

PrintFleet Optimizer

User Guide



PRINTFLEET™

As of June 25, 2010.

© 2010 PrintFleet Inc. All rights reserved.

© Copyright 2010 PrintFleet™ Inc. All rights reserved.

PrintFleet Optimizer User Guide.

The content of this user manual is furnished 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 Optimizer, PrintFleet Suite PRO, and PrintFleet Local Beacon are trademarks of PrintFleet Inc.

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

Compass Sales Solutions is a trademark or registered trademark of Compass Sales Solutions.

DocuAudit and Proposal Wizard are trademarks or registered trademarks of DocuAudit International Inc.

TCO Optimizer is a trademark or registered trademark of Kyocera Corporation.

XOPA is a trademark or registered trademark of Xerox Corporation.

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.

Contact PrintFleet:

PrintFleet Inc., 275 Ontario Street, Suite 301, Kingston, Ontario K7K 2X5, CANADA

Toll free: 1-866-382-8320 Telephone: 1 (613) 549-3221 Fax: 1 (613) 549-3222

www.printfleet.com

Table of Contents

Chapter 1	Introduction	1
1.1	Device support	1
1.2	Installation requirements	2
1.3	Obtaining software updates	2
1.4	Contacting Technical Support	3
Chapter 2	Using the Printer Data Collector Agent.	4
2.1	Obtaining the DCA software	5
2.2	Installing and activating the DCA	5
2.3	Managing the DCA service	8
	Installing and starting the DCA service	8
	Setting up the DCA as a scheduled task.	8
2.4	Configuring communication settings	9
	Changing and testing the communication method and port	9
	Using proxy settings	10
	Changing the web service timeout	10
	Enabling Intelligent Update	10
	Enabling a Service Bridge	11
	Troubleshooting DCA communication problems.	12
2.5	Configuring network scan settings.	13
	Managing scan profiles	13
	Specifying which devices to scan	14
	Enabling scanning of network and/or local devices	16
	Enabling broadcast scanning	17
	Enabling Rapid Scan	17
	Setting the scan and transmission interval.	17
	Setting the network timeout.	18
	Setting the Local Print Agent timeout	18
	Setting the number of SNMP retries	18
	Using Focus Scans	19

Storing SNMP community strings	19
Masking private data	20
Enabling SNMP traps	20
Disabling real time DCA status	21
2.6 Managing local devices with Local Print Agent	21
2.7 Viewing queue, archive, and log files.	23
Deleting old archive and log files	24
2.8 Configuring language and read/write settings.	24
2.9 Updating the DCA software	25
2.10 Understanding the network load associated with the DCA	26
Chapter 3 Using PrintFleet Optimizer	27
3.1 Working with the interface	27
Logging in to the system	28
Using the search function	29
Changing your preferences	29
3.2 Working with device views	30
Filtering and sorting data	31
Viewing new devices	32
Working with the traffic light system	32
Working with the default views.	33
Using the Technical View	33
Using the Supplies Order View	34
Using the Maps View	36
Using the Alerts View	37
3.3 Working with the Device Detail view	38
Viewing embedded web pages	40
Viewing historical LCD and error information	40
Working with the Supplies tab	40
Working with the Meters tab	41
Working with the Service tab	42
Working with the Miscellaneous tab	42
Working with the Model tab	43
3.4 Using reports	44
Generating reports	44
Scheduling reports	47
3.5 Using alerts	49
Creating new alerts.	49
Editing alerts	51

	Deleting alerts	51
	Managing alert layouts	51
	Working with alert emails	53
3.6	Using flags.	54
	Creating flags.	54
	Closing flags	55
	Editing flags	55
3.7	Tracking device service history.	55
3.8	Virtual Meters.	57

Chapter 1 Introduction

Welcome to PrintFleet Optimizer—a remote print management system designed to help you control and streamline your printing processes in order to maximize uptime and budget for cost.

This guide is designed to assist you with the following:

- Using the Printer Data Collector Agent
- Using PrintFleet Optimizer

This chapter discusses:

- Device support
- Installation requirements
- Obtaining software updates
- Contacting Technical Support

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. Stand alone devices are not supported. Locally connected devices can be partially supported by using the PrintFleet Local Print Agent add-on application.

Table 1 lists the data types that the Printer Data Collector Agent (DCA) attempts to collect from networked imaging devices during a network scan.

Table 1: Types of data collected by the Printer DCA

IP address	toner cartridge serial number
device description	maintenance kit levels
serial number	non-toner supply levels
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

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

1.2 Installation requirements

Installation requirements for the DCA are listed in “Data Collector Agent Checklist and Installation Requirements” on page 60.

All PFE Enterprise server components are installed by PrintFleet Technical support.

1.3 Obtaining software updates

New software releases are available on a periodic basis.

To update the DCA software, see “Updating the DCA software” on page 25.

Contact your PrintFleet distributor for information on obtaining software updates, or to provide suggestions for software enhancements.

1.4 Contacting Technical Support

For technical support, contact your PrintFleet distributor.

Chapter 2 **Using the Printer Data Collector Agent**

The Printer Data Collector Agent (DCA) is a software application that collects information from supported printers, copiers, fax machines, and multifunction peripherals on a network, and transmits the data back to a PrintFleet Enterprise server.

Data from locally connected devices can also be collected, provided that the Local Print Agent application is installed on each computer connected to a local printer.

For more detailed information on device support, and for a list of data types that are collected, see "Device support" on page 1.

This chapter discusses:

- Obtaining the DCA software
- Managing the DCA service
- Configuring communication settings
- Configuring network scan settings
- Managing local devices with Local Print Agent
- Viewing queue, archive, and log files
- Configuring language and read/write settings
- Updating the DCA software
- Understanding the network load associated with the DCA

Note

If you have also purchased PrintFleet Suite Pro, you will have helpful built-in features for configuring and optimizing your DCA settings (consult the *PrintFleet Suite Pro User Guide* for further details):

- Use PrintFleet Auditor to perform network scans with various settings until you are happy with the scan performance and results—these settings can then be replicated in the DCA.
- Use PrintFleet Asset Tracker to embed missing data to the non-volatile memory of imaging devices, including serial number, asset number, location, and department.

2.1 Obtaining the DCA software

You can obtain the DCA installation file from your distributor. The distributor chooses their own method of distributing the file, such as: email, CD, or USB key.

2.2 Installing and activating the DCA

The DCA should be installed on an existing networked server to collect and transmit device data. If no server is available, the DCA can be installed on a single networked computer that will remain powered on 24 hours a day, 7 days a week.

For DCA installation requirements, see “Data Collector Agent Checklist and Installation Requirements” on page 60.

Prior to installing the DCA, you should obtain the information in the following table from the network administrator at the location. This will allow you to properly configure the DCA.

Table 2: Information to Gather from the Network Administrator Prior to a DCA Installation

Find out...	Solution
if there are local devices you want to monitor.	Once the DCA is installed, you will have to enable local data collection and install Local Print Agent on applicable computers. See "Managing local devices with Local Print Agent" on page 21.
how many total printing devices reside on the network and how large the network is.	An additional DCA should be installed on a separate computer for each 10,000 imaging devices on the network or 100,000 IP addresses.
if the network uses multiple subnets.	If so, take note of the subnets and IP ranges to ensure they are all included in the network scan range.
if the network uses a Virtual Private Network (VPN) or has Wide Area Network (WAN) links.	If so, the network timeout for the DCA should be increased to 500–1000 milliseconds.
if the company has multiple offices they want monitored.	If so, a single DCA may be used if the networks are connected via a VPN, however, it is recommended that a DCA is installed at each location.

The DCA has an easy to use installation wizard that in many cases will configure the settings you need to collect data from networked printing devices. To collect data from local devices, and to further configure settings, you will need to open the DCA application after installation.

To install and activate the DCA:

1. Double-click the filename `Printer DCA 4.x.x.x.msi` installation file.
2. The Printer DCA Installation Wizard is launched. Click **Next** to continue.
3. Read through the End-User License Agreement, check **I accept the terms in the License Agreement** and select **Next** to continue. If you do not accept the terms, the installation process will not continue.

4. In the Destination Folder screen, either leave the default folder displayed, or enter a new destination folder. Click **Next** to continue.
5. In the Ready to Install Printer DCA screen, click **Install** to begin installation or click **Cancel** to exit.
6. In the Completed the Printer DCA Installation Wizard, leave checked or uncheck **Launch Printer DCA after installation** and select **Finish**.
7. After the Printer DCA is launched, in the second End-User License Agreement, select **Accept** to continue or select **Decline** to not continue.
8. In the Welcome to the Printer DCA-Setup Wizard, select the language from the drop down list and select **Next**.
9. In the Printer DCA Activation screen, enter the following:
 - Enter the server information for the server that the DCA will be sending information to in the **Server** box.
 - Enter the PIN code in the **PIN Code** box.
 - Optionally, if the location is using a proxy server that you want to configure at this point (you will also be able to do so after installation), click **Show Proxy Configuration**. See "Using proxy settings" on page 10.
 - Click **Next**.

Note

You can continue past this step without entering a PIN code, but data will not be transmitted to the server until activation is complete.

10. In the Scan Settings screen, you will be shown a list of preconfigured IP ranges that will be added to your default DCA network scan. This can be changed after installation is complete if necessary. Click **Next**.
11. In the Intelligent Updates screen, you will be given the option to disable Intelligent Updates. It is recommended that **Allow Intelligent Updates** remains selected unless there is a strong reason to turn it off. Click **Next**. See "Enabling Intelligent Update" on page 10.
12. In the Setup is Complete screen, by default, the **Open the Data Collector Agent Interface** and **Start the Data Collector Agent Service** are both selected. Optionally, you can turn off one or both of these options. Click **Finish**.

At some point over the life of the DCA installation, you may need to reactivate it, for example, if you were given an activation code with an expiry date, or if you need to redirect the DCA to a new server. You can enter a new activation code from an existing DCA installation.

To reactivate the DCA:

1. On the **Tools** menu, click **Reactivate DCA**.

2. If you are redirecting the DCA to a new server and/or port, enter the new information in the **Server** box.
3. Enter the new activation code in the **PIN Code** box.
4. Click **Activate**.

2.3 Managing the DCA service

The DCA runs as a Windows service by default. Alternatively, the DCA can be set up as scheduled task.

Installing and starting the DCA service

The DCA service can be installed, uninstalled, started, or stopped at any time. You may need to reinstall the DCA service if you have previously been running the DCA as a scheduled task, or if the DCA service was uninstalled for any other reason. If you have been running the DCA as a scheduled task, delete the scheduled task before reinstalling the DCA service.

To install, uninstall, start, or stop the DCA service:

- Under the **Status** tab of the DCA, in the **Service** area, beside **DCA Status**, click the **Options** button, and select the operation you want to perform.

Setting up the DCA as a scheduled task

To set up the DCA as a scheduled task instead of a service, you must first uninstall the DCA service, and then create the DCA scheduled task.

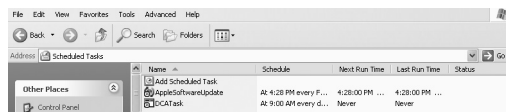
To uninstall the DCA service:

1. For DCA 3.x, on the File menu of the DCA, click **Advanced Options**.
2. In the **Service Control (Main)** area, click **Uninstall**.
3. Click **Save and Close**.
4. For DCA 4.x, in the **Status** tab, click **Options** and select **Uninstall**.
5. Click **Save and Close**.

To create a scheduled task for the DCA:

1. Click **Start**, click **Control Panel**, and then double-click **Scheduled Tasks**.
2. On the **File** menu, point to **New**, and then click **Scheduled Task**.

3. Replace **New Task** with a recognizable name for the task, such as **DCATask**, and click anywhere away from the new task icon to save the name.



4. Double-click your newly created task.
5. In the **Task** tab, type the following in the **Run** box, including the quotations:
`"C:\Program Files\Printer DCA\PrinterDCA.Service.exe"`
 commandline
6. Click the **Schedule** tab.
7. In the **Schedule Task** list, select an interval that you want the task to run.
8. In the **Start Time** box, type or select the time of day that you want the task to run.
9. Click **Apply**.
10. Type in your network login name in the **Run as** box.
11. Type in your network password in the **Password** box, and repeat in the **Confirm Password** box.
12. Click **OK**.

2.4 Configuring communication settings

During the DCA installation, the DCA will attempt to establish basic communication with the central server using either HTTPS (default) or HTTP (secondary). Proxy settings can also be configured during installation, or at any time afterwards. If communication with the server is successful during installation, it is not necessary to change the communication method, port, or proxy settings.

Changing and testing the communication method and port

There are two methods the DCA can use to send information to the central server: HTTPS and HTTP. During installation, the DCA will attempt to establish communication with the central server, first, with HTTPS (port 443), and if that fails, HTTP (port 80). If you don't use the default port for your chosen method of communication, you will need to change this in the DCA. You can change the communication method and port at any time.

To change the DCA communication method and port:

1. Under the **Communication** tab of the DCA, in the **Communication Method** area, type in the protocol, followed by the hostname.
2. Optional--only if you use a non-standard port--enter the port number after a colon after a hostname. For example, `printfleet.com:84`.

3. Click the **Test** button to verify that communication can be established with the central server. You will receive either a success or failure message.
4. Click **Save** to retain changes.

If you are having problems obtaining successful communication between the DCA and the central server, see "Troubleshooting DCA communication problems" on page 12.

Using proxy settings

If a network being scanned with a DCA uses a proxy server, you can configure the DCA to use the proxy settings, which will allow the DCA to scan the network.

To use a manual proxy configuration:

1. Under the **Communication** tab of the DCA, in the **Proxy Configuration** area, click to select one of the following: **Use Windows proxy settings** (no other configuration required), **Use custom proxy settings**, or **None** (to disable proxy settings).
2. If you have selected **Use custom proxy settings**, enter the server and port information in the **Server** and **Port** boxes, respectively.
3. If the proxy server requires authentication, click to select the **Authentication** check box, and then do one of the following:
 - Click to select **Default** to use the authentication currently being used on the computer installed with the DCA.
 - Click to select **Custom**, and then enter username, password, and domain information in the **Username**, **Password**, and **Domain** boxes, respectively, or click **Load Current** to populate the fields with the current authentication being used by the computer installed with the DCA.
4. In the **Communication Method** area, click **Test** to verify the settings are working.
5. Click **Save**.

Changing the web service timeout

The web service timeout determines the maximum time that will be allowed for communication between the DCA and the central server. By default, the web service timeout is 30 seconds; if necessary, the timeout can be increased or decreased at any time.

To change the web service timeout:

1. Under the **Communication** tab, in the **Communication Settings** area, enter or select the desired timeout in the **Web Service Timeout** box.
2. Click **Save**.

The Web Service Discovery Timeout controls the initial connection to the server and the auto-selection of http/https.

Enabling Intelligent Update

When Intelligent Update is enabled, the DCA can be remotely updated by your PrintFleet administrator. This is important to

ensure you are always able to collect the highest quantity and quality of information available.

To enable Intelligent Update:

1. Under the **Communication** tab, in the **Communication Settings** area, click to select the **Enable Intelligent Update** check box.
2. Click **Save**.

Enabling a Service Bridge

A Service Bridge allows a service technician to create a private, secure connection between a service technician and a specific networked printing device, with the DCA acting as a proxy. Once the bridge is established, the service technician can use a special (private) IP address to directly access the device as if they were on site. The technician can view the embedded web page of the device, perform an SNMP scan, update firmware, etc.

For additional security, an access code must be generated from the central server. This code must then be entered into the applicable DCA.

On the service technician's computer:

1. The PrintFleet Optimizer (PFO) user selects a Device to connect to (the Target Device) and goes to its Details page.
2. The PFO user clicks Device's IP Address shown on the page and selects **Service Bridge** option. The **Service Bridge** option is available for network devices only.
3. If the browser does not support the Click Once feature, download the PrintFleet Service Bridge Client's zip file from <http://PFE Server URL/Downloads/ServiceBridge Client x.x.x.xxxxx.zip>. Extract the zip and run the application. For browsers that do support the Click Once feature, you are prompted to run the PrintFleet.PFE.ServiceBridge.Client application (if not installed).
4. When the PFE URL is displayed, the PFO user can make changes to values or accept default and select OK.
5. The PrintFleet DCA Service Bridge dialog is displayed. If prompted to Download Driver, download the TAP driver and install. When the VPN Connection states Success, a PIN will be generated.
6. Leave this VPN Connection dialog open for the duration. The service technician gives this PIN to the DCA user for their use.

To enable a Service Bridge from the DCA:

1. Do one of the following:
 - On the **Tools** menu, click **Start Service Bridge**.
 - Under the **Communication** tab, in the **Service Bridge** area, click **Start**.
2. In the **Enter Service Bridge PIN** box, enter the access code generated on the central server (you will have to obtain this from your dealer) and click **OK**. The **Status** field in the **Service**

Bridge area will indicate when the connection has been established.

3. Enter the Remote IP value into your browser; the device's embedded web page is displayed.

To end the connection:

1. The service technician can close the PrintFleet DCA Service Bridge VPN Connection Success dialog.

**Troubleshooting
DCA
communication
problems**

If you are unable to obtain successful communication between the DCA and the central server after setting the proper communication method and port (see "Changing and testing the communication method and port" on page 9) and configuring proxy settings if necessary (see "Using proxy settings" on page 10), use the following table to troubleshooting potential communication problems.

Table 3: Troubleshooting DCA Communication Problems

Check if...	If not...
the selected send method (HTTP or HTTPS) corresponds with the port you have chosen to transmit data through.	change the send method to correspond with the port number chosen, or change the port number to correspond with the send method chosen.
the port you have selected is open on the network.	have the network administrator open the selected port.
your PrintFleet distributor has a valid SSL security certificate, if you are attempting to send via HTTPS.	contact your distributor to check if they are having problems with their security certificate.
the DCA is successfully collecting data from the internal network by looking in the <code>data_queue</code> or <code>data_archive</code> folder located in the folder where the DCA was installed—if there is data in this folder, the DCA is successfully collecting data.	the problem is not with the send method, but with the collection of data on the internal network.
the destination URL is correct by looking in the Summary area of the Status tab in the DCA.	obtain a new PIN code and reactivate the DCA. See "Installing and activating the DCA" on page 5.
the network is free of firewalls.	there are not usually problems with firewalls, but ask the network administrator if there is a chance this may be the problem.

2.5 Configuring network scan settings

The DCA network scan settings determine how the DCA collects information from the internal network, and provides options for transmitting the information to the central server. Scan profiles can be used to configure multiple types of network scans that will run independently, for example, you might want different scan and transmission settings for networked and local devices.

Network scan settings are independent of communication settings, which specify how the DCA will communicate with the central server, and if and how the central server can communicate with the DCA and/or a specific device on the network (see “Configuring communication settings” on page 9).

Managing scan profiles

You can use profiles to configure multiple types of network scans. For example, you might want to scan networked devices every hour, and local devices once a day—these would be two different scan profiles. You might 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 might have multiple uses for scan profiles, or you might not need more than one. When you first install the DCA, you will have one scan profile called `Default`.

To create a new scan profile:

1. Under the **Scan** tab, beside **Scan Profile**, click **Add**.
2. In the **New Profile** dialog box, enter a name to associate your new profile with, and click **OK**.
3. Configure all settings under the **General**, **Advanced**, and **Local** tabs that apply to the new profile, or copy the settings from another profile.
4. Click **Save**.

To edit an existing scan profile:

1. Under the **Scan** tab, select the profile you want to edit from the **Scan Profile** list.
2. Edit settings as applicable under the **General**, **Advanced**, and **Local** tabs.
3. Click **Save**.

To delete a scan profile:

1. Under the **Scan** tab, select the profile you want to delete from the **Scan Profile** list.
2. Beside **Scan Profile**, click **Delete**.

3. In the **Delete Profile?** dialog box, click **Yes**.

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.

Specifying which devices to scan

The DCA only scans the IP addresses and/or hostnames specified in each scan profile. When the 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 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 DCA to scan. If, however, you want to adjust the devices included in the default scan, or if you have more than one scan profile, you will need to further configure which IP addresses and/or hostnames to include.

Single IP addresses, ranges of IP addresses, and hostnames can all be used to specify devices to include or exclude from a network scan. There are two general purposes for excluding a device or range of IP addresses from a network scan: (1) to specifically not collect information from a device or set of devices; or (2) to remove IP addresses that you know do not have printing devices on them to create the most efficient scan range (shorter network scan time).

Important

It is recommended that the network administrator at the location with DCA installed help set up the DCA scan range.

To add devices to, or exclude devices from, a DCA network scan range:

1. Under the **Scan** tab, make sure the correct scan profile is selected from the **Scan Profile** list. For more information on scan profiles, see "Managing scan profiles" on page 13.
2. Under the **General** tab, in the **Ranges** area, do one or more of the following:
 - To automatically obtain an additional default scan range (from the one specified during DCA installation), click to select **Default Range**, and then select either **Active Directory** or the applicable network card for the system installed with the DCA.
 - To specify a range of IP addresses, click to select **IP Range**, and enter the IP address of the beginning of the range in the left box, and the IP address of the end of the range in the right box.
 - To specify a single IP address, click to select **IP Address** and enter the IP address in the box.

- To specify a hostname, click to select **Hostname** and enter the hostname in the box.
- 3. Click **Add** or **Exclude**.
- 4. Repeat steps 2-3 as necessary.
- 5. Click **Save**.

To remove devices, or device exclusions, from a DCA network scan range:

1. Under the **Scan** tab, make sure the correct scan profile is selected from the **Scan Profile** list. For more information on scan profiles, see "Managing scan profiles" on page 13.
2. Under the **General** tab, in the **Ranges** area, under **Scan List**, do one of the following:
 - To remove one or more individual items from the scan range, click to select the item, and then click **Remove**.
 - To remove every item from the scan range, click **Clear**.
3. Click **Save**.

You can also export and import entire lists of scan ranges. To create a file with scan range settings, save a text file with each specification on a separate line. Use parentheses to indicate scan range exclusions. The following is an example of the contents of a text file ready for import; the example indicates, from top to bottom: an IP range to include, a single IP address to include, a hostname to include, and an IP range to exclude.

```
10.0.0.1-10.0.0.200
10.0.1.10
examplehostname
(10.0.0.10-10.0.0.50)
```

To export current scan range settings to a text file:

1. Under the **Scan** tab, make sure the correct scan profile is selected from the **Scan Profile** list. For more information on scan profiles, see "Managing scan profiles" on page 13.
2. Under the **General** tab, in the **Ranges** area, under **Scan List**, click **Export**.
3. Save the file to the desired location.

To import scan range settings from a text file:

1. Under the **Scan** tab, make sure the correct scan profile is selected from the **Scan Profile** list. For more information on scan profiles, see "Managing scan profiles" on page 13.
2. Under the **General** tab, in the **Ranges** area, under **Scan List**, click **Import**.
3. Select and open a properly formatted text file.
4. Click **Save**.

You can also use PrintFleet Suite Pro (purchased separately) to determine the appropriate scan ranges prior to configuring the DCA.

To determine the optimal IP range settings using PrintFleet Suite Pro:

1. In PrintFleet Auditor, click **Advance Scan**.
2. Do one of the following:
 - If the location has less than 100 users, click **QuickScan**, and then click **Go**.
 - If the location has 100 users or more, click **Custom IP Range** and specify IP ranges given by the network administrator or click **Fill Ranges** to detect IP ranges automatically, and then click **Go**.
3. If the scan takes less than 25 minutes, and all document output devices were found, you can use these settings for the DCA. If the scan takes longer than 25 minutes, analyze the results to determine exactly which ranges need to be scanned. Do not include ranges that have no document output devices on them, and only include the portions of ranges that do have document output devices on them. For instance, if you are scanning a subnet of 192.168.1.1–192.168.1.254, but there are only document output devices from 192.168.1.1–192.168.1.50 and 192.168.1.200–192.168.1.250, you should input these two ranges instead of the entire subnet to make the DCA scan more efficient.
4. Input your tightened scan ranges into the Advance Scan settings of Auditor, and perform another scan to verify that the scan now takes less than 25 minutes. If it still takes longer than 25 minutes, and you cannot tighten the scan ranges any further, you may want to install more than one DCA at the location.

Enabling scanning of network and/or local devices

You must enable at least one of network or local device scanning for the DCA to collect data. For local device scanning to work, you must also have Local Print Agent installed on computers connected to the local devices you want to scan. See “Managing local devices with Local Print Agent” on page 21.

If you have created separate profiles for networked and local devices, you will enable network device scanning in one, and local device scanning in the other. For more information on scan profiles, see “Managing scan profiles” on page 13.

To enable scanning of network and/or local devices:

1. Under the **Scan** tab, make sure the correct scan profile is selected from the **Scan Profile** list. For more information on scan profiles, see “Managing scan profiles” on page 13.
2. Under the **General** tab, in the **Scanning Options** area, do one or both of the following:
 - Click **Network Devices** to enable scanning of networked printing devices.
 - Click **Local Devices** to enable scanning of locally connected printing devices.
3. Click **Save**.

Enabling broadcast scanning

Broadcast scanning targets each IP address specified at the same time, rather than in consecutive order. This makes the DCA network scan faster. Some networks may not allow this type of scanning for security purposes. Typically, this is not needed.

To enable broadcast scanning:

1. Under the **Scan** tab, make sure the correct scan profile is selected from the **Scan Profile** list. For more information on scan profiles, see "Managing scan profiles" on page 13.
2. Under the **General** tab, in the **Scanning Options** area, click **Enable Broadcast**.
3. Click **Save**.

Enabling Rapid Scan

Rapid Scan allows the DCA to use multithreading, which significantly decreases the time it takes for the DCA to complete a network scan.

To enable Rapid Scan:

1. Under the **Scan** tab, make sure the correct scan profile is selected from the **Scan Profile** list. For more information on scan profiles, see "Managing scan profiles" on page 13.
2. Under the **General** tab, in the **Scanning Options** area, click **Enable Rapid Scan**.
3. Click **Save**.

The number of threads can be controlled on the **Advanced** tab. The setting defaults to a reasonable value for the current system.

Setting the scan and transmission interval

The scan interval determines how often the DCA will scan the network and transmit the collected information to your PrintFleet server. The default scan interval is 30 minutes.

It is generally not useful to set a scan interval for more than every 30 or 60 minutes. For example, new information is posted to PrintFleet Optimizer every 10 minutes, but new alerts are generated approximately every 30 minutes.

Note

The scan interval is the time from the end of one scan to the start of the next scan.

To change the scan interval:

1. Under the **Scan** tab, make sure the correct scan profile is selected from the **Scan Profile** list. For more information on scan profiles, see "Managing scan profiles" on page 13.
2. Under the **General** tab, in the **Transmission Options** area, type or select the desired scan interval, in minutes, in the **Scan Interval** box.
3. Click **Save**.

Setting the network timeout

The network timeout is the amount of time that the DCA will wait for a networked device to respond back with its information. The default network timeout is 250 milliseconds.

The network timeout only needs to be adjusted if the DCA is not collecting complete information from networked devices. If, when you perform a DCA scan, certain data fields which should be populated are reporting no information, you may need to increase the network timeout to 500 or 1000 milliseconds. However, the higher the network timeout is set, the longer the DCA scan will take. There may be other reasons that the DCA is not collecting complete information, for example, the device may not store a specific data field (toner levels, etc.).

To change the network timeout:

1. Under the **Scan** tab, make sure the correct scan profile is selected from the **Scan Profile** list. For more information on scan profiles, see "Managing scan profiles" on page 13.
2. Under the **General** tab, in the **Transmission Options** area, type or select the desired network timeout, in milliseconds, in the **Network Timeout** box.
3. Click **Save**.

Setting the Local Print Agent timeout

The Local Print Agent timeout is the amount of time that the DCA will wait for the Local Print Agent application to respond back with information from a locally connected device. The default Local Print Agent timeout is 10,000 milliseconds per system. Local device collection takes substantially longer than networked device collection because of the extra step needed to go through the connected computer via the Local Print Agent application.

The Local Print Agent timeout only needs to be adjusted if the DCA is not collecting complete information from locally connected devices. There may be other reasons that the DCA is not collecting complete information, for example, the device does not store a specific data field (toner levels, etc.), or a Local Print Agent is not installed on the computer connected to the local device. See "Managing local devices with Local Print Agent" on page 21.

To change the Local Print Agent timeout:

1. Under the **Scan** tab, make sure the correct scan profile is selected from the **Scan Profile** list. For more information on scan profiles, see "Managing scan profiles" on page 13.
2. Under the **General** tab, in the **Transmission Options** area, type or select the desired Local Print Agent timeout, in milliseconds, in the **Local Print Agent Timeout** box.
3. Click **Save**.

Setting the number of 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.

To change the number of SNMP retries used:

1. Under the **Scan** tab, make sure the correct scan profile is selected from the **Scan Profile** list. For more information on scan profiles, see "Managing scan profiles" on page 13.
2. Under the **General** tab, in the **Transmission Options** area, type or select the desired number of SNMP retries in the **SNMP Retries** box.
3. Click **Save**.

Using Focus Scans

Without using Focus Scan, the DCA will scan each IP address, IP range, and hostname specified in the scan range settings every 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 devices found during the previous full network scan.

Using Focus Scan can decrease 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.

To enable Focus Scan:

1. Under the **Scan** tab, make sure the correct scan profile is selected from the **Scan Profile** list. For more information on scan profiles, see "Managing scan profiles" on page 13.
2. Under the **Advanced** tab, in the **Focus Scan Options** area, click to select the **Enable Focus Scan** check box.
3. Specify how often you want a full network scan to run by selecting either **Days**, **Hours**, or **Minutes** from the list, and entering a number for the interval beside **Full Discovery Every**. For example, if you enter 5 and select **Days**, a Focus Scan will run once every five days.
4. Click **Save**.

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.

To store community strings in the DCA:

1. Under the **Scan** tab, make sure the correct scan profile is selected from the **Scan Profile** list. For more information on scan profiles, see "Managing scan profiles" on page 13.
2. Do one or more of the following under the **Advanced** tab, in the **SNMP Community Strings** area:

- To add a community string, type an applicable community string in the text box, and click **Add**. Repeat as necessary.
- To remove a community string, click to select a previously entered community string, and then click **Remove**.
- To reorder the list of community strings, click to highlight a community string, and then click either the **Up** or **Down** button. Repeat as 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.

3. Click **Save**.

Masking private data

For privacy reasons, the following types of information that the DCA collects can be masked in the transmission file to the central server:

- IP addresses of devices included in the network scan
- Telephone numbers collected from devices (masked by default)
- DCA host system information (IP address, MAC address, subnet, etc.)

To mask private information in DCA transmission files:

1. Under the **Scan** tab, make sure the correct scan profile is selected from the **Scan Profile** list. For more information on scan profiles, see "Managing scan profiles" on page 13.
2. Under the **Advanced** tab, in the **Privacy Options** area, do one or more of the following:
 - Click to select the **Enable IP Masking** check box to mask device IP addresses.
 - Click to select the **Enable Phone-Number Masking** check box to mask telephone numbers collected from devices (masked by default).
 - Click to select the **Enable DCA Host Info Masking** check box to mask DCA host system information.
3. Click **Save**.

Enabling SNMP traps

SNMP traps are alerts generated by a device that allow information to be sent from a device immediately without having to continuously request information. For example, if a device experiences an error, by enabling SNMP traps, you can be notified of the error immediately instead of waiting until your regularly scheduled DCA scan.

Prior to enabling SNMP traps on the DCA, you need to specify in the internal configuration for each device that SNMP traps should be sent to the IP address of the system installed with the DCA. This only needs to be done for devices that you want to receive SNMP traps from.

After SNMP traps are enabled on the DCA, each SNMP trap received will trigger the DCA to perform a regular data scan on only the

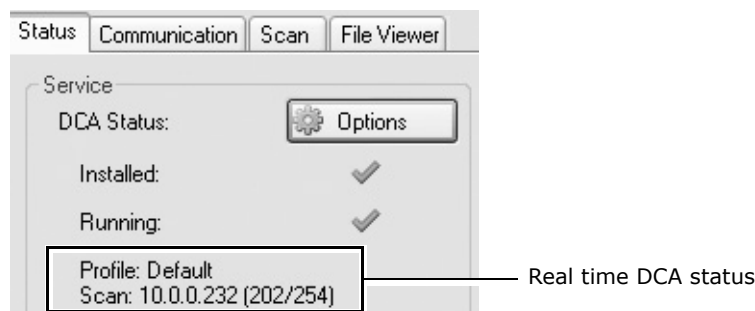
device that sent the SNMP trap. The results from this scan will immediately be sent to the central server.

To enable SNMP traps:

1. Under the **Scan** tab, make sure the correct scan profile is selected from the **Scan Profile** list. For more information on scan profiles, see "Managing scan profiles" on page 13.
2. Under the **Advanced** tab, in the **Miscellaneous** area, click to select the **Enable SNMP Traps** check box.
3. Click **Save**.

Disabling real time DCA status

By default, during a DCA scan, the DCA will display the real time status of the scan under the **Status** tab. This includes the profile name of the current scan, the IP address currently being scanned, the total number of IP addresses in the scan profile, and the number of IP addresses in the current DCA scan that have already been scanned.



You can disable this feature, if necessary.

To disable real time DCA status:

1. Under the **Advanced** tab, in the **Miscellaneous** area, click to disable **Show Realtime DCA Status**.
2. Click **Save**.

2.6 Managing local devices with Local Print Agent

There are three steps that must be taken to collect local printer data using the DCA:

1. Add the IP addresses/ranges of computers connected to local printers to the DCA network scan. See "Specifying which devices to scan" on page 14.
2. Enable the local device scanning option. See "Enabling scanning of network and/or local devices" on page 16.
3. Install Local Print Agent on computers connected to local printers (instructions follow).

Local Print Agent allows the DCA to obtain information directly from locally connected printing devices. The Local Print Agent application

must be installed on each computer connected to a local printer that you want to collect information from. Ideally, Local Print Agent will be installed on all computers at any location where you want to collect local printer information. This will allow you to collect information from new local printers as soon as they are connected.

There are three methods to install Local Print Agent:

- Manual installation from the local printer host computer
- DCA push tool installation (manual and automated)
- Third party push tool installation

In environments that do not allow push installation tools, you may be required to manually install the Local Print Agent application on each computer connected to a local printer.

To install Local Print Agent manually from the local printer host computer:

- Run the `Local Print Agent.msi` file on the computer you want to install Local Print Agent on. The installation file is found by default in: `program files\Printer DCA\Support` folder. The installation file can be copied to a USB drive, CD, etc. for portability.

The DCA has an embedded push install utility specifically for Local Print Agent. In addition, you can schedule periodic push installs to your entire DCA scan range to ensure that Local Print Agent gets installed to any new computers on the network.

To push install Local Print Agent from the DCA:

1. Under the **Scan** tab, make sure the correct scan profile is selected from the **Scan Profile** list. For more information on scan profiles, see "Managing scan profiles" on page 13.
2. On the **Tools** menu, select **Local Agent Management**.
3. Click **Scan All**. This will scan all IP addresses included in the selected scan profile.
4. Under the IP Address column, click to select the check boxes beside each IP address belonging to a computer you want to install Local Print Agent on. Optionally, click **All**, **None**, **Not installed**, or **Installed** to automatically select a set of IPs.
5. If you are not currently logged onto the computer as an administrator, in the **Credentials** area, click **Change**. Enter the local administrator credentials (for the target OS) in the **Username**, **Password**, and **Domain** boxes, and then click **OK**.
6. Click **Install**.

To schedule regular push installs using the DCA:

1. Under the **Scan** tab, make sure the correct scan profile is selected from the **Scan Profile** list. For more information on scan profiles, see "Managing scan profiles" on page 13.
2. Under the **Local** tab, select the **Enable Push Install** check box.

3. In the Change Push Install Credentials screen, enter the credentials of the user that belongs to the local administrator group on the target OS.

Warning

These credentials will be saved in an encrypted format in the DCA. If you do not want these credentials saved, do not enable scheduled push installs.

4. Beside **Start**, select a start date and time for the automated push install.
5. Beside **Repeat**, select the interval you want to perform the push install at.
6. Click **Save**.

If the environment already uses a third party push installation tool, you can use that to push install the `Local Print Agent.msi` file. The installation file can be found in the Printer DCA\support folder on the system installed with the DCA (its default location). Refer to the user guide for the third party push installation tool for further instructions.

2.7 Viewing queue, archive, and log files

For troubleshooting purposes, you might want to view DCA queue, archive, or log files.




Queue and archive files are copies of DCA scan result files; queue files have not yet been transmitted to the central server, while archive files have already been transmitted. The presence of queue files indicates that the DCA is not successfully transmitting information to the central server (unless the DCA is in the process of transmitting the most recent file). Queue and archive files are encrypted in the proprietary `.pfd` format and contain the complete results of a single DCA network scan.

Log files are in `.log` format and are not encrypted. Log files contain summary information for all DCA scans that occurred on a specific date, including scan times, transmission results, DCA application information, intelligent update actions, and the IP addresses and vendors of discovered devices. Log files do not include specific printing device data fields (meters, toner levels, etc.). By default, log files are not sent to the central server, but this can be enabled.

Queue and archive files can only be viewed using the File Viewer included in the DCA. Log files can also be viewed using this, but can also be viewed in any word processing or other application that supports `.log` files.

To locate the correct file, queue and archive file names have date and time stamps as part of the file name, and log files have a date stamp.

To view queue, archive, or log files in the DCA:

- Under the **File Viewer** tab, do one of the following:
 - To open and view a queue file, click the file folder icon () beside **Total files in queue**, and select and open the desired file.
 - To open and view an archive file, click the file folder icon () beside **Total files in archive**, and select and open the desired file.
 - To open and view a log file, click the file folder icon () beside **Open Log file from**, and select and open the desired file, or select a date via the dropdown.

Alternatively, you can drag and drop any of the files into the File Viewer area.

Deleting old archive and log files

By default, the DCA automatically deletes archive and log files after 30 days. If necessary you can adjust the number of days before these files are deleted, or even stop the DCA from deleting the files at all.

To change the period after which the DCA automatically deletes old archive files:

- Under the **File Viewer** tab, use the **Keep archived files for** combo box to specify the maximum number of days you want to retain archived files. Set the value to 0 if you do not want older archive files to be automatically deleted.

To change the period after which the DCA automatically deletes old log files:

- Under the **File Viewer** tab, use the **Keep log files for** combo box to specify the maximum number of days you want to retain log files. Set the value to 0 if you do not want older log files to be automatically deleted.

2.8 Configuring language and read/write settings

The language for the DCA will be automatically selected during installation, based on the default language selected for your Windows operating system.

To change the DCA language settings:

- On the **Options** menu, point to **Language**, and then do one of the following:
 - Click **Windows Default** to toggle using the default language for your Windows operating system.
 - Select the appropriate language from the list.

The DCA has full write permissions enabled at installation, but read-only permissions can be set through use of a password. This will

prevent anyone without the password from changing any of the DCA settings.

To make the DCA read-only:

1. On the **Options** menu, point to **Read-Only Mode**, and then click **Read-Only**.
2. In the **Set Password** dialog box, enter the password you want to use to disable read-only mode, and then click **OK**.

To disable read-only mode:

1. Click **Unlock** in the lower right corner of the DCA.
2. In the **Enter Password** dialog box, enter the password currently set for read-only mode, and then click **OK**.

The password for read-only mode can be changed during read-only mode, provided you have the current password.

To change the read-only mode password:

1. On the **Options** menu, point to **Read-Only Mode**, and then click **Change Password**.
2. In the **Enter Password** dialog box, enter the current password for read-only mode, and then click **OK**.
3. In the **Set Password** dialog box, enter the desired new password for read-only mode, and then click **OK**.

2.9 Updating the DCA software

To take advantage of the latest data collection capabilities, feature enhancements, and bug fixes, it is important to periodically update the DCA software.

You can update the DCA manually, or your distributor may update the DCA software for you if you have Intelligent Update enabled. See "Enabling Intelligent Update" on page 10.

To update the DCA software manually:

- On the **Help** menu, click **Check for Updates**.
- The update type allows for installation of Beta and Alpha releases (if available), or restricts updates to only stable releases.

2.10 Understanding the network load associated with the DCA

The following table shows approximate network byte load for various DCA scans, compared to the network load associated with loading a single standard web page.

Table 4: Network Byte Load Associated with the DCA

Event	Approximate Total Bytes
Loading a single standard web page	60 KB
DCA scan, blank IP	5.2 KB
DCA scan, 1 printer	7.2 KB
DCA scan, 1 printer, 1 254 local IP addresses	96 KB
DCA scan, network of 15 printers and 254 local IP addresses	125 KB

Chapter 3 **Using PrintFleet Optimizer**

The PrintFleet Optimizer web console is your primary means for viewing imaging device data and reports.

This chapter discusses all aspects of using the PrintFleet Optimizer web console.

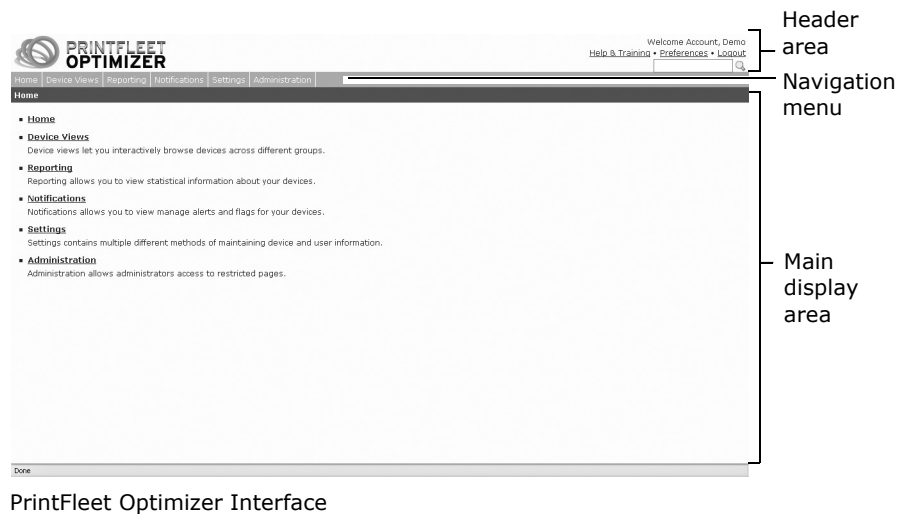
3.1 Working with the interface

The PrintFleet Optimizer web console 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.



Logging in to the system

Each user is assigned a unique user name (typically an email address) and password to log in to the PrintFleet Optimizer web console.

To log in to PrintFleet Optimizer:

1. In your browser window, navigate to your designated PrintFleet Optimizer URL, for example, <https://secure.printfleet.com>. This should have been obtained from your PrintFleet dealer.
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.

To request a password reset if you forgot your password:

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


If you are using Internet Explorer 6, upgrading to Internet Explorer 7 or 8, or another browser such as Firefox or Safari will result in a significantly improved user experience, due to improved speed and standards compliance.

The first time you log in to PrintFleet Optimizer, 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 in Optimizer allows you to quickly find specific items in the system.

To search for a specific item in PrintFleet Optimizer:

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

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

User results display the login name, first name, and last name.

Device results display the device name, group, serial number, IP address, MAC address, asset number, location, and last active date and time.

Group results display the group name, and parent groups.

Changing your 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.

To change your preferences:

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 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, \$userlogin, \$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

3. Click **Save**.

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.

3.2 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.

To view data using an available device view:

1. On the **Device Views** menu, click to select the device view you want to use from the following, or any custom view:
 - Technical View
 - Supplies Order View
 - Alerts
 - Maps
2. On the left side of the screen, select the group that contains the devices you want to view. Beside each group, it will indicate how many devices reside in that group; for example, *(5 of 15)* indicates that 5 devices are in the top level of that particular group, and 10 additional devices reside in subgroups of that group, for a total of 15 devices.

3. Use the lower toolbar to change the number of devices shown, scroll through pages, or refresh the data.



Filtering and sorting data

Data in a device view can be filtered and sorted. Filtering allows you to view a subset of the devices in the selected group. Sorting allows you to view information in ascending or descending order.

To sort data in a device view:

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

You can customize a default sort order for each view when creating or editing a view.

To filter data in a device view:

1. While on a device view, click **Change Filters**.
2. Do one or more of the following:
 - To filter devices by text string(s) that match all or a portion of a device name, serial number, asset number, IP address, or location, click to select the **Text** check box, and type the string in the text box. Multiple search strings are separated by a space, and each string will be searched individually (e.g. 10.0.0 HP would search both 10.0.0 and HP).
 - To filter devices by managed or unmanaged status, click to select **Managed**, **Unmanaged**, or **Both** (default is Both).
 - To filter devices by networked or local status, click to select **Network**, **Local**, or **Both** (default is Both).
 - To filter devices by managed supplies or service status, click to select the **Managed Supplies** and/or **Managed Service** check box.
 - To filter devices by last active date, click to select the **Active within last _ days** check box, and enter the number of days in the box.

Note

Device views are set to automatically filter based on last active date for a default number of days. The default number is 6 days, but this is can be configured by the administrator.

- To filter devices by percent toner remaining, click to select the **Toner** check box, and then select the highest percent toner remaining you want to view from the list. Optionally, click to select the **Include unknown** check box to list devices with an unknown amount of toner remaining.
- To filter devices by the last time supplies were ordered, click to select the **Last Supplies Order**, and then select the time interval for last supplies orders that you want to view: never, less than 1 week, less than 2 weeks, less than 3 weeks, or less than 30 days ago.

3. Click **Apply Filter**.

Filter By Text:
Close

☐ Text:

Filter By Status/Type:

Management:
☐ Managed
☐ Unmanaged
☒ Both

Type:
☐ Network
☐ Local
☒ Both

Restrict To:
☐ Managed Supplies
☐ Managed Service

Filter By Last Active Date:

☒ Active within last 100 days.

Filter By Supplies:

☐ Toner: < 10%
☐ Include unknown


☐ Last Supplies Order: Never

Apply Filter
Reset Filter

To clear a data filter in a device view:

1. While on a filtered device view, click **Change Filters**.
2. Click **Reset Filter**.

Viewing new devices

Devices that have recently appeared in the system will be marked with a **New** icon (). The number of days that a device will be marked as new is configured by your system administrator. The default number of days is 30.

Working with the traffic light system

Some device views use a traffic light system to display supplies status and device status. A legend appears at the bottom of applicable device views. The following table describes what each traffic light icon means for supplies status and device status.

Table 5: Understanding the Traffic Light System






Icon	Status Interpretation
	OK
	Caution (for supplies, Low Toner)
	Warning (for supplies, Out of Toner)

Table 5: Understanding the Traffic Light System

Icon	Status Interpretation
	Stale (data has not been collected from the device for 24 hours)
	Unknown (data is not available from the device or not supported by PrintFleet)

Working with the default views

The following table describes the data included in each of the default device views.

Table 6: Default Device Views

Device View	Data Included
Technical View	device name, supplies status, overall status, page count - month, serial number, IP address, location, last active date
Alerts	customer, devices, options for managing alerts
Maps	list of maps, links to each map, number of devices placed on each map, options for managing maps
Supplies Order View	device name, pages in last 30 days, supply type, current level/status, last order date, option to order supplies

Using the Technical View

The Technical View provides basic information about devices, including the name, supplies status, device status, yesterday meter count, serial number, IP address, location, and last active date. You can Edit and Override this information via Options in the Device View Manager.

To access the Technical View:

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

Device Name	Device ID	Overall St	Page Count - Month	Serial Number	IP Address	L
DP_M188A1DESIGNJET 500 LC77	-8159309525	OK	0	testserial	10.0.0.147	8
Canon R C3380	-2236563553	OK	65	TXP01240	10.0.0.50	8
HP Color LaserJet 2600n II	86940486145	OK	176	CNOC6252J7	10.0.0.104	8
HP Color LaserJet 2640	-112929676342	OK	0	CNHC78M043	10.0.0.208	8
HP LaserJet 1032n 9380	-112929418229	OK	1	SERVICE ID:	10.0.0.128	8
RM7530 9066	36013012509993	OK	0	AJA3002526	10.0.0.102	7
Kyocera EP-C220n	628632765274	Warning	47	APR7502679	10.0.0.127	8
Lexmark T934	17193981485	Warning	1698	123ABC	10.0.0.232	8
Lexmark Z550n	29880931302	Warning	38	123ABC	10.0.0.115	8
LocalBeacon...Webhooks Pa	-105417492437	OK	0		10.0.0.138	8

The Technical View will display the traffic light icon for supplies status and overall status that corresponds to the most significant status. For example, if a device is out of black toner and low on yellow toner, the Technical View will display a warning icon under the Supplies column for the black toner, rather than a caution icon for the yellow toner.

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 View for that device. See “Working with the Device Detail view” on page 38.

Using the Supplies Order View

The Supplies Order View displays supplies related information about devices, including black toner level or status, cyan toner level or status, magenta toner level or status, yellow toner level or status, device name, and a link to the report on pages for the last 30 days. Supplies can also be ordered from the Supplies Order View. You can Edit, Override, or delete this information via Options in the Device View Manager.

Supplies orders are automatically added to the service history of each applicable device.

To access the Supplies Order View:

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

Device Views > Supplies Order View

Widgets (15 of 208)

- Root (0 of 5663)
- Beta Customers (0 of 5455)
- Demo Group (0 of 0)
- Widgets (15 of 208)

Device	Pages - Last 30 days	Toner Order
KONICA MINOLTA magicolor 2530 DL 00B1	124069	Black 64% <input type="text"/> Last Order: Never Cyan <input type="text"/> Last Order: Never Magenta <input type="text"/> Last Order: Never Yellow <input type="text"/> Last Order: Never
HP LaserJet P3005 B17B	65841	Black 50% <input type="text"/> Last Order: Never
SHARP AR-M355N FFTA	59576	Black <input type="text"/> Last Order: Never
TOSHIBA e-STUDIO5520C 0D4C	50974	Black <input type="text"/> Last Order: Never Cyan <input type="text"/> Last Order: Never Magenta <input type="text"/> Last Order: Never Yellow <input type="text"/> Last Order: Never
Xerox WorkCentre Pro 55_v1 Multifunction	41246	Black <input type="text"/> Last Order: Never
KONICA MINOLTA bizhub C351 B2A2	35451	Black <input type="text"/> Last Order: Never Cyan <input type="text"/> Last Order: Never Magenta <input type="text"/> Last Order: Never Yellow <input type="text"/> Last Order: Never
Canon iR C4080 B2.03 2D62	31628	Black <input type="text"/> Last Order: Never Cyan <input type="text"/> Last Order: Never Magenta <input type="text"/> Last Order: Never Yellow <input type="text"/> Last Order: Never
KONICA MINOLTA bizhub C353 C703	30901	Black 66% <input type="text"/> Last Order: Never Cyan 83% <input type="text"/> Last Order: Never Magenta 30% <input type="text"/> Last Order: Never Yellow 85% <input type="text"/> Last Order: Never

15 Page 1 of 14 Displaying 1 to 15 of 208 items

For devices that are capable of reporting specific percentage supplies levels, toner level information will be displayed as a percentage. For devices that are not capable of reporting specific percentage supplies levels, toner level information will be displayed using the traffic light system. See "Understanding the Traffic Light System" on page 32.

Supplies can also be ordered via the Supplies Order View. Later, you can view previous supply orders.

To order supplies:

- On the **Supplies Order View**, enter the quantity of each supply to be ordered in the **Toner Order** column.

Note

If you include the **Toner Order** column in a custom device view, you will be able to order supplies directly from that view using the same method as the Supplies Order View. See "Using the Supplies Order View" on page 34.

- Click **Order Supplies**, and you will be taken to the order screen.
- Verify the information in the **Order Summary** area is correct. If it is not, return to the Supplies Order View to modify the order, or click **Cancel Order**.
- In the **Complete Order** area, complete the following fields:
 - Email To:** the email address where the order should be sent


- **Email CC:** the email address to be copied on the order, by default, the email associated with your user account
 - **Subject:** the subject line of the email
 - **Note (optional):** note to include in the body of the email
5. Click **Send Order**.

To view previous supply orders:

1. On the **Reporting** menu, click **Previous Supply Orders**. Date, ordered by, and order information are displayed.
2. Under the **Options** column, click **View Order** to see exactly which devices and supplies were included in a specific order.

The Supplies Order View provides direct access to a page count report, that displays pages printed over the past 30 days.

To view the Page Counts report for a device:

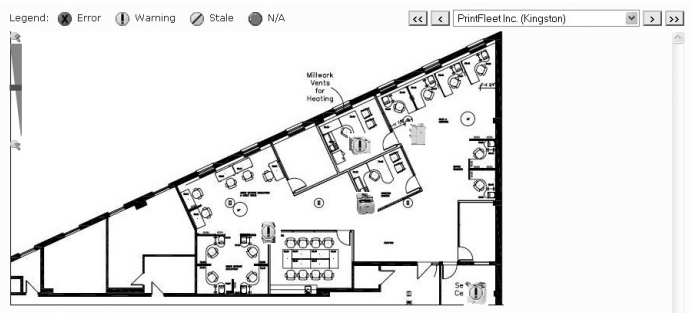
- Click the  icon under the **Pages (last 30 days)** column, in the row of the device you want to run the report for. The icon will be a smaller version of the actual report, and can be used as a quick reference.

For more information about reports, see "Using reports" on page 44.

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 View for that device. See "Working with the Device Detail view" on page 38.

Using the Maps View

The Maps View allows you to view images of document output devices, computing devices, people, and other miscellaneous items on one or more maps. Document output devices will display their status using the traffic light system. See "Understanding the Traffic Light System" on page 32.



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 view" on page 38.

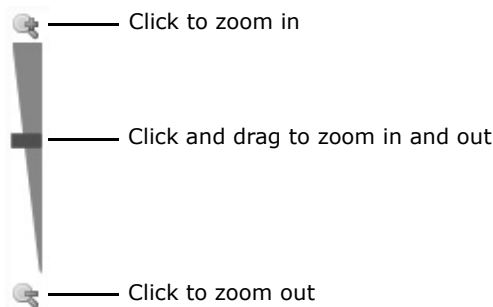


To access the Maps view:

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

To view a map:

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



Using the Alerts View

The Alerts view displays details on recently sent alerts.

The Alerts view displays the customer name, number of devices that have recent alerts, and a link to view alert details for each device.

To view the Alerts view:

- On the **Device Views** menu, click **Alerts**.
- Under the **Options** column, click **Details** to view the device name, serial number, LCD, and service code status for each device with a recent alert.

Recent Alerts Sent for Widgets Inc.			
Device	Serial #	LCD	Service Code
Leomark T304	RP1EST	Ready	[218/2008]
HP Color LaserJet 2040	CH4CT8M043	Ready Auto	[218/2008]
KONICA MINOLTA magicolor	7308001596		[213/2008]WARNING Sleep;
Leomark X550n		Power Saver	[218/2008]WARNING Sleep Mode;
Canon EC C3880	TXP01240		[212/2008]
HP Color LaserJet 5500	JPH5006445	INSTALL SUPPLIES,For status press	[1215/2008]08 6107;CRITICAL INSTALL BLACK CARTRIDGE;CRITICAL INST
Konica EP C2200	APR7502679	Sleeping	[220/2008]INFO;
HP Color LaserJet 2030	CHFO300C1	Load paper	[1/03/2008]CRITICAL TRAY EMPTY;
KONICA MINOLTA magicolor		ENERGY SAVER;ENERGY SAVER;OK TONER LOW	[1216/2008]WARNING Toner Near Empty Black;WARNING Sleep;
KONICA MINOLTA magicolor	321700611		[217/2008]WARNING Toner Near Empty Cyan;WARNING Toner Near Empty Magenta;WARNING
15 [Navigation icons] Page 1 of 2 [Navigation icons] Displaying 1 to 15 of 22 items			

- Optionally, to view additional information about a specific device, click the device name to go to the Device Detail view. See "Working with the Device Detail view" on page 38.

3.3 Working with the Device Detail view

The Device Detail view displays all information, and links to other areas in the system, relevant to a specific device. An image of the device model is also included if available.

The lower area of the Device Detail view has tabs for accessing complete meter breakdowns, supply levels, service information, miscellaneous device-specific information, and model information.

To access the Device Detail view:

- 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 30.

Navigate between devices in the same group

Home | Device Views | Reporting | Notifications | Settings | Administration

Device Views > Device View > Device Detail

hp color LaserJet 2500 79CC

Root > Widgets > Brandon Test Group

Group Name	hp color LaserJet 2500 79CC	Status	OK
Device Type	Network	Serial #	CNBD04435
IP Address	128.252.121.204	Asset #	
MAC Address	00-01-E6-4D-8C-23	Total Coverage	35.00% (Source: Estimated)
Location		Black Coverage	8.00% (Source: Default)
Last Active	19 days ago	Utilization	0%
First Seen	Monday, September 28, 2009	Firmware	SYSTEM=20020612; JETDIRECT=L.21...
Install Date	Monday, February 24, 2003		

Display: PowerSave on

Errors:

Supplies | Meters | Service | Miscellaneous | Model | Additional Information

Toner	SKU	Order	Supply	Order
Black	86% C9700A			
Cyan	52% C9701A		Imaging Drum HP C9704A	
Magenta	49% C9703A		KIT	
Yellow	52% C9702A		Unknown	

Coverage

Coverage	Value
Black	8.00% (Source: Default)
Cyan	9.00% (Source: Default)
Magenta	9.00% (Source: Default)
Yellow	9.00% (Source: Default)

Table 7: Information Displayed in the Device Detail View

Group	Name
IP address	Status
Location	Utilization
Serial number	Asset number
Total coverage (and source)	Individual color coverages (and source)
Last active (date/time)	MAC address
Firmware	First seen (date)
Install date	Display (with More link to view previous displays)
Errors (with More link to view previous errors)	Links to external web sites if configured for the device's group
Supply levels (with ability to add and remove items from a supplies order)	Meter breakdowns (with links to page count reports)
Service information (including past 100 alerts and flags, and recent service history)	Miscellaneous device-specific information
Model information (from the model database)	Device Type


Page coverages are displayed for each application color, as well as total. Coverage values can come from a variety of sources—the source being used will be indicated in brackets beside the percentage value. The following table describes the various sources.

Table 8: Page Coverage Data Sources

Coverage Data Source	Description
Device Total	A value obtained directly from the device for the lifetime average page coverage of the device.
Device Cartridge	A value obtained directly from the device for the average page coverage over the life of the current cartridge.

Table 8: Page Coverage Data Sources

Coverage Data Source	Description
Device Total / Device Cartridge	Both Device Total and Device Cartridge values may display if both are available.
Estimated ¹	If there is enough information to calculate page coverage, but no page coverage given directly from the device, a calculated estimate of page coverage will be displayed.
Default ¹	If no page coverage information is available, a default percentage of 5% will be displayed.
1. This value can be set in the Configuration page.	

The ERP icon () will appear beside the serial number of the device on the Device Detail view if the device is currently configured for meter exports.

Note	You can find additional information, including the version of the DCA being used, by hovering your mouse over the device image.
-------------	---

Viewing embedded web pages

From the Device Detail view, you can view the embedded web page of the device, provided you are within the internal network that the device resides.

To view the embedded web page:

- Click the **IP address** of the device. Two options appear: Internal Webpage and Service Bridge. To access the Service Bridge for network devices, see "Enabling a Service Bridge" on page 11.

Viewing historical LCD and error information

From the Device Detail view, you can view historical LCD and error data, useful for determining whether or not there are recurring or serious problems with a device.

To view historical LCD data:

- Click **More** to the right of the **Display** area.

To view historical error data:


- Click **More** to the right of the **Errors** area.

Working with the Supplies tab

The Supplies area on the Device Detail view displays toner and non-toner supply levels, supply SKUs, and provides the ability to add items to a supplies order (if this feature is enabled).

To access supplies information:

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

Supplies									
Meters		Service		Miscellaneous		Model		Additional Information	
Toner		SKU		Order		Supply		Order	
Black	<div><div>86%</div></div>	C9700A	<input type="text" value="1"/>	<input type="text" value="1"/>					
Cyan	<div><div>52%</div></div>	C9701A	<input type="text" value="1"/>	<input type="text" value="1"/>	Imaging Drum HP C9704A	<div><div>72%</div></div>	<input type="text" value="1"/>	<input type="text" value="1"/>	
Magenta	<div><div>49%</div></div>	C9703A	<input type="text" value="1"/>	<input type="text" value="1"/>	KIT	 Unknown	<input type="text" value="1"/>	<input type="text" value="1"/>	
Yellow	<div><div>52%</div></div>	C9702A	<input type="text" value="1"/>	<input type="text" value="1"/>					
Coverage									
Black	8.00% (Source: Default)								
Cyan	9.00% (Source: Default)								
Magenta	9.00% (Source: Default)								
Yellow	9.00% (Source: Default)								

To add items to a supplies order:

- Under the **Order** column, click the + icon in the row of the supply you want to order. Click additional times to increase the order quantity.
- If you are finished adding items to your order, click **Place Order** to proceed to the order screen. See "Using the Supplies Order View" on page 34.

Working with the Meters tab

The meters area displays complete meters information, including standard, virtual, and device-specific meters, for several different time periods: today, yesterday, past 7 days, past 31 days, current month, year, and life of the device. You can also access trend reports for each of these time periods.

To access meters information:

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

Supplies Meters Service Miscellaneous Model Additional Information								
	Today	Yesterday	Past 7 Days	Past 31 Days	Current Month	Year	Life	
Total	0	0	0	28	0	1338	1833	
Mono	0	0	0	26	0	878	1305	
Color	0	0	0	2	0	460	527	
Fax	0	0	0	27	0	788488	1117	
Scan	0	0	0	16	0	34226	820	
CopierMono	0	0	0	0	0	45	97	
CopierColor	0	0	0	0	0	0	1	
PrintMono	0	0	0	1	0	788104	92	
PrintColor	0	0	0	2	0	69399	526	
FIRMWARE	0	0	0	0	0	0	20060517	

To access a meter trend report:







- On the **Meters** tab, click one of the following column titles for the time period you want to run the report for:
 - Today.** Displays a report showing pages printed since 12:00am on the current day.
 - Yesterday.** Displays a report showing pages printed on the previous day.
 - Past 7 Days.** Displays a report showing pages printed during the previous seven days.
 - Past 31 Days.** Displays a report showing pages printed during the previous 31 days.
 - Current Month.** Displays a report showing pages printed from the start of the current month until the current day.

- **Year.** Displays a report showing pages printed from the start of the current year until the current day.
- **Life.** Displays a report showing pages printed from the start of when the DCA began collecting information from the device until the current day.

Working with the Service tab

The service area provides quick access to information about the past 100 alerts, past 100 flags, and service history for the device.

To access service information:

1. On the **Device Detail** view, click the **Service** tab.
2. Do one or more of the following:
 - To view past alerts, click the  icon beside Alerts and view the Send Date, To, From, and Subject for the past 100 alert emails directly in the Service tab, or click **Alerts** or  to go to the **Alert Settings** screen. See "Using alerts" on page 49.
 - To view past flags, click the  icon beside Flags to view the Send Date, To, From, and Subject for the past 100 flag emails directly in the Service tab, or click **Flags** or  to go to the **Flag Settings** screen. See "Using flags" on page 54.
 - To view the service history for the device, click the  icon beside Service History to view the Date/Time, Severity, Updated By, Maintenance, and Notes for each service history item directly in the Service tab, or click **Service History** or  to go to the **Service History** screen. See "Tracking device service history" on page 55.

Supplies Meters Service Miscellaneous Model Additional Information				
+ Alerts (past 100 e-mails) + Flags (past 100 e-mails) + Service History				
Date/Time	Severity	Updated By	Maintenance	Notes
Feb 25 2010 4:10PM	Low	Cheryl Hurley	Customer Order	Ordered: Yellow QTY(1)
Feb 25 2010 4:09PM	Low	Cheryl Hurley	Customer Order	Ordered: Magenta QTY(1) Yellow QTY(2)

Working with the Miscellaneous tab

The miscellaneous area provides additional device information that does not fit into any particular category. This information will vary by device, but may include such things as paper levels, amount of memory, duplex capability, etc.

To access miscellaneous device information:

- On the **Device Detail** view, click the **Miscellaneous** tab. This will display the Label, Value, and Date the information was obtained for each miscellaneous data item.

Supplies	Meters	Service	Miscellaneous	Model	Additional Information
Label	Value	Date			
DEVICEINFO_DUPLEX	FALSE	Feb 18, 2010 07:55:10			
DEVICEINFO_ENTERPRISENUMBERS	11	Nov 11, 2009 07:21:54			
DEVICEINFO_HOSTNAME	HP7C4BE5	Nov 10, 2009 09:35:19			
DEVICEINFO_IMPRESSION_BASED_METERING	Not Supported	Nov 10, 2009 09:35:19			
DEVICEINFO_INSTALLDATE	20051007T1310ZZ	Nov 10, 2009 09:35:19			
DEVICEINFO_MEMORY	34 MB	Feb 18, 2010 08:12:52			
DEVICEINFO_SUPPLYCOUNT_BLACK	11	Nov 10, 2009 09:35:19			
DEVICEINFO_SUPPLYCOUNT_BLACK_PRINTHEAD	1	Nov 10, 2009 09:35:19			
DEVICEINFO_SUPPLYCOUNT_CYAN	7	Nov 10, 2009 09:35:19			
DEVICEINFO_SUPPLYCOUNT_CYAN_PRINTHEAD	1	Nov 10, 2009 09:35:19			
DEVICEINFO_SUPPLYCOUNT_MAGENTA	7	Nov 10, 2009 09:35:19			
DEVICEINFO_SUPPLYCOUNT_MAGENTA_PRINTHEAD	1	Nov 10, 2009 09:35:19			
DEVICEINFO_SUPPLYCOUNT_YELLOW	8	Nov 10, 2009 09:35:19			
DEVICEINFO_SUPPLYCOUNT_YELLOW_PRINTHEAD	1	Nov 10, 2009 09:35:19			
DEVICEINFO_SYSNAME	HP7C4BE5	Nov 10, 2009 09:35:19			
DEVICEINFO_TECHNOLOGYTYPE	Unknown	Feb 18, 2010 07:55:10			
DEVICEINFO_TRAYLEVEL_UNKNOWN.1	0/150	Feb 18, 2010 08:12:52			
DEVICEINFO_TRAYLEVEL_UNKNOWN.2	-2/250	Nov 10, 2009 09:35:19			
FIRMWARE_MAIN	20041001	Nov 10, 2009 09:35:19			
	MMR2016W				
SUPPLY_BLACK	13.2%(91/690)	Sep 30, 2009 09:03:10			
SUPPLY_BLACK_PRINTHEAD	inserted	Nov 10, 2009 09:35:19			
SUPPLY_CYAN	23.6%(66/280)	Sep 29, 2009 11:01:40			

Working with the Model tab

The model area provides information about the device model, rather than the specific device. This information is stored in the model database, and is not collected by the DCA (although some of the information may also be available through the DCA).

To access model information:

- On the **Device Detail** view, click the **Model** tab. The information contained here is displayed below.

Supplies	Meters	Service	Miscellaneous	Model	Additional Information
Model Information					
Model Name		Hewlett-Packard Color LaserJet 2500			
Duty Cycle		30000			
Color Device		Yes			
PPM Black		16			
PPM Color		4			
Date Introduction		9/23/2002			
Toner Information		Product Code	Product Yield		
Black Cartridge		C9700A	5000		
Cyan Cartridge		C9701A	4000		
Magenta Cartridge		C9703A	4000		
Yellow Cartridge		C9702A	4000		
Miscellaneous					
Color		Yes			
Copier		No			
Printer		No			
Fax		No			
Scanner		No			
Operating Power Usage		400 watts			
Idle Power Usage		30 watts			

3.4 Using reports

PrintFleet Optimizer reports let you view data when and how you want it. In addition to the default Primary Reports, you can generate Custom Reports and Executive Reports (multiple reports combined into one). You can also schedule reports to be sent via email.

Generating reports

PrintFleet Optimizer allows you to generate a variety of Primary, Custom, and Executive reports.

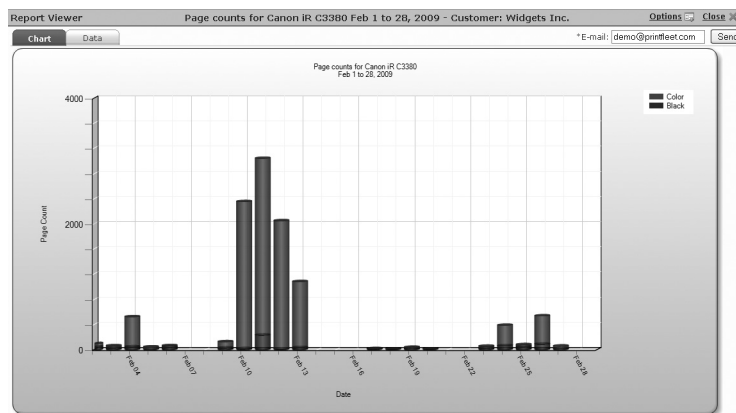
To generate a report:

1. On the **Reporting** menu, point to **Report Console**, and then click **Create Report**.
2. In the **Report Information** area, do the following:
 - Select a report from the **Report Selection** list.
 - Select other options as necessary, depending on which report you have chosen. This may include selecting a group, a specific device, etc.
3. In the **Run Now** area, do one of the following:
 - Select a **Start Date** and **End Date** for the report.

- Select a date range from the **Data Range** list (This Month, This Year, or Last Month). This will automatically populate the start and end dates for the report.
4. Click **View Report**.
 5. For Executive Reports, navigate through each individual report by selecting a page to view from the list in the **Report Viewer** header.

The Report Viewer allows you to do various things with a generated report, including:

- View in chart form.
- View in data form.
- Email the report.
- Download the report in .pdf format.
- Download the report in .csv format.



To view a report in chart form (if applicable):

- After generating a report, in the **Report Viewer**, click the **Chart** tab.

To view a report in data (text) form:

- After generating a report, in the **Report Viewer**, click the **Data** tab.

To email a report:

1. After generating a report, in the **Report Viewer**, type in the email address you want to send the report to in the **E-mail** box.
2. Click **Send**.

To download a report in .pdf format:

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

To download a report in .csv format:

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

Primary reports are default reports you can generate to view information about document output devices.

Table 9: Description of Primary Reports

Report	Description
Advanced Volume Report	A text report that displays device name, serial number, start page count, end page count, page total, mono total, color total, copier mono, copier color, print mono, print color, fax count, IP address, asset number, and last active date. Additional machine-specific meters can be shown if selected. You can choose to run the report for either managed or unmanaged devices.
CPC Report	A text report that displays the device name, serial number, asset number, location, count mono, count color, CPC mono, CPC color, CPC total mono, CPC total color, and CPC total based on a specified date range.
Current Meters	A text report that displays the device name, serial number, IP address, asset number, all available meters (standard and custom) based on a specified end date, and the last active date, for either managed or unmanaged devices for the selected group.
Individual Page Count Report	A graphical report that displays total page count, total monochrome count, and total color count for a single device over a specified time period.
Individual Toner Level Report	A graphical report that displays black, cyan, magenta, and yellow toner levels (where applicable) for a single device over a specified time period.

Table 9: Description of Primary Reports

Report	Description
Individual Page & Toner Report	A graphical report that displays black pages, color pages, and black, cyan, magenta, and yellow toner levels for a single device over a specified time period.
Individual Misc. Supplies Report	A graphical report that displays the level of a specified supply item (i.e. imaging drum), for a single device over a specified time period.
Power Usage Report	A text report that displays the device name, serial number, operating watts, idle watts, total pages (in the selected time period), estimated kWh usage, estimated cost (at selected kWh price), power cost per page, and total power cost of the selected group over the specified time period.
Toner Reorder Report	A text report that displays the device name, asset number, mono and color pages based on a specified start date, supply (toner) types, and current supply levels for the selected group.

Custom reports are created by your PrintFleet administrator and are accessed through the PrintFleet Optimizer console. Some custom reports are included in the system.

Scheduling reports

Scheduled reports are configured to email to a specified recipient at predetermined intervals.

A scheduled report email contains the data and chart (if applicable) embedded in the body of the email, as well as the report in a .csv format attachment.

To create a scheduled report:

1. On the **Reporting** menu, point to **Report Console**, and then click **Create Report**.
2. In the **Report Information** area, do the following:
 - Select a report from the **Report Selection** list.

- Select other options as necessary, depending on which report you have chosen. This may include selecting a group, a specific device, date range, etc.
3. Click to select **Set Up Schedule**.
 4. Type an email subject line for the report in the **Schedule Name** box.
 5. Type in one or more email addresses for the report to be sent to in the **Email address(es)** box. Multiple email addresses can be separated by commas, semicolons, or spaces.
 6. In the **Start Date** area, type or select a start date and time for the report to begin sending.
 7. In the **Repeat** area, select one of the following intervals for the report to send:
 - **Daily**. Type in the interval, in days, that you want the report to run.
 - **Weekly**. Type in the interval, in weeks, that you want the report to run, and select the day of the week that you want the report to run.
 - **Monthly**. Type in which day of the month and interval in months that you want the report to run.
 - **Advanced**. Select which occurrence of which day of the week in a month, and interval in months that you want the report to run.
 8. In the **Date Range** area, select one of the following intervals for each report to analyze:
 - **Last 24 hours**
 - **Last 7 days**
 - **Last 30 days**
 - **Previous Month**
 - **Current Month**
 - **Last 90 days**
 - **Advanced**. Select a **Report Start**, typically **Month Start**, and optionally select +/- a specified amount of days or months. Select a **Report End**, typically **Month End**, and optionally select +/- a specified amount of days or months.
 9. Click **Save Schedule**.

☒ Set Up Schedule

Schedule Name:

E-mail address(es):

Start Date:

Repeat: The of every month(s)

Date Range:

Report Start:

Report End:

To view existing scheduled reports:

- On the **Reporting** menu, point to **Report Console**, and then click **Scheduled Reports**. The email address, title, last sent

date, and options to edit and delete each schedule are displayed.

To edit a scheduled report:

1. On the **Reporting** menu, point to **Report Console**, and then click **Scheduled Reports**.
2. Under the **Options** column, click **Edit** in the row of the scheduled report you want to edit. This will take you to the **Edit Report** tab.
3. Make the changes you want to the scheduled report. In addition to the standard items, you also have the option to change the **Next Send Date**. The last sent date will also be displayed.
4. Click **Save Schedule**.

To delete a scheduled report:

1. On the **Reporting** menu, point to **Report Console**, and then click **Scheduled Reports**.
2. Under the **Options** column, click **Delete** in the row of the scheduled report that you want to delete.
3. Click **Confirm** to verify deletion of the schedule.

3.5 Using alerts

Alerts are configured to notify you via email when a document output device has a status that you have indicated you want to be notified of. This gives you or your dealer the ability to respond to service issues quickly. Recently sent alerts are also summarized on the Alerts view; for more information, see "Using the Alerts View" on page 37.

Creating new alerts

To create a new alert:

1. On the **Notifications** menu, point to **Alert Settings**, and then click **Alert Manager**.
2. Click the **New Alert** button.
3. Complete the following required items:
 - Select a company from the **Customer** list.
 - Type in an email subject line for the alert in the **Title** box.
 - Type in the email address that you want the alert to be sent to in the **E-mail** box.
4. Optionally, select a layout from the **Alert Layout** list. See "Managing alert layouts" on page 51.
5. Optionally, to assign the alert to individual devices instead of all devices, do the following:
 - Click to select the **Individual Devices** check box.
 - Click the **Assign Devices** button.
 - Under the **Assigned** column, click to select the check box beside each device you want the alert assigned to.
 - Click **Assign Devices**.

6. Do one or more of the following to choose the device status items you want to be alerted on:
 - Type custom error codes you want to be alerted on in the **Alert Codes** box. Use semicolons to separate multiple items.
 - Click to select specific status items listed under the **Critical**, **Warning**, and **Toner** columns. For black, cyan, yellow, and magenta threshold (%) items, type in the percent level you want to be alerted on in the text box to the right of the item.
7. Click **Save**.

Table 10: Status items that can be part of an alert

Status	Category
Critical	Critical
Door open	Critical
Paper jam	Critical
Offline	Critical
No paper	Critical
Warning	Warning
Low paper	Warning
Stale	Warning
Service requested	Warning
Low toner	Toner
No toner	Toner
Black threshold (%) (input a custom percentage)	Toner
Cyan threshold (%) (input a custom percentage)	Toner
Magenta threshold (%) (input a custom percentage)	Toner


Table 10: Status items that can be part of an alert

Status	Category
Yellow threshold (%) (input a custom percentage)	Toner
Alert codes (custom inputs)	N/A

Editing alerts

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

To edit an alert:

1. On the **Notifications** menu, point to **Alert Settings**, and then click **Alert Manager**.
2. Select a company to view their existing alerts.
3. Click  under the **Edit** column in the row of the alert you want to edit.
4. Make changes to the alert as desired, and then click **Update**.

Deleting alerts

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

To delete an alert:

1. On the **Notifications** menu, point to **Alert Settings**, and then click **Alert Manager**.
2. Select a company to view their existing alerts.
3. Click **Delete** in the **Options** column in the row of the alert you want to delete.
4. Click **Confirm** to verify deletion.

Managing alert layouts

Alert layouts determine what columns appear in alert emails, and in what order the columns will be displayed. Unlimited custom alert layouts can be created. A single layout can be assigned to multiple alerts.







By default, alerts will contain the following fields in this order: Device Name, Serial Number, IP Address, Supplies (status), Status, Service Codes, LCD, Alert Items, Last Active Date, Toner Black (level or status), Toner Cyan, Toner Magenta, Toner Yellow, Black SKU, Cyan SKU, Magenta SKU, Yellow SKU, Location, Last Action Date, Last Action Notes, and Asset Number.

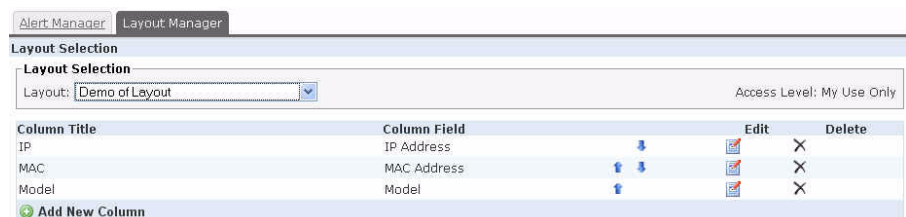
To create a new alert layout:

1. On the **Notifications** menu, point to **Alert Settings**, and then click **Layout Manager**.
2. Click the **New Layout** button.
3. Type a name for the layout in the **Layout Name** box.
4. Select either **Everyone** (available for every user in the database) or **My Use Only** (for your own use only) from the **Access Level** list.
5. Click the **Save** button.











You will then need to edit the alert layout in order to specify the columns and order of columns you want in your layout.


To edit an alert layout:

1. On the **Notifications** menu, point to **Alert Settings**, and then click **Layout Manager**.
2. Select the layout you want to edit from the **Layout** list.
3. Do one or more of the following:
 - To change the layout title and access level, click the **Edit** button, make the desired changes and then click **Save**.
 - To add a column, click **Add New Column**. Under the **Column Title** column, type in a name for the column in the text box. Under the **Column Field** column, select the type of data you want to appear in that column. Click  to save the column.
 - To edit a column, click  under the **Edit** column in the row of the data field you want to edit. Make the desired changes and then click  to save the changes.
 - To delete a column from the layout, click  under the **Delete** column in the row of the data field you want to delete.
 - To change the order that a data field appears in your alert layout, click  in the row of a field that you want to move one column to the left in your alert layout, or click  in the row of a field that you want to move one column to the right in your alert layout. Repeat until you have the data in the order you want it to appear.



The screenshot shows the 'Layout Manager' window. At the top, there are tabs for 'Alert Manager' and 'Layout Manager'. Below the tabs is a 'Layout Selection' section with a dropdown menu showing 'Demo of Layout' and an 'Access Level: My Use Only' label. The main area contains a table with the following columns: 'Column Title', 'Column Field', 'Edit', and 'Delete'. The table has three rows of data: 'IP' (IP Address), 'MAC' (MAC Address), and 'Model' (Model). Each row has a 'Move left' icon, a 'Move right' icon, an 'Edit' icon, and a 'Delete' icon. At the bottom left of the table is a green button labeled 'Add New Column'.

Column Title	Column Field		Edit	Delete
IP	IP Address			
MAC	MAC Address	 		
Model	Model			



If an alert layout is no longer needed, it can be deleted at any time.

To delete an alert layout:

1. On the **Notifications** menu, point to **Alert Settings**, and then click **Layout Manager**.
2. Select the layout you want to delete from the **Layout** list.
3. Click the **Delete** button.
4. Click **Confirm** to verify deletion.

Working with alert emails

Alerts are sent via email to the email address specified when creating a new alert. See “Creating new alerts” on page 49.

Subject: Alert Widgets Inc. Low Toner
Attachments: [] _AVG certification.txt (268 B)

Device Name	Serial Number	IP Address	Supplies	Status	Service Codes	LCD	Alert Items	Last Active
Ekttronix Inc. Phaser 820	LTH071423	10.0.0.210	OK	ERROR	CRITICAL.Engine Failure;	2'OK'hXcS;Printer error - Contact service report f	Offline, Service Requested	Feb 04, 200
hp LaserJet 4200 010C	CN8K402580	192.168.1.12	OK	WARNING		Ready;To enter menu;press	Low Paper	Feb 04, 200
Lexmark T634 4130420 551	4130420	10.0.0.44	OK	WARNING	WARNING.Tray 1 Low;	Power Saver;Tray 1 Low	Low Paper	Feb 04, 200

[Acknowledge Alert - 24 Hours \(Sleep until Feb 05, 2008 08:45:52\)](#)

Sample alert email

New alerts are received only if a device triggers an alert status indicated in the alert settings, or if a device status condition escalates (for example, from warning to critical).

The interval that alerts are sent at will depend on the interval that individual DCAs are set to scan the network. See “Setting the scan and transmission interval” on page 17. The alert mechanism itself runs every 30 minutes.

To disable a specific alert for 24 hours, click the **Acknowledge Alert - 24 Hours** link in the alert email. This will not stop new alerts from being sent if the status of any device changes to an alert condition within the 24 hours.

Other links in the alert email will take you directly to the device detail page for the corresponding device (after logging into PrintFleet Optimizer).

Devices displayed in alert emails will display a specific background color in the Device Name and Status columns depending on the type of warning or error being reported. The meaning of each background color is outlined in the following table.

Table 11: Alert email background color definitions

Background Color	Definition
Yellow	New warning that has not been reported in a previous alert
Pale yellow	Warning that has been reported in a previous alert
Red	New error that has not been reported in a previous alert
Orange	Error that has been reported in a previous alert

Table 11: Alert email background color definitions

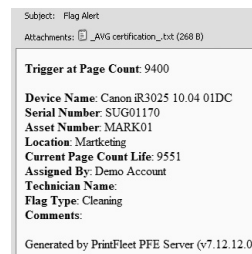
Background Color	Definition
Cyan	New stale/offline device that has not been reported in a previous alert
Gray	Stale/offline device that has been reported in a previous alert

3.6 Using flags

Flags are used to schedule preventative maintenance. Maintenance can be scheduled at a trigger life page count or a trigger date. When a flag is created and the trigger is hit, a flag icon will appear beside the appropriate device in any standard layout device view, which can be clicked to view the device's flag settings. An email will also be sent to the specified address.



Flag notification




Sample flag email

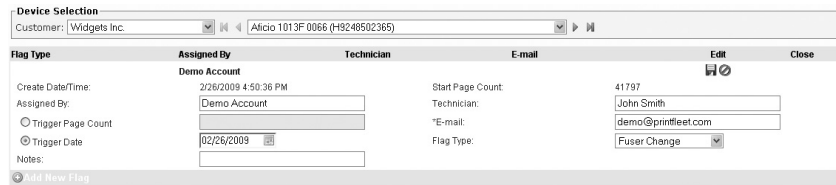
Creating flags

Multiple flags can be created to schedule different types of preventative maintenance for each device.

To create a new flag:

1. On the **Notifications** menu, click **Flag Settings**.
2. Select a company from the **Group** list.
3. Select a device from the list.
4. Click **Add New Flag**.
5. Type your name or title in the **Assigned By** box, if different from the default.
6. Type in the name of the technician who will perform the maintenance, if applicable, in the **Technician** box.
7. Type in an email address where a flag notification will be sent in the **E-mail** box.
8. Click to select either **Trigger Page Count** or **Trigger Date**. If **Trigger Page Count** is selected, type the life page count you want the flag to be triggered at in the **Trigger Page Count** box. If **Trigger Date** is selected, select or type the date you want the flag to be triggered at in the **Trigger Date** box.


9. Select the type of maintenance to be done from the **Flag Type** list. If the type of flag you want is not listed, select **Other**, and type in a description in the **Notes** box.
10. Click  to save the flag.



Closing flags

Once a flag is created, the trigger has been met, and the maintenance has been performed, the flag should be closed to delete it from the system.




To close a flag:

1. On the **Notifications** menu, click **Flag Settings**.
2. Select a company from the **Customer** list.
3. Select a device from the **Device** list.
4. Click  under the **Close** column in the row of the flag you want to close.
5. Click **Confirm** to verify you want to close the flag.

Editing flags

After a flag is created and before the trigger has been met, the flag can be edited at any time.

To edit a flag:

1. On the **Notifications** menu, click **Flag Settings**.
2. Select a company from the **Customer** list.
3. Select a device from the **Device** list.
4. Click  under the **Edit** column in the row of the flag you want to edit.
5. Make changes to the flag settings as desired.
6. Click  to save your changes.
7. Click the Remove icon () in the row of the custom field you want to remove.

3.7 Tracking device service history


PrintFleet Optimizer can keep a record of maintenance performed on each device. This is useful for tracking costs, and keeps you informed of which devices are requiring the most amount of maintenance, which can indicate which devices are being overused or which should be retired, replaced, or reallocated.

Toner orders are automatically entered as service history items. See "Using the Supplies Order View" on page 34.

To view and export the service history for a device:



1. On the **Settings** menu, point to **Device Management**, and then click **Service History**.
2. Select a group from the **Group Selection** list.
3. Select a device from the **Device Selection** list. Service history for that device will be displayed.
4. Optionally, to export the service history of that device, click **More Options**, click **Report**, type your email address in the **Email** box, and click **Send**.

To add a new service history item:


1. On the **Settings** menu, point to **Device Management**, and then click **Service History**.
2. Click **New Item**.
3. Input relevant information about the service item:
 - Under the **Date/Time** column, select or type in the date of the service in *mm/dd/yyyy* format, and select the time of day from the list. By default, it will display the current date at 12:00am.
 - Under the **Severity** column, select a severity level from the list. Available severities are Low (1), Moderate (2), and Urgent (3).
 - Under the **Updated By** column, type in your name, the name of the service technician, etc.
 - Under the **Duration** column, type in the amount of time the service event took. This can be in any units—you can specify the units to be clear, or use whatever is standard practice at your company.
 - Under the **Maintenance** column, type in a description of the maintenance or service that was performed.
 - Under the **Notes** column, type in any additional notes about the service performed.
4. Click  to save the service item.

Group Selection		Device Selection		Date/Time	Severity	Updated By	Duration	Maintenance	Notes	Edit Delete
Widgets Inc.		LANIER LW326 00A2		3/6/2009 12:30	MODERATE	Demo Account	30 minutes	Fuser change		 

To edit a service history item:

1. On the **Settings** menu, point to **Device Management**, and then click **Service History**.
2. Select a group from the **Group Selection** list.
3. Select a device from the **Device Selection** list.
4. Click  under the **Edit** column in the row of the service item you want to edit.
5. Change information for the service entry as desired, and then click  to save the entry.

To delete a service history item:

1. On the **Settings** menu, point to **Device Management**, and then click **Service History**.
2. Select a group from the **Group Selection** list.
3. Select a device from the **Device Selection** list.
4. Click  under the **Delete** column in the row of the service item you want to delete.
5. Click **Confirm** to verify deletion.

3.8 Virtual Meters

Virtual Meters create meters that add up values for other meters, optionally including a multiplier, to create a new meter value. Virtual Meters can perform many tasks, such as, add up different page sizes, create impression counters, and convert units.

To create Virtual Meters:

1. On the **Settings** menu, click **Virtual Meter Manager**.
2. Click **New Virtual Meter**.
3. In the **Meter Configuration** tab, enter the Meter Name and select a group from the **Group** drop down. Optionally, in the **Group/Device Assignment (Optional)** tab, select the group or individual devices.
4. Check the required **Meter Labels** and optionally edit the Multiplier value.
5. Click **Save**.

See "Contacting Technical Support" on page 3.

Appendix A PrintFleet End User License Agreement

END USER LICENSE AGREEMENT

PLEASE READ CAREFULLY BEFORE USING THIS SOFTWARE PRODUCT: This End-User License Agreement ("EULA") is a contract between (a) End User (either an individual or the entity End User represents) and (b) PrintFleet Inc. ("PFI") that governs End User use of the software product ("Software"). The term "Software" may include (i) associated media, (ii) a user guide and other printed materials, and (iii) "online" or electronic documentation (collectively "User Documentation"). If you do not agree with the terms of this AGREEMENT, promptly delete the SOFTWARE or return the unused SOFTWARE to PRINTFLEET or your service provider.

1. LICENSE RIGHTS. End User will have the following rights provided End User complies with all terms and conditions of this EULA:

a. Use. PFI grants End User a license to Use one copy of the PFI Software. "Use" means installing, copying, storing, loading, executing, displaying, or otherwise using the PFI Software. End User may not modify the PFI Software or disable any licensing or control feature of the PFI Software. End User may not separate component parts of the PFI Software for Use. End User does not have the right to distribute the PFI Software.

b. Copying. End User right to copy means End User may make archival or back-up copies of the PFI Software, provided each copy contains all the original PFI Software's proprietary notices and is used only for back-up purposes.

2. UPGRADES. To Use PFI Software provided by PFI as an upgrade, update, or supplement (collectively "Upgrade"), End User must first be licensed for the original PFI Software identified by PFI as eligible for the Upgrade. To the extent the Upgrade supersedes the original PFI Software, End User may no longer use such PFI Software. This EULA applies to each Upgrade.

3. TRANSFER RESTRICTIONS. End User may not rent, lease or lend the PFI Software or Use the PFI Software for commercial timesharing or bureau use. End User may not sublicense, assign or otherwise transfer the PFI Software except with the consent of PFI, not to be unreasonably withheld.

4. PROPRIETARY RIGHTS. All intellectual property rights in the Software and User Documentation are owned by PFI or its suppliers and are protected by law, including applicable copyright, trade secret, patent, and trademark laws. End User will not remove any product identification, copyright notice, or proprietary restriction from the Software.

5. LIMITATION ON REVERSE ENGINEERING. End User may not reverse engineer, decompile, or disassemble the PFI Software, except and only to the extent that the right to do so is allowed under applicable law.

6. **CONSENT TO USE OF DATA.** In providing service to END USER through the PRINTFLEET Web site, PRINTFLEET and its PARTNER may collect and use data and statistical information generated thereby. Unless otherwise provided in a separate agreement, such information shall be aggregated with data from other licensees of PRINTFLEET and its PARTNER and use and disclosure of such information shall only be done in the aggregate for statistical purposes and the information of any single licensee shall not be disclosed. Information such as END USER's name, address, telephone number, email address, IP address and other personal information such as credit card numbers related to particular transactions with the PRINTFLEET site will be considered customer identifiable information and will not form part of such collected information and will be kept confidential.

7. **LIMITATION OF LIABILITY.** Notwithstanding any damages that End User might incur, the entire liability of PFI and its suppliers under this EULA to the End User and End User exclusive remedy under this EULA will be limited to the greater of the amount actually paid by End User for the Product or U.S. \$5.00. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT WILL PFI OR ITS SUPPLIERS BE LIABLE FOR ANY SPECIAL, INCIDENTAL, INDIRECT, OR CONSEQUENTIAL DAMAGES (INCLUDING DAMAGES FOR LOST PROFITS, LOST DATA, BUSINESS INTERRUPTION, PERSONAL INJURY, OR LOSS OF PRIVACY) RELATED IN ANY WAY TO THE USE OF OR INABILITY TO USE THE SOFTWARE, EVEN IF PFI OR ANY SUPPLIER HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES AND EVEN IF THE ABOVE REMEDY FAILS OF ITS ESSENTIAL PURPOSE. Some states or other jurisdictions do not allow the exclusion or limitation of incidental or consequential damages, so the above limitation or exclusion may not apply to End User.

8. **U.S. GOVERNMENT CUSTOMERS.** If End User is a U.S. Government entity, then consistent with FAR 12.211 and FAR 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed under the applicable PFI commercial license agreement.

9. **COMPLIANCE WITH EXPORT LAWS.** End User will comply with all laws, rules, and regulations (i) applicable to the export or import of the Software, or (ii) restricting the Use of the Software, including any restrictions on nuclear, chemical, or biological weapons proliferation.

10. **RESERVATION OF RIGHTS.** PFI and its suppliers reserve all rights not expressly granted to End User in this EULA.

11. **NO IMPLIED RIGHTS.** This software is being loaded into applicable devices solely to enable remote monitoring of covered printers by End User service provider and its licensors. This software may not be copied, transferred, disclosed, or used by anyone other than the service provider and its designees. No rights or licenses to the software will be implied. The software is provided "AS-IS", except for any express warranties in the service provider services agreement.

(c) 2008 PrintFleet Inc.

Appendix B Data Collector Agent Checklist and Installation Requirements

Please use the following guide to ensure you are meeting all installation requirements prior to installing the PrintFleet Data Collector Agent (DCA).

Network requirements:

- TCP/IP configured

System requirements:

- Hardware: Non-dedicated server powered on 24 hours a day, 7 days a week. If a server is not available, the Data Collector Agent can be installed on a desktop computer system powered on 24 hours a day, 7 days a week, but this method carries a risk of transmission difficulties.
- Network card: 100mbit or higher
- RAM: 512MB or higher
- Internet connected browser

Virtualization software support:

If you want to install the DCA on a virtual machine, the following virtualization software will support the installation:

- Microsoft Virtual Server 2005
- VMWare GSX

Important:

- Do not install the DCA on a laptop.
- If you plan to use the DCA to collect data via VPN, please be aware that due to the extended transmission, there is a **risk of data loss**. Extended transmissions can result in timeouts during a Read access from a remote device.

Instructions for installing a DCA 3.x on Windows Vista, Windows 7, or Windows Server 2008

Windows Server 2008, Vista, and Windows 7 implement a new feature called User Account Control (UAC), which can cause installation problems with the DCA and/or the DCA Health Check service. These issues can be avoided by using the following procedures.

Note: If UAC is turned off, you do not need to use these special instructions.

After downloading the DCA installation file (DCA_Install.msi):

1. Right click on the DCA_Install.msi file and select Properties.

2. Under the Compatibility tab, click to enable the Run as Administrator check box.
3. Proceed to installing the DCA.

After the DCA is installed, repeat steps 1 and 2 above for the following two files:

- C:\Program Files\Data Collector Agent\DCAService.exe
- C:\Program Files\Data Collector Agent\Support\DCAServiceHC.exe

Index

A

- activating the DCA 5
- active date, last 33
- alerts
 - create 49
 - deleting 51
 - editing 51
 - e-mail 53
 - individual devices 49
 - layouts
 - assigning 49
 - managing 51
 - overview 49
 - status items 50
- archive files, deleting 24

C

- caution, status 32
- charts 45
- copiers. *See* devices
- coverage
 - data source 39
 - device detail 39
- CPC
 - report 46
- custom reports
 - generating 44

D

- Data Collector Agent
 - activating 5
 - installing 5
 - introduction 4
 - multiple subnets 6
 - network load 26
 - network timeout 6
 - obtaining the software 5
 - questions to ask prior to installation 6
 - recommended number of devices 6
 - requirements 60

- setting up as scheduled task 8
 - troubleshooting 12
 - VPNs 6
 - See also* PrintFleet Optimizer
 - See also* PrintFleet Enterprise
- data_queue folder 12
- Device Detail View 38
- device views
 - default 33
 - Maps 36
 - Supplies Order View 34
 - Technical View 33
 - traffic light system 32
 - working with 30
- devices
 - new 32
 - support 1
- downloading reports 45

E

- e-mailing reports 45
- e-mails, alert 53
- end user license agreement 58
- ERP icon 40
- EULA 58
- executive reports
 - generating 44

F

- fax machines. *See* devices
- firewalls 12
- flags
 - closing 55
 - creating 54
 - editing 55
 - overview 54
 - triggers 54

H

- history, service 55

I

installation
 Data Collector Agent 5
 requirements 2
IP address
 Technical View 33

L

last active date 33
layouts, alerts
 assigning 49
 managing 51
location 33
log files, deleting 24
logging in to PrintFleet Optimizer 28

M

maintenance
 See flags
 See service history
map images
 zoom 37
Maps view 36
maximum devices, DCA 6
meters
 tab, Device Detail View 41
 yesterday 33
 See *also* reports
model support 1
multiple subnets 6

N

network load, DCA 26
network timeout 6
new devices
 viewing 32
notifications
 alerts 49
 flags 54
 See *also* alerts
 See *also* flags

O

OK, status 32
Optimizer. See PrintFleet Optimizer

P

page counts. See meters
page coverage
 data source 39
 device detail 39
power usage report 47

primary reports
 See *also* reports
primary reports, list of 46
printers. See devices
PrintFleet Optimizer
 introduction 1
 updating 3
 using 27-??
 See *also* Data Collector Agent
PrintFleet Suite PRO
 optimizing DCA scans 5, 16

R

Report Viewer 45
reports
 charts 45
 downloading 45
 e-mailing 45
 generating 44
 overview 44
 Primary 46
 Report Viewer 45
 scheduling 47
requirements
 DCA 60

S

scheduled task, DCA 8
search 29
serial number 33
service history, tracking 55
service, DCA
 control
 main 8
stale
 status 33
status
 caution 32
 device 33
 indicators 32
 OK 32
 stale 33
 supplies 33
 unknown 33
 warning 32
subnets, multiple 6
supplies
 levels 34
 ordering
 Supplies Order View 34
 status 33
support, models 1
support, technical. See technical support

T

- technical support
 - contacting 3
- Technical View 33
- timeout, network 6
- toner levels. *See* supplies
- traffic light system 32
- trigger, flag 54
- troubleshooting
 - DCA transmission problems 12

U

- unknown, status 33
- updates
 - PrintFleet Optimizer 3
- URL, PrintFleet Optimizer 28

V

- VPNs (Virtual Private Networks) 6

W

- warning, status 32

Z

- zoom, map image 37