Instruction

Z-Ware 7.18.x Web Server Installation Guide

Document No.:	INS14486
Version:	15
Description:	Z-Ware Web Server Installation, Configuration, Administration & Building Guide
Written By:	KAJAROSZ;MIKOZIK;ADGIELNI;JFR;MASZPIEC
Date:	2022-05-30
Reviewed By:	JCC;SCBROWNI;TRBOYD;PINOWOBI;ABUENDIA;JFR
Restrictions:	Public

Approved by:				
Date	CET	Initials	Name	Justification
2022-05-30	06:14:14	NTJ	Niels Johansen	

REVISION RECORD

Doc. Ver.	Date	By	Pages affected	Brief description of changes
1	20181126	AYY	2.5, 2.7, 7.1	Removed reference of BBB in Z-Ware build and configuration commands.
2	20190306	AYY	1.1, 2.1, 6.3, 7.1, References	V7.11.0: changed Rpi reference to 3B+ with respective URL and images. Removed Ubuntu 14.04 support and updated dependency list for Ubuntu 16.04. Added firmware backup section.
3	20190532	SNA		V7.11.1: No change
4	20191128	SNA		V7.13.0; No change
5	20200110	SNA		V7.13.1 - no changes
6	20200326	AYY	3.4.1, 3.4.2, 3.4.3 4, 4.1	Change @sigmadesigns.com email example to @silabs.com example Remove reference to Openldap
7	20200610	JFR	Front page	Typo
8	20200629	SCBROWNI	All	Tech Pubs Review
8	20200703	MIKOZIK	All	Change title to 7.14.x
9	20201124	KAJAROSZ	3, 4, 5, 6, 10, 11, 14, 15, 17, 19, 20, 21	Change title to 7.15.x, target deployment systems, installation procedure, paths zwarelocal -> zware, zwave_device_rec.txt path, remove description for zwareportal, remove memcached service description, build platforms, move 7.3 to 7.1, remove 7.5
10	20201130	SCBROWNI	All 3.4.3	Tech Pubs Review Fixed broken cross-reference
11	20201202	MIKOZIk	Front Page, 3.4.3	Fixed revision numer Removed Note 2 referencing the section 3.1.5. Email Settings (portal only) removed in previous revisions
12	20201214	KAJAROSZ	2.5	Update release package naming
13	20210518	MIKOZIK	All	Bump version to 7.16.x
14	20211122	KAJAROSZ	Cover, 6	Bump version to 7.17.x. Remove duplicate
15	20220525	KAJAROSZ	1	Change version to 7.18.x

Table of Contents

Table of Tables

1 INTRODUCTION

1.1 Purpose

Z-Ware Web Server (see [1]) can be built on a Linux PC for 2 targets:

- Linux PC
- RPi3B+ (Raspberry Pi 3 Model B+ board, See https://www.raspberrypi.org/products/raspberry-pi-3-model-b-plus/)

The document covers the Installation, Configuration, Administration, and Building of Z-Ware Web Server for these targets.

1.2 Audience and Prerequisites

Z-Wave Partners who are familiar with:

- ZIPGW (Z-Wave over Internet Protocol Gateway)
- Z-Ware Web User Guide
- Linux Administration

2 Installation

2.1 Deployment Systems

The web server is tested on Ubuntu 18.04.5 LTS 64-bit, Ubuntu Mate 18.04.5 32-bit and RPi3B+. RPi3B+ version is tested with Raspbian 9 (stretch) OS. During RPi3B+ installation, the installation configuration will automatically handle the differences between BeagleBone Debian and Raspbian OS.

2.2 Runtime Package Dependencies

The following is the list of required dependency packages in addition to the ones that get installed by default as part of the OS distribution.

- gettext
- ia32-libs (applicable only for 64-bit OS and needed only when 32-bit version of this software is required to run in 64-bit OS)
- sendmail-bin (needed only when SMTP Server is not used)
- rsyslogd (needed only when logging via syslog is used)
- binutils (needed only for LTS Server version)

2.3 User Privilege

The deployment user should not be ‘root’ but must have super user privileges via sudo.

2.4 Selection of Deployment Directory

The absolute path name of the deployment directory must not contain white spaces.

2.5 Installation (Deployment) Procedure

1) If this software is already installed and one or more services running, stop those services. Refer to the ‘Service Management’ section to find instructions on shutting down the services.
2) Change directory to the path where the installer is placed:

```
cd /home/<user>/installer/
```

3) Extract the contents of the installer. Use one of the following commands depending on the OS type – 64 bit or 32 bit:

```
tar -zxvf zware-v.vv.v-x86_64.tar.gz      # (64-bit)
tar -zxvf zware-v.vv.v-i386.tar.gz        # (32-bit)
```

```
tar -zxvf zware-v.vv.v-rpi.tar.gz          # (32-bit)
```

where: *v.vv.v* is the zware web server version.

4) For PC installation, start installation by specifying the deployment path:

```
cd zware-v.vv.v-x86_64      # OR cd zware-v.vv.v-i386
./install.sh /home/<user>/zware/
```

On a fresh RPi3B OS, run the following command, and Z-Ware will auto configure RPi3B OS network and the ZIPGW config file:

```
cd zware-v.vv.v-rpi/
./install.sh --configure-rpi /home/<user>/zware/
```

For reinstallation of Z-Ware on RPi3B or if RPi3B OS network configuration and the ZIPGW config file modification are not desired, run the following command:

```
cd zware-v.vv.v-rpi/
./install.sh /home/<user>/zware/
```

'sudo' password for the user shall be prompted.
System configurations shall be prompted, if there were no previous configurations or if there were an additional set of configurations after an update of this software. Refer to the 'System Configuration' section for details on various configuration options.

2.6 Install Time Only Configurations

These settings are only available during installation.

2.6.1 Upstart Settings

This determines whether various Z-Ware services should be added to system 'upstart' service manager.

Table 2-1: Upstart Settings

Z-Ware Service	Option	Default
zware-http	Y/N	N
zware-portal	Y/N	N

2.6.2 Autostart Setting

This determines if Z-Ware is auto-started on system boot.
Setting: Enable this package to be auto started after system boot up?
Option: Y/N
Default: Y for RPi3B, N for PC platform

2.7 Software License

The license applicable for the software is placed at the following location. Licenses applicable to external (third-party) software are pointed to from this file.

<install-path>/LICENSE

Here, <install-path> is the deployment directory in deployment machine which is usually /home/<user>/zware/.

3 System Configuration

Web server system configuration is performed as part of installation (See 2). If a change in system configuration is required in an existing installation, perform the following steps:

1) Change to deployment directory in the deployment machine:

```
cd /home/<user>/zware/
```

2) Get system configuration from user:

```
./config/config-config.sh
```

The texts shown between square brackets [ ] indicate current configuration values. Pressing just the 'Enter/Return' key at the prompt retains the current configuration value. The texts shown between less-than and greater-than symbols < > indicate comments. The texts separated by pipe symbols | indicate the valid set of values for a given configuration item. If the options are given as (y|n), the character 'y' indicates 'yes' and the character 'n' indicates 'no'.

3) Stop selected or all services depending on the set of configuration parameters being changed. Refer to the 'Service Management' section to find instructions on shutting down the services.

4) Apply the system configuration in various configuration files:

```
./config/configure.sh
```

5) Start the stopped services. Refer 'Service Management' section to find instructions on starting the services.

3.1 Configuration Description

The following is a description of various configuration settings.
For each of these settings, a list of services is listed against 'Services to restart'. For the changes in a given set of configuration settings to take effect, the corresponding set of these services must be stopped before running the "configure.sh" script and started again afterwards. Refer to the 'Service Management' section for instructions on stopping and starting services.

3.1.1 System Settings

Table 3-1: System Settings

Setting	Option	Default
Hostname	<string>	zware-portal.com
Services to restart: httpd		

Hostname is the network label that identifies the deployment machine. Usually, this is set to the name with which the web service shall be hosted. If not already set, a FQDN hostname is suggested.		
Target Configuration	debug|release	release
Services to restart: httpd, zwportald		
This setting helps to select the tradeoff between ease of debugging and better performance. The 'debug' configuration selects debug versions of Z-Ware Portal Daemon and Z-Ware Web thus enabling extensive logging for easier debugging. The 'release' configuration selects release versions of Z-Ware Portal Daemon and Z-Ware Web thus going with minimal logging and improved performance.		

3.1.2 Z-Ware Portal Daemon Settings

Services to restart: zwportald

Table 3-2: Z-Ware Portal Daemon Settings

Setting	Option	Default
Log Target	console|release	console
The 'console' setting results in logging to a file. The 'syslog' setting results in sending the log to LOG_USER facility of rsyslogd. Refer manual of rsyslogd for more information.		
Log Rotate Size	Eg. 100, 100k, 100M, 100G	500M
Size above which the Portal Daemon log is rotated. The setting must be a valid value for 'size' directive in logrotate configuration file. The size check is done every 5 minutes (*/etc/cron.d/logrotate*)		
Z-Ware Portal Http server - Access Log Rotate Size	Eg. 100, 100k, 100M, 100G	10M
Size above which Apache server access log is rotated. The setting must be a valid value for 'size' directive in logrotate configuration file. The size check is done every 5 minutes (*/etc/cron.d/logrotate*)		
Z-Ware Portal Http server - Error Log Rotate Size	Eg. 100, 100k, 100M, 100G	10M
Size above which Apache server error log is rotated. The setting must be a valid value for 'size' directive in logrotate configuration file. The size check is done every 5 minutes (*/etc/cron.d/logrotate*)		
Z-Ware Portal Zweb - Access Log Rotate Size	Eg. 100, 100k, 100M, 100G	10M
Size above which Zweb access log is rotated. The setting must be a valid value for 'size' directive in logrotate configuration file. The size check is done every 5 minutes (*/etc/cron.d/logrotate*)		

Z-Ware Portal Zweb - Error Log Rotate Size	Eg. 100, 100k, 100M, 100G	10M
Size above which Zweb error log is rotated. The setting must be a valid value for 'size' directive in logrotate configuration file. The size check is done every 5 minutes (*/etc/cron.d/logrotate*)		
Server Initial Thread Count	<number>	10
This parameter sets the initial number of worker threads that can service concurrent requests from Z-Ware Web (FastCGI). This value will also be used as the maximum number of idle worker threads. This value decides how well the daemon responds to sudden spike in the number of concurrent users. Lower values (when number of concurrent users is high) shall result in longer latency response time for a short period of time until the required number of additional worker threads are made available. Higher values (when number of concurrent users is low) shall result in unused (idle) worker threads occupying system resources wastefully for longer period of time.		
Server Maximum Thread Count	<number>	50
This parameter sets the maximum number of worker threads that can service concurrent requests from Z-Ware Web (FastCGI). This value provides an upper limit for the number of worker threads to have control over the daemon's impact on overall system load. Lower values (when number of concurrent users is high) shall result in longer latency response time for a long period of time. Higher values (when number of concurrent users is low) typically does not have any adverse impact. But, if there is spike in the number of concurrent users, there shall be spike in overall system load and thus also starving other processes.		
Z-Wave Report Wait Timeout	<number>	11
This parameter sets the time (in seconds) to wait for a Z-Wave Report from the Z-Wave node to which a Z-Wave Get command is sent. Note: The value for this setting must be *at most* a few seconds less than the value for 'Portal Receive Timeout' setting of Z-Ware Web. Lower values for this setting shall increase the likelihood of older report values being sent in the response. This is especially true for Z-Wave nodes that take longer time to respond with a Z-Wave Report. In such cases, typically the newer report values are carried by subsequent Passive Get calls from the UI. Since Passive Get calls are sent periodically, the end result shall be slower UI reaction time for the expected report values. Higher values for this setting shall result in worker threads being occupied for longer duration thus increasing the worker thread count. In a severe case, this may even hit the 'Server Maximum Thread Count'. The problem is aggravated by more number of Z-Wave nodes that take longer time to respond with a Z-Wave Report.		

3.1.3 Z-Ware Web Settings

Table 3-3: Z-Ware Web Settings

Setting	Option	Default
Portal Receive Timeout	<number>	15
Services to restart: httpd		
This parameter sets the time (in seconds) for which Z-Ware Web (FastCGI) shall wait for Z-Ware Portal Daemon to respond to its request. Note: The value of this setting must be *at least* a few seconds more than the value for 'Z-Wave Report Wait Timeout' setting of Z-Ware Portal Daemon. Lower values for this setting shall force lower values for 'Z-Ware Report Wait Timeout' setting of Z-Ware Portal Daemon. So the corresponding impact mentioned under its section applies. Higher values for this setting shall result in FastCGI processes being occupied for longer duration thus increasing the number of FastCGI processes. In a severe case, this count may hit the maximum limit for the number of FastCGI processes.		

3.1.4 HTTP Server Settings

Table 3-4: HTTP Server Settings

Setting	Option	Default
Use Secure HTTP?	y|n	y
Services to restart: httpd		
The option 'y' enables HTTPS in the web server. The option 'n' disables HTTPS in the web server thus supporting only unsecure HTTP.		

3.1.5 Operating System Common CA Certificate Configuration

Table 3-5: Operating System Common CA Certificate Settings

Setting	Option	Default
Operating System Common CA certificates directory	<String>	/etc/ssl/certs
Services to restart: httpd		
This parameter specifies the directory where Operating System Common CA certificates can be found. Every Operating System is likely to have installed the 'ca-certificates' package. In Ubuntu, these CA certificates are installed in the directory: /etc/ssl/certs/. When PHP attempt TLS/SSL connection with SMTP server, PHP will try to verify the SMTP server certificate is been signed by a valid certificate authority (CA).		

3.1.6 SSL Settings

These setting will only be used when no official HTTPS certificate is available.

Table 3-6: SSL Settings

Setting	Option	Default
CA Certificate DN Organization (O)	<String>	Certification Authority Name
This setting is to specify the 'Organization' (O) of Certification Authority.		
CA Certificate DN Organizational Unit (OU)	<String>	Certification Authority Name
This setting is to specify the 'Organizational Unit' (OU) of Certification Authority.		
CA Certificate DN Common Name (CN)	<String>	Certification Authority Name
This setting is to specify the 'Common Name' (CN) of Certification Authority.		
CA Certificate Validity	<Number>	5000
This setting is to specify the number of days for which a generated CA certificate is valid.		
CA Key Length	<Number>	2048
This setting is to specify the length (in bits) of a generated CA key.		
Portal Certificate DN Organization (O)	<String>	Company Name
This setting is to specify the 'Organization' (O) of Portal Service Provider.		
Portal Certificate DN Organizational Unit (OU)	<String>	Portal
This setting is to specify the 'Organizational Unit' (OU) of Portal Service Provider.		
Portal Certificate DN Common Name (CN)	<String>	<hostname>
This setting is to specify the 'Common Name' (CN) of Portal Service Provider.		
Portal Certificate Validity	<Number>	5000
This setting is to specify the number of days for which a generated Portal Service Provider certificate is valid.		
Portal Key Length	<Number>	2048
This setting is to specify the length (in bits) of a generated Portal Service Provider key.		

3.2 Secure HTTP

The web server expects the security related files in the following locations under the deployment folder (/home/<user>/zware/).

Table 3-7: SSL File Locations

File	Location
Server Certificate	install/httpd/conf/Z-Wave/ssl.crt/<hostname>.crt
Server Key	install/httpd/conf/Z-Wave/ssl.key/<hostname>.key
CA Certificate	install/httpd/conf/Z-Wave/ssl.ca.crt/<hostname>.ca.crt
CA Key	install/httpd/conf/Z-Wave/ssl.ca.key/<hostname>.ca.key

<hostname> is the 'Hostname' given during installation or configuration of this software.
Server Certificate and Server Key are minimal requirements for enabling secure HTTP. If Server Certificate is signed by using a Certificate Authority, the corresponding CA Certificate shall also be placed under the relevant directory.
Though a CA Key is needed for signing the Server Certificate, the CA Key itself is not needed for the working of the secure server. In fact, the CA Key should not be placed anywhere in the deployment system due to security considerations.
If a Server Certificate and/or Server Key is not present for the configured Hostname, when Apache httpd service is started, a prompt is shown to check if Server Key and Server Certificate can be generated. If a CA Certificate and CA Key are present in the expected location, they are used to sign the generated Server Certificate.
Server Certificates, Server Keys, and CA Certificates are installed for the following hostnames. Since these files are bundled within the installer and Server Certificates being self-signed, these are not meant to be used directly in any serious deployment.

- zware-portal.com
- zipr.sigmadesigns.com

Note: If the Server Certificate is not signed by any CA, a security warning message will be thrown by the web client (browser) indicating that the certificate is not trusted because it is self-signed.
Note: If the Server Certificate is signed by a CA Key and CA Certificate that are locally generated, a security warning message will be thrown by the web client (browser) indicating that the certificate is not trusted because the issuer is not trusted.
The ideal solution is to use certificates obtained from SSL certificate providers like Symantec (Verisign) or DigiCert. The CA certificates of such providers are typically included in most browsers out-of-the-box as trusted CA certificates.

3.3 Certificate and Key Generation

The self-signed, security-related files can be directly generated using the following commands after changing to the deployment directory (/home/<user>/zware/).
The following command generates Server Certificate and Server Key:

```
./install/openssl/scripts/ssl-certificate-generate.sh <certificate-path> <key-path> [<CA-certificate-path> <CA-key-path>]
```

<certificate-path> is the generated Server Certificate.
<key-path> is the Server Key. If already present, it is used. Otherwise it is also generated.
<CA-certificate-path> is the CA Certificate. If it is not present, CA signing is skipped.
<CA-key-path> is the CA Key. If it is not present, CA signing is skipped.
The following command generates CA Certificate and CA Key:

```
./install/openssl/scripts/ssl-ca-certificate-generate.sh <CA-certificate-path> <CA-key-path>
```

<CA-certificate-path> is the generated CA Certificate.
<CA-key-path> is the generated CA Key.
Generating your own CA Certificate and CA Key is not recommended for any serious deployment.

3.4 Scenes Configuration

Scenes configuration file zwscenes.conf can be found at the following location:
install-path>/install/zwportald/var/networks/zwscenes.conf
The format of this file is as follows:

```
[GROUP 1]
key1=value1
key2=value2
[GROUP 2]
key1=value1
…
```

The valid groups and keys are described below.

3.4.1 Group: SECURITY SCENE NOTIFICATION EMAIL

This group contains settings of the Security Scenes email feature.

Table 3-8: Security Scene Notification Email Settings

Key	Value	Description
enable	<true | false>	Enable or disable Security Scenes sending notification email
sender	<string>	Sender's email address

Example:

```
[SECURITY SCENE NOTIFICATION EMAIL]
enable=true
sender=example@silabs.com
```

3.4.2 Group: SECURITY SCENE NOTIFICATION SMS

This group contains settings of the Security Scenes SMS (text message) feature.

Table 3-9: Security Scene Notification SMS Settings

Key	Value	Description
enable	<true | false>	Enable or disable Security Scenes sending notification SMS
sender	<string>	Sender's email address
gateway	<string>	Email to SMS gateway server

The gateway will be used to send SMS using <number>@<gateway> format where the number would be given in a Security Scene while the gateway must be defined in zwscene.conf.
If the number is +6512345678 and the configuration file contains “gateway=onewaysms.asia”, then libzwscene will send an email to +6512345678@onewaysms.asia.
Example:

```
[SECURITY SCENE NOTIFICATION SMS]
enable=true
sender=example@silabs
gateway=onewaysms.asia
```

3.4.3 Group: SMTP

This group contains settings of SMTP.

Table 3-10: Scene SMTP Settings

Key	Value	Description
enable	<true | false>	Enable or disable Security Scenes sending SMS
auth_enable	<true | false>	Enable SMTP authentication
username	<string>	SMTP username
password	<string>	SMTP user’s password
server_hostname	<string>	SMTP server’s hostname/IP address
server_port	<number>	SMTP server’s port number
secure_method	<string>	Security method e.g. tls

Security Scenes email for notification email or SMS through email-to-SMS gateway can be sent either via local installation of “sendmail” program or via an external SMTP server.
If key “enable” in group SMTP is true, then the Security Scenes email is sent via the SMTP server.
If key “auth_enable” is true, then authentication information (username and password) is used to authenticate with the SMTP server.
Example:

```
[SMTP]
enable=true
auth_enable=true
username=example@silabs.com
password=_Pass100
server_hostname=smtpcorp.com
server_port=2525
secure_method=tls
```

NOTE 1: When key “enable” in group “SMTP” is true, then values of key “sender” in group “SECURITY SCENE NOTIFICATION EMAIL” and “SECURITY SCENE NOTIFICATION SMS” do not matter as the sender’s address will always be the SMTP user only.

This means that, when using “sendmail” to send email, we can have different senders for email and SMS, but, when using SMTP, the sender to both would be the same as we only have a single connection to the the SMTP server.

3.5 Device-Specific Configuration and Information Database

The device-specific configuration and information database is used by Z-Ware to compensate (early versions of) devices that do not provide supported device types or properties. In addition, it also includes configuration settings for the devices during inclusion or even at run time. The device database configuration file, `zwave_device_rec.txt`, can be found at the following location:

<install-path>/install/zwportald/etc/zwave_device_rec.txt

The database file adopts a standard JSON format to enable easy editing by the user- See [2].

4 Service Management

Two services must be up and running to use the Z-Ware Local – Apache HTTP Server and Z-Ware Portal Daemon.

- Change to deployment directory in the deployment machine:

```
cd /home/<user>/zware/
```

- To start/stop/restart all services:

```
./service/service.sh start|stop|restart
```

  One of these actions is applied on all services.
- To start/stop/restart Z-Ware Portal Daemon:

```
./service/service-zwportald.sh start|stop|restart
```

- To start/stop/restart Apache HTTP Server:

```
./service/service-httpd.sh start|stop|restart
```

The above scripts first try to start the services using upstart. If this fails, the scripts fall back by trying to launch the services on their own.
Z-Ware services launched via upstart have a re-spawn mechanism – that is, when a service is found to be down, upstart launches it again. This is to mitigate the impact of application crashes in an unattended deployment setup. So, 'killing' the services directly does not guarantee that the service is shut down. When a service is started via upstart, its shutdown is guaranteed only when it is stopped via upstart.

4.1 Managing Services Directly Using Upstart

The following commands are applicable if Z-Ware services are added to 'upstart' service manager. This is done during installation only if the user accepts installation of upstart scripts under the '/etc/init/' directory.

- To start/stop/restart Apache HTTP Server, use one of the following commands:

```
sudo start|stop|restart|status zware-http
sudo service zware-http start|stop|restart|status
sudo initctl start|stop|restart|status zware-http
```

- To start/stop/restart Z-Ware Portal Daemon, use one of the following commands:

```
sudo start|stop|restart|status zware-portal
sudo service zware-portal start|stop|restart|status
sudo initctl start|stop|restart|status zware-portal
```

4.2 Auto Start Z-Ware Service after System Boot

During installation, the user has an option to enable the auto-start Z-Ware service every time after system boot. If the target platform is a PC, the option will be default OFF.

5 Log Files

<install-path> in this section is the deployment directory in the deployment machine, which is usually /home/<user>/zware/.
Five log files (Z-Ware portal daemon log, Z-Ware Web error log and access log, Apache server error log and access log) will be monitored by Logrotate of the system. Once a particular log file reaches the size defined during the configuration stage, Logrotate will “rotate” the log file by renaming the file with a “.1” extension. The subsequent log messages will be logged into a new log file with the original file name. Currently, at most, only one extra “rotation” will be kept. This means that, when the new log file reaches the configured size again, the old “.1” extension file will be deleted and the new log file will be renamed with a “.1” extension. The interval for Logrotate to check the file size is five minutes.

5.1 Z-Ware Portal Daemon

When the ‘Log Target’ setting is 'console', the daemon logs the messages at the following location:

<install-path>/install/zwportald/var/log/zwportald.log

When the ‘Log Target’ setting is 'syslog', the daemon logs the messages at syslog’s LOG_USER facility. By default, rsyslogd logs them at the following location:

/var/log/syslog

The location of this log file may change depending on the configuration of rsyslogd. The log file may also be rotated and compressed. Refer to the manual for rsyslogd.

5.2 Z-Ware Web (CGI)

The error log for the Z-Ware Web is at the following location:

<install-path>/install/zweb/logs/error_log

The access log for the Z-Ware Web is at the following location:

<install-path>/install/zweb/logs/access_log

5.3 Apache HTTP Server

The error log for the HTTP Server is at the following location:

<install-path>/install/httpd/logs/error_log

The access log for the HTTP Server is at the following location:

<install-path>/install/httpd/logs/access_log

6 User Interface (Web)

The web interface can be accessed at:

http://<hostname>/

<hostname> is the name assigned to the deployment machine using a name service like DNS. Any IP address by which the deployment machine is reachable shall also be used. But, the browser may throw security warning messages because of a mismatch between the hostname and CN in the certificate.

6.1 Security

When 'y' is selected for the "Use Secure HTTP?" configuration option, even when the browser accesses unsecure URL (HTTP), it gets redirected to a secure URL (HTTPS). Depending on the security settings in the web server, the browser shall throw security warnings. Some such cases are as follows:

- The server certificate is self-signed.
- The server certificate is not signed by a trusted Certificate Authority (CA).
- The common name (CN) in the certificate does not match the host name.

In a test setup, it may be fine to proceed further by ignoring such warnings and accepting the risks. But, in a production setup, such warnings are typically not acceptable and would require an appropriate fix in the web server.

6.1.1 HTTPS Server Certificate

The first time Z-Ware service starts, it will check the server certificates, and, if there are not any, it will auto-generate self-signed certificates according to the domain names specified during the installation/configuration.
If the official server certificates are available, they should be placed / replaced in the following location:

<install-path>/install/httpd/conf/zwave/ssl.ca.crt/<domain-name>.ca.crt
<install-path>/install/httpd/conf/zwave/ssl.crt/<domain-name>.crt
<install-path>/install/httpd/conf/zwave/ssl.key/<domain-name>.key

Z-Ware also supports Letsencrypt HTTPS certificates by default. It will look at the default location for Letsencrypt certificates at

/etc/letsencrypt/live/<domain-name>/cert.pem

If official server certificates exist in the above location, Z-Ware will create a symbolic link in the installation path to the Letsencrypt certificates instead of copying the certificates over to facilitate the certificate renewal process.

6.2 Firmware Update

The firmware files to be used for updating devices using the 'Firmware Update Meta Data' command class are to be placed under the following directory location:

<install-path>/install/zwportald/var/firmwares/

Here, <install-path> is the deployment directory in the deployment machine, which is usually /home/<user>/zware/.

6.3 Firmware Backup

The firmware files generated/backup from devices using the 'Firmware Update Meta Data' command class will be placed under the following directory location:

<install-path>/install/zwportald/var/firmwares_backup/

Here, <install-path> is the deployment directory in the deployment machine, which is usually /home/<user>/zware/.

7 Building

7.1 Platforms

Release builds are generated in two Docker environments:

- Ubuntu 18.04.5 LTS amd64 – for 64 bit PC and RPI3B+ targets,
- Ubuntu 18.04.5 LTS i386 – for 32 bit PC target.

Z-Ware Server for RPi3B+ is cross-compiled using the gcc-linaro-6.2.1 toolchain. The toolchain will be automatically downloaded and configured properly should the user follow the build procedure. For backward compatibility, the old build and configuration commands with 'beaglebone' keyword will still be working.

7.2 Dependencies

```
$ apt-get install -y build-essential git curl wget python sudo rsync doxygen cmake libtool autoconf default-jre-headless g++ unzip pkg-config patch gettext libglib2.0-dev-bin zlib1g-dev flex bison bc groff texinfo patchelf zip
```

7.3 User Privilege

The (build) user in build machine needs to have root privilege via sudo.

7.4 Building from source code

1) Change directory to the source bundle:

```
cd /home/<user>/zwportal/
```

2) To build for target platforms 'x86-64' or 'i386' on PC, run the main build script as follows:

```
./build/build.sh local [rpi] [parallel] [debug]
```

[rpi] builds the RPi3B version, or the PC version otherwise. This should prompt for a sudo password. System configurations (like hostname etc) will be prompted for, if there were no previous configurations or if there were additional set of configurations after an update of this software (See Section 3).
[parallel] enables parallel compilation for faster machine (eg. Machine with multiple CPUs and > 1GRAM).

3) Build the installer

```
./build/build-installer.sh
```

The installer will be created automatically for the given product type.

1) To fully clean up the generated files and folders during the build process and restore the project to a fresh check-out state, add the "fullclean" keyword, e.g.,

```
./build/build.sh local fullclean
```

If the project is already in clean state, it may prompt for configuration settings before executing the clean procedure.

5) For clean rebuild by component:

```
zwportald:
        rm -rf compile/zwave/zwportald
        ./build/build-zwportald.sh
zweb:
        rm -rf compile/zwave/zweb/
        ./build/build-zweb.sh
openssl:
        rm -rf compile/openssl*
        ./build/build-openssl.sh
```

References

[1] Silicon Labs, INS14428, INS, Z-Ware Web User Guide
[2] Silicon Labs, INS14416, INS, Z-Ware Library User Guide