nomenclature and maps them into a single framework that can easily be read and interpreted at a glance.

### Using Wildcards

If you want, you can include an asterisk '\*' in the supply name. This character acts as a wildcard, matching any text. For example, if you wanted to set up an alert to monitor all toner levels, you could either add one entry for each toner color and specify the complete name of each toner supply, or you could add one entry such as 'TONER\*' (which would match any supply name that started with TONER) or even '\*TONER\*' (which would match any supply name that included the word TONER anywhere in the name).

### Threshold Values

Just as different models have different supplies, or different names for similar supplies, they can also report their supplies in different ways. For example, some devices do not report toner supplies as a percentage at all, but rather just report the toner levels as OK, Low, or No Toner. For such devices, if you want to set up an alert for toner levels, you will have to use an **Error Codes** condition type and select the **Low Toner** check box in the **Standard Bits** area.

Other devices that do report toner levels as a percentage can still vary widely in the precision with which they report the levels. For example, some devices only report toner levels in 25% increments (100%, 75%, 50%, 25%, 0%). For such a device it won't be much help to set a supply threshold of 5% or even 10%, because the device will continue to report it has 25% toner remaining right up until the first time it reports that it has 0% toner level, by which time the alert will be too late to prevent some inconvenience for those using the device.

### Detecting a Supply Replacement

PrintFleet uses different methods to detect when a supply has been replaced. For a toner cartridge, these might include:

- detecting that the supply is reporting a different serial number
- detecting a significant change in the toner level reported by the supply

When PrintFleet determines a supply has been replaced, it automatically ends any alert events for that supply that were started.

### Alternate Methods

A given device will typically report an issue using more than one method. For example, when a toner level gets below a certain level the device may do one or more of the following:

- Continue to report the current toner level as a percentage. You can monitor for this using the **Supply** condition type.
- Set the **Low Toner** bit which is standard across manufacturers. You can monitor for this using the **Standard Bits** area of the **Error Code** condition type.
- Set a manufacturer-specific code. You can monitor for this using the **Vendor Codes** area of the **Error Code** condition type.
- Display a message on its display panel indicating that the toner level is low. You can monitor for this using the **Display Panel** area of the **Error Code** condition type.

### Estimated Days To Empty (EDTE) and Supplies

Supply alerts can be triggered when either level reaches a specified threshold and/or a specified EDTE is met. Supply alerts will fall back to level if EDTE is not specified, and EDTE will take precedence over level percentage when triggering alerts. (Example: if the percentage has not fallen to below the specified threshold, but the EDTE does meet the specified threshold, then an alert would still be triggered.)

You can choose the method which works best in your circumstances.

## Adding a supply condition to an alert definition

### Procedure

1. From the **Create/Edit Alert Definition** page, click **Add Condition Type** and choose **Supply** from the drop-down list that appears. A **Supply** tab opens with default conditions predefined for the most common toner supplies.
2. In the **Supply Thresholds** area, select the **Use same value for all thresholds** check box if you are going to be adding multiple supply thresholds to the alert definition and want all of them to use the same value. For example, if you are creating an alert definition that monitors toner levels for a color-capable device, you can select this option and PrintFleet will automatically adjust the threshold values for each toner supply you enter based on the first value.
3. For each supply you want PrintFleet to monitor, do the following:
  - In the **Supply** box enter the name of the supply.
  - In the **Threshold** box, enter the value (as a percentage) which the supply must reach or fall below before you want to be alerted. For example, to specify a threshold of 15%, type *15*.

- If there are additional supply conditions you want to include in this alert definition, click **Add Supply** and repeat this step.

## Adding an EDTE to a supply alert definition

### Procedure

1. From the **Create/Edit Alert Definition** page, click **Add Condition Type** and choose **Supply** from the drop-down list that appears. A **Supply** tab opens with default conditions predefined for the most common toner supplies.
2. In the **Supply Thresholds** drop-down box, choose from **EDTE** or **EDTE with Level Fallback**. If you choose, EDTE, enter your desired EDTE Threshold in days in the text box. If you choose EDTE with Level Fallback, enter your desired EDTE in days, as well as your desired Level Threshold in a percentage.
3. Once complete, click **Save Definition**.

### Note

The EDTE alert will only be triggered for active devices

## Error code alert conditions

Devices are able to report issues (or 'errors'), in a variety of ways. The method can vary from one manufacturer to another, or from one device to another within the same manufacturer. The information can even change for the same device based on the version of the firmware it is using.

PrintFleet provides you with the flexibility to choose which method (or combination of methods) you want to use to check the device conditions.

### Standard "bits"

In an early attempt to standardize the error information provided by devices, the manufacturers in the printing industry came up with a list of conditions that all devices would report on through the use of assigned bits. (There are 8 "bits" in a byte, thus there are 8 conditions that can be represented in this way.)

With only 8 conditions to choose from it is impossible to represent all the conditions that devices might need to report. Despite this obvious limitation, the broad acceptance and use of this standard means that it can still be a convenient method for monitoring some basic conditions, especially when applying an alert definition to a group of devices from multiple manufacturers.

### Standard Codes

The standard codes are the result of another effort

(specifically RFC 1759 - Printer MIB) to define a more comprehensive standard. With more conditions to choose from, standard codes allow you to create alerts that are more specific, while still being generally applicable to devices from different manufacturers (compliance with the standard varies among manufacturers).

**Vendor Codes**

Despite various efforts to provide a single comprehensive list of device codes that covers all manufacturers, there remain differences among manufacturers in the way they report

information. It is not possible to list all the vendor-specific codes, but if you know the codes that a device uses when reporting specific conditions, you can set up an alert definition to monitor the device for those conditions by entering the associated codes in the **Vendor Codes** area. For example, a device might report the code 140 to indicate the Image Drum Up/Down Process is not working properly for the Yellow drum. To watch for this you could enter 140 in the box in the **Vendor Codes** area of an alert definition applied to this device.

**Note**

PrintFleet will match the text you type with any text string that includes that text. For example, if you simply type 140, PrintFleet will consider the condition to be met if the device returns a code of 140, 1140, or even XG31406Y.

**Display Panel**

Most devices have a display panel on which they display information to indicate their current status. Usually the status is something like *Ready, Idle, Printing, or Power Save*, but when a device encounters a problem, the display will change to reflect that. Depending on the device, the display panel message can be generic (such as *Warning or Error*), but may also provide specific details. Similarly, you can set up a generic alert definition that monitors the text appearing on a device's display for the words *Warning or Error*, or you can create more specific alert definitions that check for other text strings.

**Occurrence Threshold**

Sometimes you might not care about a trivial issue that appears infrequently, but will want to be alerted if the issue becomes persistent. For example, you might not want to be alerted about a single paper jam, but might want to be notified if a given device reports say 10 paper jams in a day. The occurrence threshold allows you to specify how many separate occurrences of the indicated error code(s) must occur in a designated period before an alert event is created. Note that when a device reports a given error code in consecutive DCA reports it is considered to be a single occurrence of the error code; to count as a separate occurrence the error code must be absent from a subsequent report from that device and then reappear again.

Note also that the occurrence threshold applies collectively to all the error codes selected within a given alert definition. For example, if you had created an alert definition that included the codes for **Low Paper, No Paper, and Low Toner**, and set the occurrence threshold to "any 3 occurrences in 1-hour(s)", an alert event would not be created unless some combination of those codes totaling three (or more) times occurred within a given hour (such as **2 Low Paper** codes and **1 No Paper** code). If you only wanted to assign an occurrence threshold to one of those codes you could create a separate alert definition just for that code.

## Adding an error code condition to an alert definition

### Procedure

1. On the **Create/Edit Alert Definition** page, click **Add Condition Type** and choose **Error Codes** from the drop-down list that appears. An **Error Codes** tab opens.
2. In the **Standard "bits"** area, select all the conditions you want to include in the alert definition.
3. In the **Standard Codes** area, select all the conditions you want to include in the alert definition.
4. In the **Vendor Codes** area, if you want to add a vendor code to the alert definition, do the following:
  - In the **Match text** box, type a vendor code you want PrintFleet to watch for.
  - If there are additional vendor codes you want to include in this alert definition, click **Add Vendor Code** and repeat this step.
5. In the **Display Panel** area, if you want to add display-panel text to the alert definition, do the following:
  - In the **Match text** box, type the display-panel text you want PrintFleet to watch for.
  - If there are additional display-panel messages you want to include in this alert definition, click **Add Display Panel** and repeat this step.
  - In the **Occurrence Threshold** area, if you want to specify a collective frequency for the error codes, do the following:
    - In the first box, type the total number of specified errors that must occur in a given period.
    - If the second box, type the number of time units in the period.
    - In the third box, click the drop-down arrow and choose a time unit for the period.

## Stale DCA alert conditions

To be sure you are receiving the most current information from the devices you are monitoring, you can create an alert definition to notify you when a DCA becomes stale (meaning it fails to provide an update for a specified period).

PrintFleet Optimizer has a system setting which defines the length of time that a device or DCA must be inactive before being designated as stale. When creating an alert definition for a stale DCA, you can either use the system setting, or specify an inactivity period just for use in the alert definition.

## Adding a Stale DCA condition to an alert definition

### Procedure

1. On the **Create/Edit Alert Definition** page, click **Add Condition Type** and choose **Stale DCA** from the drop-down list that appears. A **Stale DCA** tab opens.
2. In the **Stale DCA** area, do one of the following:

- If you want to use the setting for stale days as defined in the system settings, select the **Use system stale days** check box.
- If you want to use a different number of days in the alert definition, or simply have the alert definition setting be independent of the system setting, enter the number of days you want to use in the **or when a DCA is stale for <#> days** box.

## Activated DCA alert conditions

Administrators can receive an alert confirming that a DCA was activated. This gives you the opportunity to follow-up with account support.

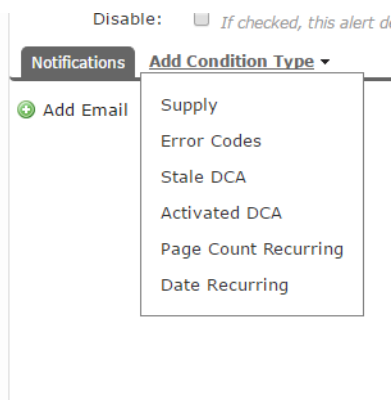
## Adding an Activated DCA condition to an alert definition

### Procedure

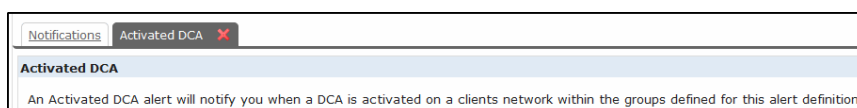
1. On the **Main Menu**, click **Alerts**.
2. Click **Create Alert Definition**.

The **Create/Edit Alert Definition** page appears.

3. In the **Alert Definition** area, do the following:
  - In the **Name** box, enter a name for the alert.
  - From the **Group** list, select the group to which the alert will apply.
  - (Optional) Select the **Use advanced security** check box if you want to apply additional security options available on the **Advanced Security** tab.
  - (Optional) Select the **Disable** check box if you want to disable the alert definition so that it will be temporarily turned off.
4. (Optional) On the **Notifications** tab, to send a notification at the start or end of the alert event, do any of the following:
  - Click **Add Email** to add an email notification.
  - Click **Add Webhook** to add a Webhook notification.
5. On the **Add Condition Type** tab, click **Activated DCA** to add an Activated DCA condition to the alert definition.



The **Activated DCA** confirmation message appears.



(Optional) If you selected the **Use advanced security** check box, in the **Advanced Security** tab do the following:

- In the **Events visible to** list, specify who can see the associated alert event.
- In the **Applies to** area, select the group(s) and/or device(s) to which the alert definition applies.

6. Click **Save Definition**.

The saved alert definition is displayed in the list of definitions on the **Alerts** page.

Alerts				
Filter by Group: Grp1 (0 of 0)				
Name	Create Date	Created By	Is Enabled	Options
DCA Activation Alert	3/11/2015 4:32:53 PM	System Admin	True	Edit  Disable  Delete

## Page count recurring alert conditions

Sometimes you might want to be alerted when a device has reached some milestone in terms of pages generated. For example, to schedule preventive maintenance, you might want to know every time that a device has printed another 25000 pages. You can do this by creating an alert definition that includes a page count recurring condition.

**Note**

If you apply a page count recurring alert definition to a group, an alert event will be created for every device within that group that passes the specified page count threshold (according to the indicated meter). If you only want the page count recurring definition to apply to a single device, set the alert definition to use advanced security and then select the device.

## Adding a page count recurring condition to an alert definition

### Procedure

1. From the **Create/Edit Alert Definition** page, click **Add Condition Type** and choose **Page Count Recurring** from the drop-down list that appears. A **Page Count Recurring** tab opens.
2. In the **Page Count Recurring** area, do the following:
  - In the **Meter Label** box, enter the name of the meter to use to monitor pages printed. You can find the meter names associated with a given device by going to the **Meters** tab in the **Device Detail** page for that device.
  - In the **Recur Cycle** box, enter the number of pages the device must generate each time before an alert event will be created.

## Date recurring alert conditions

Sometimes you might want to be alerted at regular intervals, or at a specific date, in order to perform preventive maintenance on a device. You can do this by creating an alert definition that includes a date recurring condition.

**Note**

If you apply a date recurring alert definition to a group, an alert event will be created for every device within that group when the specified date arrives. If you only want the date recurring definition to apply to a single device, set the alert definition to use advanced security and then select just the device you want.

## Adding a date recurring condition to an alert definition

### Procedure

1. From the **Create/Edit Alert Definition** page, click **Add Condition Type** and choose **Date Recurring** from the drop-down list that appears. A **Date Recurring** tab opens.
2. In the **Date Recurring** area, select one of the following intervals for the alert:
  - **Once.** Click the Calendar icon and choose the date and time that you want the alert event to be created.
  - **Daily.** Type in the interval, in days, that you want the alert event to be created, then choose the starting date and time.

- **Weekly.** Type in the interval, in weeks, and select the day of the week that you want the alert event to be created, then choose the starting date and time.
- **Monthly.** Type in which day of the month and the interval in months that you want the alert event to be created, then choose the starting date and time.
- **Advanced.** Select which occurrence of which day of the week in a month, and the interval in months that you want the alert event to be created, then choose the starting date and time.

## Combining multiple error code conditions

If you want, you can include more than one error code within the **Error Codes** condition type. PrintFleet combines them using an 'inclusive OR' form of logic. You can specify one or more standard bits, standard codes, vendor codes, or display-panel strings (or any combination of these), and PrintFleet will generate an alert event for the definition as soon as any one of them is satisfied.

### Occurrence Threshold

One significant exception to this occurs when you use the **Occurrence Threshold** setting.

Suppose you had set the **Occurrence Threshold** setting to "Any 3 occurrences in 8 hour(s)". In this case, if you had specified multiple conditions within the **Error Code** tab, any three of them (such as the same condition three separate times, or three different conditions once) within a given 8-hour period would satisfy the overall **Error Codes** condition.

### Redundant Conditions

There is often more than one way to watch for a given condition. For example, with toner supplies you can use a **Supply** condition where you can enter a specific toner supply and threshold. You could also use an **Error Code** condition and choose one of the **Standard Bits** codes (**Low Toner** or **No Toner**), or one of the **Standard Codes** ([1104] Marker toner almost empty), or a **Display Panel** message (such as "Low Toner"), or possibly even a **Vendor Code** specific to one of your devices.

Everyone's circumstances are different, and it will likely take a little bit of experimentation to determine which method works best for you in your circumstances.

## 4.5 Managing Alert Definitions

As you create and refine your alert definitions you will likely find it convenient to be able to perform various management activities, such as viewing, editing, and deleting alert definitions, as well as enabling and disabling alert definitions.

When viewing the alert definitions on the Alerts page, note that you can click any column heading to sort the definitions by that column.

This may help you to locate a particular definition if you have many alert definitions.

## Viewing the alert definitions

### Procedure

1. On the main menu, click **Alerts**. The **Alerts** page opens.
2. The alert definitions are displayed in a table. If necessary, you can:
  - scroll down to view additional alert definitions on the page
  - change the number of alert definitions that can be displayed on the page
  - view other pages of alert definitions
  - sort the alert definitions by clicking any column heading
  - filter the alert definitions by choosing a group from the **Filter by Group** list. Only the alert definitions that have been applied to the specified group (or to any subgroup of the specified group) will be displayed.

### Note

For simplicity, any advanced security settings that may have been applied to the alert definitions are ignored when filtering.

## Editing alert definitions

After an alert definition is created, it can be edited at any time.

### Procedure

1. On the main menu, click **Alerts**.
2. On the **Alerts** page, under **Options**, click **Edit** beside the alert definition you want to edit.
3. Make changes to the alert definition as desired, and then click **Save Definition**.

## Disabling and enabling alert conditions

If you want, you can disable an alert definition. When an alert definition is disabled, PrintFleet will ignore the definition; it will not check for the conditions specified in the definition, nor will it send any notifications specified in the definition. Some possible reasons to disable an alert definition might be:

- the alert definition targets a specific device, and you know in advance that the device will be going offline
- a key contact specified in multiple alert definitions has left the company and you want to change all affected alert definitions before any further notifications are sent

Once the situation has changed, you can easily re-enable the alert definition.

### Procedure

1. On the main menu, click **Alerts**.

2. On the **Alerts** page, under **Options**, do one of the following:
  - Click **Disable** beside the alert definition you want to disable.
  - Click **Enable** beside the alert definition you want to enable.

## Deleting alert definitions

After an alert definition is created, it can be deleted at any time.

### Procedure

1. On the main menu, click **Alerts**.
2. On the **Alerts** page, under **Options**, click **Delete** beside the alert definition you want to delete.
3. Click **Continue** to verify deletion.

## 4.6 Working with Alert Emails

For each alert definition you create, you can specify one or more email addresses to which an alert notification message will be sent. See "Creating Alert Definitions" on page 77.

### Email Subject

The subject line of an alert email is configurable. When you are creating an alert definition, the format of the subject line is automatically populated based on your Alert Subject Template settings. If you want, you can easily change this default. For information on changing your default Alert Subject Template, see "Changing Preferences" on page 95.

You can also override the default format for the subject line for individual alert definitions when creating or editing the definitions. For more information, see "Creating Alert Definitions" on page 77.

### Email Body

The body of an alert email includes more detailed information about the alert event and about the device or DCA for which the associated alert event was created. The information will include hyperlinks to related objects, such as the alert definition, the error code, meter or supply that you were monitoring, and the device or DCA for which the alert event was triggered. You can click these links to open the associated pages in PrintFleet Optimizer.

### Email Headers and Footers

Each email also has optional header and footer areas that you can use to provide additional information. For example, if you are creating an alert definition for a specific error code, you could enter information in the header or footer of that definition that describes the action you would like the service technician to take. For more information, see "Creating Alert Definitions" on page 77.

## 4.7 Working with Alert Webhooks

For each alert definition you create, you can specify one or more Webhooks. A Webhook uses HTTP POST to send the alert information in JSON format to a specified URL where it can then be accessed by a third-party API (Application Program Interface). See "Creating Alert Definitions" on page 77.

The following is an example of a Webhook posting:

```
{
  "AlertDefinitionId":"0f1ae6f0-3113-4e28-bbbc-ca7247ca6b40",
  "Description":"Date-Recurring condition has been met.",
  "EventAt":"2013-07-24T19:08:00Z",
  "Id":"81ca2775-d8aa-471b-8cf7-38d014c7b77f",
  "IsActive":false,
  "LastUpdatedAt":"2013-07-25T18:15:09Z",
  "Name":"Webhook Alert Test",
  "StartedAt":"2013-07-24T19:08:00Z",
  "Term":"end",
  "Device": {
    "AssetNumber":null,
    "FirstReportedAt":"2013-06-27T17:12:49.193Z",
    "GroupId":"7ae2df44-8cb7-440c-8582-e36e66fd3802",
    "Id":"0cb08805-0940-49b5-bb06-fbf544366960",
    "IpAddress":"10.0.0.64",
    "LastReportedAt":"2013-07-18T16:48:40Z",
    "LicenseStatus":"Full",
    "Location":null,
    "MacAddress":"00-14-38-92-BB-01",
    "ManagementStatus":"Managed",
    "SerialNumber":"CNGC6292J7",
    "Status":0,
    "Type":"Network"
  }
}
```

You can perform a basic test of the Webhook functionality when creating the alert definition by clicking **Test POST** in the **Webhook** box on the **Notifications** tab. PrintFleet will attempt to send a mock alert notification to the specified URL and will display a message box indicating the outcome.

Once you have saved the alert definition and it is active in a live environment, PrintFleet will attempt to post the Webhook notification when the conditions of the alert definition are met. If PrintFleet receives anything other than a valid 2XX response from the URL, the notification request will be placed in a queue to be retried again periodically. After 5 failed attempts the Webhook is removed from the queue and the message container table is updated to reflect this (for future reference).

## 4.8 Supplies Notification

Each device has a variety of supplies (such as toner) that it consumes as part of its normal operation. If one of these supplies becomes empty, the device stops working until the supply is replaced. To minimize the time a device is unavailable, you will want to ensure that you have a replacement for the supply on hand as soon as it is needed. This will typically involve an ordering system.

PrintFleet Optimizer is not an ordering system, but it plays an integral role in the overall supply-ordering process by:

- monitoring the supplies of each device  
See "Working with the Supplies tab" on page 30.
- tracking and displaying the usage history of each supply  
See "Working with the Supply Detail page" on page 34.
- scheduling reports on supplies
- notifying you when a supply reaches a specified minimum level  
See "Supply alert conditions" on page 80.
- sending requests for replacements  
See "Using the Supplies Order View" on page 16.
- detecting (and optionally notifying you) when a supply has been replaced

### Possible supplies notification workflow

There are different ways that you might use the available functionality to implement a supplies notification system, but to have the most effective system in place it is strongly recommended that the notification system within PrintFleet be leveraged to automate your process. The following is a suggested workflow that could be used.

#### Setup

To ensure you have adequate alert coverage for your devices' supplies, you should:

- Create alert definitions with **Supply** conditions for every combination of device and supply you want PrintFleet to monitor.
- Create one or more catch-all alert definitions for the supplies. For example, you could create an alert definition based on the "No Toner" error code. If this alert definition gets triggered, it could help you identify devices that were either not covered by any supply alert definitions, or that were covered by a definition that needs to be modified (such as for devices that do not report levels as percentages).
- Verify that a given supply is covered by an alert definition by viewing the **Metric History** page for that supply.

#### Notification

When a supply that is being monitored by an alert definition meets the specified criteria, PrintFleet automatically generates an alert event. If a notification (such as an email or Webhook) has been

---

specified in the alert definition, PrintFleet automatically sends the notification. The notification identifies which supply is needed, which device it applies to, and (if available) the serial number, asset number, and location information. The alert event remains open until PrintFleet detects that the supply has been replaced.

### **Assessment**

The person receiving the notification can access details of the alert, such as the levels for the supply over the last 90 days, and the date the supply was last requested. Based on this information they can determine whether to request a replacement supply.

### **Request**

Using the **Supplies Order View**, you can specify which supplies you want to request, and how many of each supply. You can then submit the request. PrintFleet sends an email summarizing the details of the request to the address you specify. The details of the request can also be attached to the email in either XML or CSV format. The person receiving the request email will then be able to process the request using their third-party ordering system.

### **Replacement**

When the third-party order is processed and the replacement supply is available, someone replaces the supply in the device. The next time the device reports its supply, PrintFleet automatically detects that the supply has been replaced and closes the alert event. If necessary you can open the **Metric History** page for the supply and view a chart of the supply history. The chart displays an icon at the point at which the replacement was detected. The associated alert definition does not need to be manually reset, but will automatically resume monitoring the supply for the next time it meets the specified criteria.

### **Manual Intervention**

If you are using alerts you should be able to automate most of the supplies replacement process. However, because some devices do not provide detailed supply-level information, you may find that in some cases you need to adopt a more manual approach. If necessary, you can:

- Use the graph on the **Metric History** page to assess the rate at which the supply is depleting. You might find that the supply is being used at a rate different than what you had expected, and could use this information to adjust the level threshold in the associated alert definition.
- Create a report on supplies (for toner only), and use that to identify other devices with the same supply where the level is approaching the replacement criteria. You might do this to increase the efficiency of your order delivery and replacement.

# Chapter 5 Settings

---

## 5.1 Changing Preferences

Preferences, including your password and the way you want device names to display throughout the system, can be changed. It is recommended you change your password periodically for additional security. Passwords are encrypted, and cannot be recovered, so you must change your password if you lose it. If you do not have access to the area to change your password, you must request a reset from your distributor if you want to change it.

### Procedure

1. Do one of the following:
  - Click **Preferences** on the upper right side of the interface.
  - On the **Settings** menu, click **My Preferences**.
2. Do one or more of the following:
  - To change your password, type your current password in the **Old Password** box, type your new password in the **New Password** box, and retype your new password in the **Confirm Password** box.
  - To change the page that appears upon logging, select a page from the **Starting Page** drop-down list. To change the language in which the interface is displayed, select a language from the **Language** drop-down list.
  - To specify the time zone to use when displaying dates, select a time zone from the **Time Zone** drop-down list.

---

**Note**

When working with dates, be aware of the following exceptions:

- All SQL data aggregated or filtered by aggregate SQL date calculations (by month, day, etc.) are not "time zone aware" and the periods are therefore relative to either UTC or date parameters provided via the function or report. (eg. Color vs Mono by Month report)
  - Scheduled reports with a Reporting Period parameter of Calendar Month or Previous Calendar Month use midnight UTC for the start/end times.
-

**Note**

- Any part of the user interface that shows relative time periods (such as '2 days ago') calculates the difference between the date value provided from the server (in the user's time zone) and current time reported by the browser. If the user's time zone preference and the user's client PC time zone settings are different, the 'time ago' will be reported incorrectly.
- Custom device fields of type Date are not converted to or from UTC.
- The DCA 4.x "Released" date is not converted to or from UTC.

different, the 'time ago' will be reported incorrectly.

- Custom device fields of type Date are not converted to or from UTC.
- The DCA 3.x "Released" date on the DCA Install page is not converted to or from UTC.
- To specify your regional electricity cost per kWh, enter the rate as a decimal value in the **Cost per kW h** box. This value is used in various reports when calculating power cost estimates for devices.
- To change the way device names, display throughout the system, enter an acceptable string in the **Device Name Template** box, or select a method from the list underneath. The following properties are accepted: \$description, \$name, \$id, \$serial, \$asset, \$ip, \$mac, \$location, \$hostname, \$lcd, \$systemname, \$systemlocation, \$systemdescription, \$grouping, \$groupbreadcrumb, \$userid, and \$username. The following are examples of strings that can be used:
 

```
$name (Serial: $serial, Asset: $asset)
sample output: HP 1000 (Serial: 1234, Asset: ABC)

$name-$ip-$mac
sample output: HP 1000-192.168.1.1104-
00:01:02:aa:bb:cc
```
- If you are going to create alert definitions that include email notifications, you can specify what information will appear by default in the subject line of the emails that are sent. To set the default format for the subject line of alert email notifications, enter an acceptable string in the **Alert Subject Template** box, or select a method from the list underneath. The template you specify here will be used as the default subject line for any new alert definitions you create, regardless of whether they are for devices or DCAs. If necessary you can easily override this default definition on a case-by-case basis by specifying a different format when creating or editing each individual alert definition. The template can include text (such as "This is an alert") as well as one or more placeholders for properties that will be filled

in when an alert definition is triggered (such as \$alertname). For a list of the properties that can be specified in the template, hover your mouse cursor over the icon to the right of the **Alert Subject Template** box. A tooltip will appear. For more information on creating alerts, see "Creating Alert Definitions" on page 77.

3. Click **Save**.

<b>Note</b>	Your password must be of a certain strength, as set by the administrator. The Strength bar must turn green for it to be an acceptable password. To increase the strength of your password, use both upper and lower case, both letters and numbers, symbols, or increase the length of the password.
-------------	--

## 5.2 Managing Groups

You can create a new group and a new DCA from the **Administration** menu. For more information, see "Downloading the Manual Installer" on page 142.

Groups are used to segment devices into useful divisions, such as by dealer, customer, location, account rep, or any other grouping you see fit. Each group can have as many subgroups as you need, and all groups belong to the Root Group. Each device can be assigned to one group.

Group properties can be changed at any time, including the hierarchical placement. You can also view related items for existing groups, such as users and a breakdown of device counts, from the **Manage Groups** tab. For groups of type **Customer**, there is also a link to create a DCA Key. To change the devices contained in a group, see "Assigning devices to groups" on page 99.

### Creating, editing, and deleting groups

You can create unlimited groups to properly segment devices. Each group can have an unlimited number of subgroups.

#### Create a new group

##### Procedure

1. On the **Settings** menu, point to **Group Management**, and then click **Manage Groups**.
2. Select the group that will be the parent for the new group. For example, to create a location group for a customer, select the group for the specific customer, or to create a top-level group, select Root Group.
3. Click **New Group**.
4. Under **Basic Information**, select one of the following group types from the **Type** list:

- **Dealer** for groups that represent a dealer.
  - **Customer** for groups that represent a customer.
  - **Generic** for any other group type.
5. Enter a name for the group in the **Name** box.
  6. Enter an alias for the group in the **Alias** box.
  7. If you selected a group of type **Dealer** or **Customer**, complete the address and other fields under the **Dealer Information** or **Customer Information** areas.
  8. Click **Save**.

### Editing users and device counts for a group

#### Procedure

1. On the **Settings** menu, point to **Group Management**, and then click **Manage Groups**.
2. Select the group you want to edit.
3. Do one or both of the following:
  - To change the hierarchical placement of the group, drag and drop the group to be under the new parent group.
  - To change other group properties, click **Edit**, and change the name, alias, and other group properties as desired.
4. Click **Save**.

### Viewing users and device counts for a group

#### Procedure

- On the **Manage Groups** page, in the **Related Items** area, click to expand **Users** or **Device Counts** to display users or device counts for the group. Device counts will display devices directly in the group, and in a separate area, devices in subgroups, with a breakdown of their management status.

### Creating a DCA key for the group

You can create a DCA key for the group or perform a simplified install. For more information, see "DCA Installations" on page 135.

#### Procedure

- On the **Manage Groups** page (found under **Group Management**), select a group and then click **Create DCA**. You will be taken to the **DCA Creation** page with the group already selected. See "Administrating PrintFleet Optimizer" on page 127.

### Deleting a group

Groups can be deleted at any time. Associated subgroups and devices will be either deleted or moved, depending on what option you choose.

### Procedure

1. On the **Settings** menu, point to **Group Management**, and then click **Manage Groups**.
2. Select the group you want to delete.
3. Click **Remove**.
4. In the box that appears, do one of the following:
  - Select **Delete this group and all associated sub-object(s)**.
  - Select **Delete this group and re-assign all associated sub-object(s)**, and then use the **Move To** list to specify the group to which you want the objects reassigned.
5. Click **Remove Group**.
6. In the dialog box that appears, click **OK**.

#### Note

Users cannot delete groups they have been given specific access to. For example, if a user is given access to the `Widgets` group, they cannot delete the `Widgets` group, but they can delete any child group of `Widgets` (provided they have full access to the **Manage Groups** page).

## Assigning devices to groups

Each device must be assigned to a group. By default, devices will be placed into the group that the DCA is targeted to.

If a device is physically moved from one location to another, PrintFleet makes the necessary adjustments automatically:

- a new device will be created in the new group
- the device in the original group will go stale

This behavior ensures that information such as printed pages and device history is maintained in the original location up to the point of the move, and new information begins accumulating for the device in the new location. This is particularly important if the device is being moved from one customer to another; this way each customer is billed the proper amount.

#### Note

PrintFleet only looks for a device in or under the group to which the corresponding DCA is connected. If you move a device to a group outside the scope of the DCA that reported that device, the device in the new group location will go stale, and a new device will appear in the original group.

### Procedure

1. On the **Settings** menu, point to **Group Management**, and then click **Organize Devices**.
2. Select the group that contains the devices you want to move to a different group.

3. Optionally, click **Filters** and make selections or enter a search string to narrow down the devices you want to view.
4. Select the check box beside each device you want to move to another group.



5. Click and drag one of the selected devices (it will automatically drag all selected devices) to the group you want them moved to.



6. Click **Save**.

## Managing group types

You can create custom group types to assign to the groups that you create. By default, there are three group types: **Dealer**, **Customer**, and **Generic**. You may want to create additional group types that define additional properties, such as location or account representative.

## Create a new group type

A group type is assigned to a group when the group is created.

### Procedure

1. On the **Settings** menu, point to **Group Management**, and then click **Manage Group Types**.
2. Click **New Group Type**.
3. Enter a name for the group type in the **Name** box.
4. From the **Display Image** list, select the image to be displayed beside groups of this type when viewing a group list. Having a unique icon for each group type makes it possible to identify the group types when they are presented in the group lists used throughout the user interface. A preview of the image will display to the right of the list after it is selected.
5. Optionally, under **Group Information Designer**, add one or more group attributes by repeating the following steps for however many attributes are needed:
  - Enter a name for the attribute in the **Attribute Name** box.
  - Select an attribute type from the **Attribute Type** list.
  - Optionally, enter a default value for the attribute in the **Attribute Default** box.
  - Click **Add**.

6. In the **Attribute Viewer** area, click and drag attributes to place them in their appropriate display order.
7. Click **Save**.

### Attribute Types for Custom Group Types

Attribute	Description
True/False	A check box value that can be either selected or not selected
Date (yyyy-mm-dd)	Date value, in the format yyyy-mm-dd
Decimal	Numeric value that accepts decimal places
Unique Identifier (GUID)	16-character hexadecimal identifier value
Number	Numeric integral value (no decimal places)
Text	Plain text value
Industry Code	Industry vertical code value used to classify businesses
External Service Link	A URL value that becomes a link shown on the Device Detail page.

### Creating a new group by copying an existing group

A new group can also be created by copying the properties of an existing group, and then modifying it if necessary.

#### Procedure

1. On the **Settings** menu, point to **Group Management**, and then click **Manage Group Types**.
2. Click **Copy** in the row of the group type you want to copy.
3. Enter a name for the new group type in the **Name** box.
4. Adjust any other properties of the group type as desired.
5. Click **Save**.

### Editing a group type

Group types can be edited at any type, except for the name of the type, which must remain the same. Images and attributes that are associated with the group type can be changed.

#### Procedure

1. On the **Settings** menu, point to **Group Management**, and then click **Manage Group Types**.
2. Click **Edit** in the row of the group type you want to edit.

3. If you receive a warning notification about existing groups associated with the group type, read through and then click **Close Notice**.
4. Do one or more of the following:
  - Select a new image to be associated with the group type from the **Display Image** list.
  - In the **Group Information Designer** area, add one or more new attributes to the group type by completing the listed fields.
  - In the **Attribute Viewer** area, change the display order of attributes by clicking and dragging attributes to the desired order.
  - In the **Attribute Viewer** area, click the edit icon (📄) in the row of an attribute you want to change, and then change desired properties in the **Group Information Designer** area.
  - In the **Attribute Viewer** area, click the remove icon (⊖) in the row of an attribute you want to remove.
5. Click **Save**.

**Warning**

Any changes made to a group type will take immediate effect on existing groups of that type. A warning will be displayed showing you how many groups are currently associated with the group type you are about to edit.

## Deleting a group type

Custom group types without any associated groups can be deleted.

**Procedure**

1. On the **Settings** menu, point to **Group Management**, and then click **Manage Group Types**.
2. Click **Remove** in the row of the group type you want to delete.

## 5.3 Managing Devices

The core aspect of managing devices comes from collecting data stored in imaging devices using the DCA. Devices can be managed further by entering information into PrintFleet Optimizer that cannot or is not being collected directly from the device. You can also set the **License Status** and **Management Status** for a device.

### License status

Each device has a **License Status**. The License Status of a device determines such things as whether the device appears in the user interface, whether the data for the device is stored in the database, and whether you will be billed for the device. You can set the license status manually for a device, but there are also various

scenarios where the License Status for a device is set automatically. The possible license states are: **Full, Hidden, Deleted, Auto Hidden (Missing Info), Stale Deleted.**

The license states are described in greater detail in the following paragraphs.

**Note**

In the following descriptions license states are described as either billable or not billable. Be aware that even if a given device is in a non-billable state at the end of a billing period, it will still be considered billable if it has been in a billable state for any length of time during that billing period.

### Full

This is the normal state for a device. Devices with a **Full** license show up in the user interface, and can be used in reports and alerts. A device will be automatically set to **Full** when it is first detected. The system will also automatically change a device to **Full** if the device was in a state of **Auto Hidden (Missing Information)** and a valid serial number or page count is provided.

A device with a **Full** license has the following properties:

Property	Description
Billable	Is billable
Availability	Available in user interface
Storage	Associated data is stored

### Hidden

A device with a **Hidden** license is still monitored, and its history is retained, but it does not appear in the user interface (including reports, alerts, and import/export). Devices can be hidden manually by a user, but they can also be hidden automatically by the system, as follows:

- A device will be automatically set to **Auto Hidden (Missing Info)** if the device does not have either a serial number or a page count. A new device may be missing information for any of the following reasons:
  - The device does not support collection of this data
  - The firmware version of the device does not support collection of this data
  - The DCA version being used does not support the device (or the particular firmware version of the device)
  - The DCA timed out while trying to read the data for the initial scan (subsequent scans might provide the missing information)

A **Hidden** device has the following properties:

Property	Description
Billable	A Hidden device is billable An Auto Hidden device is not billable
Availability	Limited availability in user interface (no reports, alerts, or import/export)
Storage	Associated data is stored but not accessible by user

### Deleted

A device with a **Deleted** license is not monitored, no history is retained, no new data is added, and it does not appear in the user interface (including reports, alerts, and import/export). The purpose of this state is so that the system can identify the devices that have been deleted and thereby avoid having these same devices appear as new devices the next time they are scanned. Devices can be deleted manually by a user, but they can also be deleted automatically by the system, as follows:

- A device will be automatically set to **Stale Deleted** if it has been inactive for a prolonged period (currently 548 days). If a device becomes active again after it has been set to **Stale Deleted**, the device will be automatically set to the most applicable non-manual state.

A **Deleted** device has the following properties:

Property	Description
Billable	Is not billable
Availability	Limited availability in user interface (no reports, alerts, or import/export)
Storage	Associated data is not stored or updated; historical data is deleted; attributes are updated

## Management status

Each device has a **Management Status** of either **Managed** or **Unmanaged**. Setting the **Management Status** allows sales representatives to separate devices under their control from devices managed by the competition. This is useful in planning strategies for moving more of the page volume to internally managed devices. By default, all devices captured with the DCA are marked as **Managed**, but you can change this status if you want.

---

You can filter devices by **Management Status** when you are looking at any device view. See "Sorting data" on page 6.

### Editing device information as a group

The **Devices** tab of the **Device Management** page displays all the devices for a specified group. If you want, you can add or update the following information for devices on a group-wide basis:

- Device name
- Serial number
- Asset number
- Location

### Adding or editing device information on a group-wide basis

#### Procedure

1. On the **Settings** menu, point to **Device Management**, and then click **Devices**.
2. Select a group from the **Group** list.
3. Under the **Name**, **Serial Number**, **Asset Number**, and **Location** columns, enter new or updated information as desired.
4. Click **Save**.

### Editing device information

The **Device Information** tab of the **Device Management** page allows you to add or update the following information for individual devices:

- Device name
- Serial number
- Asset number
- Location
- Model (matched to the PrintFleet model database to pull information such as duty cycle, device image, release date, supply SKUs, etc.)
- Management status (see "Management status" on page 104)
- License status (see "License status" on page 102)
- Custom device fields. For information on creating custom device fields, see "Creating custom device fields" on page 106.

### Adding or editing device information for an individual device

#### Procedure

1. On the **Settings** menu, point to **Device Management**, and then click **Device Information**.
2. Select a group from the **Group Selection** list.
3. Select a device from the **Device Selection** list.

4. Add or edit information in the **Device Information** and/or **Device Custom Information** areas as desired.

**Warning**

If you change the **License Status** of a device to **Deleted**, the change is permanent. All historical data for the device will be deleted.

5. Click **Save Changes**.

**Note**

To go to the **Device Detail** page from the **Device Information** page, click **View**. See "Working with the Device Detail page" on page 24.

## Device-reported values

For the fields **Device Name**, **Serial Number**, **Asset Number**, and **Location**, PrintFleet records the values reported by the device. By default, these device-reported values are displayed on this page. If you change any of the values for these fields, either by editing them using this page or by importing them from a CSV file, PrintFleet then displays the edited value and displays an icon to the right of the field to indicate it is a user-defined value. If you click the icon beside a field, PrintFleet displays a pop-up menu showing the device-reported value. From the pop-up menu you can choose to either:

- Keep the user defined value
- Update to use the device value

If you choose to use the device value, the user-defined value is discarded, and the icon disappears. You must click **Save Changes** on this page if you want to preserve your changes.

## Creating custom device fields

If you want to add a specific type of device information that does not, by default, have a field in the software, you can add a custom device field, which will be added to the **Device Information** tab of the **Device Management** page (see "Editing device information" on page 105). Custom device fields can also be added to a Device View by selecting them from the **Columns** area in the **Add/Edit Device View** page. You can use custom device fields to add new information such as departments and account representatives. Custom device fields are applied on a group-wide basis.

In some cases, you may want to use additional groups instead of, or in addition to, custom device fields. For example, if you wanted to categorize your devices by location (such as "Floor 1", "Floor 2", etc.) or by department (such as "Finance", "Marketing", etc.), you could create these groups and reassign the devices into them. This is particularly helpful if you want to apply something (such as an alert or report) to the devices in those groups. See "Managing Groups" on page 97.

## Creating a custom device field

### Procedure

1. On the **Settings** menu, point to **Device Management**, and then click **Custom Device Fields**.
2. Select the group that the custom field will apply to from the group list at the left side of the page.
3. Type the name that will be displayed with the custom device field in the **Attribute Name** box.
4. If the field will be required for all devices in the group, select the **Attribute is required** check box.
5. By default, the **Attribute is enabled** check box is selected, which will make the custom field enabled as soon as it is saved. If you do not want the custom field immediately enabled, clear the **Attribute is enabled** check box.
6. Select the type of data that will be entered in the field from the **Attribute Type** list.
7. Enter a default value for the custom field in the **Default Value** box—this is optional for fields that are not required, and mandatory for fields that are required.
8. Click **Add**.
9. Click **Save**.

### Attribute Types for Custom Device Fields

Attribute Type	Description
UniqueIdentifier	Globally Unique Identifier (32-character hex value)
Text	Plain text value
Date	Date value
Email	Email address value
Yes/No	A check box value that can either be selected or not
Number	Integer value (no decimals)
Decimal	Decimal value

## Group inheritance

You can specify if a group will inherit the custom device fields created for its parent group (the closest group that contains the selected group). By default, this option is selected.

### Procedure

1. On the **Settings** menu, point to **Device Management**, and then click **Custom Device Fields**.
2. Select a group from the group list at the left side of the page.
3. Do one of the following:

- To have the group inherit the custom device fields of its parent group, select the **Inherit attributes from parent** check box.
  - To have the group not inherit the custom device fields of its parent group, clear the **Inherit attributes from parent** check box.
4. Click **Save**.

## Viewing inherited attributes

### Procedure


1. On the **Settings** menu, point to **Device Management**, and then click **Custom Device Fields**.
2. Select a group from the group list at the left side of the page.
3. Click the **Inherited Attribute(s)** tab.

## Editing a custom device field

Custom device fields can be edited or removed at any time. However, attribute types for custom fields cannot be edited.

### Warning


Removing a custom device field will remove information currently stored in the field for applicable devices.

1. Procedure
1. On the **Settings** menu, point to **Device Management**, and then click **Custom Device Fields**.
2. Select the group that the custom field is assigned to from the group list.
3. In the **Custom Fields** area, locate the field you want to edit under the **Group Attribute(s)** tab.
4. Click the edit icon (  ) in the row of the custom field you want to edit.
5. Under **Add/Edit Field**, change field properties as desired (except for **Attribute Type** which cannot be changed).
6. Click **Update**.
7. Click **Save**.

## Removing a custom device field

### Procedure

1. On the **Settings** menu, point to **Device Management**, and then click **Custom Device Fields**.
2. Select the group that the custom field is assigned to from the group list.

3. In the **Custom Fields** area, locate the field you want to remove under the **Group Attribute(s)** tab.
4. Click the Remove icon (  ) in the row of the custom field you want to remove.
5. Click **OK** to confirm deletion.

## Editing device status as a group

The **Device Status** tab of the **Device Management** page displays all the devices for a specified group. If you want, you can add or update the following information for devices on a group-wide basis:

- **License Status (Full, Hidden, Deleted, Auto Hidden)**
- **Management Status (Managed, Unmanaged)**

You can also click a device name to open the **Device Detail** page for that device.

## Adding or editing device status on a group-wide basis

### Procedure

1. On the **Settings** menu, point to **Device Management**, and then click **Device Status**.
2. Select a group from the **Group Selection** list.
3. Under the **License Status** and **Management Status** columns, make changes to the status information as desired. When you change a value, PrintFleet automatically saves your changes.

### Warning

If you change the **License Status** of a device to **Deleted**, the change is permanent. All historical data for the device will be deleted.

## Editing the management status for one or more devices

### Procedure

1. On the **Settings** menu, point to **Device Management**, and then click **Device Status**.
2. Select a group from the **Group Selection** list.
3. Optionally, click **Filters** and make selections or enter a search string to narrow down the devices you want to view.
4. Do one or both of the following:
  - Select one of **Full**, **Hidden**, or **Deleted** in the row of each device for which you want to change the license status.

### Warning

If you change the **License Status** of a device to **Deleted**, the change is permanent. All historical data for the device will be deleted.

- Select one of **Managed** or **Unmanaged** in the row of each device for which you want to change the management status.

Management status for individual devices can also be changed from the **Device Information** tab of the **Device Information** page. See "Editing device information" on page 105.

## 5.4 Virtual Meters

You can create virtual meters that combine the values of other meters (and optionally include a multiplier). Virtual meters can perform many tasks, such as adding up different page sizes, creating impression counters, and converting units.

For example, a device might have multiple individual Duplex meters. You might find it convenient to combine them into one virtual meter called Total Duplex.

### Creating a virtual meter

#### Procedure

1. On the **Settings** menu, click **Virtual Meter Manager**.
2. Click **New Virtual Meter**.
3. In the **Meter Configuration** tab of the **Virtual Meter Configuration** page, from the **Group** drop-down list, select the group to which you want to apply the virtual meter.
4. Enter the name you want to use for the virtual meter in the **Meter Name** box.
5. Under **Include**, select the check boxes corresponding to each of the meters you want to include in the virtual meter and optionally edit the **Multiplier** values for the selected meters.

#### Note

If you position your cursor over a meter name, the full meter name will be displayed in a tooltip. This can be helpful for identifying longer meter labels that are not fully visible.

6. Optionally, in the **Group/Device Assignment (Optional)** tab, restrict the virtual meter to a subset of the specified group by selecting individual subgroups or devices.
7. Click **Save**.

### Editing a virtual meter

#### Procedure

1. On the **Settings** menu, click **Virtual Meter Manager**.
2. Click **Edit** beside the virtual meter you want to edit.
3. In the **Meter Configuration** tab of the **Virtual Meter Configuration** page, make the necessary changes to the virtual meter.
4. Click **Save**.

## Copying a virtual meter

### Procedure

1. On the **Settings** menu, click **Virtual Meter Manager**.
2. Click **Copy** beside the virtual meter you want to copy.
3. In the **Meter Configuration** tab of the **Virtual Meter Configuration** page, enter a name for the virtual meter in the **Meter Name** box, and make any other changes to the virtual meter as necessary.
4. Click **Save**.

## Deleting a virtual meter

### Procedure

1. On the **Settings** menu, click **Virtual Meter Manager**.
2. Click **Delete** beside the virtual meter you want to delete.
3. In the **Delete Confirmation** dialog, click **Continue**.

## Adding Priority Levels to Virtual Meters

### Procedure

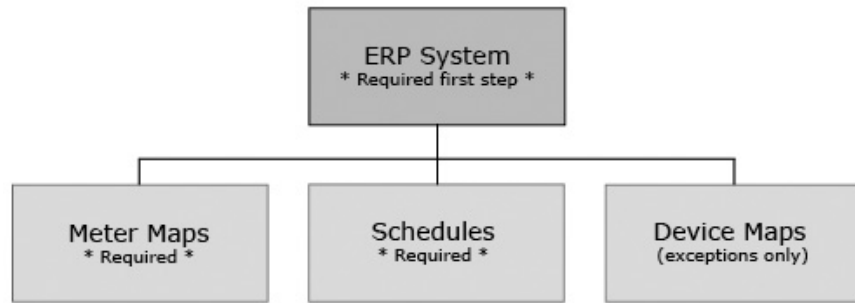
1. Please navigate to the **Settings > Virtual Meter Manager** page to access any already created Virtual Meters or to be able to create a New Virtual Meter with the priority selections now available.
2. Once on this next page, please select the desired group level for the new Virtual Meter to apply to and display within under the **Device Detail > Meters**.
3. Then, please ensure that a Meter Name is selected and then the desired meter(s) checkbox has been selected.
4. Next, please make any changes to the **Multiplier** column (default will be 1.0 which is recommended unless there exists a need to have the meter multiplied by the defined value) and the **Priority** column which will define which meter that the system will look to first to be able to provide a value for the created Virtual Meter as well as add multiple meters together (if within the same priority group level).

**Note:** For group selection, please select the **Root Group Level** if this is to be applied to all devices across the system.

## 5.5 Configuring Meter Exports

The meter export function allows you to automatically export meter information to an external ERP system or file. Regardless of which of these you want to do, you must start by specifying the configuration details.

If you are exporting meters to an ERP system, you will also need to set up meter maps, export schedules, and if necessary, device maps for your ERP system.



## Configuring a meter export system

You can export meter information either to a commercial ERP system, or to a file.

### Commercial ERP Systems

PrintFleet meter export is compatible with the following commercial ERP systems:

- Digital Gateway's e-automate
- OMD NetVision or OMD iManager, with H2O component
- Evatic
- La Crosse NextGen or La Crosse NextGen Web

## Other Export Types

In addition to the commercial ERP systems, you can also use **Meter Export** to export information to a file.

- **PFI Export**  
This sends a standard XML file to a designated URL.
- **Advanced Volume**  
This sends a CSV file to a specified email address. The file includes device name, group, IP address, asset number, device ID, start page count, end page count, last active date, as well as various general and machine-specific meters.
- **Current Meters**  
This sends a CSV file to a specified email address. The file includes the device name, serial number, device ID, all available meters (standard and custom) based on a specified end date, for either **Managed** devices, **Unmanaged** devices, or both, for the selected group.
- **Canon Meters**  
This sends a CSV file to a specified email address. The file includes all available meters based on a specified end date, for either **Managed** devices, **Unmanaged** devices, or both, for Canon devices in the selected group.

Each system only must be set up once. For example, if you are using a single Digital Gateway e-automate system exclusively, your system only needs to be configured once. However, you have the option of creating multiple instances of a system if there is a need. For example, suppose you have multiple locations that use a single ERP system, and each location should only be given access to the meter export configurations for their applicable groups/devices. If you are using more than one system, each system must be configured separately.

## Creating a new meter export configuration

### Procedure

1. On the **Settings** menu, click **Meter Export**.
2. Click **New System**.
3. Enter a name for the configuration in the **Name** box.
4. Select the group that the configuration applies to from the **Group** list (all other configuration items and permissions for the export will be based on the group selected here; if it applies to your entire system, select the root group).
5. Select the type of export system you are using from the **Export Type** list.
6. If you have chosen **Digital Gateway - e-automate**, do the following:
  - Enter the URL of the e-automate system in the **Destination URL** box.
  - Enter the meter source name configured in the ERP system (e.g. PrintFleet) in the **Meter Source** box.

- Enter your company ID for the e-automate system in the **Company ID** box.
  - Enter the version of e-automate you are using in the **Version** box.
  - Enter a username for the e-automate system in the **Username** box.
  - Enter the corresponding password for the e-automate system in the **Password** box.
  - Choose the field that you want devices to be automatically mapped by from the **Sync By** list. Most commonly, serial number is used, and this is the default selection.
  - Optionally, enter the number of days a device must have reported in to be included in the meter export in the **Device Stale Days** box (value must be greater than 1).
  - Select the **Send Full Meter Group Only** check box to force the system to reject any changes unless all meters are successfully imported. This can help avoid getting the ERP system into a mixed state including both current and old meter values.
7. If you have chosen **OMD Multimeter** or **OMD Non-Multimeter**:
- Enter the URL of your H2O system in the **H2O Destination URL** box (required for all OMD meter exports).
  - Enter the URL of your iManager system in the **iManager Destination URL** box (required for automated device mapping).
  - Enter the username for iManager in the **Username** box.
  - Enter the corresponding password for iManager in the **Password** box.

**Important**

The username and password for iManager must be associated with the accounts in iManager that you want to set up meter exports for. To create a username and password that is associated with multiple accounts, obtain the REQL83 program from OMD.

- Choose the field that you want devices to be automatically mapped by from the **Sync By** list. Most commonly, serial number is used, and this is the default selection.
  - Optionally, enter the number of days a device must have reported in to be included in the meter export in the **Device Stale Days** box (value must be greater than 1).
8. If you have chosen **La Crosse NextGen**:
- Enter the URL of the NextGen system in the **Destination URL** box.

- Choose the field that you want devices to be automatically mapped by from the **Sync By** list. Most commonly, serial number is used, and this is the default selection.
  - Optionally, enter the number of days a device must have reported in to be included in the meter export in the **Device Stale Days** box (value must be greater than 1).
9. If you have chosen **La Crosse NextGen Web**:
- Enter the URL of the NextGen system in the **Destination URL** box.
  - Enter the meter source name configured in the ERP system (e.g. PrintFleet) in the **Meter Source** box.
  - Enter the user name in the **User** box and the application in the **App** box.
  - Choose the field that you want devices to be automatically mapped by from the **Sync By** list. Most commonly, serial number is used, and this is the default selection.
  - Optionally, enter the number of days a device must have reported in to be included in the meter export in the **Device Stale Days** box (value must be greater than 1).
10. If you have chosen **Evatic**:
- Enter the email address that was designated for your company to export information into your Evatic system in the **Email To** box.
  - Enter any email address into the **Email From** box.
  - Enter any email subject line into the **Subject** box.
  - Choose the field that you want devices to be automatically mapped by from the **Sync By** list. Most commonly, serial number is used, and this is the default selection.
  - Optionally, enter the number of days a device must have reported in to be included in the meter export in the **Device Stale Days** box (value must be greater than 1).
11. If you have chosen **PFI Export**:
- Enter the URL of the PFI Export system in the **Destination URL** box.
  - Optionally, enter the number of days a device must have reported in to be included in the meter export in the **Device Stale Days** box (value must be greater than 1).
12. If you have chosen **Advanced Volume**:
- Enter the email address where you would like the information to be sent in the **Email To** box.
  - From the **Device Status** list, choose whether to export information on **Managed** devices, **Unmanaged** devices, or **Both**.
  - If your meter export configuration is going to cover a long period, and you want PrintFleet to include the average values for a specified time unit (**Monthly**, **Quarterly**, or **Yearly**), select the time unit you want to use from the **Averaging**

**Interval** drop-down list. The default value is **None** (so no averaging value will appear in the exported file).

- Optionally, enter the number of days a device must have reported in to be included in the meter export in the **Device Stale Days** box (value must be greater than 1).
- From the **Date Range** list, choose the period for which you want to export the information.

13. If you have chosen **Current Meters**:

- Enter the email address where you would like the information to be sent in the **Email To** box.
- From the **Device Status** list, choose whether to export information on **Managed** devices, **Unmanaged** devices, or **Both**.
- Optionally, enter the number of days a device must have reported in to be included in the meter export in the **Device Stale Days** box (value must be greater than 1).
- From the **End Date** list, choose the last day for which you want to export the information.

14. If you have chosen **Canon Meters**:

- Enter the email address where you would like the information to be sent in the **Email To** box.
- From the **Device Status** list, choose whether to export information on **Managed** devices, **Unmanaged** devices, or **Both**.
- Optionally, enter the number of days a device must have reported in to be included in the meter export in the **Device Stale Days** box (value must be greater than 1).
- From the **End Date** list, choose the last day for which you want to export the information.

15. Click **Save**.

## Configuring meter maps

When exporting to a commercial ERP system, the meter labels used by PrintFleet software must be mapped to the meter labels used by the ERP system. For example, if the meter called Total in the PrintFleet system is called Total\_Count in the external ERP system, this association must be defined for the meter to export properly. A meter map in PrintFleet is a series of these associations applied to one or more groups and/or individual devices.

Multiple meter maps can be created for one external ERP system. Meter maps will be applied to devices based on the meter map applied to the group closest to it. For example, if the root group (which includes all groups and all devices) has a meter map assigned to it, and the group Widgets has another meter map assigned to it, devices within the group Widgets will use the meter map assigned to Widgets in any cases where the meter maps for the root group and the Widgets group overlap (in areas where they do not overlap, it will use the meter map with the additional information). This allows you to assign a basic meter map to all

---

groups and devices, and customize additional maps for specific groups and devices on an as needed basis.

## Creating a new meter map

### Procedure

1. On the **Settings** menu, click **Meter Export**.
2. Click **Meters** in the row of the meter export configuration for which you want to create a meter map. The **Meters** page appears. Any existing meter maps for the selected configuration will be listed on this page.
3. Click **New Meter(s)**. The **Meter Configuration** page appears.
4. Specify the devices to which you want to apply the meter map by doing one or both of the following:
  - Select the check box beside each group you want to add. All the devices associated with any selected group will be added automatically.
  - Click on the name of a group to view individual devices associated with the group. Select the check box beside each individual device you want to add. You can use the **Check All**, **Uncheck All**, or search function to simplify this process.
5. Click **Continue**. A list of meters appears.
6. Under the **Destination Meter** column, enter the meter labels from the external ERP system as they correspond to the meters listed under the **Meter Label** column. All available meters for the devices you selected will be displayed, however, you only must enter corresponding field names for the ones you want included in the meter export.
7. Optionally, under the **Multiplier** column, enter a multiplier for one or more meters that will be used to calculate the meter value during export. By default, the value is 1, which will not change the collected value during export. The following are some examples of how you could use a multiplier:
  - export a duplex meter as two pages (multiplier=2)
  - export a legal page as 1.3 letter pages (multiplier=1.3)
  - convert square feet to square inches (multiplier=144).
8. Click **Save**.

## Editing a meter map

### Procedure

1. On the **Settings** menu, click **Meter Export**.
2. Click **Meters** in the row of the meter export configuration for which you want to edit a meter map. The **Meters** page appears. Any existing meter maps for the selected configuration will be listed on this page.
3. Click **Edit** beside the meter map you want to edit. The **Meter Configuration** page appears.
4. Do one or both of the following:

- Enter a new multiplier value in the **Multiplier** box.
  - Use the **Assigned Groups** and **Assigned Devices** areas to change the devices to which the meter map applies.
5. Click **Save**.

## Using Priority Meters in Meter Mapping

### Procedure

1. Select the custom virtual meter that has been created previously when selecting the PrintFleet Meter Labels when creating a new **Meter Mapping**.
2. Under the **Destination Meter** column, enter the meter labels from the external ERP system as they correspond to the meters listed under the **Meter Label** column.
3. Click **Save**.

## Deleting a meter map

### Procedure

4. On the **Settings** menu, click **Meter Export**.
5. Click **Meters** in the row of the meter export configuration for which you want to delete a meter map. The **Meters** page appears. Any existing meter maps for the selected configuration will be listed on this page.
6. Click **Delete** beside the meter map you want to delete. A Delete Confirmation dialog appears.
7. Click **Continue**.

## Viewing the log for a meter map

### Procedure

1. On the **Settings** menu, click **Meter Export**.
2. Click **Meters** in the row of the meter export configuration for which you want to view the log. The **Meters** page appears. Any existing meter maps for the selected configuration will be listed on this page.
3. Click **Logs** beside the meter map for which you want to view the log. The **Schedule Log** page appears, displaying a summary of each time the mapped meter value was exported.
4. If you want to view the results of a particular export instance, in the **Options** column, click **View Results** in the row of the export instance for which you want to view the results. The **Device Log** page appears. From the **Device Log** page, you can see the actual meter values exported for each device from the scheduled instance.

## Setting up meter export schedules

Meter export schedules determine what specific meters are exported and how often they are exported. Multiple schedules can be configured for a single external ERP system, for example, if you have one client that is billed on the 15th of each month, and one client that is billed at the end of each month, these can be

configured as two separate export schedules.

## Creating a new meter export schedule

### Procedure

1. On the **Settings** menu, click **Meter Export**.
2. Click **Schedules** in the row of the meter export configuration for which you want to create a new schedule. The **Schedule** page appears. Any existing schedules for the selected configuration will be listed on this page.
3. Click **New Schedule**. The **Schedule Configuration** page appears.
4. Enter a name or description for the schedule in the **Description** box.
5. Choose one of the following time intervals for the schedule from the **Cycle Pattern** list. Time intervals are based on the iCalendar standard.
  - **Daily**. Requires you to enter how often, in days, you want the meters to export. For example, if you enter 1, meters will export every day, if you enter 2, meters will export every other day, etc.
  - **Weekly**. Requires you to enter how often, in weeks, you want the meters to export. You are also required to select which day of the week you want the meter exported. For example, if you enter 2 and select Monday, meters will be exported every other Monday.
  - **Monthly**. Requires you to enter the day of the month you want meters exported, and how often, in months, you want the meters to export. For example, if you enter 15 and 3, meters will be exported on the fifteenth day of every third month.
  - **Advanced**. Requires you to select the day of the week, which occurrence of that day during the month, and how often, in months, you want the meter export to occur. For example, if you select 2nd, Mon, and enter 2, the meter export will occur on the second Monday of every other month.
6. Enter a start date and time for the export in the **starting** box.
7. Specify which devices the schedule applies to by doing one or both of the following:
  - Select the check box beside each group you want to add. All the devices associated with any selected group will be added automatically.
  - Click on the name of a group to view individual devices associated with the group. Select the check box beside each individual device you want to add. You can use the **Check All**, **Uncheck All**, or search function to simplify this process.
8. Click **Save**.

## Editing a meter export schedule

### Procedure

1. On the **Settings** menu, click **Meter Export**. The **Meter Export** page appears.
2. Click **Schedules** in the row of the meter export configuration for which you want to edit a schedule. The **Schedule** page appears. Any existing schedules for the selected configuration will be listed on this page.
3. Click **Edit** beside the schedule you want to edit. The **Schedule Configuration** page appears.
4. Do one or more of the following:
  - Edit the name of the schedule in the **Description** box.
  - Change the **Cycle Pattern** for the schedule.
  - Use the **Assigned Groups** and **Assigned Devices** areas to change the devices to which the schedule applies.
5. Click **Save**.

## Deleting a meter export schedule

### Procedure

1. On the **Settings** menu, click **Meter Export**. The **Meter Export** page appears.
2. Click **Schedules** in the row of the meter export configuration for which you want to delete a schedule. The **Schedule** page appears. Any existing schedules for the selected configuration will be listed on this page.
3. Click **Delete** beside the schedule you want to delete. A Delete Confirmation dialog appears.
4. Click **Continue**.

## Viewing the log for a meter export schedule

### Procedure

1. On the **Settings** menu, click **Meter Export**. The **Meter Export** page appears.
2. Click **Schedules** in the row of the meter export configuration for which you want to view the schedule log. The **Schedule** page appears. Any existing schedules for the selected configuration will be listed on this page.
3. Click **Logs** beside the schedule for which you want to view the log. The **Schedule Log** page appears. The results of any schedules already run are displayed.
4. If you want to view the results of a particular export instance, in the **Options** column, click **View Results** in the row of the export instance for which you want to view the results. The **Device Log** page appears.

## Running a meter export schedule

### Procedure

1. On the **Settings** menu, click **Meter Export**. The **Meter Export** page appears.
2. Click **Schedules** in the row of the meter export configuration for which you want to run a schedule. The **Schedule** page appears. Any existing schedules for the selected configuration will be listed on this page.
3. Click **Run** beside the schedule you want to run. The meter export will occur within the next 10 minutes.

## Configuring device maps (exceptions only)

If you are exporting to an ERP system, devices detected by PrintFleet software must be associated with devices residing in the ERP system. For e-automate and OMD exports, the device mapping process will attempt to complete automatically.

You will need to manually configure device maps if:

- You are using an ERP system other than e-automate or OMD.
- You are using e-automate or OMD, but not all devices were successfully mapped automatically; this should usually be corrected by changing the sync field (serial number, asset number, or device ID) in the PrintFleet system to match the same field in the ERP system.

## Mapping PrintFleet devices to ERP system devices

### Procedure

1. On the **Settings** menu, click **Meter Export**. The **Meter Export** page appears.
2. Click **Device Mapping** in the row of the ERP system you want to configure device maps for. The **Device Mapping** page appears.
3. Click the name of the group that contains the devices for which you want to configure device maps.
4. Do one of the following:
  - Enter the ERP system device ID for each device you want to map under the **External ID** column. Depending on your system, this may be a unique ID, serial number, asset number, etc.
  - If you are using e-automate or OMD, click **Auto Map** to automatically populate the **External ID** column.

### Note

This will occur automatically without having to click the **Auto Map** button, however, it can be used to force an additional sync with the ERP system, for instance, if you have corrected a serial/asset number in the PrintFleet system and want to immediately map the changed device.

5. Click **Save**.

## Testing and troubleshooting

You can manually force a meter export to occur the next time the export process runs (every 10 minutes), without considering your permanent export schedules. This allows you to test and troubleshoot a meter export configuration.

You should follow these steps to test and troubleshoot:

1. Manually force a meter export to occur.
2. Verify that all desired meters have been exported.
3. If there are any meters that you expected to be exported but were not, check the PrintFleet meter export log to determine the reason that those specific meters did not export.

## Manually forcing a meter export to occur

### Procedure

1. On the **Settings** menu, click **Meter Export**.
2. Click **Schedules** in the row of the configuration you want to test.
3. Under the **Run Export** column, click **Run** in the row of the schedule you want to test. The meter export will occur within the next 10 minutes.

## Viewing the meter export log

### Procedure

1. On the **Settings** menu, click **Meter Export**.
2. Do one of the following:
  - Click **Logs** in the row of the configuration you want to view.
  - Click **Schedules** in the row of the configuration you want to view, and then click **Logs** in the row of the specific schedule you want to view logs for.
  - Click **Meters** in the row of the configuration you want to view, and then click **Logs** in the row of the specific meter map you want to view logs for.
3. Click **View Results** in the row of the export you want to view logs for.

The meter export logs will tell you why a specific meter was not exported. It is important to understand that the PrintFleet logs may display errors for meters that you would not expect to be successful, for example, a color meter export for a monochrome device.

The following two tables list all possible entries in the **Result Message** column of the meter export log.

The following table lists error messages, with their causes and possible solutions.

Result Message	Cause	Possible Solutions
MeterPostFail	The ERP system did not accept our meter post (generic failure message not covered by the below cases).	Start by looking in the ERP system for the specific device to ensure it is configured correct and has the proper meters assigned to it.  Double check PrintFleet has established a device mapping for the device and ensure the correct meters are assigned to it in PrintFleet.
MeterSourceDoesnt Exist	The meter source does not exist in the ERP system.	The meter source entered for the ERP system in PrintFleet must match exactly to a meter source configured in the ERP system (case sensitive).
Communication Error	PrintFleet could not communicate with the ERP system (timeout, ERP system is offline, etc.).	Ensure the ERP system is online and accepting web requests.  Double check the system configuration to ensure the correct credentials have been added for this system.
AuthenticationError	The credentials entered for the ERP system are incorrect.	Double check the system configuration to ensure the correct credentials have been added for this system.

Result Message	Cause	Possible Solutions
OtherError	PrintFleet did not receive a specific error message from the ERP system (an unhandled exception) so we log a generic error message.	The error message returned will always be different. It should be very specific to what the problem is.
MeterDoesntExist	The meter label configured in PrintFleet for the meter mappings does not exist for this specific device in the ERP system.	Ensure this device in the ERP has this meter assigned to it.  Double check the meters mapped for this device in the PrintFleet system.
EquipmentDoesnt Exist	A device has been configured to export from PrintFleet that does not exist in the ERP system.	Check the ERP system to ensure the device has been setup and has an external id assigned to it.  If it is setup in the ERP system, double check PrintFleets device mapping and if need be, apply the external id manually here.
NoModelAssigned	No model is associated to the device in the ERP system (OMD only).	Assign the device a model in OMD.

The following table lists informational messages and their causes.

<b>Result Message</b>	<b>Cause</b>
MeterPostSuccess	The meter was posted successfully.
MissingRequiredMeters	A required meter for a device in an ERP system was not configured in PrintFleet. This is informational to let you know for the additional meter posts to be successful, PrintFleet had to post this required meter (e-automate only).
MeterReadingLessThanPrevious	The current meter reading in the ERP system is greater than the current PrintFleet meter reading. This log should be followed by an additional message indicating that PrintFleet re-exported the current value in the ERP system so the other meter posts would not fail.
MeterReadingEmpty	PrintFleet obtained a meter reading of 0, or could not obtain a meter reading from our system to post into the ERP system.

# Chapter 6 Administrating PrintFleet Optimizer

---

## 6.1 Managing Users

An unlimited number of users can be created. In addition to user name and password, the following settings can be configured for each user:

- Name of the user
- Groups the user has access to
- Roles the user will have for each group
- Expiry date of the account (if applicable)
- Starting page for the user
- Time zone preference for the user
- Elements that will make up device names in the system for the user (may include, name, serial number, IP address, etc.)

For more information on groups, see "Managing Groups" on page 97.

You can view a list of existing users and their login name (typically their email address), first name, last name, last login date and time, and groups and role access.

### Viewing existing users

#### Procedure

- On the **Administration** menu, click **Users**.

---

**Note**

If you want, you can filter the list of users by choosing a group from the **Filter by Group** list. Only the users that have been assigned to the specified group (or to any subgroup of the specified group) will be displayed.

---

A separate user account should be created for everyone who is granted access to the user interface. The following describes how to create a new user account, and how to create a new user by copying the permissions of an existing account.

### Creating a new user account

#### Procedure

1. On the **Administration** menu, click **Users**. The **Users** page appears.

2. Click **New User**. The **User Add/Edit** page appears.
3. In the **Information** area, enter the following:
  - **User Name** (often the user's email address)
  - **First Name**
  - **Last Name**
  - **Password** (repeat in the **Confirm Password** box)
4. Optionally, in the **Settings** area, complete one or more of the following:
  - Type or select an expiry date for the account in the **Expiry Date** box. Note that the account will expire at the start of the specified date, not at the end.
  - Select the **Disabled** check box to deactivate the account. The user will appear in the user list, but will not be able to access the software.
  - Select the **Force Password Change at Next Login** box to require the user to change their password the next time they login.
  - From the **Starting Page** list select the first page that will appear each time the user logs in.
  - From the **Language** list select the language in which the user interface will appear.
  - From the **Time Zone** list select the time zone in which the user is located. See "Changing Preferences" on page 95 for more information about the way time zones are used.
  - To specify your regional electricity cost per kWh, enter the rate as a decimal value in the **Cost per kW h** box. This value is used in various reports when calculating power cost estimates for devices.
  - Enter a customized way to display device names throughout the system in the **Device Name Template** box, or select a method from the list underneath. For more information on the **Device Name Template**, see "Changing Preferences" on page 95.
5. In the **User Access** area, click **Add Entry**.
6. Click the name of a group that the user will have access to. If a group contains one or more subgroups, the user will have access to those groups as well. To give a user access to all groups, select Root Group.
7. Select one or more roles the user will have for the selected group. The user's permissions are the combination of the permissions granted to all selected roles. For more information on permissions and security, see "Configuring Scan Intervals" on page 162.
8. Repeat steps 6 and 7 to give the user access to additional groups.
9. Click **Save**.

## Creating a user account with duplicate permissions

You can create a user account with the same permissions (group access and roles) as an existing account.

### Procedure

1. On the **Administration** menu, click **Users**. The **Users** page appears.
2. Under the **Options** column, click **Copy** in the row of the user account with the permissions you want to duplicate (alternatively, click **Edit** and then click **Copy** on the **User Add/Edit** page).
3. Complete the fields in the **Information** and **Settings** areas.
4. Optionally, edit default permissions in the **User Access** area.
5. Click **Save**.

After a user account is created, it can be edited at any time.

## Editing an existing user account

### Procedure

1. On the **Administration** menu, click **Users**. The **Users** page appears.
2. Under the **Options** column, click **Edit** in the row of the user account you want to edit. The **User Add/Edit** page appears.
3. Change the user account information as desired.
4. Click **Save**.

## Deleting a user account

If a user account is no longer needed, it can be deleted or disabled at any time. Deleting a user will remove it from the system.

Disabling a user will retain the user record in the system, but will remove access to the software.

### Procedure

1. On the **Administration** menu, click **Users**. The **Users** page appears.
2. Under the **Options** column, click **Delete** in the row of the user account you want to remove.
3. Before the user is deleted, you will receive a notification informing you that in removing the user from the DCA, alerts and reports associated with that user will stop relaying information. While they will still exist, you will cease to receive potentially important information because they no longer have a specified host. This could impact business processes. If business processes are related to this account, we recommend that you assign that user's account another user **or rename** the account to reflect the function of the reports/alerts. By doing this, you will still receive data. You can contact your System Administrator if you need help, or **Confirm** or **Cancel** the delete.

## Disabling a user account

### Procedure

1. On the **Administration** menu, click **Users**. The **Users** page appears.
2. Under the **Options** column, click **Edit** in the row of the user account you want to disable. The **User Add/Edit** page appears.
3. Under the **Settings** area, select the **Disabled** check box.
4. Click **Save**.

### Note

The effects of disabling a user account are not instantaneous—there may be a delay before the system process the information and actually disables the account.

## 6.2 Exporting and Importing Device Data

You can export and import device information. The primary intended use for this functionality is to allow customers to easily make bulk updates by exporting device information to an external file, making changes to the data in the file, and then importing the file with the changes back into PrintFleet. You might do this if you were changing a property that affects many devices, such as adding a prefix to all your asset numbers, or changing the names of your locations. You might also want to export device information to be able to view the information for many devices at once, or to use the information with a third-party application.

### Exporting device information

You can export the device information for a selected group to a file in comma separated values (.CSV) format. The file includes information for the devices in the selected group and for all subgroups of that group. The exported fields are as follows:

- Device ID
- Device Name
- Serial Number
- Asset Number
- Location
- Device Type
- IP Address
- MAC Address
- Subnet Mask
- Service Tag
- Host Name
- Creation Date
- Last Active Date
- Custom Fields

<b>Note</b>	<p>When PrintFleet exports custom fields for a selected group, it only exports the custom fields that are enabled and which are shared by all of the devices in the selected group.</p> <p>Also, if a group and a subgroup both have custom fields defined with the same name, and both fields are enabled, the value associated with the lower level group will be exported.</p>
-------------	---

**Procedure**

1. On the **Administration** menu, click **Import/Export**. The **Import/Export** page appears.
2. On the **Export** tab, from the **Device Group** list, choose the group from which you want to export device information.
3. Click **Download CSV**. The file is downloaded according to your browser settings. The name of the downloaded file is ExportedDevices followed by a date and time stamp (such as ExportedDevices-2012-02-28-02-43-PM.csv).

After you export the device information, you can edit the .CSV file, and then use the Import function to load the changes into PrintFleet.

<b>Note</b>	<p>When editing the .CSV file, make sure that the unique ID value for each device (the value in the DeviceId column) stays with the relevant row. If the IDs become mixed up, and you import the changes, the integrity of your system could be compromised.</p>
-------------	--

**Importing device information**

You can import the following device fields from a file:

- Device Name
- Serial Number
- Asset Number
- Location
- Custom Fields

<b>Note</b>	<p>When PrintFleet imports custom fields, it will only import a column from the file if the column name is an exact match to a custom device field name.</p> <p>If a group and a subgroup both have custom fields defined with the same name, and both fields are enabled, values for that field will be imported to the subgroup.</p>
-------------	--

<b>Notes</b>	If you are entering information for a custom device field that has an Attribute Type of Date, be sure to enter the date value using a format that is consistent with the format being used on your PrintFleet server.
--------------	---

The file you import must include a column containing device IDs for existing devices; you cannot use the **Import** function to add new records.

Changes to any fields other than those listed above will be ignored. Unlike the export operation, you can import information for devices belonging to different groups.

<b>Note</b>	You can only import comma or tab delimited files. If you are editing the file using Microsoft Excel, and the file includes unicode characters, you must save the file in Unicode (.txt) format.
-------------	---

#### Procedure

1. On the **Administration** menu, click **Import/Export**. The **Import/Export** page appears.
2. On the **Import** tab, click the **Browse** button, then select the file containing the device information you want to import. PrintFleet automatically checks the specified file to ensure it meets the requirements, then displays a check box for each field which could be imported from the file.
3. Select the check box beside each field you want to import.
4. Click **Import changes**.

## 6.3 Branding the User Interface

The user interface can be branded to match your company's marketing initiatives. If necessary, branding settings can be customized for different groups. The following items can be branded in the user interface:

- Product logo
- Executive report cover (front and back)
- Primary and link colors
- Product name
- Login page

### Customizing the product logo

The logo that appears in the upper left corner of the user interface can be customized. Any web format image is acceptable. PrintFleet

will automatically scale the image to fit, but an original size of 70 pixels high by 280 pixels wide would be ideal.

### Procedure

1. On the **Administration** menu, click **Custom Branding**. The **Custom Branding** page appears.
2. Select the group that the branding applies to.
3. On the **Images** tab, in the **PFO Logo** area, do one of the following:
  - To use an image from a file, click the **Browse** button to locate an image file on your computer, and then click **Upload**.
  - To use an image from a URL, type the URL of an uploaded image (including the file name and extension of the image) in the **From URL** box, and then click **Load**.
4. Click **Test** to preview the changes.
5. Click **Save**.

## Customizing the Executive Report cover

The front and back pages that appear on executive reports can be customized. If you choose a new custom image, PrintFleet will automatically scale the image to fit as necessary. The custom image appears when any user from the specified group runs an executive report that has been set up to include a cover page with custom branding.

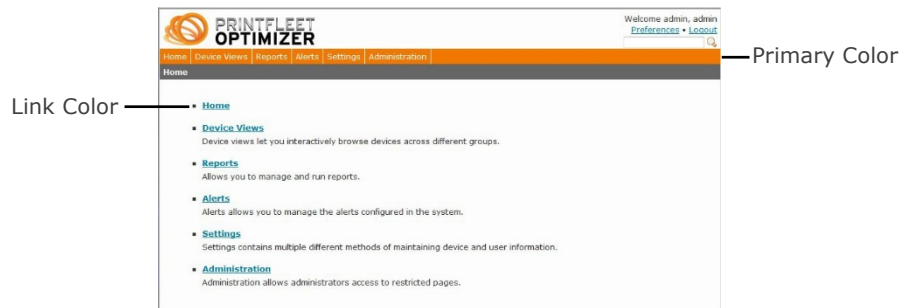
### Procedure

1. On the **Administration** menu, click **Custom Branding**. The **Custom Branding** page appears.
2. Select the group that the branding applies to. On the **Images** tab, in the **Exec Report Start** area, do one of the following to customize the front cover:
  - To use an image from a file, click the **Browse** button to locate an image file on your computer, and then click **Upload**.
  - To use an image from a URL, type the URL of an uploaded image in the **From URL** box, and then click **Load**.
3. In the **Exec Report End** area, do one of the following to customize the back cover:
  - To use an image from a file, click the **Browse** button to locate an image file on your computer, and then click **Upload**.
  - To use an image from a URL, type the URL of an uploaded image in the **From URL** box, and then click **Load**.
4. Click **Save**.

## Customizing Interface Colors

Some interface colors can be customized. Specifically, you can change:

- **Primary color**  
This color is used for the menu background color as well as the color for some buttons.
- **Link color**  
This color is used for links (such as the device name links that appear on the **Technical View**).



### Procedure

1. On the **Administration** menu, click **Custom Branding**. The **Custom Branding** page appears.
2. Select the group that the branding applies to.
3. Click the **Styles** tab.
4. Do one or both of the following:
  - Click in the **Primary Color** box, and then click one of the colors in the color selection panel that appears. The color you selected is displayed in the **Primary Color** box along with the corresponding hexadecimal RGB value. If necessary you can also specify a color by typing the hexadecimal code for the color you want.
  - Click in the **Link Color** box, and then click one of the colors in the color selection panel that appears. The color you selected is displayed in the **Link Color** box along with the corresponding hexadecimal RGB value. If necessary you can also specify a color by typing the hexadecimal code for the color you want.
5. Click **Test** to preview the changes.
6. Click **Save**.

### Notes

With versions of PrintFleet Optimizer/Enterprise prior to 3.1 you could set different custom branding options. These custom branding settings are preserved when you upgrade to version 3.1 (or later).

**Notes**

However, the first time you change either the Primary Color or Link Color setting, all of the other legacy branding settings automatically and permanently revert to their default values.

**Customizing the product name**

The name of the product (software) that appears in the title bar of the web browser can be customized.

**Procedure**

1. On the **Administration** menu, click **Custom Branding**. The **Custom Branding** page appears.
2. Select the group that the branding applies to.
3. Click the **Miscellaneous** tab.
4. In the **Product Name** box, type your customized product name.
5. Click **Test** to view the new product name in the title bar of the web browser.
6. Click **Save**.

**Customizing the login page**

Your log in page is not only a simple, secure and familiar portal into PrintFleet Optimizer - it can also reflect your brand. To see how we can customize our login page for your business, contact your account manager, CARE representative or tech support.

## 6.4 DCA Installations

Effective with PrintFleet Optimizer 3.6.0, you can install the DCA without having to provide a PIN. For more information, see "Downloading the simplified DCA installer" on page 142.

Prior to version 3.6.0, each DCA installation required a PIN Code to activate to run. These PIN Codes can be generated and managed using PrintFleet Optimizer. For more information about the DCA, see the *PrintFleet DCA User Guide*.

**Activating a new PrintFleet DCA: 4.x and Pulse**

In the PrintFleet Optimizer, administrators can create a new group and a DCA.

Prior to the activation of a new DCA, you have the following options: to install DCA 4.x, or to install DCA Pulse - PrintFleet's next generation software.

- If you decide to install **DCA 4.x**, you have two options:

To let the DCA client automatically configure scan setting. This allows the DCA client to configure the scan settings

automatically by scanning the network and populating the scan ranges.

OR

To manually preconfigure scan settings. You can specify a custom scan range and other related settings, which are downloaded by the DCA immediately after activation and the service starting up (prior to the first scan). For more information, see "Manually preconfiguring scan settings" on page 141.

<b>Note</b>	Preconfiguring the DCA is available with DCA4.4.3 and later.
-------------	--

## Installing DCA Pulse

If you **install DCA Pulse**, there are two install options:

1. To install remotely with PrintFleet `s installer.
2. To install Pulse on Raspberry Pi on an ISO image.

Whichever option you choose, DCA Pulse installs automatically and allows users a more comprehensive and effectual range of configuration settings than those available in DCA 4.x.

<b>Note</b>	If you wish to install DCA Pulse for a client, but already have DCA 4.x running, there is no need to uninstall DCA 4.x first. DCA Pulse and DCA 4.x run seamlessly side-by-side, operating harmoniously and independently.
-------------	--

### Procedure

1. On the **Administration** menu, click **DCAs**.  
The **DCAs** page appears.
2. Click **New DCA**.
3. On the **Create DCA** page, under **Server Setup**, click **Create New Group**.

DCA Dealer 1 [✕](#) [Delete DCA](#)

Activation [Config](#)

**DCA Activation**  
Please complete the DCA setup by installing and activating the client software.

Server Setup

Group [Root Group > PvK Test](#) [✕](#)

Expiry  Never

Device Manufacturer Extensions

HP SDS  Enable (Windows only)  
 Disable

Client Setup

Download [v1.0.1.3617 GA](#) [Other Downloads](#)

Activation PIN [P323RE1DWXAZ](#) [✕](#)

Send the download link via email:

Email To  [Send](#)

4. In the **Parent** group box, select an existing group.
5. In the **Create New Group** section, do the following:
  - In the **Type** box, select a type of group that you want to create. The type can be a dealer, distributor, or customer.
  - In the **Name** box, enter a name for the group that you want to create.
6. In the **Name** box, enter a name for a new DCA.
7. In the **Expiry** area, do one of the following:
  - If you do not want the DCA to expire, select the **Never** check box.
  - The date in the **Expiry** area is only associated with the DCA. It does not affect the DCA group. To set a date for the DCA to expire, clear the **Expiry** check box, click in the date box, and select a date in the calendar.  
You can also manually enter the date using the format: *dd-mmm-yyyy*.
  - At this point you have the option to choose to install DCA Pulse or DCA 4.x under **Client Setup**. Select DCA 4.x or DCA Pulse.
  - Click the **Override Activation PIN** box if you wish to insert a prefixed PIN.
  - Click **Create DCA**.
  - Unclick the **Expiry** box if you wish to set an expiration date for the DCA.

- In the Device Manufacturer Extension you have the option to pre-register the HP SDS option.
- DCA Pulse will give you the option to Override the activation pin with a self-defined one.
- The installation will recommend a platform based on the operating system you are currently using. If PrintFleet Optimizer cannot detect the operating system, it will provide a drop-down list with options, including Windows, Linux versions and macOS. Select the platform on which you would like to run DCA Pulse. You will have the option to configure the manual settings in the **Configuration** tab after you click **Create DCA**.



(Optional) In the **Email To** box, enter the email address to send the download link. The PIN is embedded in the link, so there is no need to enter it separately.

- The download button will take you to the download page where you need accept the End User License Agreement. Once DCA Pulse has downloaded, follow the prompts on your **Setup Wizard** to install. The URL and PIN are integrated into the download link, so you will not need to enter your Activation PIN.

<b>Note</b>	For Linux and macOS, your computer server will need to be pre-installed with MONO v5.4 or higher framework setup prior to installation.
-------------	---

## Installing DCA Pulse on Raspberry Pi

To install DCA Pulse on Raspberry Pi, you are required to deploy an image onto a compatible SD card and then install the card into Raspberry Pi.

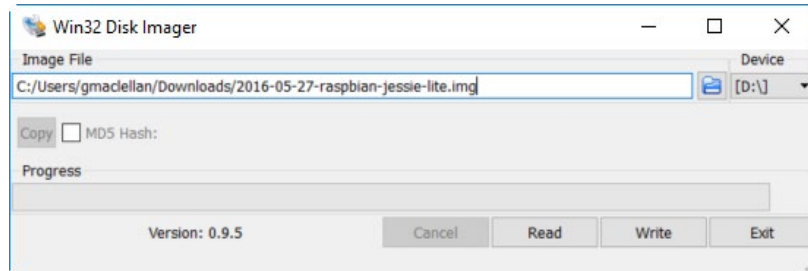
Follow these steps to complete installation:

### You'll need:

- Raspbian Jessie Lite image
- Win32DiskImager
- An SSH client (e.g., PuTTY)
- A blank SD card

**Next:**

1. Insert a blank SD card. This card will be erased.
2. Run Win32DiskImager. Select the appropriate drive and image you downloaded, and select **Write**.



3. Insert the SD card and turn the power on Raspberry Pi.
4. Get its IP address.
5. Plug in a monitor and keyboard, then login using the defaults: Username: pi; password: raspberry. Then, run ifconfig.

OR

Find the device on the network by looking for its MAC address. All of them start with B8-27-EB.

6. Enable SSH on Raspberry Pi by running raspi-config. Select **Advanced Options** then select **SSH** (Secure Socket Shell) and enable it.

**Note**

SSH is a network protocol that provides administrators with a secure means to access a remote computer.

7. SSH to the IP and login using the defaults: Username: pi; password: raspberry.  
*Optional:* Update the package list and download latest package upgrades.
8. Install MONO.
9. Download Pulse using wget and the link from the DCA download page in PrintFleet Optimizer.
10. Mark the downloaded file as executable.
11. Run the installer.

**Install Details**

Default install location: /opt/dcapulse

Service name: dcapulse (works with SysV init, upstart, and systemd)

Config location (One of the following):

~/.dcapulse/dcapulse.config

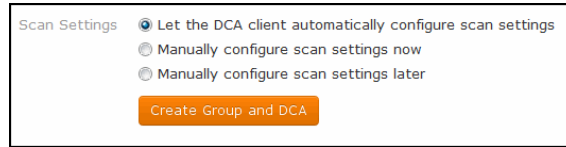
/etc/dcapulse/dcapulse.config

/boot/dcapulse.config

**Installing DCA 4.x**

If you select **DCA 4.x**, follow these steps:

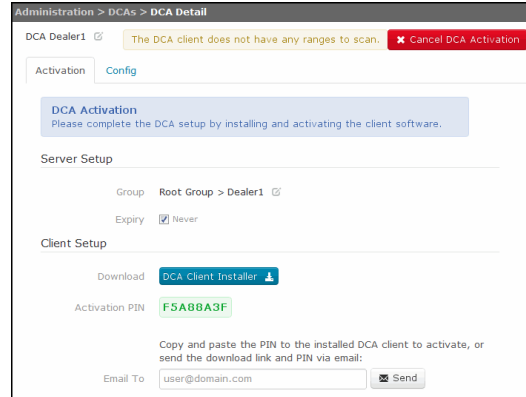
In the **Scan Settings** area, do one of the following:



- To allow the DCA to configure the scan settings automatically, click **Let the DCA client automatically configure scan settings**.
- To manually configure the scan settings, click one of the following:
  - **Manually configure scan settings now.** For more information, see "Manually preconfiguring scan settings" on page 141.
  - **Manually configure scan settings later.** If you select this option and then activate the DCA, the DCA will scan empty scan ranges until you configure new scan ranges.

12. Click **Create Group and DCA**.

13. If you selected the **Let the DCA client automatically configure scan settings** option, the **Activation** tab (**DCA Detail** page) appears. Go to step 10.



14. Once DCA 4.x has downloaded, follow the prompts on your **Setup Wizard** to install. The URL and PIN are integrated into the download link, so you will not need to enter your Activation PIN unless you activate it manually, or install the DCA from a file without the URL or PIN.

15. (Optional) In the **Email To** box, enter the email address to send the download link. The PIN is embedded in the link, so there is no need to enter it separately.

**Important:** DCA activation must be completed before you can successfully use the PrintFleet DCA application. If you attempt to use DCA functions before the activation is finished, you will

receive a message asking you to wait until activation is complete.

An email is queued for: print@printfleet.com

16. Once activated, log on to the PrintFleet DCA application.

## Manually preconfiguring scan settings

DCA 4.x allows you to manually preconfigure the scan settings to specify the scan ranges to be downloaded by the DCA before it is activated.

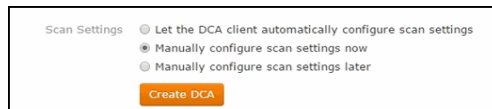
You can manually configure the scan settings now or choose to manually configure the settings later.

If you click **Manually configure settings later**, the **Activation** tab appears. Copy the **Activation PIN** and activate the DCA. The PrintFleet Optimizer will download empty scan ranges so you can configure the DCA later.

## Manually preconfiguring scan settings now

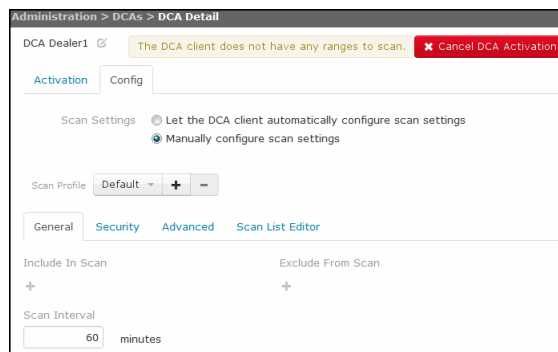
### Procedure

1. Follow steps 1 to 7 in "Activating a new PrintFleet DCA: 4.x and Pulse" on page 135.
2. On the **Server Setup** page, in the **Scan Settings** area, click **Manually configure scan settings now**.

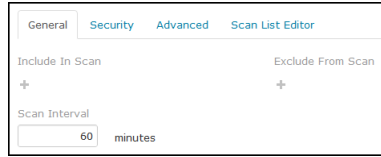


3. Click **Create DCA**.

The **DCA Detail** page appears.



4. (Optional) On the **General** tab, do the following:

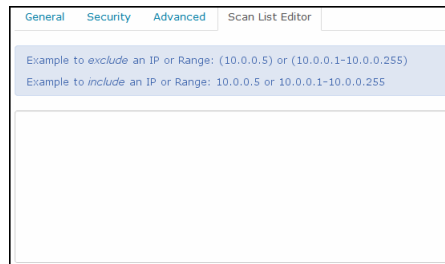


- In the **Include in scan** box, click the **Add (+)** button and enter an IP address.
  - In the **Exclude from scan** box, click the **Add (+)** button and enter an IP address.
5. (Optional) On the **Scan List Editor** tab, enter an IP address range.

**Note**

If you want to set multiple IP addresses or multiple IP ranges, you can enter the values in bulk on the **Scan List Editor** tab.

For more information, see "Specifying multiple scan ranges" on page 153.



6. Click **Save Changes**.
- The **Activation** tab appears.
7. Download the installer and install the DCA.
8. (Optional) In the **Email To** box, enter the email address to send the download link.

An email is queued for: [print@printfleet.com](mailto:print@printfleet.com)

9. Log on to the PrintFleet DCA application.

## Downloading the simplified DCA installer

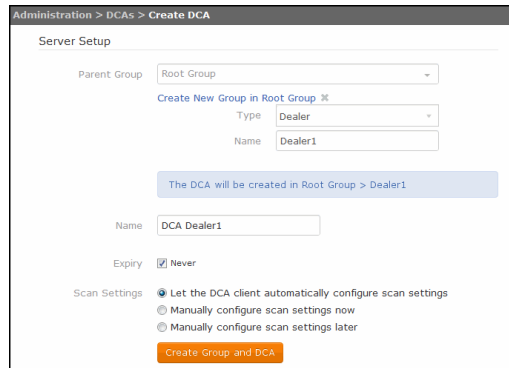
When a DCA and associated group are created, PrintFleet Optimizer generates a download URL (link) specific to that customer.

An administrator can either run the software directly on the end user's system or email a download link with instructions on how to download the DCA.

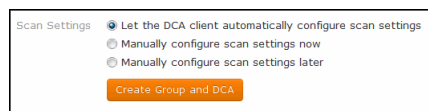
<b>Note</b>	The simplified DCA install is designed for new installations only.
-------------	--

**Procedure**

1. On the **Administration** menu, select **DCAs**.  
The **DCAs** page appears.
2. Click **New DCA**.  
The **Server Setup** page appears.
3. In the **Group** list, select an existing group.

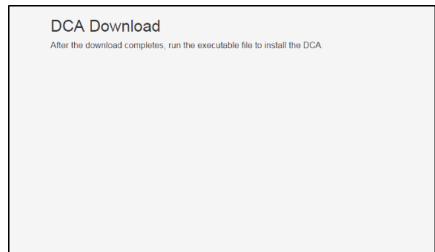


4. In the **Name** box, enter a name for the new DCA.
5. In the **Expiry** area, do one of the following:
  - If you do not want the DCA to expire, select the **Never** check box.  
The date in the **Expiry** area is only associated with the DCA. It does not affect the DCA group.
  - To set a date for the DCA to expire, clear the **Expiry** check box, click in the date box, and select a date in the calendar.  
You can also manually enter the date using the *dd-mmm-yyyy* format.
6. In the **Scan Settings** area, do one of the following:

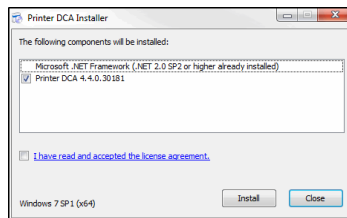


- To allow the DCA to configure the scan settings automatically, click **Let the DCA client automatically configure scan settings**.

- To manually configure the scan settings, click one of the following:
    - **Manually configure scan settings now.** For more information, see "Manually preconfiguring scan settings" on page 141.
    - **Manually configure scan settings later.** If you select this option and then activate the DCA, the DCA will scan empty scan ranges until you configure new scan ranges.
7. Click **Create DCA**.
- The **DCA Detail** page appears.
8. On the **DCA Detail** page, in the **Client Setup** area, click **DCA Client Installer**.
- A DCA download page appears and you are prompted to run the executable file to install the DCA.

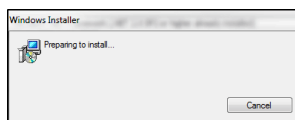


9. In the **DCA Installer** dialog box, read the EULA and then select the **I have read and accepted the license agreement** box.

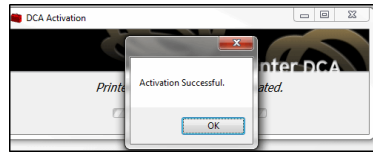


<b>Note</b>	If the .Net Framework is not installed on your computer, you will be prompted to install it.
-------------	--

10. Click **Install**.
- The DCA starts the installation process.



- When the installation is complete, click **OK** in the **Activation Successful** dialog box.



The DCA application appears in the **Start** Menu.



## Downloading the Manual Installer

If you are dealing with complex and highly personalized networks, then you may want to download the manual DCA installer. Doing this will allow you to change default installation settings, like installation path within the PrintFleet Optimizer server.

To download the Manual DCA Installer:

- Select the **Administration** option on the Home Page, or from the list of tabs at the top left corner of your screen.
- Select **DCAs**.
- Select the DCA for which you would like to download the Manual DCA Installer.
- Check the **Manual Installer** box under the DCA Client Installer button. The button will now read, "Manual DCA Installer". Click to begin download.
- Once the download is complete, the DCA Setup Wizard will prompt you to personalize the installation. Click **Next** to continue, or **Cancel** to exit.
- You now have the option to **Modify** the way DCA features are installed, **Repair** errors in the recent installation, and to **Remove** DCA from your computer. Click the "Modify", "Repair" or "Remove" icon to select the operation you would like to perform.

## Managing DCAs

You can check the installation status of DCAs on the **DCAs** page and the status of a selected DCA on the **DCA Detail** page. A DCA can also be disabled or enabled. You can also create a new PIN Code for a DCA 4.x.0 or higher.

## Checking the status of a DCA

### Procedure

1. On the **Administration** menu, select **DCA**. The **DCAs** page appears.
2. Select the group for which you want to view the DCA status.
3. In the **Status** column, the status of the DCA is displayed:
  - **Pending Activation** – PIN Code has not been used to activate DCA client.
  - **Active** – DCA has been activated using PIN Code.
  - **Inactive** – the DCA has been set to Inactive or has expired.
  - **Disabled** - the DCA has not been enabled.
  - **Stale** - the DCA has not reported for more than three days.
  - **Expired** - the DCA became invalid after the date of expiry. To help avoid unwanted DCA expiration, refer to the DCA creation date, which you can see in the DCA detail page of any activated DCA. Administration>DCAs.

## Viewing DCA information

### Procedure

1. On the **Administration** menu, select **DCA**. The **DCAs** page appears.
2. Select the group for which you want to view the DCA status.
3. In the **DCA** column, click on the DCA that you want to view. The **DCA Detail** page appears with the **Overview** tab displayed.

## Updating multiple DCAs

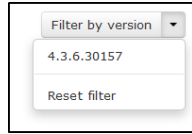
Administrators can perform a software update on one or more DCAs at the same time.

### Procedure

1. On the **Administration** menu, select **DCAs**.  
The **DCAs** page appears.
2. In the **Group** box, select a DCA group.  
All DCAs associated with this group are listed on the **DCA** page.

Group	Status	Last Reported
PrintFleet Kingston HQ		
1st Floor Office	OK	2 minutes ago
2nd Floor Office	OK	2 minutes ago
300 Ontario Street	Inactive	8 minutes ago
Main Office	OK	7 minutes ago
PF Kingston HQ	OK	18 minutes ago
PrintFleet EU	Inactive	8 minutes ago
Test	Pending Activation	

- (Optional) To show only DCAs that are running on a specific software version, click the **Filter by version** button and select a version number.



The **DCAs** page refreshes to display only those DCAs that are at the selected software version.,

- In the **DCA** column, select one or more DCAs.
- (Optional) To alphabetically sort the DCAs in ascending or descending order, click the sort button beside the column title.
- In the **With Selected** box, select one of the following:
  - **Update** to update to most recent version
  - **Auto update** to update to most recent version and when a new DCA version is released, an update should be issued automatically
  - **Cancel update**

**Note**

**Update versus Auto update**

If you want to test the DCA before applying multiple DCA updates, it is recommended that you select the **Update** option. After testing the latest DCA, you can then select the DCAs that you want to update and queue an update.

If you want to have DCAs automatically update to the most recent software version, select the **Auto update** option.

- Click **Queue**.

A confirmation message appears: *Bulk operation queued successfully.*

## Viewing software update status

Administrators can view the DCA client software update status by clicking **Administration > DCAs**.

You can determine at a glance whether the status of DCAs are update queued, available, or set to auto update. On the **DCAs** page, in the **Version** column, icons identify the state of updates for the DCAs:

**Icons:**

- Update queued: Update queued
- Auto update: Auto update
- Update available: Update available
- Enforced updated: Auto update enforced

On the **DCAs** page, in the **Last Update** column, you can also view whether a DCA successfully updated or failed to update and the related time stamp:

Host Info	Last Update
WORKGROUP\1740-1143	Update failed on 17-Feb-2015 11:43 am
PRINTFLEET\PFI-DK-LTP-001	
PRINTFLEET\PFI-DK-DTP-003	Update succeeded on 17-Mar 10:39 pm

## Viewing update status of selected DCAs

Administrators can view the update status for a selected DCA on the **DCA Detail** page.

### Procedure

1. On the **Administration** menu, select **DCAs**.  
The **DCAs** page appears.
2. In the **DCA** column, click on a DCA.  
The **DCA Detail** page appears.

### Note

Under the **Version** button, the status of the software update for the selected DCA is displayed.

Version **4.3.6.30157**

Update available

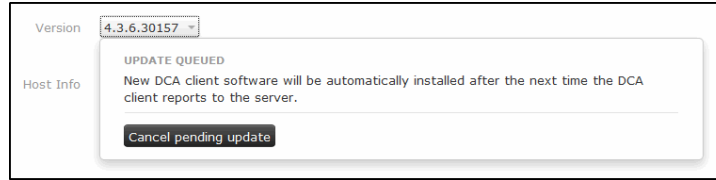
3. (Optional) To view detailed host details, select the down arrow in the **Host Info** box.
4. Click the **Version** button and select **Queue DCA client update** to update the software.

Version **4.4.0.30147**

Auto Update

Host Info **Queue DCA client update**

The status changes to Update Queued. The new DCA client software will be automatically installed after the next time the DCA client reports to the server.

**Note**

To Cancel the update, click the **Cancel pending update** button.

## Disabling and deleting a DCA

You can set the DCA to a disabled state in PrintFleet Optimizer.

### Procedure

1. On the **Administration** menu, click **DCAs**.  
The **DCAs** page appears.
2. In the **Group** box, select a DCA group.  
All DCAs associated with this group are listed on the **DCAs** page.
3. In the **DCA** column, select the DCA that you want to disable.  
The **DCA Detail** page appears.
4. Click the **Disable** button to disable the DCA.  
A confirmation message confirms the DCA is disabled.

**Disabled.** Device scans reported by this DCA client are ignored.

### Deleting a DCA

There are several reasons you may want to delete a DCA, including when a DCA is created by mistake, when a DCA is a duplicate, or when a DCA is no longer active or relevant.

#### To delete a DCA:

1. Select the **Administration** option on the **Home Page**, or from the list of tabs at the top left corner of your screen.
2. Select **DCAs**.
3. Chose the DCA you would like to delete from the **Group** drop down menu.
4. Once the DCA list appears, click on the DCA you would like to delete. This will take you to a screen that shows you the DCA details.

5. Select the red **Delete DCA** button.
6. Confirm you would like to delete the DCA by clicking on **Yes, I'm sure, delete this DCA**. Select **Cancel** if you do not wish to delete the DCA.

## Enabling and reactivating a DCA

When a DCA is disabled, the DCA checks in every 24 hours to confirm if it is in a disabled state.

On enabling the DCA, the next time the DCA checks in, it is enabled and starts reporting.

You can enable a disabled DCA to a new PrintFleet Optimizer 3.6.0 server or a previously registered PrintFleet Optimizer 3.6.0 server.

### Procedure

1. On the **Administration** menu, click **DCAs**.  
The **DCAs** page appears.
2. In the **Group** box, select a DCA group.  
All DCAs associated with this group are listed on the **DCAs** page.
3. In the **DCA** column, select the DCA that you want to reactivate.  
The **DCA Detail** page appears.
4. Click **Reactivate DCA**.
5. You will receive this warning message: "The DCA has reported within the last three days. Are you sure you want to reactivate? The DCA will deactivate and will be assigned a new pin pending activation." Select either **Cancel** or **Reactivate DCA**.  
Log on to the DCA application to configure the reactivation.

## 6.5 Configuring Scan Settings

The Data Collection Agent (DCA) network scan settings can be configured remotely from the PrintFleet Optimizer (PFO) using DCA 3.6.0 (or higher) as well as DCA Pulse.

However, DCA Pulse offers enhanced scan settings, allowing users to set more customized scan intervals. The process for accessing your scan settings is the same for DCA 4.x and DCA Pulse, but what and how you can configure settings is quite different, as outlined below.

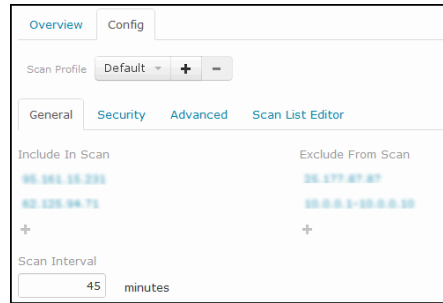
### Viewing Scan Configuration settings

Whether using DCA 4.x or DCA Pulse, administrators can view the scan configuration details of DCAs on the PrintFleet Optimizer server.

#### Procedure

1. On the **Administration** menu, click **DCAs**.  
The **DCAs** page appears.

2. In the **Group** box, select a DCA group.  
All DCAs associated with this group are listed on the **DCAs** page.
3. In the **DCA** column, select a DCA.  
The **DCA Detail** page appears.
4. Click the **Config** tab.



This is where DCA 4.x and DCA Pulse will differ.

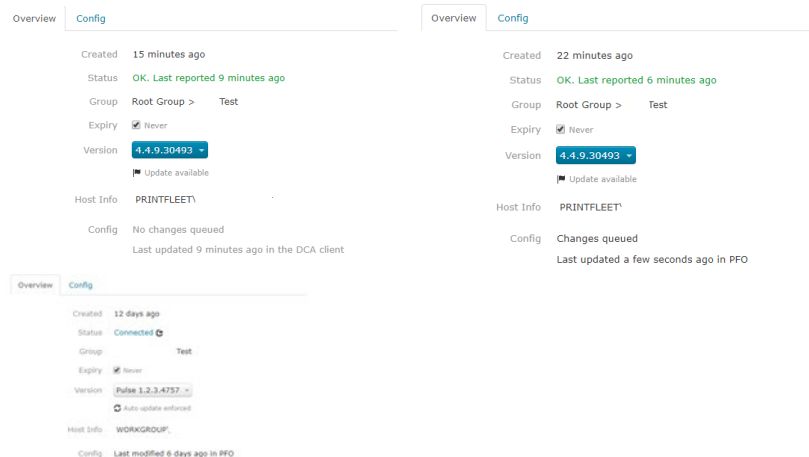
For **DCA 4.x**, the scan configuration settings for the selected DCA are displayed on the following tabbed pages:

- **General** tab
- **Security** tab
- **Advanced** tab
- **Scan List Editor** tab

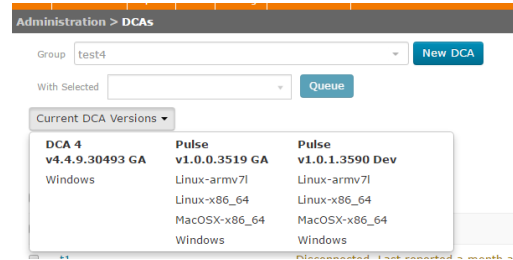
Those using **DCA Pulse** will see tabbed pages for the following:

- **Scan List** tab
- **Scan Intervals** tab
- **Security** tab
- **Communication** tab
- **Log** tab

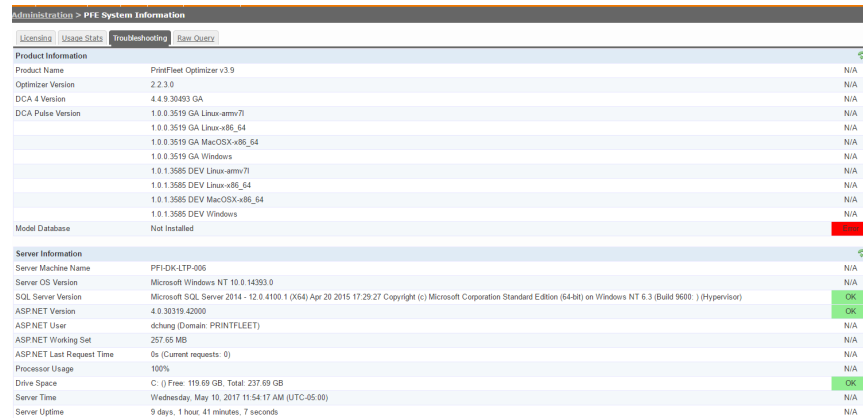
The **Overview** tab of the **DCA Detail** page shows when the DCA configuration was last modified and whether the configuration change came from PFO or the DCA 4.x user interface.



The **Overview** tab of the **DCA Detail** page will show the current versions of the DCAs.



For administrators we will also show it on the troubleshooting page.



## 6.6 DCA 4.x: Managing Scan Profiles

DCA 4.x allows administrators to use profiles to configure multiple types of network scans.

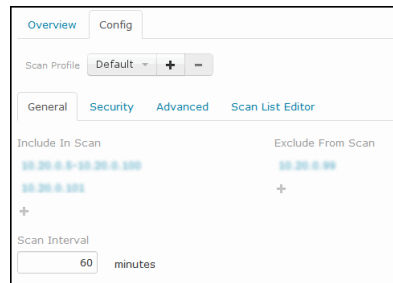
For example, you may want to scan networked devices every hour and local devices once a day — these would be two different scan profiles. You may also want a different scan profile for one or two high priority devices that you want to scan more frequently.

Depending on your environment, you may have multiple uses for scan profiles or you may only require one profile. When you initially install the DCA, you have one scan profile called **Default**.

## Creating Scan Profiles

### Procedure

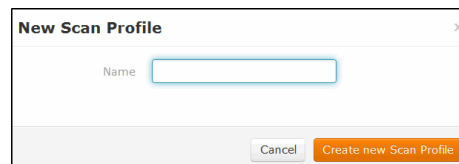
1. On the **Administration** menu, click **DCAs**.  
The **DCAs** page appears.
2. In the **Group** box, select a DCA group.  
All DCAs associated with this group are listed on the **DCAs** page.
3. In the **DCA** column, select a DCA created for the device.  
The **DCA Detail** page appears.
4. Click the **Config** tab and then click the **General** tab.



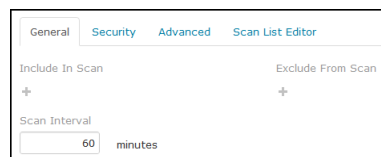
5. In the **Scan Profile** area, click the **Add (+)** button.



6. In the **New Scan Profile** box, enter a name for the new profile.

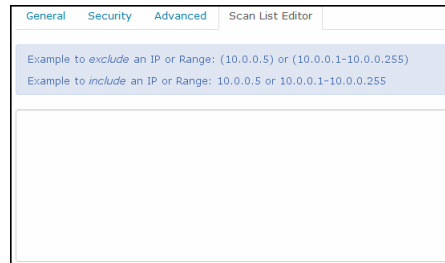


7. Click the **Create new Scan Profile** button.
8. To specify the IP address range for the scan profile, do any of the following:
  - Click the **General** tab and do the following:



- In the **Include in scan** box, click the **Add (+)** button and enter an IP address.
- In the **Exclude from scan** box, click the **Add (+)** button and enter an IP address.

- Click the **Scan List Editor** tab and enter the IP addresses/ ranges. For more information, see "Specifying multiple scan ranges" on page 153.



9. (Optional) In the **Scan Interval** box, enter a new scan interval if you want to change the default interval. For more information, see "Scan Intervals" on page 154.

10. Do one of the following:



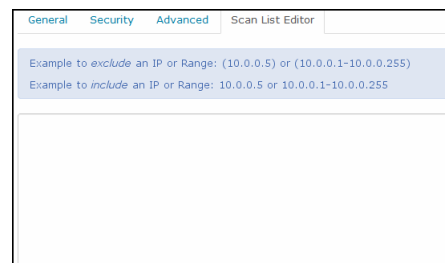
- Click **Save Changes** to add the new profile. The profile appears in the profile list.
- Click **Undo Changes** to cancel the new profile.

**Note**

If you enter an invalid scan range or scan value, an error message appears indicating that the server was unable to process the request.

## Specifying multiple scan ranges

To include or exclude multiple IP addresses or multiple IP ranges, you can enter all the values in the **Scan List Editor** box at one time, rather than entering the values individually in the **Include in Scan** and **Exclude From Scan** boxes (**General** tab).



You can copy and paste a list of scan ranges or IP addresses in a CVS/Excel/Word format directly into the **Scan List Editor** box either before or after DCA activation. Click the **Save** button and the DCA will scan the configured ranges.

<b>Note</b>	The new scan ranges entered in the <b>Scan List Editor</b> box will override any values you had previously entered in the <b>Include in Scan</b> and <b>Exclude From Scan</b> boxes on the <b>General</b> tab.
-------------	--

### Specifying which devices to scan

The PrintFleet DCA only scans the IP addresses and/or PFE Server Hostnames specified in each scan profile. When the PrintFleet DCA is first installed, it selects a default set of IP addresses to scan based on either Active Directory or, if that is not available, the primary network card on the system installed with the PrintFleet DCA. These IP addresses are automatically added to the Default scan profile.

If the default set of IP addresses captures all the devices on the network that you want to scan, and you do not want multiple scan profiles, you do not have to further specify the devices for the PrintFleet DCA to scan.

### Scan Intervals

The scan interval is the amount of time to wait after the completion of one scan before beginning the next scan. The default scan interval is 60 minutes, and this is appropriate for most customer networks, and for the dealership's purposes. To change the interval, navigate to the **General** tab and enter a new **Scan Interval** value.

### Editing scan profiles

#### Procedure

1. On the **Administration** menu, click **DCAs**.  
The **DCAs** page appears.
2. In the **Group** box, select a DCA group.  
All DCAs associated with this group are listed on the **DCAs** page.
3. In the **DCA** column, select a DCA.  
The **DCA Detail** page appears.
4. Click the **Config** tab.
5. In the **Scan Profile** list, select the profile that you want to edit.



6. Edit the required settings on the **General**, **Security**, **Advanced**, and **Scan List Editor** tabs.
7. Click **Save Changes** to save the modified profile settings.

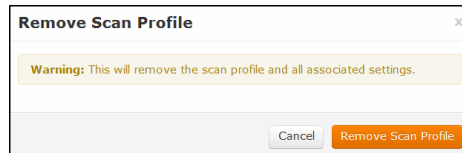
### Deleting scan profiles

#### Procedure:

1. On the **Administration** menu, click **DCAs**.  
The **DCAs** page appears.
2. In the **Group** box, select a DCA group.  
All DCAs associated with this group are listed on the **DCAs** page.
3. In the **DCA** column, select a DCA.  
The **DCA Detail** page appears.
4. Click the **Config** tab.
5. In the **Scan Profile** list, select the profile that you want to delete.



6. Click the **Delete (-)** button.
7. In the **Remove Scan Profile** box, click **Remove Scan Profile**.



8. Click **Save Changes** to delete the profile.

**Warning**

If you delete a scan profile, you will no longer be collecting information from the devices specified in the profile, unless they are included in a different profile.

## Setting network timeouts

The network timeout is the amount of time that the DCA will wait for a networked device to respond back with its information.

The network timeout only needs to be adjusted if the DCA is not discovering networked devices. If, when you perform a DCA scan, certain networked devices are not being discovered, you may need to increase the network timeout (for example, you might try doubling it to 10,000 milliseconds). The higher the network timeout is set, the longer the DCA scan will take.

### Procedure

1. On the **Administration** menu, click **DCAs**.  
The **DCAs** page appears.
2. In the **Group** box, select a DCA group.  
All DCAs associated with this group are listed on the **DCAs** page.
3. In the **DCA** column, select a DCA.  
The **DCA Detail** page appears.
4. Click the **Config** tab.

- In the **Scan Profile** box, select a profile.

A screenshot of a dropdown menu labeled 'Scan Profile' with 'Default' selected.

- Click the **Advanced** tab.

A screenshot of the 'Advanced' tab in the configuration interface. It shows several settings: Network Timeout (5000 ms), SNMP Retries (5), Web Page Scraping Timeout (7500 ms), Focus Scan Interval (0 minutes), Scan Type (Network), and Local Agent Timeout (30000 ms).

- In the **Network Timeout** box, enter the number of milliseconds for the timeout.

A close-up screenshot of the 'Network Timeout' input field, showing the value '5000' and the unit 'ms'.

Default value: 5000 ms

- Click **Save**.

**Note**

The Network Timeout setting only affects how long the DCA will wait for the initial discovery of networked devices. For each printer that has been discovered, the DCA will wait up to 60 seconds to receive complete information from the device.

## Setting SNMP retries

The number of SNMP retries entered in the DCA settings is the number of times the DCA will attempt to get information from a device that is responding with incomplete or no information. Increasing the number of SNMP retries may increase the completeness of a DCA scan, but will also increase the amount of time it takes to complete a network scan.

### Procedure

- On the **Administration** menu, click **DCAs**.  
The **DCAs** page appears.
- In the **Group** box, select a DCA group.  
All DCAs associated with this group are listed on the **DCAs** page.
- In the **DCA** column, select a DCA.  
The **DCA Detail** page appears.
- Click the **Config** tab.
- In the **Scan Profile** box, select a profile.

Scan Profile **Default** ▾

6. Click the **Advanced** tab.

The screenshot shows the 'Advanced' tab of the 'Scan List Editor'. It contains several configuration fields:
 

- Network Timeout:** 5000 ms
- SNMP Retries:** 5
- Web Page Scraping Timeout:** 7500 ms
- Focus Scan Interval:** 0 minutes
- Scan Type:** Network (dropdown menu)
- Local Agent Timeout:** 30000 ms

7. In the **SNMP Retries** box, enter the number of SNMP retries.

SNMP Retries

Default value: 5 minutes

8. Click **Save**.

## Setting Web Page scraping timeouts

The **WebPage Timeout** setting controls how long the DCA waits if any Web page data scraping is done. Increasing the value may increase the completeness of a DCA scan, but will also increase the amount of time it takes to complete a network scan.

### Procedure

1. On the **Administration** menu, click **DCAs**.  
The **DCAs** page appears.
2. In the **Group** box, select a DCA group.  
All DCAs associated with this group are listed on the **DCAs** page.
3. In the **DCA** column, select a DCA.  
The **DCA Detail** page appears.
4. Click the **Config** tab.
5. In the **Scan Profile** box, select a profile.
6. Click the **Advanced** tab.

This is a duplicate of the screenshot in step 6, showing the 'Advanced' tab of the 'Scan List Editor' with the following settings:
 

- Network Timeout:** 5000 ms
- SNMP Retries:** 5
- Web Page Scraping Timeout:** 7500 ms
- Focus Scan Interval:** 0 minutes
- Scan Type:** Network (dropdown menu)
- Local Agent Timeout:** 30000 ms

7. In the **Web Page Scraping Timeout** box, enter the number of milliseconds for the timeout.  
Default value: 7500 milliseconds
8. Click **Save Changes**.

## Setting Focus Scans

DCA will scan each IP address, IP range, and hostname specified in the scan range settings each time the DCA performs a full network scan. Using Focus Scan, you can specify a periodic interval for the DCA to perform a full network scan, and the scans performed between the intervals will scan only printer devices found during the previous full network scan.

Focus Scan decreases the amount of total time and bandwidth that the DCA occupies, particularly on large networks, while ensuring that new or relocated document output devices are discovered on a periodic basis.

### Procedure

1. On the **Administration** menu, click **DCAs**.  
The **DCAs** page appears.
2. In the **Group** box, select a DCA group.  
All DCAs associated with this group are listed on the **DCAs** page.
3. In the **DCA** column, select a DCA.  
The **DCA Detail** page appears.
4. Click the **Config** tab.
5. In the **Scan Profile** box, select a profile.
6. Click the **Advanced** tab.

The screenshot shows the 'Advanced' configuration tab for a DCA. It contains several settings:
 

- Network Timeout:** 5000 ms
- SNMP Retries:** 5
- Web Page Scraping Timeout:** 7500 ms
- Focus Scan Interval:** 0 minutes (highlighted with a red box)
- Scan Type:** Network (dropdown menu)
- Local Agent Timeout:** 30000 ms

7. In the **Focus Scan Interval** box, enter the number of minutes for the interval.

A close-up of the 'Focus scan interval' input field, showing a text box with the number '0' and the unit 'minutes' to its right.

Default value: 0 minutes (scan is disabled)

8. Click **Save**.

## Setting scan types

Administrators must select a scan type for the DCA to collect data.

### Procedure

1. On the **Administration** menu, click **DCAs**.  
The **DCAs** page appears.
2. In the **Group** box, select a DCA group.  
All DCAs associated with this group are listed on the **DCAs** page.
3. In the **DCA** column, select a DCA.  
The **DCA Detail** page appears.
4. Click the **Config** tab.
5. In the **Scan Profile** box, select a profile.
6. Click the **Advanced** tab.

The screenshot shows the 'Scan List Editor' configuration page with the following settings:

- Network Timeout: 5000 ms
- SNMP Retries: 5
- Web Page Scraping Timeout: 7500 ms
- Focus Scan Interval: 0 minutes
- Scan Type: Network (selected in a dropdown menu)
- Local Agent Timeout: 30000 ms

7. In the **Scan Type** box, click **Network** to scan networked DCAs.

The screenshot shows a close-up of the 'Scan Type' dropdown menu with 'Network' selected.

8. Click **Save Changes**.

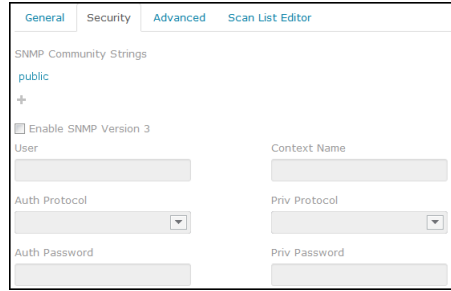
## Storing SNMP community strings

Community strings act as passwords on networked devices that limit access via SNMP. Since the DCA uses SNMP to collect data from devices, any custom community strings on printing devices put in place by network administrators can be manually entered in the DCA to allow it SNMP access to the device. Most devices have a community string of `public`, and the DCA stores a community string of `public` by default.

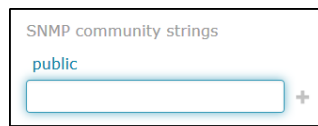
### Procedure

1. On the **Administration** menu, click **DCAs**.  
The **DCAs** page appears.
2. In the **Group** box, select a DCA group.  
All DCAs associated with this group are listed on the **DCAs** page.
3. In the **DCA** column, select a DCA.  
The **DCA Detail** page appears.
4. Click the **Config** tab.
5. In the **Scan Profile** box, select a profile.

6. Click the **Security** tab.



7. In the **SNMP Community Strings** area, do any of following:



- To add a community string, enter an applicable community string in the text box and then click the **Add** (+) button. Repeat as necessary.
- To remove a community string, select a previously entered community string and then click the **Delete** (-) button.

**Note**

Although it is possible to remove the `public` community string, you should only do so if you know that all of the devices you want to monitor are accessible via custom community strings.

If you remove the `public` community string, a **Fix** link will automatically appear below the list to allow you to replace the `public` community string later if necessary.

When the DCA encounters a device using a community string during the network scan, it will attempt to use the first community string listed, then the next, etc., until it is successful or it runs out of community strings to attempt.

8. Click **Save Changes**.

## Using SNMP Version 3

By default, the DCA communicates with devices using SNMP version 1. If you want, you can have the DCA use SNMP version 3 instead when communicating with devices that support SNMP version 3. The primary benefit to using SNMP version 3 is that it supports authentication (ensures that the message is from a valid source) and privacy (encrypts the content of a packet to prevent snooping by an unauthorized source). Conversely, the use of these additional security options typically results in the communication being slower, so it takes longer to scan devices that use SNMP version 3.

SNMP version 3 can be used with three different security levels:

- **NoAuthNoPriv**—This uses neither authentication nor privacy, so in terms of security is the same as just using SNMP version 1.
- **AuthNoPriv**—This uses authentication but not privacy, and is still relatively quick.
- **AuthPriv**—This uses both authentication and privacy. This is the slowest mode, but the only one that offers encryption.

These three levels are reflected in the options available through the PrintFleet Optimizer server user interface.

---

**Note**

Enabling SNMP version 3 in the DCA will have no significant effect on devices that do not support SNMP version 3. When this option is enabled the DCA will first attempt to communicate with each specified IP address using SNMP version 3. For any addresses that do not respond, the DCA will then automatically revert to using the previous SNMP version.

---

**Procedure**

1. On the **Administration** menu, click **DCAs**.  
The **DCAs** page appears.
2. In the **Group** box, select a DCA group.  
All DCAs associated with this group are listed on the **DCAs** page.
3. In the **DCA** column, select a DCA.  
The **DCA Detail** page appears.
4. Click the **Config** tab.
5. In the **Scan Profile** box, select a profile.
6. Click the **Security** tab.
7. Select the **Enable SNMP Version 3** check box.
8. To use authentication, do the following:
  - In the **User** box, enter the name of the user you want to use to authenticate against.
  - Select the authentication protocol you want to use from the **Auth protocol** list.
  - In the **Auth password** box, enter the password for the authentication protocol. Note that each character of your password will be masked by an asterisk (\*) to help ensure security.
9. To use privacy, do the following:
  - Select the privacy protocol you want to use from the **Priv protocol** list.
  - In the **Priv password** box, enter the password for the privacy protocol. Note that each character of your password will be masked by an asterisk (\*) to help ensure security.

10. (Optional) If a Context Name or ID is required, enter the identifier in the **Context name** box.
11. Click **Save Changes**.

<b>Note</b>	An individual scan profile in DCA can only specify one security level, and within that level can only specify one combination of authentication and privacy protocols. If you need to use different security levels, or different combinations of protocols, for the devices you need to scan, you will have to create a separate scan profile for each such combination you require.
-------------	---

## 6.7 DCA Pulse: Managing Scan Configuration

DCA Pulse facilitates quick and easy configuration that allows for more customized scan settings and the collection of more meaningful and valuable data.

### Adding a Scan Range

DCA Pulse acquires the IP range of where the DCA is installed upon activation. If you wish to add a different scan range, follow these steps:

#### Procedure

1. On the **Administration** menu, click **DCAs**.  
The **DCAs** page appears.
2. In the **Group** box, select a DCA group.  
All DCAs associated with this group are listed on the **DCAs** page.
3. In the **DCA** column, select a DCA created for the device.  
The **DCA Detail** page appears.
4. Click the **Config** tab and then click the **Scan List** tab.
5. In the **Scan List Editor** box, you can add a different range and save it. The scan will be then automatically be edited and updated to reflect the new range.

<b>Note</b>	If you want to set multiple IP addresses or multiple IP ranges, you can enter the values in bulk on the <b>Scan List Editor</b> tab.  For more information, see "Specifying multiple scan ranges" on page 153.
-------------	--

### Configuring Scan Intervals

DCA Pulse allows users to set a separate scan interval for Discovery, Meters, Supplies, Errors and Attributes. The ability to customize how often you receive specific types information both simplifies and maximizes the power of Pulse, since you'll be getting the data you

want, when you want it - and only then. This dramatically cuts down on slow interval times.

**Procedure**

1. On the **Administration** menu, click **DCAs**.  
The **DCAs** page appears.
2. In the **Group** box, select a DCA group.  
All DCAs associated with this group are listed on the **DCAs** page.
3. In the **DCA** column, select a DCA created for the device.  
The **DCA Detail** page appears.
4. Click the **Config** tab and then click the **Scan Intervals** tab.

The screenshot shows the 'Scan Intervals' configuration page. At the top, there are five tabs: 'Scan List', 'Scan Intervals' (which is active), 'Security', 'Communication', and 'Log'. Below the tabs, there are four sections, each with a text input field and a unit label:

- Discovery:** Input field contains '30', unit is 'minutes'.
- Errors:** Input field contains '60', unit is 'seconds'.
- Meters:** Input field contains '120', unit is 'minutes'.
- Supplies:** Input field contains '60', unit is 'minutes'.

The scan intervals are set to their respective default settings. To change these settings, type in the time you would like to establish as your customized interval.

<b>Note</b>	The minimum and maximum time for everything except Errors is 10 minutes MIN and 720 minutes MAX. Errors has a MIN of 30 seconds, and a MAX 600 seconds.
-------------	---

**Configuring Security: SNMP Version 1/2**

By default, DCA Pulse communicates with devices using SNMP version 1/2. If you wish to use this security protocol, do the following:

**Procedure**

1. On the **Administration** menu, click **DCAs**.  
The **DCAs** page appears.
2. In the **Group** box, select a DCA group.  
All DCAs associated with this group are listed on the **DCAs** page.
3. In the **DCA** column, select a DCA.  
The **DCA Detail** page appears.
4. Click the **Config** tab.
5. Click the **Security** tab.

6. Click **Add SNMP Profile** button.
7. A pop-up will appear.

SNMP Version

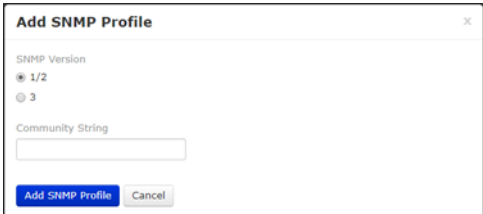
1/2

3

Community Strings

public

Enter one community string per line.



By default, **SNMP Version 1/2** will be selected. Enter **Community Strings** in the text box. Community strings act as passwords on networked devices that limit access via SNMP. Since DCA Pulse uses SNMP to collect data from devices, any custom community strings on printing devices put in place by network administrators can be manually entered in the DCA to allow it SNMP access to the device. Most devices have a community string of `public`, and the DCA stores a community string of `public` by default.

## Configuring Security: SNMP Version 3

If you want, you can have DCA Pulse use SNMP version 3 instead when communicating with devices that support SNMP version 3. The primary benefit to using SNMP version 3 is that it supports authentication (ensures that the message is from a valid source) and privacy (encrypts the content of a packet to prevent snooping by an unauthorized source). Conversely, the use of these additional security options typically results in the communication being slower, so it takes longer to scan devices that use SNMP version 3.

However, since DCA Pulse communicates with HTTPS rather than HTTP, you can expect this update to help expedite communication, while also providing an added layer of security.

SNMP version 3 can be used with three different security levels:

- **NoAuthNoPriv** – this uses neither authentication nor privacy, so in terms of security is the same as just using SNMP version 1.
- **AuthNoPriv** – this uses authentication but not privacy, and is still relatively quick.
- **AuthPriv** – this uses both authentication and privacy. This is the slowest mode, but the only one that offers encryption.

These three levels are reflected in the options available through the PrintFleet Optimizer server user interface.

**Note**

Enabling SNMP version 3 in the DCA will have no significant effect on devices that do not support SNMP version 3. When this option is enabled the DCA will first attempt to communicate with each specified IP address using SNMP version 3. For any addresses that do not respond, the DCA will then automatically revert to using the previous SNMP version.

**Procedure**

1. On the **Administration** menu, click **DCAs**.  
The **DCAs** page appears.
2. In the **Group** box, select a DCA group.  
All DCAs associated with this group are listed on the **DCAs** page.
3. In the **DCA** column, select a DCA.  
The **DCA Detail** page appears.
4. Click the **Config** tab.
5. Click the **Security** tab.
6. The default setting is **SNMP Version 1/2**. If you wish to select SNMP Version 3, click **Add SNMP Profile**.
7. A pop-up screen will appear with default SNMP 1/2 selected. Select 3.

---

### Add SNMP Profile

---

SNMP Version

1/2

3

Context Name

User

Security Level

Add SNMP Profile

Cancel

8. To complete set up, do the following:
  - In the **User** box, enter the name of the user you want to use to authenticate against.
  - Select the authentication and privacy protocol you want to use from the **Security Level** list.

- If a Context Name or ID is required, enter the identifier in the **Context name** box.

Click **Save Changes**.

## View Security Configuration Details

To view the details of a SNMP profile, do the following:

### Procedure

- On the **Administration** menu, click **DCAs**.  
The **DCAs** page appears.
- In the **Group** box, select a DCA group.  
All DCAs associated with this group are listed on the **DCAs** page.
- In the **DCA** column, select a DCA.  
The **DCA Detail** page appears.
- Click the **Config** tab.
- Click the **Security** tab.
- Click the table icon.
- A pop-up screen will appear with the relevant SNMP details.

## Delete a SNMP Profile

To delete a SNMP profile, do the following:

### Procedure

- On the **Administration** menu, click **DCAs**.  
The **DCAs** page appears.
- In the **Group** box, select a DCA group.  
All DCAs associated with this group are listed on the **DCAs** page.
- In the **DCA** column, select a DCA.  
The **DCA Detail** page appears.
- Click the **Config** tab.
- Click the **Security** tab.
- Click on the "x" button beside the profile you wish to remove to delete.

## Configuring Communication

Configuring communication settings allows you to control the frequency with which your DCA communications with devices. This can vary widely depending on the nature of your client's network and the unique demands of their business.

DCA Pulse allows you to configure all your communication settings in one place, thereby streamlining and simplifying the process.

### Procedure

1. On the **Administration** menu, click **DCAs**.  
The **DCAs** page appears.
2. In the **Group** box, select a DCA group.  
All DCAs associated with this group are listed on the **DCAs** page.
3. In the **DCA** column, select a DCA created for the device.  
The **DCA Detail** page appears.  
Click the **Config** tab and then click the **Communication** tab.

[Scan List](#)   [Scan Intervals](#)   [Security](#)   **Communication**   [Log](#)

If a setting is empty, the DCA client will use the value from the config file or the default value.

<p>SNMP Retries <input type="text" value="2"/></p> <p>SNMP Timeout <input type="text" value="10000"/> ms</p> <p>DNS Timeout <input type="text" value="10000"/> ms</p> <p>Disconnected Device Grace Period <input type="text" value="60000"/> ms</p>	<p>SNMP Max Concurrent <input type="text" value="100"/></p> <p>SNMP Max Per Target <input type="text" value="1"/></p> <p>Registry Interval <input type="text" value="30"/> minutes</p>
---	--

**Note**

Each option is automatically set to its default setting. (As seen in previous image.) Your ability to alter settings is confined to the **maximum** and **minimum** limits outlined below:

- SNMP Retries: MAX 10 times, MIN 0 times
- SNMP Timeout: MAX 300,000 milliseconds, MIN 500 milliseconds
- SNMP Max Concurrent: MAX 1000 requests, MIN 5 requests
- DNS Timeout: MAX 300,000 milliseconds, MIN 500 milliseconds
- Disconnected Device Grace Period: MAX 300,000 milliseconds, MIN 10,000 milliseconds
- SNMP Max Per Target: MAX 10 requests, MIN 1 request
- Registry Interval: MAX 90 minutes, MIN 3 minutes

**SNMP Retries.** The number of SNMP retries entered is the number of times DCA Pulse will attempt to get information from a device that is responding with incomplete or no information. Increasing the number of SNMP retries may increase the completeness of a DCA

scan, but will also increase the amount of time it takes to complete a network scan. Each option is automatically set to its default.

**SNMP Timeout.** The SNMP timeout is the amount of time that DCA Pulse will wait for a networked device to respond back with its information.

The network timeout only needs to be adjusted if the DCA is not discovering networked devices. If, when you perform a DCA scan, certain networked devices are not being discovered, you may need to increase the network timeout (for example, you might try doubling it to 10,000 milliseconds). The higher the network timeout is set, the longer the DCA scan will take.

**DNS Timeout.** The Pulse client, on the customer’s network, communicates with DCA Registry using DNS requests. This setting controls how long the request is expected to wait for a response from the Registry server before the request times out and fails. This setting is set in milliseconds.

**Disconnect Device Grace Period.** Devices can go off-line for several reasons (small blip in the network, the device is unplugged periodically, etc). This setting controls how long Pulse will remember the device before it is considered to be disconnected. Once a device is disconnected, Pulse will stop scanning it.

**SNMP Max Concurrent.** This setting controls the total amount of SNMP requests that Pulse will send out simultaneously, across all devices.

**SNMP Max Per Target.** This controls the amount of simultaneous SNMP requests that may be sent to a single device.

**Registry Interval.** The Registry Interval is the amount of time that Pulse will wait between checking in with a network to determine if it is still live, even if there are no updates.

## Configuring Logs

By default, DCA Pulse logs Info, Warnings, Errors, and Fatal. These types of logs are available upon a fresh install with no configuration changes made yet.

Default Log Name	Meaning
<b>Fatal</b>	Used for fatal errors when the application can no longer continue at all. Typically, this means the application is exiting (or the ASP.NET Request is ending) prematurely or unexpectedly. To fix a Fatal error, restart the application.

**(continued)**

Default Log Name	Meaning
<b>Error</b>	These are recoverable (non-Fatal) errors that are visible to an administrator. Typically, entries classified as Error are actionable by a user or an operator in some way.
<b>Warning</b>	Warnings are potential problems and non-actionable errors that don't necessarily require an administrator to act on them. For example, a problem parsing data passed to a web service could cause a Warning log. There isn't anything an administrator can or should do, but it may cause an issue, so it is flagged as a Warning, as opposed to just Info.
<b>Info</b>	Info is for basic informational coarse-grained messages about what the system is doing, and no messages should require the operator to act. Info is typically the default log level (so only Info or higher will normally be logged).

In addition to these default logs, DCA Pulse offers more advanced logging capabilities than previous DCA versions, giving users the ability to more accurately record, monitor, control and troubleshoot activity within the system.

Here are the new DCA Pulse configuration log options:

Log Name	Purpose
<p><b>Debug</b></p>	<p>Debug logging expands on information provided in an Info log. For example, when processing items in a file, there may be a single Info message that says the file is being processed, a Debug message that lists the file timestamp and permissions, a Debug message for every item in the file, and a Debug message when the file has been closed.</p> <p>This application is usually only utilized by a developer debugging an application or an advanced user trying to troubleshoot a difficult problem.</p>
<p><b>Trace Logging</b></p>	<p>Trace is the highest detail of logging messages. It may include an entry whenever any function in the code is entered or exited, and otherwise expand on the level of detail provided by Debug. It may be wired to System.Diagnostics.Trace (so it receives messages from the framework trace levels aswell).</p> <p>Often, Trace will generate an order of magnitude or more log output than even Debug, so should only be enabled by a developer while necessary and turned off afterwards. It's not unusual for Trace to generate several GB of log files in a day.</p>
<p><b>SNMP Log Level</b></p>	<p>SNMP logging will log activities that are directly associated with SNMP (requests, responses, etc). When SNMP logging is enabled, it will be stored in a new file with an snmp.log suffix.</p>

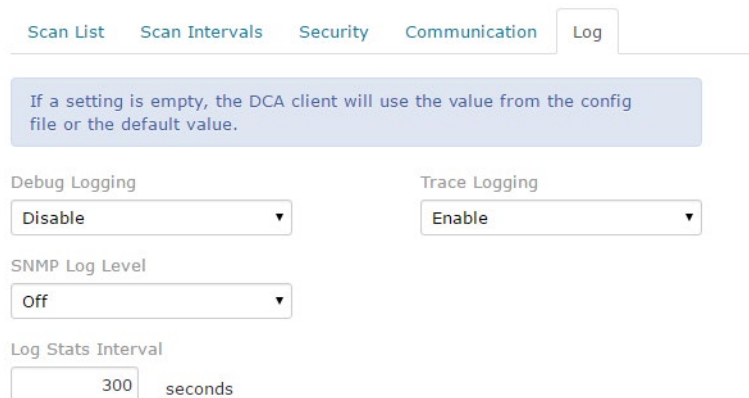
(continued)

Log Name	Purpose
<b>Log Stats Intervals</b>	<p>There are Info logs that contain stats that clearly contain information regarding how many data values are being monitored across the number of devices, how many devices are potentially lacking scan instructions, etc. <b>Log Stats Interval</b> determines how frequently these "stats" are logged inside the log file.</p> <p><b>Note:</b> the MIN time for this option is 0 seconds, and the MAX is 3200 seconds.</p>

To configuring your Log options, do the following:

**Procedure**

1. On the **Administration** menu, click **DCAs**.  
The **DCAs** page appears.
2. In the **Group** box, select a DCA group.  
All DCAs associated with this group are listed on the **DCAs** page.
3. In the **DCA** column, select a DCA.  
The **DCA Detail** page appears.
4. Click the **Config** tab.
5. Click the **Log** tab.



The log options are set to their default settings. To change the **Debug, Trace or SNMP Logging** settings, click on the drop-down menu and select an option.

To adjust **Log Stats Interval**, either manually type in the desired interval time, or hover your mouse over the space after the text box and the up-down arrows will appear.

**Note**

The **Debug Logging** and **Trace Logging** settings in PrintFleet Optimizer may disable each respective level of logging, with one caveat: when Trace is enabled, Debug will also be enabled, because Trace provides the highest detail of logging available.

## 6.8 Understanding PrintFleet Security

The functionality available to a given user is determined by what permissions that user has. The permissions are determined by the groups and roles to which that user belongs.

### Basic group/ role assignment

Suppose a user named Henry is assigned to a group called HQ, and within the HQ group Henry is assigned the Default role. Assuming the Default role has not been modified, Henry can view the devices assigned to the HQ group, and the report definitions that have been shared with the HQ group. Henry would also be able to run and schedule report definitions shared with the HQ group.

Although Henry was specifically assigned to the HQ group, he may also be able to access devices and reports in other groups depending on where those groups sit in the group hierarchy relative to the HQ group to which he was assigned.

### Group inheritance

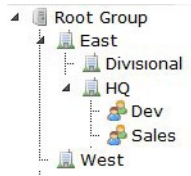
When PrintFleet Optimizer is first installed it has just one group. This first group is typically called the root group. You will usually go on to add other groups to reflect the structure of your organization. The first group you add is always added below the root group. This reflects two important points:

- There can only ever be one root group.
- The root group is always above all other groups.

The concept of one group being considered above or below another group is a critical one to understand because it is used to determine what permissions users have in the various levels of the group hierarchy. The 'higher' a group, the more powerful it is; users in a higher group automatically inherit permissions in lower groups. Specifically:

- The roles (and by extension the permissions) that a user has in each group will also apply to any groups below that group.

For example, suppose you have set up your groups like this:



If Henry is assigned to the HQ group as a user having the Default role, he will also be considered to have the Default role in the groups below the HQ group: Dev and Sales. If a device was assigned to the Dev group, Henry would be able to see that device. Similarly, a user who is assigned to the Root Group would be able to see the devices in that group as well as in any groups below that group (effectively all groups in the system).

The inheritance of permissions from group to group only applies in a downward direction. Henry would not be able to see devices from groups above the HQ group (such as East), or even from groups at the same level as the HQ group (such as Divisional). For more information, see "Managing Groups" on page 97.

## Role inheritance

Some functionality is restricted based on the role itself rather than on the specific permissions associated with that role. For example, when a user creates a report definition and wants to share it with other users, in addition to specifying what group they want to share the report definition with they can also specify what role(s) they want to share it with; if a user in the specified group does not also have the specified role, they will not be able to access the shared report definition.

### Default Role

When you create a new user, you specify what group to assign them to, and then you choose what role to assign them to within the specified group. Every user automatically has the **Default** role selected (it is not possible to remove the selection). Regardless of what other roles might be selected for a new user (such as **Dealer**), she will also have the **Default** role.

## Reports security

When a user creates a report definition, they have the option of either keeping the report definition private or sharing it with a group (or, if they want, with a specific role within the group).

Report schedules also have an inherent security associated with them. Specifically, a user can see the report schedules of another user if they have been assigned to all the same group/role combinations as that other user. For more information, see "Report Security" on page 72.

## Alerts security

When a user creates an alert definition they can set restrictions on which group's users can edit the definition, and which users can see the alert events associated with the definition. For more information, see "Alerts Security" on page 76.

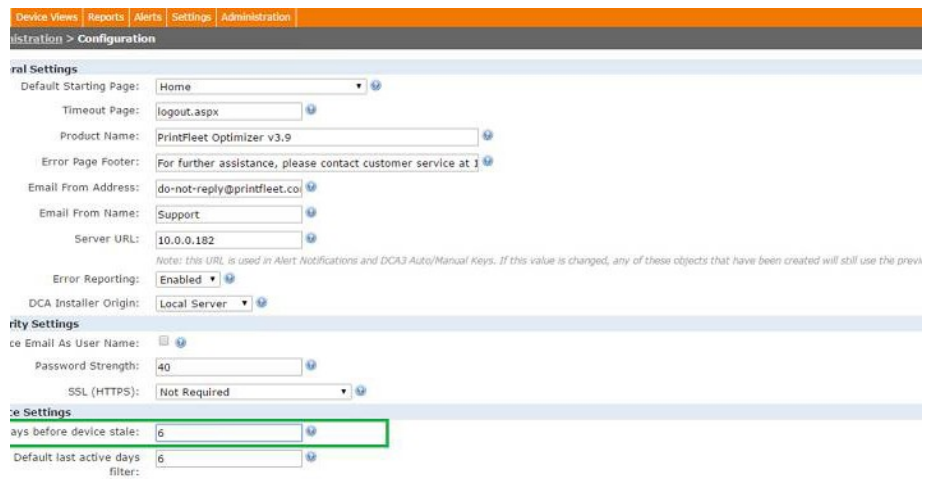
## 6.9 Troubleshooting Stale Data Issues

Devices will appear as stale if the DCA has not been able to collect data from the device for a period of 24 hours.

Root Administrators can configure this period by following these steps:

### Procedure

1. Go to Administration.
2. Select the Configuration option.
3. Enter your desired time in the **Days before device stale** text box.



If customers are showing stale devices without an obvious explanation, the customer should be contacted to determine the reason. A device may appear as stale for many reasons, including:

- The device has been removed from the network
- The device is turned off
- The transmission port on the network is closed (all devices display as stale)
- The computer installed with the DCA is turned off (all devices display as stale)

## 6.10 Providing Technical Support

The following best practices are recommended for providing technical support to your PrintFleet customers:

**Notes**

All issues should be tracked with a custom or commercially available CRM (Customer Relationship Management) software solution.

- Track all incoming calls and emails. Specifically, record the caller's name, phone number, company, the reason for the call, if there was a resolution to their situation, and what the resolution was or what the next step is.
- Use email as a support tool, since it automatically records all the details in writing.
- Ensure that callers phoning support, as much as possible, do not have to wait longer than five rings to get a technical person on the line.
- Try to deliver resolutions to routine problems within 30 minutes of the support call. There should be a plan in place that specifies levels of problems and their expected response times.
- Make self-help materials available to your customers to minimize the need for telephone and email support.
- Review support call records on a weekly basis to flag any recurring issues that might be preventable by changing the installation or initial training process.
- Monitor new customers and installations closely for the first two weeks while they are getting started with the software.
- Consider providing 24-hour support using mobile devices.

## 6.11 Distributing Software Updates

It is the responsibility of the PrintFleet administrator to distribute software updates to their clients as they see fit. Updates at the client location would primarily be for the DCA. Updates for the DCA can be distributed to remote installations from your central server.