AirWatch Connector

User Guide

ZEBRA

P1058563-08EN

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.

Publication Date

October 19, 2022

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).

Contents

Contents

Introduction

The Zebra AirWatch Connector partners with the AirWatch 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 www.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, use the Zebra Setup Utilities.

Installation in a Windows Operating System

Minimum System Requirements

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

- Windows Server 2019
- Windows Server 2022

Minimum Server Requirements

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

NOTE: Check the zebra.com support page for the latest system requirements information.

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: Obtain a Zebra-Signed Certificate

During installation you will be asked to provide a Zebra certificate which is necessary for printers to connect to the AirWatch Connector server. Follow the steps below to obtain the signed certificate prior to starting the installation.

You will need the Fully Qualified Domain Name of the AirWatch Connector server during this process.

This process has the following requirements:

- Java is installed on the computer
- Internet connectivity and access to acs.zebra.com on port 443.

1. Extract the included Registration.zip file to a folder on any computer that has the above requirements.
2. Run SHA1.BAT file and follow the on-screen instructions.

3. This process will create a .p12 certificate file and keyPass.txt file containing the password.

NOTE: You will be prompted for the .p12 file and password during the installation.

4. The certificate generation process is complete.

Step 2: Configure Your AirWatch Server

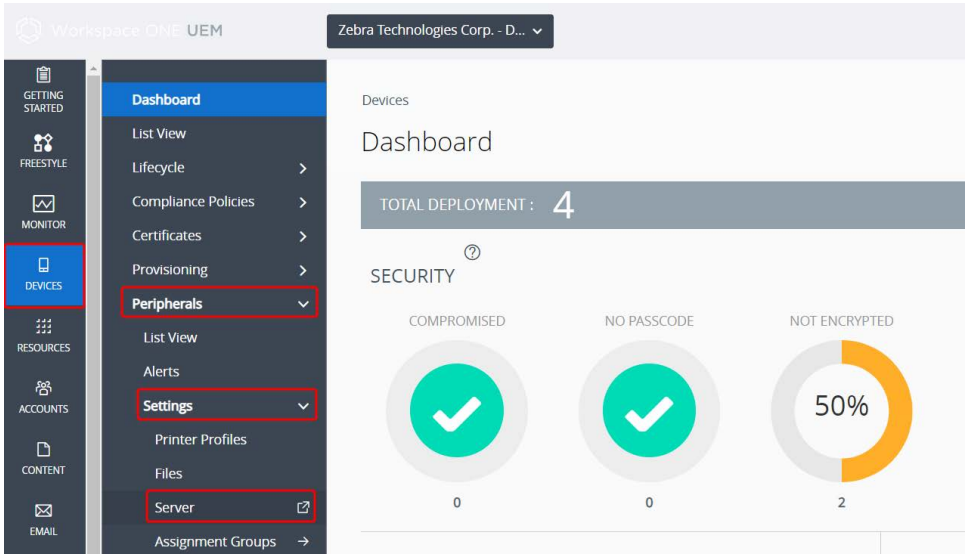
The following installation steps assume you already have an AirWatch server.

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

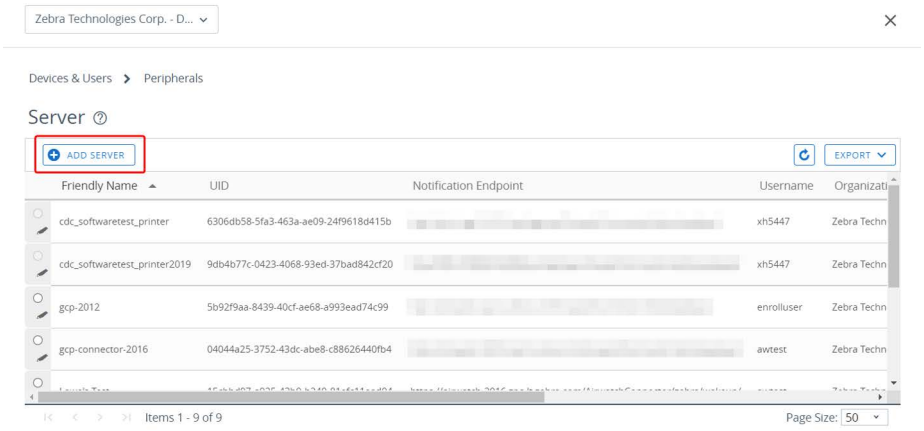
- Zebra Wakeup Location
- AirWatch Group ID
- AirWatch Server Location
- AirWatch Token
- Unique ID for Zebra Server

2. Log into AirWatch

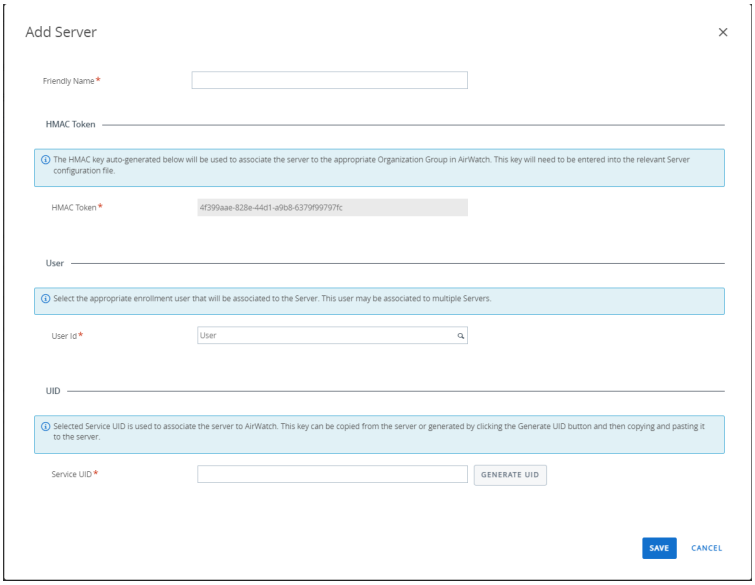
   i. **Devices > Peripherals > Settings > Server**



3. Click **Add Server.**



4. Fill in your **Friendly Name**.
5. Select your **User ID**.
6. Generate a **Service UID**.



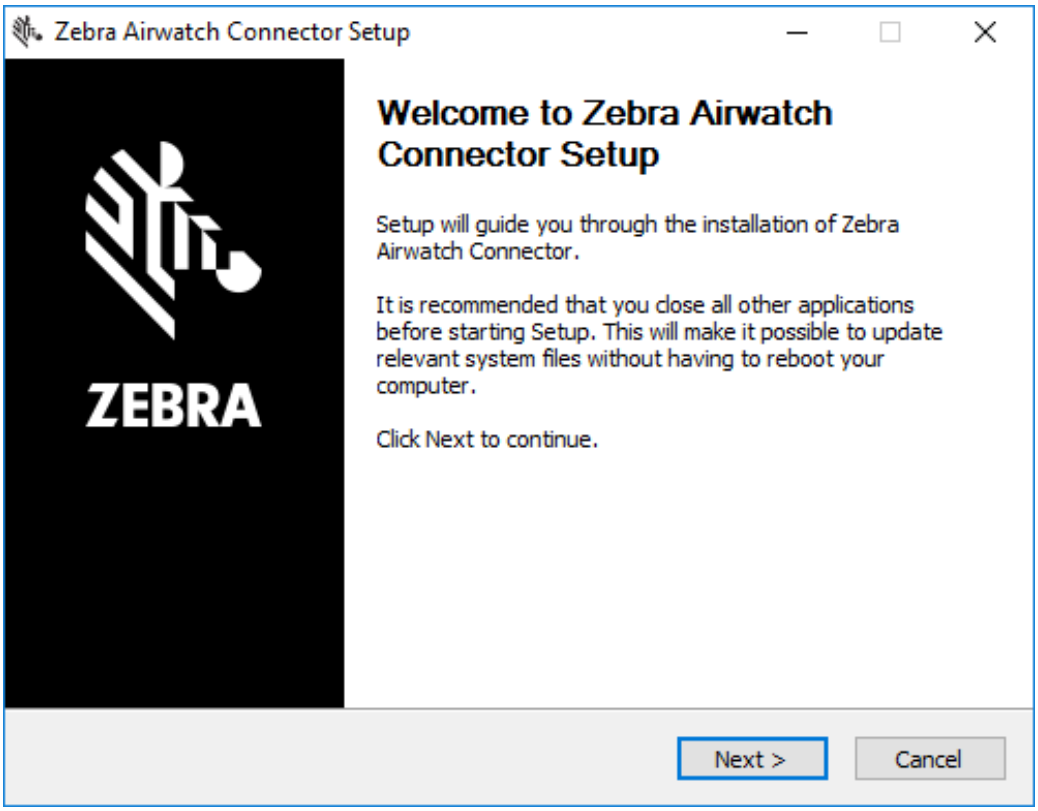
7. Click **Save**.

Step 3: Install Wizard

1. Run **AirwatchConnector.exe**

   Depending on your account security settings, you may see a User Account Control dialog box.

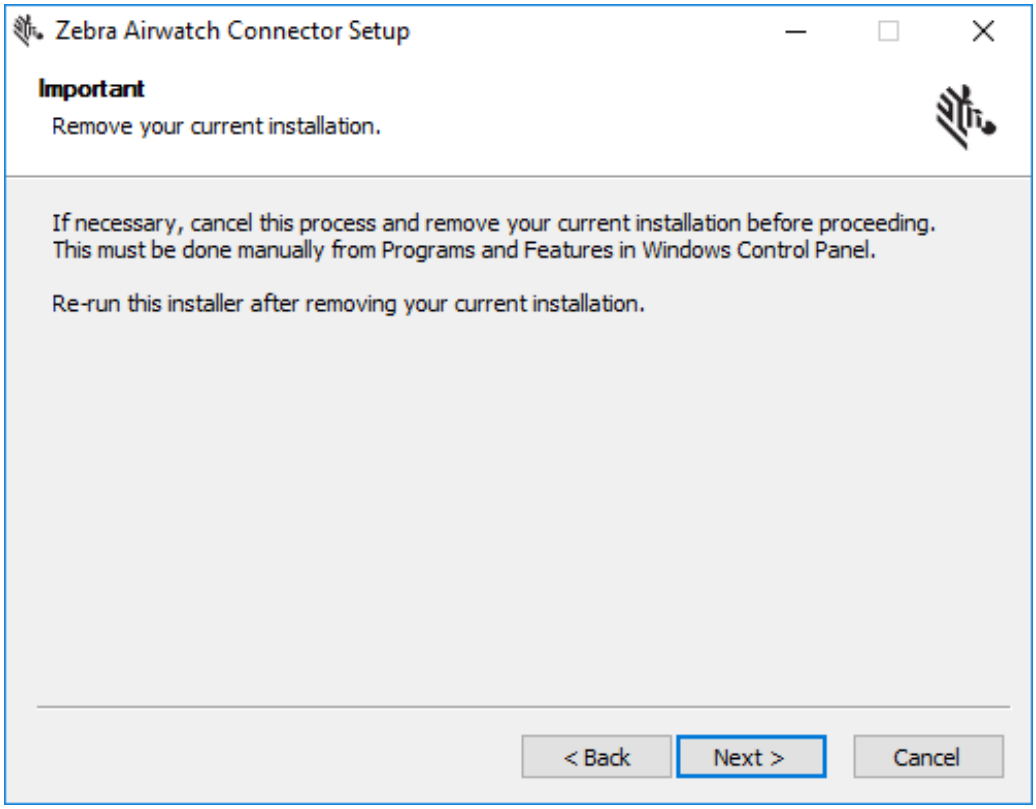
i. Click **Yes** to begin installing AirWatch Connector.

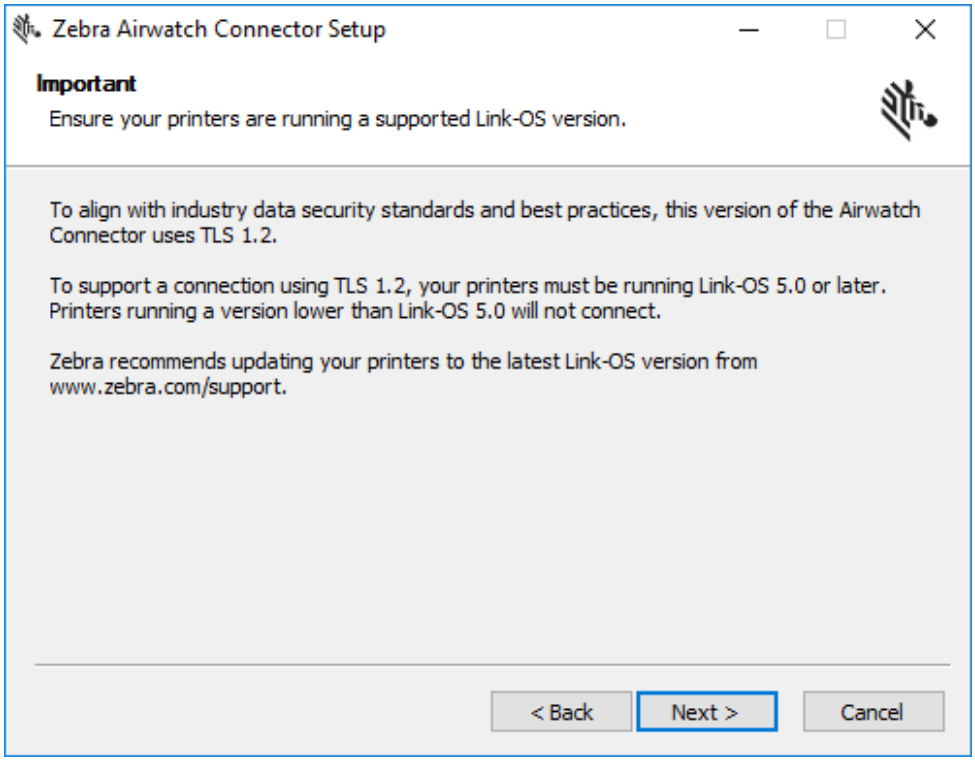


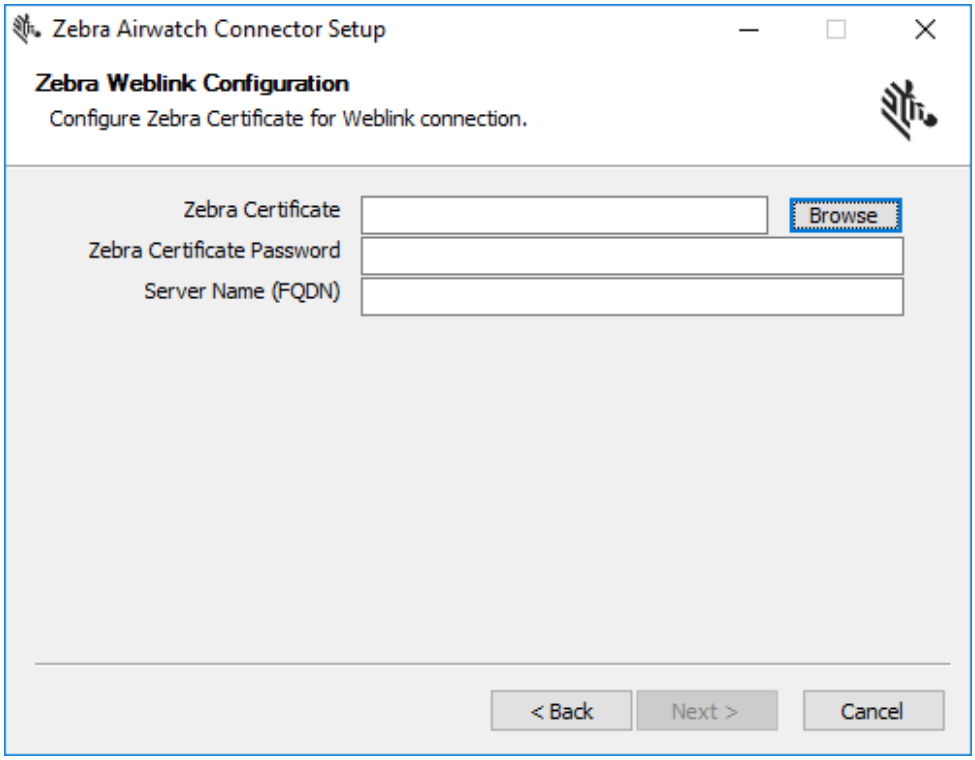
ii. Click **Next** to continue.

iii. You must accept the terms of the License Agreement to continue.

iv. Click **I Agree**.





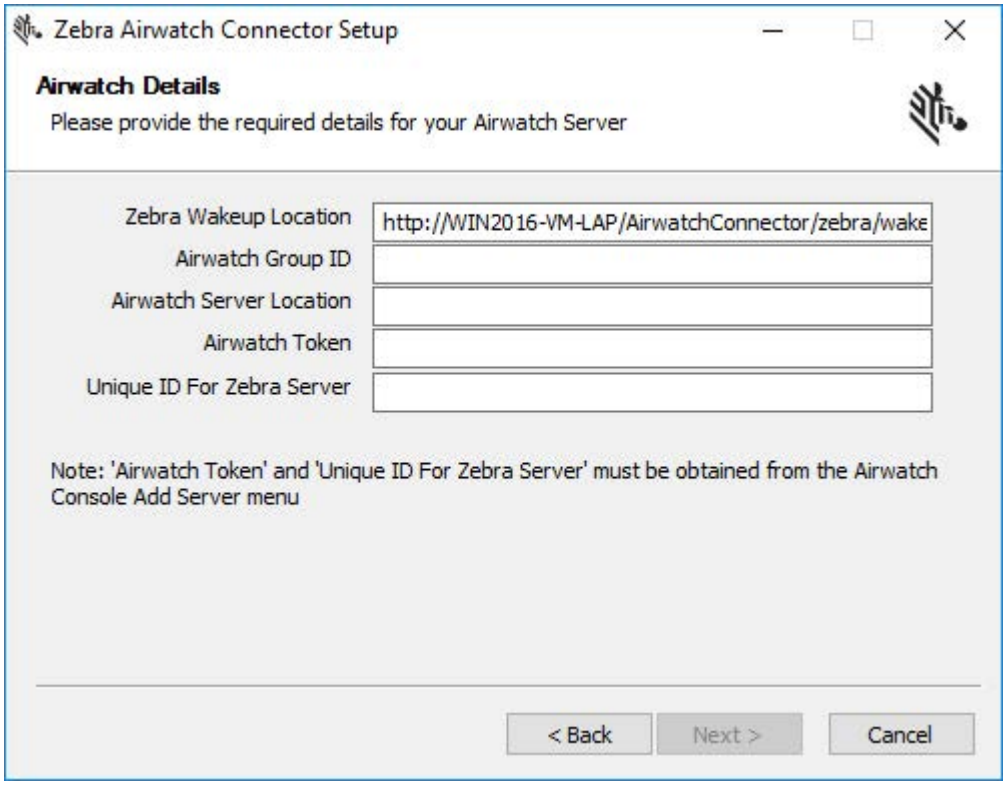


2. Browse and select the .p12 file you generated in Step 1 (Obtain a Zebra-Signed Certificate).
3. Enter the Zebra Certificate Password from the keyPass.txt file also generated in Step 1.
4. Enter the Fully Qualified Domain Name (FQDN) of your server.
5. Click **Next**.

6. Using the information gathered from Step 2 (Configure Your AirWatch Server), enter the below details in the appropriate fields and click **Next**.
   i. The installer will fill in the **Zebra Wakeup Location**.
   ii. Enter the **Airwatch Group ID.**
   iii. Enter the **AirWatch Server Location** in the format below and replace your.airwatchportals.com with the correct domain for your server.

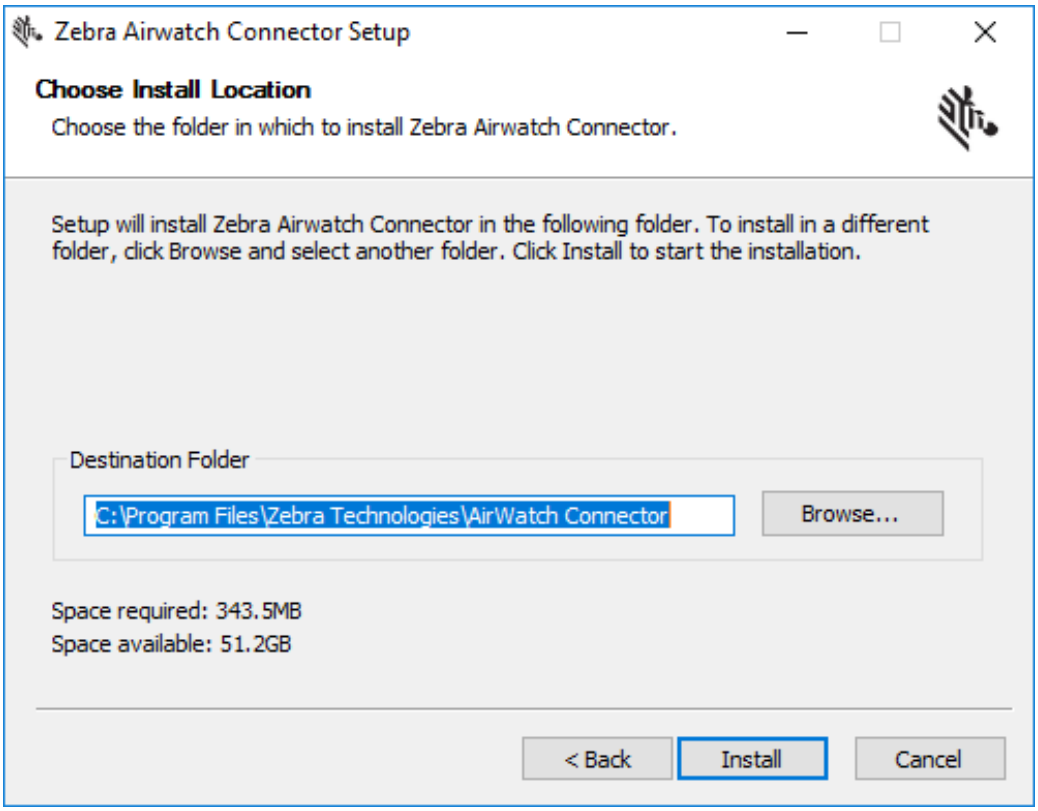
   [http|https]://your.airwatchportals.com/deviceservices/peripheralservice/v1/register

   iv. Enter the HMAC Token in the **Airwatch Token** field.
   v. Enter the Service UID in the **Unique ID for Zebra Server** field.

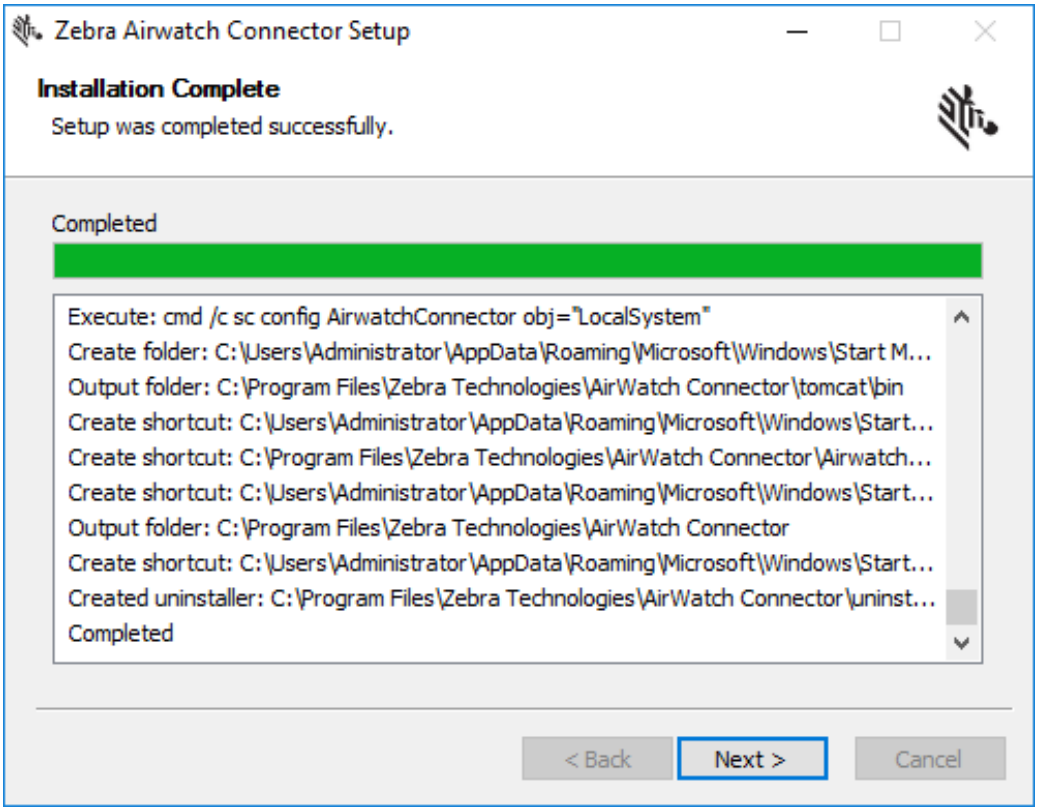


7. Click **Next**.

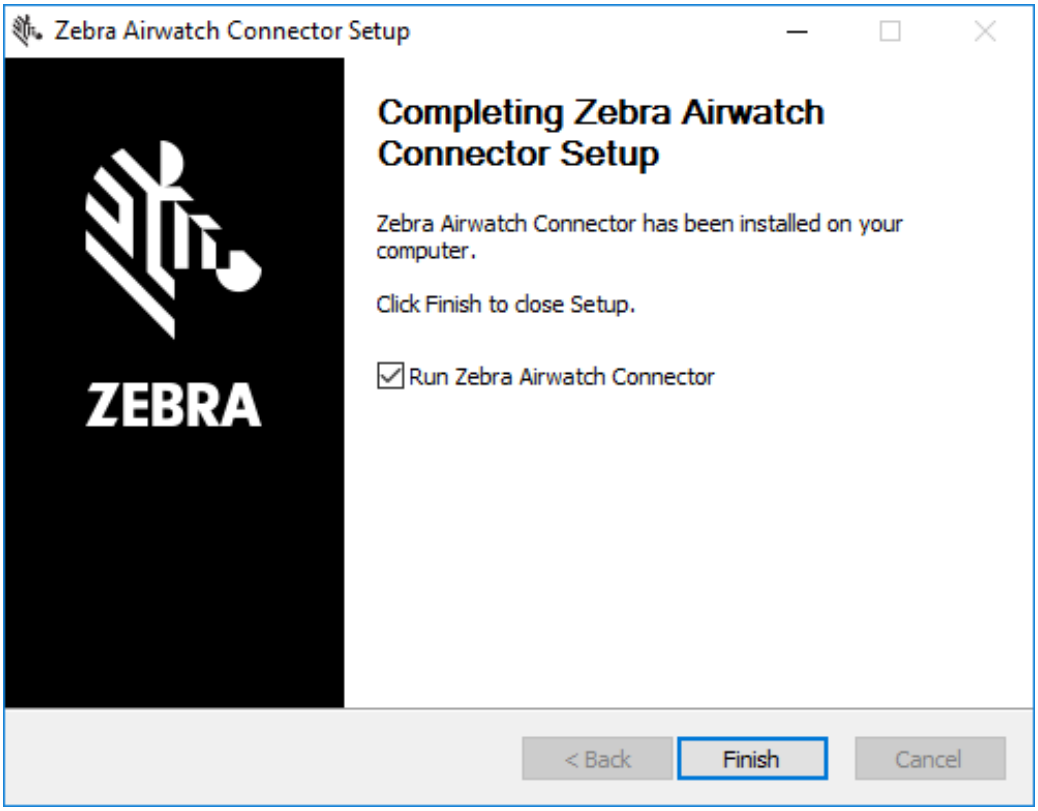
8. Choose the destination folder.



9. Click **Install**.



10. Click **Next**.



11. Click **Finish**.

Step 4: Set Up Printers

1. Upgrade your printer OS:
   i. Download the latest operating system for your printers from https://www.zebra.com/linkos
   ii. Using the ZDownloader Utility, install the Printer OS on your Zebra printers. (To obtain a copy of the ZDownloader Utility, go to www.zebra.com//us/en/support-downloads/printer-software/zdownloader.html)
   iii. The Zebra Setup Utilities software can be used to configure your printers to connect to your wireless network and the AirWatch Connector. Go to www.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.

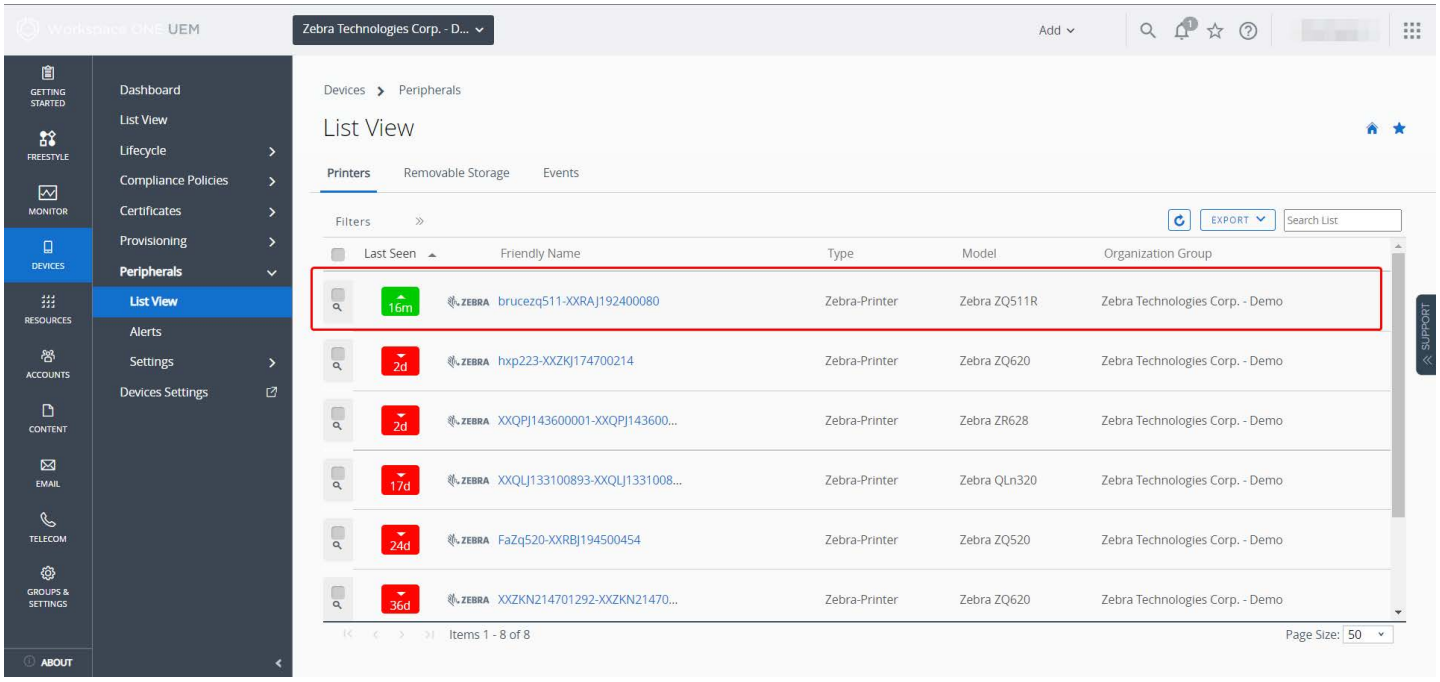
Step 5: Test a Printer

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.

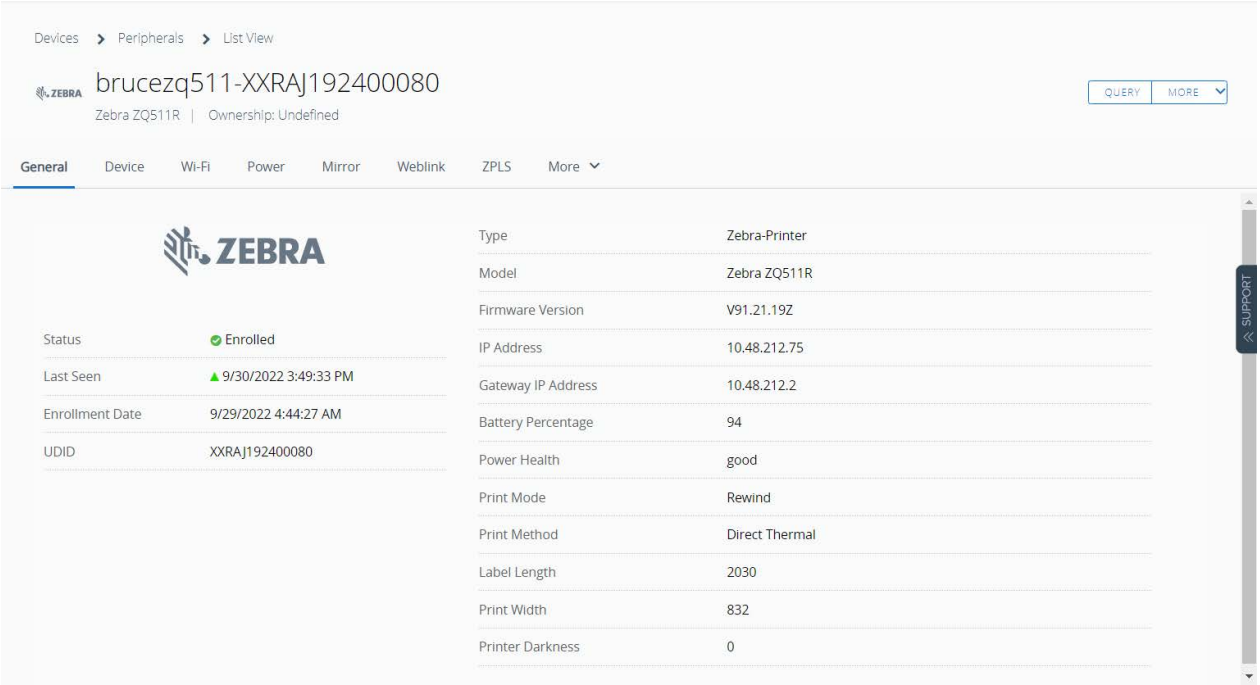
1. Turn on the printer.
2. Log into the AirWatch console, if necessary.

   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.

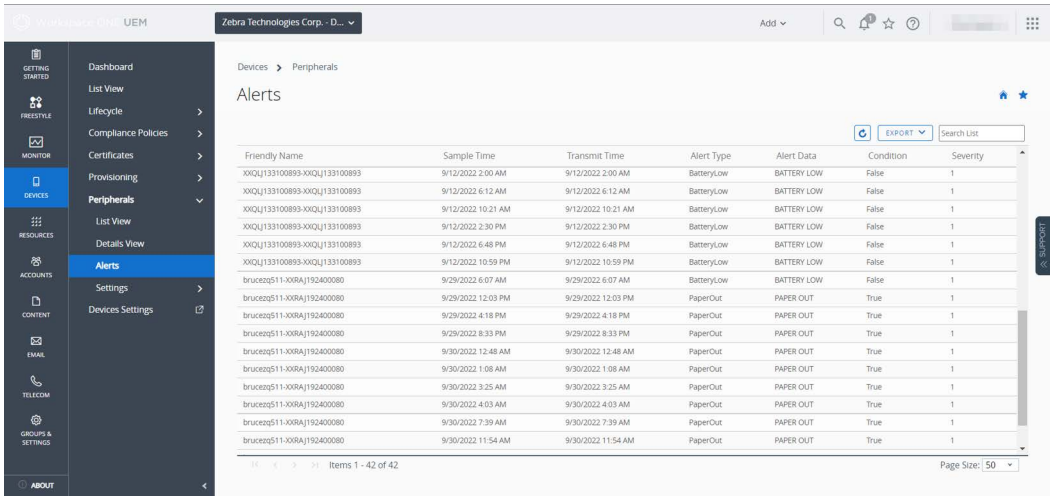


Receiving Alerts from a Printer

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

1. Click **Devices** > **Peripherals** > **Alerts**.
2. Create an alert condition such as opening the media door on the printer or media out.
3. 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.



4. 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.

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.ietf.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
- 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 newconnections 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:

```
[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 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 **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

Installation

Issue	Reason	Solution
Error when starting Tomcat	Various reasons can cause this error.	See Apache Tomcat website — http://tomcat.apache.org/
Tomcat Port conflict error	There is another server trying to use the same port as Zebra AirWatch Connector on the computer.	Choose one of the following: • Stop the other servers using Windows services. • Change the port in Tomcat. The default port is 443. **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

Issue	Reason	Solution
I 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.	**a.** Create a generic profile for the Location Group. **b.** Set the option to Auto install and click Publish. (All settings are saved and sent to all of the printers within the group.)
I added a printer to a Location Group. After I click Soft Reset on the AirWatch console, and 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.
"SSL certificate problem: certificate has expired"	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 **rtc.date** and **rtc.time** are set correctly. 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. 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" **"SSL certificate subject name 'examplecorpinc.com' does not match target host name '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.
"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 Troubleshooting Sequence on page 27 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 Troubleshooting Sequence on page 27 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"	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. 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.
"Failed to connect (SP = #, CI = #, UW = #, AC = #, PC = #)"	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.

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. 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:

   i. disallow POST messages

   ii. only operate in HTTP/1.0 mode 3

   iii. disallow SSL connections.

Refer to your Linux Squid documentation for complete details.

1. Does the firewall permit HTTPS connections initially or do I need to connect via HTTP first?
2. Is the remote server configured to use TLS 1.2?
3. Are the Zebra Certificate Authority Certificates correctly installed on the remote server?
4. Was the server's certificate issued by Zebra and is it signed by the Zebra Certificate Authority?
5. Has the server's certificate expired?
6. Is the printer's date and time within the issue and expired period of the server's certificate?
7. 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?
8. Is the proxy server configured correctly and does the respective proxy server allow HTTPS connections via the HTTP CONNECT method?
9. Are there any HTTP authentication attempts when trying to connect that fail?
10. 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.
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.

Change Log

Version	Date	Changes
1.6.0162	October 2022	• The Tomcat version has been updated to version 9.x • The Java version has been updated to version 17.x • TLS 1.0/1.1 connections are now disabled so only TLS 1.2 is supported. • Library versions have been updated in the AirwatchConnector.war and Zebra.war components. • Due to the changes listed above, the minimum required Link-OS version in the printer is no 5.0.