Link-OS™

PrintSecure

Printer Administration Guide

ZEBRA

P1099957-002

Terms of Use

Proprietary Statement

This manual contains proprietary information of Zebra Technologies Corporation and its subsidiaries (“Zebra Technologies”). It is intended solely for the information and use for parties operating and maintaining the equipment described herein. Such proprietary information may not be used, reproduced, or disclosed to any other parties for any other purpose without the express, written permission of Zebra Technologies.

Product Improvements

Continuous improvement of products is a policy of Zebra Technologies. All specifications and designs are subject to change without notice.

Liability Disclaimer

Zebra Technologies takes steps to ensure that its published Engineering specifications and manuals are correct; however, errors do occur. Zebra Technologies reserves the right to correct any such errors and disclaims liability resulting therefrom.

Limitation of Liability

In no event shall Zebra Technologies or anyone else involved in the creation, production, or delivery of the accompanying product (including hardware and software) be liable for any damages whatsoever (including, without limitation, consequential damages including loss of business profits, business interruption, or loss of business information) arising out of the use of, the results of use of, or inability to use such product, even if Zebra Technologies has been advised of the possibility of such damages. Some jurisdictions do not allow the exclusion or limitation of incidental or consequential damages, so the above limitation or exclusion may not apply to you.

P1099957-002

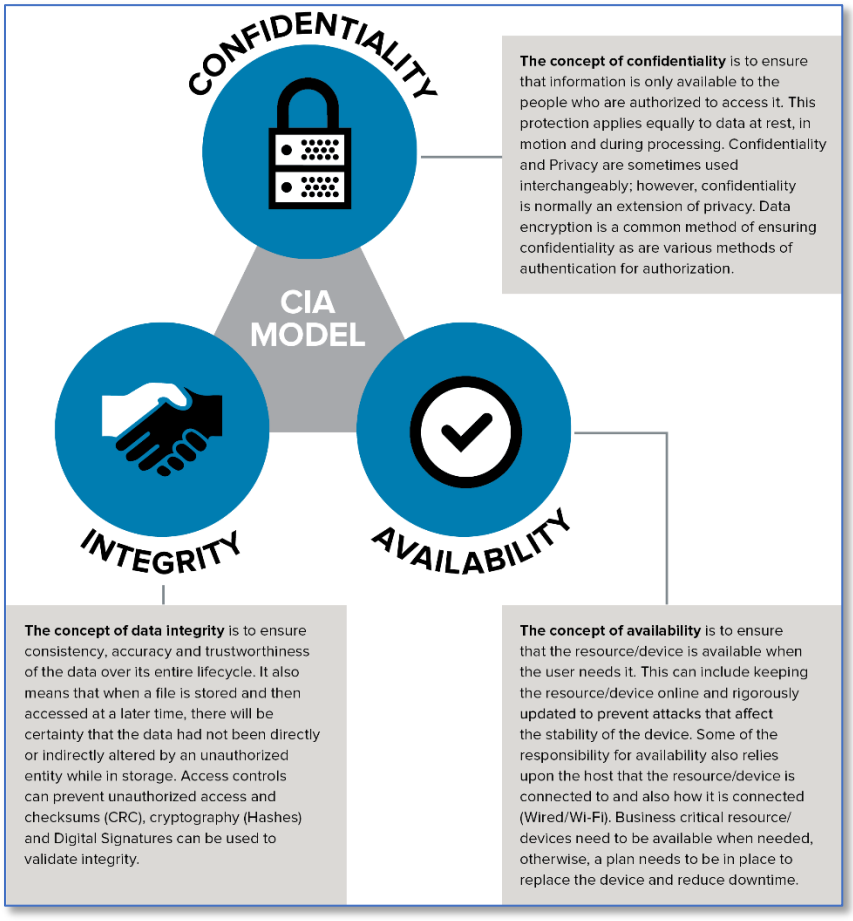
Introduction

This document details how to Administer a Zebra Label or Receipt printer. The content in this document covers both Link-OS® and ZebraLink™ printers, though the degree to which the two types of printers can be Administered is different. To make it easy to see where a given Administrative feature is available, the document will display the Link-OS or ZebraLink icon to indicate if the feature is available on the printer being configured.

Overview

Administering Thermal label and receipt printers can, at first, appear to be a very different task than managing other devices, such as computers or smartphones. Fortunately, there is a well-established, reliable model and a set of best practices that can be easily applied to minimize risks and make the task straightforward.

The “CIA Model” provides a guiding framework when considering how to reasonably and effectively raise the bar on risk mitigation. The model can be applied to all devices that utilize the data protected by enterprise information systems, from the more traditional connected solutions to the new players in the connected environment, such as intelligent thermal barcode printers. It includes three components:



Common Sense Best Practices

There are a set of Best Practices you can put in place to align your printer Administration with the CIA concepts. By applying these common sense Best Practices, you can reduce risk, while still optimizing your use of thermal barcode printers.

1	•Start early. Plan for incoming devices, and how you'll protect them.
2	•Use encrypted and authenticated connections where possible.
3	•Plan to rotate access passwords, access keys and authentication credentials.
4	•Defaults typically represent documented methods to access a device. Activate User Interface Passwords and consider turning off the device services that you don't plan to use.
5	•Leverage a remote management system to allow you to quickly update settings and standards. The longer devices are using out of date settings, the longer they represent the "easier target."
6	•Keep update schedules and plans only in the hands of those who need to have them. Knowing when updates are planned can inadvertently encourage inappropriate actions.
7	•Plan for a method to continuously monitor your system for "out of touch" devices. Where you suspect a device has been taken out of your environment, withdraw its credentials until the device status is determined.
8	•Choose devices that can be updated across their long service lives so they keep current with new standards. Verify that the update system uses a method to ensure the update file hasn't been tampered with.
9	•Plan for device retirement by removing enterprise system settings, deleting device user Accounts/Credentials and checking to make sure the existing system isn't hardcoded to look for retired devices.
10	•Consider "Confidentiality", "Integrity" and "Availability" during all stages of the devices lifecycle.

Steps To Take

Applying these Best Practices is straightforward. The process involves four steps:

1. Census – which devices do you have?
2. Consider – which Admin capabilities do your printers have?
3. Configure – send commands to alter Admin settings
4. Confirm – validate the new settings

Census: Which Devices Do You Have?

Zebra printers have been manufactured for over 30 years. Through that time, the scope of Administrative settings has grown. It's important to know which printer models you are working with to know which Admin controls are available. The chart below will help you "place" your printer model into one of three categories.

Legacy Models (no admin features)	Zebra Link™ (limited admin features)	**Link-OS®** (most admin features)
Desktop Printers A100 series A300 series Bravo series Companion Encore series LP/TLP series Tiger Writer 2746 series HT146 DA402 R402 T300/T402	**Desktop Printers** LP/TLP-Z series LP/TLP Plus series S300 S400 S500 S600 G series HC100	**Desktop Printers** ZD400 series ZD500 series ZD600 series
Mobile Printers Cameo series MP series QL series PA400 series PT400 series PS2000-PS400 series TR220 ZQ110	**Mobile Printers** QLPlus series P4T series RW Series	**Mobile Printers** iMZ series QLn series ZQ300 series ZQ500 series ZQ600 series ZR300 series ZR600 series
Industrial Printers Z60 series Z90 series Z100 series Z140 series Z200 series 105Se	**Industrial Printers** Z4000/Z6000 Z4M/Z6M ZM400/600 series 105SL series 105SL Plus series XiII through Xi4 series	**Industrial Printers** ZT200 series ZT400 series ZT500 series ZT600 series
Others TTP Kiosk printer series	**Others** PAX 2 through PAX5 series ZE500 series KR403	**Others** N/A

Consider: Which Admin Capabilities Does Your Printer Have?

Link-OS printers support a wide range of administrative commands and features, ZebraLink printers support a more limited set. Before using these capabilities please review the following pages to carefully consider how changing these features settings could impact your application.

	Supported Printers	
	Zebra Link™	
Services		
HTTP	☑	☑
HTTPS		☑
FTP	☑	☑
LPD	☑	☑
UDP		☑
SMTP	☑	☑
SNMP	☑	☑
Raw Telnet	☑	☑
POP3	☑	☑
Network Time Protocol		☑
Communications		
Bluetooth	☑	☑
BTLE		☑
USB Host		☑
Ethernet		☑
WLAN		☑
802.11x		☑
RTS/CTS protection		☑
IP Address Whitelist		☑
IP Port		☑
IP Alternate port		☑
JSON port		☑
Single connection port		☑
TLS IP Port		☑
TLS JSON Port		☑
TLS Enable		☑
Web sockets port		☑
Asset Visibility Agent		☑
Applications		
Data Capture		☑
XML Printing	☑	☑
USB Mirror		☑
FTP Mirror	☑	☑
SFTP Mirror		☑
Zebra Basic Interpreter		☑
User Interface		
Password	☑	☑

Premade Administration Files

Zebra has created four pre-made files that you can send to your printer to quickly enable some of the most common security settings. These Premade Admin Files were designed and built using the commands documented in this guide. However, because different user's networks operate in different ways, there is no one configuration file that could address every user's needs.

You should edit the files to adapt to your unique needs. As you work with the Printer Administration Guide, you'll quickly discover which commands and settings that are appropriate for your use case. For example, if your application uses Mirror, then turning off FTP wouldn't make sense, since Mirror uses FTP to communicate to the printer. This example demonstrates why it is important to consider the following pages below before sending the files.

Sending the Administration files is simple. You can send the files to any port on the printer using our Z-Downloader or Printer Setup Utility for Windows. The Z-Downloader app can be downloaded from the zebra web site. The Printer Setup Utility for Windows can be downloaded here.

The Premade Administration files come in four groups:

1. **applications** – Three files, which can be used to set, check settings, or default the application settings on the printer.

2. **communications.** – Three files, which can be used to set, check settings, or default the communication settings on the printer.

3. **services**– Three files, which can be used to set, check settings, or default the services settings on the printer.

4. **userinterface** – Two files, which can be used to set or default the user interface settings on the printer. (Important note: Do not use the sample password shown in this file, please change it.)

Configure – Confirm

- Send Commands to Alter Admin Settings
- Validate the New Settings

This can be the most time-consuming portion of the process. Each Administrative capability used will have consequences for how the printer works, what it can do, and how it will work with other devices. Time should be taken to carefully consider which Administrative features are used, and how they may impact the use of the printer.

In this section, each Admin capability will be detailed, along with its defaults, its range of settings, how to activate/deactivate it, along with some notes to help you carefully consider the use of the capability.

NOTE: Many of the Administrative capabilities are controlled using the Set-Get-Do command language. If you are not familiar with this language, please consult the Zebra Programming Guide, SGD Chapter for help with syntax and how to use this printer feature.

Services, Networking, Commands

HTTP SERVICE	**Supported Printers**	
Description: This port is used to provide HTTP access to the printer	Zebra Link™	
Considerations: The HTTP service runs on port 80 and provides support for the printer's internal web pages. It is also important to note that any POST to URL capability is disabled when this service is not enabled. The printer can still be managed by the Printer Profile Manager Enterprise app or via direct commands when this is disabled.		
Control Commands: The HTTP capability is controlled by the ip.http.enable command To set the command: ! U1 setvar "ip.http.enable" "on" ! U1 setvar "ip.http.enable" "off" To confirm the command is set: ! U1 getvar "ip.http.enable" The printer should respond with the current setting value, or "?" if not supported To Default the command: ! U1 setvar "ip.http.enable" "on"		

HTTPS SERVICE	Supported Printers	
Description: This port is used to provide HTTPS access to the printer		
Considerations: The HTTPS service runs on port 443 and provides support for the printer's internal web pages.		
Control Commands: The HTTPS capability is controlled by the ip.https.enable command To set the command: ! U1 setvar "ip.https.enable" "on" ! U1 setvar "ip.https.enable" "off" To confirm the command is set: ! U1 getvar "ip.https.enable" The printer should respond with the current setting value, or "?" if not supported To Default the command: ! U1 setvar "ip.https.enable" "on"		

Note:

This command requires that a valid certificate is present on the printer.

The certificate and private key can be deployed to the device as a single file, or separate files. If using a single file, the name of the file must be:

HTTPS_CERT.NRD

If using multiple files:

HTTPS_CERT.NRD – certificate file

HTTPS_KEY.NRD – private key file

Once TLS communication is verified and operational, it is a security best practice to disable unencrypted forms of communicating with the printer over a network.

Certificate Size Requirements

In keeping with latest industry wide recommendations (NIST, 2016), the printer will only accept certificates with a digest of SHA-224 or higher. For keys based on RSA or DSA the size must be 2048 bits or higher. For keys based on ECDSA the size must be 224 bits or higher. Any certificates with digest or key sizes smaller than this will be rejected.

FTP SERVICE	Supported Printers	
Description: This port is used to send commands or files that the printer will act upon (this can include, CPCL, EPL, ZPL and Set-Get-Do commands).	Zebra Link™	
Considerations: FTP (port 21) can be used to place files on the printers file system, or for printing. It is also the protocol used by the Mirror device management features. It is not a port that is typically used for printing. As such, it's a good candidate to be disabled, however, it's important to first check if your organization plans to use it for file transfer, printing or device management.		
Control Commands: The FTP capability is controlled by the "ip.ftp.enable" command To set the command: ! U1 setvar "ip.ftp.enable" "on" ! U1 setvar "ip.ftp.enable" "off" To confirm the command is set: ! U1 getvar "ip.ftp.enable" The printer should respond with the current setting value, or "?" if not supported To Default the command: ! U1 setvar "ip.ftp.enable" "on"		

Note:

Only Link-OS printer can use SFTP.

For further information on FTP and SFTP Mirror refer to the Programming Guide.

<table>
<tr><td><u>LPD SERVICE</u></td><td colspan="2"><u>Supported Printers</u></td></tr>
<tr><td>Description: This port is used to send print jobs to the printer that it will act upon (this can include, CPCL, EPL, ZPL).</td><td>Zebra Link™</td><td>  </td></tr>
<tr><td colspan="3">Considerations: The LPD (Port 515) or Line Printer Daemon is a printing protocol typically used in Unix/Linux systems and the Mac OS environment. This can be supported on a Windows network with the addition of software features. Check which printing technology you are using and disable the appropriate port(s).</td></tr>
<tr><td colspan="3">Control Commands: The LPD capability is controlled by the ip.lpd.enable command

To set the command:

! U1 setvar "ip.lpd.enable" "on"
! U1 setvar "ip.lpd.enable" "off"

To confirm the command is set:

! U1 getvar "ip.lpd.enable"

The printer should respond with the current setting value, or “?” if not supported

To Default the command:

! U1 setvar "ip.lpd.enable" "on"</td></tr>
</table>

UDP SERVICE	**Supported Printers**	
Description: The UDP socket is only used for port defined by ip.port.		
Considerations: The User Datagram Protocol (UPD) is a connectionless protocol in contrast to Transmission Control Protocol (TCP) which requires a validated connection and an IP address.		
Control Commands: The UPD capability is controlled by the ip.upd.enable command To set the command: ! U1 setvar "ip.upd.enable" "on" ! U1 setvar "ip.upd.enable" "off" To confirm the command is set: ! U1 getvar "ip.upd.enable" The printer should respond with the current setting value, or “?” if not supported To Default the command: ! U1 setvar "ip.upd.enable" "on"		

SMTP SERVICE	Supported Printers	
Description: This Simple Mail Transfer Protocol (SMTP) service (port 25) is used.	Zebra Link™	
Considerations: This SMTP service is used to receive printer jobs using the Simple Mail Transfer Protocol (this can include, CPCL, EPL, ZPL).		
Control Commands: The SMTP capability is controlled by the ip.smtp.enable command To set the command: ! U1 setvar "ip.smtp.enable" "on" ! U1 setvar "ip.smtp.enable" "off" To confirm the command is set: ! U1 getvar "ip.smtp.enable" The printer should respond with the current setting value, or “?” if not supported To Default the command: ! U1 setvar "ip.smtp.enable" "on"		

Note:

Ensure that the other dependent settings are configured correctly when using this capability

For further information on SMTP refer to the Programming Guide.

For example:

ip.smtp.server_addr

ip.smtp.domain

SNMP SERVICE	Supported Printers	
Description: The SNMPv1 service on UDP port 161 enables the manageability of the printer using SNMP.		
Considerations: The SNMP (UDP port 161) allows the configuration of the printer and supports the issuance of SNMP trap messages. Some of the basic printer MIB is supported as well as a private MIB that contains Zebra specific settings and configuration. By default, this uses the public community name, if you intend to use this consider changing the community name from the default.		
Control Commands: The SNMP capability is controlled by the ip.snmp.enable command To set the command: ! U1 setvar "ip.snmp.enable" "on" ! U1 setvar "ip.snmp.enable" "off" To confirm the command is set: ! U1 getvar "ip.snmp.enable" The printer should respond with the current setting value, or “?” if not supported To Default the command: ! U1 setvar "ip.snmp.enable" "on"		

TELNET SERVICE	Supported Printers	
Description: The printer telnet service is used to access the printer configuration utility.	Zebra Link™	
Considerations: The Telnet service (port 23) is mainly used to setup and configure print server settings and enable/disable printer daemons. Settings changed here will be reflected by the values in the relevant SGD's. It is important to note that a limited subset of capabilities is available using the telnet capability. This is primarily retained for backwards compatibility.		
Control Commands: The Telnet capability is controlled by the ip.telnet.enable command To set the command: ! U1 setvar "ip.telnet.enable" "on" ! U1 setvar "ip.telnet.enable" "off" To confirm the command is set: ! U1 getvar "ip.telnet.enable" The printer should respond with the current setting value, or "?" if not supported To Default the command: ! U1 setvar "ip.telnet.enable" "on"		

Note:

It is not possible to disable the telnet service over a telnet session.

POP3 MAIL SERVICE	Supported Printers	
Description: The printer has a pop3 mail service and can poll a mailbox for incoming emails.		
Considerations: The POP3 service can query a mailbox for incoming emails, which can contain ZPL/CPL/EPL in the body of the email. The printer will execute the command language.		
Control Commands: The POP3 capability is controlled by the ip.pop3.enable command To set the command: ! U1 setvar "ip.pop3.enable" "on" ! U1 setvar "ip.pop3.enable" "off" To confirm the command is set: ! U1 getvar "ip.pop3.enable" The printer should respond with the current setting value, or "?" if not supported To Default the command: ! U1 setvar "ip.pop3.enable" "on"		

Note:

Ensure that the other dependent settings are configured correctly when using this capability

For further information on POP3 refer to the Programming Guide.

For example:

ip.pop3.server_addr

ip.pop3.poll

ip.pop3.username

ip.pop3.password

NETWORK TIME PROTOCOL SERVICE	Supported Printers	
Description: This command enables or disables the Network Time Protocol (NTP) feature.		
Considerations: The NTP command will enable or disable the Network Time Protocol capability which allows the printer to synchronize with time servers. This may be important if there are date or time fields printed on the label. Time and data can also be provided by the host system.		
Control Commands: The NTP capability is controlled by the ip.ntp.enable command To set the command: ! U1 setvar "ip.ntp.enable" "on" ! U1 setvar "ip.ntp.enable" "off" To confirm the command is set: ! U1 getvar "ip.ntp.enable" The printer should respond with the current setting value, or “?” if not supported To Default the command: ! U1 setvar "ip.ntp.enable" "off"		

Note:

Ensure that the other dependent settings are configured correctly when using this capability

For further information on NTP refer to the Programming Guide.

For example:

ip.ntp.servers

ip.ntp.log

BLUETOOTH	**Supported Printers**	
Description: This command enables or disables the Bluetooth radio in a printer that has that option installed.	Zebra Link™	
Considerations: The Bluetooth enable command will disable all Bluetooth connectivity on the printer. If you utilize Bluetooth for connection to a mobile computer for printing this will need to be configured correctly.		
Control Commands: The Bluetooth enable capability is controlled by the bluetooth.enable command To set the command: ! U1 setvar "bluetooth.enable" "on" ! U1 setvar "bluetooth.enable" "off" To confirm the command is set: ! U1 getvar "bluetooth.enable" The printer should respond with the current setting value, or “?” if not supported To Default the command: ! U1 setvar "bluetooth.enable" "on"		

BLUETOOTH LE	**Supported Printers**	
Description: For printer that support both Bluetooth classic and BTLE, this command controls the mode of operation.		
Considerations: The printer Bluetooth radio can be configured to work in the following mode; BTLE, Classic or Both.		
Control Commands: The Bluetooth controller mode is controlled by the bluetooth.le.contoller_mode command To set the command: ! U1 setvar "bluetooth.le.contoller_mode" "both" ! U1 setvar "bluetooth.le.contoller_mode" "le" ! U1 setvar "bluetooth.le.contoller_mode" "classic" To confirm the command is set: ! U1 getvar "bluetooth.le.contoller_mode" The printer should respond with the current setting value, or “?” if not supported To Default the command: ! U1 setvar "bluetooth.le.contoller_mode" "both"		

Note:

There are many other settings related to BT communication and these need to be reviewed and configured accordingly.

For further information on Bluetooth refer to the Programming Guide.

For example:

bluetooth.discoverable

bluetooth.minimum_security_mode

bluetooth.allow_non_display_numeric_comparison

bluetooth.bonding

bluetooth.pin

Commands no longer supported in Link-OS v5

bluetooth.le.minimum_security

bluetooth.le.print_passkey

USB HOST	**Supported Printers**	
Description: This command is used to enable or disable USB host capabilities in a printer that supports USB Host		
Considerations: The USB host lockout command disables the USB host capability in a printer that has support for it. USB devices connected to the printer will stop functioning when this is disabled. This will include USB mirror if that is being used.		
Control Commands: The USB host lock out capability is controlled by the usb.host.lock_out command To set the command: ! U1 setvar "usb.host.lock_out" "on" ! U1 setvar "usb.host.lock_out" "off" To confirm the command is set: ! U1 getvar "usb.host.lock_out" The printer should respond with the current setting value, or “?” if not supported To Default the command: ! U1 setvar "usb.host.lock_out" "off"		

WIRED ETHERNET	**Supported Printers**	
Description: Enable or disable the internal wired ethernet port on printers equipped with this option.		
Considerations: The wired LAN enable command will disable or enable the internal wired Ethernet connection. The primary use for this command is to disable a port that is unused, where a different port is being used as the primary connection.		
Control Commands: The wired LAN capability is controlled by the internal_wired.enable command To set the command: ! U1 setvar "internal_wired.enable" "on" ! U1 setvar “internal_wired.enable" "off" To confirm the command is set: ! U1 getvar "internal_wired.enable" The printer should respond with the current setting value, or “?” if not supported To Default the command: ! U1 setvar "internal_wired.enable" "on"		

Note:

NEW with Link-OS v5

WLAN	**Supported Printers**	
Description: This command can be used to enable or disable the WLAN functionality in a printer fitted with a wireless option.		
Considerations: The WLAN command will fully disable all 802.11 wireless functionality. This should only be disabled if the wireless option is present but is not being used for any reason.		
Control Commands: The WLAN capability is controlled by the wlan.enable command To set the command: ! U1 setvar "wlan.enable" "on" ! U1 setvar "wlan.enable" "off" To confirm the command is set: ! U1 getvar "wlan.enable" The printer should respond with the current setting value, or “?” if not supported To Default the command: ! U1 setvar "wlan.enable" "on"		

WIRELESS OPTION	**Supported Printers**	
Description: This option provides a mechanism to authenticate devices on a LAN		
Considerations: When using the 802.1x authentication user must be aware of the movement of data to the printer during setup. Best practices should be employed to ensure that certificates and passphrases are protected at all time. Configuration should be done over a local connection to prevent eavesdropping.		
Control Commands: To set the command: ! U1 setvar "wlan.8021x.enable" "on" ! U1 setvar "wlan.8021x.enable" "off" ! U1 setvar "wlan.8021x.enable" "wpa" To confirm the command is set: ! U1 getvar "wlan.8021x.enable" The printer should respond with the current setting value, or “?” if not supported To Default the command: ! U1 setvar "wlan.8021x.enable" "off"		

Note:

There are many other settings related to 802.1x Authentication and these need to be reviewed and configured accordingly.

For further information on 802.1x refer to the Programming Guide.

For example:

wlan.8021x.authentication

wlan.8021x.ttls_tunnel

wlan.8021x.peap.peap_username

wlan.8021x.peap.peap_password wlan.8021x.peap.privkey_password

wlan.8021x.peap.validate_server_certificate

wlan.8021x.peap.anonymous_identity

wlan.8021x.eap.username

wlan.8021x.eap.password

wlan.8021x.eap.privkey_password

WIRELESS OPTION	**Supported Printers**	
Description: This mode is to protect the transmissions from interference from nearby 802.11 signals	Zebra Link™	
Considerations: The WLAN RTS_CTS feature when enabled will put the WLAN radio in RTS/CTS protection mode. If this is not enabled the radio will default to CTS-to-Self mode. The mode that you run in will be dependent on your specific wireless LAN configuration and the devices that connect to it.		
Control Commands: The WLAN RTS_CTS capability is controlled by the wlan.rts_cts_enable command To set the command: ! U1 setvar "wlan.rts_cts_enabled" "on" ! U1 setvar "wlan.rts_cts_enabled" "off" To confirm the command is set: ! U1 getvar "wlan.rts_cts_enabled" The printer should respond with the current setting value, or “?” if not supported To Default the command: ! U1 setvar "wlan.rts_cts_enabled" "off"		

Note:

This command functions on the QLn and ZQ500 series printers.

WHITELISTING	**Supported Printers**	
Description: The whitelisting capability allows only authorized IP addresses to connect to the printer.		
Considerations: The whitelisting capability is to ensure that only authorized hosts can connect to the printer. The parameters that you set are the IP addresses that are permitted to connect and can be single IP address or ranges. The maximum string length allowed is 256 bytes.		
Control Commands: The whitelist capability is controlled by the ip.firewall.whitelist_in command To set the command: ! U1 setvar "ip.firewall.whitelist_in" "192.168.1.20" ! U1 setvar "ip.firewall.whitelist_in" "192.168.1.20, 192.168.100.21" ! U1 setvar "ip.firewall.whitelist_in" "192.168.1.20-192.168.1.100" To confirm the command is set: ! U1 getvar "ip.firewall.whitelist_in" The printer should respond with the current setting value, or “?” if not supported To Default the command: ! U1 setvar "ip.firewall.whitelist_in" ""		

Note:

This command allows up to 256 characters that define what IP’s or ranges of IP’s can connect to the printer. If the IP address is not listed the connection will be refused. To reset this list, you will need to connect to a local port and send this command if the IP you are trying to connect with is not in the allowed range.

Examples:

Single IP address

! U1 setvar "ip.firewall.whitelist_in" "192.168.1.20"

Multiple IP addresses

! U1 setvar "ip.firewall.whitelist_in" "192.168.1.20, 192.168.1.21"

IP address ranges

! U1 setvar "ip.firewall.whitelist_in" "192.168.1.20-192.168.1.40"

IP ranges and Single/Multiple IPs

! U1 setvar "ip.firewall.whitelist_in" "192.168.1.20-192.168.1.40, 192.168.1.50, 192.168.1.75"

TCP RAW PORT	Supported Printers	
Description: This port is used to send commands or files that the printer will act upon (this can include, CPCL, EPL, ZPL and Set-Get-Do commands).		
Considerations: Since this is frequently the primary port used for network based printing, disabling it could disable printer. Of course, printing could be happening over another port, via FTP or web sockets. Additionally, changing the port number used could help obscure the printing port, but note that the most port scanning tools can easily discover which ports are open on a networked device.		
Control Commands: The TCP Raw Port setting is controlled by the "ip.port" command To set the command: ! U1 setvar "ip.port" "9100" ! U1 setvar "ip.port" "0" (Disables port) To confirm the command is set: ! U1 getvar "ip.port" The printer should respond with the current setting value, or “?” if not supported To Default the command: ! U1 setvar "ip.port" "9100" (All printers except mobile) ! U1 setvar "ip.port" "6101" (Mobile printers)		

Note:

Port numbers cannot be the same as any other SGD’s in the group below. If you try to set the value to something that is in use it will be ignored. Setting the value to “0” disables the port and can be used to clear the current value, before it is set to a new value. However, remember setting the port to “0” will disable the port.

For further information on ports, refer to the Programming Guide.

For example:

ip.port

ip.port_alternate

ip.port_json_config

ip.port_single_conn

Mobile printers ip.port is 6101 and ip.port_alternate is 9100.

Everything else is ip.port 9100 and ip.port_alternate 6101.

TCP RAW PORT	Supported Printers	
Description: This is a secondary raw port that can be used to communicate with the printer.		
Considerations: Secondary raw printing port that allows multiple connections to the printer. These are served on and first come first served basis and allow up to x connection before additional connections are refused. This is primarily used for CPCL based printers and there to support legacy application. If ZPL is being used this port could be disabled without any impact. If this port is not being used setting the value to 0 will disable the port		
Control Commands: The IP Port alternative capability is controlled by the ip.port_alternate command To set the command: ! U1 setvar "ip.port_alternate" "6101" ! U1 setvar "ip.port_alternate" "0" (Disables port) To confirm the command is set: ! U1 getvar "ip.port_alternate" The printer should respond with the current setting value, or "?" if not supported. To Default the command: ! U1 setvar "ip.port_alternate" "6101" (All printers except QLn) ! U1 setvar "ip.port_alternate" "9100" (QLn)		

Note:

Port numbers cannot be the same as any other SGD's in the group below. If you try to set the value to something that is in use it will be ignored. Setting the value to "0" disables the port and can be used to clear the current value, before it is set to a new value. However, remember setting the port to "0" will disable the port.

For further information on ports refer to the Programming Guide.

For example:

ip.port

ip.port_alternate

ip.port_json_config

ip.port_single_conn

Mobile printers ip.port is 6101 and ip.port_alternate is 9100.

Everything else is ip.port 9100 and ip.port_alternate 6101

JSON RAW PORT	Supported Printers	
Description: This is a JSON port that can be used to send configuration commands to the printer.		
Considerations: This port is used to carry out printer configuration utilizing the JSON format and generally used by Zebra Applications and Utilities (PPME included), which would include 3rd party applications built using our SDKs. If this port is disabled, printers can still be recognized by PPME but communication will be slower.		
Control Commands: The JSON port capability is controlled by the ip.port_json_config command To set the command: ! U1 setvar "ip.port_json_config" "9200" ! U1 setvar "ip.port_json_config" "0" (Disables port) To confirm the command is set: ! U1 getvar "ip.port_json_config" The printer should respond with the current setting value, or "?" if not supported To Default the command: ! U1 setvar "ip.port_json_config" "9200"		

Note:

Port numbers cannot be the same as any other SGD's in the group below. If you try to set the value to something that is in use it will be ignored. Setting the value to "0" disables the port and can be used to clear the current value, before it is set to a new value. However, remember setting the port to "0" will disable the port.

For further information on ports refer to the Programming Guide.

For example:

ip.port

ip.port_alternate

ip.port_json_config

ip.port_single_conn

Mobile printers ip.port is 6101 and ip.port_alternate is 9100.

Everything else is ip.port 9100 and ip.port_alternate 6101.

TCP RAW PORT	Supported Printers	
Description: This is a port that can be used to send commands to the printer but only allows a single connection.		
Considerations: This port is designed to work in the same way as ip.port but it will only allow a single connection to the printer at a time. Any other connection attempts while this port is in use will be rejected.		
Control Commands: The IP port single connection capability is controlled by the ip.port_single_conn command To set the command: ! U1 setvar "ip.port_single_conn" "9300" ! U1 setvar "ip.port_single_conn" "0" (Disables port) To confirm the command is set: ! U1 getvar "ip.port_single_conn" The printer should respond with the current setting value, or "?" if not supported To Default the command: ! U1 setvar "ip.port_single_conn" "9300"		

Note:

Port numbers cannot be the same as any other SGD's in the group below. If you try to set the value to something that is in use it will be ignored. Setting the value to "0" disables the port and can be used to clear the current value, before it is set to a new value. However, remember setting the port to "0" will disable the port.

For further information on ports refer to the Programming Guide.

For example:

ip.port

ip.port_alternate

ip.port_json_config

ip.port_single_conn

ip.port_single_conn_idle_timeout

Mobile printers ip.port is 6101 and ip.port_alternate is 9100.

Everything else is ip.port 9100 and ip.port_alternate 6101

TLS RAW PORT	Supported Printers	
Description: This port is used to send commands or files that the printer will act upon over a secure TLS channel (this can include, CPCL, EPL, ZPL and Set-Get-Do commands).		
Considerations: This port is designed to work in the same way as ip.port but it requires a valid certificate loaded on the printer to enable TLS encryption. If you are using the TLS channel it is recommended that you disable the non-encrypted ports		
Control Commands: The TLS Parser Port connection capability is controlled by the ip.tls.port command To set the command: ! U1 setvar "ip.tls.port" "9143" ! U1 setvar "ip.tls.port" "0" (Disables port) To confirm the command is set: ! U1 getvar "ip.tls.port" The printer should respond with the current setting value, or "?" if not supported To Default the command: ! U1 setvar "ip.tls.port" "9143"		

Note:

This command requires that ip.tls.enable is on and that a valid certificate is present on the printer.
The certificate and private key can be deployed to the device as a single file, or separate files. If using a single file, the name of the file must be:

TLSRAW_CERT.NRD

If using multiple files:

TLSRAW_CERT.NRD – certificate file

TLSRAW_KEY.NRD – private key file

Once TLS communication is verified and operational, it is a security best practice to disable unencrypted forms of communicating with the printer over a network.

Certificate Size Requirements

In keeping with latest industry wide recommendations (NIST, 2016), the printer will only accept certificates with a digest of SHA-224 or higher. For keys based on RSA or DSA the size must be 2048 bits or higher. For keys based on ECDSA the size must be 224 bits or higher. Any certificates with digest or key sizes smaller than this will be rejected.

TLS JSON PORT	**Supported Printers**	
Description: This is a TLS JSON port that can be used to send configuration commands to the printer over a secure connection.		
Considerations: This port is used to carry out printer configuration utilizing the JSON format and when utilizing the TLS connection.		
Control Commands: The TLS connection JSON config port capability is controlled by the ip.tls.port_json_config command To set the command: ! U1 setvar "ip.tls.port_json_config" "9243" ! U1 setvar "ip.tls.port_json_config" "0" (Disables port) To confirm the command is set: ! U1 getvar "ip.tls.port_json_config" The printer should respond with the current setting value, or “?” if not supported To Default the command: ! U1 setvar "ip.tls.port_json_config" "9243"		

Note:

Port numbers cannot be the same as any other SGD’s in the group below. If you try to set the value to something that is in use it will be ignored. Setting the value to “0” disables the port and can be used to clear the current value but remember it will disable the port.

For further information on ports, refer to the Programming Guide.

For example:

ip.tls.port

ip.tls.port_json_config

TLS ENABLE	**Supported Printers**	
Description: This is a command that enables or disables the TLS capability.		
Considerations: This is for securing communications to the printer over wired and wireless Ethernet and depends on preloaded certificates on the printer. Ensure that this capability is working before disabling any non-TLS connections.		
Control Commands: The TLS Enable command is controlled by the ip.tls.enable command To set the command: ! U1 setvar "ip.tls.enable" "on" To confirm the command is set: ! U1 getvar "ip.tls.enable" The printer should respond with the current setting value, or “?” if not supported To Default the command: ! U1 setvar "ip.tls.enable" "on"		

Note:

This command enables TLS communication with the printer and requires a valid certificate is present on the printer.

Once TLS communication is verified and operational, it is a security best practice to disable unencrypted forms of communicating with the printer over a network.

WEBLINK CONNECT	**Supported Printers**	
Description: This command is a global switch that either enables or disables the Weblink capabilities.		
Considerations: The Weblink Cloud Connect capability is utilized to make secure connections to a cloud-based service.		
Control Commands: The cloud connect capability is controlled by the weblink.cloud_connect.enable command To set the command: ! U1 setvar "weblink.cloud_connect.enable" "on" ! U1 setvar "weblink.cloud_connect.enable" "off" To confirm the command is set: ! U1 getvar "weblink.cloud_connect.enable" The printer should respond with the current setting value, or "?" if not supported To Default the command: ! U1 setvar "weblink.cloud_connect.enable" "off"		

Note:

Many apps use the weblink connection to connect the printer to a server-based app. These include Printer Profile Manager Enterprise, AirWatch Connector, Soti Connector. Take care when turning this feature off if you are using one of those programs.

ASSET VISIBILITY AGENT	**Supported Printers**	
Description: This command turns the Asset Visibility agent off or on.		
Considerations: This feature can connect a networked Link-OS printer to Zebra's Asset Visibility Service (AVS). The Asset Visibility Service is a Zebra-managed service offering that provides Zebra partners and customers 'at-a-glance' visibility to analytical insights about their device health, utilization, and performance.		
Control Commands: The Asset Visibility capability is controlled by the weblink.zebra_connector.enable command To set the command: ! U1 setvar "weblink.zebra_connector.enable" "on" ! U1 setvar "weblink.zebra_connector.enable" "off" To confirm the command is set: ! U1 getvar "weblink.zebra_connector.enable" The printer should respond with the current setting value, or "?" if not supported To Default the command: ! U1 setvar "weblink.zebra_connector.enable" "on"		

CAPTURE PORT	Supported Printers	
Description: This command specifies the port that should be monitored for user data.		
Considerations: The capture channel command will collect user data from the specified port and store it in the capture.channel1.data.raw. To disable the capture channel the port should be set to “off”		
Control Commands: The capture channel capability is controlled by the capture.channel1.port command To set the command: ! U1 setvar "capture.channel1.port" "serial" ! U1 setvar "capture.channel1.port" "usb" ! U1 setvar "capture.channel1.port" "bt" ! U1 setvar "capture.channel1.port" "parallel" ! U1 setvar "capture.channel1.port" "off" To confirm the command is set: ! U1 getvar "capture.channel1.port" The printer should respond with the current setting value, or “?” if not supported To Default the command: ! U1 setvar "capture.channel1.port" "off"		

<table>
<tr><td><u>XML PRINTING</u></td><td colspan="2"><u>Supported Printers</u></td></tr>
<tr><td>Description: This command enables or disables the XML parsing capability in the printer</td><td>Zebra Link™</td><td>  </td></tr>
<tr><td colspan="3">Considerations: The XML enable command is primarily used to allow the variable data for a stored format to be passed to the printer in an XML format. This is often used in the Oracle environment and if disabled will stop the printer from printing. The XML Data can be in two distinct formats, one for Oracle and one for SAP.</td></tr>
<tr><td colspan="3">Control Commands: The XML capability is controlled by the device.xml.enable command

To set the command:

! U1 setvar "device.xml.enable" "on"
! U1 setvar "device.xml.enable" "off"

To confirm the command is set:

! U1 getvar "device.xml.enable"

The printer should respond with the current setting value, or “?” if not supported

To Default the command:

! U1 setvar "device.xml.enable" "on"</td></tr>
</table>

USB MIRROR	**Supported Printers**	
Description: This command enables or disables the ability to perform mirroring using a USB device memory stick.		
Considerations: The USB mirror capability is only supported by printers that have USB host capability.		
Control Commands: The USB mirror enabled capability is controlled by the usb.mirror.enable command To set the command: ! U1 setvar "usb.mirror.enable" "on" ! U1 setvar "usb.mirror.enable" "off" To confirm the command is set: ! U1 getvar "usb.mirror.enable" The printer should respond with the current setting value, or “?” if not supported To Default the command: ! U1 setvar "usb.mirror.enable" "on"		

Note:

This command only works on printers with USB Host capabilities.

SYSLOG	Supported Printers	
Description: The printer can collect logging events and store them in non-volatile memory for analysis and debugging.		
Considerations: The syslog enable command turns on the logging capability which is turned off by default. There are other commands that configure the content of the file and max file size etc.		
Control Commands: The syslog capability is controlled by the device.syslog.enable command To set the command: ! U1 setvar "device.syslog.enable" "on" ! U1 setvar "device.syslog.enable" "off" To confirm the command is set: ! U1 getvar "device.syslog.enable" The printer should respond with the current setting value, or “?” if not supported To Default the command: ! U1 setvar "device.syslog.enable" "off"		

Note:

For further information on the syslog command refer to the Programming Guide.

For example:

device.syslog.clear_log

device.syslog.configuration

device.syslog.entries

device.syslog.log_max_file_size

device.syslog.save_local_file

ZEBRA BASIC INTERPRETER	Supported Printers	
Description: This is to disable the Zebra Basic Interpreter (ZBI) capability in the printer.		
Considerations: The ZBI enable command allows an administrator to disable the ZBI Interpreter in the printer. A license is still required to be able to run ZBI scripts on a printer, however this is a global command to turn off the ZBI capability whether a license is installed or not. If you are not utilizing a ZBI script it is recommended that this is disabled.		
Control Commands: The ZBI enable capability is controlled by the zbi.enable command To set the command: ! U1 setvar "zbi.enable" "on" ! U1 setvar "zbi.enable" "off" To confirm the command is set: ! U1 getvar "zbi.enable" The printer should respond with the current setting value, or “?” if not supported To Default the command: ! U1 setvar "zbi.enable" "on"		

Note:

New to Link-OS v5.

PASSWORD	**Supported Printers**	
Description: This is the define password command and allows an admin to change the password for the web page	Zebra Link™	
Considerations: The command allows the changing of the default password for control panel switches and web page access. The default password is well known and should be changed. It should also be noted that defaulting the password is trivial.		
Control Commands: The Define Password capability is controlled by the ^KP command To set the command: ^XA ^KPxxxx – where xxxx is any four-digit numeric sequence. ^JUS ^XZ To confirm the command is set: To confirm the command worked, use the web page and validate that the password changed. To Default the command: ^XA ^JUF ^XZ		

Note:

The default password is 1234. Since it is documented and well-known default, it is a good idea to change the password to something other than the default.

Certificates Best Practices

Link-OS v5 has added support for user certificates for Weblink, TLS, and HTTPS. This section discusses in general some best practice considerations for creating and using certificates for these network services.

PKI Recommendations

PKI, or public key infrastructure, refers to the organization, creation, maintenance, and disposal of certificates in use for your devices. This section will not exhaustively detail all the best practices for PKI; it will touch on key points to consider for using certificates on your printer.

Provisioning

A certificate consists of public information identifying the device and a set of public and private keys used for encrypted communication to the device.

Because the private key data must be kept secure, it is a best practice to deploy this key to the printer over a physical connection (USB), encrypted secure channel (SFTP mirror), or a segregated provisioning network that is separate from the production or company network. Files can be loaded using any existing file loading mechanism.

Files

The certificate and private key can be deployed to the device as a single file, or separate files. If using a single file, the name of the file must be:

XXXX_CERT.NRD

If using multiple files:

XXXX_CERT.NRD – certificate

XXXX_KEY.NRD – private key

XXXX_CA.NRD – certificate authority chain

Where XXXX is the name of the network service the certificates are intended for.

Acceptable values for XXXX are “WIRED”, “TLSRAW”, “HTTPS”, “WEBLINK1” and WEBLINK2”.

The printer supports PEM, and P12 certificate formats.

Certificate Size Requirements

In keeping with latest industry wide recommendations (NIST, 2016), it is recommended to use only certificates with a digest of SHA-224 or higher. For keys based on RSA or DSA, the size must be 2048 bits or higher. For keys based on ECDSA, the size must be 224 bits or higher. Any certificates with digest or key sizes smaller than this will still be accepted but will not function.

Unique Device Certificates

In general, a certificate is used to uniquely identify a device, determine ownership, and ensure you are communicating with the correct endpoint. The more times a single certificate is used on different devices, the more times the private key must be shared, which increases the risk that the information can be compromised. It is therefore recommended that each printer use its own unique certificate, preferably with a common name that contains the printer hostname. If desired, you can use the same TLS certificate on that device for Weblink, TLS, and HTTPS.

Certificate Life

The longer a certificate is in use, the higher chance it has of being compromised. It is therefore recommended to use the shortest valid certificate life as feasible with the printer in your network. A one-year expiration is the generally accepted recommendation for devices.

Certificate Creation

Because certificates rely on sufficiently random numbers, you will want to ensure the system entropy is sufficiently high for the creation of a new certificate and key. On Linux-based systems, this can be achieved by:

```
cat /proc/sys/kernel/random/entropy_avail
```

You will need to create certificates that contain the host name that the printer will have on the network as its common name in the certificate. As an example, here are some OpenSSL commands to achieve this:

RSA

```
openssl genrsa 2048 > XXXX_KEY.NRD
openssl req -new -x509 -nodes -sha256 -days 365 -key XXXX_KEY.NRD >
XXXX_CERT.NRD
```

You must fill out a valid Country, State, City, Company, and Common name.

ECC

```
openssl ecparam -out ec_params.pem -name prime256v1
openssl req -new -x509 -nodes -sha256 -days 365 -newkey ec:ec_params.pem -keyout
XXXX_KEY.NRD > XXXX_CERT.NRD
```

Supported Ciphers

The following ciphers are supported for Weblink, HTTPS, and TLS:

ECDHE-ECDSA-AES256-GCM-SHA384

ECDH-RSA-AES256-GCM-SHA384

ECDH-ECDSA-AES256-GCM-SHA384

ECDHE-RSA-AES128-GCM-SHA256

ECDHE-ECDSA-AES128-GCM-SHA256

ECDH-RSA-AES128-GCM-SHA256

ECDH-ECDSA-AES128-GCM-SHA256

DH-DSS-AES256-GCM-SHA384

DH-RSA-AES256-GCM-SHA384

DHE-RSA-AES256-GCM-SHA384

DH-DSS-AES128-GCM-SHA256

DH-RSA-AES128-GCM-SHA256

DHE-RSA-AES128-GCM-SHA256

ECDHE-RSA-AES256-SHA384

ECDHE-ECDSA-AES256-SHA384

ECDH-RSA-AES256-SHA384

ECDH-ECDSA-AES256-SHA384

DHE-RSA-AES256-SHA256

DH-RSA-AES256-SHA256

DH-DSS-AES256-SHA256

ECDHE-RSA-AES128-SHA256

ECDHE-ECDSA-AES128-SHA256

ECDH-RSA-AES128-SHA256

ECDH-ECDSA-AES128-SHA256

DHE-RSA-AES128-SHA256

DH-RSA-AES128-SHA256

DH-DSS-AES128-SHA256

AES256-GCM-SHA384

AES128-GCM-SHA256

AES256-SHA256

AES128-SHA256

Printer Time

As certificates rely on a time that they remain valid, the printer must also have the correct time set. If the printer is set to an earlier time than the certificate specifies, the connection will be rejected. To configure the printer time, use the following SGD commands:

rtc.time

rtc.date

LAN 802.1x Security Best Practices

802.1x over LAN provides a mechanism to authenticate devices connecting to a network. To get this set up on the printer, a few settings must be configured. Once configured, the settings will take effect after a reset.

Security

The printer currently supports peap, eap-tls, and eap-ttls security. The choice of printer authentication mode should be driven by what is already in place on your network. In general, eap-tls provides a more robust mutual authentication and requires client certificates. If starting from scratch and with a robust PKI (public key infrastructure) already in place, eap-tls provides a more secure option, but may be more challenging to deploy. You can select your security method by using the following SGD command:

internal_wired.8021x.security

Username

The username is something that is needed for connection to the network and can be configured with the following SGD:

internal_wired.8021x.username

Private Key Passphrase

The client private key for use with TLS security can be optionally encrypted with a passphrase. This is useful if the private key file is in an unprotected part of your network, or needs to be transmitted in the clear.

It is important to note that the passphrase itself is not stored in an encrypted fashion on the printer. Because the passphrase must be kept secure, it is a best practice to configure this passphrase over a physical connection (USB), or a segregated provisioning network that is separate from the production or company network. The private key passphrase can be configured with the following SGD:

internal_wired.8021x.private_key_password

Certificate Files

The certificate filename prefix is WIRED

WIRED_CERT.NRD – certificate file

WIRED_KEY.NRD – private key file (optionally encrypted with private key password)

WIRED_CA.NRD – certificate authority file for the certificate received from the RADIUS server. This is used by the printer to verify the server's identity.

The printer supports PEM, DER, and P12 certificate formats.

TCP Parser Channel Security Best Practices

TCP Configuration

TCP Raw Parser Ports

The printer allows parser communication over TCP via multiple ports. For unencrypted TCP raw access, there are two ports available, 6101 and 9100, and may be configured respectively using the following SGD commands:

ip.port

ip.port_alternate

To make use of TCP raw communication, ensure that it is enabled using the following SGD command:

ip.tcp.enable

TCP Raw JSON Port

In addition to the printer parser, the JSON parser is used exclusively for configuration retrieval and modification with no label formatting support. This JSON parser is accessible via a separate port, 9200, which is configurable using the following SGD command:

ip.port_json_config

TCP Raw Communication

To easily verify the printer is responding, you can attempt to connect to the printer via telnet using one of the ports specified above. Then, send a simple command to the parser to verify it was received and sends data back. You will also be able to view traffic unencrypted via any packet capturing software.

TLS Configuration

Certificate Files

Starting in Link-OS v5, you can also communicate using TLS to provide an encrypted channel to the printer. To begin communicating with the printer over TLS, you first need to deploy a certificate to the device. A certificate consists of public information identifying the device and a set of public and private keys used for encrypted communication to the device.

Please note that any common name will be accepted. However, you should select a common name that preferably contains the printer's host name.

The certificate filename prefix is TLSRAW

TLSRAW_CERT.NRD – certificate file

TLSRAW_KEY.NRD – private key file (cannot be encrypted)

TLSRAW_CA.NRD – certificate authority chain

The certificate authority chain will be presented during connection to the client. It should contain all the appropriate intermediary certificates in the trust chain between the printer's certificate and a trusted authority.

TLS Parser Port

Once the device certificates are loaded and the printer has rebooted, you can begin encrypted communication using TLS. The port for TLS connecting to the printer parser is, by default, 9143, and can be configured using the following SGD command:

ip.tls.port

This, of course, assumes that TLS is enabled using the following SGD command:

ip.tls.enable

TLS JSON Port

As before, the printer also has a JSON parser interface for encrypted communication with TLS using port 9243, and can be configured using the following SGD command:

ip.tls.port_json_config

TLS Communication

To verify the printer is working with the device certificates over TLS, you can issue the following OpenSSL command:

```
echo “~WC” | openssl s_client – connect 10.80.124.159:9143 -quiet
```

This sends the ~WC ZPL print config label command to openssl for a TLS connection to the printer and port specified. If you attempt to view captured packets, you will also find that the data is encrypted and unreadable.

TLS Security Best Practice

Disable Unsecure Network Access

Once TLS communication is verified and operational, it is a security best practice to disable unencrypted forms of communicating with the printer over a network. This includes disabling:

ip.tcp.enable

ip.udp.enable

ip.ftp.enable

ip.lpd.enable

ip.http.enable

ip.snmp.enable

ip.telnet.enable

Enable Firewall Whitelist

It is important to note that in the steps above, we have only established encrypted communication, but not authentication. The printer accepts any connection over TLS and does no authentication of the host. As such, you could also ensure that only communication from the desired host IP address is allowed through use of the following SGD:

ip.firewall.whitelist_in

Public Key Validation

As stated earlier, the TLS implementation does no authentication of devices connecting to it. The client connecting to the printer can, however, validate it is, in fact, talking directly to the printer through the use of comparing public keys. The client should know the public key of the printer that was originally loaded. When making first connection to the printer, the client can verify this pinned public key to the one it is currently receiving from the printer to ensure there is no Man In The Middle (MITM) interference occurring.

HTTPS Security Best Practices

Certificate Files

Starting in Link-OS v5, you can also communicate using HTTPS to view printer web pages over a TLS channel to ensure that communication is encrypted. To begin communicating with the printer over HTTPS, you first need to deploy a certificate to the device. A certificate consists of public information identifying the device and a set of public and private keys used for encrypted communication to the device.

Please note that any common name will be accepted by most browsers. However, you should select a common name that preferably contains the printer's host name.

The certificate filename prefix is HTTPS.

HTTPS_CERT.NRD – certificate file

HTTPS_KEY.NRD – private key file

HTTPS_CA.NRD – certificate authority chain

The certificate authority chain will be presented during connection to the client. It should contain all the appropriate intermediary certificates in the trust chain between the printer's certificate and a trusted authority.

HTTPS Port

Once the device certificates are loaded and the printer has rebooted, you can begin using HTTPS. The port for HTTPS is, by default 443, and can be configured using the following SGD command:

ip.https.port

This assumes that HTTPS is enabled with the following SGD command:

ip.https.enable

Disable HTTP Access

Once HTTPS communication is verified and operational, it is a security best practice to disable unencrypted forms of communicating with the printer over a network. This includes disabling HTTP access using the ip.http.enable command.

Public Key Validation

As stated earlier, the HTTPS implementation does no authentication of devices connecting to it. The client connecting to the printer can, however, validate it is, in fact, talking directly to the printer through the use of comparing public keys. The client should know the public key of the printer that was originally loaded. When making the first connection to the printer, the client can verify this pinned public key to the one it is currently receiving from the printer to ensure there is no Man In The Middle (MITM) interference occurring.

Weblink Security Best Practices

User Supplied Certificates

By default, the printer comes supplied with a generic weblink device certificate and Zebra server certificate authority. These certificates can be used for connecting to a weblink server with a Zebra signed server certificate. Starting with Link-OS v5, the printer can support user-provided weblink certificates, which will be used instead of the default Zebra-provided certificates. Upon reset, once the printer has an IP address, it will attempt to use the provided certificates to make an initial weblink connection.

Certificate Files

Each connection uses its own certificate files: “WEBLINK1” is the filename prefix for connection 1 files, “WEBLINK2” is the filename prefix for connection 2 files. The following filenames shall be used to store the certificates:

WEBLINKX_CERT.NRD – device printer certificate

WEBLINKX_KEY.NRD – device printer private key (cannot be encrypted)

WEBLINKX_CA.NRD – server certificate authority chain

WEBLINKX_CRL.NRD – certificate revocation list

Where “WEBLINKX” is either “WEBLINK1” or “WEBLINK2”

Retry Interval

To prevent flooding a weblink server with connections, it is recommended to configure a random retry interval. This allows for all the devices connecting to the weblink server to attempt reconnection at different times after a connection loss event. The SGD to configure this is:

weblink.ip.connX.retry_interval_random_max

Where connX is the connection 1 or 2 for weblink

If this is set to a non-zero value, the printer will wait a random number of seconds between 1 and the value specified when attempting to reconnect. If the value is zero, then another SGD will be used to configure the number of seconds it will wait before attempting reconnection. The SGD to configure this is:

weblink.ip.connX.retry_interval

Where connX is the connection 1 or 2 for weblink

How to Create a Weblink Server Certificate

1. Download and install the latest version of Open SSL.
2. Create a directory named zebra_certs.
   This directory may reside anywhere you choose (desktop, etc.).
3. From the Start menu, choose “run” and type cmd.exe.

   This opens a DOS prompt.

Note: This step requires that you are an administrator.

4. Navigate to your zebra_certs directory. Run the following commands from this directory:
   - Type: set RANDFILE=.rnd
   - On the command line, type openssl, and then press Enter.
5. Zebra supports RSA and ECC certificates. Enter one the following commands and fill in the fields based on the information provided below:

   Note: zserver.abccompanyinc.com = full DNS name of the server. The DNS name must match the DNS name supplied to the printer as the location URL.

   Note: These commands generate the key and is part of the security for the server communications. DO NOT give this information out to anyone.

   Note: The certificate requires additional information "/C=xx/ST=yyyyy/L=aaaaa/O=jjjjj/OU=rrrrrr/emailAddress=sssss/CN=uuuuu" -key uuuuu.key -out uuuuu.csr

   xx is the two-digit Country Code

   yyyyy is the full State name

   aaaaa is the City or town name

   jjjjj is the Organization or company name

   rrrrrr is the Organizational unit name

   sssss is the contact email address for the certificate creator

   uuuuu is the full DNS name of the server

Listed below is an example of a complete certificate creation request. Type the following commands and hit enter:

RSA

genrsa -out zserver.abccompanyinc.com.key 2048

req -new -sha256 -subj "/C=US/ST=Illinois/L=Anytown/O=ABC Company Inc/OU=IT Team/emailAddress=John@abccompanyinc.com/CN=zserver.abccompanyinc.com" -key zserver.abccompanyinc.com.key -out zserver.abccompanyinc.com.csr

ECC

ecparam -out ec_params.pem -name prime256v1

req -new -sha256 -subj "/C=US/ST=Illinois/L=Anytown/O=ABC Company Inc/OU=IT Team/emailAddress=John@abccompanyinc.com/CN=zserver.abccompanyinc.com" -newkey ec:ec_params.pem -keyout zserver.abccompanyinc.com.key -out zserver.abccompanyinc.com.csr -nodes

6. Email the certificate file (.csr file) to softpm@zebra.com.

   The certificate will be signed and sent back to you.

7. Copy the zip file containing the signed certificate files to the zebra_certs directory.
8. Extract the signed certificate files into the same directory.
9. Enter the following command and fill in the fields based on the information provided below:

   pkcs12 -export -in zserver.abccompanyinc.com.cer -inkey zserver.abccompanyinc.com.key -out zserver.abccompanyinc.com.p12 -name tomcat -CAfile ZebraCAChain.cer -caname root –chain

   Where zserver.abccompanyinc.com is the full DNS name of the server

   Note: This step converts the certificate and asks you to set a passkey.

10. Enter a standard alphanumeric passkey, but do not include any special characters (for example, do not use characters such as $, %, &, or @).

    Note: The passkey should be something easy to remember, but should not be distributed to anyone.

11. Configure your server to use the passkey (created in step 9) and the certificate file. If you are using a Tomcat server, navigate to the Tomcat server.xml in the following directory:

    %TOMCAT_INSTALL_LOCATION%\conf

12. To use the new key/cert, modifiy the ssl connector as follows:

    - Edit the XML document to include the following text within the <Service> XML block.

    <Service name=”Catalina”>

    …

    <Connector SSLEnabled="true" acceptorThreadCount="5"

    clientAuth="want" keyAlias="tomcat"

    keystoreFile="conf/zserver.abccompanyinc.com.p12"

    keystorePass="YourPasskey" keystoreType="pkcs12"

    maxConnections="-1" maxThreads="2500" port="443"

    protocol="org.apache.coyote.http11.Http11NioProtocol"

    scheme="https" secure="true" sessionTimeout="0"

    socket.soKeepAlive="true" sslProtocol="TLS"/>

    …

    </Service>

    - Where zserver.abccompanyinc.com is the full DNS name of the server.
    - Where YourPasskey = passkey from Step 9.

13. Run the following command from the zebra_certs directory:

    %> keytool -importcert -file ZebraCAChain.cer –keystore

    "%JRE_HOME%\lib\security\cacerts" -alias "ZebraCAChain"

    Note: The default password for the Java cacert keystore is changeit.

    Note: Run this command for the same JRE in use by the Tomcat instance being used.

Bluetooth Security Best Practices

Bluetooth security on Link-OS printers is very important when deploying large numbers of remotely-accessible devices into a customer site. Many times, Bluetooth-enabled Zebra devices will follow associates for the duration of a shift - and come into range of the public many times during that shift.

The goal of securing Bluetooth-enabled Zebra printers is to prevent unauthorized access to the printer from a distance. Certain information and profiles can be accessed by any remote device, but some profiles contain sensitive data and/or allow administrative capabilities. For these reasons, it is important to secure Bluetooth connected devices.

Overview

Transports

Bluetooth functionality is divided into two supported *transports*: Classic (also known as BR/EDR) and Low Energy (also known as BTLE or LE). Each transport has slightly different security features and considerations; this document will address them separately.

Some Bluetooth-capable Zebra printers support only Bluetooth Classic, some support only Bluetooth LE, and some support both.

Pairing and Encryption

Pairing in Bluetooth refers to a process in which you can associate two Bluetooth devices with a shared, private encryption key. The storage of these encryption keys for later use is referred to as *bonding.* It is important to note that once two Bluetooth devices are paired, they are considered **trusted.** That is, future connections between those two devices will resume the encrypted session silently, and the remote device will retain access to sensitive profiles. This makes it crucial that two untrusted devices are never paired.

Authentication

Establishing an encrypted connection between two Bluetooth devices is not the only consideration for secure communications; it is often important to establish an *authenticated* connection in addition to an *encrypted* connection. An encrypted connection is considered authenticated if it can be proven that the connected devices exchanged encryption keys without a Man-in-the-Middle (MITM) being able to intercept the keys. Bluetooth uses distinct security procedures depending on whether devices can provide authenticated connections; these will be discussed below for both Classic and LE.

Bluetooth Classic

Discoverability

The bluetooth.discoverable SGD command controls whether the Zebra printer will respond to *inquiry requests* from a remote device. This Classic feature is called *discoverable mode*: if it is disabled, remote devices are not able to easily find the printer. By default, Zebra printers ship with discoverable mode always-on. This implies that as soon as the printer's Bluetooth system is up and running, other devices can see and connect to the printer.

If discoverability is disabled, the printer is still *connectable* if the remote devices knows its Bluetooth address. A handheld computer or phone paired with a printer knows the Bluetooth address of the printer and does not need it to be discoverable to re-connect and re-establish an encrypted connection.

RECOMMENDATION: Only keep discoverable mode enabled for enough time to pair with a remote device; once paired, discoverable mode should be disabled.

NOTE: Zebra devices do not automatically disable discoverability after a duration of time, but this can be achieved via a custom WML menu or by disabling Bluetooth discoverability by communicating with it on another interface (e.g., USB, Ethernet, Wi-Fi).

Pairing

Bluetooth Classic security and pairing modes have evolved with revisions to the standard, and can be divided into three major groups:

1) **No security** – Neither encryption nor authentication are required to access sensitive profiles. Unfortunately, all Bluetooth Zebra printers ship in this default state.
2) **Legacy security (pre-SSP)** – Prior to Bluetooth 2.1, Classic connections could only be secured with a "PIN"; this is a variable-length shared passphrase that allows two devices to start encryption and pairing. Any sequence of bytes may be used to form a PIN, including ASCII characters. It is not limited to numeric values, although not all Bluetooth devices support alphanumeric PIN entry.
3) **Secure Simple Pairing (SSP)** – With the introduction of Bluetooth 2.1, Secure Simple Pairing allows for several types of simple modes to encrypt and authenticate communications between two SSP-enabled devices. The modes available depend on the *I/O capabilities* of the two devices wishing to communicate and provide varying levels of authenticity guarantees and protection against Man-In-The-Middle (MITM) attacks.

When a device supporting SSP tries to access one of the printer's Serial Port Profiles, SSP pairing will always be used. If both devices have a display and support MITM protection, the *Numeric Comparison* pairing procedure will be used. This procedure requires both sides to display and confirm a 6-digit numeric code that is securely exchanged between the two devices. If a third device attempts to Man-In-The-Middle the desired Bluetooth devices, the target devices will display different numeric codes and pairing should be rejected by the user.

If one or both devices do not support a display, the *Just Works* pairing procedure will be used, if allowed by the printer's configuration. *Just* Works mode encrypts the connection, but no prompts will be shown by either side to confirm this process. There is no way to verify that a third device has not performed an MITM attack; *Just Works* is an *unauthenticated* pairing procedure.

Zebra printers also support "no security" and legacy PIN pairing modes to be backwards compatible with early Bluetooth radios and stacks, many of which are still in use by our customers. This feature is enabled by default. However, it is recommended that customers who do not need these modes disable them to prevent unauthorized access.

Bluetooth Classic security capabilities are controlled by four SGDs:

- bluetooth.minimum_security_mode : Selects minimum level of security required for a remote device to access all profiles and services on the printer.
    - 1: No security is required. (**default**)
    - 2: Encryption is required; MITM protection is *not* required.
    - 3: Encryption and MITM protection are required; legacy pairing is enabled.
    - 4: Encryption and MITM protection are required; SSP is required. This will force Numeric Comparison mode.
- bluetooth.allow_non_display_numeric_comparison : for printers without a display, this setting controls whether the Numeric Comparison confirmation code is displayed by physically printing it (**default**), automatically confirming it, or disabling Numeric Comparison entirely.
- bluetooth.bonding : enable (**default**) or disable storage of link keys for paired printers. It is **not recommended** to disable this feature.
- bluetooth.pin *:* Configure the legacy PIN shared secret; we support PINs up to the maximum of 16 bytes. If the PIN is empty, legacy PIN pairing is disabled. The PIN is **empty by default**.

RECOMMENDATIONS: The recommended Bluetooth security configuration will depend on the types of printers in use and the remote devices connecting to them. If the remote devices expected to connect to Zebra printers have a display and support Secure Simple Pairing, and the Zebra printer has a display, it is highly recommended to configure the minimum security level to 4. This forces the remote device to use a pairing mode that supports MITM protection and will not allow legacy nor unencrypted access.

If the printer is a model without a display, it is a bit trickier to use minimum security level 4, as the numeric comparison code for SSP cannot be displayed. Such printers are configured by default to print the comparison code on the customer's media; however, this may not be desirable if frequent pairing is required or if the customer's media is expensive.

If the remote device does not support Bluetooth 2.1 with SSP, the minimum security level should be set to 3 and *bluetooth.pin* must be set to the desired shared secret. This forces MITM protection while allowing legacy PIN pairing. **Legacy PIN pairing is not recommended for new integrations.**

Low Energy

Advertising

The concept of *advertising* mode is similar to discoverable mode in Bluetooth Classic, with a few key differences. Unlike in Bluetooth Classic, Bluetooth LE devices are only connectable while they are MPTES.

NOTE: Zebra printers do not currently support a capability to disable LE advertising without completely disabling Bluetooth LE support, which implies LE-enabled printers are always connectable. To disable Bluetooth LE on dual-mode (Classic+LE) printers, you can set the SGD bluetooth.le.controller_mode to “classic”.

Pairing

Pairing in Bluetooth LE is similar to Classic; pairing can be both authenticated (with MITM protection) and unauthenticated. The SGD bluetooth.le.minimum_security controls whether pairing/encryption is required to access the Zebra Parser Service.

Much like Classic, LE supports a “Just Works” mode (no MITM protection) for devices without a display, and a “passkey” mode that is similar to “Numeric Comparison” on Classic.[1] Passkey pairing provides MITM protection. The SGD bluetooth.le.print_passkey allows printers without a display to print the passkey on media.

RECOMMENDATION: Force pairing requiring MITM support by setting bluetooth.le.minimum_security to “auth_key_encrypt”. If the printer cannot support display of the passkey, set it to “unauth_key_encrypt”.

[1] Bluetooth LE 4.1+ support a true Numeric Comparison mode, but this is not yet supported in Zebra products.

Certificate Downloading

To download the various certificate files to the printer, choose one of the following methods:

1. FTP:
   - If using FTP, make sure that the printer's "execute file" function is turned off while you send the file, so the file is stored and not processed as a printing command. This can be done by sending the following command:

! U1 setvar "ip.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 certificate files.

   - Connect to the printer via FTP and download the certificates to the printer.

Note: Use the appropriate file name as discussed in the *Certificates Best Practices* section of this document.

2. Zebra SDK:
   - Use the Zebra Multiplatform SDK command line STORE function to send the files to the printer. The SDK is available for download at www.zebra.com/sdk

Note: Use the appropriate file name as discussed in the *Certificates Best Practices* section of this document.

3. ZPL:
   - Use the `! CISDSFCRC16` command, with the appropriate headers to the certificate to store the files on E: drive of the printer. Details available in the ZPL Programming Guide, available at www.zebra.com.
   - Use the ~DY command, with the appropriate header to the certificate to store the files on E: drive of the printer. Details available in the ZPL Programming Guide, available at www.zebra.com.

Note: Use the appropriate file name as discussed in the *Certificates Best Practices* section of this document.

Validating Certificates

To validate that your certificates are loaded onto the printer correctly, choose one of the following methods.

1. ZPL
   - Issuing one of the following commands allows you to confirm that the certificates have been stored on the file system. This can be done utilizing a terminal program or Zebra Setup Utilities.

^XA^WDE:*.nrd^XZ

Note: The above command will print a label listing all the files on the E: drive that have the ".nrd" extension.

^XA^HWE:*.NRD^XZ

Note: The above command will transmit a listing back to the host with all the files on the E: drive that have the ".nrd" extension.

2. Internal Web Page:
   - Log into the internal web page and select Directory Listing.

You will be able to confirm that the certificate files are on the file system. However, you will only be able to see the files; you not be able to download them or view the contents.

Deleting Certificates

To delete certificates loaded on the printer, use the following method.

1. ZPL
   a. Issuing the following command allows you to delete a certificate file stored on the file system. This can be done utilizing a terminal program or Zebra Setup Utilities.

^XA^IDE:CERTNAME.NRD^XZ

where "CERTNAME" is a single certificate file name.

or

^XA^IDE:*.NRD^XZ

This will delete all files with the .nrd extension.

   b. Issuing the following SGD command allows you to delete the specified file stored on the file system.

! U1 do "file.delete" "value"

Corporate Headquarters

Zebra Technologies Corporation
3 Overlook Point
Lincolnshire, IL 60069 USA
T: +1 847 634 6700
Toll-free +1 866 230 9494
F: +1 847 913 8766

http://www.zebra.com

P1099957-002