

# DATA COLLECTION AGENT USER'S MANUAL



## Table of Contents

TABLE OF CONTENTS .....	2
USING THE PRINTER DATA COLLECTOR AGENT .....	3
OBTAINING THE DCA SOFTWARE .....	4
MANAGING DCA INSTALLATIONS .....	5
<i>Generating PIN Codes for DCA version 4.0 or greater</i> .....	5
<i>Generating Manual Keys for DCA version 3.x</i> .....	5
<i>Generating Automatic Keys for DCA version 3.x (pre-generated)</i> .....	6
MANAGING DCA'S .....	7
INSTALLING AND ACTIVATING THE DCA .....	9
MANAGING THE DCA SERVICE .....	12
INSTALLING AND STARTING THE DCA SERVICE .....	12
CONFIGURING COMMUNICATION SETTINGS.....	14
CHANGING AND TESTING THE COMMUNICATION METHOD AND PORT .....	14
USING PROXY SETTINGS.....	14
CHANGING THE WEB SERVICE TIMEOUT .....	15
ENABLING INTELLIGENT UPDATE.....	16
ENABLING A SERVICE BRIDGE.....	17
CONFIGURING NETWORK SCAN SETTINGS.....	18
MANAGING SCAN PROFILES .....	18
SPECIFYING WHICH DEVICES TO SCAN .....	19
ENABLING SCANNING OF NETWORK AND/OR LOCAL DEVICES.....	20
ENABLING BROADCAST SCANNING .....	21
ENABLING RAPID SCAN .....	21
SETTING THE SCAN AND TRANSMISSION INTERVAL.....	21
SETTING THE NETWORK TIMEOUT .....	22
SETTING THE LOCAL PRINT AGENT TIMEOUT .....	22
SETTING THE NUMBER OF SNMP RETRIES .....	23
USING FOCUS SCANS .....	23
STORING SNMP COMMUNITY STRINGS .....	23
MASKING PRIVATE DATA.....	24
ENABLING SNMP TRAPS .....	24
DISABLING REAL TIME DCA STATUS .....	25
MANAGING LOCAL DEVICES WITH LOCAL PRINT AGENT .....	26
VIEWING QUEUE, ARCHIVE, AND LOG FILES .....	28
CONFIGURING LANGUAGE AND READ/WRITE SETTINGS .....	29
UPDATING THE DCA SOFTWARE.....	30
UNDERSTANDING THE NETWORK LOAD ASSOCIATED WITH THE DCA .....	31
TROUBLESHOOTING DCA COMMUNICATION PROBLEMS .....	<a href="#">324</a>

## Using the Printer Data Collector Agent

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

This chapter discusses:

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

## Obtaining the DCA software

You can access the DCA installation file through Axess 2.2 . Instructions for obtaining the DCA installation are provided below.

To obtain the DCA installation file from PrintFleet Optimizer:

1. On the Administration menu click DCA Install.
2. In DCA 4.x tab, click the Printer DCA 4.x.x.x.msi link and save the file to the computer.

Optionally you can install DCA 3.x tab, click the DCA\_Install.msi link and save the file to the computer.

The DCA Install screen displays the most recent release notes and other software prerequisites.

## Managing DCA Installations

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

### *Generating PIN Codes for DCA version 4.0 or greater*

To generate a PIN Code for DCA version 4.0 or greater:

1. On the Administration menu, select DCA Administration, and then click New DCA.
2. Select Version 4.0 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. This will be the name of the customer the DCA is being installed for. Optionally, enter a custom message in the Custom Message field, or 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.

### *Generating Manual Keys for DCA version 3.x*

Generating a manual key for DCA can only be done for DCA 3.x versions. Generating a manual DCA key requires the DCA to already be installed, but not yet activated, at the location. The person who installed the DCA needs to provide you with either the fingerprint code from the DCA activation screen, or the hardDisk serial number of Volume Drive C.

*To generate a manual Key for DCA version 3.x:*

1. On the Administration menu, select DCA Administration, and then click New DCA.
2. Select Version 3.0.
3. Select the appropriate group from the dropdown list or click Create New Group button.
4. Select Manual for the DCA 3.0 Key Generation Method.
5. Do one of the following:
  - Enter the fingerprint code as displayed on the DCA activation screen in the Fingerprint Code box.



- Enter the hardDisk serial number of Volume Drive C of the computer installed with the DCA in the HardDisk Serial # box.

6. Define the DCA information: enter the DCA Name. Optionally, enter a custom message in the Custom Message field, or set an Expiry date by selecting the calendar button and selecting a date.

7. 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.

#### *Generating Automatic Keys for DCA version 3.x (pre-generated)*

Automatic DCA Keys can be generated in advance of a DCA installation. This allows the person installing the DCA to have the DCA PIN Code on hand during installation.

**Note**                      Pregenerated DCA Automatic Keys may not work in environments using proxy servers. In these instances, you must use a Key from a manual DCA 3.0 generated using the DCA's fingerprint code.

#### *To generate an Automatic Key for DCA version 3.x:*

1. On the Administration menu, select DCA Administration, and then click New DCA.
2. Select Version 3.0.
3. Select the appropriate customer group from the group list or click on Create New Group.
4. Set Automatic for the DCA 3.0 Key Generation Method
5. Define the DCA information: enter the DCA Name. Optionally, enter a custom message in the Custom Message field, or set an Expiry date by selecting the calendar button and selecting a date.
6. 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.

## Managing DCA's

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 or set to inactive or active. A new PIN Code can also be created for a DCA version 4.0 or greater.

### *To check the status of a DCA:*

1. On the Administration menu, select DCA Administration.
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.

### *To view DCA information:*

1. On the Administration menu, select DCA Administration.
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, Expiry Date or Custom Message 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.

### *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.

***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 (only available for DCA version 4.0 or greater):***

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.

## 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.

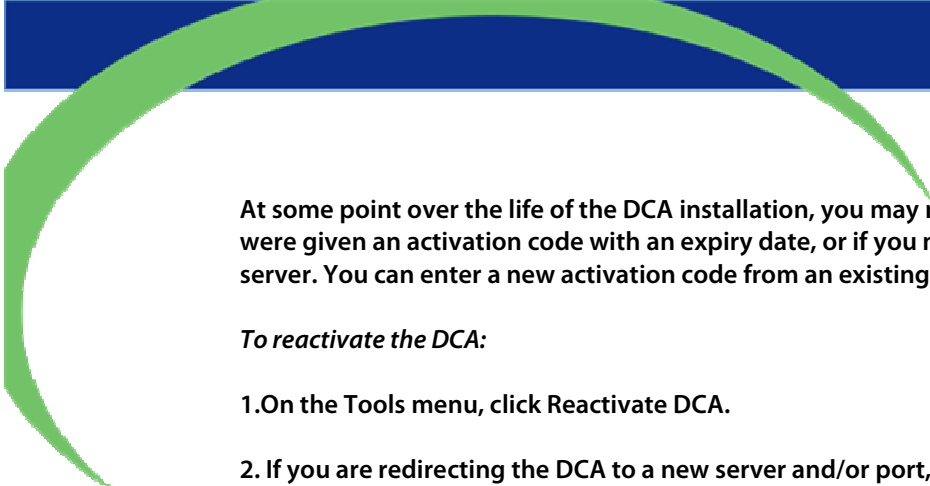
Prior to installing the DCA, you should obtain the information in the following table from the network administrator at the location. This will allow you to properly configure the DCA.

Table 2: Information to Gather from the Network Administrator Prior to a DCA Installation	
Find out...	Solution
if there are local devices you want to monitor.	Once the DCA is installed, you will have to enable local data collection and install Local Print Agent on applicable computers.
how many total printing devices reside on the network and how large the network is.	An additional DCA should be installed on a separate computer for each 10,000 imaging devices on the network or 100,000 IP addresses.
if the network uses multiple subnets.	If so, take note of the subnets and IP ranges to ensure they are all included in the network scan range.
if the network uses a Virtual Private Network (VPN) or has Wide Area Network (WAN) links.	If so, the network timeout for the DCA should be increased to 500–1000 milliseconds.
if the company has multiple offices they want monitored.	If so, a single DCA may be used if the networks are connected via a VPN, however, it is recommended that a DCA is installed at each location.

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

*To install and activate the DCA:*

1. Double-click the filename Printer DCA 4.x.x.x.msi installation file.
  2. The Printer DCA Installation Wizard is launched. Click Next to continue.
  3. Read through the End-User License Agreement, check I accept the terms in the License Agreement and select Next to continue. If you do not accept the terms, the installation process will not continue.
  4. In the Destination Folder screen, either leave the default folder displayed, or enter a new destination folder. Click Next to continue.
  5. In the Ready to Install Printer DCA screen, click Install to begin installation or click Cancel to exit.
  6. In the Completed the Printer DCA Installation Wizard, leave checked or uncheck Launch Printer DCA after installation and select Finish.
  7. After the Printer DCA is launched, in the second End-User License Agreement, select Accept to continue or select Decline to not continue.
  8. In the Welcome to the Printer DCA-Setup Wizard, select the language from the drop down list and select Next.
  9. In the Printer DCA Activation screen, enter the following:
    - Enter the Server information for the server that the DCA will be sending information to in the Server box. ( [axess.printfleet.com:443](https://axess.printfleet.com:443) )
    - Enter the PIN code in the PIN Code box.
    - Optionally, if the location is using a proxy server that you want to configure at this point (you will also be able to do so after installation), click Show Proxy Configuration.
    - Click Next.
- Note**      You can continue past this step without entering a PIN code, but data will not be transmitted to the server until activation is complete.
10. In the Scan Settings screen, you will be shown a list of preconfigured IP ranges that will be added to your default DCA network scan. This can be changed after installation is complete if necessary. Click Next.
  11. In the Intelligent Updates screen, you will be given the option to disable Intelligent Updates. It is recommended that Allow Intelligent Updates remains selected unless there is a strong reason to turn it off. Click Next.
  12. In the Setup is complete screen, by default, the Open the Data Collector Agent Interface and Start the Data Collector Agent Service are both selected. Optionally, you can turn off one or both of these options. Click Finish.



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

*To reactivate the DCA:*

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

## Managing the DCA Service

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

### *Installing and starting the DCA service*

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

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

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

### *Setting up the DCA as a scheduled task*

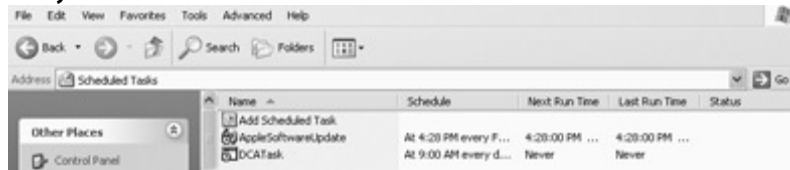
To set up the DCA as a scheduled task instead of a service, you must first uninstall the DCA service, and then create the DCA scheduled task.

To uninstall the DCA service:

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

To create a scheduled task for the DCA:

1. Click Start, click Control Panel, and then double-click Scheduled Tasks.
2. On the File menu, point to New, and then click Scheduled Task.
3. Replace New Task with a recognizable name for the task, such as DCATask, and click anywhere away from the new task icon to save the name.



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

### *Configuring Communication Settings*

During the DCA installation, the DCA will attempt to establish basic communication with the central server using either HTTPS (default) or HTTP (secondary).

Proxy settings can also be configured during installation, or at any time afterwards. If communication with the server is successful during installation, it is not necessary to change the communication method, port, or proxy settings.

### *Changing and testing the communication method and port*

There are two methods the DCA can use to send information to the central server: HTTPS and HTTP.

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

To change the DCA communication method and port:

1. Under the Communication tab of the DCA, in the Communication Method area, type in the protocol, followed by the hostname.
2. Optional--only if you use a non-standard port--enter the port number after a colon after a hostname. For example: **axess.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" at the end of this manual.

### *Using proxy settings*

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

To use a manual proxy configuration:

1. Under the Communication tab of the DCA, in the Proxy Configuration area, click to select one of the following: Use Windows proxy settings (no other configuration required), Use custom proxy settings, or None (to disable proxy settings).
2. If you have selected Use custom proxy settings, enter the server and port information in the Server and Port boxes, respectively.



3. If the proxy server requires authentication, click to select the Authentication check box, and then do one of the following:

- Click to select Default to use the authentication currently being used on the computer installed with the DCA.

- Click to select Custom, and then enter username, password, and domain information in the Username, Password, and Domain boxes, respectively, or click Load Current to populate the fields with the current authentication being used by the computer installed with the DCA.

4. In the Communication Method area, click Test to verify the settings are working.

5. Click Save.

#### *Changing the web service timeout*

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

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 30,000 milliseconds; 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 controls transmission timeout.

2. Click Save.



### *Enabling Intelligent Update*

When Intelligent Update is enabled, the DCA can be remotely updated by your administrator. This is important to ensure you are always able to collect the highest quantity and quality of information available.

To enable Intelligent Update:

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

### *Enabling a Service Bridge*

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

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

On the service technician's computer:

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

To enable a Service Bridge from the DCA:

1. Do one of the following:
  - On the Tools menu, click Start Service Bridge.
  - Under the Communication tab, in the Service Bridge area, click Start.
2. In the Enter Service Bridge PIN box, enter the access code generated on the central server (you will have to obtain this from your dealer) and click Ok. The Status field in the Service Bridge area will indicate when the connection has been established.
3. Enter the Remote IP value into your browser; the device's embedded web page is displayed.

To end the connection:

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



### *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.

### *Managing scan profiles*

You can use profiles to configure multiple types of network scans. For example, you might want to scan networked devices every hour, and local devices once a day—these would be two different scan profiles.

You might also want a different scan profile for one or two high priority devices that you want to scan more frequently.

Depending on your environment, you might have multiple uses for scan profiles, or you might not need more than one. When you first install the DCA, you will have one scan profile called Default.

To create a new scan profile:

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

To edit an existing scan profile:

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

To delete a scan profile:

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

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

**Warning**

If you delete a scan profile, you will no longer be collecting information from the devices specified in the profile, unless they are included in a different profile.

*Specifying which devices to scan*

The DCA only scans the IP addresses and/or hostnames specified in each scan profile. When the DCA is first installed, it selects a default set of IP addresses to scan based on either Active Directory or, if that is not available, the primary network card on the system installed with the DCA. These IP addresses are automatically added to the Default scan profile.

If the default set of IP addresses captures all the devices on the network that you want to scan, and you do not want multiple scan profiles, you do not have to further specify the devices for the DCA to scan. If, however, you want to adjust the devices included in the default scan, or if you have more than one scan profile, you will need to further configure which IP addresses and/or hostnames to include.

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

**Important**

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

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

1. Under the Scan tab, make sure the correct scan profile is selected from the Scan Profile list.
2. Under the General tab, in the Ranges area, do one or more of the following:
  - To automatically obtain an additional default scan range (from the one specified during DCA installation), click to select Default Range, and then select either Active Directory or the applicable network card for the system installed with the DCA.
  - To specify a range of IP addresses, click to select IP Range, and enter the IP address of the beginning of the range in the left box, and the IP address of the end of the range in the right box.
  - To specify a single IP address, click to select IP Address and enter the IP address in the box.
  - To specify a hostname, click to select Hostname and enter the hostname in the box.
3. Click Add or Exclude.
4. Repeat steps 2-3 as necessary.

5. Click Save.

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

1. Under the Scan tab, make sure the correct scan profile is selected from the Scan Profile list.
2. Under the General tab, in the Ranges area, under Scan List, do one of the following:
  - To remove one or more individual items from the scan range, click to select the item, and then click Remove.
  - To remove every item from the scan range, click Clear.

3. Click Save.

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

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

To export current scan range settings to a text file:

1. Under the Scan tab, make sure the correct scan profile is selected from the Scan Profile list.
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.
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.

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.



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.
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.
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:

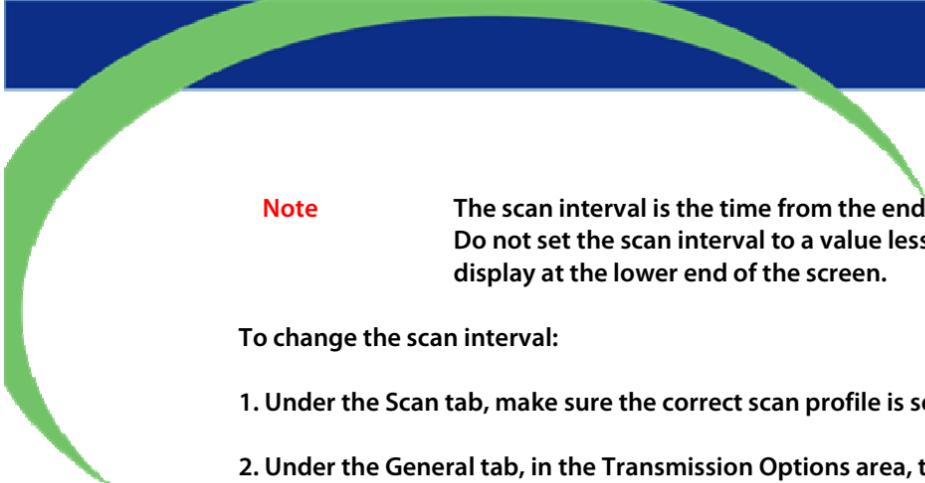
1. Under the Scan tab, make sure the correct scan profile is selected from the Scan Profile list.
2. Under the General tab, in the Scanning Options area, click Enable Rapid Scan.
3. Click Save.

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

#### *Setting the scan and transmission interval*

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

It is generally not useful to set a scan interval for more than every 30 or 60 minutes. For example, new information is posted to Axess Database every minute, but new alerts are generated approximately every 15 minutes.



**Note**

The scan interval is the time from the end of one scan to the start of the next scan. Do not set the scan interval to a value less than the estimated Scan Time which is display at the lower end of the screen.

To change the scan interval:

1. Under the Scan tab, make sure the correct scan profile is selected from the Scan Profile list.
2. Under the General tab, in the Transmission Options area, type or select the desired scan interval, in minutes, in the Scan Interval box.
3. Click Save.

*Setting the network timeout*

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

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

To change the network timeout:

1. Under the Scan tab, make sure the correct scan profile is selected from the Scan Profile list.
2. Under the General tab, in the Transmission Options area, type or select the desired network timeout, in milliseconds, in the Network Timeout box.
3. Click Save.

*Setting the Local Print Agent timeout*

The Local Print Agent timeout is the amount of time that the DCA will wait for the Local Print Agent application to respond back with information from a locally connected device.

The default Local Print Agent timeout is 10,000 milliseconds per system. Local device collection takes substantially longer than networked device collection because of the extra step needed to go through the connected computer via the Local Print Agent application.

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

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.
2. Under the General tab, in the Transmission Options area, type or select the desired Local Print Agent timeout, in milliseconds, in the Local Print Agent Timeout box
3. Click Save.

#### *Setting the number of SNMP retries*

The number of SNMP retries entered in the DCA settings is the number of times the DCA will attempt to get information from a device that is responding with incomplete or no information. Increasing the number of SNMP retries may increase the completeness of a DCA scan, but will also increase the amount of time it takes to complete a network scan.

To change the number of SNMP retries used:

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

#### *Storing SNMP community strings*

Community strings act as passwords on networked devices that limit access via SNMP. Since the DCA uses SNMP to collect data from devices, any custom community strings on printing devices put in place by network administrators can be manually entered in the DCA to allow it SNMP access to the device. Most devices have a 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.
2. Do one or more of the following under the Advanced tab, in the SNMP Community Strings area:
  - To add a community string, type an applicable community string in the text box, and click Add. Repeat as necessary.
  - To remove a community string, click to select a previously entered community string, and then click Remove.
  - To reorder the list of community strings, click to highlight a community string, and then click either the Up or Down button. Repeat as necessary. When the DCA encounters a device using a community string during the network scan, it will attempt to use the first community string listed, then the next, etc., until it is successful or it runs out of community strings to attempt.
3. Click Save.

#### *Masking private data*

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

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

To mask private information in DCA transmission files:

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

#### *Enabling SNMP traps*

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

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

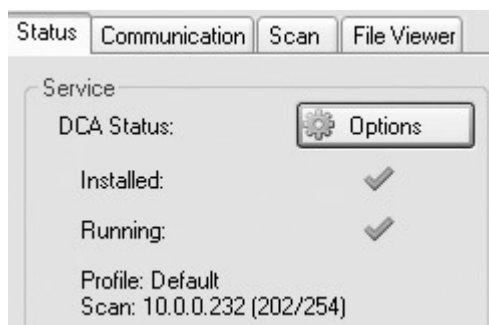
After SNMP traps are enabled on the DCA, each SNMP trap received will trigger the DCA to perform a regular data scan on only the device that sent the SNMP trap. The results from this scan will immediately be sent to the central server.

To enable SNMP traps:

1. Under the Scan tab, make sure the correct scan profile is selected from the Scan Profile list.
2. Under the Advanced tab, in the Miscellaneous area, click to select the Enable SNMP Traps check box.
3. Click Save.

#### *Disabling real time DCA status*

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



You can disable this feature, if necessary.

To disable real time DCA status:

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

## Managing Local Devices with Local Print Agent

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

1. Add the IP addresses/ranges of computers connected to local printers to the DCA network scan.
2. Enable the local device scanning option.
3. Install Local Print Agent on computers connected to local printers (instructions follow).

Local Print Agent allows the DCA to obtain information directly from locally connected printing devices. The Local Print Agent application must be installed on each computer connected to a local printer that you want to collect information from.

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

There are three methods to install Local Print Agent:

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

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

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

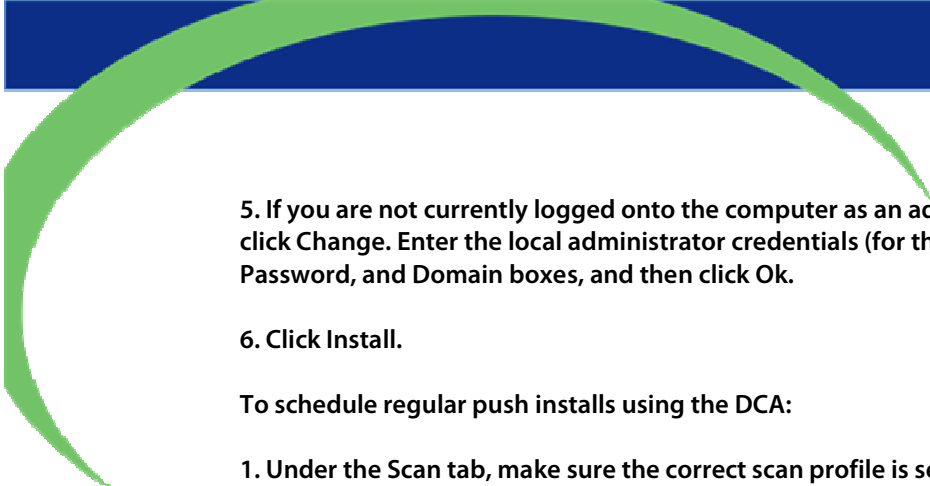
- Run the Local Print Agent.msi file on the computer you want to install Local Print Agent on. The installation file is found by default in: program files\Printer DCA\Support folder.

The installation file can be copied to a USB drive, CD, etc. for portability.

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

To push install Local Print Agent from the DCA:

1. Under the Scan tab, make sure the correct scan profile is selected from the Scan Profile list.
2. On the Tools menu, select Local Agent Management.
3. Click Scan All. This will scan all IP addresses included in the selected scan profile.
4. Under the IP Address column, click to select the check boxes beside each IP address belonging to a computer you want to install Local Print Agent on. Optionally, click All, None, Not installed, or Installed to automatically select a set of IPs.



5. If you are not currently logged onto the computer as an administrator, in the Credentials area, click Change. Enter the local administrator credentials (for the target OS) in the Username, Password, and Domain boxes, and then click Ok.

6. Click Install.

To schedule regular push installs using the DCA:

1. Under the Scan tab, make sure the correct scan profile is selected from the Scan Profile list.
2. Under the Local tab, select the Enable Push Install check box.
3. In the Change Push Install Credentials screen, enter the credentials of the user that belongs to the local administrator group on the target OS.
4. Beside Start, select a start date and time for the automated push install.
5. Beside Repeat, select the interval you want to perform the push install at.
6. Click Save.

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

## Viewing queue, archive, and log files

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

Queue and archive files are copies of DCA scan result files;

- queue files have not yet been transmitted to the central server,
- while archive files have already been transmitted.

The presence of queue files indicates that the DCA is not successfully transmitting information to the central server (unless the DCA is in the process of transmitting the most recent file). Queue and archive files are encrypted in the proprietary .pfd format and contain the complete results of a single DCA network scan.

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

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

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

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

- Under the File Viewer tab, do one of the following:
    - To open and view a queue file, click the file folder icon beside Total files in queue, and select and open the desired file.
    - To open and view an archive file, click the file folder icon beside Total files in archive, and select and open the desired file.
    - To open and view a log file, click the file folder icon beside Open Log file from, and select and open the desired file, or select a date via the dropdown.
- Alternatively, you can drag and drop any of the files into the File Viewer area.

## Configuring language and read/write settings

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

To change the DCA language settings:

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

The DCA has full write permissions enabled at installation, but read-only permissions can be set through use of a password. This will prevent anyone without the password from changing any of the DCA settings.

To make the DCA read-only:

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

To disable read-only mode:

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

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

To change the read-only mode password:

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



## Updating the DCA software

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

You can update the DCA manually, or your distributor may update the DCA software for you if you have Intelligent Update enabled.

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.

## 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

## 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 use the following table to troubleshooting potential communication problems.

Table 3: Troubleshooting DCA Communication Problems	
Check if...	If not...
the selected send method (HTTP or HTTPS) corresponds with the port you have chosen to transmit data through.	change the send method to correspond with the port number chosen, or change the port number to correspond with the send method chosen.
the port you have selected is open on the network.	have the network administrator open the selected port.
Axess has a valid SSL security certificate, if you are attempting to send via HTTPS.	contact your distributor to check if they are having problems with their security certificate.
the DCA is successfully collecting data from the internal network by looking in the data_queue or data_archive 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.
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.

