

# SOTI<sup>®</sup> MobiControl<sup>™</sup> Connector



**ZEBRA**

## **User Guide**

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.  
© 2022 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)

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.

### Open Source Usage

For more detailed information on the Link-OS Open Source usage, please visit:

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

## Publication Date

September 27, 2022

# Contents

Terms of Use .....	2
Publication Date .....	2
Contents .....	3
Introduction .....	5
Overview .....	5
Supported Printers .....	5
System Requirements .....	5
Installation .....	6
Installation Steps .....	6
Configuring Printers with WebLink .....	23
Configuring Weblink .....	23
Troubleshooting .....	27
Installation Errors .....	27
Locating the SOTI MobiControl Connector Log File .....	28
SSL/TLS Certificate Errors .....	29
Other Typical Errors .....	31
Troubleshooting .....	31
HTTP Messages .....	33
WebLink Set/Get/Do Commands .....	34
Introduction to SGD Commands .....	34
weblink.enable .....	35
weblink.ip.conn[1 2].authentication.add .....	36
weblink.ip.conn[1 2].authentication.entries .....	38
weblink.ip.conn[1 2].authentication.remove .....	39
weblink.ip.conn[1 2].enable .....	40
weblink.ip.conn[1 2].location .....	41
weblink.ip.conn[1 2].maximum_simultaneous_connections .....	42
weblink.ip.conn[1 2].proxy .....	43
weblink.ip.conn[1 2].retry_interval .....	45
weblink.ip.conn[1 2].test.location .....	46

weblink.ip.conn[1 2].test.retry_interval .....	48
weblink.ip.conn[1 2].test.test_on .....	49
weblink.logging.clear .....	51
weblink.logging.entries .....	52
weblink.logging.max_entries .....	53
weblink.printer_reset_required .....	55
weblink.restore_defaults .....	56

# Introduction

This section provides general information about the SOTI MobiControl Connector.

## Overview

The Zebra SOTI MobiControl Connector partners with the SOTI MobiControl server to manage your Zebra Print DNA printers.

The SOTI MobiControl Connector is the gateway between Zebra Print DNA printers and the SOTI MobiControl server.

Alerts generated by the printer are sent via the SOTI MobiControl Connector and appear in the MobiControl console.

Objects and profiles are sent from the MobiControl console to the printers via the SOTI MobiControl Connector.

## Supported Printers

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

## System Requirements

The SOTI MobiControl Connector is supported on the following operating systems:

- Windows® Server 2019
- Windows® Server 2022

Minimum Server Requirements:

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

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



**NOTE:** This software should be installed on a clean windows Server. A clean server 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

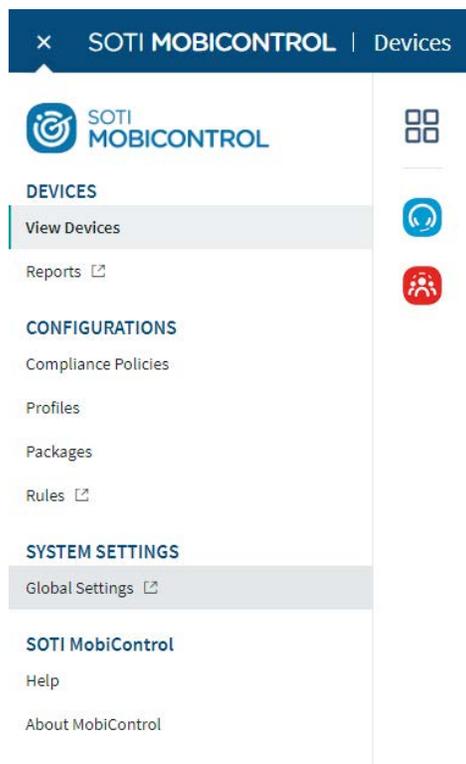
This section provides specific details for the installation of SOTI MobiControl Connector.

## Installation Steps

### Step 1: Create a Printer Administration Server (PAS) in MobiControl

The following installation steps assume you have already installed MobiControl.

1. Log in to the SOTI MobiControl Console using the username and password provided by the SOTII Customer Support.
2. From the top left menu, go to Global Settings.

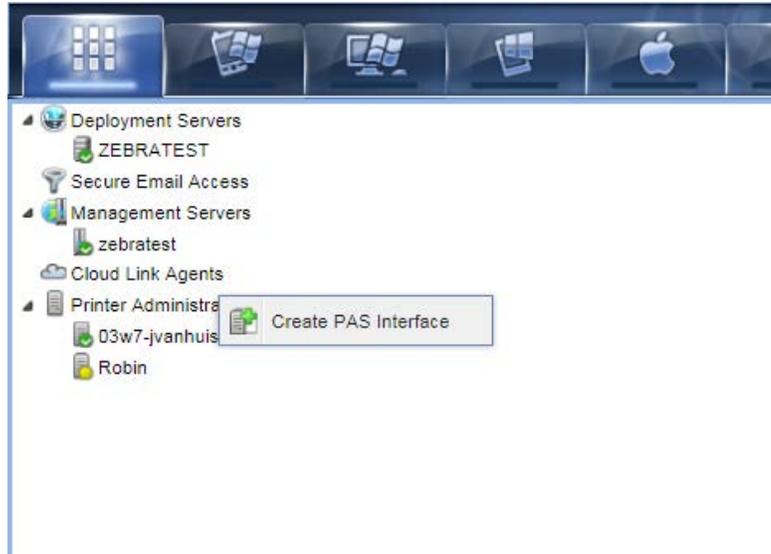


## Installation

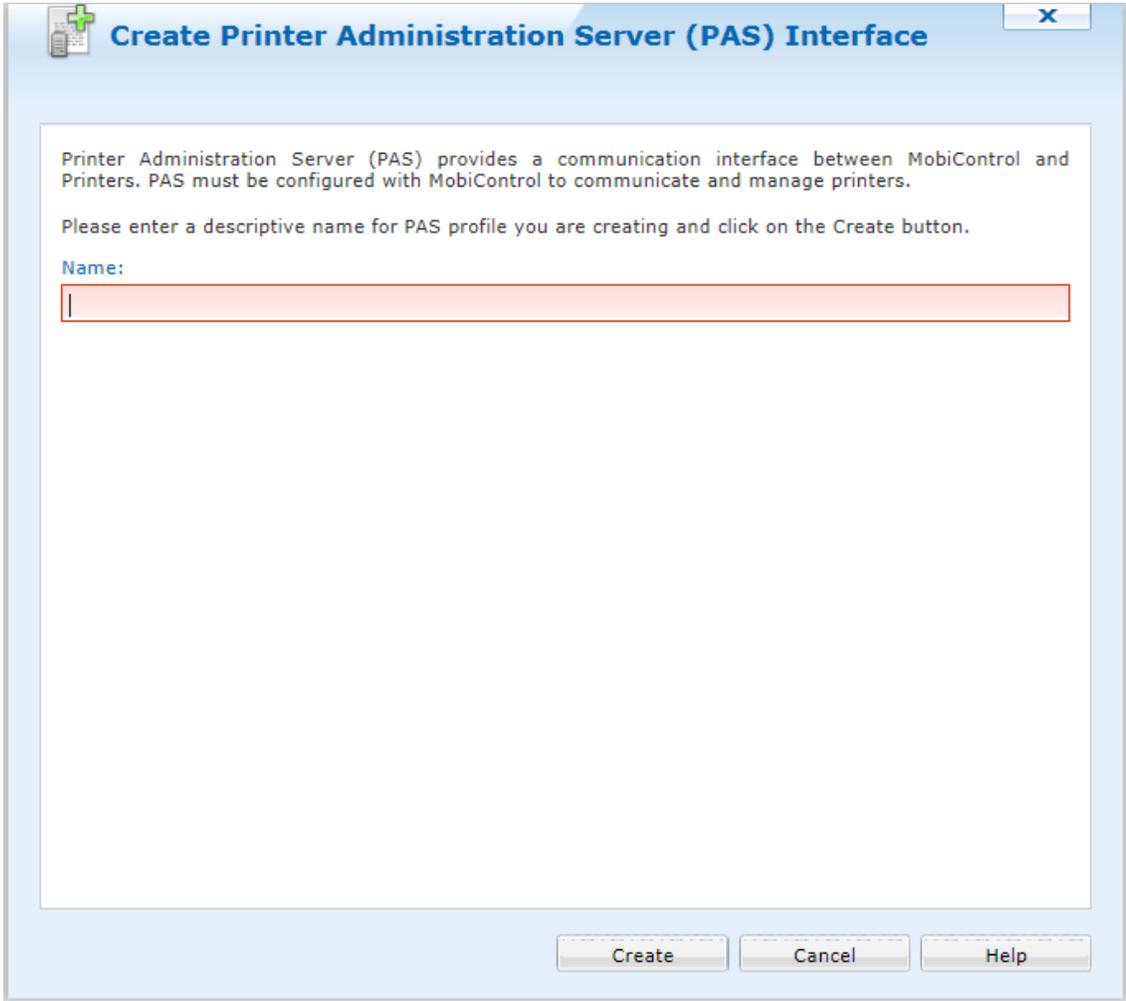
3. At the bottom of the screen, click on **Servers tab**.



4. Right-click on **Printer Administration Servers**, and then click **Create PAS Interface**.



5. Enter a name for the Printer Administration Server (PAS) Profile, and then click **Create**.



**Create Printer Administration Server (PAS) Interface**

Printer Administration Server (PAS) provides a communication interface between MobiControl and Printers. PAS must be configured with MobiControl to communicate and manage printers.

Please enter a descriptive name for PAS profile you are creating and click on the Create button.

**Name:**

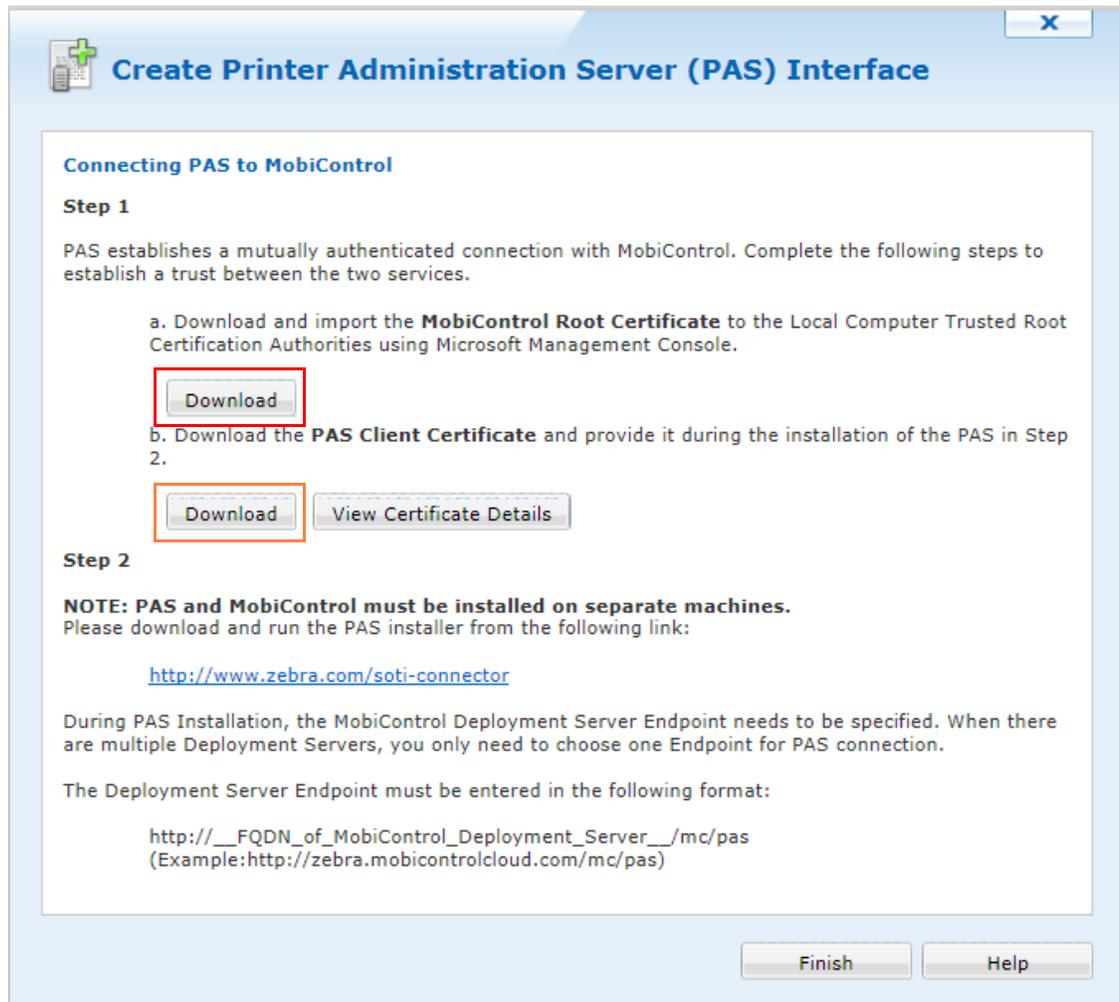
**Create** **Cancel** **Help**

6. In Step 1a, click **Download** ((highlighted in the red box on the following page) to start generating the MobiControl Root Certificate.
7. When prompted, select Save As to save the certificate to the following directory::  
**My Documents\zebra\_certs\**



**NOTE:** You may have to create the directory for the certificate.

8. In Step 1b, click **Download** (highlighted in the orange box below) to start generating the PAS Client Certificate.



9. Create a password to proceed with the download process.



**IMPORTANT:** Be sure to record or write down the password for future reference.



10. Click **Download**.
11. Download the PAS Client Certificate and save it in the following directory::  
     **My Documents\zebra\_certs\**
12. Click **Finish**.

## Step 2: Obtain a Zebra Signed Certificate for the Server

During the installation you will be asked to provide a Zebra certificate. This will be installed on the server and is necessary for the printer to connect to the server. In accordance with industry standards and our recommended security best practices, Zebra shall only issue a SHA-256 signed certificate for use on the server.

 **IMPORTANT:** Zebra shall issue a SHA-256 signed certificate having a 3- year expiration period which will need to be renewed prior to the expiration date. Zebra does not provide a notification service of certificate expiry.

These steps describe how to get a signed SHA-256 certificate from Zebra for the SOTIIMobiControl Connector server.

1. Download and install the latest version of OpenSSL on your computer.
2. Create a folder on your computer named zebra\_certs. This folder may reside anywhere you choose ((e.g. desktop, etc.).
3. From the Start menu, choose "Run" and type cmd.exe to open a Command prompt.



**NOTE:** This step requires that you have administrator privileges.

4. In the Command prompt, navigate to your zebra\_certs folder and type the following commands, pressing Enter after each command. All the following OpenSSL commands should be run in this Command Prompt.

```
set RANDFILE=.rnd
openssl
```

5. Enter the command and substitute the field values for your information::

These are the required certificate fields used in the certificate request generation command:  
**"/C=xx/ST=yyyy/L=aaaa/0=jjjjj/OU=rrrrr/emailAddress=sssss/CN=uuuuu" -key uuuuu.key -out uuuuu.csr**

Where:

**xx is the two-digit ISO Country Code**

**yyyy is the full State name**

**aaaa is the City or Town name**

**jjjjj is the Organization or company name**

**rrrrr is the Organizational unit name**

**sssss is the contact email address for the certificate creator**

**uuuuu is the FQDN of your MobiControl Connector (PAS) server**

Type the following commands followed by Enter. The commands should be entered on a single line.

**NOTE:** zserver.abccompanyinc.com is the FQDN of your MobiControl Connector (PAS) server.





**IMPORTANT:** These commands generate the key which is part of the security for the server communications. It should be kept secure and backed up and not given out to anyone. If unauthorized individuals get the key, the security of the connection between the Zebra printer and the server may be compromised.

```
genrsa -out zserver.abccompanyinc.com.key 2048
```

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

6. Email the certificate request file (.csr) to [softpm@zebra.com](mailto:softpm@zebra.com) and indicate this is for a MobiControl Connector server.
7. The certificate will be signed and sent back to you along with the WeblinkCACHain.crt certificate file.
8. Copy and extract the zip file containing the certificate files to the zebra\_certs folder.
9. This step will create a .p12 file and password (passkey) that will be needed during the installation. Enter the following command and replace the filenames where necessary:

```
pkcs12 -export -in zserver.abccompanyinc.com.crt -inkey zserver.abccompanyinc.com.key -out zserver.abccompanyinc.com.p12 -name tomcat -CAfile WeblinkCACHain.crt -caname root -chain
```

Where: zserver.abccompanyinc.com is the FQDN of your MobiControl Connector (PAS) server.



**NOTE:** This step asks you to set a passkey. Enter standard alphanumeric characters, but do not include any special characters (e.g. do not use characters such as \$, %, &, or @).

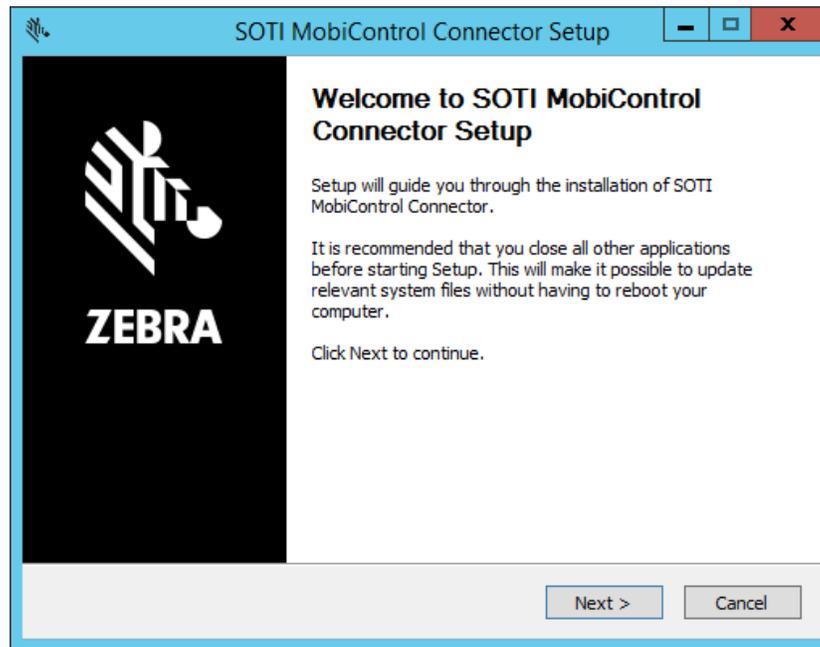


**NOTE:** The passkey should be something easy to remember but should not be distributed to anyone.

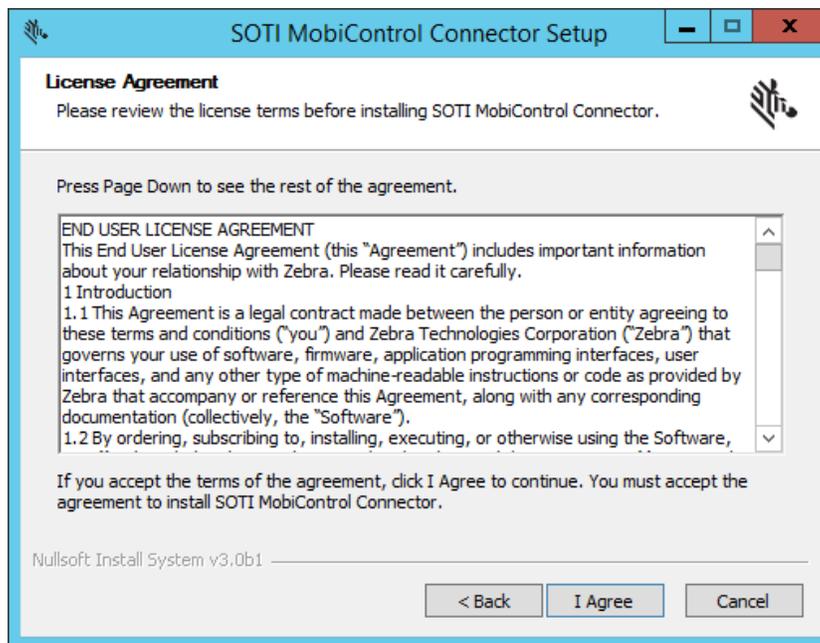
10. The process is complete. You will be prompted for the .p12 file and password during the installation.

## Step 3: Install the SOTI MobiControl Connector

1. Run SotiConnector-v1-x-x.exe.



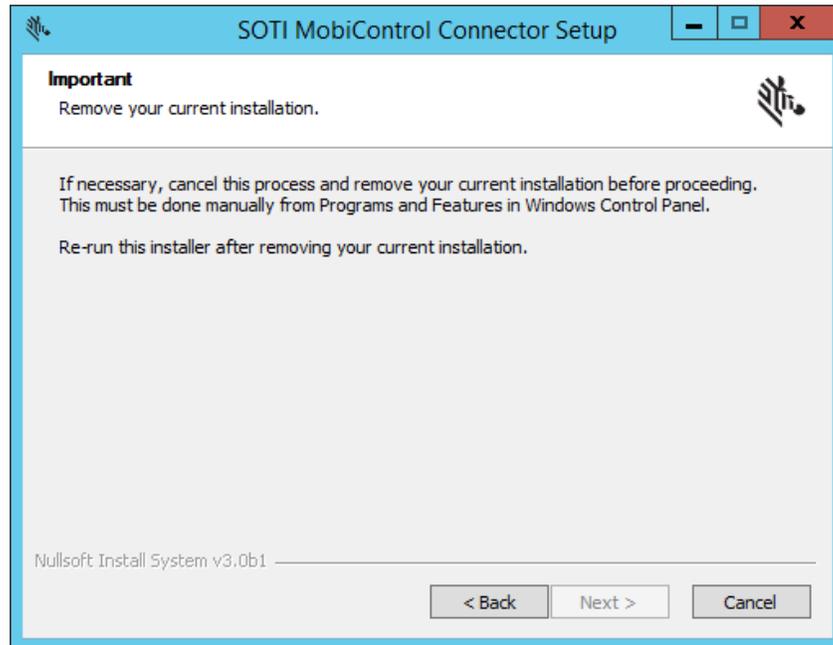
2. Click **Next**.



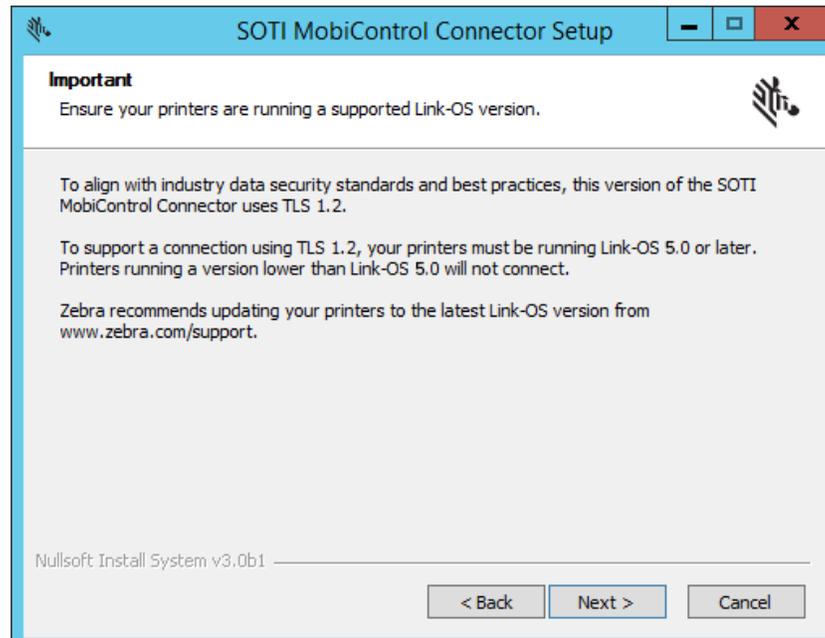
3. Click **I Agree** to accept the terms of the License Agreement.

## Installation

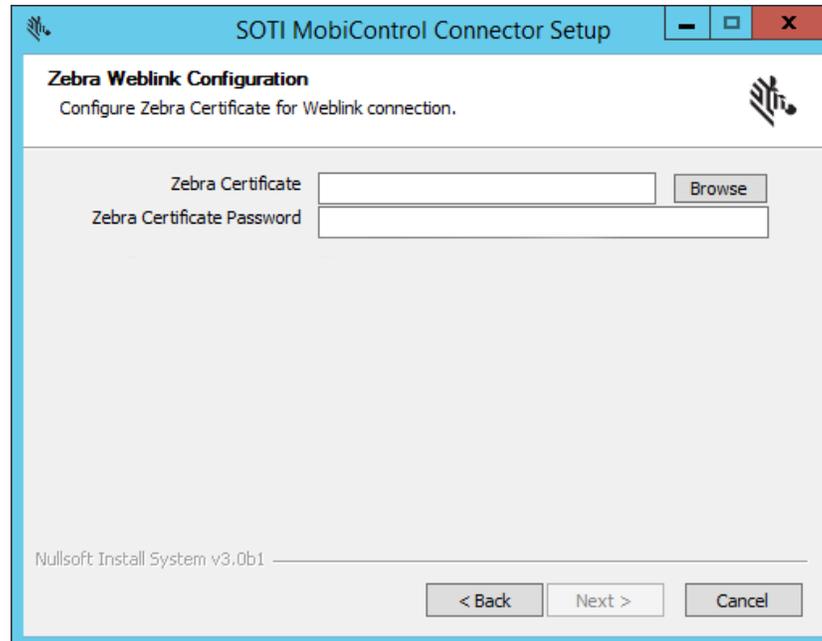
4. Ensure you have removed a previous installation.



5. Ensure you have upgraded all your printers to a supported version of Link-OS.



6. Complete the fields in the Zebra Weblink Configuration dialog below.
  - i. Select the .P12 file created in Step 2.
  - ii. Enter the password used in Step 2.



iii. Click **Next**.

7. Fill in all of the open fields in this form.

The MobiControl Server Location is the Deployment Server End Point to which SOTI MobiControl Connector is connected.

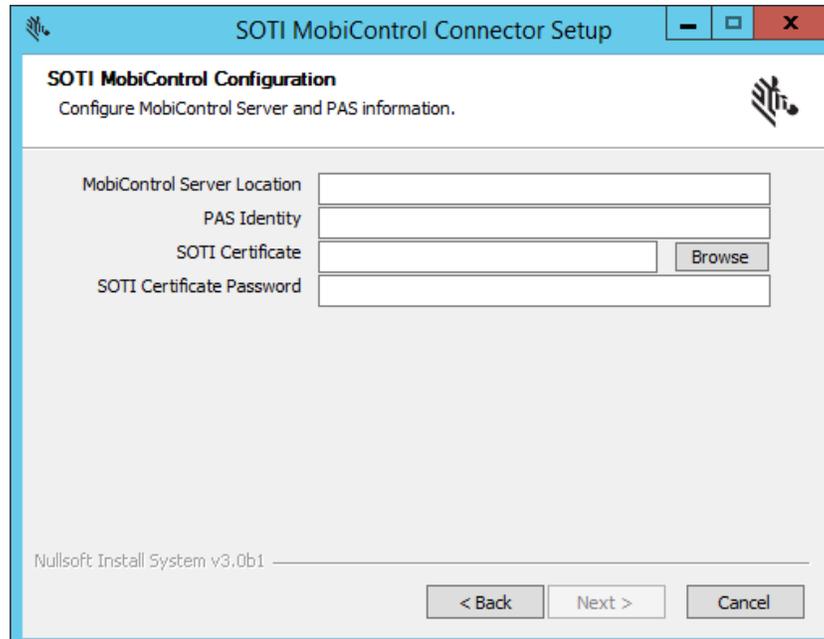
i. The MobiControl Server location is usually going to have the format of your MobiControl Server DNS name followed by **mc/pas** (see the example below).

For example: <http://mobicontrol.com/mc/pas/>

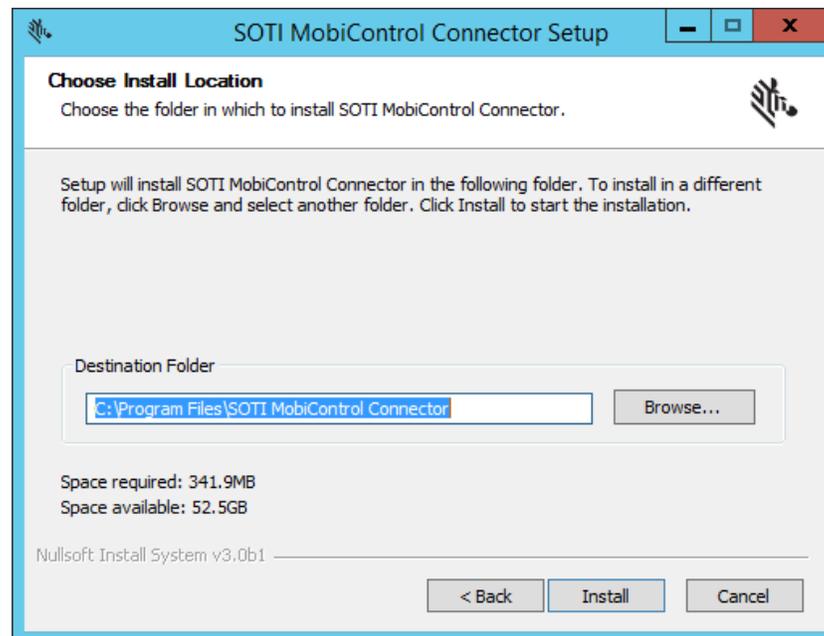
ii. Enter the name of the PAS Server from [step 5 on page 8](#).

iii. The certificate (downloaded in [step 11 on page 10](#)) will be located in the following directory: **My Documents\zebra\_certs\**

iv. Enter the password selected in [step 9 on page 9](#).



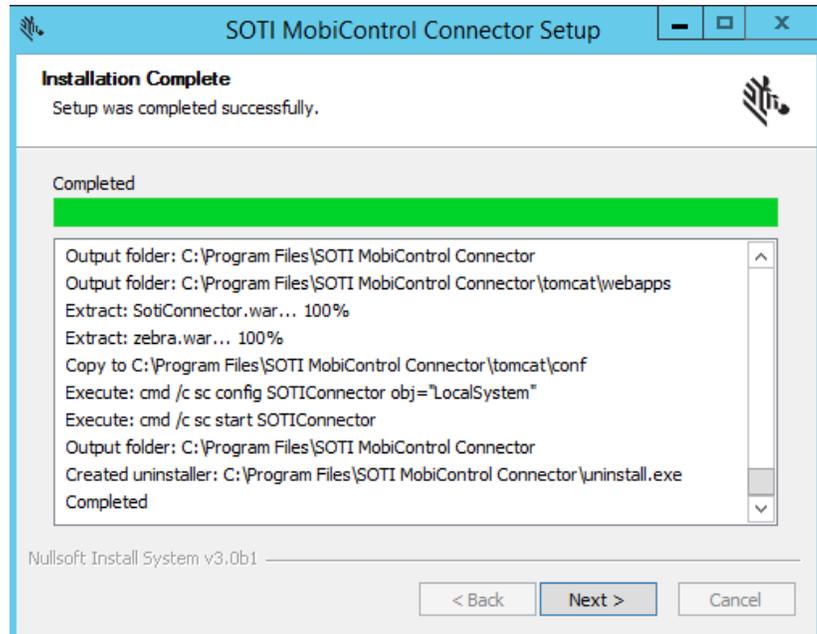
8. Click **Next**.



9. Choose the location where you wish to install the SOTI MobiControl Connector software.

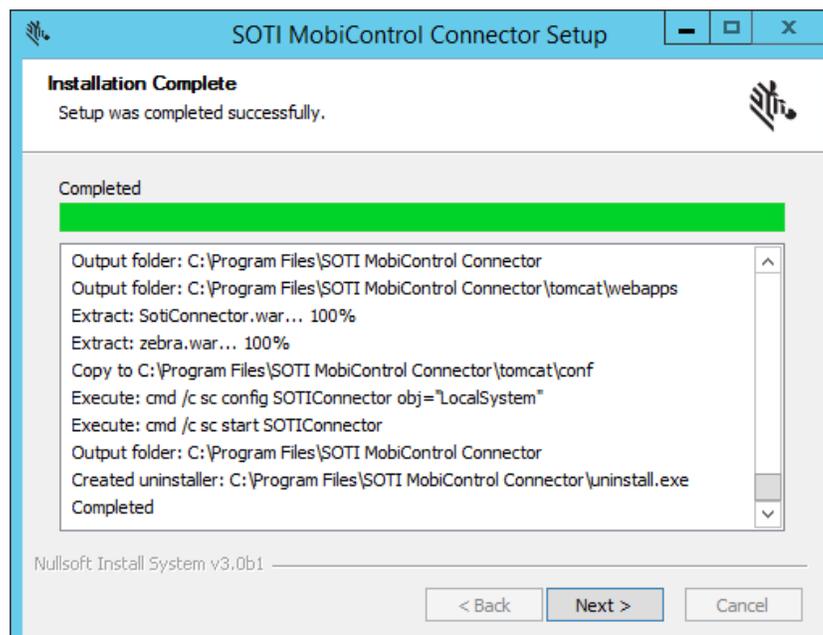
10. Click **Install** to proceed.

# Installation

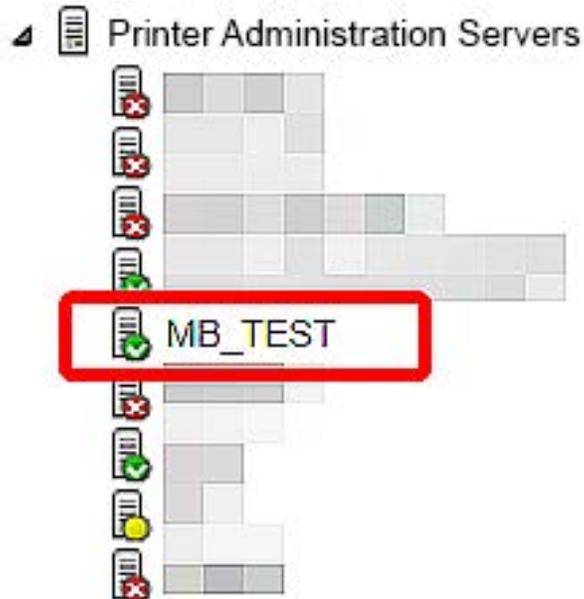


11. Wait for the installation process to complete, and then click **Next**.

12. Click **Finish** to close the Setup Wizard.



13. Verify your PAS is connected to MobiControl as noted by a green check mark where you created the PAS in [step 5 on page 8](#).



## Step 3: Test a Printer

### Enable Printer Discovery

In this section, you must create a "rule" in the SOTI MobiControl Console in order to discover your printers.

1. Click on the **Printer** tab on the SOTI MobiControl Console.

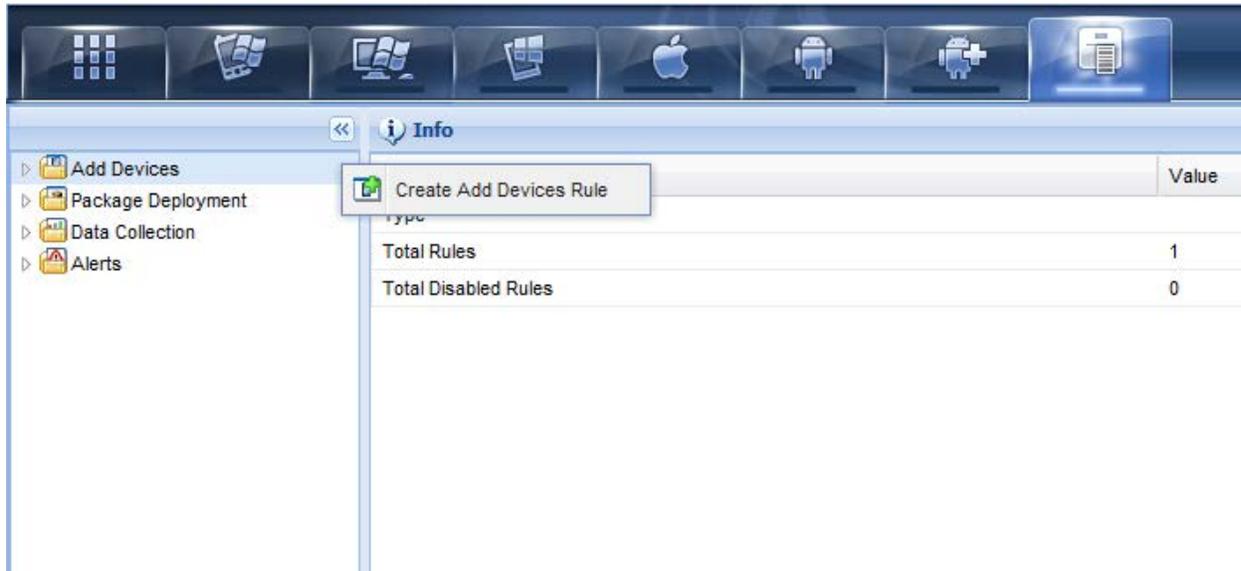


2. Click **Rules** in the task bar on the bottom of the screen.



3. To create a new Add Devices rule:
  - i. Right-click on **Add Devices**.

- ii. Click on **Create Add Devices Rule**.



4. Enter the name of the rule.



**IMPORTANT:** A best practice is to create a default rule to enroll devices automatically. For example, you might choose "Discover Printers" or "Auto Enroll" as the rule name.

**Create Add Devices Rule**

To Add Devices, you need to create an "Add Devices Rule" which allows Printers to be added to specified groups. During creation of "Add Device rule", administrator will be required to specify printer enrollment criteria based on printer properties. Zebra Printers enrolling to MobiControl with matching enrollment criteria will be enrolled to specified device group.

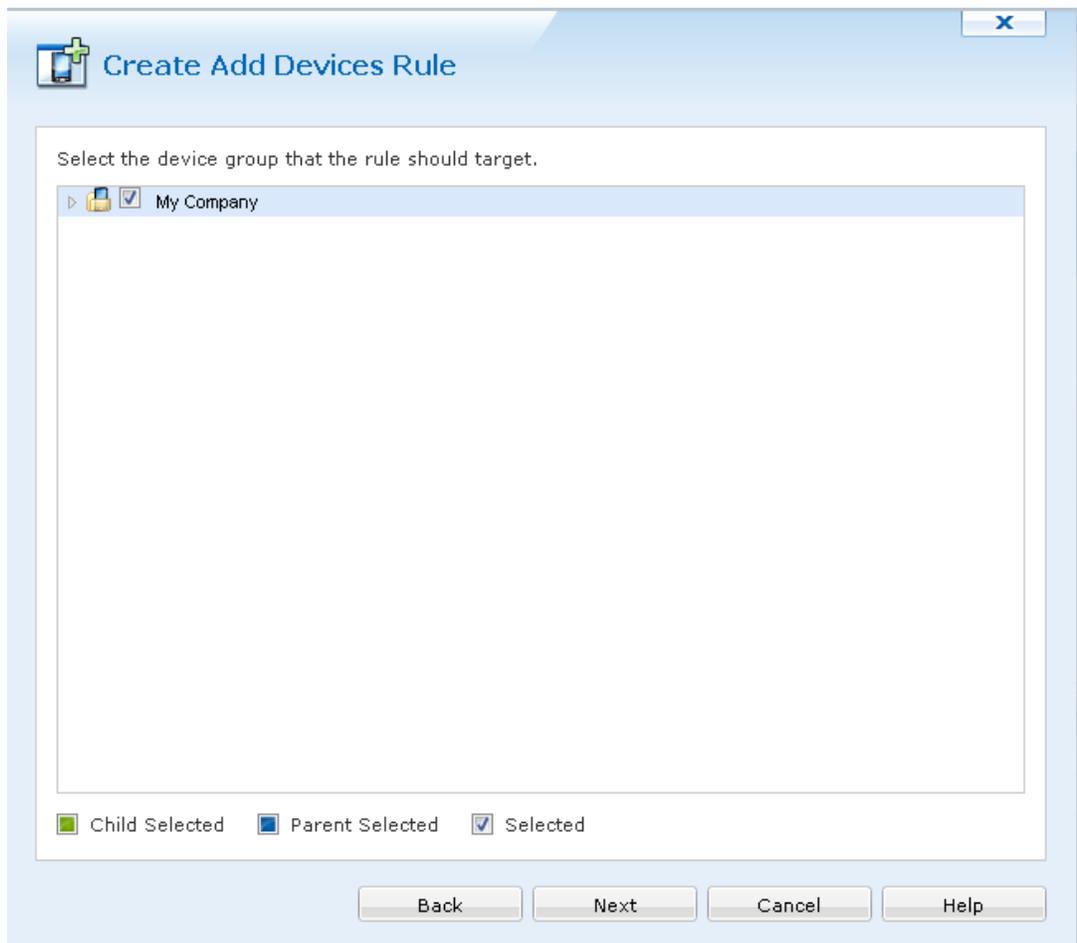
To create a new Add Devices Rule, enter a descriptive name for the Add Devices Rule you are creating and click on the Next button.

Name:

Example: Add Management Devices

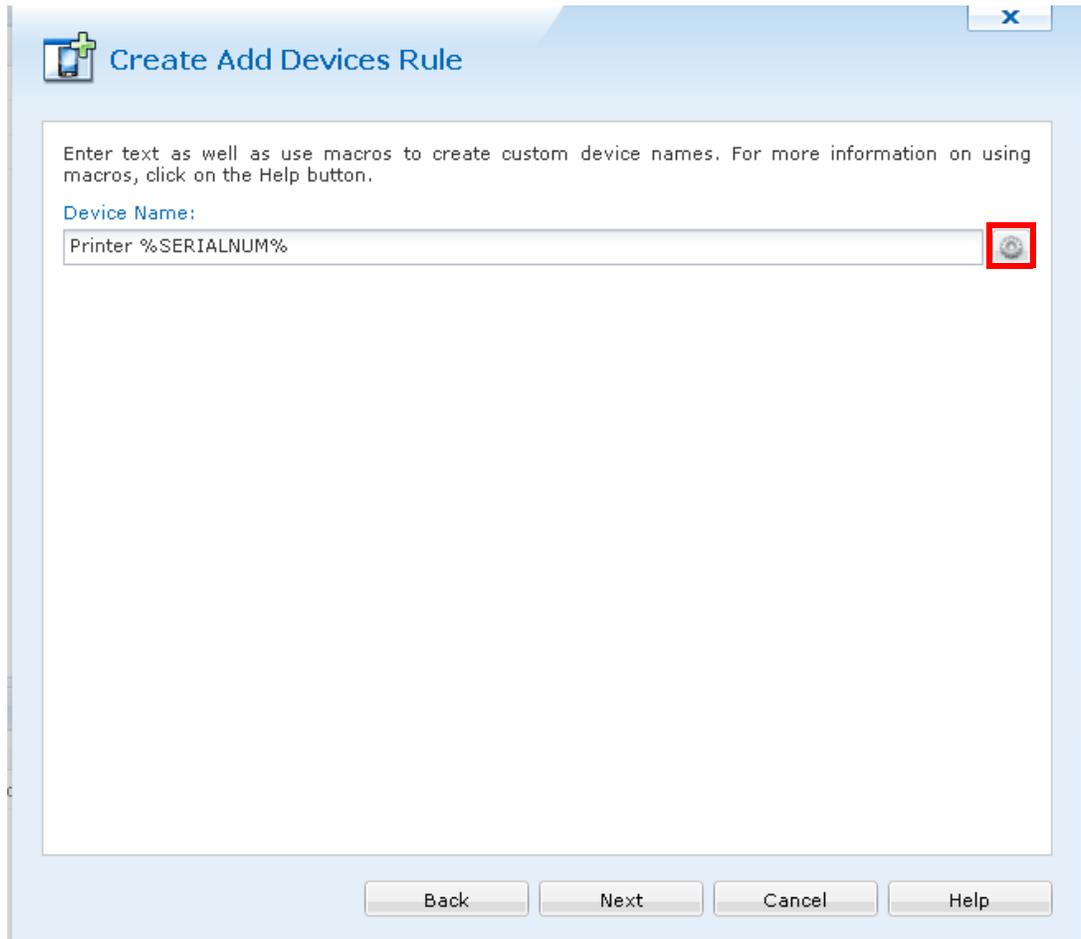
Back Next Cancel Help

5. Select the top level Device Group.



6. Click **Next**.
7. Click **Next** on the Blacklist/Whitelist dialog box.
8. Click **Next** on the Filter dialog box.

9. To change the device name to show the serial number of the printer, click on the gear icon and select **Device Serial Number**.



10. Click **Next**.

11. Review the Create Add Devices Rule information, and click **Finish**.

Name	Value
Type	
Name	auto enroll
Status	Enabled
Activate Date	2014-03-27 10:10:00 AM
Target Device Groups	
	WMy Company\
Device Name	Printer %SERIALNUM%

T...	Date	Time	Message
	2014-03-27	10:29:31 AM	Rule 'auto enroll' created

## Step 4: Set Up Printers

1. Upgrade your printer OS:
  - i. Download the latest operating system for your printers from <https://www.zebra.com/us/en/support-downloads/printers.html>
  - ii. Using the ZDownloader Utility, install the Printer OS on your Zebra printers. (To obtain a copy of the ZDownloader Utility, go to <https://www.zebra.com/us/en/support-downloads/printer-software/zdownloader.html>.)
2. Enrolling printers in SOTI MobiControl
  - i. See the following article on how to configure your printers to communicate with the SOTI MobiControl Connector (PAS): <https://www.soti.net/mc/help/v15.5/en/console/devices/managing/enrollment/printer/printers.html>

# Configuring Printers with WebLink

This section describes basic, network, and firewall configurations for printers connected to SOTI MobiControl Connector.

## 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 25](#).

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/"
```

### 1. 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 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.



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.



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

# Troubleshooting

## Installation Errors

Issue	Reason	Solution
Error when starting Tomcat	Various reasons can cause this error.	See Apache Tomcat website <a href="http://tomcat.apache.org/tomcat-9.0-doc/index.html">http://tomcat.apache.org/tomcat-9.0-doc/index.html</a>
Tomcat Port conflict error	There is another server trying to use the same port as SOTI MobiControl 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.   If you change the port, you must change the <code>weblink.location</code> on the printer. From the Control Panel, open Windows Firewall, Advanced settings, and manually add the Port to the allowed Inbound/Outbound list.
SOTI MobiControl server restarts and the SOTI MobiControl Connector fails to reconnect.	Communication is dropped.	Create a batch file with the string: <b>NET STOP "SOTI MobiControl Connector" &amp;&amp; NET START "SOTI MobiControl Connector"</b>  Create a Windows task to run this batch file approximately 20 minutes after the SOTI MobiControl server restarts.

## Restarting the SOTI MobiControl Connector

1. Navigate to the **Control Panel > Administrative Tools**.
2. Start the **Services** application.
3. Click on the **SOTI MobiControl Connector** service.
4. In the left pane of the screen, click on **Restart the service**.

## Locating the SOTI MobiControl Connector Log File

The SOTI MobiControl Connector Log File is located in the following directory:

**C:\Program Files\SOTI\MobiControl Connector\tomcat\logs\zsoticonnector.log**

## 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
<p>"SSL certificate problem: self signed certificate in certificate chain"</p>	<p>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.</p>
<p>"SSL certificate problem: unable to get local issuer certificate"</p>	<p>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.</p>
<p>"SSL certificate problem: certificate has expired"</p>	<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> 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>app1.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
"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> 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>app1.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>
"subjectAltName does not match 1.2.3.4"	<p>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 <code>'examplecorpinc'</code> and the SAN set to <code>'examplecorpinc.com'</code> or <code>'alias.for.examplecorpinc.com'</code>. 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.</p>
"SSL certificate subject name 'examplecorpinc.com' does not match target host name '1.2.3.4'"	
"Unknown SSL protocol error in connection to ..."	<p>When this message is seen it means that the remote server's SSL/TLS configuration is incorrect. Refer to <a href="#">Troubleshooting on page 31</a> to ensure the server and printer are both configured correctly.</p>
I do not see any of these errors, but the printer still does not connect.	<p>Refer to <a href="#">Troubleshooting on page 31</a> to ensure the server and printer are both configured correctly.</p>

## 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
<p>"Read failed with an unexpected error"</p>	<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> 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.</p>
<p>"Failed to connect (SP = #, CI = #, UW = #, AC = #, PC = #)"</p>	<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 setup according to the Servlet configuration in the Zebra Link-OS SD 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

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.

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??  
Only TLS1.2 is 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.)

```
! 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.

# WebLink Set/Get/Do Commands

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

## 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™

`getvar`

Commands	Details
<code>getvar</code>	<p>This command indicates if one or more of the weblink connections are active.</p> <p><b>Format:</b> ! U1 getvar "weblink.enable"</p> <p><b>Result:</b></p> <ul style="list-style-type: none"> <li>• "yes" if any of the <code>.location</code> values are set</li> <li>• "off" if all connections are disabled</li> </ul>

## 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™™

`setvar`

Commands	Details
<code>setvar</code>	<p>This command adds a single server/username/password triplet to the list of authentication entries.</p> <p><b>Format:</b></p> <pre>! U1 setvar "weblink.ip.conn1.authentication.add" "servername[ username][ password]"  ! U1 setvar "weblink.ip.conn2.authentication.add" "servername[ username][ password]"</pre> <p><b>Values:</b> servername [username][ password] has a maximum length of string is 2048 characters</p> <p><b>Default:</b> NA</p>



**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™™

`getvar`

Commands	Details
getvar	This command lists the server names for the specified connection. <b>Format:</b> <pre>! U1 getvar "weblink.ip.conn1.authentication.entries" ! U1 getvar "weblink.ip.conn2.authentication.entries"</pre>

## 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™

™setvar

Commands	Details
setvar	<p>This command removes a single server/username/password triplet from the list of authenticaiton entries.</p> <p><b>Format:</b></p> <pre>! U1 setvar "weblink.ip.conn1.authentication.remove" "servername" ! U1 setvar "weblink.ip.conn2.authentication.remove" "servername"</pre> <p><b>Values:</b> servername has a maximum length of string is 2048 characters.</p> <p><b>Default:</b> NA</p>



**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™™

setvar, getvar

Commands	Details
setvar	<p>This command enables/disables the weblink IP connection.</p> <p><b>Format:</b></p> <pre>! U1 setvar "weblink.ip.conn1.enable" "value" ! U1 setvar "weblink.ip.conn2.enable" "value"</pre> <p><b>Values</b> "on", "off"</p> <p><b>Default:</b> "off"</p>
getvar	<p>This command retrieves the current setting.</p> <p><b>Format:</b></p> <pre>! U1 setvar "weblink.ip.conn1.enable" ! U1 setvar "weblink.ip.conn2.enable"</pre> <p><b>Result:</b></p> <p>"on" if the connection is enabled</p> <p>"off" if the connection is disabled</p>

## 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
- `setvar`, `getvar`

Commands	Details
<code>setvar</code>	<p>This command sets the server URL for the specified connection.</p> <p><b>Format:</b></p> <pre>! U1 setvar "weblink.ip.conn1.location" "value" ! U1 setvar "weblink.ip.conn2.location" "value"</pre> <p><b>Values</b> any HTTPS URL up to 2048 characters</p> <p><b>Default:</b> ""</p>
<code>getvar</code>	<p>This command returns the server URL currently assigned to the connection.</p> <p><b>Format:</b></p> <pre>! U1 getvar "weblink.ip.conn1.location" ! U1 getvar "weblink.ip.conn2.location"</pre>



### 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™™

setvar, getvar

Commands	Details
setvar	<p>This command sets the maximum number of connections.</p> <p><b>Format:</b></p> <pre>! U1 setvar "weblink.ip.conn1.maximum_simultaneous_connections" "value" ! U1 setvar "weblink.ip.conn2.maximum_simultaneous_connections" "value"</pre> <p><b>Values:</b> Any integer from 1-100</p> <p><b>Default:</b> "10"</p>
getvar	<p>This command retrieves the maximum set number of connections.</p> <p><b>Format:</b></p> <pre>! U1 getvar "weblink.ip.conn1.maximum_simultaneous_connections" ! U1 getvar "weblink.ip.conn2.maximum_simultaneous_connections"</pre>



**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™™

**setvar, getvar, do**

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



**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™™
- `setvar`, `getvar`, `do`

Commands	Details
<code>setvar</code>	<p>This command sets the number of seconds to wait before attempting to reconnect to the server.</p> <p><b>Format:</b></p> <pre>! U1 setvar "weblink.ip.conn1.retry_interval" "value" ! U1 setvar "weblink.ip.conn2.retry_interval" "value"</pre> <p><b>Values:</b> 1 - 600</p> <p><b>Default:</b> "10"</p>
<code>getvar</code>	<p>This command returns the number of seconds to wait between connection attempts.</p> <p><b>Format:</b></p> <pre>! U1 getvar "weblink.ip.conn1.retry_interval" ! U1 getvar "weblink.ip.conn2.retry_interval"</pre>
<code>do</code>	<p>This command sets the number of seconds to wait before attempting to reconnect to the server.</p> <p><b>Format:</b></p> <pre>! U1 do "weblink.ip.conn1.retry_interval" "value" ! U1 do "weblink.ip.conn2.retry_interval" "value"</pre> <p><b>Values:</b> 1 - 600</p> <p><b>Default:</b> "10"</p>

## 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>).

^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™™
- setvar, getvar, do

Commands	Details
setvar	<p>This command sets the URL to hold for testing a connection.</p> <p><b>Format:</b></p> <pre>! U1 setvar "weblink.ip.conn1.test.location" "url" ! U1 setvar "weblink.ip.conn2.test.location" "url"</pre> <p><b>Values:</b> Any HTTPS URL up to 2048 characters  <b>Default:</b> "http://www.zebra.com/apps/linktest"</p>
getvar	<p>This command retrieves the printer's test connection URL.</p> <p><b>Format:</b></p> <pre>! U1 getvar "weblink.ip.conn1.test.location" ! U1 getvar "weblink.ip.conn2.test.location"</pre>
do	<p>This command sets the URL to hold for testing a connection.</p> <p><b>Format:</b></p> <pre>! U1 do "weblink.ip.conn1.test.location" "url" ! U1 do "weblink.ip.conn2.test.location" "url"</pre> <p><b>Values:</b> Any HTTPS URL up to 2048 characters  <b>Default:</b> "http://www.zebra.com/apps/linktest"</p>



**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™™

setevar, getvar, do

Commands	Details
setvar	<p>This command sets the interval for how often a connection to the test.location URL should be attempted.</p> <p><b>Format:</b></p> <pre>! U1 setvar "weblink.ip.conn1.test.retry_interval" "value" ! U1 setvar "weblink.ip.conn2.test.retry_interval" "value"</pre> <p><b>Values</b> 0-1800 (in seconds, providing 0 second - 30 minute interval)</p> <p><b>Default:</b> "900"</p>
getvar	<p>This command retrieves the retry interval.</p> <p><b>Format:</b></p> <pre>! U1 getvar "weblink.ip.conn1.test.retry_interval" ! U1 getvar "weblink.ip.conn2.test.retry_interval"</pre>
do	<p>This command sets the interval for how often a connection to the test.location URL should be attempted.</p> <p><b>Format:</b></p> <pre>! U1 do "weblink.ip.conn1.test.retry_interval" "value" ! U1 do "weblink.ip.conn2.test.retry_interval" "value"</pre> <p><b>Values:</b> 0-1800</p> <p><b>Default:</b> "900"</p>

## 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™™

setvar, getvar, do

Commands	Details
setvar	<p>This command indicate when the test connection should be attempted.</p> <p><b>Format:</b></p> <pre>! U1 setvar "weblink.ip.conn1.test.test_on" "value" ! U1 setvar "weblink.ip.conn2.test.test_on" "value"</pre> <p><b>Values:</b> off, failure, interval, both</p> <p><b>Default:</b> "failure"</p>
getvar	<p>This command retrieves the test connection setting.</p> <p><b>Format:</b></p> <pre>! U1 getvar "weblink.ip.conn1.test.test_on" ! U1 getvar "weblink.ip.conn2.test.test_on"</pre>
do	<p>This command sets when the test connection should be attempted.</p> <p><b>Format:</b></p> <pre>! U1 do "weblink.ip.conn1.test.test_on" "value" ! U1 do "weblink.ip.conn2.test.test_on" "value"</pre> <p><b>Values</b> off, failure, interval, both</p> <p><b>Default:</b> "failure"</p>



**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.

^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™™

`setvar`, `do`

Commands	Details
<code>setvar</code>	<p>This command clears the weblink log entires.</p> <p><b>Format:</b> <code>! U1 setvar "weblink.logging.clear" "value"</code></p> <p><b>Values:</b> Any string value, including an empty string.</p> <p><b>Default:</b> NA</p>
<code>do</code>	<p>This command clears the weblink log entires.</p> <p><b>Format:</b> <code>! U1 do "weblink.logging.clear" "value"</code></p> <p><b>Values:</b> Any string value, including an empty string.</p> <p><b>Default:</b> NA</p>



**Example:** This example clears the weblink log entries with an empty string value.

```
! U1 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™™

`getvar`

Commands	Details
<code>getvar</code>	<p>This command returns a lists of entries in the weblink log.</p> <p><b>Format:</b> ! U1 <code>getvar "weblink.logging.entries"</code></p> <p><b>Values:</b> NA</p> <p><b>Default:</b> " "</p>



**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_entries` 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™™
- `setvar`, `getvar`, `do`

Commands	Details
<code>setvar</code>	<p>This command sets the maximum number of log entires that will be stored.</p> <p><b>Format:</b> ! U1 setvar "weblink.logging.max_entries" "value"</p> <p><b>Values</b> 0 - 10000</p> <p>Setting the value to 0 disables logging.</p> <p><b>Default:</b> "0"</p>
<code>getvar</code>	<p>This command returns the setting for the maximum number of log entries that will be stored.</p> <p><b>Format:</b> ! U1 getvar "weblink.logging.max_entries"</p>
<code>do</code>	<p>This command sets the maximum number of log entires that will be stored.</p> <p><b>Format:</b> ! U1 do "weblink.logging.max_entries" "value"</p> <p><b>Values:</b> 0 - 10000</p> <p>Setting the value to 0 disables logging.</p> <p><b>Default:</b> "0"</p>



**Example:** 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:** 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™™

`getvar`

Commands	Details
<code>getvar</code>	<p>This command retrieves whether any of the weblink settings are modified.</p> <p><b>Format:</b> ! U1 <code>getvar "weblink.printer_reset_required"</code></p> <p><b>Values:</b> "yes" or "no"</p> <p><b>Default:</b> "no"</p>

## 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.

Zebra recommends using Preventive Maintenance kit (p/n 47362 or p/n 105950-035 for a multipack). In place of this kit, you may use a lint-free cloth dipped in 99.7% isopropyl alcohol.



**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™™

`setvar`, `do`

Commands	Details
<code>setvar</code>	This command defaults the weblink branch settings. <b>Format:</b> ! U1 setvar "weblink.restore_defaults" "value" <b>Values:</b> Any value, including an empty string, will default the branch <b>Default:</b> NA
<code>do</code>	This command defaults the weblink branch settings. <b>Format:</b> ! U1 do "weblink.restore_defaults" "value" <b>Values:</b> Any value, including an empty string, will default the branch <b>Default:</b> 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"
```

# Change Log

Version	Date	Changes
1.2x	September 2022	<p>The Tomcat version has been updated to version 9.x</p> <p>The Java version has been updated to version 17.x</p> <p>TLS 1.0/1.1 connections are now disabled so only TLS 1.2 is supported.</p> <p>Zebra no longer issues SHA1 certificates for the printer connection and there is now a manual process to get a Zebra-signed SHA256 certificate.</p> <p>Library versions have been updated in the SotiConnector.war and Zebra.war components.</p> <p>Due to the changes listed above, the minimum required Link-OS version in the printer is now 5.0.</p>

