

# AirWatch Connector



**ZEBRA**

## User Guide

2023/11/17

ZEBRA and the stylized Zebra head are trademarks of Zebra Technologies Corporation, registered in many jurisdictions worldwide. All other trademarks are the property of their respective owners. ©2023 Zebra Technologies Corporation and/or its affiliates. All rights reserved.

Information in this document is subject to change without notice. The software described in this document is furnished under a license agreement or nondisclosure agreement. The software may be used or copied only in accordance with the terms of those agreements.

For further information regarding legal and proprietary statements, please go to:

SOFTWARE: [zebra.com/linkoslegal](https://zebra.com/linkoslegal).

COPYRIGHTS: [zebra.com/copyright](https://zebra.com/copyright).

PATENTS: [ip.zebra.com](https://ip.zebra.com).

WARRANTY: [zebra.com/warranty](https://zebra.com/warranty).

END USER LICENSE AGREEMENT: [zebra.com/eula](https://zebra.com/eula).

## 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 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.

# Contents

<b>Introduction.....</b>	<b>5</b>
Supported Printers.....	5
SGD Commands.....	5
Sequence Diagram.....	6
 <b>Installation on Windows.....</b>	 <b>7</b>
Operating System Requirements.....	7
Server Requirements.....	7
Printer Requirements.....	7
Certificate Requirements.....	7
SSL/TLS Certificates.....	8
Pre-Installation Tasks.....	8
Installation Procedure.....	9
Step 1: Configure Your AirWatch Server.....	9
Step 2: Installing the Zebra AirWatch Connector.....	10
Step 3: Set Up Printers.....	13
Step 4: Test a Printer.....	14
Receiving Alerts from a Printer.....	15
 <b>Configuring Printers with WebLink.....</b>	 <b>17</b>
Basic Configuration.....	17
Configuring the Printer to Connect to a Remote Server.....	17
When a Proxy Server is Part of the Network Configuration.....	18
When HTTP Authentication is Necessary.....	18
Additional Firewall Configuration.....	19

Difference Between Conn1 and Conn2.....	19
Enable Logging.....	19
Navigating the Log Output.....	20
<b>Troubleshooting.....</b>	<b>21</b>
Installation.....	21
AirWatch.....	22
SSL/TLS Certificate Errors.....	22
Other Typical Errors.....	25
Troubleshooting Sequence.....	25
HTTP Messages.....	26
<b>Printer Configuration.....</b>	<b>28</b>
Printer Configuration File.....	28
Multi-Part Form Format.....	28
Configuration File Example.....	28
Revision History.....	30

# Introduction

The Zebra AirWatch Connector partners with the AirWatch (Workspace ONE) server to manage your Zebra Print DNA™ 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

## Supported Printers

Wired and wireless Zebra Print DNA printers running Link-OS™ 5 or later.



**NOTE:** Printers running the Link-OS™ Basic operating system are not supported.

Visit [zebra.com/linkos](https://zebra.com/linkos) for details about the latest version of Link-OS™ for your printers.

## SGD Commands

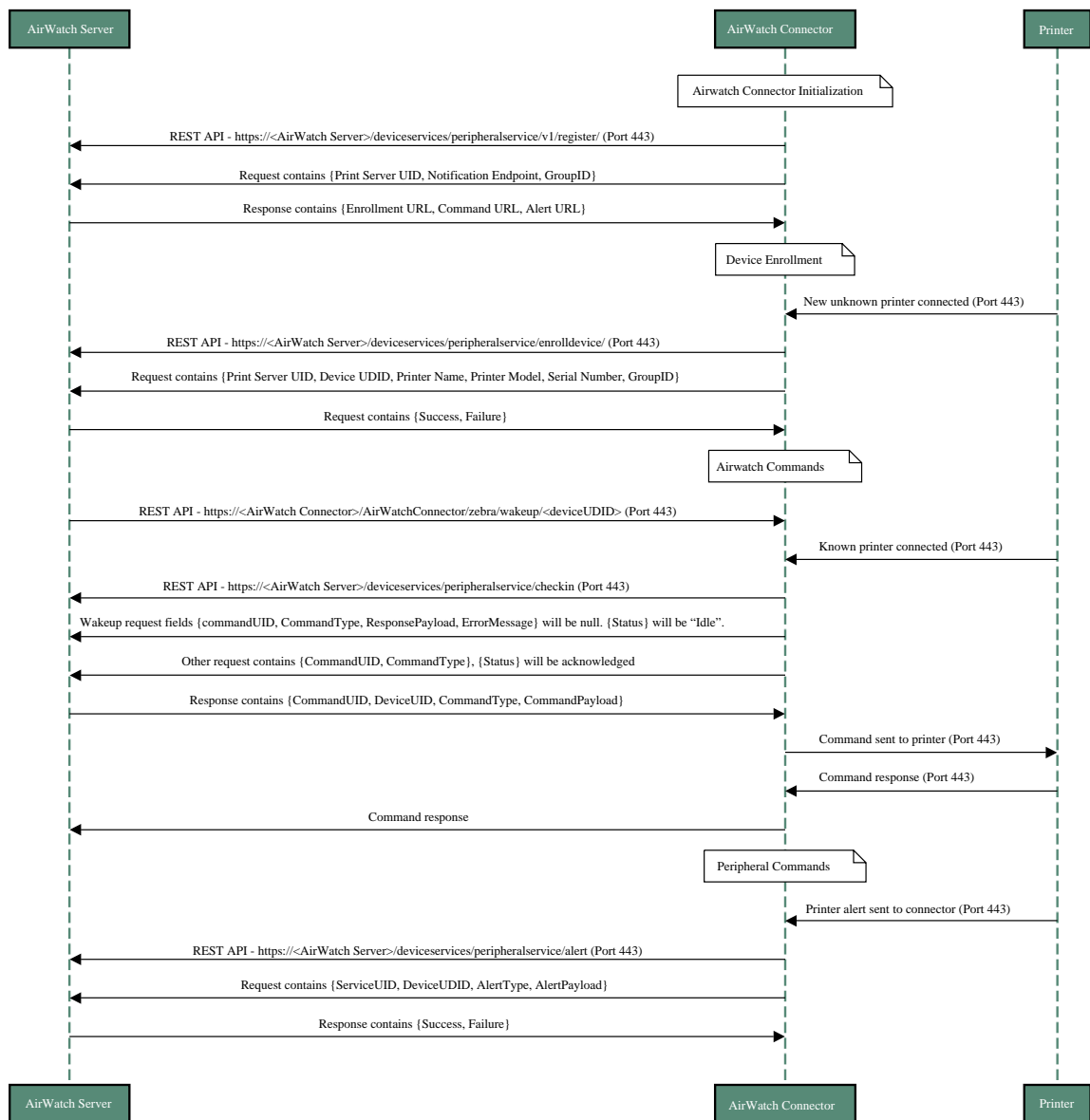
For information about Set/Get/Do commands, parameters, and values that are used by the Zebra AirWatch Connector, see the Zebra Programming Guide.

To send SGD commands to a printer, go to [Zebra Setup Utilities](#).

## Sequence Diagram

The following sequence diagram provides a dynamic view of the interactions and flow-of-control messages between different components within the AirWatch system, and it will help you understand the system's behavior.

**Figure 1** Sequence Diagram



# Installation on Windows

This section describes installing the connector on a Windows operating system.

## Operating System Requirements

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

- Windows Server 2019
- Windows Server 2022

## Server Requirements

- CPU cores: 8
- Memory (RAM): 16GB
- Minimum: 50GB available drive space



### NOTE:

Using the above server specifications and outside of the AirWatch (Workspace ONE) environment, Zebra has validated the AirWatch Connector with 10,000 printers connected.

Performance may be degraded when the quantity of printers used approaches that number due to variables related to, but not limited to, the Windows Server, the network environment, the AirWatch (Workspace ONE) software and printer management actions performed from within AirWatch (Workspace ONE). If necessary, multiple AirWatch Connector servers can be used.

## Printer Requirements

- Print DNA printers running Link-OS version 5 and later.
- Printers with an Emulation (previously known as Virtual Device) enabled are not supported by the Zebra AirWatch Connector.

## Certificate Requirements

A certificate for the Zebra AirWatch Connector server, obtained from a **publicly trusted Certificate Authority** such as DigiCert, is required. For further clarity, a certificate from a customer's internal Certificate Authority should not be used as it is not publicly trusted. Customers are responsible for tracking any server certificate expiration dates and the renewal and replacement of the certificates.

**NOTE:**

Check the [zebra.com](http://zebra.com) support page for the latest system requirements information.

**NOTE:**

The Zebra AirWatch Connector 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.

## SSL/TLS Certificates

An SSL/TLS certificate for the Zebra AirWatch Connector server is required during the installation of the Zebra AirWatch Connector. The certificate and private key need to be in PKCS#12 format. **Organizations need to provide this certificate by obtaining one from a publicly trusted Certificate Authority such as DigiCert. This should be obtained prior to performing the Zebra AirWatch Connector installation. The root certificate from the Certificate Authority is also required to be deployed to each printer.**

The common name used in the certificate must be the Fully Qualified Domain Name (FQDN) of the Zebra AirWatch Connector server.

Organizations should take note of the server certificate expiration date and are responsible for the renewal and replacement of the certificate on the Zebra AirWatch Connector server. This can be done by performing the task below to create a new .p12 file and, if necessary, update the KeystorePass parameter in the server.xml file.

## Pre-Installation Tasks

The administrator performing the Zebra AirWatch Connector installation should perform the following tasks before installation.

**1. Prepare the server certificate file.**

- a) Create a PKCS#12 format (.pfx/.p12) file containing the certificate chain and private key. The installer requires this and its password during installation.

The following OpenSSL command can be used to create a .p12 file.

```
openssl.exe pkcs12 -export -in "path\to\server-certificate.pem" -inkey  
"path\to\private-key.key" -out "path\to\server\pkcs12.p12" -certfile  
"path\to\ca-root.pem" -name airwatchconnector
```

**2. Prepare the printer certificate file.**

- a) Create a file containing the root certificate from the Certificate Authority that can be deployed to the printer. This file can also contain the configuration settings required for the printer to connect to the Zebra AirWatch Connector. Go to [Printer Configuration](#) for details.



## Installation Procedure

The following steps describe the installation of AirWatch Connector.

### Step 1: Configure Your AirWatch Server

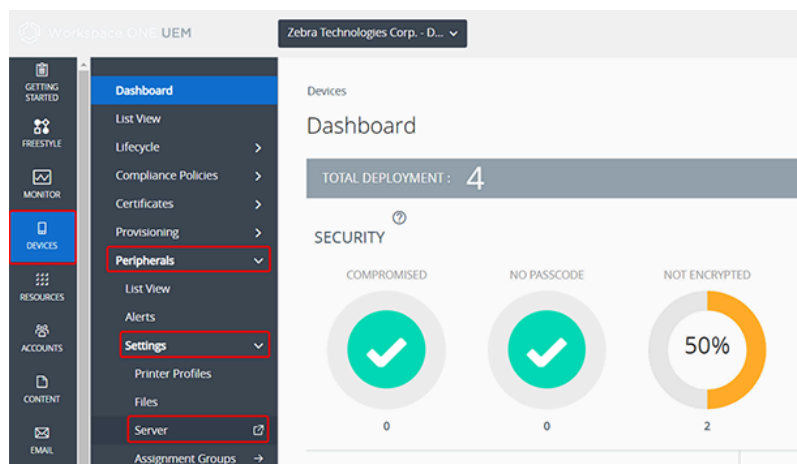
The following installation steps assume you already have an AirWatch server.

1. Setup a peripheral server in AirWatch (Workspace ONE) and obtain the following information needed during the Zebra AirWatch Connector installation.

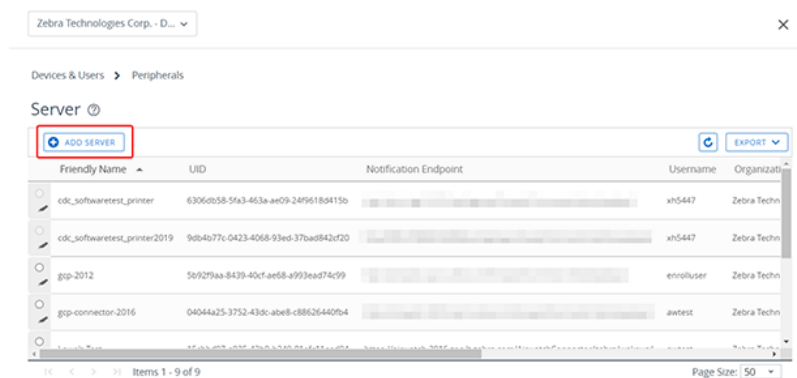
- Zebra Wakeup Location
- AirWatch Group ID
- AirWatch Server Location
- AirWatch Token
- Unique ID for Zebra Server

2. Log into AirWatch.

**Devices > Peripherals > Settings > Server**



3. Click **Add Server**.



4. Fill in your **Friendly Name**.

5. Select your **User ID**.

### 6. Generate a **Service UID**.

The screenshot shows the 'Add Server' dialog box. It has a title bar with a close button. The form includes the following elements:

- Friendly Name**: A text input field with a red asterisk indicating it is required.
- HMAC Token**: A text input field.
- HMAC Token**: A blue informational box stating: "The HMAC key auto-generated below will be used to associate the server to the appropriate Organization Group in AirWatch. This key will need to be entered into the relevant Server configuration file." Below this is a grey box containing the token: `2f399a3e-828e-4d41-a9b8-6379f97977c`.
- User**: A text input field.
- User**: A blue informational box stating: "Select the appropriate enrollment user that will be associated to the Server. This user may be associated to multiple Servers." Below this is a text input field with the placeholder 'User' and a search icon.
- UID**: A text input field.
- UID**: A blue informational box stating: "Selected Service UID is used to associate the server to AirWatch. This key can be copied from the server or generated by clicking the Generate UID button and then copying and pasting it to the Server." Below this is a text input field and a 'GENERATE UID' button.
- Service UID**: A text input field with a red asterisk.
- Buttons**: 'SAVE' and 'CANCEL' buttons at the bottom right.

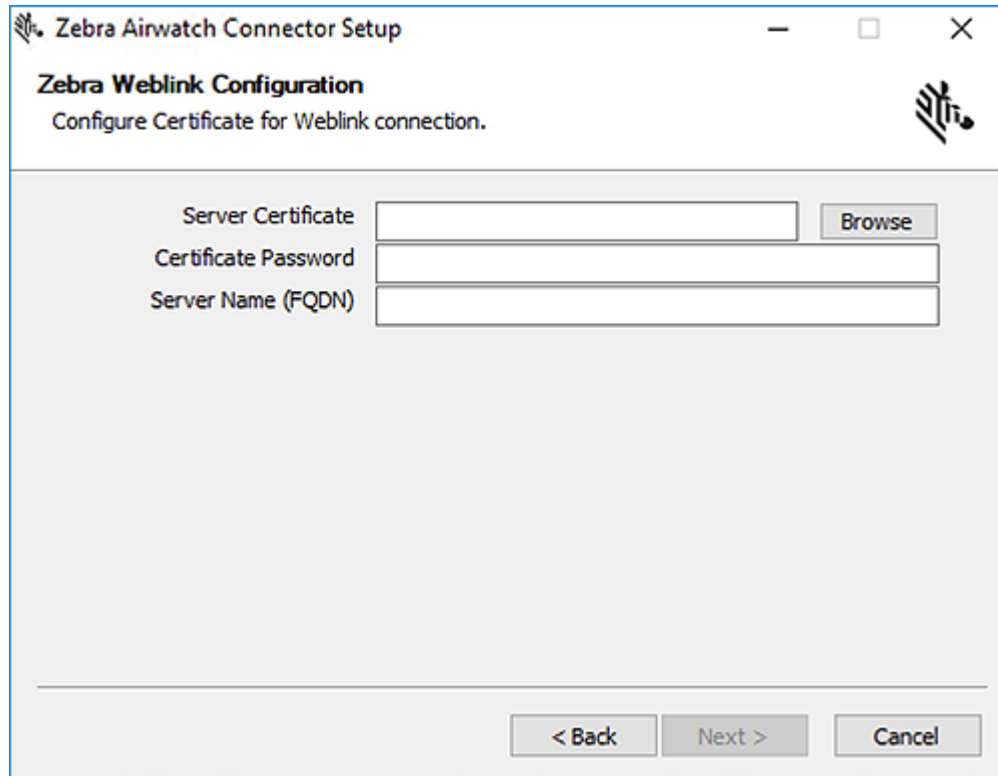
### 7. Click **Save**.

## Step 2: Installing the Zebra AirWatch Connector

The Zebra AirWatch Connector installer should be copied to the server on which it will be installed.

1. The installer does not perform an upgrade so any exiting installation should be removed first.
2. Right-click **AirwatchConnector.exe** and select **Run as administrator**.
3. Click **Next**.
  - a) Click **I Agree** to the License Agreement.
  - b) Click **Next** through the Important notice screens.

4. On the Zebra Weblink Configuration screen, click **Browse** and select the PFX file for the SHA-256 hashed certificate (for example: server.p12).
  - a) In the **Zebra Certificate Password** field, enter the password for the PFX file.
  - b) In the **Server Name (FQDN)** field, enter the FQDN of the server (for example: zc.example.com).
  - c) Click **Next**.



The screenshot shows a Windows application window titled "Zebra Airwatch Connector Setup". Inside the window, the section "Zebra Weblink Configuration" is active, with the subtitle "Configure Certificate for Weblink connection." and a Zebra logo. The configuration area contains three input fields: "Server Certificate" (with a "Browse" button to its right), "Certificate Password", and "Server Name (FQDN)". At the bottom of the window, there are three buttons: "< Back", "Next >", and "Cancel".

5. On the Airwatch Details screen:

- a) In the **Airwatch Group ID** field enter the alphanumeric group ID of the Organization Group where the Peripheral Server configuration is defined. This can be found by hovering your cursor over the OG selector at the top of the Workspace ONE UEM console and looking for the **Group ID** value.



- b) In the **Airwatch Server Location**, enter the following URL, setting the DS server FQDN as applicable: <https://ds1234.awmdm.com/deviceservices/peripheralservice/v1/register> Be sure to use the FQDN of the DS server and not the CN server.



**IMPORTANT:** Be sure to use the FQDN of the DS server and not the CN server.

- c) In the **Airwatch Token** field, enter the UUID from the **HMAC Token** generated by the peripheral server configuration in Workspace ONE.
- d) In the **Unique ID for Zebra Server** field, enter the **Service UID** from the peripheral server configuration in Workspace ONE.

- e) After all the fields have been filled in and validated, click **Next**.

6. Click **Install** to begin the installer; the install should only take a minute. When the install completes, click **Next**.

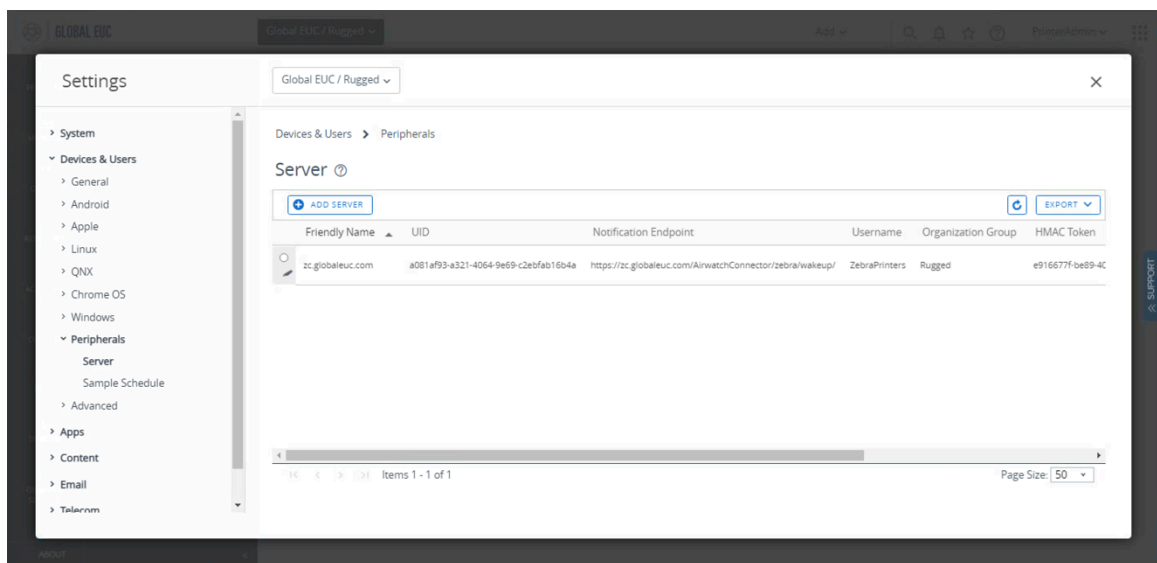
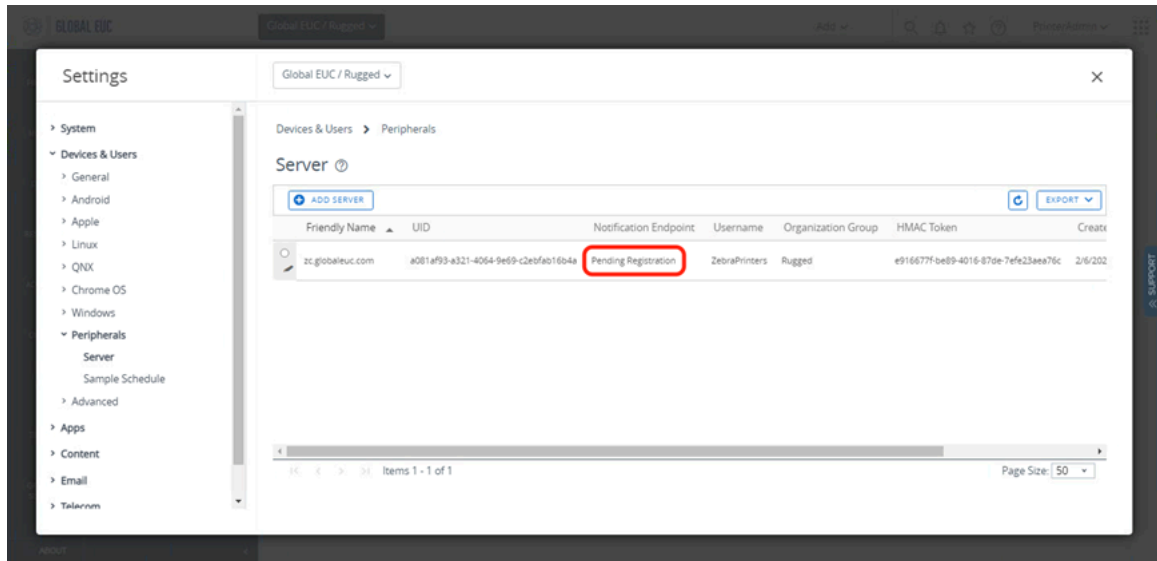
7. On the final screen, click **Finish**.

The Zebra AirWatch Connector has now been installed.

When the Zebra AirWatch Connector application service starts, it will attempt to register itself with Workspace ONE by contacting the URL specified in the **Airwatch Server Location** field in the Zebra AirWatch Connector installer and providing the supplied **UID** and **HMAC Token** for authentication. The

## Installation on Windows

Peripheral Server configuration in Workspace ONE should change from 'Pending Registration' status to the wakeup URL.



### Step 3: Set Up Printers

Upgrade your printer OS:

- Download the latest operating system for your printers from [zebra.com/linkos](https://zebra.com/linkos).
- Using the ZDownloader Utility, install the Printer OS on your Zebra printers.  
(To obtain a copy of the ZDownloader Utility, go to [zebra.com//us/en/support-downloads/prINTER-software/zdownloader](https://zebra.com//us/en/support-downloads/prINTER-software/zdownloader))
- The Zebra Setup Utilities software can be used to configure your printers to connect to your wireless network and the AirWatch Connector. Go to [zebra.com/setup](https://zebra.com/setup) to download. Send the

following commands to configure the printer to connect to your AirWatch Connector. Replace YourAirWatchServerLocationURL with the FQDN of your server:

```
! U1 setvar "weblink.ip.conn1.location" "https://YourAirWatchServerLocationURL/zebra/weblink/"  
! U1 setvar "device.reset" ""
```



**NOTE:** The trailing / is required.

### Step 4: Test 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.

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

The screenshot shows the AirWatch ONE UEM console interface. The left sidebar contains navigation options: GETTING STARTED, FREESTYLE, MONITOR, DEVICES, RESOURCES, ACCOUNTS, CONTENT, EMAIL, TELECOM, GROUPS & SETTINGS, and ABOUT. The main content area is titled 'Zebra Technologies Corp. - D...' and shows a 'List View' of 'Printers'. A table lists several printers, with the first one highlighted by a red box:

	Last Seen	Friendly Name	Type	Model	Organization Group
	16m	brucezq511-XXRAJ192400080	Zebra-Printer	Zebra ZQ511R	Zebra Technologies Corp. - Demo
	2d	hxp223-XXZKJ174700214	Zebra-Printer	Zebra ZQ620	Zebra Technologies Corp. - Demo
	2d	XXQPJ143600001-XXQPJ143600...	Zebra-Printer	Zebra ZR628	Zebra Technologies Corp. - Demo
	17d	XXQLJ133100893-XXQLJ1331008...	Zebra-Printer	Zebra QLn320	Zebra Technologies Corp. - Demo
	24d	FaZq520-XXRBJ194500454	Zebra-Printer	Zebra ZQ520	Zebra Technologies Corp. - Demo
	36d	XXZKN214701292-XXZKN21470...	Zebra-Printer	Zebra ZQ620	Zebra Technologies Corp. - Demo

At the bottom of the table, it says 'Items 1 - 8 of 8' and 'Page Size: 50'.

- 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.

The screenshot shows the AirWatch console interface. At the top, the breadcrumb navigation is 'Devices > Peripherals > List View'. The printer's 'Friendly Name' is 'brucezq511-XXRAJ192400080'. Below this, it says 'Zebra ZQ511R | Ownership: Undefined'. There are 'QUERY' and 'MORE' buttons. A tab bar at the top includes 'General' (selected), 'Device', 'Wi-Fi', 'Power', 'Mirror', 'Weblink', 'ZPLS', and 'More'. The main content area is split into two columns. The left column shows the Zebra logo and a status section with the following details:

Status	Enrolled
Last Seen	9/30/2022 3:49:33 PM
Enrollment Date	9/29/2022 4:44:27 AM
UDID	XXRAJ192400080

The right column shows a list of printer settings:

Type	Zebra-Printer
Model	Zebra ZQ511R
Firmware Version	V91.21.19Z
IP Address	10.48.212.75
Gateway IP Address	10.48.212.2
Battery Percentage	94
Power Health	good
Print Mode	Rewind
Print Method	Direct Thermal
Label Length	2030
Print Width	832
Printer Darkness	0

## Receiving Alerts from a Printer

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

- Click **Devices > Peripherals > Alerts**.
- Create an alert condition such as opening the media door on the printer or media out.
- Wait 10 seconds, and then refresh the AirWatch console display.

You should see the alert appear in the list with the appropriate Alert Type and condition of True/False.

The screenshot shows the 'Alerts' section in the AirWatch console. The breadcrumb navigation is 'Devices > Peripherals > Alerts'. There are 'EXPORT' and 'Search List' buttons. The main area contains a table of alerts:

Friendly Name	Sample Time	Transmit Time	Alert Type	Alert Data	Condition	Severity
XXQJ133100893-XXQJ133100893	9/12/2022 2:00 AM	9/12/2022 2:00 AM	BatteryLow	BATTERY LOW	False	1
XXQJ133100893-XXQJ133100893	9/12/2022 6:12 AM	9/12/2022 6:12 AM	BatteryLow	BATTERY LOW	False	1
XXQJ133100893-XXQJ133100893	9/12/2022 10:21 AM	9/12/2022 10:21 AM	BatteryLow	BATTERY LOW	False	1
XXQJ133100893-XXQJ133100893	9/12/2022 2:30 PM	9/12/2022 2:30 PM	BatteryLow	BATTERY LOW	False	1
XXQJ133100893-XXQJ133100893	9/12/2022 6:48 PM	9/12/2022 6:48 PM	BatteryLow	BATTERY LOW	False	1
XXQJ133100893-XXQJ133100893	9/12/2022 10:59 PM	9/12/2022 10:59 PM	BatteryLow	BATTERY LOW	False	1
brucezq511-XXRAJ192400080	9/29/2022 6:07 AM	9/29/2022 6:07 AM	BatteryLow	BATTERY LOW	False	1
brucezq511-XXRAJ192400080	9/29/2022 12:03 PM	9/29/2022 12:03 PM	PaperOut	PAPER OUT	True	1
brucezq511-XXRAJ192400080	9/29/2022 4:18 PM	9/29/2022 4:18 PM	PaperOut	PAPER OUT	True	1
brucezq511-XXRAJ192400080	9/29/2022 8:33 PM	9/29/2022 8:33 PM	PaperOut	PAPER OUT	True	1
brucezq511-XXRAJ192400080	9/30/2022 12:48 AM	9/30/2022 12:48 AM	PaperOut	PAPER OUT	True	1
brucezq511-XXRAJ192400080	9/30/2022 1:08 AM	9/30/2022 1:08 AM	PaperOut	PAPER OUT	True	1
brucezq511-XXRAJ192400080	9/30/2022 3:25 AM	9/30/2022 3:25 AM	PaperOut	PAPER OUT	True	1
brucezq511-XXRAJ192400080	9/30/2022 4:03 AM	9/30/2022 4:03 AM	PaperOut	PAPER OUT	True	1
brucezq511-XXRAJ192400080	9/30/2022 7:39 AM	9/30/2022 7:39 AM	PaperOut	PAPER OUT	True	1
brucezq511-XXRAJ192400080	9/30/2022 11:54 AM	9/30/2022 11:54 AM	PaperOut	PAPER OUT	True	1

The table footer indicates 'Items 1 - 42 of 42' and 'Page Size: 50'.

- Clear the error on the printer.

5. Wait 10 seconds, and then refresh the AirWatch console display.

You should see the True/False condition of the alert change. If the alerts appear on the screen, you have verified that the printer is able to send alerts to the AirWatch console.



# Configuring Printers with 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 21](#).

## Configuring the Printer to Connect to a 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.ietf.org/rfc/rfc3986.txt>). For example, if the remote server's full URL is: <https://www.examplecorpinc.com/zebra/weblink/>

then 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
- The proxy server port (optional)
- The username and password for the proxy (optional)

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

```
! U1 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:

```
! U1 setvar "weblink.ip.conn1.proxy" "https://my.internal.proxy:3128/"
```

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

```
! U1 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:

```
! U1 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:

```
! U1 getvar "weblink.ip.conn1.authentication.entries"
```

To remove authentication credentials issue the following:

```
! U1 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 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:

```
[12-04-2012 14:57:10.625] [conn1.1] Attempting connection to https://  
www.examplecorpinc.com/zebra/weblink/
```

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.



**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 `apl.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 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:** Channels are additional connections that are requested by the server when the server needs to perform a specific operation that cannot be done on the channel(s) currently open. Typically only the RAW channel is open, which operates similar to the RAW TCP port. It is typical to see two channels opened the main channel and the RAW channel.

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 24](#) to understand what it means when certain logging messages/errors appear in the log.

# Troubleshooting

This section provides troubleshooting solutions for potential problems during operation.

## Installation

The following table describes installation errors and possible causes and solutions.

Issue	Reason	Solution
Error when starting Tomcat	Various reasons can cause this error.	See Apache Tomcat website — <a href="https://tomcat.apache.org/">https://tomcat.apache.org/</a>
Tomcat Port conflict error	There is another server trying to use the same port as Zebra AirWatch Connector on the computer.	<p>Choose one of the following:</p> <ul style="list-style-type: none"><li>• Stop the other servers using Windows services.</li><li>• Change the port in Tomcat. The default port is 443.</li></ul> <p> <b>IMPORTANT:</b> 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.</p>

## AirWatch



The following table describes Location Group related issues and possible causes and solutions.

Issue	Reason	Solution
Added a printer to a Location Group. Once the printer is powered off and on, it is no longer associated with the original location group.	Some settings are not stored until a profile is published to that printer.	<ol style="list-style-type: none"> <li>1. Create a generic profile for the Location Group.</li> <li>2. Set the option to Auto install and click Publish.</li> </ol> <p>(All settings are saved and sent to all of the printers within the group.)</p>
Added a printer to a Location Group. Then, clicked Soft Reset on the AirWatch console, it is no longer associated with the original location group.		

## 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.

Error	Cause/Solution
"SSL certificate problem: self signed certificate in certificate chain"	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.
"SSL certificate problem: unable to get local issuer certificate"	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.


Error	Cause/Solution
"SSL certificate problem: certificate has expired"	<p>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.</p> <p> <b>NOTE:</b> 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 <code>rtc.date</code> SGD is managed. If it has never been set then it will default to the firmware build date (the value in <code>appl.date</code>). Otherwise, the value in <code>rtc.date</code> will default to the value that it was last set to. This does not mean the value of the <code>rtc.date</code> when it was power cycled. It means that when a user sets <code>rtc.date</code> that becomes the new default value.</p> <p>If the printer has a battery, then the <code>rtc.date</code> is never default and continues to track the date as expected.</p>
"SSL certificate problem: certificate is not yet valid"	<p>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 (<code>rtc.date</code> and <code>rtc.time</code>) are set correctly and that the certificate's start and expiration date are valid.</p> <p> <b>NOTE:</b> 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 <code>rtc.date</code> SGD is managed. If it has never been set then it will default to the firmware build date (the value in <code>appl.date</code>). Otherwise, the value in <code>rtc.date</code> will default to the value that it was last set to. This does not mean the value of the <code>rtc.date</code> when it was power cycled. It means that when a user sets <code>rtc.date</code> that becomes the new default value.</p> <p>If the printer has a battery then the <code>rtc.date</code> is never default and continues to track the date as expected.</p>

Error	Cause/Solution
"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 <code>weblink.ip.conn1.location</code> 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'"	
"Unknown SSL protocol error in connection to ..."	When this message is seen it means that the remote server's SSL/TLS configuration is incorrect. Refer to <a href="#">Troubleshooting Sequence on page 27</a> to ensure the server and printer are both configured correctly.
I do not see any of these errors, but the printer still does not connect.	Refer to <a href="#">Troubleshooting Sequence on page 27</a> 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.

Error	Cause/Solution
"Read failed with an unexpected error"	<p>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.</p> <p> <b>NOTE:</b> 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 the attempt to connect to the remote server so that when the server comes back online the printer will re-establish communication.</p>
"Failed to connect (SP = #, CI = #, UW = #, AC = #, PC = #)"	<p>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 set up according to the Servlet configuration in the Zebra Link-OS™ SDK documentation.</p> <p>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.</p>

## Troubleshooting Sequence

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. Does the firewall permit HTTPS connections initially or do I need to connect via HTTP first?
11. Is the remote server configured to use TLS 1.2?
12. Are the Certificate Authority Certificates correctly installed on the remote server?
13. Has the server's certificate expired?
14. Is the printer's date and time within the issue and expired period of the server's certificate?
15. 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?
16. Is the proxy server configured correctly and does the respective proxy server allow HTTPS connections via the HTTP CONNECT method?
17. Are there any HTTP authentication attempts when trying to connect that fail?
18. 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 SGD command. Ensure that logging is enabled and that the error(s) appear within the entries)

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

## HTTP Messages

Message	Cause/Solution
HTTP/1.1 100 Continue	This indicates that the server and printer have begun communicating and is often seen in place of HTTP/1.1 200 OK.
HTTP/1.1 101 Switching Protocols	This indicates that the basic connection to the server worked and the protocol is being switched to a more efficient protocol for data transfer.
HTTP/1.1 200 OK	This indicates that an HTTP GET or HTTP POST was successful.
HTTP/1.1 30x Moved/Redirect/etc	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).
HTTP/1.1 401 Unauthorized	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).
HTTP/1.1 403 Forbidden	This typically means that the authentication was provided and valid; however, the user does not have access to the requested resource.

## Troubleshooting

Message	Cause/Solution
HTTP/1.1 404 Not Found	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.

# Printer Configuration

This section provides details on the printer configuration file.

## Printer Configuration File

Zebra printers can accept data in the multi-part form format, which provides the preferred method to store PEM format certificates on the printer. All printers should be updated to the latest OS version.

Other methods to store certificates on the printer are described in the PrintSecure Printer Administration Guide, available from [Zebra's PrintSecure Support Page](#).

## Multi-Part Form Format

```
{ }--<boundary characters><CR><LF>
Content-Disposition: form-data; name="files"; filename="<service name>"
<CR><LF>
Content-Type: application/octet-stream<CR><LF>
Content-Transfer-Encoding: binary<CR><LF>
<CR><LF>
<pem cert data><CR><LF>
--<boundary characters>--<CR><LF>
```

### Where

**<boundary characters>** = no more than 70 ASCII characters, no white space.

**<CR><LF>** = carriage return and line feed characters

**<service name>** = WEBLINK1\_CA.NRD if weblink.ip.conn1 is used or WEBLINK2\_CA.NRD if weblink.ip.conn2 is used.

**<pem cert data>** = PEM file contents of the certificate.

## Configuration File Example

The following is an example of a configuration file. The `file.dir` command as described in this [Zebra support article](#) can be used to validate that the certificate was successfully stored on the printer.

The example shows file content containing printer configuration commands and a Certificate Authority root certificate file.

```
{ }{"weblink.logging.max_entries":"600","weblink.ip.conn1.location":"https://
<your-zac-fqdn>/zebra/
weblink/","weblink.ip.conn1.proxy":"","weblink.ip.conn1.retry_interval":"120"}

{ }--lJNjwf8Ism5aRhxyJAvmRWcvIR3ABY
Content-Disposition: form-data; name="files"; filename="E:WEBLINK1_CA.NRD"
Content-Type: application/octet-stream
Content-Transfer-Encoding: binary

-----BEGIN CERTIFICATE-----
MIIFFjCCAv6gAwIBAgIRAJErCERPDBinU/bWLiWnXlowDQYJKoZIhvcNAQELBQAw
TzELMAkGA1UEBhMCVVMxKTAnBgNVBAoTIEludGVybmV0IFNlY3VyaXR5IFJlc2Vh
cmNoIEdyb3VwMRUwEwYDVQQDEwxJUlJHIFJvb3QgWDEwHhcNMjAwOTA0MDAwMDAw
WhcNMjUwOTE1MTYwMDAwWjAyMQswCQYDVQGEwJVUzEWMBQGA1UEChMNTGV0J3Mg
RW5jcmlwdDELMAkGA1UEAxMCUjMwggeEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEK
AoIBAQC7AhUozPaglNMPEuyNVZLD+ILxmaZ6QoinXSaqtSu5xUyxr45r+XXIo9cP
...
lines removed for brevity.
...
yJMC6allBbFODALZvYH7n7dolAZls4I9d1P4jnkDrQoxB3UqQ9hVl3LEKQ73xF10
yK5GhDDX8oVfGKF5u+decIsH4YaTw7mP3GFxJSqv3+0lUFJoi5Lc5da149p90Ids
hCExroL1+7mryIkXPeFM5TgO9r0rvZaBF0vV2z0gp35Z0+L4WPlbuEjn/lxPFIn+
HlUjr8gRsI3qfJOQFy/9rKIJR0Y/8OmwT/8oTWgylmdeHmMjk7jlnYsvC9JSQ6Zv
MldlTTKB3zhThV1+XWYp6rjd5JW1zbVWEkLNxE7GJThEUG3szgBVGP7pSWTUTsqX
nLRbwHOoq7hHwg==
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIFYDCCBEigAwIBAgIQQAF3ITfU6UK47naqPGQKtZANBgkqhkiG9w0BAQsFADA/
MSQwIgYDVQQKEExtEaWdpdGFsIFNpZ25hdHVyZSBUCnVzdCBDbY4xZzAVBgNVBAMT
DkRTVCBSb290IENBIFgzMB4XDTIxMDEyMDE5MTQwM1oXDTI0MDkzMDE4MTQwM1ow
TzELMAkGA1UEBhMCVVMxKTAnBgNVBAoTIEludGVybmV0IFNlY3VyaXR5IFJlc2Vh
cmNoIEdyb3VwMRUwEwYDVQQDEwxJUlJHIFJvb3QgWDEwggEiMA0GCSqGSIb3DQEB
AQUAA4ICDwAwggIKAoICAQCt6Crz9BQ385ueK1coHie+3LffOJCMbjzmV6B493XC
ov71am72AE8o295ohmxEk7axY/0UEmu/H9LqMZshftEzPLpI9d153704/xLxIZpL
wYqGcWlKZmZsj348cL+tKSIG8+TA5oCu4kuPt5l+1AOfo0eXfJlIIlPoOK5PCm+D
LtFJV4yAdLbaL9A4jXsDcCEbdfIwPPqPrt3ay6vrFk/CjhFLfs8L6P+ldy70sntK
4EwSJQxwjqMpoOFTJOwT2e4ZvxCzSow/iaNhUd6shweU9GNx7C7ibluYgeGJXDR5
...
lines removed for brevity.
...
c3QuY29tL3Jvb3RzL2RzdHJvb3RjYXgzLnA3YzAfBgNVHSMEGDAWGBTEp7Gkeyxx
+tvhS5B1/8QVYIWIJEDBUBgNVHSAETTLBMAgGBmeBDAECATA/BgsrBgEEAYLfEwEB
ATAwMC4GCCsGAQUFBwIBFiJodHRwOi8vY3BzLnJvb3QteDEubGV0c2VvY3J5cHQu
b3JnMDwGA1UdHwQ1MDMwMaAvoC2GK2h0dHA6Ly9jcmwuaWRlbnRydXN0LmNvbS9E
U1RST09UQ0FYM0NSTC5jcmwwHQYDVROBBYEFHm0WeZ7tuXkAXOACIjIGlj26Ztu
MA0GCSqGSIb3DQEBECwUAA4IBAQAkwBslm7/DlLQrt2M51oGrS+o44+/yQoDFVDC
5WxCu2+b9LRPwkSICXHM6webFGJueN7sJ7o5XPWioW5WlHAQU7G75K/QosMrAdSW
9MUGnTP52GE24HGNTLilqoJfLcDyqSMo59ahy2ci2qBDLKobkx/J3vWraV0T9VuG
WCLKTVXkcGdtwlfFRjlbZ4pYglhtmf5X6DYO8A4jqv2il9DjXA6USbW1FzXSLr90
he8Y4IWS6wY7bCkjCWDcRQJMEhg76fsO3txE+FiYruq9RUWhiF1myv4Q6W+CyBFC
Dfvp70OGAN6deOM4+qR9sdjoSYKEBpsr6GtPAQw4dy753ec5
-----END CERTIFICATE-----
--lJNjwf8Ism5aRhxyJAvmRWcvIR3ABY--
```

```
{{"device.reset":""}}
```

## Revision History

Version	Date	Changes
1.7.0.126	November 2023	<ul style="list-style-type: none"> <li>Added ciphers to the server.xml file to ensure weak ciphers are not used</li> <li>The Tomcat version has been updated to version 10.x.</li> <li>Updated libraries in AirwatchConnector.war and zebra.war</li> <li>Removed Zebra SHA1 root certificates</li> <li>Removed the batch file for the creation of Zebra-signed SHA1 certificates. Zebra intends to retire the server that is used in this automated process.</li> </ul>
1.6.0162	October 2022	<ul style="list-style-type: none"> <li>The Tomcat version has been updated to version 9.x.</li> <li>The Java version has been updated to version 17.x.</li> <li>TLS 1.0/1.1 connections are now disabled, so only TLS 1.2 is supported.</li> <li>Library versions have been updated in the AirwatchConnector.war and Zebra.war components.</li> <li>Due to the changes listed above, the minimum required Link-OS version in the printer is now 5.0.</li> </ul>

