# PrintFleet DCA Best Practices

Follow these steps to ensure a successful PrintFleet DCA installation. A careful PrintFleet DCA installation will save you troubleshooting in the future.

## Preparation

Before starting the PrintFleet DCA installation, determine any problem areas that may be present on the client network by asking the IT/Network Manager at the customer site the following questions:

- **How many document output devices are there on the network?**

  Knowing how many devices are on the network helps you determine whether any devices are not reporting.

- **How many local printing devices are on the network? Where are they?**

  This information helps you determine the most effective installation strategy. For example, if there are only a few local devices and they are within easy walking distance you can simply use a USB key, whereas if there are hundreds of local devices, or they are in different cities, you would likely consider setting up a push installation.

- **How many document output devices use an external print server (e.g. HP Jet direct)?**

  External print servers typically prevent most (sometimes all) information from being gathered from the devices which connect to them. At best you can hope to collect serial number, LCD status, and life page count information from at most one device per external print server. Take this into account when determining how many devices you expect to report, as well as when setting up support contracts for such devices.

- **Does the network use multiple subnets?**

  If there multiple subnets, and you want the PrintFleet DCA to detect the devices on those subnets, you will need to set up the PrintFleet DCA to scan those subnets.

- **Does the network use a VPN?**

  If there are devices in satellite offices that connect via a VPN, you may need to extend the network timeout value to ensure those devices have enough time to respond.

- **Does the network use a proxy server?**

  A proxy server can prevent data from being transmitted from the customer site back to the PrintFleet Enterprise server. If a proxy server is being used you will want to obtain credentials which have access to authenticate with the proxy server before you start the installation.

- **Does the network use Internet Protocol version 6 (IPv6)?**

  The PrintFleet DCA does not support IPv6. If you install the PrintFleet DCA on a computer in an IPv6-enabled network, the PrintFleet DCA will not activate.

- **Are there any devices that use non-public community strings? If so, which devices and can we obtain the community strings?**

  The PrintFleet DCA requires the community strings to log in and get information from internal memory.

  - *What is an SNMP community string?* The SNMP Community String is like a user ID or password that allows access to a device's statistics. If the community string is incorrect, the device simply discards the request and will not respond to the DCA.

- **Are there any devices that support SNMP v3? If so, do you want to use SNMP v3 to communicate with these devices?**

  If you want to use SNMP v3 authentication, the PrintFleet DCA requires the authentication protocol, user, and password. If you want to use SNMP v3 privacy, PrintFleet DCA requires the privacy protocol and password.

- **Is there anything else we should know about the network?**

  It can be helpful to know about any unusual aspects of the network, such as web content filters, port restrictions, and so forth.

**NOTE:** Some virus detection vendors (such as Symantec) are now using the crowd-based information to determine potential threats. Unfortunately, this methodology is prone to produce 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 protection software. When this happens, it may be quarantined, which prevents it from being installed. If this occurs, contact your system administrator or virus protection vendor for information about removing it from quarantine.

- For more information about the Symantec issue specifically, visit this page: http://community.norton.com/t5/Norton-Internet-Security-Norton/Clarification-on-WS-Reputation-1-detection/m-p/232155/highlight/true#M112299

## DCA Installation

The PrintFleet DCA should be installed on an existing networked server to collect and transmit device data. If no server is available, the PrintFleet DCA can be installed on a single networked computer that will remain powered on 24 hours a day, seven days a week. Never install the PrintFleet DCA on a laptop.

You may obtain the PrintFleet DCA by whatever method you choose—from PrintFleet Optimizer download, USB key, etc.

The PrintFleet DCA can be installed using the Simplified DCA Installer, where the DCA client will automatically configure the scan settings, or by using the Advanced Installer where you can configure the scan settings by hand.

Since the Simplified DCA does not require any manual intervention; the only step that needs to be performed is to launch the installer. In many cases, the DCA will configure the settings that you need to collect from networked printing devices. To collect the data from local devices, and to further configure settings, you will need to open the Printer DCA application after installation.

A Manual Installation allows you configure the DCA using the setup wizard. This installation method requires user interaction to ensure that it is configured to scan the desired networked and local printing devices. Follow the steps provided below to complete a manual installation of the Printer DCA.

1. **Install the PrintFleet DCA**

2. **Follow the steps as outlined in the wizard. While completing the wizard, please note the following:**

    - On the Activation page, if you have obtained information regarding a proxy server from your IT/Network Manager, you can click Show Proxy Configuration and enter the information now.

    - On the Intelligent Update page, ensure the Intelligent Update feature is enabled. This is another critical step that allows you to remotely update the Printer DCA software. The Intelligent Update feature can only be enabled if the Service Control (Health Check) feature is installed. This feature can also be enabled later by selecting the Enable Intelligent Update check box from the Communication tab.

    - On the Completion page, if you do not think any further changes are required, you do not need to open the Printer DCA interface. You should leave the Start the Printer DCA Service check box selected unless you have a strong reason not to.

3. **If you need to change the IP ranges from what was displayed in the wizard, do the following:**

    - Click the Scan tab, then the General tab, and enter the information (determined in your preliminary investigation of the network) in the Scan List box.

4. **Adjust the scan interval as necessary.**

The scan interval is the amount of time to wait after the completion of one scan before beginning the next scan. The default scan interval is 60 minutes, and this is appropriate for most customer networks, and for the dealership's purposes. To change the interval, click the Scan tab, then the General tab, and enter a new Scan Interval value.

There is no single value that is appropriate for all situations. The best answer for your situation will depend on such things as the number of devices being scanned and the resources allocated to perform the scan (essentially how long it takes to complete a scan of your devices).

*Scenario 1:*

• Scanning 2 devices
• Non-dedicated DCA hardware
• Scan time takes almost no time at all

*Summary:* With only a few devices a scan takes very little time to complete, so a short scan interval (such as a minute) would result in the PrintFleet DCA scanning the devices almost constantly. This is probably unnecessary, and may affect the performance of the computer performing the scans. In this case the default scan interval would likely be reasonable.

*Scenario 2:*

• Scanning 5,000 devices
• Dedicated DCA hardware
• Scan takes 3-6 hours

*Summary:* With each scan taking a long time to complete, you will probably want to start the next scan fairly soon to ensure you detect any important changes in a timely manner. For this reason you would likely want to set the scan interval to a small value, such as 1 minute.

5. **Adjust the default network timeout as necessary.**

There are two ways to determine an appropriate network timeout. Choose whichever method you are most comfortable with:

- From the DOS command prompt, ping the IP addresses of the devices at the furthest part of the customer's network. Set the PrintFleet DCA network timeout to the average response time (in milliseconds).

- Perform a test scan and see how many devices respond. If the number of responding devices is significantly lower than the total number of devices you expected, double the network timeout (250, 500, 1000, and 2000) and repeat the test. A timeout of 2000 ms is typically sufficient even for scanning over VPNs across continents.

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

Typically, you should never have to decrease the default network timeout unless the network is so large that there is a benefit to decreasing the total PrintFleet DCA scan time. To change the timeout, click the Scan tab, then the General tab, and enter a new Network Timeout value.

6. **Store any non-public community strings in the PrintFleet DCA.**

Any non-public community strings should have been obtained during your initial discussion with the IT/Network Manager. Input these into the PrintFleet DCA to obtain complete information from your scan. Click the Scan tab, then the advanced tab, enter the information in the SNMP Community Strings box, and click Add.

7. **Input any required proxy settings.**

You should have obtained information regarding a proxy server during your initial conversation with the IT/Network Manager. Enter this information into the PrintFleet DCA, if applicable, by clicking the Communication tab, and adjusting the settings under Proxy Configuration.

8. **Enable and configure any optional settings as desired.**

You may want to enable or adjust the following settings:

On the General tab of the Scan tab:

- **Enable Broadcast:** to use broadcast scanning (not needed when Rapid Scan is enabled; can only be used in conjunction with Quick Scan)
- **Enable Rapid Scan:** to use multithreading for more efficient scans

On the Advanced tab of the Scan tab:

- **Enable Focus Scan**: consider configuring this for very large networks
- **Enable SNMP Traps:** must be enabled on the device itself for SNMP traps to function
- **Enable IP Masking:** use if the customer requests their IP addresses to be masked (hidden)

On the File Viewer tab:

- Change the days to keep log and archive files

9. **Run a test scan and troubleshoot any issues.**

Ensure you review the PrintFleet DCA log and transmission files to determine if all devices are being collected and that the files are being successfully transmitted to the PrintFleet Optimizer server.