Wireless access controllers
WLC-15, WLC-30, WLC-3200, WLC-3250, WLC-3350, vWLC

Firmware version update guide
Firmware version 1.42.0

Contents

1 Introduction 4
1.1 Abstract 4
1.2 Target audience 4
1.3 Symbols 4
1.4 Notes, warnings and information 5
2 Files used for the update 6
3 Creating a backup copy of the current configuration 7
3.1 Preparation 7
3.2 Copying the configuration backup file 7
3.2.1 Using remote file copy protocols 7
3.2.2 To a locally connected USB/MMC storage 9
4 Restoring configuration from a backup 10
4.1 Preparation 10
4.2 Copying configuration backup file 10
4.2.1 Using remote file copy protocols 10
4.2.2 From locally connected USB/MMC media 12
4.3 Applying and confirming the loaded configuration 13
5 Checking the current firmware version and secondary bootloader (U-boot) version 14
5.1 Checking current firmware version and version of the secondary bootloader (U-boot) in the main firmware CLI 14
5.2 Checking the current firmware version and the version of the primary (sbi, bl1) and secondary (U-boot) bootloaders in the output of the console interface when loading the service router 14
6 Firmware update via CLI of the WLC main firmware 16
6.1 Firmware update from version 1.39.2 to 1.42.0 16
6.2 Firmware update from version 1.39.1 to 1.39.2 17
6.3 Firmware update from version 1.36.4 to 1.39.1 18
6.4 Firmware update from version 1.36.3 to 1.36.4 19
6.5 Firmware update from version 1.36.2 to 1.36.3 20
6.6 Firmware update from version 1.30.8 to 1.36.2 21
6.7 Firmware update from version 1.30.6 to 1.30.8 22
6.8 Firmware update from version 1.30.4 to 1.30.6 23
6.9 Firmware update from version 1.30.2 to 1.30.4 24
6.10 Firmware update from version 1.30.0 to 1.30.2 25
6.11 Firmware update from version 1.26.1 to 1.30.0 26
6.12 Firmware update from version 1.19.2 to 1.26.1 27
6.13 Firmware update from version 1.19.1 to 1.19.2 27

6.14 Firmware update from version 1.19.0 to 1.19.1 28
6.15 Firmware update from version 1.15.3 to 1.19.0 29
6.15.1 Secondary bootloader update 32
6.16 Preparation for firmware upload 35
6.17 Firmware upload 36
6.17.1 Using one of the remote file upload protocols 36
6.17.2 Using USB/MMC media 37
6.18 Selecting version 1.39.2 firmware image for the next upload 38
7 Rebooting the controller 40

1 Introduction

1.1 Abstract

This guide provides instructions on how to update the firmware components of the WLC series controllers, considering the specific models and previous firmware versions of the device being update.

1.2 Target audience

This guide is intended for technical personnel who perform device updates through the command line interface (CLI).

1.3 Symbols

Designation	Description
[ ]	In the command line, optional parameters are shown in square brackets; when entered, they provide additional options.
{ }	In the command line, mandatory parameters are shown in curly braces. Select one of the parameters.
«,» **«-»**	In the command description, these characters are used to define ranges.
«|»	In the description of the command, this sign means 'or'.
Semibold font	Notes, warnings, or information are shown in bold.
<Semibold italic>	Keyboard keys are shown in bold italic within angle brackets.
`Text box`	Examples and results of the commands are given within the text boxes.

1.4 Notes, warnings and information

Notes contain important information, tips or recommendations on device operation and setup.

Warnings inform users about hazardous conditions which may cause injuries or device damage and may lead to the device malfunctioning or data loss.

The information block contains information on the use of the device.

2 Files used for the update

Depending on the model and update component, the following files should be used later in the guide body:

WLC model	HW version	Firmware <firmware-file>	Secondary bootloader <uboot-file>	Primary bootloader <xload-file>
WLC-15	all	wlc15-1.42.0-build9.firmware	wlc15-1.42.0-build9.uboot	none
WLC-30	all	wlc30-1.42.0-build10.firmware	wlc30-1.42.0-build10.uboot	none
WLC-3200	all	wlc3200-1.42.0-build9.firmware	wlc3200-1.42.0-build9.uboot	wlc3200-1.42.0-build9.bdk
WLC-3250	all	wlc3250-1.42.0-build9.firmware	wlc3250-1.42.0-build9.uboot	wlc3250-1.42.0-build9.ebf
WLC-3350	all	wlc3350-1.42.0-build10.firmware	wlc3350-1.42.0-build10.uboot	wlc3350-1.42.0-build10.ebf
vWLC	—	vwlc-1.42.0-build6.firmware	—	—

3 Creating a backup copy of the current configuration

Prior to initiating the firmware update on WLC controllers, it is necessary to create a backup of the current configuration. Copying the current configuration from the WLC controllers is possible both using remote file copying protocols and to locally connected USB/MMC media.

When migrating from a newer version of the firmware to an older one (downgrade), it is possible that the older version of the firmware will not be able to apply the configuration saved in the newer version. As a result, the configuration will be lost and the WLC controller will boot with an empty configuration.

3.1 Preparation

To create a backup copy of the current configuration of the controller using remote file copy servers, do the following:

1. Start the corresponding server on the PC/server in the network.
2. Provide the ability to save files in the server working directory.
3. Provide IP connectivity between the upgdated WLC controller and the remote file copy server (routing).
4. Ensure operation of the remote copy protocol between the WLC and the remote file copy server (intermediate firewalls).
5. If necessary (for ftp, sftp, scp, http protocols), find out the username and password to write the required file.

To create a backup copy of the current configuration of the service router on a locally connected USB/MMC storage:

1. Format USB/MMC partition as FAT32.
2. Connect the USB/MMC storage to the appropriate WLC slot.

3.2 Copying the configuration backup file

3.2.1 Using remote file copy protocols

Depending on the remote file copy protocol, one of the following commands must be executed in the CLI of the controller:

Configuration backup via TFTP protocol

```
wlc# copy system:running-config tftp://<tftp-server-ip>:/<config-file-name>
```

Configuration backup via FTP protocol

```
wlc# copy system:running-config ftp://<ftp-username>:<ftp-userpassword>@<ftp-server-ip>:/<config-file-name>
```

Configuration backup via SFTP protocol

```
wlc# copy system:running-config sftp://<sftp-username>:<sftp-userpassword>@<sftp-server-ip>:/
<config-file-name>
```

Configuration backup via SCP protocol

```
wlc# copy system:running-config scp://<scp-username>:<scp-userpassword>@<scp-server-ip>:/<config-
file-name>
```

Configuration backup via HTTP protocol

```
wlc# copy system:running-config http://<http-username>:<http-userpassword>@<http-server-ip>:/
<config-file-name>
```

- <config-file-name> – file name with which the current configuration of the controller will be saved;
- <tftp-server-ip> – IP address of the TFTP server in use;
- <ftp-username> – user name on the FTP server;
- <ftp-userpassword> – user password on the FTP server;
- <ftp-server-ip> – IP address of the FTP server in use;
- <sftp-username> – user name on the SFTP server;
- <sftp-userpassword> – user password on the SFTP server;
- <sftp-server-ip> – IP address of the SFTP server in use;
- <scp-username> – user name on the SCP server;
- <ftp-userpassword> – user password on the FTP server;
- <scp-server-ip> – IP address of the SCP server in use;
- <http-username> – user name on the HTTP server;
- <http-userpassword> – user password on the HTTP server;
- <http-server-ip> – IP address of the HTTP server in use.

3.2.2 To a locally connected USB/MMC storage

1. Define the volume label of the connected USB/MMC storage.

Defining the volume label name on a USB storage

```
wlc# show storage-devices usb
Name                          Filesystem  Total, MB   Used, MB    Free, MB
----------------------------  ----------  ----------  ----------  ----------
<USB_DISK>                    vfat        7664.01     6391.69     1272.32
```

Defining the volume label name on a MMC storage

```
wlc# show storage-devices mmc
Name                          Filesystem  Total, MB   Used, MB    Free, MB
----------------------------  ----------  ----------  ----------  ----------
<MMC_DISK>                    vfat        7664.01     6391.69     1272.32
```

2. Copy the file to the USB/MMC storage that is currently in use.

⚠ When executing copy commands to USB/MMC media, instead of the <USB_DISK> or <MMC_DISK> fields, use the real volume labels defined in step 1.

Configuration backup to USB storage

```
wlc# copy system:running-config usb://<USB_DISK>:/<config-file-name>
|****************************************| 100% (576B) Success!
```

Configuration backup to MMC storage

```
wlc# copy system:running-config mmc://<MMC_DISK>:/<config-file-name>
|****************************************| 100% (576B) Success!
```

- <config-file-name> – file name with which the current configuration of the controller will be saved;
- <USB_DISK> – partition name on the USB storage;
- <MMC_DISK> – partition name on the MMC storage.

4 Restoring configuration from a backup

In case of configuration loss on the controller due to operational issues, firmware update, or rollback to a previous firmware version, the controller configuration can be restored using a previously created backup copy.

Copying a configuration backup to the WLC controllers is possible both using remote file copying protocols and to locally connected USB/MMC media.

When migrating from a newer version of the firmware to an older one (downgrade), it is possible that the older version of the firmware will not be able to apply the configuration saved in the newer version. As a result, the configuration will be lost and the WLC controller will boot with an empty configuration. If the configuration is empty, the controller can only be connected to using a console connection and the default login/password (admin/password).

4.1 Preparation

To restore the configuration of the service router from a backup copy using remote file copy servers, do the following:

1. Start the corresponding server on the PC/server on the network.
2. Place the file with the previously created backup copy of the controller in the server working directory.
3. Configure the controller to establish IP connectivity with the remote file copy server.
4. Provide IP connectivity between the updated WLC controller and the remote file copy server (routing).
5. Ensure operation of the remote copy protocol between the WLC and the remote file copy server (intermediate firewalls).
6. If necessary (for ftp, sftp, scp, http protocols), find out the username and password to write the required file.

To restore the controller configuration from a backup copy from a locally connected USB/MMC storage, do the following:

1. Format USB/MMC partition as FAT32.
2. File with a previously created backup copy of the controller configuration must be placed on the USB/MMC media.
3. Connect the USB/MMC storage to the appropriate WLC slot.

4.2 Copying configuration backup file

4.2.1 Using remote file copy protocols

Depending on the protocol for remote file copying, run one of the following commands in the CLI of the controller:

Configuration backup via TFTP protocol

```
wlc# copy tftp://<tftp-server-ip>:/<config-file-name> system:candidate-config
```

Configuration backup via FTP protocol

```
wlc# copy ftp://<ftp-username>:<ftp-userpassword>@<ftp-server-ip>:/<config-file-name>
system:candidate-config
```

Configuration backup via SFTP protocol

```
wlc# copy sftp://<sftp-username>:<sftp-userpassword>@<sftp-server-ip>:/<config-file-name>
system:candidate-config
```

Configuration backup via SCP protocol

```
wlc# copy scp://<scp-username>:<scp-userpassword>@<scp-server-ip>:/<config-file-name>
system:candidate-config
```

Configuration backup via HTTP protocol

```
wlc# copy http://<http-username>:<http-userpassword>@<http-server-ip>:/<config-file-name>
system:candidate-config
```

- <config-file-name> – name of the service router configuration backup file;
- <tftp-server-ip> – IP address of the TFTP server in use;
- <ftp-username> – user name on the FTP server;
- <ftp-userpassword> – user password on the FTP server;
- <ftp-server-ip> – IP address of the FTP server in use;
- <sftp-username> – user name on the SFTP server;
- <sftp-userpassword> – user password on the SFTP server;
- <sftp-server-ip> – IP address of the SFTP server in use;
- <scp-username> – user name on the SCP server;
- <ftp-userpassword> – user password on the FTP server;
- <scp-server-ip> – IP address of the SCP server in use;
- <http-username> – user name on the HTTP server;
- <http-userpassword> – user password on the HTTP server;
- <http-server-ip> – IP address of the HTTP server in use.

4.2.2 From locally connected USB/MMC media

1. Define the volume label of the connected USB/MMC storage.

Defining the volume label name on a USB storage

```
wlc# show storage-devices usb
Name                          Filesystem  Total, MB   Used, MB    Free, MB
----------------------------  ----------  ----------  ----------  ----------
<USB_DISK>                    vfat        7664.01     6391.69     1272.32
```

Defining the volume label name on a MMC storage

```
wlc# show storage-devices mmc
Name                          Filesystem  Total, MB   Used, MB    Free, MB
----------------------------  ----------  ----------  ----------  ----------
<MMC_DISK>                    vfat        7664.01     6391.69     1272.32
```

2. Copy the file to the USB/MMC storage that is currently in use:

⚠ When executing copy commands to USB/MMC media, instead of the <USB_DISK> or <MMC_DISK> fields, use the real volume labels defined in step 1.

Configuration backup to USB storage

```
wlc# copy usb://<USB_DISK>:/<config-file-name> system:candidate-config
|****************************************| 100% (576B) Success!
```

Configuration backup to MMC storage

```
wlc# copy mmc://<MMC_DISK>:/<config-file-name> system:candidate-config
|****************************************| 100% (576B) Success!
```

- <config-file-name> – name of the controller configuration backup file;
- <USB_DISK> – partition name on the USB storage;
- <MMC_DISK> – partition name on the MMC storage.

4.3 Applying and confirming the loaded configuration

To apply and confirm operation of the configuration loaded earlier in the 'system:candidate-config' section, run the following commands:

Configuration backup to MMC storage

```
wlc# commit
Configuration has been successfully applied and saved to flash. Commit timer started, changes
will be.
wlc# confirm
Configuration has been confirmed. Commit timer canceled.
```

5 Checking the current firmware version and secondary bootloader (U-boot) version

Currently used secondary bootloader (U-Boot) and main firmware versions can be checked:

- in the CLI of the main firmware;
- in the console interface output when loading the controller.

5.1 Checking current firmware version and version of the secondary bootloader (U-boot) in the main firmware CLI

To check the current firmware version and the version of the secondary bootloader (U-boot) in the CLI of the main firmware, execute the **show version** command:

Obtaining secondary bootloader and main firmware versions in CLI

```
wlc# show version

Boot version:

 1.15.3.3 (date 14/11/2022 time 13:30:27)                 <-- secondary bootloader (U-Boot)
version

SW version:

 1.15.3 build 3[a813b5c65] (date 14/11/2022 time 13:20:25) <-- active image version of the
controller main firmware

HW version:

 1v2                                                      <-- hardware version of the controller
```

5.2 Checking the current firmware version and the version of the primary (sbi, bl1) and secondary (U-boot) bootloaders in the output of the console interface when loading the service router

To check the current firmware version and the version of the secondary bootloader (U-boot) in the output of the console interface when loading the controller, do the following:

1. Connect to the WLC controller via the Console interface on the front panel of the controller using the following parameters of the PC RS-232 interface:

- Baud rate: 115200 bps;
- Data bits: 8 bits;
- Parity: no;
- Stop bits: 1;
- Flow control: no.

2. Reboot the controller using one of the following methods:

- Switch the power off and then switch it back on. The interval between switching off and on must be at least 20 seconds. Briefly press the function button F on the front panel of the controller.
- Execute the **reload system** command in the CLI of the main firmware of the controller.

Reboot using a command in the main firmware CLI

```
WLC# reload system
Do you really want to reload system ? (y/N): y
```

3. During the loading, information about the versions will be displayed in the console:
   - Primary bootloader (sbi, bl1 depending on the controller model):

Primary bootloader version on WLC-15

```
SBI:1.17.3.11 (14/11/2022 - 12:55:55)
  Chip is NSP B1
  Booting from SPI-NOR
```

Primary bootloader version on WLC-30

```
NOTICE: Cold boot
NOTICE: BL1:1.15.3.2 (28/12/2022 - 15:56:46)
```

Primary bootloader version on WLC-3200

```
BRCM XLP Stage 1 Loader (X-Loader:1.17.3.11) [Big-Endian] (14/11/2022 - 13:21:58)
XLP316B2: Node 0 frequency: CPU=1400MHz, SOC=1999MHz, REF=133MHz
POWER ON RESET CFG:43F94FA8,VRM: 0x6868, PRID: 0xC1104
```

   - Secondary bootloader (U-boot):

Secondary bootloader version

```
NOTICE: BL31:1.15.3.2 (28/12/2022 - 15:56:46)
U-Boot:1.15.3.2 (28/12/2022 - 15:56:46)
```

   - Main firmware version:

Main firmware version:

```
[ 0.000000] Booting Linux on physical CPU 0x0
[ 0.000000] Software version: 1.15.3 build 3[2555a4e8a] date 28/12/2022 time 17:44:53
```

6 Firmware update via CLI of the WLC main firmware

6.1 Firmware update from version 1.39.2 to 1.42.0

Before updating, use the **show date** command to verify that the correct date and time are set on the device.
If an incorrect date is set on the controller, certificate validation will prevent the configuration changes from being applied after the update.

Firmware version 1.42.0 is cumulative (it contains updated versions of the primary and secondary loaders), so it will be enough to:

- Make a backup copy of the configuration.
- Check that the date and time on the controller are correct.
- Download the firmware for the AP to the controller.
- Download the firmware for the WLC controller.
- Select fimware image version 1.42.0 for the next download.

Turning off the power before the **boot system {image-1|image-2}** command is finished may cause the controller to malfunction.

- Reboot the controller.

Minimal firmware version of AP:

- WEP-1L/2L and WOP-2L — **2.8.0** or higher
- WEP-30L/30L-Z and WOP-30L/30LI/30LS — **2.8.0** or higher
- WEP-200L and WOP-20L — **2.8.0** or higher
- WEP-3L, WOP-3L-EX — **2.7.0** or higher
- WEP-3ax — **1.15.0** or higher
- WEP-50L — **3.1.0** or higher
- WEP-2ac/2ac Smart, WOP-2ac/2ac rev.B/2ac rev.C — **1.25.6** or higher
- WEP-550K — **1.2.2** or higher
- WEP-500K — **1.3.1** or higher

The firmware for the AP must be downloaded to the controller before updating it.

Starting with the WLC version 1.36.4, **breaking the connection to the controller for the AP that were already under its control, does not start the automatic update process of the AP firmware.**
The AP firmware should be updated using one of the following methods:
- Immediate and deferred firmware update created via **update wlc ap firmware**
- Daily (cyclical) firmware updates for all access points via **update-manager**
- WEB interface of the WLC using the ***Update Firmware*** button

The detailed process of updating AP firmware can be found in the Access points update article.

Updating to version 1.42.0 can be done from any previous version, but the recommendations for each version described below must be followed.
When updating from version 1.15.3, the secondary bootloader must be updated at the same time as the main firmware (see section Secondary bootloader update).

6.2 Firmware update from version 1.39.1 to 1.39.2

Before updating, use the **show date** command to verify that the correct date and time are set on the device.
If an incorrect date is set on the controller, certificate validation will prevent the configuration changes from being applied after the update.

Firmware version 1.39.2 is cumulative (it contains updated versions of the primary and secondary loaders), so it will be enough to:

- Make a backup copy of the configuration.
- Check that the date and time on the controller are correct.
- Download the firmware for the AP to the controller.
- Download the firmware for the WLC controller.
- Select fimware image version 1.39.2 for the next download.

Turning off the power before the **boot system {image-1|image-2}** command is finished may cause the controller to malfunction.

- Reboot the controller.

Minimal firmware version of AP:

- WEP-1L/2L and WOP-2L — **2.8.0** or higher
- WEP-30L/30L-Z and WOP-30L/30LI/30LS — **2.8.0** or higher
- WEP-200L and WOP-20L — **2.8.0** or higher
- WEP-3L, WOP-3L-EX — **2.7.0** or higher
- WEP-3ax — **1.15.0** or higher
- WEP-50L — **3.1.0** or higher
- WEP-2ac/2ac Smart, WOP-2ac/2ac rev.B/2ac rev.C — **1.25.6** or higher
- WEP-550K — **1.2.2** or higher
- WEP-500K — **1.3.1** or higher

The firmware for the AP must be downloaded to the controller before updating it.

Starting with the WLC version 1.36.4, **breaking the connection to the controller for the AP that were already under its control, does not start the automatic update process of the AP firmware.**
The AP firmware should be updated using one of the following methods:

- Immediate and deferred firmware update created via **update wlc ap firmware**
- Daily (cyclical) firmware updates for all access points via **update-manager**
- WEB interface of the WLC using the ***Update Firmware*** button

The detailed process of updating AP firmware can be found in the Access points update article.

Updating to version 1.39.2 can be done from any previous version, but the recommendations for each version described below must be followed.
When updating from version 1.15.3, the secondary bootloader must be updated at the same time as the main firmware (see section Secondary bootloader update).

6.3 Firmware update from version 1.36.4 to 1.39.1

Before updating, use the **show date** command to verify that the correct date and time are set on the device.
If an incorrect date is set on the controller, certificate validation will prevent the configuration changes from being applied after the update.

Firmware version 1.39.1 is cumulative (it contains updated versions of the primary and secondary loaders), so it will be enough to:

- Make a backup copy of the configuration.
- Check that the date and time on the controller are correct.
- Download the firmware for the AP to the controller.
- Download the firmware for the WLC controller.
- Select fimware image version 1.39.1 for the next download.

Turning off the power before the **boot system {image-1|image-2}** command is finished may cause the controller to malfunction.

- Reboot the controller.

Minimal firmware version of AP:

- WEP-1L/2L and WOP-2L — **2.8.0** or higher
- WEP-30L/30L-Z and WOP-30L/30LI/30LS — **2.8.0** or higher
- WEP-200L and WOP-20L — **2.8.0** or higher
- WEP-3L, WOP-3L-EX — **2.7.0** or higher
- WEP-3ax — **1.15.0** or higher
- WEP-50L — **3.1.0** or higher
- WEP-2ac/2ac Smart, WOP-2ac/2ac rev.B/2ac rev.C — **1.25.6** or higher
- WEP-550K — **1.2.2** or higher
- WEP-500K — **1.3.1** or higher

The firmware for the AP must be downloaded to the controller before updating it.

Starting with the WLC version 1.36.4, **breaking the connection to the controller for the AP that were already under its control, does not start the automatic update process of the AP firmware.**
The AP firmware should be updated using one of the following methods:

- Immediate and deferred firmware update created via **update wlc ap firmware**
- Daily (cyclical) firmware updates for all access points via **update-manager**
- WEB interface of the WLC using the ***Update Firmware*** button

The detailed process of updating AP firmware can be found in the Access points update article.

Updating to version 1.39.1 can be done from any previous version, but the recommendations for each version described below must be followed.
When updating from version 1.15.3, the secondary bootloader must be updated at the same time as the main firmware (see section Secondary bootloader update).

6.4 Firmware update from version 1.36.3 to 1.36.4

Before updating, use the **show date** command to verify that the correct date and time are set on the device.
If an incorrect date is set on the controller, certificate validation will prevent the configuration changes from being applied after the update.

Firmware version 1.36.4 is cumulative (it contains updated versions of the primary and secondary loaders), so it will be enough to:

- Make a backup copy of the configuration.
- Check that the date and time on the controller are correct.
- Download the firmware for the AP to the controller.
- Download the firmware for the WLC controller.
- Select fimware image version 1.36.4 for the next download.

Turning off the power before the **boot system {image-1|image-2}** command is finished may cause the controller to malfunction.

- Reboot the controller.

Minimal firmware version of AP:

- WEP-1L/2L and WOP-2L — **2.8.0** or higher
- WEP-30L/30L-Z and WOP-30L/30LI/30LS — **2.8.0** or higher
- WEP-200L and WOP-20L — **2.8.0** or higher
- WEP-3L, WOP-3L-EX — **2.7.0** or higher
- WEP-3ax — **1.15.0** or higher
- WEP-50L — **3.1.0** or higher
- WEP-2ac/2ac Smart, WOP-2ac/2ac rev.B/2ac rev.C — **1.25.6** or higher
- WEP-550K — **1.2.2** or higher

The firmware for the AP must be downloaded to the controller before updating it. Then after rebooting the WLC, the AP will automatically update to the new firmware. If the firmware has been downloaded to the controller after it has been updated, then the **renew wlc ap all** command must be executed to reconnect the APs and update the firmware.

Starting with the WLC version 1.36.4, **breaking the connection to the controller for the AP that were already under its control, does not start the automatic update process of the AP firmware.**
The AP firmware should be updated using one of the following methods:

- Immediate and deferred firmware update created via **update wlc ap firmware**
- Daily (cyclical) firmware updates for all access points via **update-manager**
- WEB interface of the WLC using the ***Update Firmware*** button

The detailed process of updating AP firmware can be found in the Access points update article.

Updating to version 1.36.4 can be done from any previous version, but the recommendations for each version described below must be followed.
When updating from version 1.15.3, the secondary bootloader must be updated at the same time as the main firmware (see section Secondary bootloader update).

6.5 Firmware update from version 1.36.2 to 1.36.3

Before updating, use the **show date** command to verify that the correct date and time are set on the device.
If an incorrect date is set on the controller, certificate validation will prevent the configuration changes from being applied after the update.

Firmware version 1.36.3 is cumulative (it contains updated versions of the primary and secondary loaders), so it will be enough to:

- Make a backup copy of the configuration.
- Check that the date and time on the controller are correct.
- Download the firmware for the AP to the controller.
- Download the firmware for the WLC controller.
- Select fimware image version 1.36.3 for the next download.

Turning off the power before the **boot system {image-1|image-2}** command is finished may cause the controller to malfunction.

- Reboot the controller.

Minimal firmware version of AP:

- WEP-1L/2L and WOP-2L — **2.8.0** or higher
- WEP-30L/30L-Z and WOP-30L/30LI/30LS — **2.8.0** or higher
- WEP-200L and WOP-20L — **2.8.0** or higher
- WEP-3L, WOP-3L-EX — **2.7.0** or higher
- WEP-3ax — **1.15.0** or higher
- WEP-2ac/2ac Smart, WOP-2ac/2ac rev.B/2ac rev.C — **1.25.6** or higher
- WEP-550K — **1.2.2** or higher

The firmware for the AP must be downloaded to the controller before updating it. Then after rebooting the WLC, the AP will automatically update to the new firmware. If the firmware has been downloaded to the controller after it has been updated, then the **renew wlc ap all** command must be executed to reconnect the APs and update the firmware.

Updating to version 1.36.3 can be done from any previous version, but the recommendations for each version described below must be followed.
When updating from version 1.15.3, the secondary bootloader must be updated at the same time as the main firmware (see section Secondary bootloader update).

6.6 Firmware update from version 1.30.8 to 1.36.2

Before updating, use the **show date** command to verify that the correct date and time are set on the device.
If an incorrect date is set on the controller, certificate validation will prevent the configuration changes from being applied after the update.

When using a redundancy configuration scheme, ensure that the total size of the AP firmware does not exceed 50 MB before updating. To do this, use the following command:

```
wlc-30-2# dir system:access-points-firmwares
Name                                                    Type          Size
Last modified
------------------------------------------------------------   ----------   --------   --
-------------------------
WEP-200L-2.8.5_build_40.tar.gz                          File          11.79      MB
Mon Jan 26 16:05:13 2026

WEP-30L-2.8.5_build_40.tar.gz                           File          18.81      MB
Mon Jan 26 16:05:07 2026

WEP-3ax-1.15.1_build_14.tar.gz                          File          37.19      MB
Mon Jan 26 16:05:11 2026
```

If the total size of the firmware exceeds 50 MB, delete some of it **on the Master device** using the following command: **delete system:access-points-firmwares/<file name>**.

When using a failover configuration, due to a change in the synchronization mechanism, SoftGRE tunnel synchronization will not take place between versions 1.30.8 and 1.36.2. After switching the master to a device running version 1.36.2, wait for the tunnels to be reinitialised.

In firmware version 1.36.2, the VMware Tools component has been added for vWLC. To activate it, a clean installation of vWLC is required, as per the instructions.

Firmware version 1.36.2 is cumulative (it contains updated versions of the primary and secondary loaders), so it will be enough to:

- Make a backup copy of the configuration.
- Check that the date and time on the controller are correct.
- Download the firmware for the AP to the controller.
- Download the firmware for the WLC controller.
- Select fimware image version 1.36.2 for the next download.

Turning off the power before the **boot system {image-1|image-2}** command is finished may cause the controller to malfunction.

- Reboot the controller.

Minimal firmware version of AP:

- WEP-1L/2L and WOP-2L — **2.8.0** иor higher
- WEP-30L/30L-Z and WOP-30L/30LI/30LS — **2.8.0** or higher
- WEP-200L and WOP-20L — **2.8.0** or higher
- WEP-3L, WOP-3L-EX — **2.7.0** or higher
- WEP-3ax — **1.15.0** or higher

- WEP-2ac/2ac Smart, WOP-2ac/2ac rev.B/2ac rev.C — **1.25.2** or higher
- WEP-550K — **1.2.2** or higher

The firmware for the AP must be downloaded to the controller before updating it. Then after rebooting the WLC, the AP will automatically update to the new firmware. If the firmware has been downloaded to the controller after it has been updated, then the **renew wlc ap all** command must be executed to reconnect the APs and update the firmware.

Updating to version 1.36.2 can be done from any previous version, but the recommendations for each version described below must be followed.
When updating from version 1.15.3, the secondary bootloader must be updated at the same time as the main firmware (see section Secondary bootloader update).

6.7 Firmware update from version 1.30.6 to 1.30.8

vWLC is updated using the same algorithm.

Before updating, use the **show date** command to verify that the correct date and time are set on the device.
If an incorrect date is set on the controller, certificate validation will prevent the configuration changes from being applied after the update.

Firmware version 1.30.8 is cumulative (it contains updated versions of the primary and secondary loaders), so it will be enough to:

- Make a backup copy of the configuration.
- Check that the date and time on the controller are correct.
- Download the firmware for the AP to the controller.
- Download the firmware for the WLC controller.
- Select fimware image version 1.30.8 for the next download.

Turning off the power before the **boot system {image-1|image-2}** command is finished may cause the controller to malfunction.

- Reboot the controller.

Minimal firmware version of AP:

- WEP-1L/2L and WOP-2L — **2.8.0** or higher
- WEP-30L/30L-Z and WOP-30L/30LI/30LS — **2.8.0** or higher
- WEP-200L and WOP-20L — **2.8.0** or higher
- WEP-3L, WOP-3L-EX — **2.7.0** or higher
- WEP-3ax — **1.15.0** or higher
- WEP-2ac/2ac Smart, WOP-2ac/2ac rev.B/2ac rev.C — **1.25.2** or higher
- WEP-550K — **1.1.0** or higher

The firmware for the AP must be downloaded to the controller before updating it. Then after rebooting the WLC, the AP will automatically update to the new firmware. If the firmware has been downloaded to the controller after it has been updated, then the **clear wlc ap** command must be executed to reconnect the APs and update the firmware.

Updating to version 1.30.8 can be done from any previous version, but the recommendations for each version described below must be followed.
When updating from version 1.15.3, the secondary bootloader must be updated at the same time as the main firmware (see section Secondary bootloader update).

6.8 Firmware update from version 1.30.4 to 1.30.6

vWLC is updated using the same algorithm.

Before updating, use the **show date** command to verify that the correct date and time are set on the device.
If an incorrect date is set on the controller, certificate validation will prevent the configuration changes from being applied after the update.

Firmware version 1.30.6 is cumulative (it contains updated versions of the primary and secondary loaders), so it will be enough to:

- Make a backup copy of the configuration.
- Check that the date and time on the controller are correct.
- Download the firmware for the AP to the controller.
- Download the firmware for the WLC controller.
- Select fimware image version 1.30.6 for the next download.

Turning off the power before the **boot system {image-1|image-2}** command is finished may cause the controller to malfunction.

- Reboot the controller.

Minimal firmware version of AP:

- WEP-1L/2L and WOP-2L — **2.8.0** or higher
- WEP-30L/WEP-30L-NB/30L-Z and WOP-30L/30LI/30LS — **2.8.0** or higher
- WEP-200L and WOP-20L — **2.8.0** or higher
- WEP-3L, WOP-3L-EX — **2.8.0** or higher
- WEP-3ax — **1.15.0** or higher
- WEP-2ac/2ac Smart, WOP-2ac/2ac rev.B/2ac rev.C — **1.25.2** or higher
- WEP-550K — **1.1.0** or higher

The firmware for the AP must be downloaded to the controller before updating it. Then after rebooting the WLC, the AP will automatically update to the new firmware. If the firmware has been downloaded to the controller after it has been updated, then the **clear wlc ap** command must be executed to reconnect the APs and update the firmware.

Updating to version 1.30.4 can be done from any previous version, but the recommendations for each version described below must be followed.
When updating from version 1.15.3, the secondary bootloader must be updated at the same time as the main firmware (see section Secondary bootloader update).

6.9 Firmware update from version 1.30.2 to 1.30.4

vWLC is updated using the same algorithm.

Before updating, use the **show date** command to verify that the correct date and time are set on the device.
If an incorrect date is set on the controller, certificate validation will prevent the configuration changes from being applied after the update.

Starting with version 1.30.4, the maximum size of WLC logs is limited to 90 days. When updating, the size of existing logs will be automatically reduced.

Firmware version 1.30.4 is cumulative (it contains updated versions of the primary and secondary loaders), so it will be enough to:

- Make a backup copy of the configuration.
- Check that the date and time on the controller are correct.
- Download the firmware for the AP to the controller.
- Download the firmware for the WLC controller.
- Select fimware image version 1.30.4 for the next download.

Turning off the power before the **boot system {image-1|image-2}** command is finished may cause the controller to malfunction.

- Reboot the controller.

Minimal firmware version of AP:

- WEP-1L/2L and WOP-2L — **2.5.6** or higher
- WEP-30L/30L-Z and WOP-30L/30LI/30LS — **2.6.0** or higher
- WEP-200L and WOP-20L — **2.7.0** or higher
- WEP-3L — **2.5.3** or higher
- WEP-3ax — **1.14.0** or higher
- WEP-2ac/2ac Smart, WOP-2ac/2ac rev.B/2ac rev.C — **1.25.2** or higher

The firmware for the AP must be downloaded to the controller before updating it. Then after rebooting the WLC, the AP will automatically update to the new firmware. If the firmware has been downloaded to the controller after it has been updated, then the **clear wlc ap** command must be executed to reconnect the APs and update the firmware.

Updating to version 1.30.4 can be done from any previous version, but the recommendations for each version described below must be followed.
When updating from version 1.15.3, the secondary bootloader must be updated at the same time as the main firmware (see section Secondary bootloader update).

6.10 Firmware update from version 1.30.0 to 1.30.2

vWLC is updated using the same algorithm.

Before updating, use the **show date** command to verify that the correct date and time are set on the device.
If an incorrect date is set on the controller, certificate validation will prevent the configuration changes from being applied after the update.

Firmware version 1.30.2 is cumulative (it contains updated versions of the primary and secondary loaders), so it will be enough to:

- Make a backup copy of the configuration.
- Check that the date and time on the controller are correct.
- Download the firmware for the AP to the controller.
- Download the firmware for the WLC controller.
- Select fimware image version 1.30.2 for the next download.

Turning off the power before the **boot system {image-1|image-2}** command is finished may cause the controller to malfunction.

- Reboot the controller.

Minimal firmware version of AP:

- WEP-1L/2L and WOP-2L — **2.5.6** or higher
- WEP-30L/30L-Z/200L and WOP-20L/30L/30LI/30LS — **2.6.0** or higher
- WEP-3L — **2.5.3** or higher
- WEP-3ax — **1.14.0** or higher
- WEP-2ac/2ac Smart, WOP-2ac/2ac rev.B/2ac rev.C — **1.25.2** or higher

The firmware for the AP must be downloaded to the controller before updating it. Then after rebooting the WLC, the AP will automatically update to the new firmware. If the firmware has been downloaded to the controller after it has been updated, then the **clear wlc ap** command must be executed to reconnect the APs and update the firmware.

Updating to version 1.30.2 can be done from any previous version, but the recommendations for each version described below must be followed.
When updating from version 1.15.3, the secondary bootloader must be updated at the same time as the main firmware (see section Secondary bootloader update).

6.11 Firmware update from version 1.26.1 to 1.30.0

vWLC (started with 1.27.0 version) is updated using the same algorithm.

Before updating, use the **show date** command to verify that the correct date and time are set on the device.
If an incorrect date is set on the controller, certificate validation will prevent the configuration changes from being applied after the update.

Firmware version 1.30.0 is cumulative (it contains updated versions of the primary and secondary loaders), so it will be enough to:

- Make a backup copy of the configuration.
- Check that the date and time on the controller are correct.
- Download the firmware for the AP to the controller.
- Download the firmware for the WLC controller.
- Select fimware image version 1.30.0 for the next download.

Turning off the power before the **boot system {image-1|image-2}** command is finished may cause the controller to malfunction.

- Reboot the controller.

Minimal firmware version of AP:

- WEP-1L/2L and WOP-2L — **2.5.6** or higher
- WEP-30L/30L-Z/200L and WOP-20L/30L/30LI/30LS — **2.6.0** or higher
- WEP-3L — **2.5.3** or higher
- WEP-3ax — **1.14.0** or higher
- WEP-2ac/2ac Smart, WOP-2ac/2ac rev.B/2ac rev.C — **1.25.2** or higher

The firmware for the AP must be downloaded to the controller before updating it. Then after rebooting the WLC, the AP will automatically update to the new firmware. If the firmware has been downloaded to the controller after it has been updated, then the **clear wlc ap** command must be executed to reconnect the APs and update the firmware.

Updating to version 1.30.0 can be done from any previous version, but the recommendations for each version described below must be followed.
When updating from version 1.15.3, the secondary bootloader must be updated at the same time as the main firmware (see section Secondary bootloader update).

After updating to version 1.30.0 it will be possible to update the controller and AP firmware via WEB interface.

6.12 Firmware update from version 1.19.2 to 1.26.1

Before updating, use the **show date** command to verify that the correct date and time are set on the device.
If an incorrect date is set on the controller, certificate validation will prevent the configuration changes from being applied after the update.

Firmware version 1.26.1 is cumulative (it contains updated versions of the primary and secondary loaders), so it will be enough to:

- Make a backup copy of the configuration.
- Download the firmware for the AP to the controller.
- Download the firmware for the WLC controller.
- Select fimware image version 1.26.1 for the next download.

Turning off the power before the **boot system {image-1|image-2}** command is finished may cause the controller to malfunction.

- Reboot the controller.

Minimal firmware version of AP:

- WEP-1L/2L/30L/30L-Z/200L and WOP-2L/20L/30L/30LS — **2.5.0** or higher
- WEP-3ax — **1.12.0** or higher
- WEP-2ac/2ac Smart, WOP-2ac/2ac rev.B/2ac rev.C — **1.25.0** or higher

The firmware for the AP must be downloaded to the controller before updating it. Then after rebooting the WLC, the AP will automatically update to the new firmware. If the firmware has been downloaded to the controller after it has been updated, then the **clear wlc ap** command must be executed to reconnect the APs and update the firmware.

Updating to version 1.26.1 can be done from any previous version, but the recommendations for each version described below must be followed.
When updating from version 1.15.3, the secondary bootloader must be updated at the same time as the main firmware (see section Secondary bootloader update).

6.13 Firmware update from version 1.19.1 to 1.19.2

Firmware version 1.19.2 is cumulative (it contains updated versions of the primary and secondary loaders), so it will be enough to:

- Make a backup copy of the configuration.
- Download the firmware for the AP to the controller.
- Download the firmware file for the WLC controller.
- Select fimware image version 1.19.2 for the next download.
- Reboot the controller.
- Check parameters in the configuration.

In version 1.19.2 there is a transition from personal board-profiles to universal radio-profiles, the transition will convert the configuration, board-profiles will be replaced by pre-configured radio-profiles, you should check the radio-profile configuration.

If you have customized individual profiles for access points and have redefined board-profiles (settings of radio interfaces of access points), in which auto channel selection was enabled and the list of channels in the parameter limit-channel was not set, then after the update the list of channels from the common radio-profiles

will be used. If it is necessary to change channels – set the required limit-channel list in the individual profile of the required access point.

Minimal firmware version of AP:

- WEP-1L/2L/30L/200L and WOP-2L/20L/30L/30LS — **2.3.2**
- WEP-3ax — **1.11.0**

It is necessary to download the firmware for the AP to the controller. The AP will be updated automatically after connection.

> Updating to version 1.19.2 can be done from any previous version, but the recommendations for each version described below must be followed.

6.14 Firmware update from version 1.19.0 to 1.19.1

After the update, you need to edit the configuration according to the changes:

1. In 1.19.1, selective inclusion of vlan in SoftGRE tunnels is supported. **service-vlan** command is added in softgre-controller section, the specified vlans will be included in tunnels after update. In 1.19.0 all created vlans were included in tunnels. Need to add used vlans for Wi-Fi to the configuration.

```
softgre-controller
  service-vlan add 3
exit
```

2. Configuration of telnet, ssh, web, snmp services on AP is supported, after update they will be disabled. They can be enabled in ap-profile.

   > On AP web is disabled/enabled simultaneously for HTTP/HTTPS services.

   To enable, go to wlc → ap-profile default-ap → services.

```
wlc(config-wlc-ap-profile)# services
wlc(config-wlc-ap-profile-services)#
  snmp-server  Enable SNMP service

wlc(config-wlc-ap-profile-services)# ip
  http    Configure web-configurator service
  https   Configure web-configurator service
  ssh     Configure SSH service
  telnet  Configure telnet service
```

6.15 Firmware update from version 1.15.3 to 1.19.0

Unlike firmware version 1.19.0 and later, earlier versions do not support cumulative updates. Therefore, in addition to the main firmware, the secondary bootloader must also be updated. As a result, the update process is as follows:

- Upload the secondary bootloader (U-boot) to the WLC controller.
- Upload the firmware file to the WLC controller.
- Select the updated version firmware image for the next download.
- Reboot the controller.

1. After the update it is necessary to edit the configuration according to the changes. The scheme of access point registration on the controller has been changed. Now not only port 8043 but also port 8044 is used. It is necessary to add port 8044 to object-group service sa:

```
object-group service sa
  port-range 8044
exit
```

After the WLC is updated, the APs will be listed in the provisioning service and will be waiting for authorization. To view the list of unauthorized access points, use the command:

```
show wlc service-activator aps
```

The following command is used to authorize all AP in the list:

```
join wlc ap
```

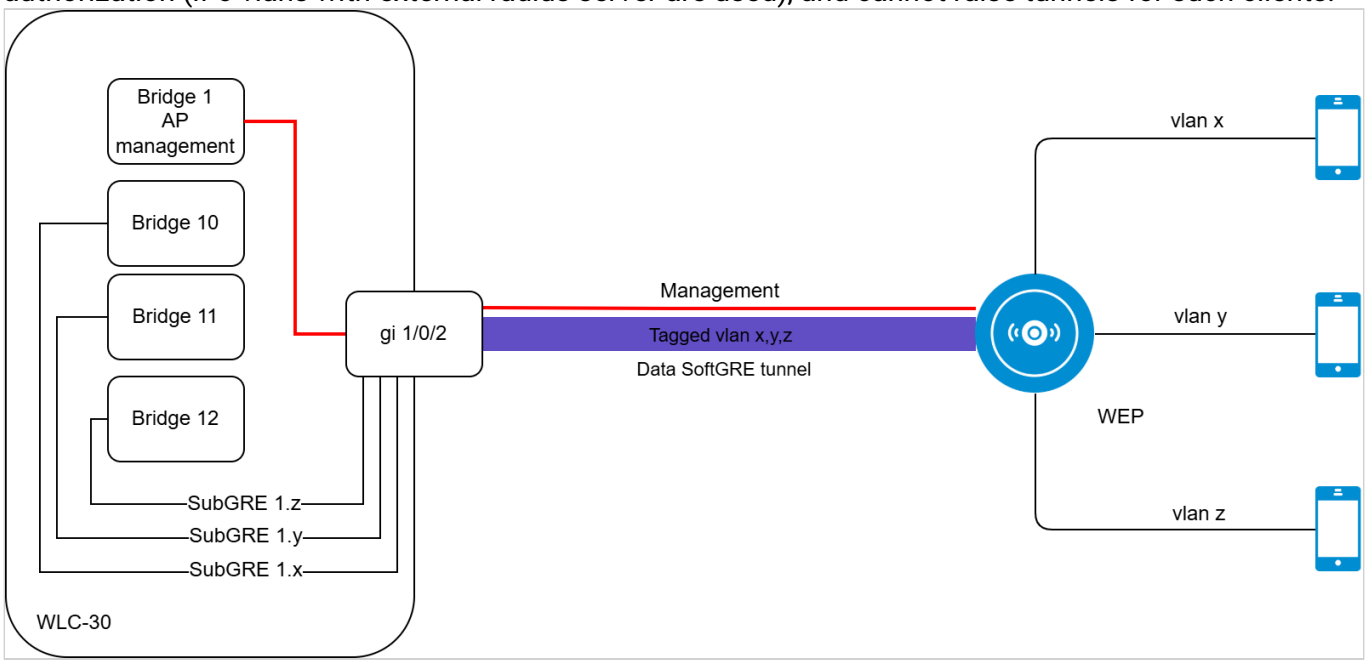
The following command is used to authorize a specific AP:

```
join wlc ap <MAC_AP>
```

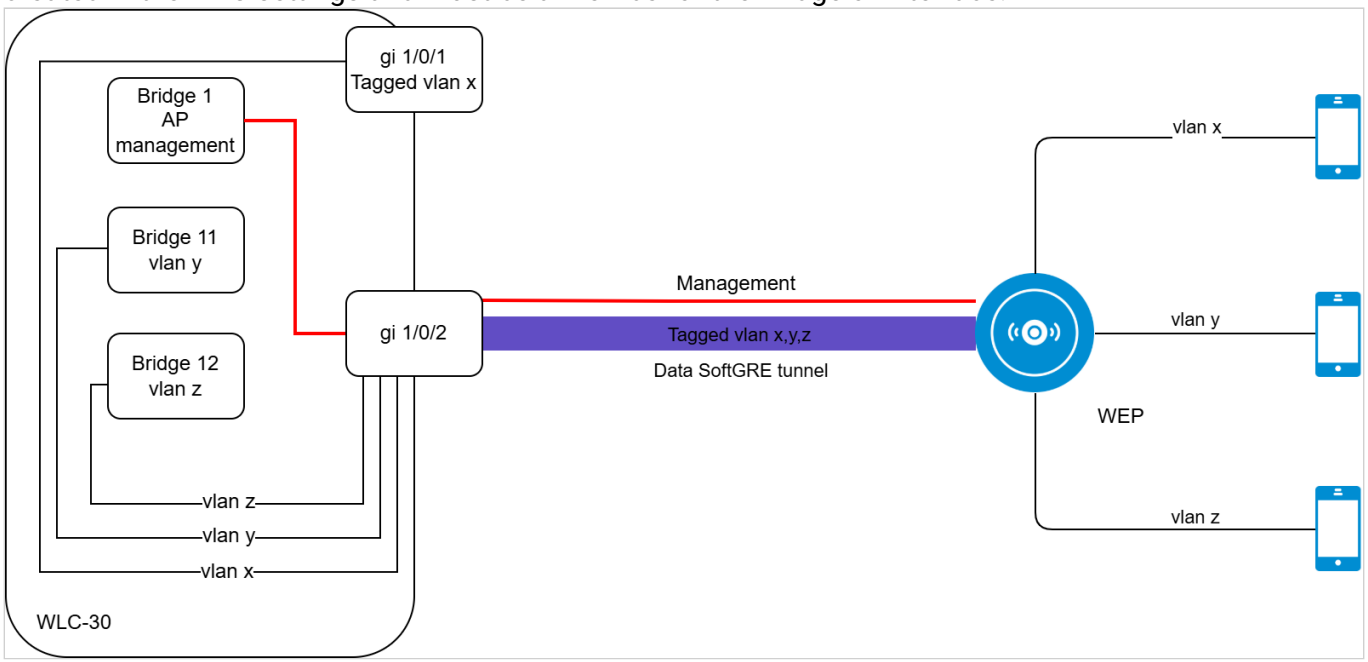
It is possible to enable automatic authorization mode in the configuration:

```
wlc# configure
wlc(config)# wlc
wlc(config-wlc)# service-activator
wlc(config-wlc-service-activator)# aps join auto
wlc(config-wlc-service-activator)# do commit
wlc(config-wlc-service-activator)# do confirm
```

2. The scheme of SoftGRE tunnels enabling has been changed:
   In 1.15.3 version:
   Client traffic comes from the AP to a gre-tunnel with a specified vlan tag, on the WLC side a separate subgre-tunnel is created for each vlan and included in the specified Bridges, when leaving the subgre the vlan tag is removed. With this implementation, a subgre-tunnel must be created for each vlan and included in one of the Bridges. WLC does not know vlans that are issued at the moment of radius authorization (if c-vlans with external radius server are used), and cannot raise tunnels for such clients.



   In 1.19.0 version:
   The logic of SoftGRE tunnels operation in wlc mode has been changed. Previously subgre was unconditionally included in Bridge by WLC configuration, in the new implementation subgre tunnels are absent. Vlan specified in SSID configuration is included in WLC without sub-tunnel termination in Bridge. The use of c-vlan in client traffic tunneling scheme is supported. For correct operation, the vlan must be created in the WLC settings and must be a member of the Bridge or interface.



3. To raise tunnels, the location parameter, which was previously set on Bridge and in ap-location for SSIDs, is no longer used. Instead, you must enable tunnel mode in ap-location. The vlan-id in ssid-profile must match the vlan-id in bridge users.

Firmware version 1.15.3	**Firmware version 1.19.0**
bridge 3 security-zone users ip address 192.168.2.1/24 location default enable exit	bridge 3 vlan 3 (=vlan-id в SSID-profile) mtu 1458 security-zone users ip address 192.168.2.1/24 enable exit
ap-location default-location description default-location board-profile WEP-1L default_wep-1l_profile board-profile WEP-20L default_wep-20l_profile board-profile WEP-2L default_wep-2l_profile board-profile WEP-3ax default_wep-3ax_profile board-profile WEP-3ax-Z default_wep-3ax-z_profile board-profile WOP-20L default_wop-20l_profile board-profile WOP-2L default_wop-2l_profile board-profile WOP-3ax default_wop-3ax_profile ssid-profile default-ssid default exit	ap-location default-location description default-location mode tunnel ap-profile default-ap board-profile WEP-1L default_wep-1l_profile board-profile WEP-200L default_wep-200l_profile board-profile WEP-20L default_wep-20l_profile board-profile WEP-2L default_wep-2l_profile board-profile WEP-30L default_wep-30l_profile board-profile WEP-3ax default_wep-3ax_profile board-profile WEP-3ax-Z default_wep-3ax-z_profile board-profile WOP-20L default_wop-20l_profile board-profile WOP-2L default_wop-2l_profile board-profile WOP-30L default_wop-30l_profile board-profile WOP-3ax default_wop-3ax_profile ssid-profile default-ssid exit
	vlan 3 force-up exit

4. Wireless-controller is renamed to softgre-controller:

Firmware version 1.15.3	**Firmware version 1.19.0**
wireless-controller nas-ip-address 127.0.0.1 data-tunnel configuration wlc aaa radius-profile default_radius keepalive-disable enable exit	softgre-controller nas-ip-address 127.0.0.1 data-tunnel configuration wlc aaa radius-profile default_radius keepalive-disable enable exit

5. WLC monitoring commands have been changed:

In 1.15.3 version	In 1.19.0 version	Command description
show wlc connected-ap	show wlc ap	View the list of access points monitored by the controller
show wlc connected-ap detailed	sh wlc ap detailed	View detailed information on all authorized access points
show wlc connected-ap detailed <MAC_AP>	sh wlc ap detailed <MAC_AP>	View detailed information on one of the authorized access points
show wlc connected-ap-clients <MAC_AP>	sh wlc clients ap <MAC_AP>	View information about the wireless client connections of a specific access point
show wlc connected-ap-clients <MAC_AP> detailed	sh wlc clients ap <MAC_AP> detailed	View detailed information about the wireless client connections of a specific access point
show wlc connected-client <MAC_STA>	sh wlc clients <MAC_STA>	View wireless client connection information by its MAC address
show wlc connected-client <MAC_STA> detailed	sh wlc clients <MAC_STA> detailed	View detailed connection information of a wireless client by its MAC address
show wlc connected-ap-interfaces <MAC_AP>	show wlc ap interfaces <MAC_AP>	View information and counters on access point interfaces
show wlc connected-ap-radios <MAC_AP>	show wlc ap radios <MAC_AP>	View the basic parameters of the access point's radio interfaces

6.15.1 Secondary bootloader update

Updating the secondary bootloader requires uploading the file to the controller and rebooting the controller. The operation can be combined with updating the main firmware.

When downloading the secondary bootloader using remote file copying servers, it is necessary to:

1. Start the appropriate server on the network (tftp/ftp/sftp/http/https/scp).
2. Copy the <uboot-file> file to the working partition of the remote file upload server.
3. Provide IP connectivity between the WLC controller being upgraded and the remote file copy server (routing).
4. Provide remote copy protocol operation between the WLC and the remote file copy server (intermediate firewall).
5. If necessary (for ftp, sftp, scp, http, https protocols) find out the username and password for downloading the required file.

When loading the secondary bootloader using a USB/MMC key, it is necessary to:

1. Format the USB/MMC key partition in FAT32 or exFAT format.
2. Copy the <uboot-file> file to the root partition of the USB/MMC key.
3. Plug the USB/MMC drive into the appropriate slot on the controller.
4. Determine the volume label of the connected USB/MMC drive.

Loading the secondary bootloader using one of the remote file upload protocols

Firmware upload via TFTP

```
wlc# copy tftp://<tftp-server-ip>:/<uboot-file> system:boot-2
|****************************************| 100% (697kB) Bootloader updated successfully.
```

Firmware upload via FTP

```
wlc# copy ftp://<ftp-username>:<ftp-userpassword>@<ftp-server-ip>:/<uboot-file> system:boot-2
|****************************************| 100% (697kB) Bootloader updated successfully.
```

Firmware upload via SFTP

```
wlc# copy sftp://<sftp-username>:<sftp-userpassword>@<sftp-server-ip>:/<uboot-file> system:boot-2
|****************************************| 100% (697kB) Bootloader updated successfully.
```

Firmware upload via SCP

```
wlc# copy scp://<scp-username>:<scp-userpassword>@<scp-server-ip>:/<uboot-file> system:boot-2
|****************************************| 100% (697kB) Bootloader updated successfully.
```

Firmware upload via HTTP

```
wlc# copy http://<http-username>:<http-userpassword>@<http-server-ip>:/<uboot-file> system:boot-2
|****************************************| 100% (697kB) Firmware updated successfully.
```

Firmware upload via HTTPS

```
wlc# copy https://<https-username>:<https-userpassword>@<http-server-ip>:/<uboot-file>
system:boot-2

|****************************************| 100% (697kB) Bootloader updated successfully.
```

- <tftp-server-ip> – IP address of the TFTP server in use;
- <ftp-username> – user name on the FTP server;
- <ftp-userpassword> – user password on the FTP server;
- <ftp-server-ip> – IP address of the FTP server in use;
- <sftp-username> – user name on the SFTP server;
- <sftp-userpassword> – user password on the SFTP server;
- <sftp-server-ip> – IP address of the SFTP server in use;
- <scp-username> – user name on the SCP server;
- <ftp-userpassword> – user password on the FTP server;
- <scp-server-ip> – IP address of the SCP server in use;
- <http-username> – user name on the HTTP server;
- <http-userpassword> – user password on the HTTP server;
- <http-server-ip> – IP address of the HTTP server in use.

The rules for using firmware files for the different models are described in the section Files used for the update.

Secondary bootloader update using USB/MMC storage

1. Define the volume label of the connected USB/MMC storage:

Defining the volume label name on a USB storage

```
wlc# show storage-devices usb
Name                          Filesystem  Total, MB   Used, MB    Free, MB
----------------------------  ----------  ----------  ----------  ----------
<USB_DISK>                    vfat        7664.01     6391.69     1272.32
```

Defining the volume label name on a MMC storage

```
wlc# show storage-devices mmc
Name                          Filesystem  Total, MB   Used, MB    Free, MB
----------------------------  ----------  ----------  ----------  ----------
<MMC_DISK>                    vfat        7664.01     6391.69     1272.32
```

2. Copying file from the USB/MMC storage:

> ⚠ When executing copy commands to USB/MMC media, instead of the <USB_DISK> or <MMC_DISK> fields, use the real volume labels defined above.

Load firmware from USB

```
wlc# copy usb://<USB_DISK>:/<uboot-file> system:boot-2

|****************************************| 100% (697kB) Bootloader updated successfully.
```

Load firmware from MMC

```
wlc# copy usb://<MMC_DISK>:/<uboot-file> system:boot-2

|****************************************| 100% (697kB) Bootloader updated successfully.
```

- <USB_DISK> – partition name on the USB storage;
- <MMC_DISK> – partition name on the MMC storage.

6.16 Preparation for firmware upload

When uploading firmware using remote file copy servers:

1. Start the corresponding server on the network (tftp/ftp/sftp/http/https/scp).
2. Copy the firmware file (<firmware-file>) to the working directory of the remote file copy server. The names of the required files depending on the model and hardware version of the device are listed in the section Files used for the update.
3. Provide IP connectivity between the upddated WLC controller and the remote file copy server (routing).
4. Ensure operation of the remote copy protocol between the WLC and the remote file copy server (intermediate firewalls).
5. If necessary (for ftp, sftp, scp, http, https protocols), find out the username and password to write the required file.

When loading the firmware using a USB/MMC media:

1. Format USB/MMC media partition as FAT32 or exFAT.
2. Copy the firmware file (<firmware-file>) to the root of the USB/MMC drive. The names of the required files depending on the model and hardware version of the device are listed in the section Files used for the update.
3. Connect the USB/MMC storage to the appropriate WLC slot.
4. Define the volume label of the connected USB/MMC storage.

6.17 Firmware upload

6.17.1 Using one of the remote file upload protocols

Firmware upload via TFTP

```
wlc# copy tftp://<tftp-server-ip>:/<firmware-file> system:firmware
|****************************************| 100% (0B) Firmware updated successfully.
```

Firmware upload via FTP

```
wlc# copy ftp://<ftp-username>:<ftp-userpassword>@<ftp-server-ip>:/<firmware-file>
system:firmware
|****************************************| 100% (0B) Firmware updated successfully.
```

Firmware upload via SFTP

```
wlc# copy sftp://<sftp-username>:<sftp-userpassword>@<sftp-server-ip>:/<firmware-file>
system:firmware
|****************************************| 100% (0B) Firmware updated successfully.
```

Firmware upload via SCP

```
wlc# copy scp://<scp-username>:<scp-userpassword>@<scp-server-ip>:/<firmware-file>
 system:firmware
|****************************************| 100% (0B) Firmware updated successfully.
```

Firmware upload via HTTP

```
wlc# copy http://<http-username>:<http-userpassword>@<http-server-ip>:/<firmware-file>
 system:firmware
|****************************************| 100% (0B) Firmware updated successfully.
```

Firmware upload via HTTPS

```
wlc# copy https://<https-username>:<https-userpassword>@<http-server-ip>:/<firmware-file>
 system:firmware
|****************************************| 100% (0B) Firmware updated successfully.
```

- <tftp-server-ip> — IP address of the TFTP server in use;
- <ftp-username> — user name on the FTP server;
- <ftp-userpassword> — user password on the FTP server;
- <ftp-server-ip> — IP address of the FTP server in use;
- <sftp-username> — user name on the SFTP server;
- <sftp-userpassword> — user password on the SFTP server;
- <sftp-server-ip> — IP address of the SFTP server in use;
- <scp-username> — user name on the SCP server;
- <ftp-userpassword> — user password on the FTP server;
- <scp-server-ip> — IP address of the SCP server in use;
- <http-username> — user name on the HTTP server;
- <http-userpassword> — user password on the HTTP server;
- <http-server-ip> — IP address of the HTTP server in use.

The rules for using firmware files for the different models are described in the section Files used for the update.

6.17.2 Using USB/MMC media

1. Define the volume label of the connected USB/MMC storage:

Defining the volume label name on a USB storage

```
wlc# show storage-devices usb
Name                          Filesystem  Total, MB   Used, MB    Free, MB
----------------------------  ----------  ----------  ----------  ----------
<USB_DISK>                    vfat        7664.01     6391.69     1272.32
```

Defining the volume label name on a MMC storage

```
wlc# show storage-devices mmc
Name                          Filesystem  Total, MB   Used, MB    Free, MB
----------------------------  ----------  ----------  ----------  ----------
<MMC_DISK>                    vfat        7664.01     6391.69     1272.32
```

2. Copying file from the USB/MMC storage:

⚠ When executing copy commands to USB/MMC media, instead of the <USB_DISK> or <MMC_DISK> fields, use the real volume labels defined above.

Load firmware from USB

```
wlc# copy usb://<USB_DISK>:/<firmware-file>  system:firmware
|****************************************| 100% (73786kB) Firmware updated successfully
```

Load firmware from MMC

```
wlc# copy mmc://<MMC_DISK>:/<firmware-file>  system:firmware
|****************************************| 100% (73786kB) Firmware updated successfully.
```

- <USB_DISK> – partition name on the USB storage;
- <MMC_DISK> – partition name on the MMC storage.

6.18 Selecting version 1.39.2 firmware image for the next upload

WLC controllers store two firmware images (image-1 and image-2) at the same time.

1. Check the contents of the firmware images uploaded to the controller:

```
wlc# show bootvar

Image  Version                    Date                  Status        After reboot
-----  -------------------------  --------------------  ------------  ------------

1      1.39.1 build               2026-08-07 16:58:39   Active        *
       15[37bbe1c645]

2      1.39.2 build               2026-08-20 18:12:54   Not Active
       14[7f0831ee60]
```

When loading a firmware file to the system:firmware partition, the upload is always made to the currently inactive partition.

2. Select the inactive partition containing firmware version 1.39.2 as bootable:

Selecting firmware section to upload

```
wlc# boot system inactive
This command cannot be interrupted, do not turn off device during process.
Continue? (y/N): y
```

3. Check that the image containing firmware version 1.39.2 is selected for upload:

```
wlc# show bootvar

Image  Version                    Date                  Status        After reboot
-----  -------------------------  --------------------  ------------  ------------

1      1.39.1 build               2026-08-07 16:58:39   Active
       15[37bbe1c645]

2      1.39.2 build               2026-08-20 18:12:54   Not Active    *

       14[7f0831ee60]
```

If a firmware version that was released earlier than the current firmware version is selected for subsequent download, the current configuration cannot be converted after a reboot and a empty configuration (no factory settings) will be applied. With an empty configuration, the controller can only be connected to using a console connection and the default admin/password.

7 Rebooting the controller

Reboot the controller using the following command:

Reboot the controller via CLI of the main firmware

```
wlc# reload system
Do you really want to reload system ? (y/N): y
```

TECHNICAL SUPPORT

For technical assistance in issues related to handling Eltex Ltd. equipment, please, address to Service Center of the company:

https://eltex-co.com/support/

You are welcome to visit Eltex official website to get the relevant technical documentation and software, to use our knowledge base or consult a Service Center Specialist.

http://www.eltex-co.com/

http://www.eltex-co.com/support/downloads/