

Technical Note

Ref.: 173148.01.TN.A4

Date: 2018-09-27

AlphaStream NovaX61 Series

Information Assurance Document

DFE Controller

Preface

The purpose of this document is to disclose information for the AlphaStream system (hereinafter called as “the product”) with respect to device security. Device Security, for this paper, is defined as how image data is stored and transmitted, how the product behaves in a network environment, and how the product may be accessed both locally and remotely.

The purpose of this document is to inform Xerox customers of the design, functions, and features of the product with respect to Information Assurance (IA).

This document does not provide tutorial level information about security, connectivity, or the product’s features and functions. This information is readily available elsewhere. We assume that the reader has a working knowledge of these types of topics.

1. Target Audience

The target audience for this document is Xerox field personnel and customers concerned with IT security.

2. Disclaimer

The information in this document is accurate to the best knowledge of the authors, and is provided without warranty of any kind. In no event shall Xerox be liable for any damages whatsoever resulting from user's use or disregard of the information provided in this document including direct, indirect, incidental, consequential, loss of business profits or special damages, even if Xerox has been advised of the possibility of such damages.

Table of contents

Preface	2
1. Target Audience	2
2. Disclaimer	2
3. Device Description	4
4. Security-relevant Subsystems	5
4.1. Physical Partitioning.....	5
4.2. User Interface.....	5
4.3. Memory Components:	6
5. System Access	7
5.1. User Accounts log-in	7
5.2. Authentication Methods	7
5.3. Network Protocols	7
5.4. Data access	8
6. Security Aspects	10
6.1. Disks encryption	10
6.2. Data overwrite	10
7. Responses to Known Vulnerabilities	11
7.1. Security @ Xerox (www.xerox.com/security).....	11
Glossary-Lexicon	Error! Bookmark not defined.

3. Device Description



The *AlphaStream Nova X61 series* is a DFE (Digital Front End) able to distribute data directly to industrial inkjet printers of the *Xerox® iPrint®* product line:

- Xerox® Impika® Compact
- Xerox® Impika® Evolution
- Xerox® Impika® Reference
- Xerox® Trivor™ 2400 Inkjet Press

It is composed by several *DELL PowerEdge R630* servers. The number of server is designed according to the printer configuration and related to the power needed to manage jobs printing.

Through a user-friendly graphics interface, the AlphaStream software allows to add and manage jobs of different formats: PDF (Portable Document Format), AFP (Advanced Function Presentation), and PostScript. Once added, it is possible to schedule printing of these jobs through a print queue.

In addition, the software offers the possibility to automate adding jobs using of "Hotfolders", shared folders in which all files stored inside are automatically added as jobs.

Multiple PDF files can also be submitted as a single job using an archive file.

Moreover, this software also allows receiving a printing dataflow from an IPDS host system.

4. Security-relevant Subsystems

This section describes the physical methods to access the product and the relationship of the subsystems. It also describes the main security features and the subsystems that provide them. The next section describes the purpose of each subsystem as well as the memory components, which may possibly store user information.

4.1. Physical Partitioning

The overall structure of the product is as follow:

- Several *DELL PowerEdge R630* servers. The number of server is related to the printer configuration and related to the power needed to manage Jobs. These servers are linked together via an Ethernet switch.



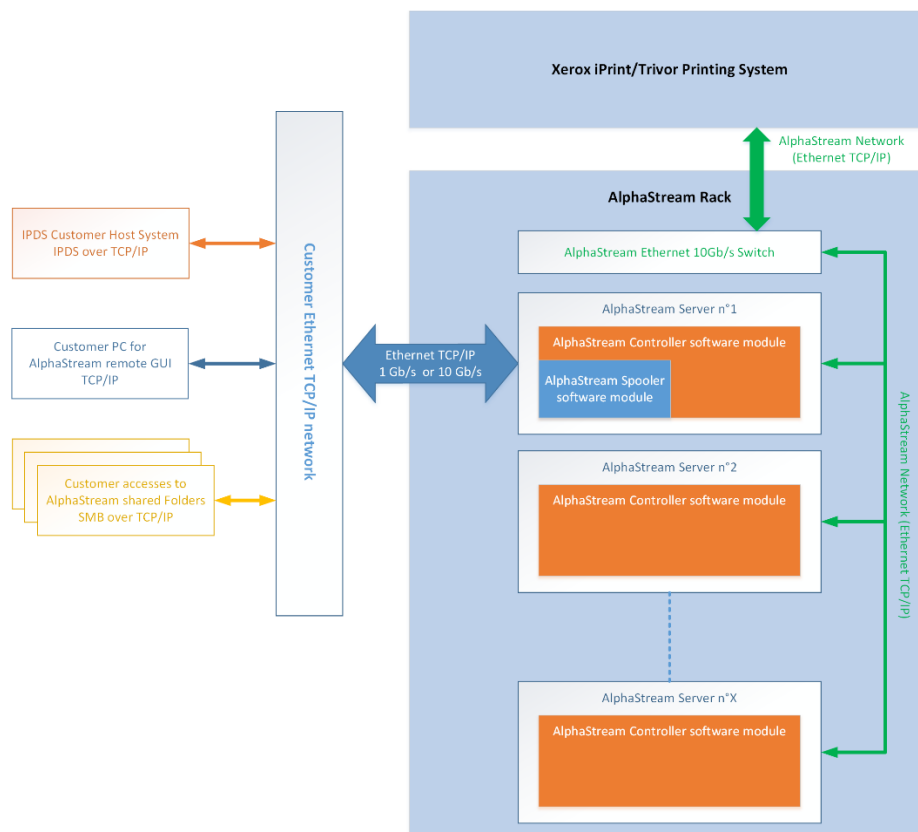
- The AlphaStream Spooler allows the management of PS, PDF and AFP jobs and their submissions to the AlphaStream Controller.

The AlphaStream Spooler is implemented on server #1.

- The AlphaStream Controller is the printer controller that manages the connection with an IPDS host or with the AlphaStream Spooler on one side and the printer on the other. It rasterizes data to print and make them available to the printer system.

The AlphaStream Controller is implemented on every server.

The figure below describes the overall structure of the product as well as the relationship of the subsystems.



It is important to note that the cabinets containing the *AlphaStream NovaX61* servers must be locked. The servers are only accessible by Xerox qualified people or authorized by Xerox.

4.2. User Interface

The Graphical User Interface (GUI) of the AlphaStream Spooler can be locally loaded on the AlphaStream server #1, only for maintenance and testing purposes, or remotely on a customer's PC.

It is a software application belonging to the Alphastream Spooler which mainly allows:

- To chain up all kinds of jobs (AFP, PDF, PS), in any order.

- To add jobs.
- To define jobs configurations (imposition, number of copies to print....)
- To delete jobs with/without settable delays.
- To create hot folders.
- To manage jobs printing.

About AlphaStream Controller, there is no dedicated user interface. This software is managed by the MMI of the printer.

See the Information Assurance Document of the printer for more information.

4.3. Memory Components:

Name	Purpose / Explanation
RAM	This volatile memory temporarily stores the data necessary to run AlphaStream software (Spooler and Controller). It also contains customers/jobs data during jobs processing. All data is lost when the product is power off.
SSD	This disk contains Operating System, system's settings information, jobs, user management information, and various types of logs. On normal operation, data are not modifiable by user.

See the external documentation "Statement Of Volatility of AlphaStream NovaX61 Series" for more information.

5. System Access

5.1. User Accounts log-in

There is only one Windows account to manage the system.

This account shall only be used by the qualified Xerox technicians for the maintenance of the AlphaStream system:

- System set-up.
- Initial system tests and validations (by using the local GUI of the AlphaStream Spooler)
- Update software versions.
- Restore the operating system.
- Replace hardware components.

This account and its password is only known by the qualified Xerox Technicians and shall not be provided to any other person.

So, in normal operation, no one is logged on the AlphaStream system and the AlphaStream Spooler GUI is only loaded on a remote computer of the customer.

About operation and settings of the AlphaStream Controller, as explained in the previous section, they are managed by the MMI of the printer. See the Information Assurance Document of the printer for more information.

5.2. Authentication Methods

A password of the Windows account described above is required for accessing to the system.

5.3. Network Protocols

The network protocols supported by the product are TCP/IP, SMB over TCP/IP and Ethernet.

- SMB over TCP/IP allows users to remotely access to Hot Folders and job resource directories of AlphaStream (see below). There is no specific authentication to access to these network folders: all those who have access to the AlphaStream system from the customer's network can deposit, retrieve and delete files there.

Access to the customer's network and its permissions is depending on the customer's security policy.

The rest of the system and other folders are protected by the Windows security of the AlphaStream servers (the local account login and password are not provided to customers/users. See section 5.1).

The following table lists the SMB versions supported by the AlphaStream X61 series and indicates these that can be disabled if desired:

Supported SMB version	Can be disabled?
1.0	YES
2.0 (including 2.1)	YES
3.0 (including 3.02)	NO

The Ethernet TCP / IP protocol is used to:

- The connection between the customer's IPDS host software and the AlphaStream system: there is no authentication required for this kind of connection. The IPDS over TCP/IP protocol is specific to the IPDS standard defined by the AFP consortium.
- The internal network to AlphaStream (Spooler and Controller): there is no authentication required but this network uses a proprietary overlay (property of TagG Informatique). This network is not accessible outside of the AlphaStream cabinet.
- The connection of the remote GUI of AlphaStream Spooler, loaded on a customer's PC: there is no authentication to connect the remote AlphaStream GUI to the AlphaStream system, but users can only manage the jobs contained in the spooler, add them and print them. They cannot interfere with the configuration of servers and cannot access to directories other than those described above and below. The user-accounts log-in of the customer's computer that loads the remote GUI of AlphaStream Spooler is protected by the customer's security policy.

5.4. Data access

- The resources:

Users can add and delete resources from shared directories (via the network over SMB protocol – see above) provided for this purpose (AFP resources, fonts, page backgrounds and images).
- Jobs:
 - Users can add jobs (AFP, PS, and PDF) from Hot Folders (via the network over SMB protocol) or from the "+" button on the AlphaStream Spooler GUI installed on the customer's computer in the customer's network.

Once a job is added to the system, it is automatically moved to a directory in the D partition of the AlphaStream Server #1, which is not accessible from the network. It cannot be retrieved: it can be printed and deleted, but there is no method to retrieve the source file of the job. Formatting the D partition or restoring the system, as described in the SOV, will completely reset D partition.
 - Printing an IPDS job is done via the IPDS TCP/IP connection dedicated to this purpose (see above): user's data are never stored on hard disk (except in the traces - see below) and are deleted of the memory (RAM) as soon as the job is printed or canceled.

To reset the RAM it is necessary to make a POPO (Put Off, Put On) of the servers of the AlphaStream system as described in the SOV.
- ICC profiles, linearization curves and TRC files:

This data can be uploaded in the AlphaStream system either from the MMI of the printer (ICC profiles, linearization curves and TRC files - see the IAD of the printer for more information) or by the AlphaStream Spooler GUI (ICC profiles only).

- Logs and traces:

These data are all stored in files contained in the C partition of each server of the AlphaStream system. Formatting the C partition or restoring these servers, as described in the SOV, will completely reset the C partition, deleting also the logs and traces files. These information are only used by the development team of AlphaStream to debug an issue.

- The AlphaStream Controller logs (audit logs) are permanently recorded. They do not contain any job data of the customers but can contain the jobs names. They are retrievable via the MMI of the printer (see the IAD of the printer for more information).

The types of information recorded in the AlphaStream Controller logs are:

- Versions of AlphaStream Controller software modules.
- Hardware information of the AlphaStream Controller (computers names, processors type, installed memory...)
- Configuration files of the AlphaStream Controller.
- Names of printed jobs.
- Settings defined by the user from the MMI of the printer (printer resolution, paper size, color management, IPDS option, drop sizes...).
- Messages and errors sent to the MMI of the printer and/or to the IPDS host system.
- Information of internal operations performed inside the software to communicate with the IPDS host software and the printing system, analyze the received dataflow, generate the output images and send them to the print heads.

There is no job data but only the sequences and the timing of the performed operations.

- Traces of the AlphaStream Controller are enableable and recoverable from the MMI printer (see the IAD of the printer for more information). They contain more information than logs and can contain job data (whatever the jobs format: IPDS, PDF, PS, AFP...).

There are three levels of traces that can be defined from the MMI of the printer:

- **Simple:** contains same information as AlphaStream Controller logs but information of internal operations performed inside the software are more detailed.
 - **Normal:** contains same information as the **Simple** level with the jobs data.
 - **Complete:** contains same information as the **Normal** level with the output images sent to the print heads.
- The AlphaStream Spooler logs (audit logs) are permanently recorded. They do not contain any job data of customers but contain the jobs names. They are retrievable from the AlphaStream Spooler GUI installed on the customer's computer in the customer's network.

They contain:

- Versions of AlphaStream Spooler modules.
- Prints screen of AlphaStream Spooler GUI taken when the logs are retrieved.
- All software settings.
- All jobs settings (jobs templates).
- All information of jobs contained in AlphaStream Spooler and not permanently deleted when logs are retrieved (see the User Guide of AlphaStream Spooler to permanently remove a job):
 - Name.
 - Number of pages.
 - All operations performed in AlphaStream Spooler with their timing (job added in the software, added in the print queue, archived, deleted...all printing sessions and all encountered problems where appropriate).

Remark:

- Logs and traces files recorded on the AlphaStream servers are encrypted if the encryption of the hard drives is enabled (see below).

Export of these files (from the MMI of the printer or from the AlphaStream GUI) are not encrypted.

6. Security Aspects

6.1. Disks encryption

The hard drives of the AlphaStream servers can be encrypted to prevent reading of customer's data in case of theft.

This encryption uses the BitLocker technology of Microsoft Windows Server 2012R2 operating system. It is based on the AES 128 bits algorithm.

It is applied on any data written on the hard drives of the AlphaStream servers, including through hot folders and resources folders.

See the documentation named ***TR.2017036.IK.EN - Configuration Bitlocker Nova X6X - V1.1*** to enable this functionality.

6.2. Data overwrite

There is no data overwrite method in the AlphaStream software.

7. Responses to Known Vulnerabilities

7.1. Security @ Xerox (www.xerox.com/security)

Xerox maintains an evergreen public web page that contains the latest security information pertaining to its products. Please see <http://www.xerox.com/security>

Xerox has created a document, which details the Xerox Vulnerability Management and Disclosure Policy used in discovery and remediation of vulnerabilities in Xerox software and hardware. It can be downloaded from this page:

<http://www.xerox.com/information-security/information-security-articles-whitepapers/enus.html>