Security Datasheet

DS-40i/64i/75i/85i/95i

quadient
Because connections matter.

Table of Contents

Preface

In a world where security and information integrity are playing a key role in businesses, it is important to know the behaviour of a device, and to understand what data is transferred.

This document is to give details on the connectivity features of Quadient folder inserters in the range of DS-40i up to DS-95i for network administrators and/or security officers.

The information reflect the situation for factory produced devices per the revision date in this document. Devices produced before the revision date are upgradable by migration/software update(s). Consult a service representative for the possibilities.

***Note**: This security sheet refers to the Document Systems as mentioned on the front page. To always obtain the latest security information refer to the relevant product page on kb.quadient.com for the newest and latest version of the security sheet for your system.*

General information

Physical interfaces

The DS-40i folder/inserter has 1 physical and 1 wireless interface.

Interface type	Purpose
WLAN IEEE 802.11 b/g/n (2.4GHz)	Wireless adapter for all online services
USB 2.0	Service activities (i.e. software update) and job history download

The DS-64i~DS-95i folder/inserters have 3 physical and 1 wireless interfaces.

Interface type	Purpose
Ethernet IEEE 802.3 (10/100/1000Mbps) *)	Wired adapter for all online services
WLAN IEEE 802.11 b/g/n (2.4GHz) *)	Wireless adapter for all online services
USB 2.0	Service activities (i.e. software update) and job history download
9-pin D-sub female proprietary port	Socket for integration with other peripherals (i.e. franking machines)

*) Adapters cannot be used simultaneously

Operating System

- **DS-40i**
  Platform: CMX for ARM Cortex M4
- **DS-64i ~ DS-95i**
  Platform: Linux Kernel
  Details: Linux 4.9.88 for IMX6

Network properties

IPv4 address assignment

- **DS-40i**
  The device can only obtain this information from a DHCP-server on the network. For full functionality, IP-address, subnet mask, gateway and DNS server-address are required, and should be provided by the DHCP-server.
- **DS-64i ~ DS-95i**
  The device allows manual assignment of IP address, subnet mask, gateway and DNS server-address, as well as obtaining this information from a DHCP server on the network.

Required Services

By default, the device resolves addresses for online services through a programmed DNS server. In case there is no DNS server on the network, it is possible to enter static IP addresses instead.

Supported Proxy Authentication Types

In case of a proxy server on the network, the following authentication types are supported:

- Transparent
- Basic
- NTLM v1.0

DS-40i does not support any proxy authentication type.

Network security

Protocols over TCP / IP

All communication over the network interfaces takes place over IPv4. The protocols used to ensure secure connections are:

- **DS-40i**
  TLS 1.2
- **DS-64i ~ DS-95i**
  TLS 1.2 from OpenSSL 1.0.1.e toolkit
  OpenVPN from OpenVPN 2.3.1 toolkit
  SSH from OpenSSH 6.2p1 toolkit (only in developer mode)

Open Ports

There are no open ports on DS-40i ~ DS-95i that can be exploited.
One exception on DS-64i ~DS-95i is TCP port 7777, intended for manufacturing purposes. This port is open the first 10 minutes after power-up. The port requires a correct SSL certificate to function. With 10 minutes passed, the port is closed and no longer detectable by a port-scanner.

Network Features (depending on model)

Web browser

The device is equipped with a built-in web browser. Cookies and browser history will be stored for the active session. Both are deleted when the browser is closed or the device is turned off.

Date and time synchronization

For a number of online features to function properly, correct date and time information is key. Once the time zone is selected, the input is used to get date/time information with a http GET from URL: https://connectedds.neopost.com/

Depending on time zone settings, the server responds with a date/time in the message body in the ISO 8601 format, i.e. 2019-03-06T16:41:16+01:00

The device synchronizes date/time automatically after start-up.

Online features

The device checks for permanent and temporary features at start-up and at least once a day with a http GET from URL: https://connectedds.neopost.com/

The device sends it serial number to the server. In return, the server responds with data with the use of a SHA-256 hash.

Online Software Update

When accessed through the Service menu, it is possible to do an online software update. Availability of software is invoked with a http GET at URL: https://connectedds.neopost.com/

The device sends serial number and model information to the server. In return, the server responds with available software update(s) to the device, to be displayed in the Service menu.

NeoStats upload

Usage data in the form of logfiles is uploaded with a http POST to URL: https://connectedds.neopost.com/

There are multiple moments programmed when the data is to be transferred from the device to the server

Inside the logfile, the following event types are reported:

Event	Timing / Interval
Software overview	Start-up
Job Summary	Once a day
State	Each operational state change
Job started	Each job start (pressing Start)
Insert	Each completed mail piece
Incident	Each raised incident (error and/or warning)

All incidents cleared	Each instance when incidents are cleared

The uploaded data does not contain personal data, nor scanned data from the optional image scanner.

Remote Assistance

With this feature, the user interface is shared to a remote operator. There is no direct connection between the device and the remote operator. A server in between, referred to as Remote Assistance server, acts as a buffer.

Next to viewing the UI, diagnostics data can be collected by the remote operator and after consent of the operator at the device, the remote operator can gain remote control.

Personal data is not captured and UI screens from the remote session are not stored.

- Between RA server and remote operator via web browser

The remote operator is logged on to https://ra.qdtmail.com/ with a username and password and starts a session. This results in the 4-digit shared key, to be shared with the operator at the device, and acts as a pin code to start the remote session with the device.

- Between device and RA server http://ra.qdtmail.com/

Directly after entering the shared key, an OpenVPN tunnel is started between device and the RA server. When established, data is exchanged via this VPN tunnel.

For DS-40i, an additional server http://lra.qdtmail.com/ is implemented. The LRA server sits in between the device and RA server and has a direct (internal) connection to the latter.

Online help

An online version of the user guide, context sensitive help and frequently asked questions are accessed through https://kb.neopost.com/ineo/document+systems/ds-*xx*i/ineofeedreference , where *xx* represents the device model.

Automated Insertion Management System

The device sends data to a data station, which allows the management and analysis of job-runs. The connection takes place over TCP port 2002, by default. The information that is read is passed to the AIMS data station, either on premise or as a cloud solution. For details on the security features of AIMS, please refer to the AIMS admin guide, provided with the AIMS solution.