

# Importing Device Setting Information on the Server

---

By managing the device setting information on the server, you can regularly apply (import) the settings to the machine.

Use the device management server or web server.

To use the device management server, see the device management server manual.

To use the web server, open the device setting information CSV file, change the data displayed under "ModuleID" to "-", and store it on the web server. For details, contact your sales representative.

The following explains how to specify and operate the related settings on machines.

## Periodically Importing Device Setting Information

This setting automatically imports the device setting information stored on a server to the machine.

1. Log in from the control panel as an administrator with user administrator, machine administrator, network administrator, and file administrator privileges.
2. Press [System Settings].
3. Press [Administrator Tools].
4. Press [▼Next] or [▼] repeatedly until [Device Setting Information: Import Setting (Server)] appears.
5. Press [Device Setting Information: Import Setting (Server)].
6. Select [Device Mangmnt Server] or [Web Server].  
[Device Mangmnt Server] cannot be selected from the machine. Enable it from the device management server.
7. Press [Server Settings] or [Change] for "Server Settings".  
Specify the server's URL, login user name, and password. In addition, specify the number of retries and an interval of time between them when importing fails.
8. Configure the import conditions.
  - Scheduled Import at Specified Time  
Select the frequency and specify the time for importing device setting information files.
  - Comparing New File to Last Import File (Cmprng. New Fl. to Last Imp. Fl.)  
Specify whether or not to import a device setting information file if it is identical as the last imported file.
  - Encryption Key (Change Encryption Key)  
Specify an encryption key.
  - Email Notification  
Specify whether or not to send an e-mail notification to the administrator when importing fails. To use Email Notification, it is necessary to specify "Auto Email Notification" in Web Image Monitor.
9. Press [OK].
10. Log out.

↓ **Note**

- If import fails, you can check the log for the error. The log is stored in the same location as the device setting information file.
- If the web server is in use, you can send the log file as an e-mail attachment to the administrator by setting [Email Notification] to [On].

## **Manually Importing the Device Setting Information File of a Server**

Manually import into the machine the device setting information file specified with [Device Setting Information: Import Setting (Server)].

1. Log in from the control panel as an administrator with user administrator, machine administrator, network administrator, and file administrator privileges.
2. Press [System Settings].
3. Press [Administrator Tools].
4. Press [▼Next] or [▼] repeatedly until [Device Setting Information: Run Import (Server)] appears.
5. Press [Device Setting Information: Run Import (Server)].
6. Press [OK].
7. Press [Exit].  
The machine restarts.

↓ **Note**

- The device setting information file is always imported without comparing it with the previous file.
- An import failure is not reported by e-mail.
- If import fails, you can check the log for the error. The log is stored in the same location as the device setting information file.

# Web Image Monitor Access Privileges

For details about using Web Image Monitor, see the Web Image Monitor help.

## [Device Setting Information: Import Setting (Server)]

Settings	Operation privileges
[Import File From]	Only an administrator with all privileges (user administrator, machine administrator, network administrator, and file administrator) can execute, change, or read these settings.
[Scheduled Import at Specified Time]	
[Comparing New File to Last Import File]	
[Email Failure Notification]	
[Number of Retries]	
[Retry Interval]	
[Encryption Key]	

## [Import Test]

Settings	Operation privileges
[Start]	Only an administrator with all privileges (user administrator, machine administrator, network administrator, and file administrator) can execute, change, or read these settings.