Axess Security Overview

Axess software products only collect the 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:

- Axess Data Collector Agent and Local Print Agent software
- Axess web console

It is also explained why using Axess 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)

Axess Data Collector Agent and Local Print Agent Software Overview

The Axess 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 Axess 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 Axess Local Print Agent acts as a proxy between a Axess 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 Axess 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.

Axess DCA Activation and DCA Submission Authentication

Axess DCA has to be activated on prior to data submission to the server.
DCA Activation is managed by Axess Server Administrators and includes:

- Creation of a DCA Account on the Axess 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 Axess 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 Axess Server are revoked automatically; Axess Server Administrator also can revoke these credentials at any time by De-Activating the DCA. Data submissions from a DCA start being rejected by the AXESS Server immediately after the DCA Expiration Date comes or the DCA is De-Activated.

For DCAs v.4.0 and later, Axess 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 Axess 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 a AXESS Server and a DCA is stored in the Axess 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 Axess (Axess Server User Interface) nor other Axess 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 A Axess 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 Axess Data Collector Agent and Local Print Agent

The Axess DCA attempts to collect the following information from networked printing devices during a network scan:

Types of information collected:

IP address (can be masked)

Device description

Serial number

Meter reads

Monochrome or color identification

LCD reading

Device status

Toner levels

Toner cartridge serial number

Maintenance kit levels

Non-toner supply levels

Asset number

Location

MAC address

Manufacturer

Miscellaneous (machine specific)

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

Manufacturer

Device description

Serial number

Meter reads

OS version of Local Print Agent Host

Asset number

Location

MAC address

Miscellaneous (machine specific)

Name of the account used to run Local Print Agent service

IP address of the machine the Local Print Agent is installed on (Local Print Agent Host)

No print job or user data is collected.

Data collection methods

The DCA's versions 3.x and 4.0 collect networked imaging device metrics at a specified interval by polling networked devices using SNMP v1, ICMP, and HTTP. DCA's version 4.0 and later collect Local Device metrics at a specified interval by polling Axess Local Print Agents using TCP and UDP requests at a predefined port (port 35). Request and response data is transferred using Axess proprietary format.

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 different DCA versions:

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

It is recommended that users transmit data using HTTPS, because this provides SSL 128-bit encryption of the data during transmission. HTTP, FTP, and SNMP do not provide encryption. To transmit using HTTPS, the machine receiving the transmitted data must be installed with an SSL security certificate.

Data transmission formats

DCA's 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 AXESS 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. Axess software uses encryption providers integrated into the Microsoft .Net Framework to encrypt data exchange between DCA 4.0 and AXESS 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

Axess Web Console

Axess is the online interface used to access the collected information.
Permissions based user management

Access to the Axess web console is controlled with permissions-based user management. Users must log in to Axess 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 will full permissions can specify exactly which screens each user can view and/or interact with.
HTTPS access

The website can be accessed using HTTPS provided that the web server is installed with an SSL security certificate. Optionally, Axess administrators can force users to access the Axess website using HTTPS, by redirecting the HTTP version of the website. This is recommended, as it ensures 128-bit encryption of data being transferred over the Internet.

Network Compliances

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

The use of Axess software applications will not have an impact on compliance with the Health Insurance Portability & Accountability Act (HIPAA) for covered entities. This is because Axess 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 Axess Software Applications

Axess 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. Axess 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://www.sec.gov/about/laws/soa2002.pdf

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

The use of Axess software applications will not have an impact on compliance with the Gramm-Leach-Bliley Act (GLBA) for covered entities. This is because Axess 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 Axess 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 Axess software applications

Axess software applications are not intended to be part of an internal control system for FISMA, but will not interfere with these controls.
The use of Axess software applications will not have an impact on compliance with the Federal Information Security Management Act (FISMA) for covered entities. This is because Axess 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 Axess software applications.
For more information about the Federal Information Security Management Act, visit http://csrc.nist.gov/groups/SMA/fisma/index.html

QLS

QLS Solutions Group, Inc.
701 Seneca Street
Buffalo, NY 14210
(716) 852-2203
http://www.QLS.com
http://www.QLS.com/Blog