



# DNA

## White Paper

Prepared by

**Ian Silvester**  
**DNA Manager**

Danwood Group Service  
Noble House  
Whisby Road  
Lincoln  
LN6 3DG

Email: [dna@danwood.com](mailto:dna@danwood.com)

Website: [www.danwood.com\dna](http://www.danwood.com\dna)

BI portal: <https://biportal.danwood.com>

## Contents

<b>Introduction .....</b>	<b>3</b>
<b>Device Discovery .....</b>	<b>4</b>
<b>Network Print Device Monitoring.....</b>	<b>5</b>
<b>Information Collected.....</b>	<b>5</b>
<b>Device Alerts – Enterprise Version only.....</b>	<b>6</b>
<b>Consumables Management.....</b>	<b>7</b>
<b>Billing and Reporting.....</b>	<b>7</b>
<b>Communication.....</b>	<b>8</b>
<b>Number of Devices Supported.....</b>	<b>9</b>
<b>Device Support.....</b>	<b>9</b>
<b>DNA Enterprise Server Hardware and Operating System Specification.....</b>	<b>10</b>
<b>SQL Server.....</b>	<b>10</b>
<b>Server specification guidelines for DNA Data Collection Application (DCA) .....</b>	<b>10</b>
<b>Virtual Machines .....</b>	<b>11</b>
<b>Data and Network Traffic.....</b>	<b>11</b>
<b>Network Ports .....</b>	<b>11</b>
<b>Firewall Rules.....</b>	<b>12</b>
<b>NHS Firewall Rules .....</b>	<b>12</b>

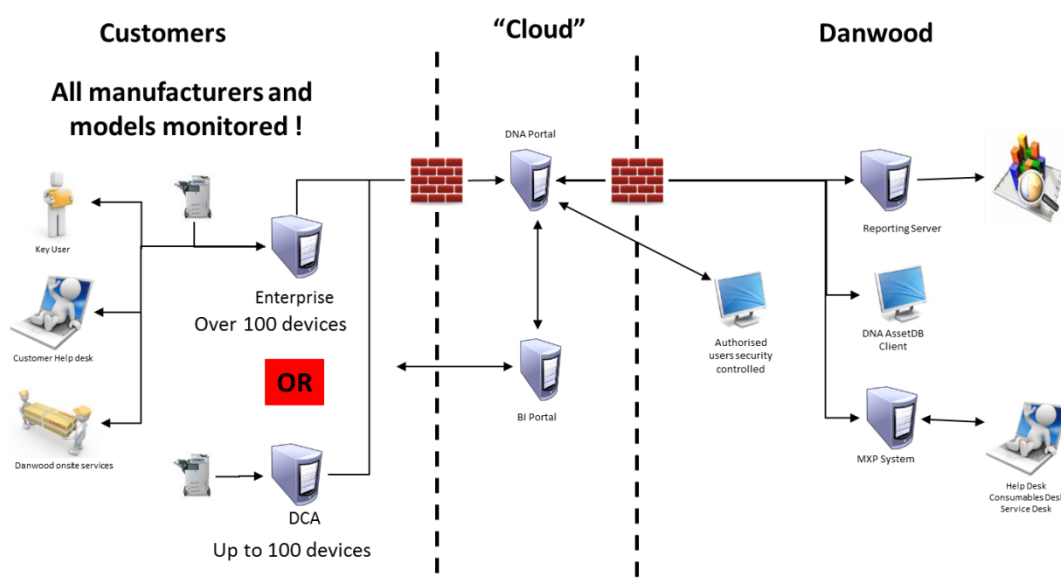
## Introduction

The purpose of this White Paper is to provide a technical overview of the Danwood DNA Device Monitoring Architecture.

DNA Device Monitoring Architecture is a solution designed to support the delivery of Managed Print Services for Danwood. It supports delivery of automated billing, consumables management and provision of management information. In addition, it can support initial fleet re-design / optimisation and allow on-going continuous improvement of the fleet and operational processes. The DNA monitoring architecture is based on the Insight II product developed and owned by EKM Global. The DNA BI Portal is solely developed by Danwood.

DNA comprises four core elements as described below;

- **DNA Monitoring Servers**
  - **DNA Enterprise Server** – For larger fleets and for customers with special requirements, installed on a server on the Customer's network to collect information from network print devices.
  - **DNA Data Collection Application (DCA)** – for smaller fleets, installed on a workstation or server on a customer's network to collect information from network devices. The DCA is also used to gather data for use with the Danwood AssetDB Manager.
- **DNA Portal Server** – installed in the 'cloud' to process all information received from the DNA Enterprise and DCA Servers. The Portal Server also has a messaging server component in the same cloud
- **DNA Reporting Server** - installed in Danwood's Data Centre providing management reports and billing data.
- **DNA BI Portal Server** – shows DNA data on asset, meters and consumables and is available to all DNA customers



## **DNA Monitoring Servers.**

The DNA monitoring servers discover and monitor network devices using only SNMP requests on port 161.

The DNA applications are Java applications that run as a single Windows service. Working data is stored in an internal database (Derby Apache) and in the Enterprise version the relevant device information is stored in a Microsoft SQL Server 2008 (or above) database which can be installed on the same server or a separate physical server or cluster.

Management of DNA Enterprise Server is provided through a web interface running over HTTPS. Danwood will require remote access to the server running the DNA Enterprise system to manage and maintain the system. The web interface is provided by a custom version of the Apache Tomcat 7 application server built into and installed with the application.

Management of the DNA DCA application can be performed remotely although remote access is preferred.

Data is transmitted to the Danwood Portal Server via the internet using XMPP over tcp port 5222 or 443.

The DNA Portal Server processes this information and initiates service delivery via integration with Danwood's ERP System.

## **Device Discovery**

During the initial fleet take on the DNA Enterprise and DCA applications are configured to discover network print devices connected to the Customer's network using defined IP address ranges, single IP addresses or hostname. IP ranges preferably with an associated location (defined as a zone in the software) may also be required in order to ensure all devices are found. If an accurate device asset list with IP addresses is available then this can be imported into the system via a simple CSV.

The discovery process is designed to create minimal network traffic. The discovery process is run at regular intervals to identify changes to the fleet e.g. new or changed devices. Once a device is found it is added to the Asset List and the DNA applications can begin to monitor the device.

The DNA discovery does not broadcast, multicast or ping, it uses an SNMP lookup on port 161. Whilst this is not the fastest method of discovery it is comprehensive and designed to work within working hours with no impact on an operational network.

If a device is relocated then the system will perform a reverse DNS lookup to attempt to relocate the device. If the devices are relocated onto an existing IP address it will be identified as a change and the IP address adjusted accordingly. Further checks are made to ensure that the MAC and Serial numbers of a device are not changed.

## Network Print Device Monitoring

Network device monitoring uses the SNMP protocol on port 161 using UDP. DNA Enterprise Server supports SNMP V1, V2 & V3. SNMP V2 provides the best performance together with minimal network traffic. The extra security requirements of SNMP V3 create extra performance and administration overheads so should be avoided unless the additional security is necessary.

The monitoring process comprises five independent sub-processes that scan devices to confirm that they are responding and if so collect device asset information. If a device is responding then alerts, consumable, media levels and page count data is collected. Device monitoring processes are self optimising with each sub-process only reading the specific information it needs to perform its specific task thereby minimising network traffic and maximising the number of actively monitored devices possible per server. The timing of the sub-processes is optimised such that information that is less time critical e.g. page counts is retrieved less frequently than time critical information e.g. device alerts.

The majority of information used by DNA is retrieved from the standard Printer MIB (RFC 1759). Additional information such as detailed page counts is retrieved from the Manufacturer's Private MIB if available

## Information Collected

DNA Applications do not collect any user identifiable information from the network print device. Although many print devices do record job information, DNA does not retrieve this information.

DNA Applications send five key types of information back to the DNA Portal Server:

- *Device Information* – manufacturer, model, location, device identification, hostname, MAC address, url
- *Volume Information* – page counts recorded by the print device
- *Alert Information* – alerts reported by the print device
- *Consumable Information* – consumable levels reported by the print device
- *Media Levels* – Media (paper tray) levels in the device

## **Device Alerts – Enterprise Version only**

DNA Applications retrieve alert information from the alert table in the MIB (Management Information Base) of the network print device. Network print devices generate a wide range of alerts which can potentially lead to a fleet of devices generating a large number of alerts. The DNA Monitoring servers support an intelligent alert triage processes. This enables the system to review each alert and based on a set of rules determine the action required e.g. ignore, record or send to the Customer for action.

Each alert contains four basic components:

- Description – text description of the alert e.g. fuser unit failure
- Code – standard public MIB code as defined in RFC 1759
- Severity – e.g. critical
- Resolver Group - e.g. trained user, engineer

Rules based on MIB code, Severity and Resolver Group define the action to take with each alert, and these actions include:

- Ignore
- Record
- Send
- Delay and Send

The alerts produced by each device are defined by the Manufacturer and typically report 'physical' events and errors. The 'events' that DNA can monitor are therefore limited by the alerts defined by the Manufacturer. DNA therefore cannot support the automation of all 'events' that would require engineer intervention. A simple example of this would be image quality issues.

The key purpose of the triage processes is to ensure that only alerts that require active intervention are addressed and that these are forwarded to the appropriate location within the Customer to action when using the DNA Enterprise software.

Whilst the alerts are transmitted to the Danwood DNA portal, these are only for Management information and reporting and they do not currently trigger an engineer call out

## Consumables Management

DNA Applications retrieve consumable level information from the MIB of the network print device. The DNA Applications use two methods to determine if a consumable will require replacement.

Firstly, the consumable analysis module uses an algorithm to predict consumable use for each device and therefore determine when the device will require a new consumable. This triggers a toner request to Danwood to ensure toner is delivered before the predicted run out date. Secondly, the consumable analysis module can determine the current consumable level in a device and a toner request is triggered when actual levels fall below a specified level (normally 15%). When either of these methods determines that a consumable is required, information is passed to the DNA Portal Server and into Danwood's consumable management processes to ensure consumables are delivered to the Customer.

Some manufacturers do not include accurate or detailed consumable level information in the MIB. In these cases the DNA Applications use device alerts where possible to trigger consumable requests.

DNA can monitor all items defined by the manufacturer as a consumable and included in the MIB of the device.

The main exception are waste toner bottles as these generally provide a "full" or "not full" status to the DNA Software. Whilst DNA sees the full status the device has by that time stopped and so an automated delivery will not arrive in time. It is therefore recommended that waste bottles are manually ordered at the moment.

## Billing and Reporting

DNA Monitoring Applications retrieve page count information from network devices, Page Count information is passed to the DNA Portal Server and then onto the DNA Reporting Server. The DNA Reporting Server has two key functions. Firstly, it processes page counts and transfers data to Danwood's billing system. Secondly, it provides management information to support service account management.

Hardware manufacturers have not agreed a 'standard' list of page counts. This has lead to the situation where some simple devices (such as A4 mono printers) have only a single page count and other more complex devices (such as A3 colour multi-functional devices) have upwards of 250 different page counts! Danwood have developed a consistent method of concatenating the multitude of page counts into mono and colour 'clicks' for billing. This is an automated process that ensures accurate and consistent page count data.

## Communication

There are two key forms of communication between the DNA Monitoring Applications and Danwood. Firstly, print device information is sent to Danwood using the XMPP protocol. Secondly, management of the DNA Enterprise Server requires some form of VPN/Remote access. This can be the Customer's standard VPN or remote access solution. Danwood recognise the security implications of remote connections and are willing to follow each Customer's standard security policy and procedures. If remote access is not available this will severely restrict management and support of the DNA Enterprise Server.

Print device information is communicated to Danwood via XMPP using tcp port 5222 or 443. Communication conforms to the XMPP standard and supports SSL. Data is coded in a custom XML format and is encrypted using a SHA-256 / Base64 encryption algorithm.

XMPP is an open standard which employs point of presence communications including store and forward in the event of lost communication. To enable this communication any Customer Firewalls will require an additional rule that allows the DNA Enterprise Server to communicate with the DNA Messaging Server.

The rule is required to be an outbound only connection with TCP session capability once connected. This ensures that the connection is only ever initiated from within the customers network

Each of the DNA Monitoring Applications and the DNA Portal Server have to be rostered with a user name and password which ensures highly secure and reliable communications. The DNA Monitoring Applications and Portal Server can only send messages to and receive messages from servers that they are rostered with.

Messages are only sent when the destination is 'available' to receive the message. When the destination is not 'available' the sending server will store the messages ready to forward them when communication is restored.

Where the DNA DCA is used as part of a Danwood Audit and Analysis the connection to the portal will be required to allow the data to be easily transferred into the AssetDB audit and Analysis application.

Alert communication using the Enterprise version of the software within the customer is via email using standard SMTP over tcp port 25 and can support authentication. The email format can be customised as required. This will require the DNA Enterprise Server to have access to an SMTP email server.



## Number of Devices Supported

The number of devices that can be monitored by a single DNA Enterprise Server depends on a variety of factors including network speed, age and complexity of the printer fleet, DNS efficiency, the capability of the MS SQL Server, the longest allowable alert response time, the processor speed and memory capacity of the actual DNA Enterprise Server. It is therefore not possible to provide a definitive answer. As a guide, typically one Enterprise server can handle between 100 and 5,000 physical devices. If there are more devices to be monitored multiple DNA Enterprise Servers can be deployed.

A DNA DCA server will typically support upto 100 devices for full operational monitoring

## Device Support

The data available from different network print devices is variable, and not all manufacturers implement SNMP in full accordance with RFC standards.

In general, post-2004 network printers from major manufacturers are likely to supply all or most of the required data, but there is NO industry agreement on the information that should be available from each device model.

## DNA Enterprise Server Hardware and Operating System Specification

It is **recommended** to use a dedicated server to host DNA Enterprise Server. If additional applications are installed that generate significant network traffic, this will interfere with DNA Enterprise Server's device monitoring processes. The DNA deployment package includes MS SQL 2008 Server Express.

The minimum hardware specification for the DNA Enterprise Server is as follows:

Fleet Size	Minimum Specification	Recommended Specification
100 - 1,000 devices	Dual Core 'Server' CPU 3 GB RAM 60 GB hard disk 10/100 Ethernet Windows Server 2003 or higher SQL Server Express 2005 or higher	Dual Core 'Server' 2.0 GHz CPU 4 GB RAM 100 GB hard disk Gigabit Ethernet Windows Server 2008 or higher SQL Server Express 2008 or higher strongly recommended
>1,000 (or if application is located on existing application server)		Customer specific evaluation and recommendation required

## SQL Server

Microsoft SQL 2008 Server Express is included in the standard DNA Enterprise installation package. DNA Enterprise can also be configured to support a full Microsoft SQL Server installation either on the local or remote server. To support a full SQL Server installation, SQL Server must be configured to support mixed authentication, Named Pipes and TCP/IP. SQL 2012 is also supported.

## Server specification guidelines for DNA Data Collection Application (DCA)

DNA Data Collection Application monitoring up to 100 devices

	Minimum Specification	Recommended Specification
<b>Processor</b>	Single CPU, Intel Atom or AMD low power notebook CPU	32bit Dual Core CPU processor
<b>Memory</b>	1.0GB	2.0GB DDR2 or higher DRAM
<b>Hard Disk</b>	20Gb (100MB per 100 printers pa)	40Gb ATA133 or SATA
<b>Network</b>	10/100 Base T Full Duplex Ethernet	Gigabit Full Duplex Ethernet
<b>Operating System</b>	Windows XP SP 3 Windows Server 2003 SP2 Windows Server 2008 R2 Windows 7	Windows XP SP 3 Windows Server 2003 SP2 Windows Server 2008 R2 Windows 7

The DCA software can be located on an existing server but it is recommended that the server / workstation has at least 4Gb RAM is available to ensure good performance. The DCA server / workstation also needs to be running 24 x 7 to ensure all data is transferred to the DNA portal.

## Virtual Machines

Virtual Machines (VM) are supported for hosting DNA Enterprise and DCA Servers. However, this does require careful planning to ensure that the virtual network infrastructure is configured to support the requirements of the DNA Enterprise Server. DNA Application Servers require constant access to the network to constantly monitor devices.

It may be required that inbound packet tagging is required to be turned on to ensure good performance, this however depends on the number of VM's on a physical server / farm and the amount of network traffic being generated. A server administrator should monitor the performance and adjust the parameters as required.

## Data and Network Traffic

SNMP network traffic generated by the DNA Monitoring Servers is generally less than 10Kbits per second.

XMPP network traffic generated by the DNA Monitoring Servers is on average less than 1Kbits per second.

Each print device generates approximately 1 Kbyte per device per day. Alternatively this can be viewed as 25 devices creating the same data as a single A4 text only page sent to print.

With regards to data growth for the Microsoft SQL Server, each device generates on average 1.5 MB of data per annum.

## Network Ports

DNA Monitor Software uses the following TCP/IP ports - Customer Network:

Protocol	Port	Function
SNMP	Port 161 UDP	Network Print Device monitoring – communication to/from DNA Enterprise Server and Print Devices
HTTPS (SSL/TLS)	Port 443 TCP	Access to DNA web management interface.
HTTPS (SSL/TLS)	Port 50000 TCP (configurable)	Access to DNA web management interface when IIS is installed
SMTP	Port 25 TCP	Internal Customer email communications e.g. email alerts to Customer Helpdesk DNA Enterprise Server communication during Due Diligence

Communication to Danwood:

Protocol	Port	Function
XMPP	Port 5222 TCP (or 443)	Data communication to Danwood
VPN	Customer Specific	Remote access to DNA server

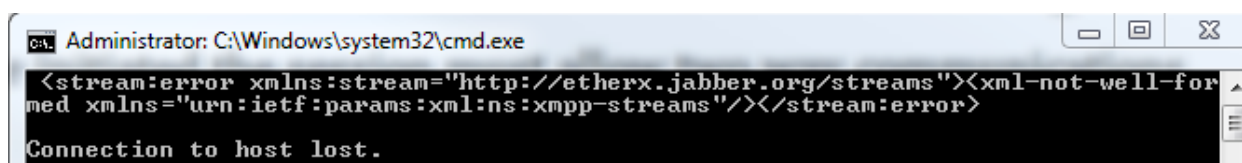
## Firewall Rules

For XMPP traffic the rule must allow the DNA Monitoring Servers to initiate a session with the Messaging Server. Once initiated the session must allow two way communications via a TCP session. The connection is only ever initiated from inside the customers firewall, it cannot be 'woken up' from outside

- Public IP: 168.63.28.202
- Address: dnaxmpp.danwood.co.uk

This can be tested by using a telnet session to the above IP / Address

- "telnet dnaxmpp.danwood.co.uk 5222" (or 443)
- Press Ctrl-C to exit the session
- This will generate a stream error if successful (see below)



```
Administrator: C:\Windows\system32\cmd.exe
<stream:error xmlns:stream="http://etherx.jabber.org/streams"><xml-not-well-for
med xmlns="urn:iETF:params:xml:ns:xmpp-streams"/></stream:error>
Connection to host lost.
```

NB: testing on port 443 will only show a blank screen, no stream error will be shown, this however IS a successful test

## NHS Firewall Rules

For NHS Organisations an additional XMPP Messaging Server is located within the N3 network to provide secure communications. This connection is outbound only, in order to setup the connection a completed Danwood N3 Firewall configuration document will be required

- Public IP: 10.199.104.165
- Address: dwpapp02

This can be tested by using a telnet session as explained above to the above IP / Address

- "telnet dwpapp02 5222"

## Server naming conventions

If a new server is provisioned please do not name it "Danwood" or "DNA" as this can lead to licensing issues with the software.