© 2015 ZIH Corp. and/or its affiliates. All rights reserved. The copyrights in this manual and the software and/or firmware in the print engine described therein are owned by ZIH Corp. and Zebra's licensors. Unauthorized reproduction of this manual or the software and/or firmware in the print engine may result in imprisonment of up to one year and fines of up to $10,000 (17 U.S.C.506). Copyright violators may be subject to civil liability.

This product may contain ZPL®, ZPL II®, and Link-OSTM programs; Element Energy Equalizer® Circuit; E3®; and Monotype Imaging fonts. Software © ZIH Corp. All rights reserved worldwide.

Link-OSTM and all product names and numbers are trademarks, and Zebra, the Zebra logo, ZPL, ZPL II, Element Energy Equalizer Circuit, and E3 Circuit are registered trademarks of ZIH Corp. All rights reserved worldwide.

All other brand names, product names, or trademarks belong to their respective holders. For additional trademark information, please see “Trademarks” on the product CD.

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 of 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.

rapidJson Library  Copyright © 2011 Milo Yip

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

libCurl Library  COPYRIGHT AND PERMISSION NOTICE Copyright © 1996 - 2012, Daniel Stenberg, <daniel@haxx.se>. All rights reserved. Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies. THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OF THIRD PARTY RIGHTS. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE. Except as contained in this notice, the name of a copyright holder shall not be used in advertising or otherwise to promote the sale, use or other dealings in this Software without prior written authorization of the copyright holder.
Apache Tomcat  Copyright © 1999-2013, The Apache Software Foundation

Sun, Sun Microsystems, Solaris, Java and JavaServer Pages are trademarks or registered trademarks of Oracle Corporation. UNIX is a registered trademark in the United States and other countries, exclusively licensed through 'The Open Group'. Microsoft, Windows, WindowsNT, and Win32 are registered trademarks of Microsoft Corporation. Linux is a registered trademark of Linus Torvalds. All other product names mentioned herein and throughout the entire web site are trademarks of their respective owners.

"Apache Tomcat" and "Tomcat" are trademarks of the Apache Software Foundation. Use of these trademarks is subject to the terms of section 6 of Apache License, Version 2.0 (current).
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Troubleshooting</td>
<td>48</td>
</tr>
<tr>
<td>Troubleshooting</td>
<td>49</td>
</tr>
<tr>
<td>SSL/TLS Certificate Errors</td>
<td>51</td>
</tr>
<tr>
<td>Other Typical Errors</td>
<td>53</td>
</tr>
<tr>
<td>Troubleshooting</td>
<td>54</td>
</tr>
<tr>
<td>HTTP Messages</td>
<td>55</td>
</tr>
<tr>
<td>WebLink Set/Get/Do Commands</td>
<td>55</td>
</tr>
<tr>
<td>Introduction to SGD Commands</td>
<td>56</td>
</tr>
<tr>
<td>weblink.enable</td>
<td>57</td>
</tr>
<tr>
<td>weblink.ip.conn[1</td>
<td>2].authentication.add</td>
</tr>
<tr>
<td>weblink.ip.conn[1</td>
<td>2].authentication.entries</td>
</tr>
<tr>
<td>weblink.ip.conn[1</td>
<td>2].authentication.remove</td>
</tr>
<tr>
<td>weblink.ip.conn[1</td>
<td>2].enable</td>
</tr>
<tr>
<td>weblink.ip.conn[1</td>
<td>2].location</td>
</tr>
<tr>
<td>weblink.ip.conn[1</td>
<td>2].proxy</td>
</tr>
<tr>
<td>weblink.ip.conn[1</td>
<td>2].retry_interval</td>
</tr>
<tr>
<td>weblink.ip.conn[1</td>
<td>2].test.location</td>
</tr>
<tr>
<td>weblink.ip.conn[1</td>
<td>2].test.retry_interval</td>
</tr>
<tr>
<td>weblink.ip.conn[1</td>
<td>2].test.test_on</td>
</tr>
<tr>
<td>weblink.logging.clear</td>
<td>73</td>
</tr>
<tr>
<td>weblink.logging.entries</td>
<td>74</td>
</tr>
<tr>
<td>weblink.logging.max_entries</td>
<td>75</td>
</tr>
<tr>
<td>weblink.printer_reset_required</td>
<td>77</td>
</tr>
<tr>
<td>weblink.restore_defaults</td>
<td>78</td>
</tr>
</tbody>
</table>
About This Document

This section provides you with contact information, document structure and organization, and additional reference documents.

Contents

Who Should Use This Document ..................................................... 8
How This Document Is Organized .................................................. 8
Document Conventions .................................................................... 9
Who Should Use This Document

This User Guide is intended for use by any person who needs to install, perform routine maintenance, upgrade, or troubleshoot problems with the Zebra AirWatch Connector software.

How This Document Is Organized

The User Guide is set up as follows:

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>This section provides general information about the Zebra AirWatch Connector.</td>
</tr>
<tr>
<td>Installation</td>
<td>This section outlines the system requirements for installation and provides specific details for the installation of Zebra AirWatch Connector.</td>
</tr>
<tr>
<td>Configuring Printers with WebLink</td>
<td>This section describes basic, network, and firewall configurations for printers connected to Zebra AirWatch Connector.</td>
</tr>
<tr>
<td>Using AirWatch Connector</td>
<td>This section provides specific information about organizing and managing printers via Zebra AirWatch Connector.</td>
</tr>
<tr>
<td>Troubleshooting</td>
<td>This section provides troubleshooting information about the Zebra AirWatch Connector.</td>
</tr>
<tr>
<td>WebLink Set/Get/Do Commands</td>
<td>This section describes the Set/Get/Do commands, parameters, and values that are available with Zebra AirWatch Connector.</td>
</tr>
</tbody>
</table>
Document Conventions

The following conventions are used throughout this document to convey certain information.

**Alternate Color** (online only) Cross-references contain hot links to other sections in this guide. If you are viewing this guide online in .pdf format, you can click the cross-reference (blue text) to jump directly to its location.

**Command Line Examples** Command line examples appear in Courier New font. For example, type `ZTools` to get to the Post-Install scripts in the `bin` directory.

**Files and Directories** File names and directories appear in Courier New font. For example, the `Zebra<version number>.tar` file and the `/root` directory.

Icons Used

- **Important** • Advises you of information that is essential to complete a task.

- **Note** • Indicates neutral or positive information that emphasizes or supplements important points of the main text.

- **Example** • Provides an example, often a scenario, to better clarify a section of text.
Introduction

This section provides general information about the Zebra AirWatch Connector.

Contents

Overview ................................................................. 12
What the AirWatch Connector Does ................................. 12
Supported Printers ..................................................... 12
Supported Operating Systems ....................................... 12
Overview

The Zebra AirWatch Connector partners with the AirWatch server to manage your Zebra Link-OS™ printers.

Zebra AirWatch Connector will:

- Monitor printers and report issues to the AirWatch system
- Monitor printer alerts
- Enable administrators to send files and operating system updates to the printer via the AirWatch server console

What the AirWatch Connector Does

Zebra AirWatch Connector sends alerts to AirWatch, watches printers coming online, monitors the status of the printers, and sends files and settings to the printers.

Supported Printers

- QLn320™ Ethernet and Wi-Fi
- QLn220™ Ethernet and Wi-Fi
- QLn420™ Ethernet and Wi-Fi
- iMZ320™ Wi-Fi
- iMZ220™ Wi-Fi
- ZD500R™ Ethernet and Wi-Fi
- ZD500™ Ethernet and Wi-Fi
- ZQ500™ Series Wi-Fi
- ZT200™ Series Ethernet and Wi-Fi
- ZT400™ Series Ethernet and Wi-Fi

Supported Operating Systems

The Zebra AirWatch Connector supports the 32-bit or 64-bit versions of the following:

- Windows® Server 2008
- Windows Server 2008 R2 (also known as Windows 7 Server)
This section outlines the system requirements for installation and provides specific details for the installation of Zebra AirWatch Connector.

Contents
- Installing in a Windows Operating System ................................................................. 14
- Minimum System Requirements ................................................................................... 14
- Installation Steps .......................................................................................................... 15
  - Step 1: Install an AirWatch Server ............................................................................. 15
  - Step 2: Install Wizard ............................................................................................... 15
  - Step 3: Set Up Printers ............................................................................................. 22
  - Step 4: Test a Printer ............................................................................................... 23
Installing in a Windows Operating System

Minimum System Requirements

The Zebra AirWatch Connector supports the 32-bit or 64-bit versions of the following:

- Windows Server 2008
- Windows Server 2008 R2 (also known as Windows 7 Server)

**Note** • This system should be installed on a “clean” Windows Server. A clean system is one that does not already include Apache Tomcat™ or any other server software installation. Tomcat will be installed as part of this installation procedure and must be the only Tomcat version resident on this system. Multiple versions of Tomcat will encounter conflicts.
Installation Steps

Step 1: Install an AirWatch Server

1. Contact AirWatch.
   a. Contact AirWatch Customer Support to obtain an AirWatch version 7.0 or later installation.
   b. Obtain the AirWatch Endpoint URL from your AirWatch support representative.

   Note • The URL you will be searching for usually starts with the deviceservices server. Ask for the Zebra printer management URL.

   Example • https://airwatchportals.com/deviceservices/peripheralservice/v1/register

Step 2: Install Wizard

1. Run AirwatchConnector-x-64.exe.
   Depending on your account security settings, you may see the following dialog box.

   ![User Account Control]
   a. Click Yes to begin installing AirWatch Connector.
b. Click **Next** to continue.
c. You must accept the terms of the License Agreement to continue.
d. Click I Agree.

2. Enter the information associated with your certificate.
3. Click **Next**.
   The installer will fill in the Zebra Wakeup Location.

4. Log into AirWatch.
   a. Click on **Devices > Printers > Print Server**.

There are 0 devices at this Organization Group level. Add at least one device to view the Device Dashboard.
5. Click **Add Print Server** (at the top of the right pane).

6. Fill in your **Friendly Name**.

7. Select your **User Id**.

8. Fill in your **Service UID**.

9. Click **Save**.
10. Re-open the Zebra AirWatch Connector Setup dialog box.

11. Enter the base Group ID for your company from your AirWatch installation.

12. Enter the **AirWatch Server Location**.

   **Note** • The URL starts with the device services server. Ask for the Zebra printer management URL.

   **Example** • http://airwatchportals.com/deviceservices/peripheralservice/v1/register

13. Copy and paste the HMAC Token (from the AirWatch Add Print Server dialog box) into the **Airwatch Token** field on the Setup dialog box (below).

14. Enter the Service UID (created in the Add Print Server dialog box on the AirWatch website) in the **Unique ID for Zebra Server** field.

15. Click **Next**.
16. Choose the destination folder.

![Choose Install Location dialog box with destination folder chosen and space required information shown.]

17. Click Install.

![Installation Complete dialog box showing successful installation.]

Nullsoft Install System v3.0b1
18. Click Next.

19. Click Finish.

Step 3: Set Up Printers

1. Set up your printers to communicate with AirWatch:
   a. Download the latest operating system for your printers from http://www.zebra.com
   b. Using the ZDownloader Utility, install the firmware on your Zebra printers. (To obtain a copy of the ZDownloader Utility, go to www.zebra.com/utilities.)
   c. Using the Zebra Setup Utilities, configure your printer on your network.
   d. Set up the printers based on the Configuring Printers with WebLink on page 27.
Step 4: Test a Printer

Request Settings from a Printer

In this section, you will test a printer to verify that the AirWatch console is able to request the current settings from the printer.

1. Turn on the printer.

2. Log into the AirWatch console, if necessary.

   **Note** • Once you are logged in, the printer appears on your console after approximately 60 seconds. (See figure below.)

3. To see specific details about this printer, click on the Friendly Name of the printer.
The printer summary appears. If the printer settings appear on the screen, AirWatch is receiving settings from the printer.
Receiving Alerts from a Printer

In this section, you will test that the AirWatch console receives alerts from the printer.

1. Click the Alerts tab.

2. Open the media door on the printer.

3. Wait 10 seconds, and then refresh the AirWatch console display.
   You should see the Head Open alert with the orange exclamation mark in the Status column.

4. Close the media door on the printer.

5. Wait 10 seconds, and then refresh the AirWatch console display.
   You should see the Head Open alert with the blue check mark in the Status column. If the alerts appear on the screen, you have verified that the printer is able to send alerts to the AirWatch console.

Note • Both the Status icon and the Sample Time change on the Alerts screen.
Notes •

__________________________________________________________________________
__________________________________________________________________________
__________________________________________________________________________
__________________________________________________________________________
__________________________________________________________________________
__________________________________________________________________________
__________________________________________________________________________
__________________________________________________________________________
Configuring Printers
with WebLink

This section describes basic, network, and firewall configurations for printers connected to Zebra AirWatch Connector.

Contents

Configuring Weblink ................................................................. 28
Basic Configuration ................................................................. 28
When a Proxy Server is Part of the Network Configuration ............... 28
When HTTP Authentication is Necessary .................................. 29
Additional Firewall Configuration .......................................... 30
Difference Between Conn1 and Conn2 ..................................... 30
Enable Logging ........................................................................ 30
Navigating the Log Output ....................................................... 31
Configuring Weblink

When any WebLink setting (with the exception of the logging settings) is adjusted either via SNMP, SGD, or JSON it is required that the printer be reset before the new value takes effect. The `weblink.printer_reset_required` setting will be set to "yes" if there are any settings that have been modified that require a printer reset.

Basic Configuration

**To determine how much configuration is necessary, consider the following questions:**

- Is the remote server that the printer is attempting to connect to outside of the corporate firewall?
- Does the firewall require a username and password to access the remote server?
- Does the printer require a proxy server to access the remote server?
- Does the firewall permit HTTPS connections initially, or does the printer need to connect via HTTP first?

If the answer to any of these questions is ‘yes’, then more than the basic configuration may be necessary. Depending upon the network environment that the printer is in, accessing the remote server may only require that a few settings be set.

The minimum requirement is that the URL for the remote server be set. For simplicity, assume that only `conn1` is being used (this is the typical scenario). See also *Difference Between Conn1 and Conn2* on page 31.

**To configure the printer to connect to the remote server:**

1. Set `weblink.ip.conn1.location` to the URL of the remote server.

   - The URL must conform to the standards described in RFC3986 ([http://www.rfc.org/rfc/rfc3986.txt](http://www.rfc.org/rfc/rfc3986.txt)). For example, if the remote servlet’s full URL is `https://www.examplecorpinc.com/zebra/weblink/` Configure the location setting as follows:

   ```
   U1 setvar "weblink.ip.conn1.location" "https://www.examplecorpinc.com/zebra/weblink/"
   ```

2. Reset the printer.

   - When the printer has an IP address, it will attempt to connect to the remote server. In the event that the remote server does not indicate that the printer has connected, logging may need to be enabled in order to determine the failure.

When a Proxy Server is Part of the Network Configuration

If a proxy server must be used to access the remote server, the printer’s proxy setting must be set to connect to the server. There are typically four properties associated with a proxy server:

- The proxy server scheme: HTTP or HTTPS
- The proxy server address
To supply the address of the proxy server (assuming a default port and no username/password), configure the proxy setting as follows:

![setvar] "weblink.ip.conn1.proxy" "https://my.internal.proxy/"

In this scenario, the proxy address is `my.internal.proxy` and the scheme is HTTPS. The default port (1080) will be used. No username or password will be used to authenticate with the proxy.

To specify an alternate port, configure the proxy as follows:

![setvar] "weblink.ip.conn1.proxy" "https://my.internal.proxy:3128/"

To specify a username and password configure the proxy as follows:

![setvar] "weblink.ip.conn1.proxy" "https://user:pass@my.internal.proxy/"

The proxy username, password, and the rest of the URL must follow the rules specified in RFC3986 (http://www.ietf.org/rfc/rfc3986.txt).

When HTTP Authentication is Necessary

Use this configuration when, for example, a firewall requires a username and/or password.

It may be necessary to specify a username and password to various routers and servers along the path to the remote server. Typically, when using a browser to access the server, the authentication request will be presented in the form of a dialog window that asks for the username and password.

Because the printer’s connection to the remote server is headless and non-interactive, the Weblink configuration allows a user to enter in a server name/username/password triplet. The triplet will be used in the event that the printer is presented with an authentication request (for example, this typically is requested via the HTTP/1.1 401 Unauthorized request).

To specify authentication credentials, issue the following:

![setvar] "weblink.ip.conn1.authentication.add" "servername.com username password"

In this scenario, the server requesting authentication is servername.com. The username and password to be supplied are ‘username’ and ‘password’. The server name can be either a DNS name or an IP address. The username and password cannot be retrieved from SGD, SNMP, or JSON once added. Only the server name will be returned.

More than one set of authentication triplets can be added. The printer will only use the credentials as they are needed. In other words, the printer will only use the credentials for servername.com if it receives a HTTP/1.1 401 Unauthorized request from servername.com.

To see what authentication triplets are specified issue:

![getvar] "weblink.ip.conn1.authentication.entries"

To remove authentication credentials issue the following:

![setvar] "weblink.ip.conn1.authentication.remove" "servername.com"
Additional Firewall Configuration

Some firewalls do not allow the first connection attempt for a device to be HTTPS, or they require new connections to be made periodically in order to keep the initial connections intact. The weblink test branch was provided to address issues that typically arise because the printer is an unattended device.

To configure the printer to attempt an HTTP connection anytime that the HTTPS connection drops, issue the following commands:

```
! U1 setvar "weblink.ip.conn1.test.location" "http://www.zebra.com/apps/linktest"
! U1 setvar "weblink.ip.conn1.test.test_on" "failure"
```

The `weblink.ip.conn1.test.location` can be any valid HTTP address. The default uses a link provided by Zebra that exists for no other purpose than to help developers test their connections to the internet. Setting `weblink.ip.conn1.test.test_on` to interval or both will force the printer to attempt a connection to the URL in location every `weblink.ip.conn1.test.retry_interval` seconds (default is 900 seconds/15 minutes).

To configure the printer to try an HTTP connection periodically, independent of the HTTPS success, issue the following commands:

```
! U1 setvar "weblink.ip.conn1.test.location" "http://www.zebra.com/apps/linktest"
! U1 setvar "weblink.ip.conn1.test.test_on" "interval"
! U1 setvar "weblink.ip.conn1.test.retry_interval" "900"
```

Difference Between Conn1 and Conn2

The printer has the ability to connect to two different servers. Connection 1 (conn1) and Connection 2 (conn2) are identical in every way in terms of their configuration. It is expected that conn2 will typically be left unmodified unless a user has an alternate server that they wish to use to configure the printer.

A typical scenario in which both connections would be used is if a user wishes to have the printer connect to both a configuration server and a data source.

Enable Logging

If your printer has trouble connecting, you may wish to enable logging. By default, logging is not enabled in order to reduce the amount of memory consumed when the Weblink feature is enabled. It is recommended that, once the Weblink feature is configured properly and is performing as expected, the logging be disabled or that a very small (less than 100) number of logging entries be permitted.

To enable logging, `weblink.logging.max_entries` needs to be modified. By default, it is set to zero (0), which indicates that no messages are logged. When attempting to troubleshoot connection issues, it is recommended that `max_entries` be set to at least 100 entries. Setting `max_entries` to 100 means that the 100 newest logging entries will be present in `weblink.logging.entries`. Older entries are discarded when the maximum number of entries is reached.

```
! U1 setvar "weblink.logging.max_entries" "100"
```
The logging settings are atypical to the Weblink settings as they do not require the printer to be reset before taking effect. This does not mean that previous logging messages that would have been logged will appear when the max_entries setting is changed from zero (0) to a greater value. It means that any new logging messages will be logged from that point forward.

Issue the following command to clear any log entries currently in the weblink.logging.entries buffer.

```
! U1 do "weblink.logging.clear" ""
```

**Navigating the Log Output**

The log will contain useful information, even in the scenario where the printer successfully connects to the remote server. This section explains how to read the log and highlights some of the key entries that will help to determine if the connection was successful.

A typical log entry looks as follows:

```
```

The first column is the date and time that the event occurred. The format of the date and time matches the format of rtc.date and rtc.time. The time, however, also includes the milliseconds to aid in troubleshooting network latency concerns.

The second column indicates the connection name and channel that the entries are associated with. The connection name will match the weblink branch that was configured with the respective URL (for example, conn1 or conn2). The channel number indicates which channel on the respective connection that the entries corresponds to.

**Note •** For printers that do not have a battery to store the Real Time Clock (RTC) value, the date will be restored to the default value upon a power cycle. The default value depends upon how the rtc.date Set/Get/Do (SGD) is managed. If it has never been set, then it will default to the firmware build date (the value in appl.date). Otherwise, the value in rtc.date will default to the value that it was last set to. This does not mean the value of the rtc.date when it was power cycled – it means that when a user sets rtc.date, that value becomes the new default value. If the printer has a battery, then the rtc.date never defaults and continues to track the date as expected.

The third column is the actual message, which contains information about what occurred in the printer at the corresponding time in column one. In the above example, the printer was initiating the connection to the URL specified in weblink.ip.conn1.location.

Review the section titled *SSL/TLS Certificate Errors on page 50* to understand what it means when certain logging messages/errors appear in the log.
This section provides specific information about organizing and managing printers via Zebra AirWatch Connector.

Contents
- Printer Discovery ................................................................. 34
- Organizing Printers ............................................................. 35
- Create a Group ................................................................. 35
- Add Printers to the Group .................................................... 37
- View the Location Group Dashboard ..................................... 38
- Profiles ................................................................. 39
- Create a Profile ................................................................. 39
- Manage a Profile ................................................................. 41
- Updating Printer Firmware and Files ............................................. 42
  - Upload a File ................................................................. 42
  - Manage a File ................................................................. 44
- Checking Printer Status ............................................................ 45
Printer Discovery

When a new printer is powered on, it will automatically notify Zebra AirWatch Connector that it is operational. There are several methods to validate that the printer is operational, settings are available, and communication is active.

- To determine if the settings are available, see Request Settings from a Printer on page 23.
- To refresh the printer settings, click Device Query on the Printer Summary page.
- To remotely power on and power off the printer, click Soft Reset.

**Important** • Do not click Factory Reset unless directed to do so by Technical Support. Factory Reset will change settings and lose the Location Group.
Organizing Printers

After you see the printers on the AirWatch console, you may wish to organize or arrange groups of printers. These groups may be established based on location, role, or region.

Create a Group

1. On the AirWatch console, select the Main Menu at the top left of the screen.

2. In the Configuration section, select Location & Groups.

3. Click on the Main Group link (on the left side of the screen).
4. Click Add Child Location Group.

5. Name the Location Group.

6. Enter the Group ID.

   **Important** • Even though the Location Group ID is not identified as required, you must fill in this field in order to group the Zebra printers.

7. Fill in the next three fields:
   a. Location Group Type
   b. Country
   c. Locale

   **Note** • You may change the fields: Internal Name and Display Name even though these and the other fields below them are auto-populated.

8. Click Save.
Add Printers to the Group

1. Navigate to the Printer Asset Management screen.

2. To add a printer to your new group, click on the Printer Friendly Name.

3. In the Device Details, select Admin > Change Location Group.

4. Click the Location dropdown menu, and select your new group.

5. Click Save.

6. Repeat step 1 through step 5 for all printers that you wish to include in the group.
View the Location Group Dashboard

1. Navigate back to your Asset Tracking screen.
2. Click on the name of your new Location Group.
Profiles

Using profiles is the preferred method to manage and ensure that printer settings within a group are the same.

Create a Profile

1. From the Main Dashboard screen, click Printer Profiles.

2. From the Printer Profiles screen, click Add a New Profile.
3. Fill in the name and description of the profile.

4. Select the Assignment Type from the dropdown menu.

**Note** • Profiles consist of three Assignment Types:
- **Auto**: the profile will be sent automatically to the printers within the Assigned Location Group.
- **Optional**: the profile will be assigned to the Assigned Location Group, but it must be manually sent to the group.
- **Interactive**: the profile will not be assigned to any group, and it can be sent to any printer in any group.

5. Fill in the printer Model and the Assigned Location Groups.

6. Choose one of the following categories:

**Note** • Do not attempt to include any Custom Settings. This category is not operational at this time.

7. Fill in all of the settings associated with your category.
8. Click Save.

9. Repeat step 6 through step 8 for all categories you wish to include in the profile.

10. Click Save & Publish.

   **Note:** The Save & Publish button will immediately send (“publish”) the settings to those groups with an Assignment Type of “Auto”.

**Manage a Profile**

1. Navigate to the Asset Tracking Dashboard.

2. Click on the Printer Friendly Name.

3. Click on the Profiles tab.

   You will see all of the profiles that are available to be downloaded.

4. Click on Actions (see red box) to load the profile immediately to the selected printer.

5. Validate that the Auto Assignment Type profile has been sent to the printer by checking the Status Indicator.
Updating Printer Firmware and Files

You can use AirWatch to update printer’s operating system and object files. The steps are similar to managing a profile.

Upload a File

1. From the Main Dashboard screen, click Printer Files.

2. From the Printer Files screen, click Add New File.
3. Fill in the name of the file.

4. Select the Assignment Type from the dropdown menu.

**Note** • Profiles consist of three Assignment Types:
- **Auto**: the file will be sent automatically to the printers within the Assigned Location Group.
- **Optional**: the file will be assigned to the Assigned Location Group, but it must be manually sent to the group.
- **Interactive**: the file will not be assigned to any group, and it can be sent to any printer in any group.

5. Fill in the printer Model and the Assigned Location Groups.

6. Choose File (left-hand menu).

7. Click Upload.

8. Select the file you wish to upload from the dialog box.

9. Click Save.

10. Click Save & Publish.

**Note** • The Save & Publish button will immediately send (“publish”) the settings to those groups with an Assignment Type of “Auto”.
Manage a File

1. Navigate to the Asset Tracking Dashboard.

2. Click on the Printer Friendly Name.

3. Click on the Files tab.
   You will see all of the files that are available to be downloaded.

4. Click on Actions (see red box) to load the file immediately to the selected printer.

5. Validate that the Auto Assignment Type file has been sent to the printer by checking the Status Indicator.
Checking Printer Status

Printer status is communicated to AirWatch via alerts. The following table identifies the current alerts managed by AirWatch Connector.

<table>
<thead>
<tr>
<th>Alert</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PAPER OUT</td>
<td>Paper is out.</td>
</tr>
<tr>
<td>RIBBON OUT</td>
<td>Ribbon is out.</td>
</tr>
<tr>
<td>HEAD TOO HOT</td>
<td>The printhead is too hot to print.</td>
</tr>
<tr>
<td>HEAD COLD</td>
<td>The printhead is too cold to print.</td>
</tr>
<tr>
<td>HEAD OPEN</td>
<td>The printhead/media door is open.</td>
</tr>
<tr>
<td>SUPPLY TOO HOT</td>
<td>The power supply is too hot.</td>
</tr>
<tr>
<td>RIBBON IN</td>
<td>The ribbon has been loaded in the printer.</td>
</tr>
<tr>
<td>REWIND</td>
<td>The rewind unit is full (for tabletop printers with a rewind unit).</td>
</tr>
<tr>
<td>CUTTER JAMMED</td>
<td>The cutter is jammed.</td>
</tr>
<tr>
<td>HEAD ELEMENT BAD</td>
<td>A printhead element has burned out.</td>
</tr>
<tr>
<td>POWER ON</td>
<td>The printer has powered on.</td>
</tr>
<tr>
<td>CLEAN PRINTHEAD</td>
<td>This alert is sent when the printing odometer has reached the number of meters printed.</td>
</tr>
<tr>
<td>MEDIA LOW</td>
<td>The paper/media is low.</td>
</tr>
<tr>
<td>RIBBON LOW</td>
<td>The ribbon is low.</td>
</tr>
<tr>
<td>REPLACE HEAD</td>
<td>The printhead needs to be replaced.</td>
</tr>
<tr>
<td>BATTERY LOW</td>
<td>The battery charge is low.</td>
</tr>
<tr>
<td>RFID ERROR</td>
<td>The RFID encoding has encountered an error.</td>
</tr>
<tr>
<td>COLD START</td>
<td>The printer has been powered on.</td>
</tr>
</tbody>
</table>

**Note**: This alert is set using the Set/Get/Do command “device.cph_interval”. The airwatch console shows the setting as “Clean Printhead Interval”.

For more specific information on viewing alerts from AirWatch console, see *Receiving Alerts from a Printer* on page 25.
Using AirWatch Connector
Checking Printer Status

Notes • ____________________________________________

__________________________________________________________________________

__________________________________________________________________________

__________________________________________________________________________

__________________________________________________________________________

__________________________________________________________________________

__________________________________________________________________________

__________________________________________________________________________

__________________________________________________________________________

__________________________________________________________________________
Troubleshooting

This section provides troubleshooting information about the Zebra AirWatch Connector.

Contents

Troubleshooting ................................................................. 48
Installation ........................................................................ 48
Using AirWatch ................................................................. 49
SSL/TLS Certificate Errors ................................................ 50
Other Typical Errors .......................................................... 52
Troubleshooting ................................................................. 53
HTTP Messages ................................................................. 54
## Troubleshooting

### Installation

<table>
<thead>
<tr>
<th>Issue</th>
<th>Reason</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Error when starting Tomcat</td>
<td>Various reasons can cause this error.</td>
<td>See Apache Tomcat website — <a href="http://tomcat.apache.org/tomcat-7.0-doc/index.html">http://tomcat.apache.org/tomcat-7.0-doc/index.html</a></td>
</tr>
</tbody>
</table>
| Tomcat Port conflict error| There is another server trying to use the same port as Zebra AirWatch Connector on the computer. The default port is 443. | Choose one of the following:  
  • Stop the other servers using Windows services.  
  • Change the port in Tomcat.  
  **Important** • If you change the port, you must change the “weblink.location” on the printer. From the Control Panel, open Windows Firewall, Advanced settings, and manually add the Port to the allowed Inbound/Outbound list. |
# Using AirWatch

<table>
<thead>
<tr>
<th>Issue</th>
<th>Reason</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>I add a printer to a Location Group. Once the printer is powered off</td>
<td>Some settings are not stored until a profile is published</td>
<td><strong>a.</strong> Create a generic profile for the Location Group.</td>
</tr>
<tr>
<td>and on, it is no longer associated with the original location group.</td>
<td>to that printer.</td>
<td><strong>b.</strong> Set the option to Auto install and click Publish.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(All settings are saved and sent to all of the printers within the group.)</td>
</tr>
</tbody>
</table>
## SSL/TLS Certificate Errors

Secure connections to the remote server present the opportunity for several errors when attempting to connect. The errors typically involve the certificates used when connecting via SSL or TLS. This section highlights some of the most common issues involving the certificates.

<table>
<thead>
<tr>
<th>Error</th>
<th>Cause / Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>&quot;SSL certificate problem: self signed certificate in certificate chain&quot;</td>
<td>One of the situations that prevent a successful connection is not having the correct Certificate Authority certificates installed on the remote server. Zebra requires that the Zebra Root Certificate Authority and the Zebra Subordinate Certificate Authority be installed on the remote server. This error typically indicates that only one of the Zebra Certificate Authority certificates is installed on the remote server.</td>
</tr>
<tr>
<td>&quot;SSL certificate problem: unable to get local issuer certificate&quot;</td>
<td>One of the situations that prevent a successful connection is not having the correct Certificate Authority certificates installed on the remote server. Zebra requires that the Zebra Root Certificate Authority and the Zebra Subordinate Certificate Authority be installed on the remote server. This error typically indicates that neither of the Zebra Certificate Authority certificates are installed on the remote server.</td>
</tr>
<tr>
<td>&quot;SSL certificate problem: certificate has expired&quot;</td>
<td>This error indicates that the remote server’s certificate has expired. This is typically an indication that the printer’s date and/or time are incorrect as the Zebra certificates are typically issued for long durations. Check that <code>rtc.date</code> and <code>rtc.time</code> are set correctly.</td>
</tr>
</tbody>
</table>

**Note** • For printers that do not have a battery to store the Real Time Clock (RTC) value, the date will be restored to the default value upon a power cycle. The default value depends upon how the `rtc.date` SGD is managed. If it has never been set then it will default to the firmware build date (the value in `appl.date`). Otherwise, the value in `rtc.date` will default to the value that it was last set to. This does not mean the value of the `rtc.date` when it was power cycled. It means that when a user sets `rtc.date` that becomes the new default value. If the printer has a battery, then the `rtc.date` is never default and continues to track the date as expected.
**Error** | **Cause / Solution**
---|---
"SSL certificate problem: certificate is not yet valid" | This error indicates that the remote server’s certificate was incorrectly issued or that the printer’s date and/or time are incorrect. Check that the printer’s date and time (rtc.date and rtc.time) are set correctly and that the certificate’s start and expiration date are valid.

**Note** • For printers that do not have a battery to store the Real Time Clock (RTC) value, the date will be restored to the default value upon a power cycle. The default value depends upon how the rtc.date SGD is managed. If it has never been set then it will default to the firmware build date (the value in appl.date). Otherwise, the value in rtc.date will default to the value that it was last set to. This does not mean the value of the rtc.date when it was power cycled. It means that when a user sets rtc.date that becomes the new default value.

If the printer has a battery then the rtc.date is never default and continues to track the date as expected.

"subjectAltName does not match 1.2.3.4" | Part of the certificate validation process involves making sure that the remote server is who it claims to be. A certificate can be created to validate against several aliases/DNS names. Typically the certificate will not contain the IP address of the server as IP addresses are subject to change. When specifying the remote server’s URL via weblink.ip.conn1.location be sure to specify one of the DNS aliases listed in the certificate. The valid names will be listed either under the Common Name (CN) field and/or the subjectAltName (SAN or Subject Alternate Name) field within the certificate. For example, the certificate may have the CN set to 'examplecorpinc' and the SAN set to 'examplecorpinc.com' or 'alias.for.examplecorpinc.com'. Any of the CN or SAN names can be used, but, as the IP address is not listed in the CN or SAN it cannot. It is not recommended that the IP address be part of the SAN if a DNS name is available to avoid connection issues that may arise due to subnet change or DHCP lease expirations, etc.

"SSL certificate subject name 'examplecorpinc.com' does not match target host name '1.2.3.4'" | When this message is seen it means that the remote server’s SSL/TLS configuration is incorrect. Refer to Troubleshooting on page 53 to ensure the server and printer are both configured correctly.

"Unknown SSL protocol error in connection to ..." | I do not see any of these errors, but the printer still does not connect. Refer to Troubleshooting on page 53 to ensure the server and printer are both configured correctly.
Other Typical Errors

While SSL/TLS connection errors are the most common, there are issues that can arise that prevent a successful connection. This section highlights the most common issues.

<table>
<thead>
<tr>
<th>Error</th>
<th>Cause / Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>&quot;Read failed with an unexpected error&quot;</td>
<td>This message typically indicates that connection to the remote server was lost. The connection can either be lost due to the server powering off or resetting, the firewall or proxy server shutting down the connection, or because the remote server gracefully requests that the connection be discontinued. <strong>Note</strong> • After 60 seconds of inactivity on the connection the printer will attempt to contact the server via a TCP Keepalive. If the connection is still present the server will respond and the connection will remain open. After 10 successive failed attempts to contact the remote the printer will assume the connection is severed and close the connection. The printer will resume it's attempt to connect to the remote server so that when the server comes back online the printer will re-establish communication.</td>
</tr>
<tr>
<td>&quot;Failed to connect (SP = #, CI = #, UW = #, AC = #, PC = #)&quot;</td>
<td>If this error is seen one or more of the ‘#’ values will be set to 0. This is an indication of an incorrect configuration of the remote server. Ensure that the remote server is setup according to the Servlet configuration in the Zebra Link-OS SDK documentation. This typically indicates an incorrect version of the remote Application Server (for example, Apache/Tomcat version may be incorrect). If this issue persists contact Zebra Technical Support.</td>
</tr>
</tbody>
</table>
Troubleshooting

Whenever troubleshooting a connection issue, the following questions should be answered to ensure the configuration is correct.

1. Is the printer connected correctly via Wireless or Ethernet?

2. Does the printer have a valid IP address?

3. Can I ping the printer’s IP address from a device on the same network as the printer?

4. Is the remote server URL in `weblink.ip.conn1.location` correct and does it point to the remote server that is configured for weblink functionality?

5. Can you connect to the location defined in the `weblink.ip.conn1.location` setting via a browser?

6. Is the remote server I am attempting to connect to outside the corporate firewall?

7. Can the URL specified in `weblink.ip.conn1.test.location` be accessed?
   If this is the case, talk with your administrator about altering restrictions for accessing HTTPS connections.

8. Does the firewall require a username and password to access the remote server?

9. Do I require a proxy server to access the remote server?

10. Is the proxy server port the default (1080) or another port (for example, 3128 for the Linux Squid proxy)?

   **Note** • If using the Linux Proxy Server Squid, and you are having trouble connecting, note that it may be configured to:
   a. disallow POST messages
   b. only operate in HTTP/1.0 mode
   c. disallow SSL connections.
   Refer to your Linux Squid documentation for complete details.

11. Does the firewall permit HTTPS connections initially or do I need to connect via HTTP first?

12. Is the remote server configured to use SSL v3.0 or TLS 1.0?
   TLS1.0 is recommended, but SSL v3.0 is also supported. Versions prior to SSL v3.0 and later than TLS v1.0 are not currently supported.

13. Are the Zebra Certificate Authority Certificates correctly installed on the remote server?

14. Was the server’s certificate issued by Zebra and is it signed by the Zebra Certificate Authority?

15. Has the server’s certificate expired?

16. Is the printer’s date and time within the issue and expired period of the server’s certificate?
17. Does the value in `weblink.ip.conn1.location` match either the Common Name or one of the names listed in the Subject Alternate Name of the remote server’s certificate?

18. Is the proxy server configured correctly and does the respective proxy server allow HTTPS connections via the HTTP CONNECT method?

19. Are there any HTTP authentication attempts when trying to connect that fail?

20. Are there any HTTP/1.1 4xx messages in the log?

If your connection issues persist and the solutions in this document do not help, contact Zebra Tech Support and provide the output of the following command. Ensure that logging is enabled and that the error(s) appear within the entries:

```bash
! U1 getvar "weblink"
```

## HTTP Messages

<table>
<thead>
<tr>
<th>Message</th>
<th>Cause / Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP/1.1 100 Continue</td>
<td>This indicates that the server and printer have begun communicating and is often seen in place of HTTP/1.1 200 OK.</td>
</tr>
<tr>
<td>HTTP/1.1 101 Switching Protocols</td>
<td>This indicates that the basic connection to the server worked and the protocol is being switched to a more efficient protocol for data transfer.</td>
</tr>
<tr>
<td>HTTP/1.1 200 OK</td>
<td>This indicates that an HTTP GET or HTTP POST was successful.</td>
</tr>
<tr>
<td>HTTP/1.1 30x Moved/Redirect/etc</td>
<td>This indicates that the URL specified has moved or that the firewall redirected the printer to another location (typically this is done to authenticate a user in a transparent proxy configuration).</td>
</tr>
<tr>
<td>HTTP/1.1 401 Unauthorized</td>
<td>This indicates that the printer either needs to authenticate with the server or failed to authenticate with the remote server (or server/router along the route to the server).</td>
</tr>
<tr>
<td>HTTP/1.1 403 Forbidden</td>
<td>This typically means that the authentication was provided and valid; however, the user does not have access to the requested resource.</td>
</tr>
<tr>
<td>HTTP/1.1 404 Not Found</td>
<td>This indicates that the remote URL provided points to an invalid location on the server. This does indicate, however, that the server name is valid. Just the path after the domain name is invalid.</td>
</tr>
</tbody>
</table>
WebLink Set/Get/Do Commands

This section describes the Set/Get/Do commands, parameters, and values that are available with Zebra AirWatch Connector.

Contents

Introduction to SGD Commands ................................................................. 56
weblink.enable ...................................................................................... 57
weblink.ip.conn[1|2].authentication.add ................................................. 58
weblink.ip.conn[1|2].authentication.entries ......................................... 60
weblink.ip.conn[1|2].authentication.remove ......................................... 61
weblink.ip.conn[1|2].enable ................................................................. 62
weblink.ip.conn[1|2].location ................................................................. 63
weblink.ip.conn[1|2].maximum_simultaneous_connections ..................... 64
weblink.ip.conn[1|2].proxy ................................................................. 65
weblink.ip.conn[1|2].retry_interval ..................................................... 67
weblink.ip.conn[1|2].test.location ....................................................... 68
weblink.ip.conn[1|2].test.retry_interval .............................................. 70
weblink.logging.clear ................................................................. 71
weblink.logging.entries ................................................................. 73
weblink.logging.max_entries ............................................................ 74
weblink.printer_reset_required ........................................................... 75
weblink.restore_defaults ................................................................. 77
Introduction to SGD Commands

For more specific information about SGD syntax and structure, see the Zebra Programming Guide section on Set/Get/Do Command Structure.

To send SGD commands to a printer, use the Zebra Setup Utilities.
**weblink.enable**

**Description**  This command indicates if one or more of the weblink connections are active.

If there is more than one connection under the weblink branch (for example, `weblink.ip.conn1`) and if any of the `.location` values are set, then this SGD will be set to "on". If all connections are disabled (all connection `.location` values set to ""), then this value will be set to "off".

`^JUF, ^JUS, ^JUN, ^JUA` and `device.restore_defaults` do not have any affect on this setting.

- iMZ 220™, iMZ 320™
- QLn220™, QLn320™, QLn420™
- ZT210™, ZT220™, ZT230™

**Type**  `getvar`

<table>
<thead>
<tr>
<th>Commands</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>getvar</strong></td>
<td>This command indicates if one or more of the weblink connections are active.</td>
</tr>
<tr>
<td><strong>Format:</strong></td>
<td><code>! U1 getvar &quot;weblink.enable&quot;</code></td>
</tr>
</tbody>
</table>
| **Result:** | • "yes" if any of the `.location` values are set  
• "off" if all connections are disabled |
**weblink.ip.conn[1|2].authentication.add**

**Description**  This command allows the user to add a single server/username/password triplet into the list of authentication entries.

When the printer attempts to connect to the server (url specified in `weblink.ip.conn[1|2].location`) the server may require HTTP authentication (e.g. digest, basic, DNS, etc.). There may be multiple authentication requests along the route to the destination (e.g. a local server first requires HTTP authentication as well as on the remote server).

For each HTTP authentication request received while attempting to connect, the printer will enumerate the authentication entries and attempt to satisfy the request with the username/password pair provided for the respective server. The server name in the entry is what determines which username/password pair should be used for which authentication request. Both DNS names and IP addresses are acceptable. The server, username, and password are separated by a single space (not a tab or other white space character). The server name is the only required field. If no username is supplied, but a password is, there must be two spaces between the server and the password fields. If there is a username but no password, or simply just the servername, no space is required at the end of the entry.

If the command is changed when the connection is enabled (`weblink.enable` is set to "on"), it will not take effect until the connection is disabled, and then re-enabled.

**Important**  • This setting only be changed when `weblink.enable` is set to "off".

^JUF, ^JUS, ^JUN, ^JUA, and `device.restore_defaults` do not have any affect on this setting.

**Supported Devices**

- iMZ 220™, iMZ 320™
- QLn220™, QLn320™, QLn420™
- ZT210™, ZT220™, ZT230™

**Type**  `setvar`
Commands| Details
---|---
setvar| This command adds a single server/username/password triplet to the list of authentication entries.

Format:
- ! U1 setvar "weblink.ip.conn1.authentication.add" "servername[ username][ password]"
- ! U1 setvar "weblink.ip.conn2.authentication.add" "servername[ username][ password]"

Values: servername [username][ password] has a maximum length of string is 2048 characters

Default: NA

Example 1 • In this example, a username and a password is supplied:

    ! U1 setvar "weblink.ip.conn1.authentication.add" "my.server.lan johndoe password"

Example 2 • In this example, no password is supplied

    ! U1 setvar "weblink.ip.conn1.authentication.add" "my.server.lan johndoe"

Example 3 • In this example, no username is supplied (note the double space)

    ! U1 setvar "weblink.ip.conn1.authentication.add" "my.server.lan password"

Example 4 • In this example, no username or password is supplied

    ! U1 setvar "weblink.ip.conn1.authentication.add" "my.server.lan"
weblink.ip.conn[1|2].authentication.entries

**Description**  This command lists the server names added to the authentication entries list. Only the server names will be shown. The username and passwords will not be shown. The server names are separated by a `\r\n` so that each shows up on its own line.

`^JUF`, `^JUS`, `^JUN`, `^JUA`, and `device.restore_defaults` do not have any affect on this setting.

**Supported Devices**
- iMZ 220™, iMZ 320™
- QLn220™, QLn320™, QLn420™
- ZT210™, ZT220™, ZT230™

**Type**  getvar

<table>
<thead>
<tr>
<th>Commands</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>getvar</td>
<td>This command lists the server names for the specified connection.</td>
</tr>
</tbody>
</table>

*Format:*
- `! U1 getvar "weblink.ip.conn1.authentication.entries"`
- `! U1 getvar "weblink.ip.conn2.authentication.entries"`
**weblink.ip.conn[1|2].authentication.remove**

**Description**  This command allows the user to remove a single server/username/password triplet from the list of authentication entries.

To remove an entry only the server name is supplied. If an invalid entry is supplied no action is taken. If the SGD is changed when the connection is enabled (weblink.ip.conn[1|2].enable), it will not take effect until the connection is disabled, and then re-enabled. It is therefore recommended that this setting only be changed when weblink.ip.conn[1|2].enable is set to "off".

^JUF, ^JUS, ^JUN, ^JUA, and device.restore_defaults do not have any affect on this setting.

**Supported Devices**

- iMZ 220™, iMZ 320™
- QLn220™, QLn320™, QLn420™
- ZT210™, ZT220™, ZT230™

**Type**  setvar

<table>
<thead>
<tr>
<th>Commands</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>setvar</strong></td>
<td>This command removes a single server/username/password triplet from the list of authenticaiton entries.</td>
</tr>
</tbody>
</table>

* Format:
  - ! U1 setvar "weblink.ip.conn1.authentication.remove" "servername"
  - ! U1 setvar "weblink.ip.conn2.authentication.remove" "servername"

* Values: servername has a maximum length of string is 2048 characters.

* Default: NA

---

**Example**  • In this example, a username and a password is supplied

    ! U1 setvar "weblink.ip.conn1.authentication.remove" "my.server.lan"
**weblink.ip.conn[1|2].enable**

**Description**  This command enables or disables the weblink IP connection #1.

A side effect of setting this SGD to "on", the *weblink.enable* will also be set to "on". When this setting is set to "off", if the *weblink.ip.conn2.enable* is also "off", the *weblink.enable* will be set to "off".

**Supported Devices**

- iMZ 220™, iMZ 320™
- QLn220™, QLn320™, QLn420™
- ZT210™, ZT220™, ZT230™

**Type**  setvar, getvar

<table>
<thead>
<tr>
<th>Commands</th>
<th>Details</th>
</tr>
</thead>
</table>
| **setvar** | This command enables/disables the weblink IP connection.  
*Format:*  
- ! U1 setvar "weblink.ip.conn1.enable" "value"  
- ! U1 setvar "weblink.ip.conn2.enable" "value"  
*Values:* "on", "off"  
*Default:* "off" |
| **getvar** | This command retrieves the current setting.  
*Format:*  
- ! U1 setvar "weblink.ip.conn1.enable"  
- ! U1 setvar "weblink.ip.conn2.enable"  
*Result:*  
- "on" if the connection is enabled  
- "off" if the connection is disabled |
weblink.ip.conn[1|2].location

**Description**  This command assigns the URL of the server for this connection. The URL must follow the URL rules for the HTTP[S] protocol outlined in RFC2396 (http://www.ietf.org/rfc/rfc2396.txt).

The setting will not take effect until the printer is reset. Changing this setting will set weblink.printer_reset_required to "yes".

^JUF, ^JUS, ^JUN, ^JUA, and device.restore_defaults do not have any affect on this setting.

**Supported Devices**

• iMz™ series
• QLn™ series
• ZT200™ series
• ZD500R™ series

**Type**  setvar, getvar

<table>
<thead>
<tr>
<th>Commands</th>
<th>Details</th>
</tr>
</thead>
</table>
| **setvar** | This command sets the server URL for the specified connection.  
*Format:*  
- ! U1 setvar "weblink.ip.conn1.location" "value"  
- ! U1 setvar "weblink.ip.conn2.location" "value"  
*Values:* any HTTPS URL up to 2048 characters  
*Default:* "" |
| **getvar** | This command returns the server URL currently assigned to the connection.  
*Format:*  
- ! U1 getvar "weblink.ip.conn1.location"  
- ! U1 getvar "weblink.ip.conn2.location" |

**Example**

! U1 setvar "weblink.ip.conn2.location"  
"https://my.linkos.server.com:8080/link/os"
**weblink.ip.conn[1|2].maximum_simultaneous_connections**

**Description** This command indicates the maximum number of simultaneous connections that can be initiated by the printer.

Via the main connection (the original connection initiated by the printer to the remote server), the remote server can request that additional connections from the printer be initiated (e.g. a connection that supports only JSON SGDs, one that behaves similar to the RAW TCP port.

The server is free to request as many as it thinks it needs, but the printer will prevent more than N number of connections, where N is the value of this command.

'^JUF, ^JUS, ^JUN, ^JUA, and device.restore_defaults do not have any affect on this setting.

**Supported Devices**
- iMZ 220™, iMZ 320™
- QLn220™, QLn320™, QLn420™
- ZT210™, ZT220™, ZT230™

**Type** setvar, getvar

<table>
<thead>
<tr>
<th>Commands</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>setvar</strong></td>
<td>This command sets the maximum number of connections.</td>
</tr>
<tr>
<td><strong>Format:</strong></td>
<td></td>
</tr>
<tr>
<td>• ! U1 setvar &quot;weblink.ip.conn1.maximum_simultaneous_connections&quot; &quot;value&quot;</td>
<td></td>
</tr>
<tr>
<td>• ! U1 setvar &quot;weblink.ip.conn2.maximum_simultaneous_connections&quot; &quot;value&quot;</td>
<td></td>
</tr>
<tr>
<td><strong>Values:</strong> Any integer from 1-100</td>
<td></td>
</tr>
<tr>
<td><strong>Default:</strong> &quot;10&quot;</td>
<td></td>
</tr>
</tbody>
</table>

| **getvar** | This command retrieves the maximum set number of connections. |
| **Format:** | |
| • ! U1 getvar "weblink.ip.conn1.maximum_simultaneous_connections" | |
| • ! U1 getvar "weblink.ip.conn2.maximum_simultaneous_connections" | |

**Example** • This example sets the conn1 maximum connections to 3.

! U1 setvar "weblink.ip.conn1.maximum_simultaneous_connections" "3"
weblink.ip.conn[1|2].proxy

**Description**  This command assigns the URL of the proxy for the connection.

The proxy server protocol, port, domain, username, and password are all encoded into the URL via the format outlined in RFC2396 (http://www.ietf.org/rfc/rfc2396.txt).

The username and password must avoid the invalid characters listed in RFC2396 (e.g. ':', '@', '/', etc). If an invalid character must be used it needs to be escaped using '%' as described in RFC2396.

[^JUF, ^JUS, ^JUN, ^JUA, and device.restore_defaults do not have any affect on this setting.]

**Supported Devices**

- iMZ 220™, iMZ 320™
- QLn220™, QLn320™, QLn420™
- ZT210™, ZT220™, ZT230™

**Type**  setvar, getvar, do

<table>
<thead>
<tr>
<th>Commands</th>
<th>Details</th>
</tr>
</thead>
</table>
| setvar   | This command assigns the URL of the connection proxy.  
  **Format:**  
  - ! U1 setvar "weblink.ip.conn1.proxy" "url"  
  - ! U1 setvar "weblink.ip.conn2.proxy" "url"  
  **Values:**  
  - Any valid URL up to 2048 characters  
  - Expected URL format: [http|https]://[user:pass@]domain[:port]/[path]  
  - The URL will need to be built according to the server/proxy environment the printer is running within.  
  **Default:** ""  
  - The user:pass, port, and path are all optional.  
  - The default scheme must be either HTTPS or HTTP. The default is HTTP.  
  - The default port is 1080.  
  - The default is to omit the username and password. |
| getvar   | This command retrieves the URL of the connection proxy.  
  **Format:**  
  - ! U1 getvar "weblink.ip.conn1.proxy"  
  - ! U1 getvar "weblink.ip.conn2.proxy" |
<table>
<thead>
<tr>
<th>Commands</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>do</td>
<td>This command assigns the URL of the connection proxy.</td>
</tr>
</tbody>
</table>

*Format:*

- ! U1 do "weblink.ip.conn1.proxy" "url"
- ! U1 do "weblink.ip.conn2.proxy" "url"

*Values:*

- Any valid URL up to 2048 characters
- Expected URL format: [scheme://][user:pass@]domain[:port]/[path]
- The URL will need to be built according to the server/proxy environment the printer is running within.

*Default:* ""

- The scheme, user:pass, port, and path are all optional.
- The default scheme is http.
- The default port is 1080.
- The default is to omit the username and password.

---

**Example** • Examples of how to connect to various proxy servers:

http://username:password@mydomain.com:3128/
http://mydomain.com/
**weblink.ip.conn[1|2].retry_interval**

**Description**  
This command sets the number of seconds between attempts to connect to the server URL provided in `weblink.ip.conn1.location`. If an attempt is unsuccessful or the connection is lost, the printer will wait `retry_interval` seconds before attempting to connect again.

`^JUF`, `^JUS`, `^JUN`, `^JUA` and `device.restore_defaults` do not have any affect on this setting.

**Supported Devices**
- iMZ 220™, iMZ 320™
- QLn220™, QLn320™, QLn420™
- ZT210™, ZT220™, ZT230™

**Type**  
`setvar, getvar, do`

<table>
<thead>
<tr>
<th>Commands</th>
<th>Details</th>
</tr>
</thead>
</table>
| **setvar** | This command sets the number of seconds to wait before attempting to reconnect to the server.  
*Format:*  
- `! U1 setvar "weblink.ip.conn1.retry_interval" "value"`
- `! U1 setvar "weblink.ip.conn2.retry_interval" "value"

*Values:* 1 - 600  
*Default:* "10"

| **getvar** | This command returns the number of seconds to wait between connection attempts.  
*Format:*  
- `! U1 getvar "weblink.ip.conn1.retry_interval"
- `! U1 getvar "weblink.ip.conn2.retry_interval"

| **do** | This command sets the number of seconds to wait before attempting to reconnect to the server.  
*Format:*  
- `! U1 do "weblink.ip.conn1.retry_interval" "value"
- `! U1 do "weblink.ip.conn2.retry_interval" "value"

*Values:* 1 - 600  
*Default:* "10"
**weblink.ip.conn[1|2].test.location**

**Description**  This command holds the URL for testing a connection to the internet. This is meant to assist users in debugging their printer’s connection to remote servers when there are issues with the main weblink connection (conn1 or conn2).

The URL must follow the URL rules for the HTTP[S] protocol outlined in RFC2396 ([http://www.ietf.org/rfc/rfc2396.txt](http://www.ietf.org/rfc/rfc2396.txt)).

`^JUF`, `^JUS`, `^JUN`, `^JUA`, and `device.restore_defaults` do not have any affect on this setting.

**Supported Devices**
- iMZ 220™, iMZ 320™
- QLn220™, QLn320™, QLn420™
- ZT210™, ZT220™, ZT230™

**Type**  setvar, getvar, do

<table>
<thead>
<tr>
<th>Commands</th>
<th>Details</th>
</tr>
</thead>
</table>
| **setvar** | This command sets the URL to hold for testing a connection.  
*Format:*  
- ! U1 setvar "weblink.ip.conn1.test.location" "url"  
- ! U1 setvar "weblink.ip.conn2.test.location" "url"  
*Values:* Any HTTPS URL up to 2048 characters  
*Default:* "http://www.zebra.com/apps/linktest" |
| **getvar** | This command retrieves the printer's test connection URL.  
*Format:*  
- ! U1 getvar "weblink.ip.conn1.test.location"  
- ! U1 getvar "weblink.ip.conn2.test.location" |
| **do** | This command sets the URL to hold for testing a connection.  
*Format:*  
- ! U1 do "weblink.ip.conn1.test.location" "url"  
- ! U1 do "weblink.ip.conn2.test.location" "url"  
*Values:* Any HTTPS URL up to 2048 characters  
*Default:* "http://www.zebra.com/apps/linktest" |
Example • The test connection can assist the user in several ways/scenarios:

1. If the `test.test_on` value is set to "failure", any time the main weblink (`conn[1|2].location`) connection fails to connect then the `test.location` URL will be used. In this situation, an attempt will be made to contact the remote URL in `test.location`, using authentication and proxy configuration that is specified by the main connection.

2. If the `test.test_on` value is set to "interval" an attempt will be made to contact the remote URL in `test.location` every `test.retry_interval` seconds, using authentication and proxy configuration that is specified by the main connection.

3. If the `test.test_on` value is set to "both", then scenario 1 and 2 will both occur. This is useful for users who will use an HTTP connection to move through their firewall - and thereafter frequently refresh the connection to indicate to their firewall that there is still activity for the purpose of keeping the connection alive.
**weblink.ip.conn[1|2].test.retry_interval**

**Description**  This command determines how often, in seconds, a connection to the test.location URL should be attempted. This setting is only applicable when the test.test_on SGD is set to "interval" or "both".

^JUF, ^JUS, ^JUN, ^JUA, and device.restore_defaults do not have any affect on this setting.

**Supported Devices**
- iMZ 220™, iMZ 320™
- QLn220™, QLn320™, QLn420™
- ZT210™, ZT220™, ZT230™

**Type**  setvar, getvar, do

<table>
<thead>
<tr>
<th>Commands</th>
<th>Details</th>
</tr>
</thead>
</table>
| **setvar** | This command sets the interval for how often a connection to the test.location URL should be attempted.  
*Format:*  
- ! U1 setvar "weblink.ip.conn1.test.retry_interval" "value"  
- ! U1 setvar "weblink.ip.conn2.test.retry_interval" "value"  
*Values:* 0-1800 (in seconds, providing 0 second - 30 minute interval)  
*Default:* "900" |
| **getvar** | This command retrieves the retry interval.  
*Format:*  
- ! U1 getvar "weblink.ip.conn1.test.retry_interval"  
- ! U1 getvar "weblink.ip.conn2.test.retry_interval" |
| **do** | This command sets the interval for how often a connection to the test.location URL should be attempted.  
*Format:*  
- ! U1 do "weblink.ip.conn1.test.retry_interval" "value"  
- ! U1 do "weblink.ip.conn2.test.retry_interval" "value"  
*Values:* 0-1800  
*Default:* "900" |
weblink.ip.conn[1|2].test.test_on

Description  This command determines when the test connection should be attempted. This assists in debugging the printer's connection to remote servers when there are issues with the main weblink connection (conn1 or conn2).

^JUF, ^JUS, ^JUN, ^JUA, and device.restore_defaults do not have any affect on this setting.

Supported Devices
- iMZ 220™, iMZ 320™
- QLn220™, QLn320™, QLn420™
- ZT210™, ZT220™, ZT230™

Type  setvar, getvar, do

<table>
<thead>
<tr>
<th>Commands</th>
<th>Details</th>
</tr>
</thead>
</table>
| setvar   | This command indicates when the test connection should be attempted.  
  Format:  
  • ! U1 setvar "weblink.ip.conn1.test.test_on" "value"  
  • ! U1 setvar "weblink.ip.conn2.test.test_on" "value"  
  Values: off, failure, interval, both  
  Default: "failure" |
| getvar   | This command retrieves the test connection setting.  
  Format:  
  • ! U1 getvar "weblink.ip.conn1.test.test_on"  
  • ! U1 getvar "weblink.ip.conn2.test.test_on" |
| do       | This command sets when the test connection should be attempted.  
  Format:  
  • ! U1 do "weblink.ip.conn1.test.test_on" "value"  
  • ! U1 do "weblink.ip.conn2.test.test_on" "value"  
  Values: off, failure, interval, both  
  Default: "failure" |
Example • The test connection can assist the user in several ways/scenarios:

1. If the `test.test_on` value is set to "failure", any time the main weblink (`conn[1|2].location`) connection fails to connect then the `test.location` URL will be used. An attempt will be made to contact the remote URL in `test.location`, using authentication and proxy configuration that is specified by the main connection.

2. If the `test.test_on` value is set to "interval" an attempt will be made to contact the remote URL in `test.location` every `test.retry_interval` seconds, using authentication and proxy configuration that is specified by the main connection.

3. If the `test.test_on` value is set to "both", then scenario 1 and 2 will both occur. This is useful for users who will use an HTTP connection to move through their firewall - and thereafter frequently refresh the connection to indicate to their firewall that there is still activity for the purpose of keeping the connection alive.
**weblink.logging.clear**

**Description**  This command clears the weblink log. Setting this value to anything will clear it, including an empty string.

\(^{\text{JUF}},^{\text{JUS}},^{\text{JUN}},^{\text{JUA}},\text{ and device.restore_defaults} \) do not have any affect on this setting.

**Supported Devices**

- iMZ 220™, iMZ 320™
- QLn220™, QLn320™, QLn420™
- ZT210™, ZT220™, ZT230™

**Type**  setvar, do

<table>
<thead>
<tr>
<th>Commands</th>
<th>Details</th>
</tr>
</thead>
</table>
| setvar   | This command clears the weblink log entries.  
  *Format: \(! \ U1 \ \text{setvar} \ \"weblink.logging.clear\" \ \"value"\)*  
  *Values: Any string value, including an empty string.*  
  *Default: NA* |

| do       | This command clears the weblink log entries.  
  *Format: \(! \ U1 \ \text{do} \ \"weblink.logging.clear\" \ \"value\"\)*  
  *Values: Any string value, including an empty string.*  
  *Default: NA* |

**Example**  • This example clears the weblink log entries with an empty string value.  
  \(! \ U1 \ \text{setvar} \ \"weblink.logging.clear\" \ \"\"\)
weblink.logging.entries

**Description**  This command returns the N number of entries in the weblink log, where N has a maximum value that is set by *weblink.logging.max_entries*.

The weblink log is a collection of events related to connecting to a remote Link-OS™ server. The log entries range anywhere from general status to errors that prevented a successful connection. The log contains entries from all connections and are labeled so that it is clear which log entries are for which connection. Each log entry also contains a timestamp for when it was logged by the system. The newest events will appear at the bottom of the list.

^JUF, ^JUS, ^JUN, ^JUA, and *device.restore_defaults* do not have any affect on this setting.

**Supported Devices**
- iMZ 220™, iMZ 320™
- QLn220™, QLn320™, QLn420™
- ZT210™, ZT220™, ZT230™

**Type**  getvar

<table>
<thead>
<tr>
<th>Commands</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>getvar</td>
<td>This command returns a lists of entries in the weblink log.</td>
</tr>
</tbody>
</table>

*Format:*  \(! U1 getvar "weblink.logging.entries"*

*Values:*  NA

*Default:*  ""

**Example**  • This example shows the result from *weblink.logging.entries*:

```
[01-04-2013 08:40:45.655] [conn1.1] HTTP/1.1 404 Not Found
[01-04-2013 08:40:45.659] [conn1.1] Received HTTP code 404 from proxy after CONNECT
[01-04-2013 08:40:45.660] [conn1.1] Closing connection
[01-04-2013 08:40:45.662] [conn1.1] Failed to connect (SP = 0, CU = 0, UW = 0, AC = 0, PC = 0)
```
weblink.logging.max_entries

Description  This command specifies the maximum number of individual log entries that will be stored in the weblink.logging.entries command.

Important  Changes to this command are immediate and may result in some log entries being lost. If there are N log entries currently in the log, the user sets the max_entires to M, where M is less than N, the oldest (N-M) log entries will be removed.

^JUF, ^JUS, ^JUN, ^JUA, and device.restore_defaults do not have any affect on this setting.

Supported Devices

• iMZ 220™, iMZ 320™
• QLn220™, QLn320™, QLn420™
• ZT210™, ZT220™, ZT230™

Type  setvar, getvar, do

<table>
<thead>
<tr>
<th>Commands</th>
<th>Details</th>
</tr>
</thead>
</table>
| setvar   | This command sets the maximum number of log entries that will be stored.  
Format:  ! U1 setvar "weblink.logging.max_entries" "value"  
Values: 0 - 10000  
Note • Setting the value to 0 disables logging.  
Default: "0" |
| getvar   | This command returns the setting for the maximum number of log entries that will be stored.  
Format:  ! U1 getvar "weblink.logging.max_entries" |
| do       | This command sets the maximum number of log entries that will be stored.  
Format:  ! U1 do "weblink.logging.max_entries" "value"  
Values: 0 - 10000  
Note • Setting the value to 0 disables logging.  
Default: "0" |
Example 1 • In this example, `weblink.logging.max_entries` is set to 3:

[01-04-2013 08:40:45.659] [conn1.1] Received HTTP code 404 from proxy after CONNECT
[01-04-2013 08:40:45.660] [conn1.1] Closing connection
[01-04-2013 08:40:45.662] [conn1.1] Failed to connect (SP = 0, CU = 0, UW = 0, AC = 0, PC = 0)

Example 2 • In this example, `weblink.logging.max_entries` is set to 2:
weblink.logging.entries becomes:

[01-04-2013 08:40:45.660] [conn1.1] Closing connection
[01-04-2013 08:40:45.662] [conn1.1] Failed to connect (SP = 0, CU = 0, UW = 0, AC = 0, PC = 0)
weblink.printer_reset_required

**Description**  This command retrieves a "yes" or "no" value indicating whether any of the weblink settings have been modified.

^JUF, ^JUS, ^JUN, ^JUA, and device.restore_defaults do not have any affect on this setting.

**Supported Devices**

- iMZ 220™, iMZ 320™
- QLn220™, QLn320™, QLn420™
- ZT210™, ZT220™, ZT230™

**Type**  getvar

<table>
<thead>
<tr>
<th>Commands</th>
<th>Details</th>
</tr>
</thead>
</table>
| getvar   | This command retrieves whether any of the weblink settings are modified.  
**Format:**  ! U1 getvar "weblink.printer_reset_required"
**Values:**  "yes" or "no"
**Default:**  "no" |
weblink.restore_defaults

**Description**  This command defaults, and saves, the weblink branch settings. Any value, including an empty string, will default the weblink branch settings.

**Note** • The entire weblink branch of settings will be defaulted and the settings are saved; however, the weblink connections will not use the new settings until the printer is restarted (e.g. the weblink.printer_reset_required SGD will be “yes” after a default).

^JUF, ^JUS, ^JUN, ^JUA, and device.restore_defaults do not have any affect on this setting.

**Supported Devices**

- iMZ 220™, iMZ 320™
- QLn220™, QLn320™, QLn420™
- ZT210™, ZT220™, ZT230™

**Type**  setvar, do

---

### Commands

<table>
<thead>
<tr>
<th>Commands</th>
<th>Details</th>
</tr>
</thead>
</table>
| setvar   | This command defaults the weblink branch settings.  

**Format:**  ! U1 setvar "weblink.restore_defaults" "value"  

**Values:**  Any value, including an empty string, will default the branch  

**Default:**  NA  
| do       | This command defaults the weblink branch settings.  

**Format:**  ! U1 do "weblink.restore_defaults" "value"  

**Values:**  Any value, including an empty string, will default the branch  

**Default:**  NA  

---

**Example** • These all default the branch:

```
! U1 setvar "weblink.restore_defaults" ""
! U1 setvar "weblink.restore_defaults" "foo"
! U1 do "weblink.restore_defaults" ""
! U1 do "weblink.restore_defaults" "foo"
```