

PrintFleet DCA

DCA Version 4.5.0 and DCA Pulse Version 1.2.4

User Guide



PRINTFLEET®

PrintFleet DCA User Guide

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

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

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

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

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

Canon is a registered trademark of Canon Inc.

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

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

Evatic is a trademark or registered trademark of Evatic AS.



PRINTFLEET®

Revision DCA v 4.5.0 and DCA Pulse v 1.2.4

© Copyright 2018 ECI Software Solutions Canada Inc. d/b/a PrintFleet. All rights reserved.

Table of Contents

Chapter 1 Introduction

1.1	Device support.....	1
1.2	Obtaining software updates	3
1.3	Contacting Technical Support.....	3

Chapter 2 Using the Data Collection Agent4

2.1	Installing and activating the DCA.....	4
	Install DCA 4.x.....	6
	Downloading the Manual DCA Installer	7
	Auto-upgrade DCA 4.x to DCA Pulse	8
	Installing DCA Pulse.....	9
	Installing DCA Pulse on Mac OS X	10
	Installing DCA Pulse on Raspberry Pi.....	11
2.2	Managing the DCA service in Windows	12
	Installing and starting DCA 4.x service	12
	Deleting a DCA.....	13
	Setting up DCA 4.x as a scheduled task	13
2.3	Configuring communication settings.....	14
	Changing and testing the communication method and port.....	14
	Using proxy settings with DCA 4.x	15
	Using proxy settings with DCA Pulse	16
	Changing the web service settings.....	16
	Enabling Intelligent Update	17
	Troubleshooting DCA communication problems	18
	Configuring network scan settings	18
2.4	DCA 4.x: Managing Scan Profiles.....	19
	Create New Scan Profile	19
	Specifying which devices to scan	21
	Enabling scanning of network and/or local devices.....	23
	Enabling broadcast scanning	23
	Enabling Rapid Scan	23

Enabling Printer Job Language (PJL)	24
Setting the scan interval	24
Setting the network timeout	25
Setting the Local Print Agent timeout.....	26
Setting the number of SNMP retries.....	26
Using Focus Scans.....	27
Storing SNMP community strings.....	27
Using SNMP Version 3.....	28
Masking private data	30
Enabling SNMP traps.....	30
Disabling real time DCA status	31
Setting the WebPage timeout	32
2.5 Managing Scan Configuration.....	32
Adding a Scan Range.....	32
Configuring Scan Intervals	32
Configuring Security: SNMP Version 1/2.....	33
Configuring Security: SNMP Version 3.....	34
View Security Configuration Details	36
Delete a SNMP Profile	36
Configuring Communication.....	36
Configuring Logs	39
2.6 Viewing queue, archive, and log files with DCA 4.x	43
Deleting old archive and log files	44
2.7 Configuring language and read/write settings in DCA 4.x	44
2.8 Updating DCA 4.x.....	45
2.9 Reviewing the End User License Agreement (EULA): DCA 4.x.....	46
2.10 Understanding the network load associated with the DCA.....	46
2.11 DCA 4.x Command Line Options.....	46
2.12 DCA Pulse Command Line Options	47
Chapter 3 Managing local devices with Local Print Agent	50
3.1 Installing Local Print Agent.....	50
3.2 Managing Local Print Agent	51
Starting the Local Agent Management tool	51
Scanning for Local Agent installations	51
Changing the active user for Local Agent Management.....	52
Interpreting the Local Agent Management scan results.....	52
Performing a Push Install of Local Print Agent	53
Uninstalling Local Print Agent.....	53

Checking the data returned by Local Print Agent	53
Rescanning specific IP addresses.....	54
Configuring a Local Print Agent installation	54
Viewing Local Print Agent log files	54
Changing the Local Print Agent version to install	55
Chapter 4 DCA Settings in PrintFleet Optimizer	56
4.1 Managing DCA installations.....	56
Generating PIN Codes for DCA	56
Managing DCAs.....	57
Adding DCA Users, Assigning Roles, Deleting Users	58
4.2 Troubleshooting stale data issues	60
4.3 Providing technical support.....	60
4.4 Distributing software updates	61

Chapter 1 Introduction

Welcome to the PrintFleet DCA User Guide. This guide covers all aspects of using and administering the PrintFleet Optimizer system, including:

- Using the Data Collection Agent - both DCA 4.x and DCA Pulse
- Managing local devices with Local Print Agent
- DCA Settings in PrintFleet Optimizer

This chapter discusses:

- Device support
- Obtaining software updates
- Contacting Technical Support

The term "DCA" is used throughout this guide to refer to both DCA 4.x and DCA Pulse, unless otherwise specified.

Note

PrintFleet Optimizer 3.9.0 or higher is required to run DCA Pulse.

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.

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

Table 1 lists the data types that the DCA attempts to collect from networked imaging devices during a network scan.

Table 1: Types of data collected by the 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 colour identification
- location
- LCD reading
- MAC address
- device status
- manufacturer
- error codes
- firmware
- toner levels
- miscellaneous (machine specific)
- toner swap history

Your toner swap history is collected and stored in the database. Available as one of our standard reports, your toner swap history allows you to see when the toner has been replaced over a period of time. This functionality gives you greater insight into usage trends and allows Supply Order users to foresee when cartridges will need to be ordered before they run out, thereby facilitating seamless operation while also preventing undue expenditure.

To learn more about reports, refer to **Chapter 3** of the **PrintFleet Optimizer User Manual**.

The Local Print Agent collects the following data types:

- Device driver name
- Device manufacturer
- Communications port

Note

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

1.2 Obtaining software updates

New software releases are available on a periodic basis.

To update DCA 4.x see "Updating DCA 4.x" on page 45.

DCA Pulse updates automatically and requires no user intervention.

1.3 Contacting Technical Support

For system requirements and technical support, contact your PrintFleet distributor.

If you are a direct customer, see Appendix A located at the end of this guide for system requirements. When reporting an issue to PrintFleet Technical Support, please be sure to clearly state the nature of the problem. If applicable, please provide screen shots and supporting log files as well.

Support - North America

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

* Excludes holidays in the province of Ontario, Canada.

Support - Europe, Middle East, Africa

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

** Excludes holidays within Switzerland.

Chapter 2 **Using the Data Collection Agent**

The DCA (Data Collection Agent) 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 Optimizer 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.

DCA 4.x and higher is what most users are accustomed to using. DCA Pulse is PrintFleet's newest software release, which offers next generation solutions to managed print services. DCA Pulse also works alongside DCA 4.x seamlessly and separately, so users can run both applications simultaneously, without risk of complicated or duplicate data.

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:

- DCA Pulse Command Line Options
- Installing and activating the DCA
- Managing the DCA service in Windows
- Configuring communication settings
- Configuring network scan settings
- Viewing queue, archive, and log files with DCA 4.x
- Configuring language and read/write settings in DCA 4.x
- Updating DCA 4.x
- Reviewing the End User License Agreement (EULA): DCA 4.x
- Understanding the network load associated with the DCA
- DCA 4.x Command Line Options
- DCA Pulse Command Line Options

2.1 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 Collection Agent Checklist and Installation Requirements” in Appendix A.

Prior to installing the DCA, you should obtain the information in the following table from the network administrator at the end user 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 48.
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 2000–4000 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 exact procedure you will use to install the DCA depends on which DCA version you would like to use. You have the options of choosing DCA 4.x, or DCA Pulse - PrintFleet’s next generation software.

Regardless, 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 using

DCA 4.x, and to further configure settings, you will need to open the DCA application after installation.

Install DCA 4.x

To install and activate DCA 4.x:

1. Double-click the filename `DCA 4.x.x.x.msi` installation file.
2. The Setup Wizard opens to the Welcome to DCA Setup Wizard screen. Click **Next** to continue.
3. Read through the End-User License Agreement, check **I accept the terms in the License Agreement** and click **Next** to continue. If you do not accept the terms, the installation process will not continue.
4. The DCA Activation box will appear. The DCA will be automatically activated. After successful activation of the DCA, the message "Activation successful. DCA is now running" will be displayed. Click **OK** to complete the installation. The DCA application can be launched from the Windows start menu.

Notes
1) Some virus detection vendors are now using crowd-based information to determine potential threats. Unfortunately, this methodology is prone to producing false positives, particularly for executable files that are not widely distributed among the sample population. As a result, you may find that the DCA installer is being flagged as a possible threat by your virus detection software. When this happens it may be quarantined, which prevents it from being installed. If this occurs, contact your system administrator or virus detection vendor for information about removing it from quarantine.

5. In the Scan Settings screen, you will be shown a list of preconfigured IP ranges that will be added to your default DCA

Downloading the Manual DCA Installer

network scan. This can be changed after installation is complete if necessary. Click **Next**.

6. 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. See "Enabling Intelligent Update" on page 16.
7. In the Setup is Complete screen, by default, the **Open the DCA Interface** and **Start the DCA Service** are both selected. Optionally, you can turn off one or both of these options. Click **Finish**.

Important: DCA activation must be completed before you can successfully use the PrintFleet DCA application. If you attempt to use DCA functions before the activation is finished, you will receive a message asking you to wait until activation is complete.

At some point over the life of the DCA 4.x 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 **Administration** menu, click **DCAs**. The **DCAs** page appears.
2. In the **Group** box, select a DCA group.
All DCAs associated with this group are listed on the **DCAs** page.
3. In the **DCA** column, select the DCA that you want to reactivate. The **DCA Detail** page appears.
4. Click **Reactivate DCA**.
5. You will receive this warning message: "The DCA has reported within the last three days. Are you sure you want to reactivate? The DCA will deactivate and will be assigned a new pin pending activation." Select either **Cancel** or **Reactivate DCA**.
6. Log on to the DCA application to configure the reactivation.

If you are dealing with complex and highly personalized networks, then you may want to download the manual DCA installer. Doing this will allow you to change default installation settings, like installation path within the PrintFleet Optimizer server.

To download the Manual DCA Installer:

1. Select the **Administration** option on the Home Page, or from the list of tabs at the top left corner of your

screen.

2. Select **DCAs**.
3. Select the DCA for which you would like to download the Manual DCA Installer.
4. Check the **Manual Installer** box under the DCA Client Installer button. The button will now read, "Manual DCA Installer". Click to begin download.
5. Once the download is complete, the DCA Setup Wizard will prompt you to personalize the installation. Click **Next** to continue, or **Cancel** to exit.
6. When re-running the DCA Installer, you will have the options to **Modify** the way DCA features are installed, **Repair** errors in the recent installation, and to **Remove DCA** from your computer. Click the "Modify", "Repair" or "Remove" icon to select the operation you would like to perform.

Auto-upgrade DCA 4.x to DCA Pulse

DCA (Auto update)

Overview **Config** Upgrade

Auto upgrade to DCA Pulse is available. [More info](#)

Created 33 minutes ago

Status **OK**. Last reported 4 minutes ago

Group PFV-

Expiry ☒ Never

Version **4.5.0.30612**

DCA software is up to date

Host Info WORKGROUP\

Config No changes queued

Last modified 18 minutes ago in the DCA client

You will have the ability to auto-upgrade DCA 4.x to **DCA Pulse**:

1. Auto install on same device.
2. Manual install.

If the current DCA 4.x is version 4.5 or higher you will have the ability to use the auto-install option.

DCA (Auto update)

Overview **Config** Upgrade

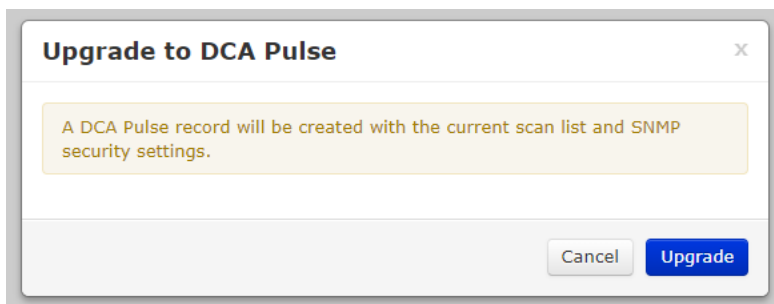
DCA Pulse Name

Upgrade type ☒ Auto install on same PC

DCA Pulse will be queued to automatically install on the same machine as DCA 4.

☐ Manual install

1. Select Upgrade to DCA Pulse button.
2. The system will create a new DCA Pulse with the same scan list and SNMP settings. The new DCA Pulse will have the same name as the original DCA 4.x but will include (Pulse).



3. After clicking on Upgrade the upgrade will be queued for installaion.

DCA (Auto update)

[Overview](#) [Config](#) [Associated DCA Pulse](#)

DCA Pulse Name [DCA \(Auto update\) \(Pulse\)](#)

Upgrade Status DCA Pulse is queued to auto install the next time DCA 4 checks in for an upgrade.

DCA (Auto update)

[Overview](#) [Config](#)

[Click here to see the associated DCA Pulse.](#) Data reported by this DCA 4 is only used if a device is not monitored by the associated DCA Pulse.

Created **an hour ago**

Status **OK. Last reported 23 minutes ago**

Group **PFV-**

Expiry ☒ Never

Version **4.5.0.30612**

DCA software is up to date

Host Info **WORKGROUP**

Config **No changes queued**

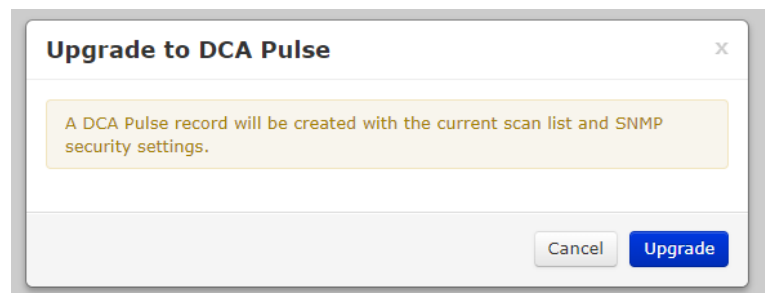
Last modified an hour ago in the DCA client

4. After a successful installation the DCAs will be associated.


To use the manual upgrade function:

1. Select More info or click on the Upgrade Tab.
2. Select the requested Upgrade type.

3. Select Upgrade to DCA Pulse button.
4. The system will create a new DCA Pulse with the same scan list and SNMP settings. The new DCA Pulse will have the same name as the original DCA 4.x including (Pulse).



5. After clicking on Upgrade the DCA Pulse download link will be available to be downloaded and installed manually.

DCA (Manual update) (Pulse)  Delete DCA

Activation **Config** Associated DCA 4

DCA Activation
Please complete the DCA setup by activating the client software. [More info](#)

Server Setup

Group PFV-


Expiry ☒ Never

Device Manufacturer Extensions

☒ HP SDS ☐ Enable (Windows only)
☐ Disable

Client Setup


Download v1.2.4.5118 GA Other Downloads ▾

Activation PIN P3759EP78V6Y 


Send the download link via email:

Email To Send

6. After the successful installation the DCA's will be associated.

DCA (Auto update)  Disable Reactivate DCA Delete DCA

Overview **Config**

 Click here to see the associated DCA Pulse. Data reported by this DCA 4 is only used if a device is not monitored by the associated DCA Pulse.

Created an hour ago

Status OK. Last reported 23 minutes ago

Group PFV-

Expiry ☒ Never

Version 4.5.0.30612 ▾

☒ DCA software is up to date

Host Info WORKGROUP\

Config No changes queued
Last modified an hour ago in the DCA client

Installing DCA Pulse

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

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

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

Note

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

Procedure

1. On the **Administration** menu, click **DCAs**.
The **DCAs** page appears.
2. Click **New DCA**.
3. On the Create DCA page, **Server Setup** section, click **Create New Group**.
4. In the **Parent** group box, select an existing group.
5. In the **Create New Group** section, do the following:
 - In the **Type** box, select a type of group that you want to create. The type can be a dealer, distributor, or customer.

- In the **Name** box, enter a name for the group that you want to create.
6. In the **Name** box, enter a name for a new DCA.
 7. In the **Expiry** area, do one of the following:
 - If you do not want the DCA to expire, select the **Never** check box. The date in the **Expiry** area is only associated with the DCA. It does not affect the DCA group.
 - To set a date for the DCA to expire, clear the **Expiry** check box, click in the date box, and select a date in the calendar. You can also manually enter the date using the format: *dd-mm-yyyy*.
 - At this point you have the option to choose to install Pulse or 4.x under **Client Setup**. Select DCA 4.x or DCA Pulse.
 - Click the **Override Activation PIN** box if you wish to insert a prefixed PIN.
 - Click **Create DCA**.
 - Unclick the **Expiry** box if you wish to set an expiration date for the DCA.
 - In the **Device Manufacturer Extension** tab you have the option to pre-register the HP Smart Device Services (SDS) option. For more information on the remote device management capabilities of HP SDS, see "Working with HP Smart Device Services" in section 2.2 of the PrintFleet Optimizer 3.10.0 or higher user guide.
 - DCA Pulse will give you the option to Override the activation pin with a self-defined one.
 - The installation will recommend a platform based on the operating system you are currently using. If PrintFleet Optimizer can not detect the operating system, it will provide a drop-down list with options, including Windows, Linux versions and macOS. Select the platform on which you would like to run Pulse. Windows is the default selection, including Linux versions and macOS.

Download [v0.2.0.3070 \(GA\) Windows](#) Other Platforms ▾

Activation PIN **P33KLLLCM3QV**

Send the download link via email

Email To

GA v0.2.0.3070

- Linux-armv7l
- Linux-x86_64
- MacOSX-x86_64
- Windows

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

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

Note

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

Installing DCA Pulse on macOS

For macOS install instructions, click the blue download link in the **Activation** tab of the **DCA Detail** page.

Home | Device Views | Reports | Alerts | Settings | Administration

Administration > DCAs > DCA Detail

Test ☒ [Delete DCA](#)

Activation [Config](#)

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

Server Setup

Group ☒

Expiry ☒ Never

Device Manufacturer Extensions

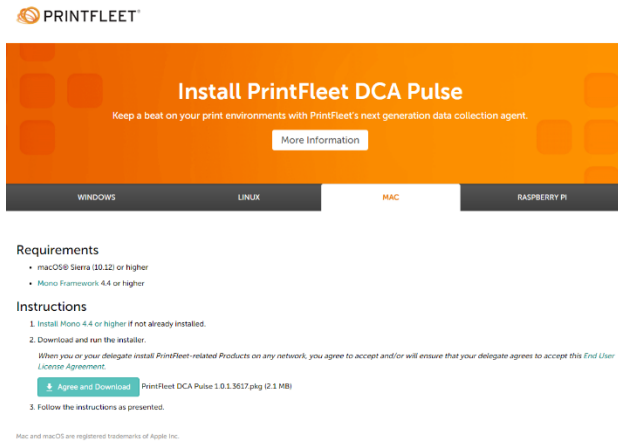
☒ HP SDS ☐ Enable (Windows only)
☐ Disable

Client Setup

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

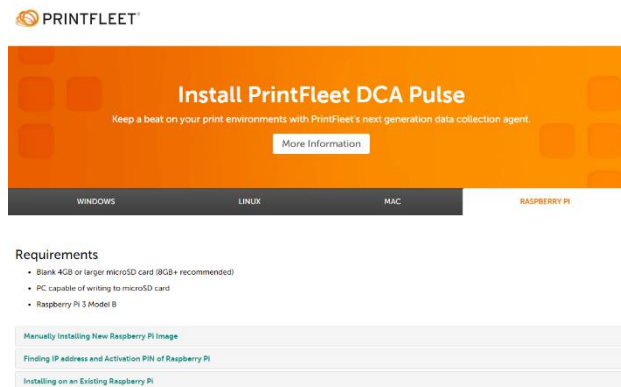
Activation PIN **P373ES3N7XH6** ☒

A new tab will open in your browser with download instructions for the available platforms. Select the **Mac** tab for macOS install requirements and instructions.



Installing DCA Pulse on Raspberry Pi

For a step-by-step guide to installing DCA Pulse on Raspberry Pi, click the blue download link in the **Activation** tab of the **DCA Detail** page.



A new tab will open in your browser with download instructions for the available platforms. Select the **Raspberry Pi** tab for install requirements and instructions on installing DCA Pulse on an existing Raspberry Pi device, installing a new Raspberry Pi image, and how to find the IP address and Activation PIN of the Raspberry Pi.

2.2 Managing the DCA service in Windows

The DCA runs as a Windows service by default. DCA Pulse can also run on select Linux and Mac versions, and can be installed on Raspberry Pi. Alternatively, the DCA can be set up as a scheduled task.

Note

For managing the DCA Service under Linux, Raspberry PI and MacOS, please reference your specific operating system user guides.

Installing and starting DCA 4.x 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.

The DCA service starts automatically.

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.

Deleting a DCA

There are a number of reasons you may want to delete a DCA, including when a DCA is created by mistake, when a DCA is a duplicate, or when a DCA is no longer active or relevant.

To delete a DCA:

1. Select the **Administration** option on the **Home Page**, or from the list of tabs at the top left corner of your screen.
2. Select **DCAs**.
3. Chose the DCA you would like to delete from the **Group** drop down menu.
4. Once the DCA list appears, click on the DCA you would like to delete. This will take you to a screen that shows you the DCA details.
5. Select the red **Delete DCA** button.
6. Confirm you would like to delete the DCA by clicking on **Yes I'm sure, delete this DCA**. Select **Cancel** if you do not wish to delete the DCA.

Setting up DCA 4.x as a scheduled task

To set up DCA 4.x as a scheduled task instead of a service, you must first uninstall the DCA service, and then create the DCA scheduled task. The procedure for creating a scheduled task varies according to your operating system.

To uninstall the DCA service:

- In the **Status** tab, click **Options** and select **Uninstall**.

To create a scheduled task for the DCA using Windows 7, 8, 10, Windows Server 2008 R2, 2012 and 2016:

1. Navigate to **Administrative Tools**, and open **Task Scheduler**.
2. In **Task Scheduler**, from the **Action** menu, click **Create Task**.
3. In the **Create Task** dialog box, on the **General** tab, in the **Name** box, type a recognizable name for the task (such as DCATask).
4. In the **Security options** area:
 - Select **Run whether user is logged in or not**.
 - Select **Run with highest privileges**.
5. Click the **Triggers** tab.
6. On the **Triggers** page, click **New**. The **New Trigger** dialog box opens.

7. In the **New Trigger** dialog box:
 - In the **Settings** area, select **Daily**.
 - In the **Advanced Settings** area, select the **Repeat task every** check box, choose **30 minutes** from the drop-down list, and set the duration to **Indefinitely**.
 - Also in the **Advanced Settings** area, select the **Enabled** check box.
 - Click **OK**.
8. Click the **Actions** tab.
9. On the **Actions** page, click **New**. The **New Action** dialog box opens.
10. In the **New Action** dialog box:
 - In the **Settings** area, use the **Browse** button to navigate to and select the PrinterDCAService.exe file.
 - In the **Add Arguments** box, type *commandline*.
 - Click **OK**.
11. Click the **Settings** tab.
12. On the **Settings** page, clear the **Stop the task if it runs longer than** check box.
13. Click **OK**.

2.3 Configuring communication settings

During DCA 4.x 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.

Note	DCA Pulse will always and only establish through HTTPS. Any mention of HTTP only applies to DCA 4.x or higher.
-------------	--

Changing and testing the communication method and port

There are two methods the DCA 4.x 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 DCA 4.x 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 17.

Using proxy settings with DCA 4.x

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.

Note

Each Windows login account has its own proxy configuration. When the **Use Windows proxy settings** option is selected, the DCA service and the DCA application GUI each use their own configuration. This can result in different settings between when a user runs the DCA application and when the service runs using local system account settings.

To use a manual proxy configuration:

1. Under the **Communication** tab of the DCA, in the **Proxy Configuration** area, 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, select the **Authentication** check box, and then do one of the following:
 - Select **Default** to use the authentication currently being used on the computer installed with the DCA.
 - Select **Custom**, and then click **Load Current** to populate the fields with the current authentication being used by the computer installed with the DCA, or choose the appropriate authentication type from the **Authentication Type** drop-down list and enter username, password, and domain information in the **Username**, **Password**, and **Domain** boxes, respectively.

Note

When you click **Load Current**, all fields will be populated with the exception of the **Password** field, which will be masked with asterisks (*****) if a password has been set, and will be blank if not.

Using proxy settings with DCA Pulse

4. In the **Communication Method** area, click **Test** to verify the settings are working.
5. Click **Save**.

DCA Pulse may connect to its HUB through proxy servers. HUB refers to the central intelligence of DCA Pulse. HUB tells the Pulse component stored in the customer's network what to scan for and when.

Note	DCA Pulse will try and auto-detect proxy settings from the operating system
-------------	---

In order to configure proxy settings yourself, you will need to uncomment (remove the "//" from in front of the setting name) and then provide the desired server, authentication, and domain. The file can be found:

- Windows: c:\ProgramData\PrintFleet DCA Pulse\dcapulse.config
- Mac: /Library/Preferences/com.printfleet.dcapulse.config
- Raspberry: /boot/dcapulse.config
- Linux: ~/.dca-pulse/dcapulse.config

Here is an example:

```
==== PROXY CONFIGURATION =====

By default, DCA Pulse auto-detects proxy settings from the OS.
It is also possible to explicitly specify proxy settings to use, below.

Address of explicitly-specified proxy server.
ProxyServer: https://qa-skealey.ad.printfleet.com/

User used for authentication. Only used if ProxyServer is set. If not set, default credentials are
ProxyUser: skealey@printfleet.com
Password for ProxyUser. Required if ProxyUser is set.
ProxyUserPassword: MySuperIncrediblyLongAndRidiculouslyUncrackablePassword
Domain for ProxyUser. Optional, but only used if ProxyUser is set.
ProxyUserDomain: PRINTFLEET
```

Changing the web service settings

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. By default, the **Web Service Discovery** timeout is 5000 milliseconds; if necessary, the discovery timeout can be increased or decreased.

Note	During the web service discovery a DNS lookup function is used to look for a DNS TXT record.
-------------	--

To change the web service discovery timeout:

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

By default, the DCA determines the location of the PrintFleet Optimizer web services by performing a web service discovery using the domain name you specified when setting up PrintFleet Optimizer. If you subsequently change your domain name, you can add a DNS TXT record in which you can specify the new location of the web services. The next time the DCA performs the web service discovery it will detect the new location.

To change the web service location:

- Create a DNS TXT record, including either of the following:
 - dca4ws=http://*your_new_domain*/PFE_WS/
 - dca4ws=https://*your_new_domain*/PFE_WS/
 where *your_new_domain* is your new domain address (such as mycompany.com).

Note

The web service location is not stored by the DCA, so the DNS TXT record will need to remain.

Enabling Intelligent Update

When Intelligent Update is enabled, the PrintFleet administrator can remotely update and perform other remote actions on the DCA. 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, select the **Enable Intelligent Update** check box.
2. Click **Save**.

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 13) and configuring proxy settings if necessary (see “Using proxy settings with DCA 4.x” on page 14), 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. Note: DCA Pulse only supports HTTPS.
the port you have selected is open on the network.	have the network administrator open the selected port.
the PrintFleet distributor has a valid SSL security certificate, if you are attempting to send via HTTPS.	see the <i>PrintFleet Optimizer User Guide</i> for instructions on setting up a proper 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 4.
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.

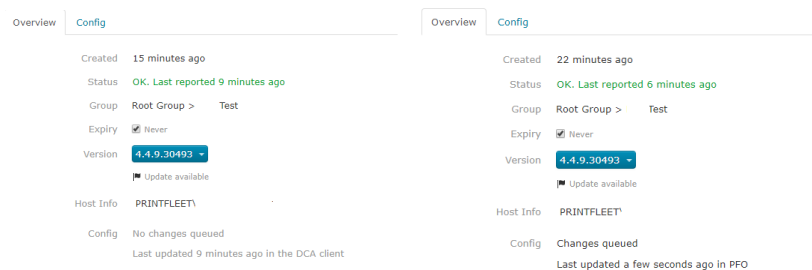
Configuring network scan settings

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.

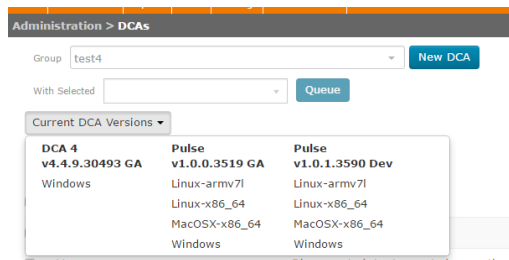
Network scan settings are independent of communication settings, which specify how the DCA will communicate with the central server, and if and how the central server can communicate with the DCA and/or a specific device on the network (see “Configuring communication settings” on page 13).

DCA 4.x and DCA Pulse have different scan configuration options. Pulse offers enhanced scan settings, allowing users to set more customized scan intervals. The process for accessing your scan settings is the same for DCA 4.x and DCA Pulse, but what and how you can configure settings is quite different, as outlined below.

The **Overview** tab of the **DCA Detail** page shows when the configuration was last updated and whether the configuration change came from PFO or the DCA 4.x user interface.



The **Overview** tab of the **DCA Detail** page we will show the current versions of the DCAs.



2.4 DCA 4.x: 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`.

Create new scan profile

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**. A **Copy Current Profile?** dialog opens.

3. In the **Copy Current Profile?** dialog, do one of the following:
 - Click **Yes** if you want to copy the settings from the **General**, **Advanced**, and **Local** tabs of the current profile.
 - Click **No** if you want to manually configure all settings under the **General**, **Advanced**, and **Local** tabs.
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 "DCA 4.x: Managing Scan Profiles" on page 18.
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), select **Default Range**, and then select either **From Active Directory** or the applicable network card for the system installed with the DCA.
 - To specify a range of IP addresses, 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, select **IP Address** and enter the IP address in the box.
 - To specify a hostname, 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 "DCA 4.x: Managing Scan Profiles" on page 18.
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, select the item, and then click **Remove**.
 - To remove every item from the scan range, click **Clear**, then click **Yes** in the **Clear Scan List?** dialog that opens.
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 "DCA 4.x: Managing Scan Profiles" on page 18.
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 "DCA 4.x: Managing Scan Profiles" on page 18.
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**.

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 48.

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 "DCA 4.x: Managing Scan Profiles" on page 18.

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 "DCA 4.x: Managing Scan Profiles" on page 18.
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 "DCA 4.x: Managing Scan Profiles" on page 18.
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 "DCA 4.x: Managing Scan Profiles" on page 18.

2. Under the **General** tab, in the **Scanning Options** area, click **Enable Rapid Scan**.
3. Click **Save**.

The number of scan threads can be controlled using the **Number of scan threads** box in the **Miscellaneous** area on the **Advanced** tab. The setting defaults to a reasonable value for the current system.

Enabling Printer Job Language (PJL)

Printer Job Language is an additional method that can be used to obtain information from devices connected to HP Jet Direct servers.

Warning

Enabling PJL can result in print jobs being sent to dot matrix and other old model or special use printers. Using PJL will result in a limited amount of information being collected from some devices connected to HP JetDirect print servers.

To enable PJL:

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 "DCA 4.x: Managing Scan Profiles" on page 18.
2. Under the **General** tab, in the **Scanning Options** area, click **Enable PJL**.
3. Click **Save**.

Setting the scan interval

The scan interval determines how often the DCA will scan the network. The default scan interval is 60 minutes.

It is generally not useful to set a scan interval for more than every 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.

Note that the frequency with which files are transmitted to your PrintFleet server is independent of the scan interval. By default, the DCA will perform a check every 5 seconds for any queued files awaiting transmission. If there are any queued files, the DCA will attempt to transmit them to your PrintFleet server. In the event that the transmission of a file is unsuccessful, the DCA will not attempt to transmit any other files, but will wait 30 seconds and then attempt the transmission of the file again. It will automatically continue to extend the retrial interval by 30 second increments as necessary up to a maximum of 5 minutes. From that point the DCA will make an attempt every 5 minutes to transmit the file until it is successful, at which point it reverts back to the default 5 second interval and proceeds to transmit any other queued files. This

automatic throttling behavior prevents your PrintFleet server from becoming overwhelmed by requests when it is experiencing problems.

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 "DCA 4.x: Managing Scan Profiles" on page 18.
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**.

If necessary, you can force the DCA to start scanning immediately, regardless of the current scan interval. You might do this if you have made changes to the DCA configuration and want to immediately see the result of those changes without waiting for the next scheduled scan.

To force an immediate 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 "DCA 4.x: Managing Scan Profiles" on page 18.
2. At the bottom of the DCA screen, click **Force Scan**.

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 5000 milliseconds.

The network timeout only needs to be adjusted if the DCA is not discovering networked devices. If, when you perform a DCA scan, certain networked devices are not being discovered, you may need to increase the network timeout (for example, you might try doubling it to 10,000 milliseconds). However, the higher the network timeout is set, the longer the DCA scan will take.

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 "DCA 4.x: Managing Scan Profiles" on page 18.
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**.

Note

This setting only affects how long the DCA will wait for the initial discovery of networked devices. For each printer that has been discovered the DCA will wait up to 60 seconds to receive complete information from the device.

Setting 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 30,000 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 48.

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 "DCA 4.x: Managing Scan Profiles" on page 18.
2. Under the **General** tab, in the **Transmission Options** area, type or select the desired Local Print Agent timeout, in milliseconds, in the **Local 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. By default, this value is set to 5. 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 "DCA 4.x: Managing Scan Profiles" on page 18.
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 "DCA 4.x: Managing Scan Profiles" on page 18.
2. Under the **Advanced** tab, in the **Focus Scan Options** area, 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 "DCA 4.x: Managing Scan Profiles" on page 18.
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, select a previously entered community string, and then click **Remove**.

Note

Although it is possible to remove the `public` community string, you should only do so if you know that all of the devices you want to monitor are accessible via custom community strings. If you remove the `public` community string, a **Fix** link will automatically appear below the list to allow you to replace the `public` community string later if necessary.

- 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**.

To replace the public community string 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 "DCA 4.x: Managing Scan Profiles" on page 18.
2. On the **Advanced** tab, in the **SNMP Community Strings** area, click **Fix**. The `public` community string will reappear in the list and the **Fix** link will disappear.
3. Click **Save**.

Using SNMP Version 3

By default, the DCA communicates with devices using SNMP versions 1. If you want, you can have the DCA use SNMP version 3 instead when communicating with devices that support SNMP version 3. The primary benefit to using SNMP version 3 is that it supports authentication (ensures that the message is from a valid source) and privacy (encrypts the content of a packet to prevent snooping by an unauthorized source). Conversely, the use of these additional security options typically results in the communication being slower, so it takes longer to scan devices that use SNMP version 3.

SNMP version 3 can be used with three different security levels:

- **NoAuthNoPriv**—This uses neither authentication nor privacy, so in terms of security is the same as just using SNMP version 1.
- **AuthNoPriv**—This uses authentication but not privacy, and is still relatively quick.
- **AuthPriv**—This uses both authentication and privacy. This is the slowest mode, but the only one that offers encryption.

These three levels are reflected in the options available through the DCA user interface.

Note

Enabling SNMP version 3 in the DCA will have no significant effect on devices that do not support SNMP version 3. When this option is enabled the DCA will first attempt to communicate with each specified IP address using SNMP version 3. For any addresses that do not respond, the DCA will then automatically revert to using the previous SNMP version.

To have the DCA use SNMP Version 3:

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 "DCA 4.x: Managing Scan Profiles" on page 18.
2. Under the **Advanced** tab, in the **SNMP Version 3** area, select the **Enabled** check box.
3. If you want to use authentication:
 - Select the authentication protocol you want to use from the **Auth Protocol** drop-down list.
 - In the **Auth User** box, type the name of the user you want to use to authenticate against.
 - In the **Auth Password** box, type the password for the authentication protocol. Note that each character of your password will be masked by an asterisk (*) to help ensure security.
4. If you also want to use privacy:
 - Select the privacy protocol you want to use from the **Priv Protocol** drop-down list.
 - In the **Priv Password** box, type the password for the privacy protocol. Note that each character of your password will be masked by an asterisk (*) to help ensure security.
5. If a Context Name or ID is required, type the identifier in the **Context Name** box.
6. Click **Save**.

Note

An individual scan profile in DCA can only specify one security level, and within that level can only specify one combination of authentication and privacy protocols. If you need to use different security levels, or different combinations of protocols, for the devices you need to scan, you will have to create a separate scan profile for each such combination you require.

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.)
- Password. Each character of your password will be masked by an asterisk (*) to help ensure security.

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 "DCA 4.x: Managing Scan Profiles" on page 18.
2. Under the **Advanced** tab, in the **Privacy Options** area, do one or more of the following:
 - Select the **Enable IP Masking** check box to mask device IP addresses.
 - Select the **Enable Phone-Number Masking** check box to mask telephone numbers collected from devices (masked by default).
 - Select the **Enable DCA Host Info Masking** check box to mask DCA host system information.
3. Click **Save**.

Enabling SNMP traps

SNMP traps are notifications generated by a device. Using SNMP traps can help ensure you have the most current device information without having to continuously request information. For example, if a device experiences an error, by enabling SNMP traps, the DCA can be notified of the error immediately instead of waiting until the next 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.

You also need to create alert definitions specifying the error conditions you want to watch for, and ensure those definitions are applied to the groups or devices for which the SNMP traps were enabled.

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 be sent to the central server as soon as possible. Once the server has processed the information, and performs the next scheduled check to determine whether the conditions in any alert definitions have

been met, the corresponding alert event will be created in PrintFleet Optimizer.

Notes

When a trap is detected, the DCA simply registers that the event occurred and initiates its own scan to collect information from the device; any other information provided by the device as part of the trap notification is ignored.

The use of SNMP traps is not supported for devices using SNMP version 3.

The DCA service will not be able to listen for traps if port 162 is already in use by another process.

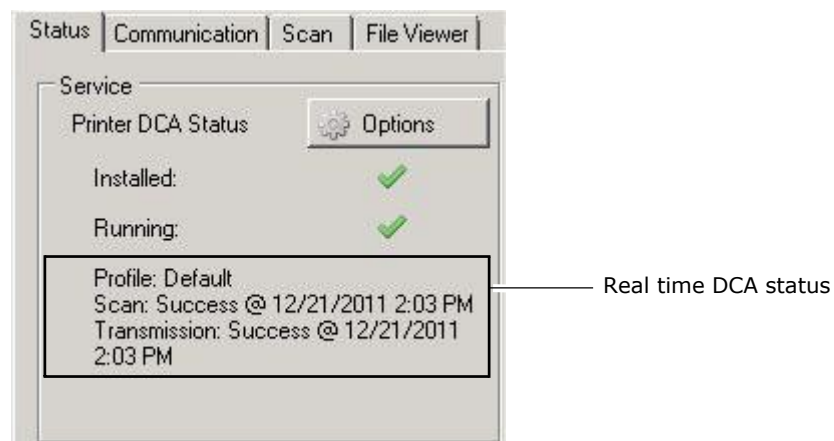
Check the log after starting up the DCA service to see if there are any issues with receiving traps.

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 "DCA 4.x: Managing Scan Profiles" on page 18.
2. Under the **Advanced** tab, in the **Miscellaneous** area, 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**.

Setting the WebPage timeout

The **WebPage Timeout** setting control how long the DCA waits if any webpage data scraping is done. By default, this value is set to 7500 milliseconds. Increasing the value may increase the completeness of a DCA scan, but will also increase the amount of time it takes to complete a network scan.

To change the WebPage timeout value:

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 "DCA 4.x: Managing Scan Profiles" on page 18.
2. Under the **Advanced** tab, in the **Miscellaneous** area, type or select the new timeout value in the **WebPage Timeout** box.
3. Click **Save**.

2.5 Managing Scan Configuration

DCA 4.x and DCA Pulse facilitate quick and easy configuration that allows for more customized scan settings and the collection of more meaningful and valuable data.

Note

All configuration for DCA Pulse is done in PrintFleet Optimizer.

Adding a Scan Range

DCA 4.x and DCA Pulse acquire the IP range of where the DCA is installed upon activation. If you wish to add a different scan range, follow these steps:

Procedure

1. On the **Administration** menu, click **DCAs**.
The **DCAs** page appears.
2. In the **Group** box, select a DCA group.
All DCAs associated with this group are listed on the **DCAs** page.
3. In the **DCA** column, select a DCA created for the device.
The **DCA Detail** page appears.
4. Click the **Config** tab and then click the **Scan List** tab.
5. In the **Scan List Editor** box, you can add a different range and save it. The scan will be then automatically be edited and updated to reflect the new range.

Note

If you want to set multiple IP addresses or multiple IP ranges, you can enter the values in bulk on the **Scan List Editor** tab.

Configuring Scan Intervals

DCA Pulse allows users to set a separate scan interval for Discovery, Meters, Supplies, Errors and Attributes. The ability to customize

how often you receive specific types information both simplifies and maximizes the power of Pulse, since you'll be getting the data you want, when you want it - and only then. This dramatically cuts down on slow interval times.

Procedure

1. On the **Administration** menu, click **DCAs**.
The **DCAs** page appears.
2. In the **Group** box, select a DCA group.
All DCAs associated with this group are listed on the **DCAs** page.
3. In the **DCA** column, select a DCA created for the device.
The **DCA Detail** page appears.
4. Click the **Config** tab and then click the **Scan Intervals** tab.

Scan List	Scan Intervals	Security	Communication	Log
Discovery	<input type="text" value="30"/> minutes	Errors	<input type="text" value="60"/> seconds	
Meters	<input type="text" value="120"/> minutes	Attributes	<input type="text" value="360"/> minutes	
Supplies	<input type="text" value="60"/> minutes			

The scan intervals are set to their respective default settings. To change these settings, type in the time you would like to establish as your customized interval.

Note

The minimum and maximum time for everything except Errors is 10 minutes MIN and 720 minutes MAX. Errors has a MIN of 30 seconds, and a MAX 600 seconds.

Configuring Security: SNMP Version 1/2

By default, DCA Pulse communicates with devices using SNMP version 1/2. If you wish to use this security protocol, do the following:

Procedure

1. On the **Administration** menu, click **DCAs**.
The **DCAs** page appears.
2. In the **Group** box, select a DCA group.
All DCAs associated with this group are listed on the **DCAs** page.
3. In the **DCA** column, select a DCA.
The **DCA Detail** page appears.

4. Click the **Config** tab.
5. Click the **Security** tab.
6. Click **Add SNMP Profile** button.
7. A pop-up will appear.



SNMP Version

☒ 1/2

☐ 3

Community Strings

public

Enter one community string per line.

By default, **SNMP Version 1/2** will be selected. Enter **Community Strings** in the text box. Community strings act as passwords on networked devices that limit access via SNMP. Since DCA Pulse uses SNMP to collect data from devices, any custom community strings on printing devices put in place by network administrators can be manually entered in the DCA to allow it SNMP access to the device. Most devices have a community string of `public`, and the DCA stores a community string of `public` by default.

Configuring Security: SNMP Version 3

If you want, you can have DCA Pulse use SNMP version 3 instead when communicating with devices that support SNMP version 3. The primary benefit to using SNMP version 3 is that it supports authentication (ensures that the message is from a valid source) and privacy (encrypts the content of a packet to prevent snooping by an unauthorized source). Conversely, the use of these additional security options typically results in the communication being slower, so it takes longer to scan devices that use SNMP version 3.

However, since DCA Pulse communicates with HTTPS rather than HTTP, you can expect this update to help expedite communication, while also providing an added layer of security.

SNMP version 3 can be used with three different security levels:

- **NoAuthNoPriv**—This uses neither authentication nor privacy, so in terms of security is the same as just using SNMP version 1.
- **AuthNoPriv**—This uses authentication but not privacy, and is still relatively quick.
- **AuthPriv**—This uses both authentication and privacy. This is the slowest mode, but the only one that offers encryption.

These three levels are reflected in the options available through the PrintFleet Optimizer server user interface.

Note

Enabling SNMP version 3 in the DCA will have no significant effect on devices that do not support SNMP version 3. When this option is enabled the DCA will first attempt to communicate with each specified IP address using SNMP version 3. For any addresses that do not respond, the DCA will then automatically revert to using the previous SNMP version.

Procedure

1. On the **Administration** menu, click **DCAs**.
The **DCAs** page appears.
2. In the **Group** box, select a DCA group.
All DCAs associated with this group are listed on the **DCAs** page.
3. In the **DCA** column, select a DCA.
The **DCA Detail** page appears.
4. Click the **Config** tab.
5. Click the **Security** tab.
6. The default setting is **SNMP Version 1/2**. If you wish to select SNMP Version 3, click **Add SNMP Profile**.
7. A pop-up screen will appear with default SNMP 1/2 selected. Select 3.

Add SNMP Profile

SNMP Version

☐ 1/2

☒ 3

Context Name

User

Security Level

NoAuthNoPriv ▼

Add SNMP Profile Cancel

8. To complete set up, do the following:
 - In the **User** box, enter the name of the user you want to use to authenticate against.
 - Select the authentication and privacy protocol you want to use from the **Security Level** list.

9. If a Context Name or ID is required, enter the identifier in the **Context name** box.
10. Click **Save Changes**.

View Security Configuration Details

To view the details of a SNMP profile, do the following:

Procedure

1. On the **Administration** menu, click **DCAs**.
The **DCAs** page appears.
2. In the **Group** box, select a DCA group.
All DCAs associated with this group are listed on the **DCAs** page.
3. In the **DCA** column, select a DCA.
The **DCA Detail** page appears.
4. Click the **Config** tab.
5. Click the **Security** tab.
6. Click the table icon.
7. A pop-up screen will appear with the relevant SNMP details.

Delete a SNMP Profile

To delete a SNMP profile, do the following:

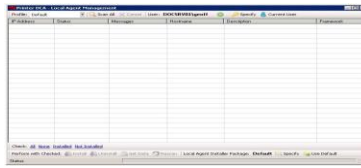
Procedure

1. On the **Administration** menu, click **DCAs**.
The **DCAs** page appears.
2. In the **Group** box, select a DCA group.
All DCAs associated with this group are listed on the **DCAs** page.
3. In the **DCA** column, select a DCA.
The **DCA Detail** page appears.
4. Click the **Config** tab.
5. Click the **Security** tab.
6. Click on the "x" button beside the profile you wish to remove to delete.

Configuring Communication

Configuring communication settings allows you to control the frequency with which your DCA communications with devices. This

can vary widely depending on the nature of your client's network and the unique demands of their business.



DCA Pulse allows you to configure all your communication settings in one place, thereby streamlining and simplifying the process.

Procedure

1. On the **Administration** menu, click **DCAs**.
The **DCAs** page appears.
 2. In the **Group** box, select a DCA group.
All DCAs associated with this group are listed on the **DCAs** page.
 3. In the **DCA** column, select a DCA created for the device.
The **DCA Detail** page appears.
- Click the **Config** tab and then click the **Communication** tab.

[Scan List](#)
[Scan Intervals](#)
[Security](#)
[Communication](#)
[Log](#)

If a setting is empty, the DCA client will use the value from the config file or the default value.

SNMP Retries	<input type="text" value="2"/>	SNMP Max Concurrent	<input type="text" value="100"/>
SNMP Timeout	<input type="text" value="10000"/> ms	SNMP Max Per Target	<input type="text" value="1"/>
DNS Timeout	<input type="text" value="10000"/> ms	Registry Interval	<input type="text" value="30"/> minutes
Disconnected Device Grace Period	<input type="text" value="60000"/> ms		

Note

Each option is automatically set to its default setting. (As seen in previous image.) Your ability to alter settings is confined to the **maximum** and **minimum** limits outlined below:

SNMP Retries: MAX 10 times, MIN 0 times

SNMP Timeout: MAX 300,000 milliseconds, MIN 500 milliseconds

SNMP Max Concurrent: MAX 1000 requests, MIN 5 requests

DNS Timeout: MAX 300,000 milliseconds, MIN 500 milliseconds

Disconnected Device Grace Period: MAX 300,000 milliseconds, MIN 10,000 milliseconds

SNMP Max Per Target: MAX 10 requests, MIN 1 request

Registry Interval: MAX 90 minutes, MIN 3 minutes

SNMP Retries. The number of SNMP retries entered is the number of times DCA Pulse will attempt to get information from a device that is responding with incomplete or no information. Increasing the number of SNMP retries may increase the completeness of a DCA scan, but will also increase the amount of time it takes to complete a network scan. Each option is automatically set to its default.

SNMP Timeout. The SNMP timeout is the amount of time that DCA Pulse will wait for a networked device to respond back with its information.

The network timeout only needs to be adjusted if the DCA is not discovering networked devices. If, when you perform a DCA scan, certain networked devices are not being discovered, you may need to increase the network timeout (for example, you might try doubling it to 10,000 milliseconds). The higher the network timeout is set, the longer the DCA scan will take.

DNS Timeout. The Pulse client, on the customer's network, communicates with DCA Registry using DNS requests. This setting controls how long the request is expected to wait for a response from the Registry server before the request times out and fails. This setting is set in milliseconds.

Disconnect Device Grace Period. Devices can go off-line for a number of reasons (small blip in the network, the device is unplugged periodically, etc). This setting controls how long Pulse will remember the device before it is considered to be disconnected. Once a device is disconnected, Pulse will stop scanning it.

SNMP Max Concurrent. This setting controls the total amount of SNMP requests that Pulse will send out simultaneously, across all devices.

SNMP Max Per Target. This controls the amount of simultaneous SNMP requests that may be sent to a single device.

Registry Interval. The Registry Interval is the amount of time that Pulse will wait between checking in with a network to determine if it is still live, even if there are no updates.

Configuring Logs

By default, DCA Pulse logs Info, Warnings, Errors, and Fatal. These types of logs are available upon a fresh install with no configuration changes made yet.

Default Log Name	Meaning
Fatal	Used for fatal errors when the application can no longer continue at all. Typically this means the application is exiting (or the ASP.NET Request is ending) prematurely or unexpectedly. To fix a Fatal error, restart the application.
Error	These are recoverable (non-Fatal) errors that are visible to an administrator. Typically entries classified as Error are actionable by a user or an operator in some way.
Warning	Warnings are potential problems and non-actionable errors that don't necessarily require an administrator to act on them. For example, a problem parsing data passed to a web service could cause a Warning log. There isn't anything an administrator can or should do, but it may cause an issue, so it is flagged as a Warning, as opposed to just Info.
Info	Info is for basic informational coarse-grained messages about what the system is doing, and no messages should require the operator to take action. Info is typically the default log level (so only Info or higher will normally be logged).

In addition to these default logs, DCA Pulse offers more advanced logging capabilities than previous DCA versions, giving users the ability to more accurately record, monitor, control and troubleshoot activity within the system.

Here are the new DCA Pulse configuration log options:

(Please see the chart on the next page.)

Log Name	Purpose
Debug	<p>Debug logging expands on information provided in an Info log. For example, when processing items in a file, there may be a single Info message that says the file is being processed, a Debug message that lists the file timestamp and permissions, a Debug message for every item in the file, and a Debug message when the file has been closed.</p> <p>This application is usually only utilized by a developer debugging an application or an advanced user trying to troubleshoot a difficult problem.</p>
Trace Logging	<p>Trace is the highest detail of logging messages. It may include an entry whenever any function in the code is entered or exited, and otherwise expand on the level of detail provided by Debug. It may be wired to <code>System.Diagnostics.Trace</code> (so it receives messages from the framework trace levels as well).</p> <p>Often, Trace will generate an order of magnitude or more log output than even Debug, so should only be enabled by a developer while necessary and turned off afterwards. It's not unusual for Trace to generate several GB of log files in a day.</p>
SNMP Log Level	<p>SNMP logging will log activities that are directly associated with SNMP (requests, responses, etc). When SNMP logging is enabled, it will be stored in a new file with an <code>snmp.log</code> suffix.</p>

(continued)

Log Name	Purpose
Log Stats Intervals	<p>There are Info logs that contain stats that clearly contain information regarding how many data values are being monitored across the amount of devices, how many devices are potentially lacking scan instructions, etc. Log Stats Interval determines how frequently these "stats" are logged inside the log file.</p> <p>Note: the MIN time for this option is 0 seconds, and the MAX is 3200 seconds.</p>

To configuring your Log options, do the following:

Procedure

1. On the **Administration** menu, click **DCAs**.
The **DCAs** page appears.
2. In the **Group** box, select a DCA group.
All DCAs associated with this group are listed on the **DCAs** page.
3. In the **DCA** column, select a DCA.
The **DCA Detail** page appears.
4. Click the **Config** tab.
5. Click the **Log** tab.

Scan List Scan Intervals Security Communication **Log**

If a setting is empty, the DCA client will use the value from the config file or the default value.

Debug Logging:

Trace Logging:

SNMP Log Level:

Log Stats Interval: seconds

The log options are set to their default settings. To change the **Debug**, **Trace** or **SNMP Logging** settings, click on the drop-down menu and select an option.

To adjust **Log Stats Interval**, either manually type in the desired interval time, or hover your mouse over the space after the text box and the up-down arrows will appear.

Note

The **Debug Logging** and **Trace Logging** settings in PrintFleet Optimizer may disable each respective level of logging, with one caveat: when Trace is enabled, Debug will also be enabled, because Trace provides the highest detail of logging available.

2.6 Viewing queue, archive, and log files with DCA 4.x

For troubleshooting purposes, you might want to view DCA 4.x queue, archive, or log files.

Note

DCA Pulse does not have a user interface to view log files. To manually view DCA Pulse client log files - located in OS>ProgramData>PrintFleet>DCA Pulse - open them with a text file editor.

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.).




Note

From DCA you can also view the log files for Local Print Agent using the DCA - Local Agent Management tool. For more information, see "Viewing Local Print Agent log files" on page 52.

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.

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.

2.7 Configuring language and read/write settings in DCA 4.x

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**.
 - In the **Set Password** dialog box, enter the password you want to use to disable read-only mode, and then click **OK**. Note that each character of your password will be masked by an asterisk (*) to help ensure security.

To disable read-only mode:

1. Click **Unlock** in the lower right corner of the DCA.
 - In the **Enter Password** dialog box, enter the password currently set for read-only mode, and then click **OK**. Note that each character of your password will be masked by an asterisk (*) to help ensure security.

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**.
 - In the **Enter Password** dialog box, enter the current password for read-only mode, and then click **OK**. Note that each character of your password will be masked by an asterisk (*) to help ensure security.
 - In the **Set Password** dialog box, enter the desired new password for read-only mode, and then click **OK**. Note that each character of your password will be masked by an asterisk (*) to help ensure security.

2.8 Updating DCA 4.x

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

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.

2.9 Reviewing the End User License Agreement (EULA): DCA 4.x

If necessary, you can access the EULA via the Help menu.

To access the EULA:

- On the **Help** menu, click **Review EULA**. The EULA is displayed. You can review it online, or print it out to review offline.

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

2.11 DCA 4.x Command Line Options

If you want, you can use a command line option to import IP ranges to your DCA scan list. This is the essentially the same as clicking the **Import** button on the **General** tab of the **Scan** tab in the DCA application interface. If your IP ranges change frequently you could set up your system to run this command on a regular basis (say once a day during off hours), thereby ensuring that the IP range information is always current.

Note	This feature clears the existing list prior to import.
-------------	--

To import IP ranges from a command line:

- Use the command `PrinterDCA.Service.exe` with the following options:

- */task*: Currently the only supported task is 'ipimport'. This is case insensitive.
- */file*: Absolute path to file with IP list to import
- */profile*: This is optional; if not included, 'Default' will be used.
- */killgui*: Must be "true", or default of "false" is assumed.

Example:

```
PrinterDCA.Service.exe /task=ipimport /
file=c:\test.txt /profile=test
```

The command will return one of the following error codes (and an appropriate message):

- -1: General failure.
- 0: Successfully imported.
- 1: Malformed input file - not imported.
- 2: Could not find or access file.
- 3: GUI open, could not exclusively lock .pfc config file.

2.12 DCA Pulse Command Line Options

DCA Pulse has a set of configuration options that may be specified within the dcapulse.config file, or may be overwritten by passing in parameters via command line.

The available command line settings and configuration settings are as follows:

Table 5: DCA Pulse Command Line Options

Setting	Description
-s, --force-server	Server HUB to connect to. Overrides Server automatically provided by DCA Registry
--transport	Force transport method for communications, one of: Auto, WebSocket, ServerSentEvents, LongPolling
--force-ranges	Force scan range(s) (one or more: IP, IP range or subnet, separate by spaces)
--snmp-timeout	SNMP Request Timeout (milliseconds)
--snmp-retries	Number of SNMP retries after timeout

Table 5: DCA Pulse Command Line Options

Setting	Description
--dns-timeout	DNS timeout (milliseconds)
-t, --hub-connection-timeout	HUB connection timeout (milliseconds)
--registration-server	DNS registration domain
--registration-interval	DNS registration interval (minutes)
--snmp-max-concurrent	Maximum concurrent SNMP request limit (total)
--snmp-max-per-target	Maximum concurrent SNMP request limit (per target)
--snmp-log-level	SNMP specific log level. One of: Off, Debug, Info. If enabled, logs to {date}.snmp.log
--logs	Path to store log files. A file with the current date will be created in this location
--log-stats-interval	Interval to log stats for (seconds). Set to 0 to disable
--local-web-port	The port the local web server should run on. Set to 'auto' to automatically pick, or 'off' to disable
--auto-update-release-channel	Specify auto-update release channel. One of: GA, Beta, Dev
-c, --config	Path of configuration file to use
--trace	Enable trace level console output
-d, --debug	Enable debug level console output
--help	Display the help screen
--version	Display version information

Table 6: DCA Pulse Configuration File Settings

Setting	Description
EdgeId	Unique ID provided to Pulse clients

Table 6: DCA Pulse Configuration File Settings

Setting	Description
PIN	Populated with a unique PIN if the DCA has yet to be activated
SharedKey	Unique ID provided for authorization purposes
Server	Server with which Pulse communicates
Transport	Desired communication type (long polling, server sent events, web sockets)
ForceScanRange	Desired scan range (overwrites value provided by PrintFleet Enterprise)
SnmpTimeout	Time before SNMP request times out
DnsTimeout	Time before DNS request times out (Pulse communications to registry via DNS requests)
RegistrationInterval	The frequency (minutes) in which Pulse will check in with Registry

Chapter 3 Managing local devices with Local Print Agent

Local Print Agent allows the DCA to obtain information directly from locally connected printing devices. 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 19.
2. Enable the local device scanning option. See "Enabling scanning of network and/or local devices" on page 21.
3. Install Local Print Agent on computers connected to local printers (instructions follow).

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.

Once Local Print Agent is installed, you can monitor how each installation is doing, and make changes as necessary, using the **DCA - Local Agent Management** tool provided with DCA.

3.1 Installing Local Print Agent

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\Program Files (x86)\Printer DCA\support`. 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. See "Performing a Push Install of Local Print Agent" on page 51.

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 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 "DCA 4.x: Managing Scan Profiles" on page 18.
2. Under the **Local** tab, select the **Enable Push Install** check box.
3. In the **Change Push Install Credentials** dialog, 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 `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.

3.2 Managing Local Print Agent

DCA includes a separate user interface called **DCA - Local Agent Management** which you can use to manage Local Print Agent.

Starting the Local Agent Management tool

To start the DCA - Local Agent Management tool:

- From the **Tools** menu in DCA, click **Local Agent Management**. The **DCA - Local Agent Management** window opens.

Scanning for Local Agent installations

Each time you start the **DCA - Local Agent Management** tool, it displays an empty table. To populate the table, you need to perform a scan of the network to locate any Local Agent installations.

To change the active user for Local Agent Management:

1. At the top of the Local Agent Management window click **Specify**. The **Change Push Install Credentials** dialog opens.

2. Use the **Username**, **Password**, and **Domain** boxes to specify the credentials you want to use.
3. Click **OK**. PrintFleet will attempt to validate the credentials you supplied. If successful, a green check mark will appear beside the new user name at the top of the window.

To revert to the current DCA user:

- At the top of the Local Agent Management window click **Current User**.

Changing the active user for Local Agent Management

By default, when performing various functions (such as scanning, installing, and uninstalling) DCA - Local Agent Management uses the same account you had been using in DCA. (The user name is displayed beside User: at the top of the window.)

Interpreting the Local Agent Management scan results

The Local Agent Management table displays one row for each IP address scanned. If necessary, you can click a column heading to sort the table by that column. Each row includes the following information:

- **IP Address**—The IP address that was scanned.
- **Status**—The status of Local Agent for that IP address (either Installed or Not Installed). If Local Agent is installed, the Status column also displays the version number of the installed Local Agent.
- **Messages**—Displays the brief message sent from Local Agent to the DCA regarding the most recent action you performed, such as the last scan, install, or uninstall. The message might indicate some limited error information, or a timeout.
- **Hostname**—The hostname of the computer or device associated with the IP address.
- **Description**—Local Agent Management will try to provide some additional information. The information will vary depending on what object is associated with the IP address. For example, if it is a computer, Local Agent Management will try to determine the operating system running on the computer, and display that (such as Microsoft Windows). If it is a printer, it will display the printer name. Not all IP addresses are associated with a specific object, so in those cases it will simply say **Unknown**. If no response was received from an IP address the description will say **Timed Out**.
- **Framework**—For IP addresses associated with Local Agents, Local Agent Management will try to determine and display the version of the .NET framework that is running. Local Print Agent requires .NET version 2 or higher in order to install and run successfully. For this reason this column is color coded to highlight potential problems: green indicates .NET version 2 or higher, red indicates a .NET version below 2, and yellow indicates an unknown .NET version.

Performing a Push Install of Local Print Agent

You can use Local Agent Management to push an installation of Local Print Agent to selected IP addresses.

To push install Local Print Agent from Local Agent Management:

1. If necessary, populate the Local Agent Management table by performing a scan. See "From the Tools menu in DCA, click Local Agent Management. The DCA - Local Agent Management window opens." on page 49.
2. Do one of the following:
 - Under the **IP Address** column, select the check box beside each IP address where you want to install Local Print Agent, then beside **Perform with Checked:**, click **Install**.
 - Right-click in the row of a specific IP address for which you want to perform an install and choose **Install** from the menu that appears.

Uninstalling Local Print Agent

You can also use Local Agent Management to uninstall Local Print Agent from selected IP addresses.

To uninstall Local Print Agent:

1. If necessary, populate the Local Agent Management table by performing a scan. See "From the Tools menu in DCA, click Local Agent Management. The DCA - Local Agent Management window opens." on page 49.
2. Do one of the following:
 - Under the **IP Address** column, select the check box beside each IP address where you want to uninstall Local Print Agent, then beside **Perform with Checked:**, click **Uninstall**.
 - Right-click in the row of a specific IP address for which you want to perform an uninstall and choose **Uninstall** from the menu that appears.

Checking the data returned by Local Print Agent

At some point you might want to check to see what data Local Print Agent is sending to DCA (and through DCA to PrintFleet Optimizer).

To check the data being sent by Local Print Agent:

1. If necessary, populate the Local Agent Management table by performing a scan. See "From the Tools menu in DCA, click Local Agent Management. The DCA - Local Agent Management window opens." on page 49.
2. Do one of the following:
 - Under the **IP Address** column, select the check box beside each IP address where you want to check the data, then beside **Perform with Checked:**, click **Get Data**.
 - Right-click in the row of a specific IP address for which you want to check the data and choose **Get Data** from the menu that appears.

The data for the selected IP address(es) are displayed in the DCA - File Viewer. You can view the data in either XML or spreadsheet format by clicking the **XML** tab or **CSV** tab respectively.

Rescanning specific IP addresses

If necessary, you can have Local Agent Management rescan one or more IP addresses. You might do this if you are waiting for a recent change to appear (such as a recently installed printer), or to get a result for an IP address that had timed out from a previous scan. You could also just click **Scan All** to scan the entire IP range in the current scan profile, but with a large IP range you might get other IP addresses timing out, so sometimes it helps to rescan just the IP address(es) you are interested in.

To rescan specific IP addresses:

- Do one of the following:
 - Under the **IP Address** column, select the check box beside each IP address you want to rescan, then beside **Perform with Checked:**, click **Rescan**.
 - Right-click in the row of a specific IP address you want to rescan and choose **Rescan** from the menu that appears.

Configuring a Local Print Agent installation

If an IP address has Local Print Agent version 4.1.2 (or later) installed, you can configure that Local Print Agent installation from Local Agent Management. This allows you to suspend the scanning of selected local devices connected to the machine at that address. For example, in some cases a device might print out unwanted pages each time it is scanned. If this occurs, you could easily suspend the scanning for that device.

To configure a Local Print Agent installation:

1. Right-click in the row of a specific IP address you want to configure (and which has version 4.1.2 or later installed), and choose **Configure** from the menu that appears. The **DCA - Local Print Agent Configuration** dialog opens. Any local devices connected to the specified machine will be listed.
2. In the **DCA - Local Print Agent Configuration** dialog, in the **Enable** column, click a check box to toggle the state of the associated device between Enabled (checked) and suspended (cleared).
3. Click **Save Changes**.

Viewing Local Print Agent log files

If necessary you can view the log file for a Local Print Agent from Local Agent Management. The log file records the requests received by the specified Local Print Agent.

To view a Local Print Agent log file:

1. If necessary, populate the Local Agent Management table by performing a scan. See "From the Tools menu in DCA, click Local Agent Management. The DCA - Local Agent Management window opens." on page 49.

2. Right-click in the row of the Local Print Agent for which you want to view the log file, then choose **Get Log Files** from the menu that appears. The **Select A Log Date** dialog box opens.
3. In the **Select A Log Date** dialog box, specify the date of the log file you want to view, then click **Accept**. The log information for the specified date is displayed in your default text viewer (such as Notepad).

Changing the Local Print Agent version to install

Each DCA automatically includes a Local Print Agent that it will use by default for push installs. If necessary, you can select a different Local Print Agent installer to push from Local Agent Management. You might do this if you need a specific Local Print Agent version for an older device (usually as directed by technical support).

To change the Local Print Agent installer to use with Local Agent Management:

1. At the bottom of the Local Agent Management window click **Specify**. The **Locate Local Print Agent Installer** dialog opens.
2. Browse to and select the Local Print Agent installer you want to use.
3. Click **Open**. The text at the bottom of the Local Agent Management window changes from **Default** to **User Specified**. If you hover the mouse over the **User Specified** text, a tooltip will appear indicating the path and file name of the selected Local Print Agent installer.

To revert to the default Local Print Agent installer:

- At the bottom of the Local Agent Management window click **Use Default**.

Chapter 4 DCA Settings in PrintFleet Optimizer

The DCA is one component of the PrintFleet Optimizer system. For this reason, some of the settings which affect the DCA are located in the Administration area in PrintFleet Optimizer. Those settings are documented in the *PrintFleet Optimizer User Guide*, but are referenced here as well for your convenience.

This chapter discusses:

- Managing DCA Installations
- Troubleshooting stale data issues
- Providing technical support
- Distributing software updates

4.1 Managing DCA Installations

Each DCA installation requires a PIN Code to activate to run. These PIN Codes can be generated and managed using PrintFleet Optimizer.

Note

DCA Pulse requires PrintFleet Enterprise 3.9.0 to manage a DCA.

Generating PIN Codes for DCA

To generate a PIN Code for DCA:

1. On the **Administration** menu, select **DCA Administration**, and then click **New DCA**.
2. Select **4.x or greater**.
3. Select the appropriate group from the dropdown list or click **Create New Group** button.
4. Define the DCA information: enter the **DCA Name**. Optionally, set an Expiry date by selecting the calendar button and selecting a date.
5. Click **Create DCA**. The Pending PIN Code is generated and displayed in the DCA Information page's General Information tab. The PIN Code can be emailed to an appropriate person via **Send this PIN via email**. Alternately, the PIN Code can be copied and pasted into the DCA Activation screen. This PIN Code remains visible in the General Information tab while the DCA is in a Pending Activation status. Once this PIN Code is used to activate a DCA client, the DCA has an active status and the PIN Code will no longer be visible.

Note

While DCA Pulse also uses PIN codes, they are embedded into email links and URLs, so there is no need for you to copy and paste.

Managing DCAs

You can check the status of a DCA installation via DCA Listing page. DCA information can be viewed or edited at any time. A DCA can also be deleted, disabled or reactivated. A new PIN code can also be created for a DCA 4.x or greater.

Important: When a DCA expires, is deleted, or is set to inactive, the next time that DCA connects it will effectively go into a state of hibernation. In hibernation, it will not perform any further scans of the network or transmit any files in the queue, but will perform a status check in starting at 45 minutes, then double at increments for up to 24 hours. (So, 45 minutes, 1.5 hours, 3 hours, 6 hours, etc, until it reaches 24 hours.) Checking hibernation mode several times over 24 hours allows for the DCA to quickly and automatically return to normal operations should anything accidentally trigger hibernation.

Causes of hibernation include:

- The DCA record on the server has been set to disabled.
- The DCA record on the server has expired.
- The shared key doesn't match.
- The DCA record was reactivated from a different installed DCA.
- The DCA configuration was copied from a DCA that has already been installed and activated, or the machine the DCA was on was cloned.
- The DCA lookup on the server failed to find a row.
- The record was manually deleted.
- DNS or network configuration issues have caused the wrong server to be presented on the server's hostname.

To check the status of a DCA:

1. On the **Administration** menu, select **DCA**.
2. In the DCA Listing page, the status of the DCA will be visible in the Status column:
 - Pending Activation – PIN Code has not been used to activate DCA client.
 - Active – DCA has been activated using PIN Code.
 - Inactive – the DCA has been set to Inactive or has expired.
 - Disabled - the DCA has not been enabled.
 - Stale - the DCA has not reported for more than three days.
 - Expired - the DCA became invalid after the date of expiry. To help avoid unwanted DCA expiration, refer to the DCA creation date, which you can see in the DCA detail page of any activated DCA. Administration>DCAs.

To view DCA information:

1. On the **Administration** menu, select **DCA**.
2. Click on the DCA name link for the DCA you want to view from the **Data Collection Agent (DCA) Listing**. The DCA Information page's General Information tab is displayed for the selected DCA.

To edit an existing DCA:

1. Click the **Edit** option beside the DCA in the **DCA Listing** page. Alternately, in the DCA Information page, click **Edit**.
2. Make changes to the **DCA Name**, **Group**, or **Expiry Date** fields, and then click **Save**.

To delete an existing DCA:

1. Click the Delete option beside the DCA in the **DCA Listing** page, or in the DCA Information page, click **Delete**.
2. A dialog box prompts you to confirm your wish to delete this DCA.
3. Click **Confirm** to complete the DCA deletion, or **Cancel** to abort the DCA deletion. After deletion, files will not be processed for the DCA, but the DCA will enter a hibernation state. If you want to completely remove the DCA, you will need to uninstall it.

To set a DCA Inactive:

1. In the DCA Information page for an active DCA, click **Set Inactive**.
2. A dialog box prompts you to confirm your wish to set this DCA to Inactive.
3. Click **Confirm** to set to inactive or **Cancel** to abort. With an Inactive status, files will not be processed for the DCA, but the DCA will enter a hibernation state.

To set a DCA Active:

1. In the DCA Information page for an inactive DCA, click **Set Active**. The DCA will have an active status and files will be processed.

To create a new PIN Code for a DCA:

1. In the DCA Information page, click **Create New PIN**.
2. A dialog box prompts you to confirm your wish to create new PIN for the DCA.
3. Click **Confirm** to create a new PIN Code or **Cancel** to abort. The new PIN Code will be generated and the DCA will be in a pending activation state. Until reactivated, files will not be processed for the DCA.

Adding DCA Users, Assigning Roles and Deleting Users

Adding or deleting users from a DCA allows you to specify what role(s) - if any - a user has within the DCA, and by extension, controls what functions they are able to perform.

To add a user to a DCA user:

1. Go the **Administration** tab and select **Users** from the dropdown menu.
2. At the bottom right hand corner of the your screen, you will see a button for **New User**. Click it.
3. Fill out the required information.

On the bottom right corner of your screen you will see the option to **Save** or go **Back**. Select **Save** if you wish to save the user or **Back** to go user main page.

Important: The option to use a default 'start user' is no longer available. Any items associated with this function may not work properly.

To assign a role:

Roles are used to assign permissions to users. One role can be assigned to an unlimited number of users. Users can be assigned multiple roles and can be assigned different roles for different groups. The total set of permissions assigned to a user is the combination of all permissions for all assigned roles.

PrintFleet Enterprise comes with four standard roles already created:

Default. Assigned to all users, and cannot be deleted.

Admin. Provides access to the entire system, and cannot be edited or deleted.

Dealer. Provides dealer level access to the system.

Customer. Provides customer level access to the system.

You can create as many additional roles as needed, and can edit the permissions for any role, with the exception of the Admin role, which always has all permissions. When roles are edited, changes to permissions are made to every user with that role.

Creating a new role

Procedure:

- 1) On the Administration menu, click Roles. The Roles page appears.
- 2) Click New Role. The Role Configuration page appears.
- 3) Under Role Information, do the following:
 - Enter a name for the role in the **Name** box.
 - Enter a description for the role in the **Description** box.
 - Under **Role Permissions**, select each permission you want the role to have.
 - Click **Save**.

For more information on roles, including how to edit and delete them, refer to Chapter 6 in the PrintFleet Enterprise User Guide.

To delete a DCA user:

1. Go the **Administration** tab and select **Users** from the dropdown menu.
2. Either select the user to choose the group the user is a member of from the **Filter by Group** drop down menu.
3. Once you have found the user you would like to delete, select the **Delete** option on the right side of your screen.
4. Before the user is deleted, you will receive a notification informing you that in removing the user from the DCA, alerts

and reports associated with that user will stop relaying information. While they will still exist, you will cease to receive potentially important information because they no longer have a specified host. This could impact business processes. If business processes are related to this account, we recommend that you assign that user's account another user **or rename** the account to reflect the function of the reports/alerts. By doing this, you will still receive data. You can contact your System Administrator if you need help, or **Confirm** or **Cancel** the delete.

4.2 Troubleshooting stale data issues

Devices will appear as stale in PrintFleet Optimizer if the DCA has not been able to collect data from the device for the number of days specified in the **Days before device stale** configuration setting in PrintFleet Optimizer.

If customers are showing stale devices without an obvious explanation, the customer should be contacted to determine the reason. A device may appear as stale for many reasons, including:

- The device has been removed from the network
- The device is turned off
- The transmission port on the network is closed (all devices display as stale)
- The computer installed with the DCA is turned off (all devices display as stale)

4.3 Providing technical support

The following best practices are recommended for providing technical support to your PrintFleet customers:

- Track all incoming calls and emails. Specifically, record the caller's name, phone number, company, the reason for the call.
- whether or not there was a resolution to their situation, and what the resolution was or what the next step is.
- Use email as a support tool, since it automatically records all of the details in writing. Ensure that callers phoning support, as
- much as possible, do not have to wait longer than five rings to get a technical person on the line.
- Try to deliver resolutions to routine problems within 30 minutes of the support call. There should be a plan in place that specifies levels of problems and their expected response times.
- Make self help materials available to your customers to minimize the need for telephone and email support.
- Review support call records on a weekly basis to flag any recurring issues that might be preventable by changing the installation or initial training process.

- Monitor new customers and installations closely for the first two weeks while they are getting started with the software.
- Consider providing 24-hour support using mobile devices.

Note

Note	All issues should be tracked with a custom or commercially available CRM (Customer Relationship Management) software solution.
-------------	--

4.4 Distributing software updates

It is the responsibility of the PrintFleet administrator to distribute software updates to their clients as they see fit. Updates at the client location would primarily be for the DCA. Updates for the DCA can be distributed to remote installations from your central server.

Appendix A Data Collection Agent Checklist and Installation Requirements

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

Network requirements:

- TCP/IP configured
- The following ports must be opened on the firewall:
 - Port 443/TCP (HTTPS), Port 80/TCP (HTTP), or an alternate port (as an option, can use HTTP or HTTPS and is dependent on the PrintFleet Optimizer server configuration). These ports need to allow outbound traffic only to the PrintFleet Optimizer server. Note that DCA Pulse only uses HTTPS. HTTP is only an option with DCA 4.x.
 - Port 35/UDP, Port 35/TCP should be opened on computers where DCA 4.x and Local Print Agent are installed. These ports need to allow inbound traffic on the Local Print Agent machine and outbound traffic on the machine hosting the DCA.
 - Port 161/UDP should be opened on the machine hosting the DCA to allow outbound traffic to devices on the network.
 - If you are planning to use SNMP traps, Port 162/UDP should be opened to allow inbound traffic from any IP address being used for SNMP traps. For more information, see "Enabling SNMP traps" on page 26.

System requirements:

- Hardware: Non-dedicated server powered on 24 hours a day, 7 days a week. If a server is not available, the DCA 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
- Requirements for Local Print Agent:
 - Operating System: Microsoft Windows Server 2008 R2, 2012 and 2016. Otherwise, if not running on a server: Windows 7, 8 or 10.
 - Microsoft .NET Framework (latest version or latest previous version) Beginning with .NET 3.5 SP1, the .NET Framework is considered a component of the Windows OS. Components follow the support life cycle of their parent product or platform.
- Requirements for DCA 4.x:
 - Operating System: Microsoft Windows Server 2008 R2, 2012 and 2016. Otherwise, if not running on a server: Windows 7, 8 or 10.
 - Microsoft .NET Framework (latest version or latest previous version) Beginning with .NET 3.5 SP1, the .NET Framework is considered a component of the Windows OS. Components follow the support life cycle of their parent product or platform.

Virtualization software support:

If you want to install the DCA on a virtual machine, the VMWare GSX virtualization software will support the installation.

Important:

- Do not install the DCA on a laptop.
- PrintFleet does not recommend using a VPN.

Index

A

- activating the DCA 4
- administrating PrintFleet Optimizer 39–43
- archive files
 - deleting 27
 - viewing 26

C

- copiers. *See* devices

D

- data_queue folder 13
- Device Manufacturer Extension 9
- devices
 - support 1

E

- enabling Intelligent Update 16

F

- fax machines. *See* devices
- firewalls 13
- forcing a scan 19

H

- hibernation 40
- HP Smart Device Services 9

I

- installation
 - Local Print Agent 31
 - DCA 4

L

- license keys, DCA
 - managing 39
- Local Agent Management
 - changing the active user 33
 - changing the Local Print Agent installer 37

- configuring Local Print Agent installations 36
- interpreting the scan results 34
- performing a push install 35
- rescanning IP addresses 36
- scanning the network 33
- starting 33
- viewing Local Print Agent log files 37

- local devices

- managing 31

- Local Print Agent

- checking the data returned 35
 - configuring 36
 - installing 31, 35
 - managing 32
 - push install 35
 - uninstalling 35
 - viewing log files 37

- log files

- Local Print Agent
 - viewing 37

- DCA

- deleting 27
 - viewing 26

M

- maximum devices, DCA 5
- model support 1
- multiple subnets 5

N

- network load, DCA 29
- network timeout 5

O

- Optimizer 39
- Optimizer. *See* PrintFleet Optimizer

P

- PIN Code, DCA

- generating 39
- DCA
 - activating 4
 - distributing the software 4
 - installing 4
 - introduction 3
 - license keys 39
 - managing 40
 - multiple subnets 5
 - network load 29
 - network timeout 5
 - obtaining the software 4
 - questions to ask prior to installation 5
 - recommended number of devices 5
 - remote update with Semaphore 41
 - requirements 44
 - setting up as scheduled task 8
 - troubleshooting 13
 - updates 41
 - VPNs 5
 - See *also* PrintFleet Optimizer
- printers. See devices
- PrintFleet Optimizer
 - administrating 39–43

Q

- queue files
 - viewing 26

R

- requirements
 - DCA 44

S

- scan
 - forcing 19
- scanning
 - suspending Local Print Agent 36
- scheduled task, DCA 8
- Semaphore 41
- SNMP Version 3
 - using 22
- stale
 - data, troubleshooting 42
- subnets, multiple 5
- support, models 1
- support, technical. See technical support

T

- technical support
 - contacting 2
 - providing 42
- throttling 19
- timeout, network 5
- troubleshooting
 - DCA transmission problems 13
 - stale data 42

U

- updates
 - distributing 43
- using SNMP Version 3 22

V

- VPNs (Virtual Private Networks) 5

W

- WebPage timeout
 - setting 26