SHARP

PN-LM551
PN-LM431

LCD MONITOR

OPERATION MANUAL for Secure Command

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 "Ethernet" or “Wireless LAN” to ON in "Admin Settings" > "Network" on the Setting menu and configure network settings in "Ethernet" or “Wireless LAN”.
- Set "Monitor Control via Network" to ON in "Admin Settings" > "Network" > "Monitor Control"
- When “Power Save Settings - Mode“ is set to “Low Power” and “Quick Start” is set to off, the control is disabled in the standby state or input signal waiting state.

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 Setting menu of the monitor.

(1) Copy the public key file (id_rsa.pub in the example above) to the USB flash drive.
(2) Connect the USB flash drive to the USB1 terminal of the monitor.
(3) Set "Use Secure Protocol for Authentication " to ON in "Admin Settings" > "Network" > "Monitor Control" on the Setting menu.
(4) Select "Upload" for "Public Key File" and the file selection screen will be displayed.
(5) Select the public key file on the USB flash drive to register the public key.
Registered public key files can be downloaded and deleted.

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) 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 (Default setting: Admin) 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.

(2) 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 there is no command communication after the “Auto Logout Time” (Default value: 5 minutes), the connection will be automatically disconnected.
- Up to one connection can be used at the same time.
- Normal and secure connections cannot be used at the same time.