

# UPSTREAMCONNECT SECURITY



## OVERVIEW

Upstream is committed to providing software products that are secure for use in all network environments. The UpstreamConnect software only collects critical imaging device metrics necessary to manage a printing environment, and never collect any personal or user information.

This document discusses network and information security as it relates to:

- UpstreamConnect Data Collector Agent and Local Print Agent software
- UpstreamConnect web console
- UpstreamConnect software testing and release process
- UpstreamConnect source code security

It is also explained why using UpstreamConnect software applications will not impact compliance of the following laws:

- Health Insurance Portability & Accountability Act (HIPAA)
- Sarbanes-Oxley
- Gramm-Leach-Bliley Act (GLBA)
- Federal Information Security Management Act (FISMA)

## UPSTREAMCONNECT DATA COLLECTOR AGENT AND LOCAL PRINT AGENT SOFTWARE OVERVIEW

The UpstreamConnect Data Collector Agent (DCA) is a software application that is installed on a non-dedicated networked server at each location where imaging device metrics are to be collected. DCA is capable of data collection from imaging devices that have network interface and are connected to the network DCA is set up to scan (Network Devices).

The UpstreamConnect Local Print Agent is a software application that is installed on a non-dedicated networked server or on a networked workstation with one or many non-networked imaging devices connected to the server / workstation (Local Devices). The UpstreamConnect Local Print Agent acts as a proxy between a UpstreamConnect DCA v.4.0 and Local Devices receiving requests from the DCA, transforming these requests into printer-compatible commands, and sending device responses back to the DCA. DCA 3.x does not support UpstreamConnect Local Print Agent.

The DCA and the Local Print Agent run as Windows® services, allowing them to operate 24 hours a day, 7 days a week. Also, DCA can optionally run as a scheduled task.

## UPSTREAMCONNECT DCA ACTIVATION AND DCA SUBMISSION AUTHENTICATION

UpstreamConnect DCA has to be activated on a UpstreamConnect Enterprise server prior to data submission to the server. DCA Activation is managed by UpstreamConnect Helpdesk and includes:

- Creation of a DCA Account on the UpstreamConnect Server
- Association of a DCA Installation and the DCA Account based on a unique PIN
- Generation of a unique Shared Key used to encrypt data exchange between the UpstreamConnect Server and the DCA Installation (for DCA v. 4.0 and later)

DCA Accounts can have an Expiration Date when their credentials to submit data to the UpstreamConnect Server are revoked automatically; Upstream can also revoke these credentials at any time by De-Activating the DCA. Data submissions from a DCA start being rejected by the UpstreamConnect Server immediately after the DCA Expiration Date comes or the DCA is De-Activated.

For DCAs v.4.0 and later, the UpstreamConnect Server checks if the submitting DCA has an Active account on the Server prior to data acceptance. If the DCA account exists and is Active, the data is saved in a file on the Server for further processing; otherwise, the submission is ignored and no data is saved on the Server.

For DCA 3.x, the submission data is saved on the UpstreamConnect Server in file. The check for DCA account existence and Activation status happens when the file is processed. If no matching DCA account exists, by default a new DCA 3.x account will be automatically created to facilitate upgrades.

The Shared Key that is used to encrypt data exchange between the UpstreamConnect Server and a DCA is stored in the PFE Server database and is protected by security means of MS Windows Server and MS SQL Server. It is responsibility of the MS Windows Server and MS SQL Server Administrator to implement appropriate security policies to exclude possibility of unauthorized access to the Shared Key. Neither the UpstreamConnect web console nor other UpstreamConnect components exposure Shared Keys to users.

For DCA 4.0 and later, DCA Installation stores the Shared Key in an encrypted local storage. The encryption algorithm uses hardware parameters and Windows® Product ID of the DCA Host; this ensures that the Shared Key will not be used on DCA Installations other that the one where it was stored during DCA Activation.

DCA 3.x stores data in unencrypted files, but starting with DCA 3.2 adds a message digest code to the filename for data integrity checks. The UpstreamConnect Server will reject any files where the message digest code does not pass validation, and optionally can be set to reject files missing a message digest code (files from versions prior to DCA 3.2). The only time files are ever encrypted is with HTTPS when it is being used for transmission.



## DEVICE DATA COLLECTION WITH THE UPSTREAMCONNECT DATA COLLECTOR AGENT AND LOCAL PRINT AGENT

Types of information collected-The UpstreamConnect DCA attempts to collect the following information from networked printing devices during a network scan:

IP address (can be masked)	Toner cartridge serial number
Device description	Maintenance kit levels
Serial number	Non-toner supply levels
Meter reads	Asset number
Monochrome or color identification	Location

For Local Devices, UpstreamConnect DCA with assistance of UpstreamConnect Local Print Agent attempts to collect the following information:

Manufacturer	Asset number
Device description	Location
Serial number	Meter reads
OS version of Local Print Agent Host	Miscellaneous (machine specific)
IP address of the machine the Local Print Agent is installed on (Local Print Agent Host)	Name of the account used to run Local Print Agent service

## DATA TRANSMISSION METHODS

DCA transmits the collected data to the centralized database via HTTPS (port 443 – recommended), HTTP (port 80), FTP (port 21/port 20), or SMTP (port 25, sends via e-mail). The following table describes protocols used by

	HTTPS – recommended	HTTP	FTP	SMTP
DCA v 3.x	Yes	Yes	Yes	Yes
DCA v 4.0	Yes	Yes	Not available	Not available



## DATA TRANSMISSION FORMATS

DCAs v.4.0 and later encrypt submission data with 128-bit TripleDES using the Shared Key and DCA Host hardware parameters and MS Windows Product ID. This adds an additional layer of data protection during transfer from the DCA to the UpstreamConnect Server, and provides server validation during DCA submission. This additional encryption ensures that if SSL (HTTPS) is not being used, even though the message header/wrappers are not encrypted, the actual content containing any printer data is encrypted. If SSL (HTTPS) is being used, it provides an additional layer of security and even the message wrappers are encrypted. The UpstreamConnect software uses encryption providers integrated into the Microsoft .Net Framework to encrypt data exchange between DCA 4.0 and PFE Server.

DCA 3.x transmits data as comma-delimited files in plain text format. Therefore, it is highly recommended to use HTTPS transmission protocol to ensure data protection.

## NETWORK TRAFFIC

The network traffic created by the DCA is minimal, and will vary depending on the number of IP addresses being scanned. The table below outlines the network load associated with the DCA compared to the network load associated with loading a single standard webpage.

Network Byte Load Associated with the DCA Event	Approximate Total Bytes
Loading a single standard webpage	60 KB
DCA scan, single empty IP address	5.2 KB
DCA scan, 1 printer only	7.2 KB
DCA scan, 1 printer, 254 total IPs	96 KB
DCA scan, 15 printers, 254 total IPs	125 KB

## OPTIONAL REMOTE UPDATES

The DCA contains an optional remote update feature, which is activated by enabling the Health Check and Intelligent Update options. Health Check will periodically ensure that the DCA service is operating, and if not, it will restart the DCA service. Intelligent Update allows the DCA to check for a receive software updates and DCA configuration changes posted by an administrator on the UpstreamConnect server. These features are enabled and disabled at the end user site, and are not required.

## DCA SEMAPHORE

<b>Deactivate</b>	Forces the target DCA to de-activate itself
<b>MIB Walk</b>	Forces the target DCA to request all available OIDs from the device whose IP is specified in the command's parameter.
<b>Redirect</b>	Forces the target DCA to stop files submission to its old PFE Server, to start submission to the PFE Server whose URL is specified in "ServerUri" parameter of the command, and , if "DeActivate" parameter is set to "True", to de-activate itself on the old PFE Server.
<b>Update</b>	Forces the target DCA to check for updated available for its current version and, if there are updates available, to upgrade itself using the update
<b>Uninstall</b>	Forces the target DCA to uninstall itself.



DCAs prior to 4.0 receive updates from the Printfleet hosted server *secure.printfleet.com*

DCA Semaphore functionality uses HTTPS (port 443 – recommended) or HTTP (port 80) for Semaphore Commands sending from the UpstreamConnect secure webserver to DCAs.

## DCA SERVICE BRIDGE

The DCA Service Bridge functionality allows Technicians to request a VPN connection to a networked imaging device from another network. A technician initiates a connection request by selecting the target device on the remote network, and which ports to access. The UpstreamConnect Server provides a PIN to the technician, but at this point, no communication has happened to the DCA or on the network the DCA is on.

The technician provides the PIN to a user to enter into the DCA graphical user interface (the DCA must be active on the UpstreamConnect Server). The user can then see the device's IP and ports being accessed, and accept or reject the connection. At any point, either the technician or the DCA user can close the connection. Communication to the UpstreamConnect Server is done using web services, using the same method as regular DCA communication/activation.

Service Bridge Session authorization leads to a Layer Two Peer-to-Peer VPN connection initialization between the technician's computer and the DCA Host computer, and then the DCA proxies requests to the device being accessed.

On both the DCA and technician sides, the VPN client connects to a *supernode* running on the UpstreamConnect Server (port 1685 udp/tcp), which negotiates a direct connection between the two, even if one or both is behind a NAT (network address translation) router/firewall. Communications between the two clients happens on a random high port (10000 to 65534) using UDP.

## UPSTREAMCONNECT WEBSITE

The UpstreamConnect website is the online interface for the UpstreamConnect system.

Permissions based user management access to the UpstreamConnect web site is controlled with permissions-based user management. Users must log in to UpstreamConnect website using a designated username and password.

Users are assigned one or more roles, which specify permissions, and are granted access to one or more groups of devices. Administrators with full permissions can specify exactly which screens each user can view and/or interact with.

## HTTPS ACCESS

The website can be accessed using HTTPS as the web server is installed with an SSL security certificate.

## UPSTREAMCONNECT SOFTWARE TESTING AND RELEASE PROCESS

Each major and minor release of the software goes through a quality control process, whereby multiple Upstream personnel test altered portions of the system to ensure there has not been a downgrade in security or functionality of the system. Major releases go through a beta release process where select clients run the new and old systems in parallel.



## UPSTREAMCONNECT SOURCE CODE SECURITY

The DCA source code is kept in a secured revision control system, accessible only to the Vendors development team. Every change to the source code is tracked, which includes which developer made the change, and why. Products are encrypted and digitally signed with a code-signing certificate before shipping.

### **Health Insurance Portability & Accountability Act (HIPAA) compliance is not affected by usage of UpstreamConnect software applications**

The use of DCA software applications will not have an impact on compliance with the Health Insurance Portability & Accountability Act (HIPAA) for covered entities. This is because UpstreamConnect software applications do not collect, house, or transmit any information regarding the content of print jobs, and thus have no way of accessing, housing, or transmitting electronic protected health information (ePHI) as defined by HIPAA.

For more information about HIPAA, visit <http://www.hhs.gov/ocr/hipaa/>

### **Sarbanes-Oxley compliance is not affected by usage of the UpstreamConnect software applications**

The UpstreamConnect software is not intended to be used as part of an internal control structure as outlined in Section 404: Management Assessment of Internal

Controls, but will not interfere with these controls.

Information Technology controls are an important part of complying with Sarbanes-Oxley. Under this Act, corporate executives become responsible for establishing, evaluating, and monitoring the effectiveness of internal control over financial reporting. There are IT systems in the market that are designed specifically for meeting these objectives. UpstreamConnect software is not designed as an IT control system, but will not interfere or put at risk other systems that are intended for that purpose.

For more information about Sarbanes-Oxley, visit <http://thecaq.aicpa.org/Resources/Sarbanes+Oxley/>

### **Gramm-Leach-Bliley Act (GLBA) compliance is not affected by usage of UpstreamConnect software applications**

The use of UpstreamConnect software applications will not have an impact on compliance with the Gramm-Leach-Bliley Act (GLBA) for covered entities. This is because the UpstreamConnect software applications do not collect, house, or transmit any information regarding the content of print jobs, and thus have no way of accessing, housing, or transmitting customers' personal financial information, even if this information is printed or otherwise sent to print devices monitored by the UpstreamConnect software applications.

For more information about the Gramm-Leach-Bliley Act, visit <http://www.ftc.gov/privacy/privacyinitiatives/glbact.html>

### **Federal Information Security Management Act (FISMA) compliance is not affected by usage of the UpstreamConnect software applications**

The UpstreamConnect software is not intended to be part of an internal control system for FISMA, but will not interfere with these controls.

The use of the UpstreamConnect software application will not have an impact on compliance with the Federal Information Security Management Act (FISMA) for covered entities. This is because UpstreamConnect software applications do not collect, house, or transmit any information regarding the content of print jobs, and thus have no way of accessing, housing, or transmitting high risk information, even if this information is printed or otherwise sent to print devices monitored by the UpstreamConnect software applications.

For more information about the Federal Information Security Management Act, visit <http://csrc.nist.gov/groups/SMA/fisma/index.html>

