

CIPHRA

Users Manual



2019-03-26
Revision 2
Original Users Manual

AUTHENTICO
TECHNOLOGIES

Table of Contents

1.	Overview	4
1.1.	Objective of this document	4
1.2.	Delivery content.....	4
1.3.	Labeling.....	4
1.4.	Technical data	4
1.5.	Break-in protection.....	4
2.	First installation	5
3.	Features	6
3.1.	Implementation.....	6
3.1.1.	Back-Up	7
3.1.2.	Migration	7
3.1.3.	Scalability.....	7
3.1.4.	API	7
4.	Hardware	8
5.	Software.....	9
5.1.	Log in.....	9
5.2.	Dashboard.....	9
5.3.	Network.....	10
5.4.	Firmware.....	10
5.5.	Device key.....	11
5.5.1.	Create device key.....	11
5.5.2.	Import device key	12
5.5.3.	Reset device key.....	13
5.6.	Log	13
6.	RS232 connection	14

1. Overview

1.1. Objective of this document

The objective of this document is to provide a guide to the CIPHRA installation and administration.

1.2. Delivery content

- 1 CIPHRA by Authentico for 19" rack mounting
- 2 Power supply units
- 1 Users Manual

1.3. Labeling

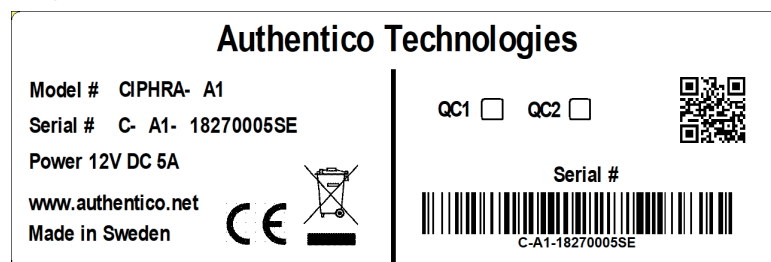


Illustration 1. Data label (example)

1.4. Technical data

Power supply	12 VDC, 5 A
Dimensions (w x h x d)	484 x 90 x 316 mm
Default user ID	admin
Default password	CIPHRA
Port	80
IP address	192.168.0.20/24
RS232 baud rate	115200/N81
RS232 log in	cilla

1.5. Break-in protection

CIPHRA is equipped with a break-in protection. If the cover is opened all information will be instantaneously deleted.

2. First installation

1. Install the CIPHRA by Autentico in a 19" rack.
2. Connect to the net-work via the ethernet port.
3. Connect the power supply. For redundancy use two power supply units.
4. Open a webbrowser on a computer connected to the network and connect to the IP address, see '1.4. Technical data' on page 4.
5. Log in to the dashboard.
6. Select *Device key* in the menu panel.
7. Select *Create device key*. Type a device key password you select.
Keep the device key password in a safe place. It is not possible to import a device key without the present password. See '5.5.2. Import device key' on page 12.
8. Download the device key to non-network connected media. Store the device key in at least two different places.

3. Features

CIPHRA is a hardware dependent cryptographic processor that ensures that passwords and encryption keys are essentially impossible to steal even if a database is stolen.

CIPHRA is based on a technology called PUF – (physically unclonable functions) which are physical objects that exploit the unavoidable variations introduced during the manufacturing of integrated circuits.

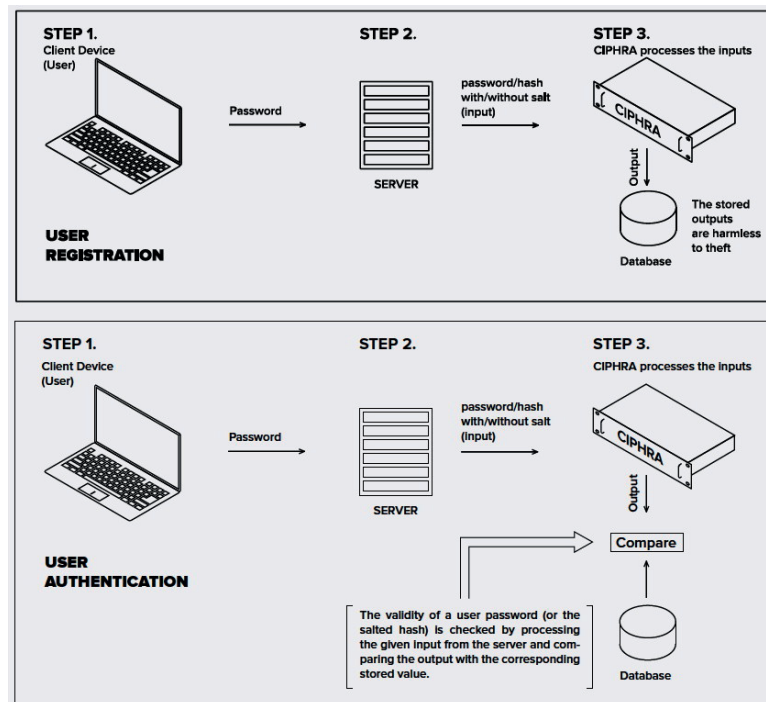


Illustration 2. CIPHRA Solution

CIPHRA processes user passwords (or the salted password hashes) and then returns the output to be stored in a database. CIPHRA's cryptographic processor checks the validity of a user password by processing the password (or its salted hash) and comparing the output with the corresponding stored value. CIPHRA processes the passwords with a unique device key protected by a SRAM-PUF key.

3.1. Implementation

The CIPHRA appliances are designed to be plug-and-play solutions. The organization's administrator needs to insert a device key in the CIPHRA only once. It is not possible to get the inserted key out from the CIPHRA appliance. If an installation process is not successful for any reason the installed device key is erased, so a new device key must be inserted.

3.1.1. Back-Up

CIPHRA's root key does not require any backup and is never stored. But additional CIPHRA appliances can function as hardware redundancy if the same device key is inserted in multiple CIPHRA appliances. This facilitates the CIPHRA customers to recover from unforeseen hardware failures.

3.1.2. Migration

To migrate from a salted password hash database to CIPHRA, the server just needs to pass the hash together with the salt to CIPHRA and store the output from CIPHRA. Then, the old hashed password database is deleted. When a user attempts to login, the user password is first hashed and then passed along to the CIPHRA appliance, the output from which is then compared with the previously stored value.

3.1.3. Scalability

CIPHRA appliances come in different versions depending on the customer requirements. The minimum throughput is around 20 000 authentication requests per second per appliance. If an organization wants to increase the number of login requests that can be handled per second, additional units can be added for redundancy and also to increase the throughput to as the required level.

3.1.4. API

CIPHRA communicates over HTTPS using REST-API.

4. Hardware

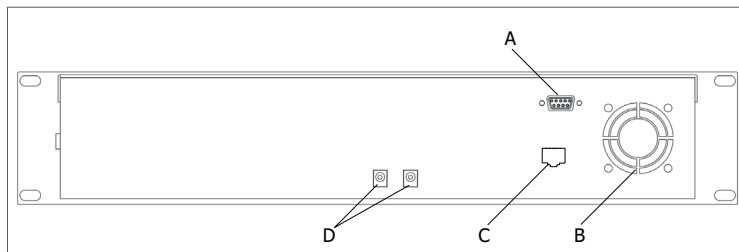


- A. Power indicator
- B. Status indicator

Illustration 3. Front view

The power indicator (A) lights when power supply is connected.

The status indicator (B) lights if an error appears.



- A. RS 232 port
- B. Cooling fan
- C. Ethernet port
- D. Power supply connectors

Illustration 4. Rear view

The primary communication is via the ethernet port (C). It is possible to use the RS232 port for simplified communication, such as re-boot.

The two power supply connectors (D) are for redundancy to secure uninterrupted operation. To increase the redundancy connect the power supply units to separated brances.

5. Software

Primary communication with CIPHRA is via internal network and the ethernet port by using a web browser. An overview of the interface and the different views are described in the following. See also '2. First installation' on page 5 for the installation process.

5.1. Log in

After the IP address is inserted this view will appear. See '1.4. Technical data' on page 4 for default log in information.

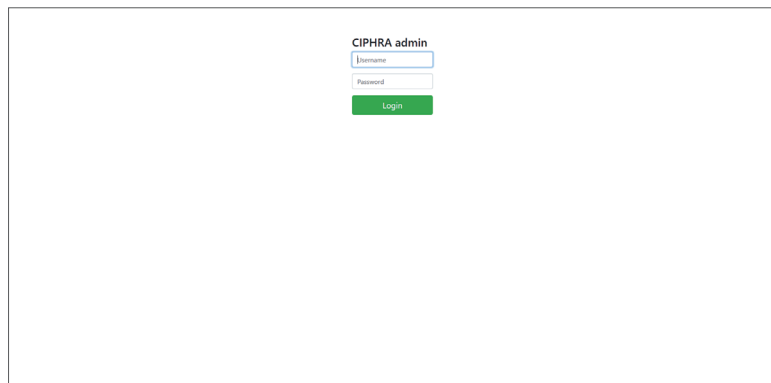


Illustration 5. Log in view

5.2. Dashboard

The first screen you meet after log in is the Dashboard view, showing the status of CIPHRA.

In the upper right corner drop down menu you will find functions for Log out and password changing.

We strongly recommend you to change the password.

To the left you find the menu panel. In the following chapters you will find descriptions of the different views.

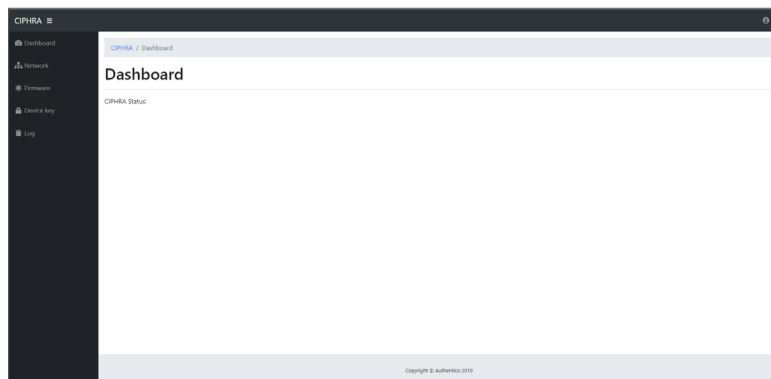


Illustration 6. Dashboard view

5.3. Network

In the Network view you set the parameters *IP address*, *Gateway* and *VLANID* for the Public API address.

To use a different Management IP, check in the *Configure management on separate IP address* and set the management parameters.

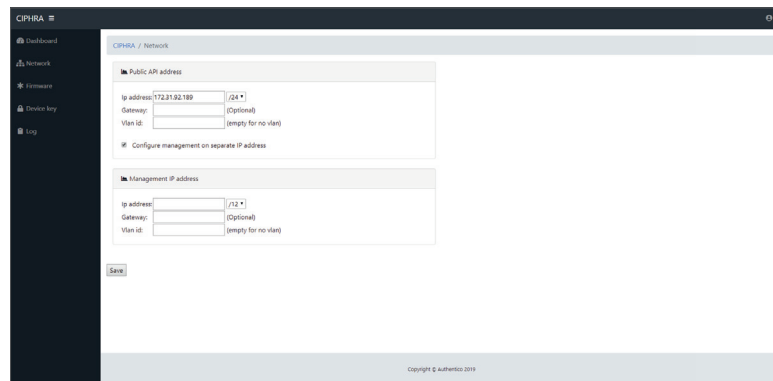
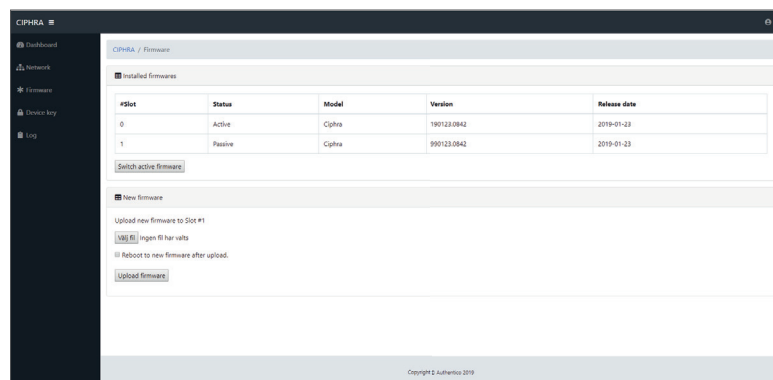


Illustration 7. Network view

5.4. Firmware

In this view you upload and select firmware. The new firmware will be placed in the passive slot.

CIPHRA will be delivered with current firmware installed.



Slot	Status	Model	Version	Release date
0	Active	Ciphra	990123.0842	2019-01-23
1	Passive	Ciphra	990123.0842	2019-01-23

Illustration 8. Firmware view

5.5. Device key

In the Device key view it is possible to create, import and reset the device key.

You always need a device key to run CIPHRA. For how to create a new device key at start up see '2. First installation' on page 5.

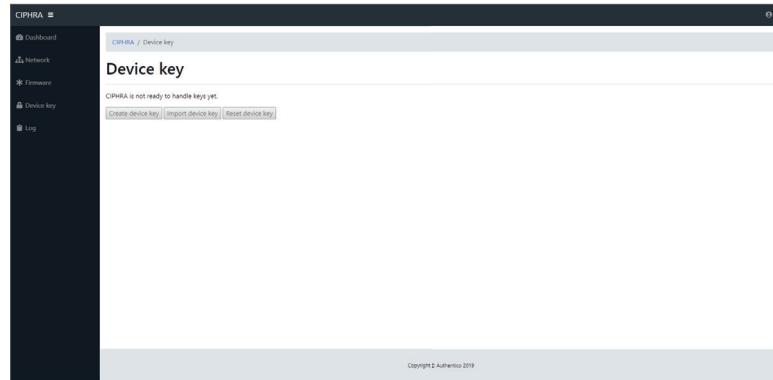


Illustration 9. Device key view

5.5.1. Create device key

Chose a strong password. It is important to keep the password in case of the need to restore the device key.

Keep the device key password in a safe place. It is not possible to import a device key without the present password. See '5.5.2. Import device key' on page 12.

When using multiple CIPHRA units, all the units must have the same device key.

Illustration 10. Create device key view

5.5.1.1. Device key receipt

This receipt shows the device key and give you the opportunity to save it.

Always store the device key on non-network connected unit, i.e. USB flash drives. It is also possible to print out or save a screen dump.

We strongly recommend having at least two copies, stored in different locations.

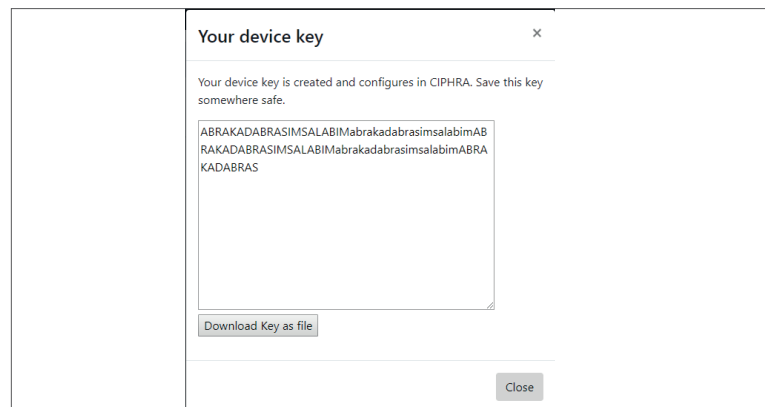


Illustration 11. Device key report

5.5.2. Import device key

To import a device key you need the device key password and the file stored as described in '5.5.1. Create device key' on page 11. It is also possible to type the string in the *Enter device key* field.

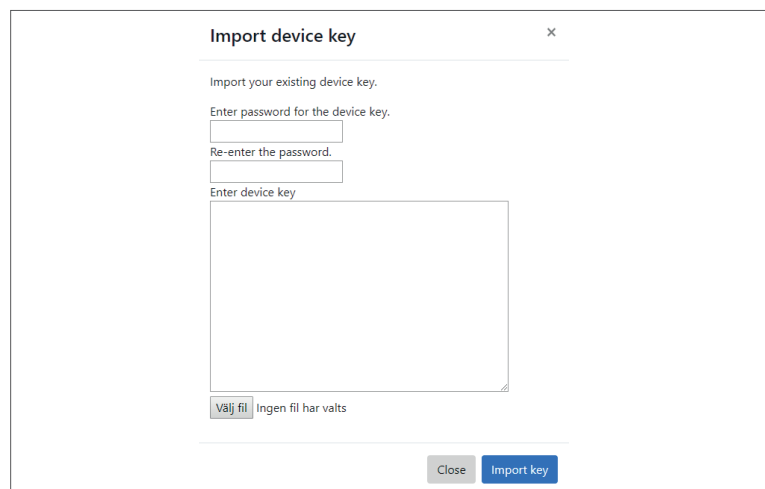


Illustration 12. Import device key dialog box

5.5.3. Reset device key

When resetting the device key CIPHRA will lose its functionality. The only way to get it up and running is to import the current device key.

Only use this function after dialog with our support team.

5.6. Log

The log view is used to create a log for troubleshooting. In case of support needed, the log file shall be send to our support team for analysis.

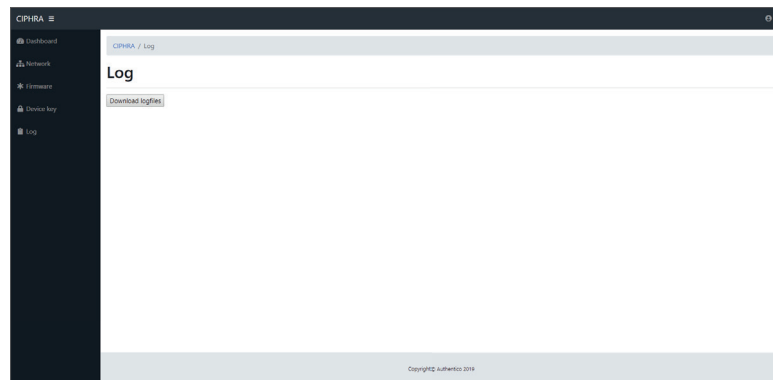


Illustration 13. Log report view

6. RS232 connection

The CIPHRA is utilized with an RS232 connection for administration. Only use the RS232 if these parameters need to be set.

- Change the IP address.
- Reset the log in user and password to factory settings.

Authentico AB
www.authentico.net
Erik Dahlbergsgatan 4, Apartment 6
411 26 Gothenburg
SWEDEN

AUTHENTICO
TECHNOLOGIES