Direct WLAN Certificate Downloading in Link-OS v3.0

Overview

As of Link-OS v3.0, Zebra's Link-OS printers support downloading PEM and DER formatted WLAN certificates for the TLS, TTLS, and PEAP security types. Additionally, P12 formatted certificates are now supported for downloading private keys, which may include the client certificates as well.

Introduction

Selected WLAN security types require certificate files be loaded on the printer so that it can be authenticated to the network. Here is the list of certificate file types and associated file names that must be stored on the printer when using different WLAN security types:

Security Type	Files Type	File Name on printer
EAP-TLS WPA-EAP-TLS WPA2-EAP-TLS	Root certificate file	CACERT.NRD
	Client certificate file	CERTCLN.NRD
	Client Private Key	PRIVKEY.NRD
EAP-TTLS WPA-EAP-TTLS WPA2-EAP-TTLS	Root certificate file	CACERTSV.NRD
PEAP WPA-PEAP WPA2-PEAP	Root certificate file	CACERTSV.NRD

Prior to Link-OS v3.0, printers required that the WLAN certificate files be stored on the printer in the PEM format. Users who created WLAN certificate files in the DER (.der) or P12 (.pfx) formats then had to convert them into the PEM format using the open source Opensll.exe utility. Details on this process are here

New In Link-OS v3

Link-OS v3.0 introduces these changes:

- P12 formatted certicates (.pfx) are now supported for the purpose of placing private keys and client certificates on the printer, within the PRIVKEY.NRD file. P12 files can be used with the EAP-TLS, WPA-EAP-TLS and WPA2-EAP-TLS security types.

Note: When using TLS, you will need to use the SGD `"wlan.private_key_password"` command if the private key is encrypted. The command works in the following way:

```
! U1 setvar "wlan.private_key_password" "value"
```

Where "value" is an alphanumeric string, up to 32 characters in length. The command must be followed by a carriage return or a space character.

- PRIVKEY.NRD: If P12 encoding is used it must contain the private key, and may optionally also contain the client certificate. This allows the client certificate to be P12 formatted, so long as it is in the same file as the private key. When this is the case, no CERTCLN.NRD should be loaded on the printer.

NOTE. If using TLS, the printer will check for the presence of a CERTCLN.NRD file. If it is not present, the printer will assume the client cert is in the PRIVKEY.NRD file.

- WLAN certificate files in the DER (.der) format can be directly downloaded to the printer, so long as the naming scheme noted in the **Introduction** above is used.

- For TLS all of the files do not need to be in the same format. Example: PRIVKEY.NRD can be in P12 format, CERTCLN.NRD can be in DER format, and CACERTSV.NRD can be in PEM format.

Use Cases

- Printer administrator receives a P12 formatted file, which includes the private key and client certificate. This file can be loaded onto the printer as PRIVKEY.NRD and used as is.

- Printer administrator receives certificate files encoded in the DER format. These files can be loaded onto the printer with the specified name(s) and used without format conversion.

Usage Details

1) Gather the appropriate certificates and private key files, as noted in the **Introduction** above.

2) Download files using the instructions noted below in "**Certificate Downloading**".

Certificate Downloading

1) There are three options for downloading the certificate files to the printer:
    1. **FTP:**
        a. If using FTP, make sure the printers “execute file” function is turned off while you send the file, so that the file is stored and not processed as a printing command. This can be done by sending the following command:

```
! U1 setvar "ftp.execute_file" "off"
```

NOTE: The command must be followed by a carriage return or a space character. If you plan on using FTP for printing purposes, be sure to reset this feature to `"on"` after storing the WLAN files.

        b. Connect to the printer via FTP and download the certificates files appropriate to the security being used. Use the CACERTSV.NRD, CERTCLN.NRD and PRIVKEY.NRD file names as noted above.

    2. **Zebra SDK:**
        a. Use the Zebra Multiplatform SDK command line STORE function to send the files to the printer's E: drive. The SDK is available for download at www.zebra.com

        b. Use the CACERTSV.NRD, CERTCLN.NRD and PRIVKEY.NRD file names as noted above.

    3. ZPL or CPCL:
        a. CPCL: use the ! CISDSF command, with the appropriate headers to the certificate to store the files on E drive of the printer. This can be done using the “Send and Store file in printer memory” feature in the Zebra Setup Utility (available when a CPCL printer is used).

        b. ZPL: use the ~DY command, with the appropriate header. Details available in the ZPL Programming Guide, available at www.zebra.com

        c. Use the CACERTSV.NRD, CERTCLN.NRD and PRIVKEY.NRD file names as noted above.

2) Configure the printer for other appropriate WLAN settings as needed (i.e. band, security type, WLAN Country, IP addressing, etc).

Document Control

Version	Date	Description
1.0	August 28, 2015	Version 1 released in Agile on Aug 31, 2015

Disclaimer

All links and information provided within this document are correct at time of writing.