Add ssh-key

Functionality

The SSH key functionality in the WCC Lite device allows you to authenticate securely without needing to enter a password each time you access the device via SSH. This method uses public-key cryptography to ensure a secure connection.

This feature enables you to paste public SSH keys into the provided interface, granting access to users whose private keys match the uploaded public keys. This enhances security and simplifies the login process.

> The add SSH key functionality was implemented in WCC Lite starting from firmware version v1.9.3.

Generating SSH Keys

To use this functionality, you first need to generate an SSH key pair on your local machine. Here are the steps for generating a key pair:

1. **Open a terminal window**.
2. **Run the following command**:

```
ssh-keygen
```

3. **Follow the prompts**:

- You will be asked to enter a file in which to save the key. Press Enter to accept the default location.
- Enter a passphrase for additional security, or leave it empty for no passphrase

```
elseta@DESKTOP-GGQNK51 ~> ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/elseta/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/elseta/.ssh/id_rsa
Your public key has been saved in /home/elseta/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:bqYxJA                              RPKOFkDc elseta@DESKTOP-GGQNK51
The key's randomart image is:
+---[RSA 3072]----+
|     .oo+=@o     |
|    . o+ EoX     |
|  + . .O B o     |
| . +  o *        |
```

4. The generated keys will be saved in the `.ssh` directory in your home folder. The public key will be named `id_rsa.pub` and the private key `id_rsa`.

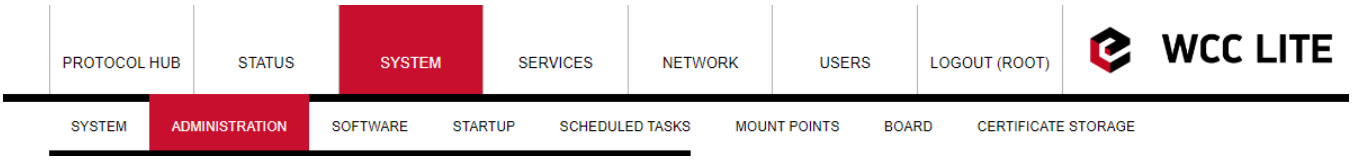
Adding the Public Key to the WCC Lite Device

1. Copy the content of your public key:

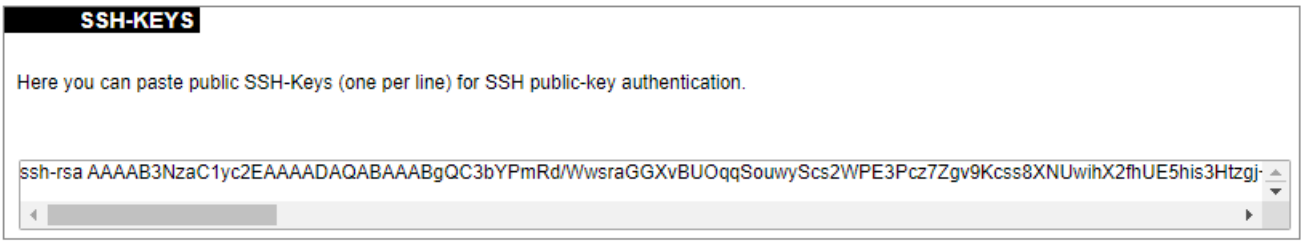
```
cat ~/.ssh/id_rsa.pub
```

```
elseta@DESKTOP-GGQNK51 ~> cat .ssh/id_rsa.pub
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQC3bYPmRd/WwsraGGXvBUOqqSouwyScs2WPE3Pcz7Zgv9Kcss8XNUwihX2fhUE5his3Htzgj+VXAwazaWB9
VjRAd4bAXVm9iGXSEUkwDpkCrMxsLbXC0p9m3+BCbVPPiGkOepZgNoo3QuBPzV9nJPUJ2zFYkBeTKWM+r4UzKruIOAB3XuCpQOMvJF8ksA5k4vxd7NbVEMao
Pot6RMr7JoT8Ia/JI6RMJ4op9PiyZ9EgAQbV/TE7T7/5bqgOHTloMXfjSV0M14z4lkqX/nFBfZtA3Z+nX0iYROY0gFLUK+1SxVyE2qNXwpXuJwqAsdcfMljJ
ZazQZwJSRDXg6ckpGnwV5ZflIeJWwQJkVYJ9fP75edhl4bZxrU+zMYgk6Eb91b92jJI4NYJgm8YXVOtE41iutX1mRDFq2Gex8+Yzli6F19NbSyeCovLSk8jx
Sqh+hZzGUbqoF3uml0l56c9Oy1YAf+RrHvBb1chHEwm6s2ApoOcUJo7/SUBFZob6CVduk2c= elseta@DESKTOP-GGQNK51
```

2. Access the WCC Lite web interface and navigate to the SSH-KEYS section *System -> Administration*



3. Paste the copied public key into the text box provided. Ensure that each key is on a new line if you are adding multiple keys.



4. Save the changes to apply the new keys.

Using the SSH Key for Authentication

After adding the public key to your WCC Lite device, you can now authenticate using the corresponding private key without entering a password.

1. Open a terminal window.
2. Use the SSH command to connect to your device:

```
ssh root@192.168.1.1
```

⚠ Replace `root` with the username (which is `root` in this case) and `192.168.1.1` with the IP address of your WCC Lite device.

You should now be able to access the WCC Lite device securely and conveniently using your SSH key pair.

Revision #8
★Created 22 July 2024 12:20:56 by Tomas
Updated 5 December 2024 15:00:33 by Tomas