Data Collector Agent: Best Practices

PageTrac Support

Data Collector Agent (DCA): Best Practices

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

Note: For additional information please view the online tutorial at http://secure.printfleet.com/training/DCA4/. The tutorial covers the creation and installation of a version 4.0 DCA.

1. **Determine any problem areas that may be present on the client network**

Ask the IT/Network Manager at the customer site the following questions prior to installing the DCA:

- How many document output devices are there on the network?
- Does the network use multiple subnets?
- Does the company have multiple offices to be monitored?
- Does the network use a VPN?
- Does the network use a proxy server?
- How many local printing devices are on the network? Where are they?
- How many document output devices use an external print server (e.g. HP Jetdirect)?
- Are there any devices that use non-public community strings? If so, which devices and can we obtain the community strings?
- Is there anything else we should know about the network?

2. **Make an initial analysis of the network**

- Determine the most concise IP ranges and subnets to scan
- Locate devices using an external print server that blocks the collection of the device description
- Embed locations, asset numbers, departments, and missing serial numbers with Asset Tracker, especially for devices using an external print server, so that service techs can locate the devices and you can match them up with your ERP system
- Determine if the default network timeout needs to be increased to obtain complete information from older devices or devices on a VPN
- Test any non-public community strings that you have obtained from the IT/Network Manager

3. Install the DCA

Install the DCA on a non-dedicated server at the client location. Reliability will be severely degraded if you install the DCA on a desktop computer. Never install the DCA on a laptop. You may obtain the DCA by whatever method you choose—from Optimizer, download, USB key, CD, etc.

4. Generate a DCA license key and activate the DCA

In Optimizer, Administration > DCA Administration > Manual Keys or Auto Keys

For best results, generate a manual license key using the Fingerprint Code on the DCA activation screen. Alternatively, generate an auto license key prior to installing the DCA to have it available immediately upon installation—auto license keys may present issues in environments using proxy servers.

Assign an account representative during the license key generation if at all possible! This will save you a step during your initial account setup.

5. Choose the DCA communication method that works best for both you and the customer: HTTPS, HTTP, or FTP

If at all possible, use HTTPS for DCA transmissions. This is the only method that encrypts the data during transmission. You will require your Enterprise server to have a valid security certificate, and the customer will have to have port 443 open on their network. Whichever method you choose, click Test to ensure proper communication between the customer network and your Enterprise server. Follow troubleshooting procedures if the test fails.

6. Select the appropriate network card

The DCA should be installed on a server that has a single network card, but if it has more than one you can select the appropriate one in the DCA configuration screen.

7. Enter the IP range(s) you have determined into the DCA

8. Adjust the transmission interval as necessary

The default transmission interval is 60 minutes, and this is appropriate for most customer networks, and for the dealership's purposes. Most importantly, the transmission interval must be longer than the time it takes for a single DCA scan to complete. The recommended minimum transmission interval is 30 minutes.

9. Adjust the default timeout as necessary

The required timeout should have been determined during your initial network analysis. Enter this number into the DCA. Typically, you should never have to decrease the default timeout unless the network is so large that there is a benefit to decreasing the total DCA scan time.

10. Install the Service Control (Health Check) feature

On the DCA File menu, click Advanced Options and find the Service Control (Health Check) area. This is a critical step that ensures that the DCA service cannot be accidentally turned off.

11. Enable the Intelligent Update feature

On the DCA File menu, click Advanced Options and find the Intelligent Update check box.

This is another critical step that allows you to remotely update the DCA software and change the DCA settings, eliminating the need to ever go to the customer site to adjust the DCA. The Intelligent Update feature can only be enabled if the Service Control (Health Check) feature is installed.

12. Store any non-public community strings in the DCA

On the DCA File menu, click Advanced Options and find the Community Strings area.

Any non-public community strings should have been obtained during your initial discussion with the IT/Network Manager. Input these into the DCA to obtain complete information from your scan.

13. Input any required proxy settings

On the DCA File menu, click Advanced Options and find the Proxy area.

You should have obtained any information regarding a proxy server during your initial conversation with the IT/Network Manager. Enter this information into the DCA if applicable.

14. Enable and configure any optional settings as desired

You may want to enable or adjust the following settings under Advanced Options:

- Focus Scan: consider configuring this for very large networks
- Enable Rapid Scan: to use multithreading for more efficient scans
- Enable Broadcast: to use broadcast scanning (not needed when Rapid Scan is enabled; can only be used in conjunction with QuickScan)
- Mask IPs: use if the customer requests their IP addresses to be masked
- SNMP traps: must be enabled on the device itself for SNMP traps to function
- NAICS: set the customer's NAICS classification if you are providing aggregate customer and device information to PrintFleet
- File Cleanup: change the days to keep log and archive files (may want to not keep them at all to minimize the amount of space the files consume)

15. Run a test scan and troubleshoot any issues

You should have minimal problems if you have gone through each of the previous steps. Most issues would have been encountered during initial testing of the send method (HTTPS, HTTP, or FTP.

16. Disable conflicting applications that use SNMP

The DCA should be installed on a server without conflicting applications that use SNMP. However, if there are any, they must be disabled to ensure that the DCA runs properly.