

Neopost Security Datasheet

DS-40i/64i/75i/85i/90i/95i

"Your security, our commitment!"

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 Neopost folder inserters in the range of DS-40i up to DS-95i for network administrators and/or security officers.

As a general reference, the Neopost DS-64i folder inserter was evaluated by a third party ethical-hacker. The results of these tests are adopted in the section Network features.

Operating System

DS-40i

- Platform: CMX for ARM Cortex M4

DS-64i ~ DS-95i

- Platform: Linux Kernel
- Details: Linux 3.0.35 for IMX6

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/inserter 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

Protocols over TCP/IP

All communication over the network interfaces takes place over IPv4. The used protocols 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)

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.

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 Types

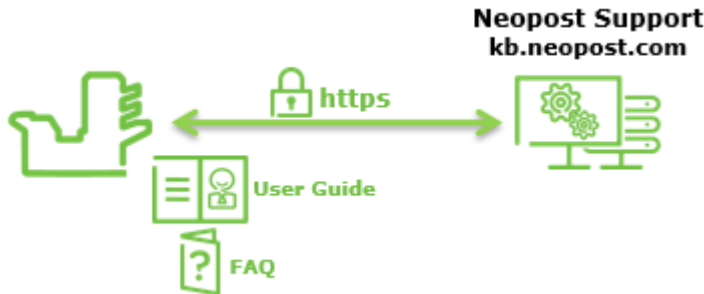
In case of a proxy server on the network, the following types are supported

- Transparent
- Basic
- NTLM v1.0

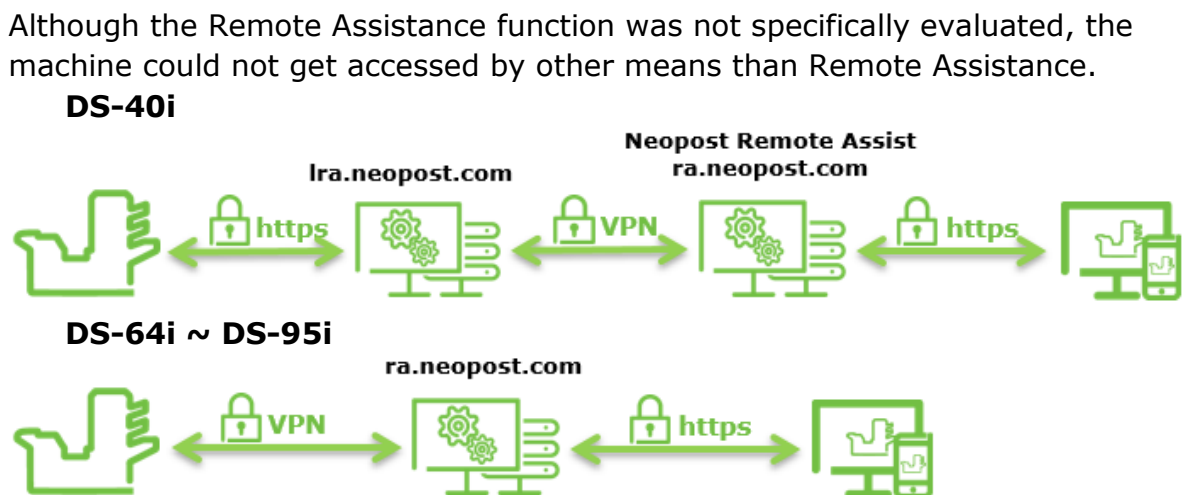
DS-40i does not support any proxy type.

Network Features (depending on model)

- **Online help** (option): An online HTML version of the user guide, context sensitive help and frequently asked questions are accessible with this feature. All information is retrieved over TCP port 443 (https), using TLS 1.2 protocol. No vulnerabilities were observed during evaluation.



- **Remote Assistance** (option): With this function, on request of a service organisation, the user can share the user interface for optimal support. Directly after the shared key is entered, an OpenVPN tunnel is started between folder/inserter and a remote assistance server. When established, data is exchanged via this VPN tunnel. The helpdesk operator from the service organisation receives the images from the user interface over an https connection with the server. In mode Remote Control, the remote operator can operate the user interface remotely. The remote operator has the ability to take a snapshot of the system information for diagnostics purposes, which contains data about errors that occurred, counter items, installed software and licensed features. It does not contain personal data. For DS-40i, an extra server Ira.neopost.com is implemented with a secure connection using TLS 1.2 protocol.



DS-40i

DS-64i ~ DS-95i

- **Data Upload** (option): In order to review the usage of the device, usage data is uploaded to a central server via a http post over TCP port 443 (https).

The transferred data contains information about the programmed jobs, events that have occurred on the folder/inserter and counter items. It does not contain personal data.

Although the Data Upload function was not specifically evaluated, there were no vulnerabilities found.



- **AIMS** (option): 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-datastation on a separate network (advised). For details on the security features on AIMS data station, please refer to the AIMS admin guide.



Open Ports

On DS-64i ~ DS-95i, TCP port 7777, intended for manufacturing purposes, will remain open the first 10 minutes after power-up. This port requires a correct SSL certificate to function.

Miscellaneous

- **Web browser:** The folder/inserter 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.