Manuals+ — User Manuals Simplified.

SHARP PN-LA862 Interactive Display Secure Command Instruction Manual

Home » Sharp » SHARP PN-LA862 Interactive Display Secure Command Instruction Manual

Contents

SHARP

SHARP PN-LA862 Interactive Display Secure Command

Product Information

Specifications

- Product Models: PN-LA862, PN-LA752, PN-LA652
- Communication Method: LAN (Local Area Network)
- Control Method: Secure Communication via Network
- Supported Public Key Methods: RSA(2048), DSA, ECDSA-256, ECDSA-384, ECDSA-521, ED25519
- Software Compatibility: OpenSSH (standard on Windows 10 version 1803 or later and Windows 11)

Product Usage Instructions

Creating Private and Public Keys

Private and public keys are required for secure communication. The following instructions explain how to create an RSA key using OpenSSH on Windows:

1. Open a command prompt from the Start button.
2. Enter the following command to create the key:

```
C:ssh-key>ssh-keygen.exe -t rsa -m RFC4716 -b 2048 -N user1 -C rsa_2048_user1 -f id_rsa
```

1. The private key (id_rsa) and public key (id_rsa.pub) will be created. Keep the private key in a safe place.

Registering a Public Key

To register the public key with the device, follow these steps:

1. Set HTTP SERVER to ON in ADMIN > CONTROL FUNCTION on the Settings menu.
2. Press the INFORMATION button on the monitor and note the IP address displayed in Product Information 2.
3. Enter the IP address of the monitor in a web browser to display the login page.
4. Login as an administrator using the default User Name: admin and Password: admin.
5. If prompted, change the password.
6. Click on NETWORK – COMMAND menu.
7. Enable COMMAND CONTROL and SECURE PROTOCOL and click APPLY.
8. Set USER1 – USER NAME to user1 (default).
9. Enter the symbol name of the key to be registered in PUBLIC KEY
   USER1, and click REGISTER to add the public key.

Command Control via Secure Communication Protocol

This device can be controlled via secure communication using SSH authentication and encryption functions. Before proceeding with command control, make sure you have created the private and public keys as explained in the previous sections.

1. Go to NETWORK – COMMAND menu on the web page.
2. Enable COMMAND CONTROL and SECURE PROTOCOL.
3. Click APPLY to save the settings.

FAQ

Q: What methods of public keys are supported by this monitor?

A: This monitor supports RSA (2048-bit), DSA, ECDSA-256, ECDSA-384, ECDSA-521, and ED25519 public key methods.

Q: Which software is compatible with this monitor for creating private and public keys?

A: OpenSSH is available as standard on Windows 10 (version 1803 or later) and Windows 11.

Controlling the Monitor via Secure Communication (LAN)

You can control this monitor with secure communication from a computer via network.

TIPS

- This monitor must be connected to a network.
- Set “LAN Port” to ON in “ADMIN” > “COMMUNICATION SETTING” on the Setting menu and configure network settings in “LAN SETUP”.
- Set “COMMAND (LAN)” to ON in “ADMIN” > “CONTROL FUNCTION” on the Setting menu.
- The settings for the commands are set in “NETWORK -COMMAND” on the web page.

Control via secure communication
User authentication and encrypted communication can be performed using public key cryptography. To perform secure communication, a private key and public key must be created in advance, and the public key must be registered with the device. Client software that supports secure communication is also required. N-format commands and S-format commands are used to control this device. Please also read the instructions for each format.

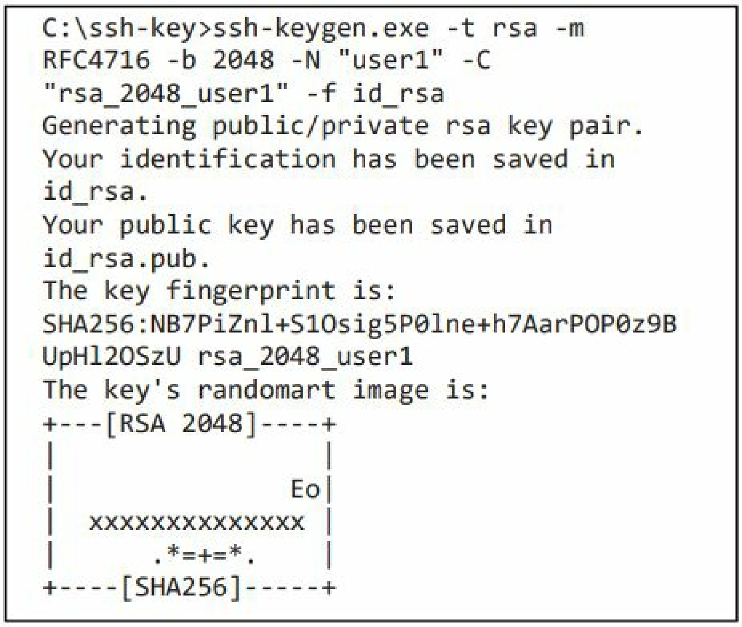
Creating Private and Public Keys
Use OpenSSL, OpenSSH, or a terminal software to create private and public keys. The following public key methods are supported in this monitor.

RSA(2048 4096bit)
DSA
ECDSA-256
ECDSA-384
ECDSA-521
ED25519

OpenSSH is available as standard on Windows 10 (version 1803 or later) and Windows 11. This section describes the procedure for creating an RSA key using OpenSSH (ssh-keygen) on Windows.

1. Open a command prompt from the Start button.
2. Send the following command to create the key with the following setting:

key type:	RSA
length:	2048bit
passphrase:	user1
public key comment:	rsa_2048_user1
file name:	id_rsa

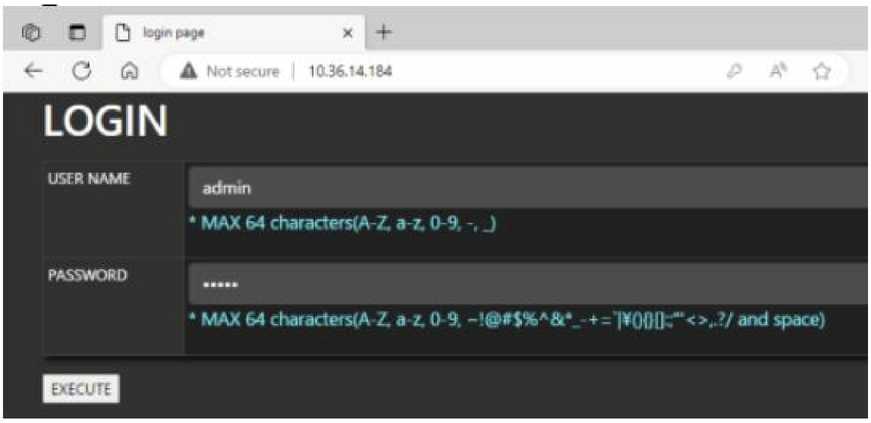


```
C:\ssh-key>ssh-keygen.exe -t rsa -m
RFC4716 -b 2048 -N "user1" -C
"rsa_2048_user1" -f id_rsa
Generating public/private rsa key pair.
Your identification has been saved in
id_rsa.
Your public key has been saved in
id_rsa.pub.
The key fingerprint is:
SHA256:NB7PiZnl+S1Osig5P0lne+h7AarPOP0z9B
UpHl2OSzU rsa_2048_user1
The key's randomart image is:
+---[RSA 2048]----+
|                 |
|               Eo|
|  xxxxxxxxxxxxxx |
|      .*=+=*.    |
+----[SHA256]-----+
```

3. “id_rsa” – private key and “id_rsa_pub” – public key will be created. Keep the private key in a safe place. For details of the commands, please refer to the description of each tool.

Registering a public key
Register the public key on the Web page of the device.

1. Set “HTTP SERVER” to ON in “ADMIN” > “CONTROL FUNCTION” on the Settings menu.
2. Press the INFORMATION button and check the IP address of the monitor in Product Information 2.
3. Enter the IP address of the monitor in the Web browser to display the login page.
4. Enter User Name: admin Password: admin (default) to login as administrator.



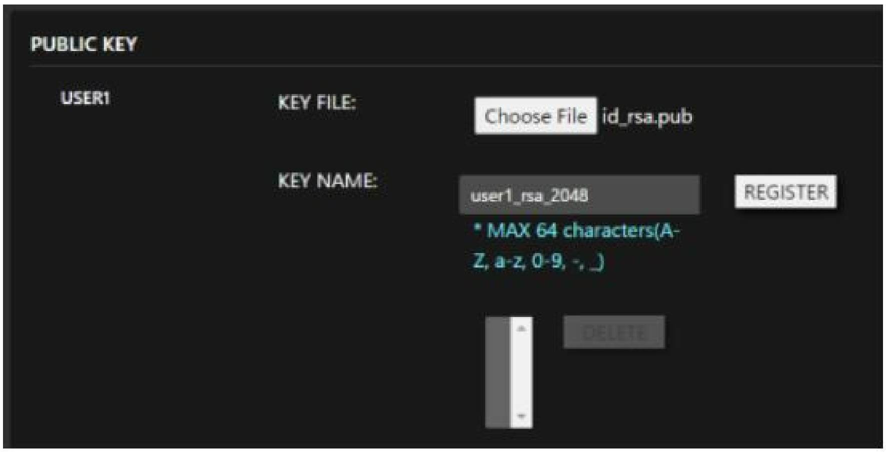
LOGIN

USER NAME: admin
* MAX 64 characters(A-Z, a-z, 0-9, -, _)

PASSWORD: •••••
* MAX 64 characters(A-Z, a-z, 0-9, -!@#$%^&*_-+=`|¥(){}[]:;"'<>,.?/ and space)

5. When logging in for the first time, you will be asked to change your password.
6. Click “NETWORK – COMMAND” menu.

7. Set “COMMAND CONTROL” to ENABLE
8. Set “SECURE PROTOCOL” to ENABLE and push APPLY button.
9. Set “USER1 – USER NAME” to user1 (default).
10. Enter the symbol name of the key to be registered in “PUBLIC KEY – USER1”, and REGISTER the public key you just created.



PUBLIC KEY

USER1

KEY FILE: id_rsa.pub

KEY NAME: user1_rsa_2048

* MAX 64 characters(A-Z, a-z, 0-9, -, _)

Command control via secure communication protocol

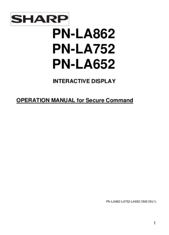
This device can be controlled via secure communication using SSH authentication and encryption functions. Implement “Creating Private and Public Keys” and “Creating Private and Public Keys” procedure before.

1. Click “NETWORK – COMMAND” menu on the web page. Enable “COMMAND CONTROL” and “SECURE PROTOCOL” and push APPLY button in ” NETWORK -COMMAND “
2. Connect the computer to the monitor.
    1. Start SSH client, specify the IP address and data port number (Default setting: 10022) and connect the computer to the monitor.
    2. Set the user name and the private key for the registered public key, and enter the passphrase for the private key.
    3. If the authentication is successful, the connection is established.
3. Send commands to control the monitor.
    1. Use N-format or S-format commands to control the monitor. For details on commands, refer to the manual for each format.

TIPS

- If “AUTO LOGOUT” is on, the connection will be disconnected after 15 minutes of no command communication.
- Up to 3 connections can be used at the same time.
- Normal and secure connections cannot be used at the same time.

Documents / Resources

 SHARP PN-LA862 PN-LA752 PN-LA652 INTERACTIVE DISPLAY OPERATION MANUAL for Secure Command PN-LA862-LA752-LA652 OM2 EN(1) 1	**SHARP PN-LA862 Interactive Display Secure Command** [pdf] Instruction Manual PN-L862B, PN-L752B, PN-L652B, PN-LA862 Interactive Display Secure Command, PN-LA862 , Interactive Display Secure Command, Display Secure Command, Secure Command, Command

References

- **User Manual**