

# 25 Cyber security

WCC Lite is based on OpenWRT operating system. OpenWrt is described as a Linux distribution for embedded devices. WCC Lite has same functionality as Linux OS including user management.

Basic configuration on WCC Lite can be done using web based frontend. More advanced configuration is available over terminal interface. For secure web access, WCC Lite can be accessed via HTTPS (TLS) instead of the unencrypted HTTP protocol. You can use openssl utility to generate your own certificate authority and certificates to be used on web interface. Certificates can also be named or placed in whatever directory you wish by editing `/etc/lighttpd/lighttpd.conf`.

Terminal is accessible over Telnet or SSH. For security reasons we strongly recommend to use SSH. SSH, also known as Secure Socket Shell, is a network protocol that provides administrators with a secure way to access a remote computer. SSH also refers to the suite of utilities that implement the protocol. Secure shell provides strong authentication and secure encrypted data communications between two computers connecting over an insecure network such as the Internet. SSH is widely used by network administrators for managing systems and applications remotely, allowing them to log in to another computer over a network, execute commands and move files from one computer to another.

## User rights

Depending on the user name, different rights are defined: admin is generally entitled to make changes while user does not have any editing permissions, the relevant buttons are disabled. User can be assigned to one of fifteen user groups that can access different amounts of device parameters. Highest (fifteenth) permission level grants the same permission as root user has. User group rights can be edited to give more rights or restrictions, except for highest (15th) level.

## User management and rights authentication

WCC Lite provides different authentication mechanisms:

- Authentication via locally stored credentials. In this scenario all users, passwords and permissions are encrypted and stored in internal WCC Lite storage.
- Authentication via external RADIUS Server. In this scenario all users, passwords and permissions (profiles) are defined in remote RADIUS Server. Login into WCC Lite is available only if RADIUS Server will grant authentication and will provide user profile with user rights on that device (more detailed description below). This also means that a password for such user cannot be changed remotely.
- Authentication via external RADIUS Server with fallback option. In this scenario users will be authenticated via RADIUS server. If server fails to respond (configured timeout is passed) WCC will use locally stored credentials. Fallback options are selected with PAM configuration.

By default only authentication via locally stored credentials is allowed. For authentication via external RADIUS server a user should at first enable RADIUS process and configure at least one server.

## Locally stored credentials management

Device has predefined default users like *root* and *user*.

*Screen containing all users*

Users	Status	Actions
user	SSH Access: Enabled Group: viewer Date Added: Mon Sep 30 13:51:28 2019 Last Entry: undefined	Edit Change Password Delete

Screen for new user configuration

PROTOCOL HUB	STATUS	SYSTEM	SERVICES	NETWORK	<b>USERS</b>	LOGOUT	
--------------	--------	--------	----------	---------	--------------	--------	--

[EDIT USERS](#)
[EDIT GROUPS](#)

[Save](#)

## Add New User

User Configuration

User Name

User Group

SSH Access

Password

[Back to Overview](#)
[Save & Apply](#)
[Save](#)
[Reset](#)

**root** user has full permission set to connect to WCC Lite over web interface and SSH or Telnet. This user is default user on WCC Lite and cannot be deleted. However, it is highly advised to change the default password to a different one less susceptible for attacks.

**user** is limited user on system and can't get root rights. A default password for access via commandline interface and web interface is wcclite. It is advised to change this password to increase a level of security.

System allows customer to set up even more users with well known commands like *adduser*, *passwd* and *userdel*. More users can also be added or edited via web interface as shown in the figures above. User should enter user name, user groups for which the user should belong (the group must be preconfigured first), SSH access permission as well as password. When editing user settings, only *User Group* and *SSH Access* permission can be changed. To change user password, *Change Password* button should be pressed as seen in figure above to lead user to a screen seen in the figure below.

### Changing user password

PROTOCOL HUB	STATUS	SYSTEM	SERVICES	NETWORK	<b>USERS</b>	LOGOUT	
--------------	--------	--------	----------	---------	--------------	--------	--

[EDIT GROUPS](#)
[EDIT USERS](#)

[Save](#)

## Change user Password

Edit password of a system user

Password

Confirmation

[Back to Overview](#)
[Save & Apply](#)
[Save](#)
[Reset](#)

A user needs to be assigned to **root** group for admin rights and have root access



It should be noted that assigning user to a root group only gives complete authority over web interface. Permissions for a commandline interface should be given by a root user via commandline interface.

Following commands may be used in comamnd line interface for user control:

**adduser** - create a new user or update default new user information


When invoked without the **-D** option, the *adduser* command creates a new user account using the values specified on the command line plus the default values from the system. Depending on command line options, the *useradd* command will update system files and may also create the new user's home directory and copy initial files.

**passwd** - change user password

The *passwd* command changes passwords for user accounts. A normal user may only change the password for his/her own account, while the superuser may change the password for any account. *passwd* also changes the account or associated password validity period.

**deluser** - delete a user account and related files

The *deluser* command modifies the system account files, deleting all entries that refer to the user name LOGIN. The named user must exist.

 If a user intends to use newly created user account via both commandline interface and web interface he should create and delete users via web interface and not using adduser and deluser commands as they don't create uci entries.

For more information about controlling users via command line interface one should refer to Linux documentation

## Authentication via external service

WCC Lite support external authentication via RADIUS service. Remote Authentication DialIn User Service (RADIUS) is a networking protocol that provides centralized Authentication, Authorization, and Accounting (AAA or Triple A) management for users who connect and use a network service. RADIUS is a client/server protocol that runs in the application layer, and can use either TCP or UDP as transport. Network access servers, the gateways that control access to a network, usually contain a RADIUS client component that communicates with the RADIUS server. RADIUS is often the backend of choice for 802.1X authentication as well. The RADIUS server is usually a background process running on a UNIX or Microsoft Windows server. In WCC Lite RADIUS Client is implemented since WCC Lite software version v1.2.4. The user sends a request to a WCC Lite to gain access to get access using access credentials posted in an HTTP/HTTPS WCC Lite web login form

This request includes access credentials, typically in the form of username and password. Additionally, the request may contain other information which the Device knows about the user, such as its network address or information regarding the user's physical point of attachment to the device. The RADIUS server checks that the information is correct using authentication schemes such as PAP, CHAP or EAP. The user's proof of identification is verified, along with, optionally, other information related to the request, such as the user's network address, account status, and specific network service access privileges. Historically, RADIUS servers checked the user's information against a locally stored flat file database. Modern RADIUS servers can do this, or can refer to external sources—commonly SQL, Kerberos, LDAP, or Active Directory servers—to verify the user's credentials. The RADIUS server then returns one of two responses to the WCC Lite:

1. **Access-Reject** - The user is unconditionally denied access to all requested resources. Reasons may include failure to provide proof of identification or an unknown or inactive user account.
2. **Access-Accept** - The user is granted access. Once the user is authenticated, the RADIUS server will periodically check if the user is authorized to use the service requested. A given user may be allowed to get admin rights or user rights depending on permissions set on RADIUS Server. Again, this information may be stored locally on the RADIUS server, or may be looked up in an external source such as LDAP or Active Directory.

To use this mechanism a RADIUS server must be configured. The parameter Radius Authentication must be Enabled on WCC Lite.

As of firmware version 1.2.13, the RADIUS service is disabled by default. The service can be enabled at System->Startup.

If the RADIUS authentication is enabled, WCC Lite uses the RADIUS server IP address and the RADIUS shared secret key for communication with External RADIUS Server. After entering the login credentials and login attempt, WCC Lite sends these credentials to the RADIUS server for authentication. If the RADIUS server is available, it compares the login credentials:

- If the comparison is successful, the RADIUS server returns the specific user role and Access-Accept;
- If the login credentials are invalid, Radius Server returns Access-Reject and the logon fails.
- If the RADIUS server is not available and fallback option is disabled login into WCC Lite will be impossible. If RADIUS server is not available and timeout occurs, login will be attempted via local login credentials.

Enabled: Enables or disables this server.

Hostname/IP: Hostname or IP address of RADIUS server.

Timeout: Timeout in seconds to wait for server response.


Shared secret: Key shared between RADIUS server and RADIUS client.

Add: Adds auxiliary (backup) server.

## Audit Log

WCC Lite OS with version >1.2.0 has integrated Audit logging for important events such as:

- Login/logout.
- Wrong password attempts to login into system.
- Device boot event, when system was started.
- Device reboot/halt event.
- Configuration changes.
- Firmware changes.
- Date and time changes in system (excluding automatic system time updates over NTP or IEC 60870510x protocol)

 Enabling external system log server setup in System properties > Logging is recommended. System stores logs in RAM memory by default due to limited flash storage. Rebooting or powering off the device will result in loss of log history.

## Secure your device's access

There are some possibilities to grant access to the device (or to any PC/Server):

1. ask for nothing: anybody who can establish a connection gets access
2. ask for username and password on an unsecured connection (e.g. telnet)
3. ask for username and password on an encrypted connection (e.g. SSH) (e.g. by following firstlogin)
4. ask for username and merely a signature instead of a password (e.g. SSH with signature.authentication)

If you ask for username/password, an attacker has to guess the combination. If you use an unencrypted connection, he could eavesdrop on you and obtain them.

If you use an encrypted connection, any eavesdropper would have to decrypt the packets first. This is always possible. How long it takes to decrypt the content, depends on the algorithm and key length you used.

Also, as long as an attacker has network access to the console, he can always run a bruteforce attack to find out username and password. He does not have to do that himself: he can let his computer(s) do the guessing. To render this option improbable or even impossible you can:

- not offer access from the Internet at all, or restrict it to certain IP addresses or IP address ranges
  - by letting the SSH server dropbear and the webServer lighttpd not listen on the external/WAN port
  - by blocking incoming connections to those ports (TCP 22, 80 and 443 by default) in your firewall
- make it more difficult to guess:
  - don't use the username root
  - don't use a weak password with 8 or less characters
  - don't let the SSH server dropbear listen on the default port (22)
- use the combination of:
  - username different than root
  - tell dropbear to listen on a random port (should be >1024): **System > Administration > Dropbear Instance > Port**
  - public key authentication. Your public keys can be specified in **Administration > System > SSHkeys**. An older guide to DropBear SSH public key authentication has detailed information on generating SSH keypairs which include the public key(s) you should upload to your configuration.

## Groups rights

If user is logged on via external server, its authentication level is acquired. As no direct mapping to existing users is used, authentication levels are a way to grant proper permissions for external users. WCC Lite uses a CISCOlike authentication system, meaning that there are fifteen different permission set level settings, of which the first 14 can be configured to enable or disable View and Edit permissions

## SSH Access

SSH Access of WCC Lite is made by Dropbear software package. To extend the basic functionality, Pluggable Authentication Module (PAM) for RADIUS is used. This enables user to add his own authentication modules as long as they are properly configured.

Fifteen levels of authorization are mapped for SSH access, meaning that user should be able to access SSH with credentials used to log into web interface. However, one should note that permissions in command line interface are not configurable via web interface. This means that first fourteen levels are restricted to basic permissions made by creating group by default. Highest level user has all the permissions root user has.

If a user intends to change permissions for user groups, it should be done via command line interfaces. It is only advised for advanced users.

## Web interface permissions

Fifteen levels of authorization permission are mapped for web interface access, meaning that user should be able to access web interface with credentials used to log into command line interface. User assigned to a highest authorization level group is able to access every possible screen therefore this group cannot be edited.

Figure below shows a screen containing already existing groups in a device. Pressing *Add New Group...* guides user to an *Edit group* screen, with *Edit* and *Delete* buttons respectively user can Edit and Delete configuration of a given user group.

Screen showing existing user groups

The screenshot shows the WCC LITE interface with the 'USERS' tab selected. Below the navigation bar, there are buttons for 'EDIT GROUPS' and 'EDIT USERS'. Under 'EDIT GROUPS', there are links for 'ADMINISTRATOR', 'VIEWER', 'ENGINEER', and 'OPERATOR'. A 'Save' button is visible. The main content area is titled 'Groups' and contains a 'GROUPS OVERVIEW' section. This section displays a table of existing groups with their authorization levels and a set of 'Actions' (Edit and Delete) for each group.

Groups	Status	Actions
administrator	Authorization level: 11	Edit Delete
engineer	Authorization level: 5	Edit Delete
operator	Authorization level: 3	Edit Delete
viewer	Authorization level: 1	Edit Delete

At the bottom of the overview section, there is a button labeled 'Add New Group...'.

Screen for user group editing

## administrator

### Group Configuration Options

The screenshot shows the 'Group Configuration Options' for the 'administrator' group. It includes fields for 'Group Name' (set to 'administrator') and 'Access level' (set to '11'). A help text explains the access level: 'Access level this group refers to. Use with external PAM module (e.g. RADIUS)'. Below these fields, there are several sections for enabling menus and services, each with checkboxes for 'View', 'Edit', and other actions. At the bottom, there is an 'Add' button for additional fields.

**Group Name:** administrator

**Access level:** 11

**Access level this group refers to. Use with external PAM module (e.g. RADIUS)**

**Enable Users menus**

- ☒ View ☒ Edit
- ☐ Password ☒ Edit groups ☐ Edit Users

**Enable Services menus**

- ☒ View ☒ Edit
- ☒ GSM Pinger ☒ Telemetry agent
- ☒ ser2net ☒ OpenVPN ☒ IPsec API

**Enable Status menus**

- ☒ View ☒ Edit
- ☒ Firewall ☒ Routes ☒ System Log
- ☒ Kernel Log ☒ Processes ☒ Realtime Graphs
- ☒ VnStat Traffic Monitor

**Enable Network menus**

- ☒ View ☒ Edit
- ☒ Interfaces ☒ Wireless ☒ DHCP and DNS
- ☒ Hostnames ☒ Static Routes ☒ Firewall
- ☒ Diagnostics ☐ VnStat Traffic Monitor

-- Additional Field -- **Add**

**Buttons:** Back to Overview, Save & Apply, Save, Reset

Edit group screen for an individual group can be seen in Figure above. Group name doesn't have any specific purpose for RADIUS, but it enables naming groups with words most meaningful for a given context. Access level values can only be integers between 1 and 14, other values will result in an error messages; only unconfigured levels are shown in a dropdown list when configuring. Other fields are dedicated for an individual menu configuration. To add more first level menus user should select from a dropdown list at the bottom named *--Additional Field--* and press Add.

Permissions for web interface are split into two parts: *View* and *Edit*.

*View* permissions can be assigned to second level menus meaning that only allowed subtabs are shown for a user. Selecting *View* checkbox show more parameters containing all the subtabs (submenus). If a user can access a given screen, it means all of the actions in that screen are available to be executed. Therefore, if a user with a lot of restrictions shouldn't, for example, import Excel configuration to WCC Lite, a tab containing this action (*Protocol Hub->Configuration*) should be disabled in his groups' configuration.

*Edit* permissions can be assigned to first level menus meaning that if this permission is given, every configuration in the first level menu can be saved and applied successfully

## Conformance to IEC 62351 standard

IEC 62351 is a standard developed by WG15 of IEC TC57. This is developed for handling the security of TC 57 series of protocols including IEC 608705 series, IEC 608706 series, IEC 61850 series, IEC 61970 series and IEC 61968 series. The different security objectives include authentication of data transfer through digital signatures, ensuring only authenticated access, prevention of eavesdropping, prevention of playback and spoofing, and intrusion detection.

Conformance to IEC 62351 standard of WCC Lite devices is described in a table below.

Conformance to IEC 62351 standard

Standard	Description	Topic	Implemented	Version
IEC 62351-3	Security for any profiles including TCP/IP	TLS Encryption	Yes	>=1.3
		Node Authentication by means of X.509 certificates	Yes	>=1.3
		Message Authentication	Yes	>=1.3
IEC 62351-4	Security for any profiles including MMS	Authentication for MMS	Yes	>=1.5
		TLS (RFC 2246)is inserted between RFC 1006 & RFC 793 to provide transport layer security	Yes	>=1.5
IEC 62351-5	Security for any profiles including IEC 608705	TLS for TCP/IP profiles and encryption for serial profiles	No	
IEC 62351-6	Security for IEC 61850 profiles	VLAN use is made as mandatory for GOOSE	No	
		RFC 2030 to be used for SNTP	No	
IEC 62351-7	Security through network and system management	Defines Management Information Base (MIBs) that are specific for the power industry, to handle network and system management through SNMP based methods	No	
IEC 62351-8	Role-based access control	Covers the access control of users and automated agents to data objects in power systems by means of rolebased access control (RBAC)	Yes	>=1.2.6
IEC 62351-9	Key Management	Describes the correct and safe usage of safety--critical parameters, e.g. passwords, encryption keys.	No	
		Covers the whole life cycle of cryptographic information (enrolment, creation, distribution, installation, usage, storage and removal)	No	
		Methods for algorithms using asymmetric cryptography	No	

		A secure distribution mechanism based on GDOI and the IKEv2 protocol is presented for the usage of symmetric keys, e.g. session keys	No	
IEC 62351-10	Security Architecture	Explanation of security architectures for the entire IT infrastructure	No	
		Identifying critical points of the communication architecture, e.g. substation control center, substation automation	No	
		Appropriate mechanisms security requirements, e.g. data encryption, user authentication	No	
		Applicability of wellproven standards from the IT domain, e.g. VPN tunnel, secure FTP, HTTPS	No	
IEC 62351-11	Security for XML Files	Embedding of the original XML content into an XML container	No	
		Date of issue and access control for XML data	No	
		X.509 signature for authenticity of XML data	No	
		Optional data encryption	No	

🔄Revision #2

★Created 7 October 2022 10:35:58 by Lukas Taroza

✎Updated 7 October 2022 11:09:21 by Lukas Taroza